آموزش شبکه و امنیت شبکه

آموزش شبکه و امنیت شبکه

نویسنده:

مرتضی معتمدیفر

ناشر چاپی:

مرکز آموزش و تحقیقات صنعتی ایران

ناشر دیجیتالی:

مرکز تحقیقات رایانه‌ای قائمیه اصفهان

فهرست

آموزش شبکه و امنیت شبکه

مشخصات کتاب

سرشناسه : معتمدی‌فر، مرتضی، ۱۳۵۱ - عنوان و نام پدیدآور آموزش شبکه و امنیت شبکه و روش پیاده‌سازی استاندارد امنیت اطلاعات (ISO ۲۷۰۰۱) در ادارات و سازمانها (ISMS)/ گردآورنده و مولف مرتضی معتمدی‌فر. مشخصات نشر : تهران: مرکز آموزش و تحقیقات صنعتی ایران، ۱۳۸۹. مشخصات ظاهری : ۲۱۰ص.:جدول، نمودار. شابک : ۹۷۸-۹۶۴-۲۸۴۱-۳۰-۱ وضعیت فهرست نویسی : فیپا یادداشت : چاپ قبلی:۱۳۸۶(۱۸۲ص.) یادداشت : چاپ دوم. موضوع : تکنولوژی اطلاعات -- اقدامات تامینی -- استانداردها موضوع : حفاظت اطلاعات موضوع : شبکه‌های کامپیوتری -- اقدامات تامینی -- استانداردها موضوع : کامپیوترها -- ایمنی اطلاعات -- استانداردها رده بندی کنگره : T۵۸/۵/م۵۷۴ر۹ ۱۳۸۹ رده بندی دیویی : ۳۰۳/۴۸۳۳ شماره کتابشناسی ملی : ۲۲۱۳۵۴۵

آموزش شبکه

مقدمه

شبکه مجموعه ای از سرویس دهنده ها و سرویس گیرنده های متعددی می باشد که به یکدیگر متصل هستند. در این بین سرویس دهنده ها (server) نقش سرویس دهنده و خدمات دهی وسرویس گیرنده ها (Client) نقش سرویس گیرنده یا همان مشتری را بازی می کنند. انواع شبکه : شبکه ها را می توان به دو دسته ی «شبکه های محلی » LAN و شبکه های بزرگ تر از آن (WAN) تقسیم کرد. شبکه های محلی : Lcal Area Netwrk این نوع شبکه ها به شبکه های((LAN) معروف هستند. شبکه های محلی معمولا میزبان ۲ تا ۲۰کامپیوتر و در غالب Wrk Grup میباشند. سرعت این نوع شبکه بسیار زیاد است (معمولا ۱۰۰MB Per Sec) و می توان حجم داده های بالا ـ را در مدت بسیار کم انتقال داد. شبکه های گسترده : Wide Area Netwrk این نوع شبکه ها به شبکه های WAN معروف هستند. این شبکه ها بزرگتر از شبکه های LAN و اغلب برای امور عمومی از آن استفاده می شود. ازجمله این شبکه ها میتوان شبکه های VAN و یا شبکه های بزرگتر مانند Internet و.. را نام برد. سرعت انتقال داده ها در این نوع شبکه ها نسبت به LAN (در ایران) بسیار ناچیز میباشد. این سرعت به خاطر استفاده از خطوط ۵۶K است. البته می توان با استفاده از خطوط DSL یا ISDN و یا بی سیم Wire Less سرعت این ارتباط را به اندازه ۵۱۲ k , ۲۵۶ k ,۱۲۸K یا بالاتر افزایش داد. Internet Prtcl: IP IP یک عدد ۳۲ بیتی (bit) است که پس از اتصال به شبکه (... , LAN , Internet) به ما متعلق می گیرد. شکل کلی IP را می توان به صورت http://www.xxx.yyy.zzz در نظر گرفت که با هر بار اتصال به اینترنت به صورت Dial Up این عدد تغییر می کند. به عنوان مثال در حال حاضر IP ما ۲۱۳.۱۵۵.۵۵.۱۰۴ است اما در اتصال بعدی ممکن است این عدد به ۲۱۳.۱۵۵.۵۵.۲۰ تغییر کند. IP چه کاربردی دارد؟ IP به عنوان یک شناسنامه در شبکه است و کاربردهای بسیاری دارد .برای توصیف کامل IP نیاز به شرح TCP/IP است که بعدا به آن اشاره خواهیم کرد. همان طور که در جامعه شناسنامه وسیله ای برای احراز هویت ماست و بدون آن جزو آن جامعه محسوب نمی شویم ، IP نیز وسیله ای برای شناسایی ما در شبکه است و امکان اتصال به شبکه بدون آن وجود ندارد. به طور مثال هنگامی که در شبکه مشغول چت (Chat) هستیم ، کامپیوتر شما دارای یک IP می باشد. و جملاتی را که شما تایپ می کنید به وسیله مسیر یابها (Ruter) مسیر یابی (Ruting) شده و به کامپیوتر شخص مقابل میرسند و متنی را هم که شخص مقابل تایپ میکند روی IP شما فرستاده می شود. خط فرمان در

ویندوز چیست؟ خط فرمان یا همان" Cmmand Prmpt "در ویندوز نوعی شبیه ساز سیستم عامل Ds در ویندوز است که فایلهای اجرایی" exe,cm "در آن اجرا می شود. خط فرمان ویندوز دستورات بسیار زیاد و کاربردی دارد که به مرور زمان انها را خواهیم آموخت. دسترسی به خط فرمان در ویندوز: دسترسی به خط فرمان به دو روش میسر است. روش اول : روی Start Menu کلیک کرده و گزینه Run را انتخاب می کنیم . سپس در پنجره ظاهر شده اگر ویندوز شما ME/۹۸ باشد عبارت "Cmmand "و اگر XP/۲۰۰۰/۲۰۰۳ باشد عبارت" CMD "را تایپ می کنیم هم اکنون محیط Cmmand Prmpt در جلوی شما قرار دارد! روش دوم : با طی کردن مسیر Start> Prgrams>Accessries و کلیک کردن برروی Cmmand Prmpt این محیط برای شما باز میشود. ادامه مبحث IP : چگونه IPخود را بدست آوریم : برای بدست آوردن IP خود در سیستم عامل ویندوز کافی است همان طور که در بالا- توضیح داده شد به محیط Cmmand Prmpt رفته و عبارت" IPCNFIG " را تایپ کنیم. به طور مثال پس از اجرای دستور به نتایج زیر می رسید : ۰ Windws IP Cnfiguratin Ethernet adapter : IP Address. . . . . : ۲۱۳.۱۵۵.۵۵.۲۳۲ Subnet Mask . . . . . : ۲۵۵.۲۵۵.۲۵۵.۰ Default Gateway . . . . . : ۲۱۳.۱۵۵.۵۵.۲۳۲ فعلا تنها به سطر IP Address که با رنگ قرمز مشخص شده است توجه کنید (Default Gateway و Subnet Mask) بعدا برسی خواهد شد. ملاحظه میکنید که IP ما۲۱۳.۱۵۵.۵۵.۲۳۲ است. آدرسهای IP به چند دسته تقسیم می شوند؟ آدرسهای IP به پنج کلاس A,B,C,D,E تقسیم می شوند. از بین این کلاسها تنها کلاسهای A,B,C کاربرد دارند که به شرح آنها می پردازیم . کلاس A : تمام IP هایی که www آنها (در درس قبل شکل کلی IP را به صورت http://www.xxx.yyy.zzz معرفی کردیم) بین ۱ تا ۱۲۶ است ، جزو کلاس A محسوب می شوند. به عنوان مثال : ۱۱۲.۱۰.۵۷.۱۳ یک IP کلاس A است. این کلاس ویژه پایگاهای بزرگ اینترنتی است. کلاس B : تمام IP هایی که WWW آنها بین ۱۲۸ تا ۱۹۱ می باشد را شامل می شود. مانند IP ی ۱۷۲.۱۵۵.۵۵.۷۳ که جزو کلاس B است. کلاس C : این کلاس تمام IP هایی که WWW آنها بین ۱۹۲ تا ۲۲۳ است را شامل می شود: مانند ۲۱۳.۱۳۳.۵۲.۱۳۸ که جزو کلاس C محصوب می شود. تحلیل IP : همان طور که گفته شد IP یک عدد ۳۲ بیتی است. هم اکنون این گفته را کاملتر شرح داده و مطلب را بازتر می کنیم/ درک این قسمت از مطلب نیازمند دانستن مفاهیم Bit و Byte است . این در حقیقت واحدهای اندازه گیری حافظه کامپیوتر هستند که در پایین آنها را شرح می دهیم : BIT :به کوچکترین واحد اندازه گیری حافظه کامپیوتری می گویند. Byte: به مجموع ۸ بیت ، یک بایت می گویند. بنابر این نتیجه می گیریم ۳۲ بیت همان ۴ بایت در مبنای اعشاری (مبنای ۱۰) است و برای این که کامپیوتر اعداد را در مبنای ۲ در نظر می گیرد آن را به صورت Binary (مبنای ۲) می نویسیم. برای اینکه این مفاهیم را بهتر متوجه شوید آنها را در جدول برسی می کنیم. IP از چند قسمت تشکیل شده است؟ IP از دو قسمت Net ID و Hst ID تشکیل شده است و مقادیر بیت ها در این دو قسمت در کلاسهای مختلف IP متفاوت است. Net ID در واقع شناسه شبکه و Hst ID شناسه میزبان در IP است. برسی Net ID در کلاساهی مختلف: Net ID در کلاس A به صورت http://www.۰.۰.۰ یعنی تنها www را شامل می شود. در کلاس B به صورت : http://www.xxx.۰.۰ است یعنی http://www.xxx در واقع Net Id می باشد. و در کلاس C به صورت : http://www.xxx.yyy.۰ است یعنی NetID .. این رودیگه باید فهمیده باشید چیه) ; کلاس A : در کلاس Net ID : A هشت بیت است و Hst ID آن ۲۴ بیت که مجموعا ۳۲ بیت می شود. این کلاس می تواند ۱۶.۷۷۷.۱۴ میزبان (Hst) داشته باشد یعنی ۱۶.۷۷۷.۱۴ IP که زیر مجموعه آن قرار می گیرند. به عنوان مثال http://www.۴۴.۴.۱۳ که ۴۴.۴.۱۳ یکی از میزبان ها (Hst) می باشد. کلاس B : در کلاس NetID : B از هشت بیت به شانزده بیت افزایش می یابد و فضا را برای hst ID کمتر می کند، به همین دلیل IP های زیر مجموعه آن به ۵۶.۵۳۴ کاهش می یابد. به عنوان مثال http://www.xxx.۵۵.۱۳۷ : IP که ۵۵.۱۳۷ یکی از میزبانهاست . کلاس C : NetID باز هم

بزرگتر شده و از ۱۶ بیت در کلاس B به بیست و چهار افزایش می یابد و Hst ID به کوچکترین مقدار خود یعنی هشت بیت می رسد. این کلاس تنها ۲۴۲ IP را پشتیبانی می کند. به عنوان مثال http://www.xxx.yyy.۹۳ که در آن ۹۳ یکی از میزبانهاست. نکات مهم درس : ۱- سعی کنید بیشتر در محیط Cmmand Prmpt کار کنید تا به آن عادت کرده و دست خود را در اجرای دستورات سریع تر کنید. سرعت در اجرای دستورات هنگام Hack کردن بخصوص Client بسیار مهم است. ۲- با کمی دقت حتما متوجه می شوید که IP ای که www آن ۱۲۷ باشد در هیچ یک از کلاسهای مطرح شده وجود ندارد. در حقیقت IP ی ۱۲۷.۰.۰.۱ از قبل برای کامپیوتر خودمان رزرو شده و به آن Lcal Hst می گویند. ۳- هنگامی که به صورت Dial Up به اینترنت متصل می شوید معمولا IP کلاس C به شما تعلق می گیرد. ۴- توصیه و پیشنهاد برای استفاده از Cmmand Line ویندوز ۲۰۰۰ یا XP است.

بخش اول

آموزش شبکه –تعاریف اولیه شبکه تعریف شبکه های کامپیوتری (Cmputer Netwrk) : مجموعه ای از کامپیوتری خود مختار و مستقل که به یکدیگر متصل بوده و با هم تبادل اطلاعات می نمایند. تعریف اینترانت (Intranet) : شبکه های مربوط به یک سازمان یا مجموعه خاص که به صورت منطقی یا فیزیکی از اینترنت جدا می باشد.این شبکه ها معمولا ترکیبی از شبکه های LAN و WAN هستند.اینترانت ها ممکن است در نقاطی به اینترنت متصل باشند یا هیچ نقطه اتصالی به آنها نداشته باشند. تعریف اکسترانت (Extranet) : به لایه های ارتباطی و نقاط اتصال Intranet و Internet گفته می شود .اکسترانت ها از بعد امنیتی برای شبکه ها بسیار حیاتی می باشند . زیرا محلی هستند برای نفوذ به شبکه و ورود ویروسها . معمولا اطلاعات عمومی مربوط به اینترانت ها یا سازمانها در این قسمت ها قرار می گیرند. تعریف اینترنت (Internet) : مجموعه ای از شبکه های مستقل و مرتبط بهم می باشد که با هم تبادل اطلاعات می کنند و گستره آن تمام دنیا می باشد ، به عبارت دیگر Internet مجموعه ای از Internet ها (Internal netwrk) و یا مجموعه ای از Interanet ها و Extranet ها می باشد ، و بزرگترین WAN موجود در جهان می باشد . سخت افزار شبکه : سخت افزار شبکه را از دو دیدگاه مورد بررسی قرار می دهیم : دیدگاه تکنولوژی و دیدگاه سخت افزار/ مقیاس ۱- (Metr Palitian Netwrk) MAN ۲- (LAN (Lcal Area Netwrk ۳- WAN (Wide Palitian Netwrk) شبکه LAN : از خواص این نوع شبکه ها می توان سرعت و کارایی بالا و فواصل کم را نام برد.(حداکثر در حد چند کیلومتر یا چند صد متر) در این شبکه ها تعداد ایستگاههای کاری محدود بوده و شبکه به یک سازمان یا محیط یک اداره ، یک ساختمان محدود می شود. برخی از توپولوژی های مربوط به شبکه های محلی به قرار زیر می باشد: الف) توپولوژی خطی(BUS): در این نوع توپولوژی کلیه ایستگاهها از طریق یک کانال فیزیکی مشترک به یکدیگر متصل هستند و انتقال اطلاعات از طریق این کانال انجام می شود ، مزیت این پروتکل سادگی و هزینه پایین آن است و مشکل عمده آن سرعت و کارایی کانال می باشد. ب) توپولوژی حلقوی (Ring): در این نوع توپولوژی کلیه ایستگاهها در یک ساختار بسته حلقوی به یکدیگر متصل می شوند. در واقع در این شبکه کامپیوتر ها اطلاعات را دست به دست می نمایند و جهت چرخش اطلاعات در شبکه ثابت و به یک سمت می باشد. ج)توپولوژی ستاره (Star): در این توپولوژی یک دستگاه متمرکز کننده به عنوان هسته مرکزی شبکه وجود دارد. و سایر ایستگاهها مستقیما به این دستگاه متصل می شوند که شکل حاصل یک ستاره است به علت کارایی بالا و ارزان بودن تجهیزات امروزه این شبکه جایگزین سایر شبکه ها شده است. شبکه های (MAN Metrplitan Area Netwrk): معمولا شبکه های MAN با اتصال راه دور چندین شبکه محلی در مقیاس هایی مانند یک شهر در صورت امکان برای فواصل راه دور از فیبر نوری، اتصال بی سیم، خطوط اجاره ای و سایر امکانات LAN یا WAN

استفاده می شود. انتخاب نوع اتصال بستگی به شرایط محیطی ، زیر ساخت شهری و یا سیاستهای کلی سازمان دارد. شبکه های WAN: این نوع شبکه ها معمولا محدودیت مقیاس جغرافیایی ندارند، این شبکه ها از اتصال راه دور شبکه های کوچکتر بوجود آمده اند و دارای ساختار یکنواخت نیستند؛ زیرا اولا شبکه های محلی با توپولوژیهای مختلف پیاده سازی می شوند، ثانیا ماشینهای موجود در این شبکه ها از سخت افزار و نرم افزار متفاوتی استفاده می کنند و به طور ذاتی با هم سازگار نیستند. اصول طراحی شبکه و لایه بندی: برای طراحی شبکه ها معمولا از طراحی لایه ای استفاده می شود. دلیل این کار سادگی پیاده سازی و خطایابی می باشد. نمونه هایی از این طراحی ها مدل SI و TCP/IP می باشد، که در مورد آنها بیشتر خواهیم گفت. مدل SI: این مدل دارای هفت لایه زیر می باشد: ۱- Physical layer (لایه سخت افزاری) پایین ترین لایه می باشد . ۲- Data link layer ۳- Netwrk layer ۴- Transprt layer ۵- Sessin layer ۶- Presentatin layer ۷- Applicatin layer (لایه کاربردی) بالاترین لایه می باشد. هیچ یک از پروتکلهای واقعی پیاده سازی شده کاملا منطبق بر مدل SI نیستند.

بخش دوم

مدل TCP/IP: از این مدل در اکثر شبکه ها و برخی از کاربردهای صنعتی و اینترنت بکار برده می شود . این مدل دارای چهار لایه زیر می باشد: ۱-۴- (Netwrk access ۲-IP (Subnet R Internet ۳-TCP (Transprt R Hst t Hst Applicatin layer حال در مورد هر لایه مختصرا توضیحاتی می دهیم: ۱-اولین لایه، لایه دسترسی به شبکه یا Netwrk access می باشد که این لایه شامل رسانه ارتباطی (تجهیزات فیزیکی و کانالهای ارتباطی) و همچنین پروتکلهای ارتباطی برای انتقال قابها (Frameها) بر روی شبکه می باشد . ۲-لایه زیر شبکه / لایه اینترنت / لایه شبکه : وظیفه اصلی این لایه ایجاد ارتباط بین میزبانها می باشد. برقراری ارتباط بین میزبانها توسط این لایه بدون در نظر گرفتن ساختار لایه پایینی انجام می شود. این لایه باید دارای توانایی برقراری ارتباط در سطح شبکه محلی و گسترده باشد. لایه اینترنت از پروتکل IP برای انتقال اطلاعات استفاده می کند. در این لایه همچنین باید پروتکلهایی برای مسیریابی در شبکه و هدایت بسته ها وجود داشته باشد که برخی از آنها عبارتند از: Internet ، Ruting Infrmatin Prtcl ، Reverse Address Reslutin Prtcl ، Address Reslutin Prtcl Internet Grup Management Prtcl ، Cntrl Massage Prtcl و ۳ Internet Prtcl-لایه میزبان به میزبان / لایه انتقال: این لایه سرویسهای مورد نیاز برای ایجاد ارتباطات غیرقابل اطمینان را بوجود می آورد. ساختار این لایه از دو پروتکل TCP و UDP تشکیل شده است. ۳-۱- TCP: این پروتکل امکان ایجاد ارتباطات قابل اطمینان و اتصال گرا را فراهم می نماید. برخی از وظایف مربوط به این پروتکل به قرار زیر می باشد •: شکستن و تقسیم بندی داده ها و پشته های دریافتی از لایه بالاتر به بسته های TCP و ساخت مجدد پشته ها از بسته های TCP در مقصد • . حصول اطمینان از رسیدن بسته ها به مقصد • . بازبینی بسته ها و مرتب کردن آنها و کنترل خطا • کنترل جریان داده ها ۳-۲- UDP: این پروتکل برای فراهم آوردن مکانیزمی جهت کاهش و کم کردن سرریز داده ها در انتقال اطلاعات بکار می رود و معمولا برای ارتباطاتی که نیاز به قابلیت اطمینان ندارند استفاده می شود. لایه انتقال در سطح بالای خود با لایه کاربرد در ارتباط است.داده های تحویلی به لایه کاربرد توسط برنامه های کاربردی قابل دریافت می باشد ، همچنین این برنامه ها می توانند با استفاده از APIها (Applicatin Prgram Interface) مستقیما با لایه انتقال ارتباط برقرار کنند . ۴- لایه کاربرد : این لایه دارای پروتکلهای سطح بالایی برای استفاده ازپروتکلهای سطح پایین تر UDP و TCP می باشد که در این پروتکلها برای ایجاد سرویسهای اینترنتی بکارمی روند . برخی از این سرویسها به قرار زیر می باشند : الف) Telnet شبیه سازی پایانه ارتباطی : با استفاده از این پروتکل می توان یک ارتباط راه دور بین دو میزبان برقرار نمود و ترمینال یا پایانه را برای دو میزبان شبیه سازی می کند . این ترمینال راه دور کلیه امکانات یک ترمینال محلی را در اختیار قرارمی

دهد . ب) FTP (File Transprt Prtcl) انتقال فایل : با استفاده از این پروتکل کاربر قادر خواهد بود از راه دور از راه دور فایلها را از میزبانی به میزبان دیگر انتقال دهد . ج) SMTP مدیریت پست الکترونیک : این پروتکل استانداردی برای ارسال و دریافت پست الکترونیک برروی اینترنت می باشد . د) HTTP انتقال صفحات وب : ازاین پروتکل برای انتقال ابرمتنها بر روی اینترنت استفاده می شود . این متنها بر روی میزبانها به وسیله مرورگرها (Explrer) قابل نمایش هستند . با استفاده از این پروتکل می توان متن ، صدا ، تصویر ، تصاویر متحرک ، موسیقی و فیلم را بر روی شبکه انتقال داد . توجه داشته باشید که معمولاـ لفظ TCP/IP برای دو موضوع متفاوت بکار برده می شود : ۱- مدل TCP/IP که مدل چهار لایه آن بررسی شد . ۲- پشته TCP/IP یا پشته پروتکلهای TCP/IP که مجموعه ای است شامل بیش از ۱۰۰ پروتکل که برای سازماندهی اجزا اینترنت بکارمی رود .

بخش سوم

تجهیزات شبکه (Netwrk structure •) : سرویس دهنده ها (۱ : (Servers- حافظه های جانبی ۲ HDD- حافظه اصلی ۳ RAM- کارت شبکه ۴- پردازنده • تجهیزات خاص شبکه : ۱- تجهیزات خاص شبکه محلی : ۲ Switch ، Hub ، MAU- تجهیزات شبکه راه دور : Ruter ، Bridge ، Gateway سرویس دهنده ها : یک سرویس دهنده ، یک کامپیوتر پر قدرت در شبکه می باشد که یک سری از منابع خود را بر روی شبکه به اشتراک گذاشته و یا سرویسی بر روی آن نصب شده و در حال اجرا می باشد . آنچه برای یک سرویس دهنده در شبکه حائز اهمیت می باشد ؛ قابلیت اطمینان ، صحت و پیوستگی سرویسها است ، همچنین کارآیی یک سرویس دهنده از اهمیت ویژه ای برخوردار است . سرویس دهنده ها دارای پردازنده قوی و میزان RAM آنها دو تا چهار برابر حافظه های اصلی بر روی PCها است و همچنین دارای حافظه جانبی با سرعت و حجم بالا می باشند . تجهیزات شبکه های محلی (LAN) : در شبکه ها با گذرگاه مشترک اطلاعات بر روی کارت شبکه کلیه کامپیوترها قرار می گیرد و هر کامپیوتری که اطلاعات مربوط به آن باشد آنرا از روی شبکه بر می دارد . در این شبکه ها کلیه کامپیوترها به یک کانال مشترک وصل هستند . معمولاـ در این شبکه ها از کابل کواکسیال استفاده می شود و در هر لحظه فقط یک کامپیوتر می تواند اطلاعات ارسال نماید . به دلیل آسیب پذیر بودن این نوع توپولوژی (۲-Base۱۰ حالت استاندارد Ethernet) ساختارهای شبکه جدیدی بوجود آمد که با توپولوژی Star عمل مشابهی را انجام می داد . در این شبکه ها (T-Base۱۰) از دستگاهی به نام Hub استفاده می شود که گذرگاه شبکه را شبیه سازی و قدری از مشکلات روش قبل را حل کرده است . Hub : سخت افزاری است که اطلاعات را از روی یک پورت خود دریافت نموده و بر روی کلیه پورتهایش در روی شبکه Brad cast یا ارسال می کند . از Hub در شبکه هایی استفاده می شود که دارای توپولوژی شبکه Star باشند ؛ در این شبکه ها امکان برخورد اطلاعات وجود دارد . Switch : این ابزار در شبکه هایی با توپولوژی Star نصب می شوند و ساختار شبکه ای مشابه با ساختار قبل بوجود می آورند . تفاوتی که Switchها یا در واقع متمرکز کننده های مجهز به سیستم Switching با Hubها دارند این است که در این ابزارها بسته ها را در شبکه Brad cast نمی کنند بلکه کامپیوترهای متصل به هر پورت خود را تشخیص داده و یک بسته دریافتی را از مبدا مستقیما به سوی مقصد هدایت می نمایند . بنابراین در این شبکه ها امکان برخورد اطلاعات تقریبا به صفر رسیده و همچنین می توان شبکه های کوچکتر را به یکدیگر متصل نمود . MAU (Multi Access Unit) : سخت افزاری است که در شبکه های Ring استفاده می شود و یک شبکه حلقه را تبدیل به شبکه ای با توپولوژی Star – مانند آنچه Hub برای شبکه Bus انجام می داد – می نماید . تجهیزات شبکه Bridge : WAN : سخت افزاری است که پل ارتباطی دو LAN مختلف می باشد . تفاوت بین یک پل یا Bridge در تکنیک برقراری ارتباط بین دو LAN و Ruter در این است که Ruter در هر شبکه ای عمل مسیریابی را انجام می دهد و بر اساس IP مبدا و مقصد اطلاعات را در شبکه انتقال می

دهد اما یک Bridge که معمولا در شبکه های مخابراتی و بی سیم بکار می رود ، سخت افزار یا نرم افزاری است که اطلاعات از جنس لایه دوم یک شبکه (Frame) را در شبکه دیگر کپی می کند ؛ به عنوان مثال دو LAN می توانند به وسیله خط تلفن به یک دیگر متصل شوند . استفاده از Bridge کارایی شبکه را تا حد زیادی کاهش می دهد و باعث کندی شبکه می شود . پلها اصولا در شبکه هایی استفاده می شوند که از پروتکل های غیر قابل مسیردهی استفاده کنند یعنی آدرس مبدا و مقصد ندارند . این پروتکل ها به راحتی از Bridge عبور می کنند . نمونه ای از این پروتکل ها NetBeui ، NetBis می باشند . Gateway یا مترجم پروتکل : وسیله ای است که معمولا مانند یک دروازه ورودی/خروجی در شبکه عمل می کند . لفظ Gateway برای هر سخت افزاری بکارمی رود که معمولا دو شبکه غیر همجنس را به هم متصل کند . یک Gateway می تواند یک کامپیوتر ، یک مسیریاب ، یک Firewall ، یک Prxy Server و یا هر چیز دیگری باشد . اما تجهیزاتی که خاص Gateway هستند معمولا در شبکه هایی بکار می روند که براساس پروتکل TCP/IP کار نمی کنند . این تجهیزات وظیفه ترجمه پروتکل بین دو شبکه غیر همجنس را انجام می دهند . به عنوان مثال در شبکه هایی TCP/IP Base نیستند با استفاده از یک Gateway می توان پروتکل شبکه را به پروتکل TCP/IP و برعکس تبدیل نمود . Ruter یا مسیریاب : وسیله ای است که بسته ها را در طول شبکه گسترده هدایت می کند و در واقع ساختار شبکه اینترنت (Back Bne) در لایه IP از مسیریابها و اتصالات بین آنها تشکیل شده است . مسیریابها در لایه سه کار می کنند ؛ یعنی هر مسیریاب بسته را شناخته و می تواند از روی Header بسته ها مبدا و مقصد را تشخیص دهد . وقتی کامپیوتری در یک شبکه بسته ای را ارسال می کند که مقصد آن در شبکه محلی متصل به آن کامپیوتر موجود نیست آن بسته را تحویل Gateway می دهد تا از شبکه خارج شود . Gatewayها در شبکه معمولا تجهیزاتی هستند که عمل مسیریابی را نیز انجام می دهند . پس Ruter شبکه یا همان Gateway آدرس مقصد بسته ها را با مسیرهای خود مقایسه می کند تا کوتاهترین و بهترین مسیر را بین مبدا و مقصد انتخاب کنند و در صورت وجود مسیر بسته به خروجی مورد نظر ارسال می شود و در صورت عدم وجود مسیر یا برای مسیریابی Ruter با مسیریابهای مجاور مشورت می نماید و یا بسته را تحویل مسیریاب بعدی که در واقع Gateway مربوط به این مسیریاب می باشد هدایت می کند . هر Ruter دارای یک Ruting table می باشد که این جدول به صورت پویا نسبت به مسیریابهای همسایه به روز رسانده می شود (پروتکلهایی مانند RIP و SPF) به عبارت بهتر مسیریابها همیشه در مورد مسیرهای موجود برروی اینترنت با یکدیگر تبادل نظر می نمایند . مسیریابها همواره به دنبال بهترین مسیر با کمترین هزینه برروی اینترنت می گردند .

بخش چهارم

RIP ، RP و غیره وجود دارد که پروتکل IP را در عملکرد بهتر ، مسیریابی صحیح ، مدیریت خطاهای احتمالی و مواردی از این قبیل کمک می کند

بخش آخر

قالب بسته IP : قالب بسته IP به شکل زیر می باشد : ۱- ۴ Bit TYPE F SERVICE ۴- ۸ Bit IHL ۳- ۴ Bit VERSIN ۲- ۱۶ Bit TTAL LENGTH ۵-۸ Bit IDENTIFICATIN ۶- ۱ Bit UNUSED! ۷- ۱ Bit DF ۸- ۱ Bit MF ۹- ۱۳ Bit FRAGMENT FFSET ۱۰- ۸ Bit TIME T LIVE ۱۱- ۸ Bit PRTCL ۱۲- ۱۶ Bit HEADER CHECK SUM ۱۳- ۳۲ Bit SURCE ADDRESS ۱۴- ۳۲ Bit DESTINATIN ADDRESS ۱۵- ۰ R Mre (۳۲ Bit) PTIN ۱۶- ۳۲ Bit PAY LAD Versin : این فیلد چهار بیت است و نسخه پروتکل IP را مشخص می کند . پروتکلی که هم اکنون در اینترنت از

آن استفاده می شود پروتکل نسخه چهار می باشد . IHL (IP Header Length) : این فیلد نیز ۴ بیتی است و طول Header بسته را مشخص می کند ، اگر عدد موجود در این فیلد در ۴ ضرب شود طول Header به بایت بدست می آید . به عنوان مثال اگر در این فیلد عدد ۱۰ قرار گرفته باشد بدین معنی است که طول ۴۰ ، Header بایت خواهد بود . حداقل طول Header (در هنگامی که ptin برابر صفر باشد) برابر ۲۰ بایت و بنابراین حداقل IHL عدد ۵ می باشد . اگر در بسته ای IHL کمتر از ۵ باشد از این بسته صرفنظر می شود . حداکثر این مقدار نیز برابر عدد ۱۵ است . بنابراین حداکثر طول Header می تواند ۶۰ بایت باشد و درنتیجه قسمت ptin می تواند بین صفر تا ۴۰ بایت تغییر کند . Type f service : در این قسمت اطلاعات مربوط به اولویت بندی و کیفیت سرویس ذخیره می شود . Ttal length : طول یک بسته شامل قسمت Header و Data را مشخص می کند . باتوجه به تعداد بیتهای Ttal length می توان گفت که ماکزیمم طول بسته ۶۴ ، IP کیلو بایت باشد . Identificatin: در این قسمت مشخص می شود که اطلاعات موجود دراین قسمت داده در این بسته IP مربوط به چه دیتاگرامی از لایه بالاتر می باشد . Fragment ffset: این فیلد در سه بخش سازماندهی شده است: الف) DF (Dn't Fragment): با یک شدن این بیت در یک بسته IP هیچ مسیریابی حق ندارد در بین راه این بسته را به بسته های کوچکتر تقسیم نماید . ب) MF Mre Fragment)) : این بیت مشخص می کند که آیا بسته IP آخرین قسمت مربوط به یک دیتاگرام می باشد و یا هنوز هم بسته های دیگری وجود دارد . ج) Fragment ffset : این قسمت ۱۳ بیتی است و در حقیقت شماره ترتیب داده های هر بسته در دیتاگرام شکسته شده می باشد . بنابراین یک دیتاگرام می تواند به حدود ۸۰۰۰ بسته تقسیم شود . : (TTL (Time T Live TTL در نقش یک شمارنده طول عمر بسته را تعیین می نماید . طول عمر بسته به زمانی اشاره می کند که یک بسته IP می تواند در شبکه سرگردان باشد . بیشترین عددی که می توان در این قسمت قرارداد عدد ۲۵۵ (یک بایت) است . این عدد توسط فرستنده بسته تنظیم شده و با عبور از هر مسیریاب – هر مرحله عبور از مسیریاب را یک hp یا پرش می نامند - یک واحد از آن کم می شود . به ازای هر ثانیه انتظار در صف نیز یک واحد از آن کم می شود . وقتی این عدد به صفر برسد بسته IP از مسیر حذف شده و از رسیدن آن به مقصد جلوگیری می شود . عددی که به طور معمول توسط سیستم عامل در این قسمت قرار می گیرد عدد ۳۰ است و عددی که معمولا بوسیله آن می توان از نقطه ای به نقطه دیگر حرکت کرد عدد ۱۵ است . Prtcl: این فیلد مشخص می کند که پروتکل تحویلی از لایه بالاتر TCP یا UDP می باشد ؛ هر پروتکل دارای یک شماره خاص است. Header check sum: برای کشف خطا بکار می رود . این فیلد به دلیل اینکه برخی از اطلاعات بسته در عبور از هر مسیریاب تغییر می نماید باید دوباره مقداردهی شود . همچنین خطاهای بوجود آمده مربوط به بسته IP در این لایه بررسی نمی شود . Surce و Destinatin: آدرسهای ۴ بایتی منحصر بفرد برروی اینترنت می باشند که مبدا و مقصد را مشخص می کنند. ptin: این قسمت اختیاری است و معمولا- اطلاعاتی در خصوص مسیریابی و مسیرهای بهینه در آن قرار می گیرد که مورد استفاده مسیریابها است. Pay lad: در این قسمت داده ها و یا در واقع قطعه ای از دیتاگرام لایه بالاتر قرار می گیرد. آدرسها در اینترنت : در اینترنت هر میزبان دارای یک آدرس یکتا و منحصر بفرد ۳۲ بیتی می باشد برای سادگی نمایش این آدرس ، آدرس به ۴ قسمت ۸ بیتی بقسیم می شود هر قسمت با نقطه از قسمت دیگر جدا شده و در مبنای ۱۰ نمایش داده می شود . برای مثال عدد ۰۰۱۰۰۰۱۰,۰۰۰۱۰۱۰۱,۱۱۱۰۰۰۰۱,۰۰۰۰۰۰۰۱ به صورت ۳۴.۲۱.۲۲۵.۱ نمایش داده می شود . نحوه پیدا کردن آدرسها بر روی اینترنت مانند پیدا کردن آدرسها برای یک آدرس پستی و یا مسیریابی تلفن براساس شماره تلفن ها می باشد . تفاوتی که بین تقسیم بندی IPها و آدرسهای پستی و شماره تلفن ها وجود دارد این است که تقسیم بندیهای پستی براساس مرزبندیهای جغرافیایی و موقعیت سیاسی – جغرافیایی می باشد اما در تقسیم بندی IPها این دسته بندی براساس شرکتهای مختلف و تامین کنندگان سرویس انجام شده است و محدودیتی از لحاظ جغرافیایی ندارد . آدرسهای IP برروی اینترنت حدود ۴ بیلیارد می باشند که در ۵

کلاس D ، C ، B ، A و E تقسیم بندی شده اند • : آدرسهای کلاس A : آدرسهای این کلاس با عددی بین ۰ تا ۱۲۷ (XXX.XXX.XXX.۰ تا XXX.XXX.XXX.۱۲۷) شروع می شوند • . آدرسهای کلاس B : آدرسهای این کلاس با عددی بین ۱۲۸ تا ۱۹۱ شروع می شوند • . آدرسهای کلاس C : آدرسهای این کلاس با عددی بین ۱۹۲ تا ۲۲۳ شروع می شوند • . آدرسهای کلاس D : دراین کلاس ۴ بیت مشخصه کلاس می باشد (۱۱۱۰) و ۲۸ بیت باقی مانده آدرسهای Multi cast هستند ، بدین معنی که با تنظیم کردن قسمت باقی مانده می توان اطلاعاتی را برای گروهی از کامپیوترها که دارای مشخصه مشترک هستند (آدرس Multi cast) ارسال نمود • . آدرسهای کلاس E : آدرسهای این کلاس با عددی بزرگتر از ۲۲۴ شروع می شوند . این آدرسها رزرو شده اند و برروی اینترنت استفاده نمی شوند . آدرسهای خاص : در بین تمامی کلاسهای آدرس (۵ گروه) گروهی از آدرسها وجود دارند که دارای معنی ویژه ای هستند و نمی توان با آنها شبکه یا میزبان خاصی را برروی اینترنت آدرس دهی نمود ؛ رنج IPهای آزادی که می توان برروی اینترنت از آن استفاده کرد از ۱۹۲.۱۶۸.۰.۰ تا ۲۵۵.۲۵۵.۰.۰ می باشد . این آدرسهای خاص عبارتند از : ۱- ۰.۰.۰.۰ : هر ماشینی که آدرس آن مشخص نیست (آدرس خودش را نمی داند) از این آدرس در قسمت Surce پاکت IP استفاده می کند . مشخص است که گیرنده Packet نمی تواند هیچ جوابی برای فرستنده ارسال نماید . ۲- XXX.XXX.XXX.۰ : هر ماشینی که مشخصه شبکه ای را که متعلق به آن است ندارد از این ساختار آدرس استفاده می کند . ۳- ۲۵۵.۲۵۵.۲۵۵.۲۵۵ : برای ارسال Brad cast در شبکه ای که ماشین ارسال کننده بسته برروی آن شبکه قرار دارد بکارمی رود . ۴ - XXX.XXX.XXX.۲۵۵ : برای ارسال Brad cast برای کلیه ماشینها در یک شبکه خاص بکارمی رود . ۵- XXX.XXX.XXX.۱۲۷ : این آدرس ، آدرس بازگشت (Lp back) می باشد . از این آدرس برای اشکال زدایی نرم افزارها و تست برنامه ها استفاده می شود ؛ به عنوان مثال آدرس ۱۲۷.۰.۰.۱ فرستنده بسته را مشخص می نماید یعنی هر Packet ارسالی به ارسال کننده Packet بازمی گردد . DNS (Dmain Name Server) : تنها هویت معتبر یک میزبان برروی اینترنت آدرس IP میزبان می باشد اما به دلیل اینکه به خاطر سپردن IPها تقریبا غیرممکن است از آدرسهای نمادین استفاده می شود که باید به آدرسهای IP تبدیل شوند . DNS یا سیستم نامگذاری دامنه روشی سلسله مراتبی است که بانک اطلاعاتی مربوط به نامها و معادل IP آنها را روی شبکه اینترنت توزیع کرده است و هر ایستگاهی می تواند در یک روال منظم و سلسله مراتبی آدرس IP معادل با نام مورد نظرش را پیدا نماید . روش کار به این صورت است که قبل از اینکه یک برنامه کاربردی بخواهد برروی اینترنت ارتباطی را برقرار کند نام میزبانی را که می خواهد به آن متصل شود با استفاده از پروتکل UDP برای سرویس دهندههای DNS که در تنظیمات آن به صورت دستی معرفی شده اند ارسال می نماید و پس از دریافت آدرس IP اطلاعات را برای مقصد مورد نظر ارسال می نماید .

Hneypt ها

قسمت اول

قدم اول در فهم اینکه Hneypt چه می باشند بیان تعریفی جامع از آن است. تعریف Hneypt می تواند سخت تر از آنچه که به نظر می رسد باشد. Hneypt ها از این جهت که هیچ مشکلی را برای ما حل نمی کنند شبیه دیواره های آتش و یا سیستمهای تشخیص دخول سرزده نمی باشند. در عوض آنها یک ابزار قابل انعطافی می باشند که به شکلهای مختلفی قابل استفاده هستند.آنها هر کاری را می توانند انجام دهند از کشف حملات پنهانی در شبکه های IPv۶ تا ضبط آخرین کارت اعتباری جعل شده! و همین انعطاف پذیریها باعث شده است که Hneypt ها ابزارهایی قوی به نظر برسند و از جهتی نیز غیر قابل تعریف و غیر قابل فهم!! البته

من برای فهم Hneypt ها از تعریف زیر استفاده می کنم: یک Hneypt یک منبع سیستم اطلاعاتی می باشد که با استفاده از ارزش کاذب خود اطلاعاتی از فعالیتهای بی مجوز و نا مشروع جمع آوری می کند. البته این یک تعریف کلی می باشد که تمامی گونه های مختلف Hneypt ها را در نظر گرفته است. ما در ادامه مثالهای مختلفی برای Hneypt ها و ارزش امنیتی آنها خواهیم آورد. همه آنها در تعریفی که ما در بالا آورده ایم می گنجند ، ارزش دروغین آنها برای اشخاص بدی که با آنها در تماسند. به صورت کلی تمامی Hneypt ها به همین صورت کار می کنند. آنها یک منبعی از فعالیتها بدون مجوز می باشند. به صورت تئوری یک Hneypt نباید هیچ ترافیکی از شبکه ما را اشغال کند زیرا آنها هیچ فعالیت قانونی ندارند. این بدان معنی است که تراکنش های با یک Hneypt تقریبا تراکنش های بی مجوز و یا فعالیتهای بد اندیشانه می باشد. یعنی هر ارتباط با یک Hneypt می تواند یک دزدی ، حمله و یا یک تصفیه حساب می باشد. حال آنکه مفهوم آن ساده به نظر می رسد (و همین طور هم است) و همین سادگی باعث این هم موارد استفاده شگفت انگیز از Hneypt ها شده است که من در این مقاله قصد روشن کردن این موارد را دارم. فواید Hneypt ها Hneypt مفهوم بسیار ساده ای دارد ولی دارای توانایی های قدرتمندی می باشد. ۱. داده های کوچک دارای ارزش فراوان: Hneypt ها یک حجم کوچکی ار داده ها را جمع آوری می کنند. به جای اینکه ما در یک روز چندین گیگابایت اطلاعات را در فایلهای ثبت رویدادها ذخیره کنیم توسط Hneypt فقط در حد چندین مگابایت باید ذخیره کنیم. به جای تولید ۱۰۰۰۰ زنگ خطر در یک روز آنها فقط ۱ زنگ خطر را تولید می کنند. یادتان باشد که Hneypt ها فقط فعالیتهای ناجور را ثبت می کنند و هر ارتباطی با Hneypt می تواند یک فعالیت بدون مجوز و یا بداندیشانه باشد. و به همین دلیل می باشد که اطلاعات هر چند کوچک Hneypt ها دارای ارزش زیادی می باشد زیرا که آنها توسط افراد بد ذات تولید شده و توسط Hneypt ضبط شده است. این بدان معنا می باشد که تجزیه و تحلیل اطلاعات یک Hneypt آسانتر (و ارزانتر) از اطلاعات ثبت شده به صورت کلی می باشد. ۲. ابزار و تاکتیکی جدید : Hneypt برای این طراحی شده اند که هر چیزی که به سمت آنها جذب می شود را ذخیره کنند. با ابزارها و تاکتیکهای جدیدی که قبلا دیده نشده اند. ۳. کمترین احتیاجات: Hneypt ها به کمترین احتیاجات نیاز دارند زیرا که آنها فقط فعالیتهای ناجور را به ثبت می رسانند. بنابراین با یک پنتیوم قدیمی و با ۱۲۸ مگابایت RAM و یک شبکه با رنج B به راحتی می توان آن را پیاده سازی کرد. ۴. رمز کردن یا IPv۶ : بر خلاف برخی تکنولوژیهای امنیتی (مانند IDS ها) Hneypt خیلی خوب با محیطهای رمز شده و یا IPv۶ کار می کنند. این مساله مهم نیست که یک فرد ناجور چگونه در یک Hneypt گرفتار می شود زیرا Hneypt ها خود می توانند آنها را شناخته و فعالیتهای آنان را ثبت کنند. مضرات Hneypt ها شبیه تمامی تکنولوژیها ، Hneypt ها نیز دارای نقاط ضعفی می باشند. این بدان علت می باشد که Hneypt ها جایگزین تکنولوژی دیگری نمی شوند بلکه در کنار تکنولوژیهای دیگر کار می کنند. ۱- محدودیت دید : Hneypt ها فقط فعایتهایی را می توانند پیگیری و ثبت کنند که به صورت مستقیم با آنها در ارتباط باشند. Hneypt حملاتی که بر علیه سیستمهای دیگر در حال انجام است را نمی توانند ثبت کنند به جز اینکه نفوذگر و یا آن تهدید فعل و انفعالی را با Hneypt داشته باشد. ۲- ریسک : همه تکنولوژیهای امنیتی دارای ریسک می باشند. دیوارهای آتش ریسک نفوذ و یا رخنه کردن در آن را دارند. رمزنگاری ریسک شکستن رمز را دارد، IDS ها ممکن است نتوانند یک حمله را تشخیص دهند. Hneypt ها مجزای از اینها نیستند. آنها نیز دارای ریسک می باشند. به خصوص اینکه Hneypt ها ممکن است که ریسک به دست گرفتن کنترل سیستم توسط یک فرد هکر و صدمه زدن به سیستمهای دیگر را داشته باشند. البته این ریسکها برای انواع مختلف Hneypt ها فرق می کند و بسته به اینکه چه نوعی از Hneypt را استفاده می کنید نوع و اندازه ریسک شما نیز متفاوت می باشد.ممکن است استفاده از یک نوع آن ، ریسکی کمتر از IDS ها داشته باشد و استفاده از نوعی دیگر ریسک بسیار زیادی را در پی داشته باشد.ما در ادامه مشخص خواهیم کرد که چه نوعی از Hneypt ها دارای چه سطحی از ریسک می باشند.

چگونگی و شیوه به کار بردن Hneypt ها می باشد که ارزش و فواید و مضرات آنها را مشخص می کند. در ادامه بیشتر روی آن بحث خواهد شد.

قسمت دوم

در بخش اول این مقاله ، تعریفی از Hneypt ها ارائه دادیم و فواید و مضرات آنها را بیان کردیم. در این بخش درباره انواع آنها بحث خواهیم کرد انوع Hneypt ها Hneypt ها در اندازه و شکلهای مختلفی هستند و همین امر باعث شده است که فهم آنها کمی مشکل شود. برای اینکه بتوان بهتر آنها را فهمید همه انواع مختلف آنها را در دو زیر مجموعه آورده ایم: ۱- Hneypt های کم واکنش ۲- Hneypt های پرواکنش این تقسیم بندی به ما کمک می کند که چگونگی رفتار آنها را بهتر درک کنیم. و بتوانیم به راحتی نقاط ضعف و قدرت آنها و توانایی ها یشان را روشن تر کنیم. واکنش در اصل نوع ارتباطی که یک نفوذگر با Hneypt دارد را مشخص می کند. Hneypt های کم واکنش دارای ارتباط و فعالیتی محدود می باشند.آنها معمولا با سرویسها و سیستم های عامل را شبیه سازی شده کار می کنند. سطح فعالیت یک نفوذگر با سطحی از برنامه های شبیه سازی شده محدود شده است. به عنوان مثال یک سرویس FTP شبیه سازی شده که به پورت ۲۱ گوش می کند ممکن است فقط یک صفحه lgin و یا حداکثر تعدادی از دستورات FTP را شبیه سازی کرده باشد . یکی از فواید این دسته از Hneypt های کم واکنش سادگی آنها می باشد. نگهداری Hneypt های کم واکنش بسیار راحت و آسان است و خیلی راحت می توان آنها را گسترش داد و ریسک بسیار کمی دارند. آنها بیشتر درگیر این هستند که چه نرم افزارهایی باید روی چه سیستم عاملی نصب شود و همچنین می خواهید چه سرویسهایی را برای آن شبیه سازی و دیده بانی (Mnitr) کنید. همین رهیافت خودکار و ساده آنها است که توسعه آن را برای بسیاری از شرکت ها راحت می کند. البته لازم به ذکر است که همین سرویسهای شبیه سازی شده باعث می شود که فعالیت های فرد نفوذگر محدود شود و همین امر باعث کاهش ریسک می گردد. به این معنی که نفوذگر نمی تواند هیچگاه به سیستم عامل دسترسی پیدا کند و به وسیله آن به سیستم های دیگر آسیب برساند. یکی از اصلی ترین مضرات Hneypt های کم واکنش این است که آنها فقط اطلاعات محدودی را می توانند ثبت کنند و آنها طراحی می شوند که فقط اطلاعاتی راجع به حملات شناخته شده را به ثبت برسانند.همچنین شناختن یک Hneypt کم واکنش برای یک نفوذگر بسیار راحت می باشد. نگران این نباشید که شبیه سازی شما چه اندازه خوب بوده است زیرا که نفوذگران حرفه ای به سرعت یک Hneypt کم واکنش را از یک سیستم واقعی تشخیص می دهند. از Hneypt های کم واکنش می توان Hneyd , Spectr و KFSensr را نام برد. Hneypt های پر واکنش متفاتند. آنها معمولاـ از راه حل های پیچیده تری استفاده می کنند زیرا که آنها از سیستم عاملها و سرویسهای واقعی استفاده می کنند. هیچ چیزی شبیه سازی شده نیست و ما یک سیستم واقعی را در اختیار نفوذگر می گذاریم. اگر شما می خواهید که یک Hneypt لینوکس سرور FTP داشته باشید شما باید یک لینوکس واقعی به همراه یک سرویس FTP نصب کنید. فایده این نوع Hneypt دو چیز است. شما می توانید یک حجم زیادی از اطلاعات را به دست آورید. با دادن یک سیستم واقعی به فرد نفوذگر شما می توانید تمامی رفتار او از rtkit های جدید گرفته تا یک نشست IRC را زیر نظر بگیرید. دومین فایده Hneypt های پرواکنش این است که دیگر جای هیچ فرضیه ای روی رفتار نفوذگر باقی نمی گذارد و یک محیط باز به او می دهد و تمامی فعالیتهای او را زیر نظر می گیرد. همین امر باعث می شود که Hneypt های پرواکنش رفتارهایی از فرد نفوذگر را به ما نشان دهند که ما انتظار نداشته ایم و یا نمی توانسته ایم حدس بزنیم!! بهترین جا برای استفاده از این نوع Hneypt ها زمانی است که قصد داریم دستورات رمز شده یک در پشتی را روی یک شبکه غیر استاندارد IP به دست بیاریم. به هر حال همین امور است که ریسک اینگونه Hneypt ها را افزایش می دهد زیرا که نفوذگر یک سیستم عامل واقعی را در اختیار دارد و

ممکن است به سیستم های اصلی شبکه صدمه بزنند. به طور کلی یک Hneypt پرواکنش می تواند علاوه بر کارهای یک Hneypt کم واکنش کارهای خیلی بیشتری را انجام دهد. برای فهم بهتر اینکه Hneypt کم واکنش و پرواکنش چگونه کار می کنند بهتر است دو مثال واقعی در این زمینه بیاوریم. با Hneypt های کم واکنش شروع می کنیم. Hneyd: یک Hneypt کم واکنش Hneyd یک Hneypt کم واکنش است که توسط Niels Prvs ساخته شده است. Hneyd به صورت کد باز می باشد و برای مجموعه سیستم عاملهای یونیکس ساخته شده است.(فکر کنم روی ویندوز هم برده شده است) . Hneyd بر اساس زیر نظر گرفتن IP های غیر قابل استفاده بنا شده است. هر چیزی که قصد داشته باشد با یک IP غیر قابل استفاده با شبکه ارتباط برقرار کند ارتباطش را با شبکه اصلی قطع کرده و با نفوذگر ارتباط برقرار می کند و خودش را جای قربانی جا می زند. به صورت پیش فرض Hneyd تمامی پورتها TCP و یا UDP را زیر نظر گرفته و تمامی درخواستهای آنها را ثبت می کند. همچنین برای زیر نظر گرفتن یک پورت خاص شما می توانید سرویس شبیه سازی شده مورد نظر را پیکربندی کنید مانند شبیه سازی یک سرور FTP که روی پروتکل TCP پورت ۲۱ کار می کند.وقتی که نفوذگر با یک سرویس شبیه سازی شده ارتباط برقرار می کند تمامی فعالیتهای او را با سرویسهای شبیه سازی شده دیگر ثبت کرده و زیر نظر می گیرد. مثلا در سرویس FTP شبیه سازی شده ما می توانیم نام کاربری و کلمه های رمزی که نفوذگر برای شکستن FTP سرور استفاده می کند و یا دستوراتی که صادر می کند را به دست آوریم و شاید حتی پی ببریم که او به دنبال چه چیزی می گردد و هویت او چیست ! همه اینها به سطحی از شبیه سازی بر می گردد که Hneypt در اختیار ما گذاشته است. بیشتر سرویسهای شبیه سازی شده به یک صورت کار می کنند. آنها منتظر نوع خاصی از رفتارهای هستند و طبق راههایی که قبلا تعیین کرده اند به این رفتارهای واکنش نشان می دهند. اگر حمله A این را انجام داد از این طریق واکنش نشان بده و اگر حمله B این کار را کرد از این راه واکنش نشان بده! محدودیت این برنامه ها در این است که اگر نفوذگر دستوراتی را وارد کند که هیچ پاسخی برای آنها شبیه سازی نشده باشد. بنابراین آنها نمی دانند که چه پاسخی را باید برای نفوذگر ارسال کنند. بیشتر Hneypt های کم واکنش – مانند Hneyd – یک پیغام خطا نشان می دهند. شما می توانید از کد برنامه Hneyd کل دستوراتی که برای FTP شبیه سازی کرده است را مشاهده کنید. Hneynet ها : یک Hneypt پر واکنش Hneynet یک مثال بدیهی برای Hneypt های پرواکنش می باشد. Hneynet ها یک محصول نمی باشند. آنها یک راه حل نرم افزاری که بتوان روی یک کامپیوتر نصب شوند نمی باشد. Hneynet ها یک معماری می باشند. یک شبکه بی عیب از کامپیوترهایی که طراحی شده اند برای حملاتی که روی آنها انجام می گیرد. طبق این نظریه ما باید یک معماری داشته باشیم که یک کنترل بالایی را روی شبکه ایجاد کند تا تمامی ارتباطات با شبکه را بتوان کنترل کرد و زیر نظر گرفت. درون این شبکه ما چندین قربانی خیالی در نظر می گیریم البته با کامپیوترهایی که برنامه های واقعی را اجرا می کنند. فرد هکر این سیستم ها را پیدا کرده و به آنها حمله می کند و در آنها نفوذ می کند اما طبق ابتکار و راهکارهای ما ! یعنی همه چیز در کنترل ما می باشد. البته وقتی آنها این کارها را انجام می دهند نمی دانند که در یک Hneynet گرفتار شده اند. تمامی فعالیت های فرد نفوذگر از نشست های رمز شده SSH گرفته تا ایمیل ها و فایلهایی که در سیستم ها قرار می دهند همه و همه بدون آنکه آنها متوجه شوند زیر نظر گرفته و ثبت می شود. در همان زمان نیز Hneynet تمامی کارهای نفوذگر را کنترل می کند. Hneynet ها این کارها را توسط دروازه ای به نام Hneywall انجام می دهند. این دروازه به تمامی ترافیک ورودی اجازه می دهد که به سمت سیستم های قربانی ما هدایت شوند ولی ترافیک خروجی باید از سیستم های مجهز به IDS عبور کند. این کار به نفوذگر این امکان را می دهد که بتواند ارتباط قابل انعطاف تری با سیستم های قربانی داشته باشد اما در کنار آن اجازه داده نمی شود که نفوذگر با استفاده از این سیستم ها به سیستم های اصلی صدمه وارد کند.

قسمت آخر

جایگاه Hneypt ها حال که آشنایی ابتدایی با هر دو نوع Hneypt داریم لازم است که ارزش و جایگاه آنها را در دنیای امنیتی بیان کنیم ، به خصوص در ادامه بیان خواهیم کرد که چگونه باید از Hneypt استفاده کنیم. همانطور که قبلا اشاره کردیم دو دسته Hneypt داریم که برای اهداف و تحقیقات ما مورد مطالعه قرار می گیرند. وقتی از Hneypt ها به صورت محصولات تولید شده برای محافظت از سازمان ها استفاده می کنیم می توانند ما را در موارد مختلفی محافظت کنند از جمله می توان محافظت ، کشف و پاسخ مناسب به یک حمله را بیان کرد. وقتی آنها را در جهت امور تحقیقاتی به کار می بریم Hneypt ها اطلاعات لازم را برای ما جمع آوری می کنند. البته این اطلاعات برای سازمانهای مختلف فرق می کند. عده ای شاید بخواهند دشمنان بیرونی خود را شناسایی کنند ، یا کارمندان و خریداران خرابکار خود را بشناسند این سازمانها نیز می توانند از این دسته Hneypt ها استفاده کنند. اگر بخواهیم به صورت کلی بیان کنیم Hneypt های کم واکنش به عنوان محصولات تولیدی به کار می روند در صورتیکه Hneypt های پرواکنش برای عملیاتهای تحقیقاتی روی شبکه به کار گرفته می شوند. البته هر کدام از آنهامی توانند در اهداف دیگر نیز به کار روند . Hneypt های تولیداتی می توانند ما را در سه رده زیر کمک کنند: ۱- پیشگیری (۲ (Preventin- ردیابی یا کشف(۳ (Detectin- پاسخ (Respnse) که در ادامه به صورت عمیق تری روی آنها بحث می کنیم. Hneypt ها از راههای مختلفی می توانند ما را از حملات حفظ کنند. ابتدا حملاتی که به صورت اتوماتیکی انجام می شود مثل کرمها و یا Aut-rter ها . این حملات به این صورت کار می کنند که نفوذگران با استفاده از بعضی از ابزارها یک رنجی از شبکه ها را پویش کرده تا آسیب پذیری سرورهای موجود در این شبکه را پیدا کنند این ابزارها پس از پیدا کردن آسیب پذیریهای موجود ، به این سیستم ها حمله می کنند. (مانند کرم ساسر که وقتی سیستمی را آلوده می کرد به صورت اتوماتیک و به وسیله یک آدرس IP تصادفی ، سیستم دیگری را نیز آلوده می کرد). روشی که Hneypt ها برای محافظت شبکه ما از این گونه حملات استفاده می کنند این است که می توانند سرعت اینگونه حملات را کند کنند و یا حتی آنها را متوقف کنند! به این دسته از Hneypt ها Hneypt های چسبنده (Sticky) می گویند. در این راه حل Hneypt ها ، آن دسته از آدرس هایی را که در شبکه استفاده نمی شوند ، در نظر می گیرند و به آنها واکنش نشان می دهند. یعنی هنگامیکه یک برنامه مخرب یا نفوذگر قصد پویش رنجی از آدرس ها را دارد ، Hnypt به آن دسته از آدرس هایی که در شبکه موجود نمی باشند واکنش نشان می دهد برای مثال با استفاده از پیغامهای TCP روند این گونه حملات را آهسته تر می کند. (برای نمونه، با دادن پیغام پنجره صفر ، نفوذگر را در یک گودال هل می دهد تا نتواند بسته های دیگر را ارسال کند) این امر برای آهسته کردن سرعت انتشار و یا محافظت در برابر کرمهایی که شبکه داخلی ما را مورد هجوم قرار می دهند بسیار مناسب است. LaBrea جزو این دسته از Hneypt ها می باشد. Hneypt های چسبنده اغلب به عنوان یک Hneypt کم واکنش شناخته می شوند. (البته شما می توانید آنها را Hneypt های بدون واکنش بنامید زیرا که آنها فقط سرعت نفوذ یک نفوذگر را در شبکه کند می کنند) Hneypt همچنین می توانند سازمان شما را از اشخاص نفوذگر محافظت کنند. البته این کار فقط حیله ای می باشد که باعث تهدید و ارعاب نفوذگر می شود. یعنی نفوذگر را گیج و دست پاچه کنیم تا بتوانیم از این طریق وقت او را به وسیله درگیر شدنش با Hneypt بگیریم. در ضمن سازمان شما می تواند با کشف فعالیتهای نفوذگر و داشتن زمان لازم برای پاسخ ، این گونه جملات را متوقف کند. حتی می توان یک مرحله بالاتر رفت . اگر نفوذگر بداند که سازمان شما از Hneypt استفاده می کند ولی نداند که کدام سیستم Hneypt می باشد همیشه یک نگرانی در ذهن خود دارد که « آیا این یک سیستم حقیقی است یا در یک Hneypt گرفتار شده ام !! » و ممکن است همین نگرانی باعث شود که هیچگاه به فکر نفوذ در شبکه شما نیفتد. بنابراین Hneypt می توانند نفوذگران را بترسانند. Deceptin Tlkit یکی از همین نوع Hneypt های کم واکنش می باشد. راه دومی که Hneypt ها به محافظت سازمانها

کمک می کنند از طریق کشف یا ردیابی است.عمل کشف خیلی بحرانی می باشد که وظیفه اش شناسایی ناتوانی ها و از کار افتادگی های بخش پیشگیری می باشد. صرف نظر از اینکه امنیت یک سازمان به چه صورت می باشد معمولا اتفاقی برای شبکه های آنها می افتد که باعث بعضی از شکست ها می گردد. صرف نظر از مشکلات و درگیری هایی که اشخاص برای کشف یک حمله انجام می دهند، وقتی یک حمله شناسایی شود می توان خیلی سریع به آن واکنش نشان داد و آن را متوقف کرد و یا حداقل اثر آن را کمتر کرد. متاسفانه کشف یک حمله بسیار کار مشکلی می باشد. تکنولوژی هایی مانند IDS ها و فایلهای ثبت وقایع(lg) از جهاتی بدون اثر می باشند. آنها داده های فراوانی را تولید می کنند که خواندن تمامی آنها زمان فراوانی را می طلبد و بسیاری از این داده ها نیز بیهوده و به درد نخور می باشند. همچنین آنها در کشف حملات جدید نیز ناتوان می باشند. حتی نمی توانند با محیط های رمز شده و یا IPV۶ کار کنند. Hneypt ها برای کشف و ردیابی یک حمله نسبت به این تکنولوژیهای قدیمی برتری دارند. Hneypt داده های کم و با قطع و یقین بیشتری جمع آوری می کند که ارزش بسیار فراوانی دارد.آنها حتی می توانند حملات جدید و یا کدهای چند شکلی را به راحتی کشف کنند و می توانند در محیطهای رمز شده و IPv۶ نیز استفاده شوند. برای اینکه اطلاعات بیشتری راجع به این دسته از Hneypt کسب کنید می توانید مقاله Hneypt:Simple,Cst Effective Detectin را مطالعه کنید. به هر جهت Hneypt های کم واکنش بهترین راه حل برای کشف می باشند. ساخت و نگهداری آنها آسان تر از Hneypt های پر واکنش می باشد و همچنین ریسک کمتری نسبت به آنها دارد. سومین و آخرین راهی که hneypt ها سازمانهای ما را محافظت می کنند پاسخ(Respnse) است. هر زمانی که یک سازمان یک خطا و مشکلی را در شبکه خود تشخیص داد حال چگونه باید پاسخ دهد؟ همین موضوع می تواند یکی از چالش هایی باشد که یک سازمان با آن مواجه می باشد. معمولا- اطلاعات کمی درباره اینکه نفوذگر چه کسی است! و چه کاری می خواهد انجام دهد!، وجود دارد. در این وضعیت کوچکترین اطلاعات درباره فعالیت های نفوذگر، مهم و حیلاتی است. معمولا در پاسخ مناسب به یک حمله دو تا مشکل وجود دارد؛ ابتدا اینکه ، بیشتر سیستم هایی که مورد هجوم قرار گرفته اند را نمی توان برای یک تجزیه و تحلیل مناسب ، از کار انداخت . سیستم های تولیداتی ، مانند سرور پست الکترونیکی برای یک سازمان بسیار مهم و حیاتی می باشند و حتی اگر متوجه بشوند که سرور آنها هک شده است باز هم حاضر نیستند این سیستم ها را از کار بیاندازند تا تجزیه و تحلیل دقیقی روی آنها انجام شود و پاسخ مناسبی به آن داده شود. در عوض باید در هنگامی که این سیستم ها در حال کار می باشند آنها را بررسی کرد. همین امر باعث می شود که نتوان به درستی پی برد که چه اتفاق افتاده است و چه مقدار خسارت توسط هکر به سیستم وارد شده است و آیا نفوذگر به سیستم های دیگر وارد شده است؟ و یا می تواند وارد شود!؟ مشکل دیگر در اینجا می باشد که حتی اگر سیستم را نیز از کار بیاندازیم آنقدر داده در سیستم وجود دارد که نمی توان به درستی متوجه شد که کدامیک متعلق به نفوذگر است. در عوض Hneypt ها برای چنین کارهایی بسیار عالی می باشند، زیرا که آنها را می توان به آسانی از کار انداخت تا تجزیه و تحلیل کاملی روی آنها انجام گیرد بدون اینکه به روند کاری سازمان صدمه ای وارد شود. همچنین Hneypt ها تنها فعالیت های غیر قانونی و بد اندیشانه را در خود ذخیره می کنند و به همین دلیل است که تجزیه و تحلیل یک Hneypt هک شده بسیار آسان تر از یک سیستم واقعی می باشد. هر داده ای که در Hneypt ذخیره شده است مربوط به فعالیت های فرد نفوذگر می باشد و همین موضوع این امکان را به یک سازمان می دهد که خیلی راحت به اطلاعات مفیدی درباره نوع حمله و هویت نفوذگر پی برده و پاسخ سریع و موثری را به آن دهد. به صورت کلی Hneypt پرواکنش برای پاسخ بهترین گزینه می باشند. برای پاسخ به یک اخلال ابتدا باید دانست که اخلال گر قصد چه کاری را داشته است و چگونه توانسته است که اخلال ایجاد کند، همچنین از چه ابزارهایی استفاده کرده است. پس برای این مرحله نیاز به Hneypt پرواکنش داریم. آنچه که مسلم است ، Hneypt ها یک تکنولوژی جدید می باشند و هنوز راه فراوانی را باید بپیمایند تا به تکامل برسند. اما آنها برای بسیاری از

اهـدافی که یـک سازمـان برای مسایل امنیتی نیاز دارد ، مناسب می باشـند و ما را برای برای پیشـگیری از یک نفوذ ، کشف نفوذ و پاسخ به آن کمک می کنند.

VPN چیست؟

نگاهی فنی به VPN

استفاده از RAS سـرور و خط تلفن برای برقراری ارتباط دو مشـکل عمده دارد عبارتند از: ۱)در صورتی که RAS سرور و سیستم تماس گیرنده در یک اسـتان قرار نداشـته باشند، علاوه بر لزوم پرداخت هزینه زیاد، سرعت ارتباط نیز پایین خواهد آمد و این مسئله وقتی بیشتر نمود پیدا می کند که کاربر نیاز به ارتباطی با سـرعت مناسب داشـته باشد. ۲)در صورتی که تعـداد اتصالات راه دور در یک لحظه بیش از یک مورد باشد، RAS سرور به چندین خط تلفن و مودم احتیاج خواهد داشت که باز هم مسئله هزینه مطرح می گردد. امـا با ارتباط VPN مشـکلات مـذکور به طور کامـل حل می شود و کاربر با اتصال به ISP محلی به اینترنت متصل شـده و VPN بین کـامپیوتر کـاربر و سـرور سازمان از طریق اینترنت ایجاد می گردد. ارتباط مـذکور می توانـد از طریق خط Dialup و یا خط اختصاصـی مانند Leased Line برقرار شـود. به هر حـال اکنون مسـئله این نیست که طریقه اسـتفاده از VPN چیست، بلکه مسـئله این است که کدامیک از تکنولوژی های VPN باید مورد اسـتفاده قرار گیرند. پنج نوع پروتکل در VPN مورد استفاده قرار می گیرد که هر کـدام مزایـا و معایبی دارنـد. در این مقاله ما قصـد داریم در مورد هر کـدام از این پروتکل ها بحث کرده و آنها را مقایسه کنیم. البته نتیجه نهایی به هدف شما در استفاده VPN بستگی دارد. ارتباط سیستم ها در یک اینترانت در برخی سازمان ها، اطلاعـات یـک دپارتمان خاص به دلیل حساسیت بالا، به طور فیزیکی از شـبکه اصـلی داخلی آن سازمان جـدا گردیـده است. این مسـئله علیرغم محافظت از اطلاعات آن دپارتمان، مشـکلات خاصی را نیز از بابت دسترسی کاربران دپارتمان مذکور به شبکه های خـارجی به وجود می آورد. VPN اجازه می دهـد که شـبکه دپارتمان مذکور به صورت فیزیکی به شـبکه مقصد مورد نظر متصـل گردد، اما به صورتی که توسط VPN سرور، جدا شده است (با قرار گرفتن VPN سرور بین دو شبکه). البته لازم به یادآوری است که نیازی نیست VPN سـرور به صورت یک Ruter مسیر یاب بین دو شـبکه عمل نماید، بلکه کاربران شبکه مورد نظر علاوه بر اینکه خصوصیات و Subnet شـبکه خاص خود را دارا هستند به VPNسرورمتصل شده و به اطلاعات درشـبکه مقصد دست می یابنـد. علاوه بر این تمام ارتباطات برقرار شده از طریق VPN، می تواننـد به منظور محرمانه ماندن رمز نگاری شوند. برای کاربرانی کـه دارای اعتبـار نـامه مجـاز نیسـتند، اطلاعـات مقصـد بـه صـورت خودکـار غیر قابـل رویـت خواهنـد بـود. مبـانی Tunneling Tunneling یـا سیسـتم ایجـاد تونل ارتباطی با نام کپسوله کردن (Encapsulatin) نیز شـناخته می شود که روشـی است برای اسـتفاده از زیر سـاخت یـک شـبکه عمومی جهت انتقال اطلاعات. این اطلاعات ممکن است از پروتکل دیگری باشـد. اطلاعات به جـای اینکه به صورت اصـلی و riginal فرسـتاده شونـد، بـا اضافه کردن یک Header (سـرایند) کپسوله می شوند. این سـزایند اضافی که به پکت متصل می شود، اطلاعات مسیر یابی را برای پکت فراهم می کند تا اطلاعات به صورت صـحیح، سـریع و فوری به مقصد برسـند. هنگامی که پکت های کپسوله شده به مقصد رسـیدند، سرایندها از روی پکت برداشته شده و اطلاعات به صورت اصـلی خود تبـدیل می شوند. این عملیات را از ابتدا تا اتمام کار Tunneling می نامند. نگهداری تونل مجموعه عملیات متشـکل از پروتکـل نگهـداری تونـل و پروتکـل تبادل اطلاعات تونل به نام پروتکل Tunneling شـناخته می شونـد. برای اینکه این تونل برقرار شود، هم کلاینت و هم سـرور می بایست پروتکل Tunneling یکسانی را مورد اسـتفاده قرار دهند. از جمله پروتکل هایی که برای عملیـات Tunneling مـورد اسـتفاده قرار می گیرنـد PPTP و L۲TP هسـتند که در ادامه مـورد بررسـی قرار خـواهند

گرفت. پروتکل نگهداری تونل پروتکل نگهداری تونل به عنوان مکانیسمی برای مدیریت تونل استفاده می شود. برای برخی از تکنولوژی های Tunneling مانند PPTP و L۲TP یک تونل مانند یک Sessin می باشد، یعنی هر دو نقطه انتهایی تونل علاوه بر اینکه باید با نوع تونل منطبق باشند، می بایست از برقرار شدن آن نیز مطلع شوند. هر چند بر خلاف یک Sessin، یک تونل ذریافت اطلاعات را به صورتی قابل اطمینان گارانتی نمی کند و اطلاعات ارسالی معمولا به وسیله پروتکلی بر مبنای دیتا گرام مانند UDP هنگام استفاده از L۲TP یا TCP برای مدیریت تونل و یک پروتکل کپسوله کردن مسیر یابی عمومی اصلاح شده به نام GRE برای وقتی که PPTP استفاده می گردد، پیکربندی و ارسال می شوند. ساخته شدن تونل یک تونل باید قبل از این که تبادل اطلاعات انجام شود، ساخته شود. عملیات ساخته شدن تونل به وسیله یک طرف تونل یعنی کلاینت آغاز می شود و طرف دیگر تونل یعنی سرور، تقاضای ارتباط Tunneling را دریافت می کند. برای ساخت تونل یک عملیات ارتباطی مانند PPP انجام می شود. سرور تقاضا می کند که کلاینت خودش را معرفی کرده و معیارهای تصدیق هویت خود را ارائه نماید. هنگامی که قانونی بودن و معتبر بودن کلاینت مورد تایید قرار گرفت، ارتباط تونل مجاز شناخته شده و پیغام ساخته شدن تونل توسط کلاینت به سرور ارسال می گردد و سپس انتقال اطلاعات از طریق تونل شروع خواهد شد. برای روشن شدن مطلب، مثالی می زنیم. اگر محیط عمومی را، که غالبا نیز همین گونه است، اینترنت فرض کنیم، کلاینت پیغام ساخته شدن تونل را از آدرس IP کارت شبکه خود به عنوان مبدا به آدرس IP مقصد یعنی سرور ارسال می کند. حال اگر ارتباط اینترنت به صورت Dialup از جانب کلاینت ایجاد شده باشد، کلاینت به جای آدرس NIC خود، آدرس IP را که ISP به آن اختصاص داده به عنوان مبدا استفاده خواهد نمود. نگهداری تونل در برخی از تکنولوژی های Tunneling مانند L۲TP و PPTP، تونل ساخته شده باید نگهداری و مراقبت شود. هر دو انتهای تونل باید از وضعیت طرف دیگر تونل با خبر باشندو نگهداری یک تونل معمولا- از طریق عملیاتی به نام نگهداری فعال (KA) اجرا می گردد که طی این پروسه به صورت دوره زمانی مداوم از انتهای دیگر تونل آمار گیری می شود. این کار هنگامی که اطلاعاتی در خال تبادل نیست انجام می پذیرد. پروتکل تبادل اطلاعات تونل زمانی که یک تونل برقرار می شود، اطلاعات می توانند از طریق آن ارسال گردند. پروتکل تبادل اطلاعات تونل، اطلاعات را کپسوله کرده تا قابل عبور از تونل باشند. وقتی که تونل کلاینت قصد ارسال اطلاعات را به تونل سرور دارد، یک سرایند (مخصوص پروتکل تبادل اطلاعات) را بر روی پکت اضافه می کند. نتیجه این کار این است که اطلاعات از طریق شبکه عمومی قابل ارسال شده و تا تونل سرور مسیریابی می شوند. تونل سرور پکت ها را دریافت کرده و سرایند اضافه شده را از روی اطلاعات برداشته و سپس اطلاعات را به صورت اصلی در می آورد. انواع تونل تونل ها به دو نوع اصلی تقسیم می گردند: اختیاری و اجباری تونل اختیاری تونل اختیاری به وسیله کاربر و از سمت کامپیوتر کلاینت طی یک عملیات هوشمند، پیکربندی و ساخته می شود. کامپیوتر کاربر نقطه انتهایی تونل بوده و به عنوان تونل کلاینت عمل می کند. تونل اختیاری زمانی تشکیل می شود که کلاینت برای ساخت تونل به سمت تونل سرور مقصد داوطلب شود. هنگامی که کلاینت به عنوان تونل کلاینت قصد انجام عملیات دارد، پروتکل Tunneling مورد نظر باید بر روی سیستم کلاینت نصب گردد. تونل اختیاری می تواند در هر یک از حالت های زیر اتفاق بیفتد: -کلاینت ارتباطی داشته باشد که بتواند ارسال اطلاعات پوشش گذاری شده را از طریق مسیریابی به سرور منتخب خود انجام دهد. -کلاینت ممکن است قبل از اینکه بتواندتونل را پیکربندی کند، ارتباطی را از طریق Dialup برای تبادل اطلاعات برقرار کرده باشد. این معمول ترین حالت ممکن است. بهترین مثال از این حالت، کاربران اینترنت هستند. قبل از اینکه یک تونل برای کاربران بر روی اینترنت ساخته شود، آن ها باید به ISP خود شماره گیری کنند و یک ارتباط اینترنتی را تشکیل دهند. تونل اجباری تونل اجباری برای کاربرانی پیکربندی و ساخته می شود که دانش لازم را نداشته و یا دخالتی در ساخت تونل نخواهند داشت. در تونل اختیاری، کاربر، نقطه انتهایی تونل نیست. بلکه یک Device دیگر بین سیستم کاربر و تونل سرور، نقطه انتهایی تونل است که به عنوان تونل کلاینت

عمل می نماید. اگر پروتکل Tunneling بر روی کامپیوتر کلاینت نصب و راه انـدازی نشده و در عین حال تونل هنوز مورد نیاز و درخواست باشد. این امکان وجود دارد که یک کامپیوتر دیگر و یا یک Device شبکه دیگر، تونلی از جانب کامپیوتر کلاینت ایجـاد نمایـد. این وظیفه ای است که به یک متمرکز کننـده دسترسـی (AS) به تونـل، ارجـاع داده شـده است. در مرحله تکمیل این وظیفه، متمرکز کننده دسترسی یا همان AS باید پروتکل Tunneling منـاسب را ایجاد کرده و قابلیت برقراری تونل را در هنگام اتصـال کـامپیوتر کلاینت داشـته باشـد. هنگامی که ارتباط از طریق اینترنت برقرار می شود، کامپیوتر کلاینت یک تونل تامین شـده (NAS) Netwrk Access Service را از طریـق ISP احضـار می کنـد. به عنوان مثـال یک سازمان ممکن است قراردادی با یک ISP داشـته باشد تا بتواند کل کشور را توسط یک متمرکز کننده دسترسـی به هم پیوند دهد. این AC می تواند تونل هایی را از طریق اینترنت برقرار کند که به یک تونل سرور متصل باشند و از آن طریق به شبکه خصوصی مستقر در سازمان مذکور دسترسی پیـدا کننـد. این پیکربندی به عنوان تونل اجباری شـناخته می شود، به دلیل این که کلاینت مجبور به اسـتفاده از تونل ساخته شده به وسیله AC شده است. یک بار که این تونل ساخته شد، تمام ترافیک شـبکه از سـمت کلاینتو نیز از جانب سرور به صورت خودکار از طریق تونل مـذکور ارسال خواهـد شـد. به وسـیله این تونل اجباری، کامپیوتر کلاینت یک ارتباط PPP می سـازد و هنگامی که کلایـنت به NAS، از طریـق شـماره گیری متصـل می شـود، تونـل سـاخته می شـود و تمـام ترافیـک به طور خودکـار از طریق تونل مسیریابی و ارسـال می گردد. تونـل اجبـاری می توانـد به طور ایستا و یـا خودکـار و پویا پیکربنـدی شود. تونل های اجباری ایستا پیکربندی تونل های Static معمولا به تجهیزات خاص برای تونل های خودکار نیاز دارند. سیستم Tunneling خودکار به گونه ای اعمـال می شودکه کلاینت ها به AC از طریق شـماره گیری (Dialup) متصل می شوند. این مسئله احتیاج به خطوط دسترسی محلی اختصاصـی و نیز تجهیزات دسترسـی شبکه دارد که به این ها هزینه های جانبی نیز اضافه می گردد. برای مثال کاربران احتیاج دارنـد که با یک شـماره تلفن خاص تماس بگیرند، تا به یک AC متصـل شونـد که تمام ارتباطات را به طور خودکار به یک تونل سرور خـاص متصـل می کنـد. در طرح هـای Tunneling نـاحیه ای، متمرکز کننـده دسترسـی بخشـی از User Name را که Realm خوانده می شود بازرسی می کند تا تصمیم بگیرد در چه موقعیتی از لحاظ ترافیک شبکه، تونل را تشکیل دهد. تونل های اجبـاری پویا در این سیسـتم انتخاب مقصـد تونل بر اساس زمانی که کاربر به AC متصـل می شود، سـاخته می شود. کاربران دارای Realm یکسان، ممکن است تونل هایی با مقصد های مختلف تشکیل بدهند. البته این امر به پارامترهای مختلف آنها مانند User Name، شـماره تماسف محل فیزیکی و زمان بسـتگی دارد. تونل های Dynamic، دارای قابلیت انعطاف عالی هسـتند. همچنین تونـل هـای پویااجـازه می دهنـد کـه AC بـه عنـوان یـک سیسـتم Multi-NAS عمـل کنـد، یعنی اینکـه همزمـان هـم ارتباطـات Tunneling را قبول می کند و هم ارتباطات کلاینت های عادی و بدون تونل را. در صورتی که متمرکز کننده دسترسـی بخواهد نوع کلاینت تماس گسـرنده را مبنی بر دارای تونل بودن یا نبودن از قبل تشخیص بدهد، باید از همکاری یک بانک اطلاعاتی سود ببرد. برای این کار باید AC اطلاعات کاربران را در بانک اطلاعاتی خود ذخیره کند که بزرگترین عیب این مسئله این است که این بانـک اطلاعـاتی به خوبی قابل مـدیریت نیست. بهترین راه حل این موضوع، راه انـدازی یک سـرور RADIUS است، سروری که اجازه می دهـد که تعـداد نا محـدودی سـرور، عمل شـناسایی USER هـای خـود را بر روی یـک سـرور خـاص یعنی همین سـرور RADIUS انجام دهند، به عبارت بهتر این سـرور مرکزی برای ذخیره و شـناسایی و احراز هویت نمودن کلیه کاربران شبکه خواهد بود. پروتکل های VPN عمده ترین پروتکل هایی که به وسیله ویندوز ۲۰۰۰ برای دسترسی به VPN استفاده می شوند عبارتند از: IP-IP، IPSEC، L۲TP، PPTP. البته پروتکل امنیتی SSL نیز جزء پروتکل های مورد استفاده در VPN به شمار می آید، ولی به علت اینکه SSL بیشتر بر روی پروتکل های SMTP، PP۳، LDAP، HTTP و... مورد اسـتفاده قرار می گیرد، بحث در مورد آن را بـه فرتی دیگر موکـول می کنیـم. پروتکـل PPTP پروتکل Tunneling نقطـه به نقطه، بخش توسـعه یـافته ای از پروتکل

PPP است که فریم های پروتکل PPP را به صورت IP برای تبادل آنها از طریق یک شبکه IP مانند اینترنت توسط یک سرایند، کپسوله می کند. این پروتکل می تواند در شبکه های خصوصی از نوع LAN-t-LAN نیز استفاده گردد. پروتکل PPTP به وسیله انجمنی از شرکت های مایکروسافت، ESI، ۳cm، Ascend Cmmunicatins و US Rbtics ساخته شد. PPTP یک ارتباط TCPرا (که یک ارتباط Cnnectin riented بوده و پس از ارسال پکت منتظرAcknwledgment آن می ماند) برای نگهداری تونل و فریم های PPP کپسوله شده توسط (GRE Generic Ruting Encapsulatin) که به معنی کپسوله کردن مسیریابی عمومی است، برای Tunneling کردن اطلاعات استفاده می کند. ضمنا اطلاعات کپسوله شده PPP قابلیت رمز نگاری و فشرده شدن را نیز دارا هستند، تونل های PPTP باید به وسیله مکانیسم گواهی همان پروتکل PPP که شامل (EAP، PAP، MS-CHAP، CHAP) می شوند، گواهی شوند. در ویندوز ۲۰۰۰ رمزنگاری پروتکل PPP فقط زمانی استفاده می گردد که پروتکل احراز هویت یکی از پروتکل های TLS، EAP و یا MS-CHAP باشد. باید توجه شود که رمز نگاری PPP، محرمانگی اطلاعات را فقط بین دو نقطه نهایی یک تونل تامین می کند و در صورتی که به امنیت بیشتری نیاز باشد، باید از پروتکل Ipsec استفاده شود. پروتکل L۲TP پروتکل L۲TP ترکیبی است از پروتکل های PPTP و (۲ Layer L۲F (Frwarding که توسط شرکت سیسکو توسعه یافته است. این پروتکل ترکیبی است از بهترین خصوصیات موجود در L۲F و PPTP. L۲TP نوعی پروتکل شبکه است که فریم های PPP را برای ارسال بر روی شبکه های IP مانند اینترنت و علاوه بر این برای شبکه های مبتنی بر Frame Relay، X.۲۵ و یا ATM کپسوله می کند. هنگامی که اینترنت به عنوان زیر ساخت تبادل اطلاعات استفاده می گردد، L۲TP می تواند به عنوان پروتکل Tunneling از طریق اینترنت مورد استفاده قرار گیرد. L۲TP برای نگهداری تونل از یک سری پیغام های L۲TP و نیز از پروتکل UDP (پروتکل تبادل اطلاعات به صورت Cnnectin Less که پس از ارسال اطلاعات منتظر دریافت Acknwledgment نمی شود و اطلاعات را، به مقصد رسیده فرض می کند) استفاده می کند. در L۲TP نیز فریم های PPP کپسوله شده می توانند همزمان علاوه بر رمزنگاری شدن، فشرده نیز شوند. البته مایکروسافت پروتکل امنیتی Ipsec را به جای رمزنگاری PPP توصیه می کند. ساخت تونل L۲TP نیز باید همانند PPTP توسط مکانیسم (PPP EAP، CHAP، MS-CHAP، PAP) بررسی و تایید شود. PPTP در مقابل L۲TP هر دو پروتکل PPTP و L۲TP از پروتکل PPP برای ارتباطات WAN استفاده می کنند تا نوعی اطلاعات ابتدایی برای دیتا را فراهم کنند و سپس یک سرایند اضافه برای انتقال اطلاعات از طریق یک شبکه انتقالی به پکت الحاق بنمایند. هر چند این دو پروتکل در برخی موارد نیز با هم تفاوت دارند. برخی از این تفاوت ها عبارتند از: ۱)شبکه انتقال که PPTP احتیاج دارد، باید یک شبکه IP باشد. ولی L۲TP فقط به یک تونل احتیاج دارد تا بتواند ارتباط Pint-t-Pint را برقرار کند. حال این تونل می تواند بر روی یک شبکه IP باشد و یا بر روی شبکه های دیگر مانند X.۲۵، Frame Relay و یا L۲TP(۲ .ATM قابلیت فشرده سازی سرایند را داراست. هنگامی که فشرده سازی سرایند انجام می گیرد، L۲TP با حجم ۴ بایت عمل می کند، در حالی که PPTP با حجم ۶ بایت عمل می نماید. ۳)L۲TP متد احراز هویت را تامین می کند، در حالی که PPTP این گونه عمل نمی کند، هر چند وقتی که PPTP یا L۲TP از طریق پروتکل امنیتی Ipsec اجرا می شوند، هر دو، متد احراز هویت را تامین می نمایند. ۴)PPTP رمزنگاری مربوط به PPP را استفاده می کند، ولی L۲TP از پروتکل Ipsec برای رمزنگاری استفاده می نماید. پروتکل Ipsec یک پروتکل tunneling لایه سوم است که از متد ESP برای کپسوله کردن و رمزنگاری اطلاعات IP برای تبادل امن اطلاعات از طریق یک شبکه کاری IP عمومی یا خصوصی پشتیبانی می کند. Ipsec به وسیله متد ESP می تواند اطلاعات IP را به صورت کامل کپسوله کرده و نیز رمزنگاری کند. به محض دریافت اطلاعات رمزگذاری شده، تونل سرور، سرایند اضافه شده به IP را پردازش کرده و سپس کنار می گذارد و بعد از آن رمزهای ESP و پکت را باز می کند. بعد از این مراحل است که پکت

IP به صورت عادی پردازش می شود. پردازش عادی ممکن است شامل مسیریابی و ارسال پکت به مقصد نهایی آن باشد. پروتکل IP-IP این پروتکل که با نام IP-IN-IP نیز شناخته می شود، یک پروتکل لایه سوم یعنی لایه شبکه است. مهمترین استفاده پروتکل IP-IP برای ایجاد سیستم Tunneling به صورت Multicast است که در شبکه هایی که سیستم مسیریابی Multicast را پشتیبانی نمی کنند کاربرد دارد. ساختار پکت IP-IPتشکیل شده است از: سرایند IPخارجی، سرایند تونل، سرایند IP داخلی و اطلاعات IP. اطلاعات IP می تواند شامل هر چیزی در محدوده IP مانند ICMP، UDP، TCP و اطلاعات اصلی پکت باشد. مدیریت VPN در بیشتر موارد مدیریت یک VPN مانند مدیریت یک RAS سرور (به طور خلاصه، سروری که ارتباط ها و Cnnectin های برقرار شده از طریق راه دور را کنترل و مدیریت می کند)، می باشد. البته امنیت VPN باید به دقت توسط ارتباطات اینترنتی مدیریت گردد. مدیریت کاربران VPN بیشتر مدیران شبکه برای مدیریت کاربران خود ار یک پایگاه داده مدیریت کننده اکانت ها برروی کامپیوتر DC و یا از سرور RADIUS استفاده می نمایند. این کار به سرور VPN اجازه می دهد تا اعتبارنامه احراز هویت کاربران را به یک سیستم احراز هویت مرکزی ارسال کند. مدیریت آدرس ها و Name Server ها سرور VPN باید رشته ای از آدرس های IP فعال را در خود داشته باشد تا بتواند آنها را در طول مرحله پردازش ارتباط از طریق پروتکل کنترل IP به نام IPCP به درگاه های VPN Server یا Client اختصاص دهد. در VPN هایی که مبتنی بر ویندوز ۲۰۰۰ پیکربندی می شوند، به صورت پیش فرض، IP آدرس هایی که به Client های VPN اختصاص داده می شود، از طریق سرور DHCP گرفته می شوند. البته همان طور که قبلا گفته شد شما می توانید یک رشته IP را به صورت دستی یعنی ایستا به جای استفاده از DHCP اعمال کنید. ضمنا VPN Server باید توسط یک سیستم تامین کننده نام مانند DNS و یا WINS نیز پشتیبانی شود تا بتواند سیستم IPCP را به مورد اجرا بگذارد.

بخش اول

برقرار کردن امنیت برای یک شبکه درون یک ساختمان کار ساده ای است . اما هنگامی که بخواهیم از نقاط دور رو ی داده های مشترک کار کنیم ایمنی به مشکل بزرگی تبدیل می شود . در این بخش به اصول و ساختمان یک VPN برای سرویس گیرنده های ویندوز و لینوکس می پردازیم . اصول VPN فرستادن حجم زیادی از داده از یک کامپیوتر به کامپیوتر دیگر مثلا" در به هنگام رسانی بانک اطلاعاتی یک مشکل شناخته شده و قدیمی است . انجام این کار از طریق Email به دلیل محدودیت گنجایش سرویس دهنده Mail نشدنی است . استفاده از FTP هم به سرویس دهنده مربوطه و همچنین ذخیره سازی موقت روی فضای اینترنت نیاز دارد که اصلا" قابل اطمینان نیست . یکی از راه حل های اتصال مستقیم به کامپیوتر مقصد به کمک مودم است که در اینجا هم علاوه بر مودم ، پیکر بندی کامپیوتر به عنوان سرویس دهنده RAS لازم خواهد بود . از این گذشته ، هزینه ارتباط تلفنی راه دور برای مودم هم قابل تامل است . اما اگر دو کامپیوتر در دو جای مختلف به اینترنت متصل باشند می توان از طریق سرویس به اشتراک گذاری فایل در ویندوز بسادگی فایل ها را رد و بدل کرد . در این حالت ، کاربران می توانند به سخت دیسک کامپیوترهای دیگر همچون سخت دیسک کامپیوتر خود دسترسی داشته باشند . به این ترتیب بسیاری از راه های خرابکاری برای نفوذ کنندگان بسته می شود . شبکه های شخصی مجاری یا Virtual private Netwrk) VPN) ها اینگونه مشکلات را حل می کند . VPN به کمک رمز گذاری روی داده ها ، درون یک شبکه کوچک می سازد و تنها کسی که آدرس های لازم و رمز عبور را در اختیار داشته باشد می تواند به این شبکه وارد شود . مدیران شبکه ای که بیش از اندازه وسواس داشته و محتاط هستند می توانند VPN را حتی روی شبکه محلی هم پیاده کنند . اگر چه نفوذ کنندگان می توانند به کمک برنامه های Packet sniffer جریان داده ها را دنبال کنند اما بدون داشتن کلید رمز نمی توانند آنها را بخوانند . -۴.۱.۱ VPN چیست ؟ VPN دو

کامپیوتر یا دو شبکه را به کمک یک شبکه دیگر که به عنوان مسیر انتقال به کار می گیرد به هم متصل می کند . برای نمونه می توان ب دو کامپیوتر یکی در تهران و دیگری در مشهد که در فضای اینترنت به یک شبکه وصل شده اند اشاره کرد . VPN از نگاه کاربر کاملا" مانند یک شبکه محلی به نظر می رسد . برای پیاده سازی چنین چیزی ، VPN به هر کاربر یک ارتباط IP مجازی می دهد . داده هایی که روی این ارتباط آمد و شد دارند را سرویس گیرنده نخست به رمز در آورده و در قالب بسته ها بسته بندی کرده و به سوی سرویس دهنده VPN می فرستد . اگر بستر این انتقال اینترنت باشد بسته ها همان بسته های IP خواهند بود . سرویس گیرنده VPN بسته ها را پس از دریافت رمز گشایی کرده و پردازش لازم را روی آن انجام می دهد . در آدرس http://www.WWN.CM\W-baeten\gifani\vpnani.gif شکل بسیار جالبی وجود دارد که چگونگی این کار را نشان می دهد . روشی که شرح داده شد را اغلب Tunneling یا تونل زنی می نامند چون داده ها برای رسیدن به کامپیوتر مقصد از چیزی مانند تونل می گذرند . برای پیاده سازی VPN راه های گوناگونی وجود دارد که پر کاربرد ترین آنها عبارتند از Pint t pint Tunneling prtcl یا PPTP که برای انتقال NetBEUI روی یک شبکه بر پایه IP مناسب است . ۲ Layer Tunneling prtcl یا L۲TP که برای انتقال IPX ، IP یا NetBEUI روی هر رسانه دلخواه که توان انتقال Datagram های نقطه به نقطه (Pint t pint) را داشته باشد مناسب است . برای نمونه می توان به Frame Relay ، X.۲۵ ، IP یا ATM اشاره کرد . IP Security prtcl یا Ipsec که برای انتقال داده های IP روی یک شبکه بر پایه IP مناسب است . ۴.۱.۲- پروتکل های درون تونل Tunneling را می توان روی دو لایه از لایه های SI پیاده کرد . PPTP و L۲TP از لایه ۲ یعنی پیوند داده استفاده کرده و داده ها را در قالب Frame های پروتکل نقطه به نقطه (PPP) بسته بندی می کنند . در این حالت می توان از ویژگی های PPP همچون تعیین اعتبار کاربر ، تخصیص آدرس پویا (مانند DHCP) ، فشرده سازی داده ها یا رمز گذاری داده ها بهره برد. با توجه به اهمیت ایمنی انتقال داده ها درVPN ، دراین میان تعیین اعتبار کاربر نقش بسیار مهمی دارد . برای این کار معمولا" از CHAP استفاده می شود که مشخصات کاربر را در این حالت رمز گذاری شده جابه جا میکند . Call back هم دسترسی به سطح بعدی ایمنی را ممکن می سازد . در این روش پس از تعیین اعتبار موفقیت آمیز ، ارتباط قطع می شود . سپس سرویس دهنده برای برقرار کردن ارتباط جهت انتقال داده ها شماره گیری می کند . هنگام انتقال داده ها ، Packet های ، IP IP X یا NetBEUI در قالب Frame های PPP بسته بندی شده و فرستاده می شوند . PPTP هم Frame های PPP را پیش از ارسال روی شبکه بر پایه IP به سوی کامپیوتر مقصد ، در قالب Packet های IP بسته بندی می کند . این پروتکل در سال ۱۹۹۶ از سوی شرکت هایی چون مایکرو سافت ، ۳ cm ، Ascend و Rbtics US پایه گذاری شد . محدودیت PPTP در کار تنها روی شبکه های IP باعث ظهور ایده ای در سال ۱۹۹۸ شد .L۲TP روی Frame Relay، X.۲۵ یا ATM هم کار می کند . برتری L۲TP در برابر PPTP این است که به طور مستقیم روی رسانه های گوناگون WAN قابل انتقال است ۴.۱.۳ - -VPN Ipsec فقط برای اینترنت Ipsec برخلافPPTP و L۲TP روی لایه شبکه یعنی لایه سوم کار می کند . این پروتکل داده هایی که باید فرستاده شود را همراه با همه اطلاعات جانبی مانند گیرنده و پیغام های وضعیت رمز گذاری کرده و به آن یک IP Header معمولی اضافه کرده و به آن سوی تونل می فرستد کامپیوتری که در آن سو قرار دارد IP Header را جدا کرده ، داده ها را رمز گشایی کرده و آن را به کامپیوتر مقصد می فرستد .Ipsec را می توان با دو شیوه Tunneling پیکر بندی کرد . در این شیوه انتخاب اختیاری تونل ، سرویس گیرنده نخست یک ارتباط معمولی با اینترنت برقرار می کند و سپس از این مسیر برای ایجاد اتصال مجازی به کامپیوتر مقصد استفاده می کند . برای این منظور ، باید روی کامپیوتر سرویس گیرنده پروتکل تونل نصب شده باشد . معمولا" کاربر اینترنت است که به اینترنت وصل می شود . اما کامپیوترهای درون LAN هم می توانند یک ارتباط VPN برقرا کنند . از آنجا که ارتباط IP از پیش موجود است تنها برقرار کردن ارتباط VPN کافی است . در شیوه تونل اجباری ،

سرویس گیرنده نباید تونل را ایجاد کند بلکه این کار ار به عهده فراهم ساز (Service prvider) است . سرویس گیرنده تنها باید به ISP وصل شود . تونل به طور خودکار از فراهم ساز تا ایستگاه مقصد وجود دارد . البته برای این کار باید همانگی های لازم با ISP انجام بگیرد . ویژگی های امنیتی در IPsec Ipsec از طریق AH (Authenticatin Header) مطمئن می شود که Packet های دریافتی از سوی فرستنده واقعی (و نه از سوی یک نفوذ کننده که قصد رخنه دارد) رسیده و محتویات شان تغییر نکرده . AH اطلاعات مربوط به تعیین اعتبار و یک شماره توالی (Seguence Number) در خود دارد تا از حملات Replay جلوگیری کند . اما AH رمز گذاری نمی شود . رمز گذاری از طریق Encapsulatin Security Header یا ESH انجام می گیرد . در این شیوه داده های اصلی رمز گذاری شده و VPN اطلاعاتی را از طریق ESH ارسال می کند . ESH همچنین کارکرد هایی برای تعیین اعتبار و خطایابی دارد . به این ترتیب دیگر به AH نیازی نیست . برای رمز گذاری و تعیین اعتبار روش مشخص و ثابتی وجود ندارد اما با این همه ، IETF برای حفظ سازگاری میان محصولات مختلف ، الگوریتم های اجباری برای پیاده سازی Ipsec تدارک دیده . برای نمونه می توان به DES ، MD۵ یا Secure Hash Algrithm اشاره کرد . مهمترین استانداردها و روش هایی که در Ipsec به کار می روند عبارتند از : Diffie-Hellman برای مبادله کلید ها میان ایستگاه های دو سر ارتباط . رمز گذاری Public Key برای ثبت و اطمینان از کلیدهای مبادله شده و همچنین اطمینان از هویت ایستگاه های سهیم در ارتباط . الگوریتم های رمز گذاری مانند DES برای اطمینان از درستی داده های انتقالی . الگوریتم های درهم ریزی (Hash) برای تعیین اعتبار تک تک Packet ها . امضاهای دیجیتال برای تعیین اعتبارهای دیجیتالی . ۴.۱.۵ – Ipsec بدون تونل Ipsec در مقایسه با دیگر روش ها یک برتری دیگر هم دارد و آن اینست که می تواند همچون یک پروتکل انتقال معمولی به کار برود . در این حالت برخلاف حالت Tunneling همه IP packet رمز گذاری و دوباره بسته بندی نمی شود . بجای آن ، تنها داده های اصلی رمزگذاری می شوند و Header همراه با آدرس های فرستنده و گیرنده باقی می ماند . این باعث می شود که داده های سرباز (verhead) کمتری جابجا شوند و بخشی از پهنای باند آزاد شود . اما روشن است که در این وضعیت ، خرابکاران می توانند به مبدا و مقصد داده ها پی ببرند . از آنجا که در مدل SI داده ها از لایه ۳ به بالا رمز گذاری می شوند خرابکاران متوجه نمی شوند که این داده ها به ارتباط با سرویس دهنده Mail مربوط می شود یا به چیز دیگر . ۴.۱.۶– جریان یک ارتباط Ipsec بیش از آن که دو کامپیوتر بتوانند از طریق Ipsec داده ها را میان خود جابجا کنند باید یکسری کارها انجام شود • . نخست باید ایمنی برقرار شود . برای این منظور ، کامپیوترها برای یکدیگر مشخص می کنند که آیا رمز گذاری ، تعیین اعتبار و تشخیص خطا یا هر سه آنها باید انجام بگیرد یا نه • . سپس الگوریتم را مشخص می کنند ، مثلا" DEC برای رمزگذاری و MD۵ برای خطایابی •. در گام بعدی ، کلیدها را میان خود مبادله می کنند . Ipsec برای حفظ ایمنی ارتباط از SA) Security Assciatin) استفاده می کند . SA چگونگی ارتباط میان دو یا چند ایستگاه و سرویس های ایمنی را مشخص می کند . SA ها از سوی SPI (Security parameter Index) شناسایی می شوند . SPI از یک عدد تصادفی و آدرس مقصد تشکیل می شود . این به آن معنی است که همواره میان دو کامپیوتر دو SPI وجود دارد : یکی برای ارتباط A و B و یکی برای ارتباط B به A . اگر یکی از کامپیوترها بخواهد در حالت محافظت شده داده ها را منتقل کند نخست شیوه رمز گذاری مورد توافق با کامپیوتر دیگر را بررسی کرده و آن شیوه را روی داده ها اعمال می کند . سپس SPI را در Header نوشته و Packet را به سوی مقصد می فرستد . ۴.۱.۷ – مدیریت کلیدهای رمز در Ipsec اگر چه Ipsec فرض را بر این می گذارد که توافقی برای ایمنی داده ها وجود دارد اما خودش برای ایجاد این توافق نمی تواند کاری انجام بدهد . Ipsec در این کار به (IKE Internet Key Exchange) تکیه می کند که کارکردی همچون IKMP (Key Management Prtcl) دارد. برای ایجاد SA هر دو کامپیوتر باید نخست تعیین اعتبار شوند . در حال حاضر برای این کار از راه های زیر استفاده می شود : Pre

shared keys : روی هر دو کامپیوتر یک کلید نصب می شود که IKE از روی آن یک عدد Hash ساخته و آن را به سوی کامپیوتر مقصد می فرستد . اگر هر دو کامپیوتر بتوانند این عدد را بسازند پس هر دو این کلید دارند و به این ترتیب تعیین هویت انجام می گیرد . رمز گذاری Public Key : هر کامپیوتر یک عدد تصادفی ساخته و پس از رمز گذاری آن با کلید عمومی کامپیوتر مقابل ، آن را به کامپیوتر مقابل می فرستد .اگر کامپیوتر مقابل بتواند با کلید شخصی خود این عدد را رمز گشایی کرده و باز پس بفرستد برا ی ارتباط مجاز است . در حال حاضر تنها از روش RSA برای این کار پیشنهاد می شود . امضاء دیجیتال : در این شیوه ، هر کامپیوتر یک رشته داده را علامت گذاری (امضاء) کرده و به کامپیوتر مقصد می فرستد . در حال حاضر برای این کار از روش های RSA و Digital Singature Standard) DSS) استفاده می شود . برای امنیت بخشیدن به تبادل داده ها باید هر دو سر ارتبا طنخست بر سر یک یک کلید به توافق می رسند که برای تبادل داده ها به کار می رود . برا ی این منظور می توان همان کلید به دست آمده از طریق Diffie Hellman را به کاربرد که سریع تر است یا یک کلید دیگر ساخت که مطمئن تر است . ۴.۱.۸ – خلاصه تبادل داده ها روی اینرنت چندان ایمن نیست . تقریبا" هر کسی که در جای مناسب قرار داشته باشد می تواند جریان داده ها را زیر نظر گرفته و از آنها سوء استفاده کند . شبکه های شخصی مجازی یا VPN ها کار نفوذ را برا ی خرابکاران خیلی سخت می کند .

بخش دوم

استفاده از اینترنت به عنوان بستر انتقال داده ها هر روزگسترش بیشتری پیدا می کند . باعث می شود تا مراجعه به سرویس دهندگان وب و سرویس های Email هر روز بیشتر شود . با کمی کار می توان حتی دو کامپیوتر را که در دو قاره مختلف قرار دارند به هم مرتبط کرد . پس از برقراری این ارتباط ، هر کامپیوتر،کامپیوتر دیگر را طوری می بیند که گویا در شبکه محلی خودش قرار دارد. از این رهگذر دیگر نیازی به ارسال داده ها از طریق سرویس هایی مانند Email نخواهند بود. تنها اشکال این کار این است که در صورت عدم استفاده از کارکردهای امنیتی مناسب، کامپیوترها کاملا در اختیار خرابکارن قرار می گیرند. VPN ها مجموعه ای از سرویس های امنیتی ردر برابراین عملیات رافراهم می کنند. در بخش قبلی با چگونگی کار VPN ها آشنا شدید و در اینجا به شما نشان می دهیم که چگونه می توان در ویندوز یک VPN شخصی راه انداخت. برای این کار به نرم افزار خاصی نیاز نیست چون مایکروسافت همه چیزهای لازم را در سیستم عامل گنجانده یا در پایگاه اینترنتی خود به رایگان در اختیار همه گذاشته. پیش نیازها برای اینکه دو کامپیوتر بر پایه ویندوز بتواند از طریق VPN به هم مرتبط شوند دست کم یکی از آنها باید به ویندوز NT یا ۲۰۰۰ کار کند تا نقش سرویس دهنده VPN را به عهده بگیرد. ویندوز های ۹x یا Me تنها می توانند سرویس گیرنده VPN باشند. سرویس دهنده VPN باید یک IP ثابت داشته باشد. روشن است که هر دو کامپیوتر باید به اینترنت متصل باشند. فرقی نمی کند که این اتصال از طریق خط تلفن و مودم باشد یا شبکه محلی. IP در سرویس دهنده VPN باید مجاز (Valid) باشد تا سرویس گیرنده بتواند یک مستقیما آن را ببیند. در شبکه های محلی که اغلب از IP های شخصی (X.X.۱۹۲.۱۶۸) استفاده می شود VPN را باید روی شبکه ایجاد کرد تا ایمنی ارتباط بین میان کامپیوترها تامین شود. اگر سرویس گیرنده VPN با ویندوز ۹۵ کار می کند نخست باید ۱.۳ Dial up Netwrking Upgrade را از سایت مایکروسافت برداشت کرده و نصب کنید. این مجموعه برنامه راه اندازهای لازم برای VPN را در خود دارد . البته مایکروسافت پس از ۱.۳ Netwrking Dial up Upgrade نگارش های تازه تری نیز عرضه کرده که بنا بر گفته خودش ایمنی و سرعت ارتباط VPN را بهبود بخشیده است . نصب سرویس دهنده VPN روی کامپیوتر بر پایه ویندوز NT نخست باید در بخش تنظیمات شبکه، راه انداز Pint t Pint Tunneling را نصب کنید. هنگام این کار، شمار ارتباط های همزمان VPN پرسیده می شود. در سرویس دهنده های NT این عدد می تواند حداکثر ۲۵۶

باشد. در ایستگاه کاری NT، این عدد باید ۱ باشد چون این سیستم عامل تنها اجازه یک ارتباط RAS را می دهد. از آنجا که ارتباط VPN در قالب Remte Access برقرار می شود ویندوز NT به طور خودکار پنجره پیکر بندی RAS را باز می کند. اگر RAS هنوز نصب نشده باشد ویندوز NT آن را نصب می کند. هنگام پیکربندی باید VPN Adapter را به پورت های شماره گیری اضافه کنید. اگر می خواهید که چند ارتباط VPN داشته باشید باید این کار را برای هر یک از VPN Adapter ها انجام دهید . پیکربندی سرویس دهنده RAS اکنون باید VPN Adapterرا به گونه ای پیکربندی کنید که ارتباطات به سمت درون (incming) اجازه بدهد. نخست باید پروتکل های مجاز برای این ارتباط را مشخص کنید . همچنین باید شیوه رمز گذاری را تعیین کرده و بگویید که آیاسرویس دهنده تنها اجازه دسترسی به کامپیوترهای موجود در شبکه کامپیوتر ویندوز NT، در این وضیعت، سرویس دهنده VPN می تواند کار مسیر یابی را هم انجام دهد. برای بالاتر بردن ایمنی ارتباط، می توانید NetBEUI را فعال کرده و از طریق آن به کامپیوترهای دور اجازدسترسی به شبکه خود را بدهید. سرویس گیرنده، شبکه و سرویس های اینترنتی مربوط به سرویس دهنده VPN را نمی بینید . برای راه انداختن TCP/IP همراه با VPN چند تنظیم دیگر لازم است. اگر سرویس دهنده DHCP ندارید باید به طور دستی یک فضای آدرس(IP) Adress Pl را مشخص کنید. به خاطر داشته باشید که تنها باید از IP های شخصی (Private) استفاده کنید. این فضای آدرس باید دست کم ۲ آدرس داشته باشد ، یکی برای سرویس دهنده VPN و دیگری برای سرویس گیرنده VPN . هر کار بر باید برای دسترسی به سرویس دهنده از طریق VPN مجوز داشته باشد. برای این منظور باید در User Manager در بخش Dialing اجازه دسترسی از دور را بدهید . به عنوان آخرین کار،Remte Access Server را اجرا کنید تا ارتباط VPN بتواند ایجاد شود. سرویس گیرنده VPN روی ویندوز NT نصب سرویس گیرنده VPN روی ویندوز NT شبیه راه اندازی سرویس دهنده VPN است بنابراین نخست باید ۴ مرحله گفته شده برای راه اندازی سرویس دهنده VPN را انجام بدهید، یعنی: . نصب PPTP . تعیین شمار ارتباط ها . اضافه کردن VPN به عنوان دستگاه شماره گیری . پیکر بندی VPN Adapter در RAS، تنها تفاوت در پیکر بندی VPN Adapter آن است که باید به جای ارتباط های به سمت درون به ارتباط های به سمت بیرون (ut ging) اجاز ه بدهید . . سپس تنظیمات را ذخیره کرده و کامپیوتر را بوت کنید. در گام بعدی، در بخش Netwrking یک ارتباط(Cnnectin) تلفنی بسازید . به عنوان دستگاه شماره گیر یا همان مودم باید VPN Adapter را انتخاب کرده و بجای شماره تلفن تماس، IP مربوط به سرویس دهنده VPN را وارد کنید. در اینجا پیکر بندی سرویس گیرنده VPN روی ویندوز NT به پایان می رسد و شبکه های شخصی مجازی ساخته می شود. سرویس گیرنده VPN روی ویندوز ۲۰۰۰ راه اندازی سرویس گیرنده VPN ساده تر و کم زحمت تر از سرویس دهنده آن است. در ویندوز ۲۰۰۰ به بخش مربوط به تنظیمات شبکه رفته یک Cnnectin تازه بسازید. گام نخست : Assistant در ویندوز ۲۰۰۰ پیکر بندی VPN را بسیار ساده کرده. به طور معمول باید آدرس IP مربوط به سرویس دهنده VPN ر اداشته باشد. در اینجا باید همان IP معمولی را وارد کنید و نه IP مربوط به شبکه VPNرا، با این کار ، VPN پیکر بندی شده و ارتباط بر قرار می شود. برای تعیین صلاحیت، باید نام کاربری و رمز عبور را وارد کنید که اجازه دسترسی از طریق Remte Access را داشته باشید. ویندوز ۲۰۰۰ بی درنگ ارتباط برقرار کرده و شبکه مجازی کامل می شود. گام دوم: کافی است آدرس IP مربوط به سرویس دهنده VPN را وارد کنید. گام سوم: در پایان فقط کافی است خود را معرفی کنید. سرویس گیرنده VPN روی ویندوز ۹x نصب سرویس گیرنده VPN روی ویندوز های ۹۵، ۹۸ و ۹۸ SE مانند هم است . نخست باید پشتیبانی از VPN فعال شود. در اینجا بر خلاف ویندوز NT به جای اضافه کردن پروتکل باید یک کارت شبکه نصب کنید. ویندوز ۹ x همه عناصر لازم را نصب می کند. به این ترتیب کار نصب راه اندازاها را هم کامل می گردد. در قدم بعدی باید Dialup adapter یک Cnnectin بسازید. به عنوان دستگاه شمار گیر باید VPN adapter را معرفی کنید. گام نخست: نصب VPN adapter گام دوم: یک Cnnectin

تازه روی VPN dapter در ویندوز x۹، سیستم عامل IP مربوط به سرویس ۹۰ دهنده VPN را در خواست می کند. گام سوم: آدرس IP مربوط به سرویس دهنده VPN را وارد کنید. پیکر بندی سرویس گیرنده VPN در اینجا پایان یافته و ارتباط می تواند برقرار شود. تنها کافی است که نام کاربری و رمز عبور را وارد کنید. اکنون ویندوز به اینترنت وصل شده و تونل را می سازد و داده های خصوصی می تواند حرکت خود را آغاز کنند. برنامه های کمکی اگر بخواهید برای نمونه از دفتر کار(سرویس گیرنده VPN) به کامپیوتر خود در خانه (سرویس گیرنده VPN) وصل بشوید با دو مشکل روبرو خواهید شد. نخست اینکه کامپیوتری که در خانه دارید پیوسته به اینترنت متصل نیست و دیگری اینکه سرویس گیرنده VPN به یک آدرس IP نیاز دارد. این IP را هنگامی که از یک شرکت فراهم ساز (ISP) سرویس می گیرید از پیش نمی دانید چون به صورت پویا(dynamic) به شما تخصیص داده می شود. nline Jack برنامه ای است که برای هر دو مشکل راه حل دارد. nline Jack یک برنامه کوچک است که باید روی کامپیوتر خانه نصب شود. از دفتر کار خود می توانید از طریق سایت nline Jack و با نام کاربری و رمز عبور به کامپیوتر خود در خانه متصل شوید. با این کار، IP که شرکت فراهم ساز به شما تخصیص داده مشخص می شود که از روی آن، سرویس گیرنده VPN پیکر بندی شده و کار خود را آغاز می کند. از این دست برنامه های کمکی موارد زیادی وجود دارد که با جستجو در اینترنت می توانید آنها را بیابید. خلاصه دامنه کاربردی VPN گسترده و گوناگون است. VPN را می توان برای متصل کردن کاربران بیرونی به شبکه محلی، ارتباط دو کامپیوتر یا دو شبکه در دو شهر مختلف یا دسترسی از دفتر کار به کامپیوتر منزل بکار برد. VPN نه تنها داده ها را با ایمنی بیشتر منتقل می کند بلکه وقتی از آن برای مرتبط کردن دو کامپیوتر دور از هم استفاده می کنیم هزینه ها بسیار کاهش می یابد. آخرین نکته اینکه راه اندازی VPN ساده و رایگان است.

بخش سوم

VPN با لینوکس (۱) یکی از توانایی های VPN امکان کاربران دور از شبکه(Remte) در دسترسی به آ ن است . IPsec در این میان نقش مهمی در فراهم کردن ایمنی لازم برای داده ها دارد . یکی از مناسب ترین و به صرفه ترین وسیله ها در پیاده سازی این امکانات لینوکس و Free S/WAN که در این بخش به آن می پردازیم . IPsec و Free S/WAN اگر چه لینوکس هم به دلیل توانایی های خوبFirewall بستر بسیار مناسبی برای یک دروازه امنیتی(Security Gateway) برپایه IPsec است مال خودش به طور پیش فرض بخش های لازم برای IPsec را به همراه ندارد. این برنامه ها را می توانید در مجموعه Free S/WAN بیابید. Free S/WAN (www.fresswan.rg) در اصل مجمعی متشکل از برنامه نویسان زبده و تامین کنندگان مالی است که برنامه های ویژه لینوکس را فراهم می کنند. برنامه Free S/WAN از دو بخش اصلی تشکیل شده یکی KLIPS(Kernel IPsec) است که پروتکل های لازم را به Kernel اضافه می کند و دیگری Daemn که وظیفهبرقراری ارتباط و رمز گذاری را بر عهده دارد. در این بخش می بینید که IPsec چگونه کار می کند و چگونه باید آن را به کمک Free S/WAN در لینوکس برای VPN پیکر بندی کرد. در ادامه خواهیم گفت که با X.۵۰۹ چطور زیر ساخت های لازم برای یک شرکت پیاده سازی می شود. نگاهی به IPsec IPsec در اصل مجموعه ای از پروتکل ها و روش هایی است که به کمک آنها می توان روی اینترنت یک ارتباط مطمئن و ایمن ایجاد کرد. جزییات IPsec یا Internet Prtcl Security در RFC های شماره ۲۴۰۱ تا ۲۴۱۰ آمده. IPsec برای اطمینان بخشیدن به ارتباط های اینترنتی از شیوه های تعیین اعتبار و رمز گذاری داده ها استفاده می کند. برای این منظور در لایه شبکه دو حالت انتقال و دو لایه ایمنی فراهم می کند. Transprt در مقایسه با Tunnel در حالت Transprt دو میزبان به طور مستقیم روی اینترنت با هم گفتگو می کنند. در این حالت می توان IPsec را برای تعیین اعتبار و همچنین یکپارچگی و درستی داده ها به کار برد. به کمک IPsec نه تنها می توان از هویت طرف گفتگو

مطمئن شدبلکه می توان نسبت به درستی و دست نخوردگی داده هاهم اطمینان حاصل کرد . به کمک عملکرد رمز گذاری می توان افزون بر آن خوانده شدن داده ها از سوی افراد غیر مجاز جلوگیری کرد. اما از آنجا که در این شیوه، دو کامپیوتر به طور مستقیم داده ها را مبادله میکنند نمی توان مبدا و مقصد داده ها را پنهان کرد. از حالت Tunnel هنگامی که استفاده می شود که دست کم یکی از کامپیوترها به عنوان Security Gateway به کار برود. در این وضعیت حداقل یکی از کامپیوترهایی که در گفتگو شرکت می کند در پشت Gateway قراردارد و در نتیجه ناشناس می ماند. حتی اگر دو شبکه از از طریق Security Gateway های خود با هم داده مبادله کنند نمی توان از بیرون فهمید که دقیقا کدام کامپیوتر به تبادل داده مشغول است. در حالت Tunnel هم می توان از کارکردهای تعیین اعتبار ،کنترل درستی داده ها و رمز گذاری بهره برد. Authenticatin Header وظیفه Authenticatin Header IP آن است که داده های در حال انتقال بدون اجازه از سوی شخص سوم مورد دسترسی و تغییر قرار نگیرد . برای این منظور از روی Header مربوط به IP و داده های اصلی یک عددHash به دست آمده و به همراه فیلدهای کنترلی دیگر به انتهای Header اضافه می شود. گیرنده با آزمایش این عدد می تواند به دستکاری های احتمالی در Header یا داده های اصلی پی ببرد. Authenticatin Header هم در حالت Transprt و هم در حالت Tunnel کاربرد دارد. AH در حالت Transprt میان Header مربوط به IP و داده های اصلی می نشیند . در مقابل، در حالت Gateway ، Tunneling کل Paket را همراه با Header مربوط به داده ها در یک IP Packet بسته بندی می کند. در این حالت، AH میان Header جدید و Packet اصلی قرار می گیرد. AH در هر دو حالت، اعتبار و سلامت داده ها را نشان می دهد اما دلیلی بر قابل اطمینان بودن آنها نیست چون عملکرد رمز گذاری ندارد. Encapsulated Security Paylad Encapsulated Security Paylad IP برای اطمینان از ایمنی داده ها به کار می رود . این پروتکل داده ها در قالب یک Header و یک Trailer رمز گذاری می کند. به طوری اختیاری می توان به انتهای Packet یک فیلدESP Auth اضافه کرد که مانند AH اطلاعات لازم برای اطمینان از درستی داده ها رمز گذاری شده را در خود دارد. در حالت ،Transprt Header مربوط به ESP و Trailer تنها داده های اصلی IP از پوشش می دهند و Header مربوط به Packet بدون محافظ باقی می ماند. اما در حالت Tunneling همه Packet ارسالی از سوی فرستنده، داده اصلی به شمار می رود و Security Gateway آن را در قالب یک Packet مربوط به IP به همراه آدرس های فرستنده و گیرنده رمز گذاری می کند. در نتیجه،ESP نه تنها اطمینان از داده ها بلکه اطمینان از ارتباط را هم تامین می کند . در هر دوحالت، ESP در ترکیب با AH ما را از درستی بهترین داده های Header مربوط به IP مطمئن می کند. Security Assciatin برای اینکه بتوانESP/AH را به کار برد باید الگوریتم های مربوط به درهم ریزی(Hashing)، تعیین اعتبار و رمز گذاری روی کامپیوترهای طرف گفتگو یکسان باشد. همچنین دو طرف گفتگو باید کلیدهای لازم و طول مدت اعتبار آنها را بدانند. هر دو سر ارتباط IPsec هر بار هنگام برقرار کردن ارتباط به این پارامترهای نیاز دارند. SA یا Security Assciatin به عنوان یک شبه استاندارد در این بخش پذیرفته شده. برای بالا بردن امنیت، از طریق SA می توان کلیدها را تا زمانی که ارتباط برقرار است عوض کرد. این کار را می توان در فاصله های زمانی مشخص یا پس از انتقال حجم مشخصی از داده ها انجام داد. Internet Key Exchang پروتکل Internet Key Exchang یا RFC ۲۴۰۹) IKE(روند کار روی IPsec SA را تعریف می کند. این روش را Internet Security Assciatin and Key Management Prtcl یا ISAKMP نیز می نامند. این پروتکل مشکل ایجاد ارتباط میان دو کامپیوتر را که هیچ چیز از هم نمی دانند و هیچ کلیدی ندارند حل می کند. در نخستین مرحله IKE(IKE Phase ۱) که به آن حالت اصلی(Main Mde) هم گفته می شود دو طرف گفتگو نخست بر سر پیکر بندی ممکن برای SA و الگوریتم های لازم برای درهم ریزی (Hashing)، تعیین اعتبار و رمزگذاری به توافق می رسند. آغاز

کننده(Initiatr) ارتباط به طرف مقابل(یا همان Respnder) چند گزینه را پیشنهاد می کند. Respnder هم مناسب ترین گزینه را انتخاب کرده و سپس هر دو طرف گفتگو، از طریق الگوریتم Diffie-Hellman یک کلید رمز(Secret Key) می سازند که پایه همه رمز گذاری های بعدی است. به این ترتیب صلاحیت طرف مقابل برای برقراری ارتباط تایید می شود. اکنون مرحله دوم IKE Phase) ۲)IKE آغاز می گردد که حالت سریع (uick Mde) هم نامیده می شود. این مرحله SA مربوط به IPsec را از روی پارامترهای مورد توافق برا ی ESP و AH می سازد. گواهینامه X.۵۰۶ همانطور که پیش از این گفتیم بهترین راه برای تبادل Public Key ها Certificate(RFC X.۵۰۹ شماره ۲۴۹۵(است. یک چنین گواهینامه ای یک Public Key برای دارنده خود ایجاد می کند. این گواهینامه، داده هایی مربوط به الگوریتم به کار رفته برای امضاء ایجاد کننده، دارنده و مدت اعتبار در خود دارد که در این میان، Public Keyمربوط به دارنده از بقیه مهمتر است. CA هم گواهینامه را با یک عدد ساخته شده از روی داده ها که با Public Key خودش ترکیب شده امضاء می کند. برای بررسی اعتبار یک گواهینامه موجود، گیرنده باید این امضاء را با Public Key مربوط به CA رمز گشایی کرده و سپس با عدد نخست مقایسه کند . نقطه ضعف این روش در طول مدت اعتبار گواهینامه و امکان دستکاری و افزایش آن است. اما استفاده از این گواهینامه ها در ارتباطهای VPN مشکل چندانی به همراه ندارد چون مدیر شبکه Security Gateway و همه ارتباط ها را زیر نظر دارد. IPsec یا FreeS/WAN همانطور که گفتیم FreeS/WAN مجموعه کاملی برای راه اندازی IPsec روی لینکوس است . البته بیشتر نگارش های لینوکس برنامه های لازم برای این کار را با خود دارند. اما بر اساس تجربه بهتر است FreeS/WANرا به کار ببرید. در اینجا ما از RedHatLinux نگارش ۲/۷ با هسته ۲.۴.۱۸ و (ftp://ftp.xs۴all.nl/pub/cryypt/freesean /FreeS/WAN۱۹۷) استفاده کرده ایم. درصورت لزوم می توان FreeS/WAN را با هسته هسته های خانواده ۲.۲ هم به کار برد. البته در این حالت دست کم به نگارش ۲.۲.۱۹ لینوکس نیاز دارید. این را هم باید در نظر داشته باشید که راه انداختن VPN Gateway همراه با دیواره آتش سودمنداست و هسته نگارش ۲.۴ امکانات خوبی برای راه انداختن دیواره آتش دارد. نصب برای نصب باید هسته را در/usr/ser/linux و Free S/WAN را در /usr/scr/freeswan-versinnumber باز کنید. سپس با فرمان های make menucnfig و make xcnfig پیکربندی هسته را انجام بدهید. گزینه های لازم برای تنظیمات اضافی را در Netwrking ptins\IPsec ptins می یابید که معمولا نیازی به تغییر دادن تنظیمات پیش فرض آن نیست . برای راه انداختن patch X.۵۰۹ باید بسته مربوطه را باز کرده و فایل freewan.diff را در فهرست Free S/WAN کپی کنید. پس از آن، فرمان freewan.diff > patch-p۱ همه چیز را برایتان تنظیم می کند. در پایان باید هسته را که اکنون تغییر کرده کامپایل کنید. این مار را با صادر کردن فرمان make kinstall وقتی در فهرست Free S/WAN هستید انجام بدهید. پس از اضافه کردن هسته تازه به مدیر بوت و راه اندازی کامپیوتر می توانید نتیجه کارهایی که انجام دادید را ببینید. فرمان dmesg پیام های آغاز به کار KLIPS را نشان می دهد. لازم است که روی Runlevel ها هم کارهایی انجام بدهید. از آنجا که Free S/WAN بع رابط های eth۰ و ipsec۰، eth۱ را اضافه می کند، سیستم نخست Netwrking سپس Free S/WAN و در پایان iptables را اجرا می کند. پیکر بندی ما قصد داریم که Security Gateway خود را به گونه ای پیکربندی کنیم که یک Firewall هم باشد. این دیواره آتش باید به هر کامپیوتر از فضای اینترنت با هر IP دلخواه اجازه ارتباط با شبکه داخلی(۱۷۲.۱۶.۰.۰/۱۶) را بدهد . این کامپیوتر برای این کار دو رابط Ethernet(eth۰ برای شبکه داخلی (۱۷۲.۱۶.۰.۰/۱۶) و eth۱ برای محیط بیرونی) دارد . باید میان این دو رابط عملکرد IP-Frwarding فعال باشد. نخست باید دیواره آتش را در این Security Gateway طوری تنظیم کنیم که Packet های AH و ESP را بپذیرد. به همین دلیل روی رابط بیرونی(همان Packet (eth۱ های UDP را روی پورت ۵۰۰(ESP) می فرستیم. تنظیمات FreeS/WAN در فایل /etc/ipsec.cnf ثبت

می شود . این تنظیمات به سه گروه تقسیم می شوند. Cnfig setup به تنظیمات پایه ای مربوط می شود و cnn٪default تنظیمات مشترک برای همه ارتباط ها را در خود دارد. گروه سوم که با لغت کلیدی cnn و یک نام دلخواه مشخص می شود پارامترهای ارتباطی با همان نام را در خود دارد. در این مثال ما نام این بخش را Radwarrir گذاشته ایم که کاربرانی که از بیرون با کامپیوترهای همراه به شبکه متصل می شوند مربوط می شود. /etc/ipsec.cnf در بخش Cnfig setup پیش از هر چیز باید رابطی که درخواست ارتباط های IPsec روی آن می روند رامشخص کرد. برای این منظور، فرمان interfaces=٪defaultrute کافی است که البته می توانید بجای ٪defaultrute آدرس IP مربوط به کارت را هم وارد کنید. با تنظیم کردن kilpsdebug و plutdebug روی nne حالت Debug را غیر فعال می کنیم . Plutlad و plutstart را روی ٪search تنظیم می کنیم تا ارتباط ها پس از درخواست از سمت مقابل ، ایجاد شوند. دربخشی cnn defqult٪ فرمان ۰ = keyingtries به Gateway می گوید که در صورت تغییر کلیدهای رمز تا پیدایش آنها صبر کند. برای انتخاب این روش تعیین اعتبار فرمان authby = rsasig باعث می شود تا هر دو طرف گفتگو حتما میان خود گواهینامه مبادله کنند: ٪cert = rightsasigkey ٪cert = leftrsasigkey برای left هم دوباره ٪defaultrute را اعلام می کنیم که به عنوان left subnet شبکه داخلی(۱۷۲.۱۶.۰.۰/۱۶) به کار می رود. کمی بعد این بخش رابا leftid کامل می کنیم که گواهینامه ما را برای Gateway مشخص می کند. در بخش cnn Radwarrir هم با فرمان ٪any = right به همه کسانی که بتوانند گواهینامه ارائه کنندااجازه دسترسی می دهیم. حالت ارتباط را هم با tunnel = type مشخص می کنیم که در آن تبادل کلیدها از طریق ike = key exchang(IKE) با (pfc = yes Perfect Frwarding Secrecy) انجام می گیرد. add = Aut هم به Free S/WAN می گوید که ارتباط در پی در خواست از سوی کاربران بیرون از شبکه برقرار شود. گواهینامه اکنون Free S/WAN برای برقرار کردن ارتباط با یک رمز گذاری قوی از طریق تبادل گواهینامه پیکربندی شده. گواهینامه لازم برای Gateway و کاربران بیرون از شبکه را خودمان می سازیم. برای این کار از توانایی های SSL pen بهره می گیریم. نخست یک ساختار فهرست برای ایجاد گواهینامه می سازیم. برای نمونه فهرست /etc/fenrisCA را در نظر می گیریم. اینجا فهرست های certs و private key ها می سازیم. فهرست private به طور منطقی باید در دسترس rt باشد. در فهرست/etc/fenrisCA به دو فایل index.txt و serial نیاز داریم. با index.txt، tuch را خالی می کنیم. SSL pen بعدا در این فایل لیستی از گواهینامه های صادر شده ثبت می کند. اکنون در فایل PENSSL.CNF (که در /usr/ssl یا usr/share/ssl/ قرار دارد) مسیر فهرست CA را به عنوان پارامتر dir وارد می کنیم. RtCA اکنون به سراغ RtCA می رویم . برای این کار نخست یک RSAPrivate به طول ۲۰۴۸ بیت می سازیم: penssl gersa –des۳ –ut private/caKey.pem۲۰۴۸ گزینه des۳ باعث می شود که از طریق روش Triple DES ساخته شود تا افراد غیر مجاز نتوانند گواهینامه را درستکاری کنند. البته اکنون گواهینامه را درستکاری کنند. البته اگر خودمان هم Passphrase را فراموش کنیم امکان انجام این کار را نخواهیم داشت. اکنون گواهینامه RtCA خودمان را ایجاد کرده و آن را به یک بازه زمانی محدوده می کنیم: penssl req –new-x۵۰۹ –days = ۱۸۲۵ – key private/cakey.pem ut caCert.pem به عنوان passphrase از همان چیزی که برای Private Key کار بردیم استفاده کرده ایم. سپس penssl تک تک عناصر مربوط به شناسایی دارنده گواهینامه می پرسد. در پایان گواهینامه Rt CA را در /eht/ipsec.d/cacerts برای Free S/WAN کپی می کنیم. گواهینامه Gateway ساختن گواهینامه برای Gateway دقیقا همانند روشی است که برای گواهینامه Rt CA شرح دادیم. به کمک گواهینامه Gateway به کاربران بیرون از شبکه اجازه ارتباط و استفاده از آن ر امی دهیم . نخست به یک Private key نیاز داریم که این بار طول آن ۱۰۲۴ بیت است: penssl gersa –des۳ –ut

penssl req –new-key private/gwKey.pem – ۱۰۲۴ private/gwKey.pem اکنون گام بعدی را بر می داریم: ut geReq.pem penssl ca –ntext –in gwReq.pem –ut اکنون Request را به عنوان Rt CA امضاء می کنیم: gwCert.pem این گواهینامه را باید در قالب فایل /etc/x۵۰۹cert.der به شکل باینر روی Gateway ذخیره کنیم . عمل تبدیل با فرمان زیر انجام می گیرد: penssl x۵۰۹ –in gwcwert.pem –utfrm der –ut /etc/x۵۰۹cert.der Private key با نام gwkey.pem را برای Free S/WAN در /etc/ipsec.d/private/ کپی می کنیم. از این گذشته باید Passphrase مربوطه به طور واضح در فایل /etc/ipsec.secrets آمده باشد. اگر Passphrase به طور نمونه « asample Passphrase » باشد آن را در سطر زیر می نویسیم : « RAS gwkey.pem: asample Passphrase » روشن است که تنها rt باید به ipsec.secrets دسترسی داشته باشد. اکنون آخرین جای خالی را در /etc/ipsec.cnf پر می کنیم. Leftid = "C = IR,ST = Tehran, L = Tehran, = Rayaneh Magazine, U = Editrial,CN = fashkain, Email = fashkain@rayanehmag.net"گواهینامه های کاربران اکنون باید عمل تعیین اعتبار را برای هر کاربر یکبار انجام بدهیم. در فرمان زیر که برای ساختن Private key برای یک کاربر به کار می رود: penssl genrsa – ۱۰۲۴ –ut private/userkey.pem –ut des۳ باید برای هر کاربر Passphrase جداگانه ای وارد کنید. در گام بعدی فرمان زیر را به کار ببرید: penssl req –new-key private/gwKey.pem –ut geReq.pem اکنون باید گواهینامه ای را که آن را در قالب Rt CA امضاءخواهید کرد بسازید.-Enddate در اینجا برای مشخص کردن مدت اعتبار به کار می رود: penssl ca –ntext –eddate ۰۲۰۹۳۱۲۰۰z in gwReq.pem –ut gwCert.pem در آخرین مرحله روی این گواهینامه یک فایل باینری با فرمت PKCS۱۲ می سازیم کهدر ادامه برای سرویس گیرنده های ویندوز ۲۰۰۰/ xp لازم داریم. penssl pkcs۱۲ –exprt –inusercert.pem –inkey private/userkey.pem –certfile caCert.pem- ut user.p۱۲ چشم انداز پیکربندی Security Gateway را با موفقیت پشت سر گذاشتیم. در بخش بعدی به سرویس گیرنده های VPN در ویندوز می پردازیم. برای این کار از ابزارهای موجود در ویندوز ۲۰۰۰ و xp بهره خواهیم برد.

بخش چهارم

VPN با لینوکس (۲) در بخش پیش بر پایه لینوکس ۲.۴ و Free S/WAN یک VPN Security Gateway راه انداختیم. با نصب patch های Gateway (www.strngsec.cm/freewan/) x.۵۰۹ را با تنامین اعتبار های مطمئن و رمز گذاری های قوی کامل کردیم. به این ترتیب پیکر بندی سرویس دهنده به پایان می رسد. اکنون باید سرویس گیرنده ها را برای دسترسی به VPN تنظیم کنیم. فرض می کنیم که سیستم عامل مورد استفاده کاربران بیرون از شبکه ویندوز ۲۰۰۰ و xp است که هر دوی آنها برنامه های لازم برای ایجاد و مدیریت ارتباط های IPsec را در خود دارند. البته باید این احتمال را نیز در نظر گرفت که شاید برخی کاربران با سیستم ویندوز ۹x/Me قصد استفاده از VPN را داشته باشند. در این حالت به یک برنامه سرویس گیرنده IPsec نیاز داریم. یکبار معروفترین این برنامه ها که برای کاربردهای شخصی رایگان است PGPnet می باشد. این برنامه را می توان حتی روی ویندوز های NT و ۲۰۰۰ هم بکار برد. ویندوز ۲۰۰۰ و XP ویندوز های ۲۰۰۰و XP با توجه به پشتیبانی از IPsec برای استفاده به عنوان سرویس گیرنده IPsec بسیار مناسبند. این دو سیستم عامل افزون بر سرویس های IPsec امکاناتی هم برای ایمنی IP دارند. برای ساختن یک تونل VPN، کافی است که به کاربر تنها سرویس IPsec را اجرا کرده و گزینه های لازم را در آن تنظیم کند. البته فرض بر این است که تنظیمات امنیتی از پیش انجام شده باشد. انجام این کار در ویندوز چندان ساده نیست. در ویندوز ۲۰۰۰ باید برنامه IPsecPL

http://agent.micrsft.cm/windws۲۰۰۰/techinf/reskit/tls/existing/ipsecpl-.asp را از ResurceKit نصب کنید. در ویندوز XP بجای آن به IPsecCmd نیاز داریم. برای دستیابی به این برنامه باید Supprt Tls را در ویندوز XP به طور کامل نصب کنید(فهرست\ SUPPRT\TLS روی CD ویندوز XP). تنظیم ipsec.cnf اکنون ipsec.cnf را که قبلاً آماده کرده بودیم مطابق کاربردمان تنظیم کنیم. در default٪ cnn ارتباط های تلفنی(Dail up) که باید به طور خودکار فعال شوند مشخص می شوند. سپس بخشی قرار می گیرد که با cnn آغاز می شود و پارامترهای ارتباط VPN را در خود دارد. آدرس های محلی که به طور خودکار برای آدرس های سرویس گیرنده ها به کار می روند با با any٪ = left مشخص می شوند. در right آدرس IP مربوط به VPNGateway را واردکنیم. پارامترrightsubnet هم آدرس IP و ماسک شبکه ای که ارتباط با آن برقرار می شود را در خود دارد. در اینجا می توانید از هر دو شیوه نوشتن آدرس ها یعنی ۱۷۲.۱۶.۰.۰/۱۶ یا ۱۷۲.۱۶.۰.۰/۲۵۵.۲۵۵.۰.۰ استفاده کنید. Netwrk مشخص می کند که ارتباط از طریق تماس تلفنی (netwrk = ras)، شبکه (netwrk = lan) یا هر دو (netwrk = bth) برقرار شود. پیکر بندی سرویس گیرنده اکنون باید فایل آرشیوی که برای گواهینامه کاربر، رمز عبور،IPsec و ipsec.cnf ساختیم را از یک راه مطمئن (مثلا Email رمز گذاری شده) به کامپیوتر سرویس گیرنده بفرستیم. پس از باز کردن این فایل، باید یکSnap in را همان طور که در شکل می بینید اضافه کنید . برای این منظور در" mmc "، "Start,Run را وارد کنید. سپس از طریق" File,Add/Remve Snap-in "یک Plug in از از جنس Certificate بسازید. این Plug in باید از جنس Cmpeuter accunt برای Lcal cmputer باشد. پس از اتمام کار و زدن کلیدهای Clse ، Finish و Plug in، k را در پنجره MMC خواهید دید. خلاصه لینوکس و Free S/WAN برای ساختن VPN راه حل هایی هستند که در مقایسه با راه حل های سخت افزاری بسیار ساده تر و کم هزینه تر است. به ویژه سرویس گیرنده های ویندوز ۲۰۰۰ و XP با توجه به دسترس بودن برنامه های لازم بسیار ساده و سریع پیکربندی می شوند. اما هنگام راه اندازی VPN نباید یک نکته فراموش کرد. VPN اگر چه مطمئن است اما این اطمینان تا وقتی است که کامپیوترها در هماهنگی کامل با یکدیگر باشند. اگر از VPN به درستی محافظت نشود بستر بسیار مناسبی برای ویروس ها، کرم ها، اسب های تروآیی و کاربران غیر مجاز خواهد بود. بنابراین استفاده از برنامه های ضد ویروس و دیواره آتش را نباید فراموش کنید.

مفاهیم پروتکل TCP IP در شبکه

پروتکل TCP/IP TCP/IP ، یکی از مهمترین پروتکل های استفاده شده در شبکه های کامپیوتری است . اینترنت بعنوان بزرگترین شبکه موجود ، از پروتکل فوق بمنظور ارتباط دستگاه های متفاوت استفاده می نماید. پروتکل ، مجموعه قوانین لازم بمنظور قانونمند نمودن نحوه ارتباطات در شبکه های کامپیوتری است .در مجموعه مقالاتی که ارائه خواهد شد به بررسی این پروتکل خواهیم پرداخت . در این بخش مواردی همچون : فرآیند انتقال اطلاعات ، معرفی و تشریح لایه های پروتکل TCP/IP و نحوه استفاده از سوکت برای ایجاد تمایز در ارتباطات ، تشریح می گردد. مقدمه امروزه اکثر شبکه های کامپیوتری بزرگ و اغلب سیستم های عامل موجود از پروتکل TCP/IP ، استفاده و حمایت می نمایند. TCP/IP ، امکانات لازم بمنظور ارتباط سیستم های غیرمشابه را فراهم می آورد. از ویژگی های مهم پروتکل فوق ، می توان به مواردی همچون : قابلیت اجراء بر روی محیط های متفاوت ، ضریب اطمینان بالا ،قابلیت گسترش و توسعه آن ، اشاره کرد . از پروتکل فوق، بمنظور دستیابی به اینترنت و استفاده از سرویس های متنوع آن نظیر وب و یا پست الکترونیکی استفاده می گردد. تنوع پروتکل های موجود در پشته TCP/IP و ارتباط منطقی و سیستماتیک آنها با یکدیگر، امکان تحقق ارتباط در شبکه های کامپیوتری را با اهداف متفاوت ، فراهم می نماید. فرآیند برقراری یک ارتباط ، شامل فعالیت های متعددی نظیر : تبدیل نام کامپیوتر به آدرس IP معادل ، مشخص نمودن موقعیت کامپیوتر

مقصد ، بسته بندی اطلاعات ، آدرس دهی و روتینگ داده ها بمنظور ارسال موفقیت آمیز به مقصد مورد نظر ، بوده که توسط مجموعه پروتکل های موجود در پشته TCP/IP انجام می گیرد. معرفی پروتکل TCP/IP TCP/IP ، پروتکلی استاندارد برای ارتباط کامپیوترهای موجود در یک شبکه مبتنی بر ویندوز ۲۰۰۰ است. از پروتکل فوق، بمنظور ارتباط در شبکه های بزرگ استفاده می گردد. برقراری ارتباط از طریق پروتکل های متعددی که در چهارلایه مجزا سازماندهی شده اند ، میسر می گردد. هر یک از پروتکل های موجود در پشته TCP/IP ، دارای وظیفه ای خاص در این زمینه (برقراری ارتباط) می باشند . در زمان ایجاد یک ارتباط ، ممکن است در یک لحظه تعداد زیادی از برنامه ها ، با یکدیگر ارتباط برقرار نمایند. TCP/IP ، دارای قابلیت تفکیک و تمایز یک برنامه موجود بر روی یک کامپیوتر با سایر برنامه ها بوده و پس از دریافت داده ها از یک برنامه ، آنها را برای برنامه متناظر موجود بر روی کامپیوتر دیگر ارسال می نماید. نحوه ارسال داده توسط پروتکل TCP/IP از محلی به محل دیگر ، با فرآیند ارسال یک نامه از شهری به شهر، قابل مقایسه است . برقراری ارتباط مبتنی بر TCP/IP ، با فعال شدن یک برنامه بر روی کامپیوتر مبدا آغاز می گردد . برنامه فوق ،داده های مورد نظر جهت ارسال را بگونه ای آماده و فرمت می نماید که برای کامپیوتر مقصد قابل خواندن و استفاده باشند. (مشابه نوشتن نامه با زبانی که دریافت کننده ، قادر به مطالعه آن باشد) . در ادامه آدرس کامپیوتر مقصد ، به داده های مربوطه اضافه می گردد (مشابه آدرس گیرنده که بر روی یک نامه مشخص می گردد) . پس از انجام عملیات فوق ، داده بهمراه اطلاعات اضافی (درخواستی برای تائید دریافت در مقصد) ، در طول شبکه بحرکت درآمده تا به مقصد مورد نظر برسد. عملیات فوق ، ارتباطی به محیط انتقال شبکه بمنظور انتقال اطلاعات نداشته ، و تحقق عملیات فوق با رویکردی مستقل نسبت به محیط انتقال ، انجام خواهد شد . لایه های پروتکل TCP/IP TCP/IP ، فرآیندهای لازم بمنظور برقراری ارتباط را سازماندهی و در این راستا از پروتکل های متعددی در پشته TCP/IP استفاده می گردد. بمنظور افزایش کارآئی در تحقق فرآیند های مورد نظر، پروتکل ها در لایه های متفاوتی، سازماندهی شده اند . اطلاعات مربوط به آدرس دهی در انتها قرار گرفته و بدین ترتیب کامپیوترهای موجود در شبکه قادر به بررسی آن با سرعت مطلوب خواهند بود. در این راستا، صرفا" کامپیوتری که بعنوان کامپیوتر مقصد معرفی شده است ، امکان باز نمودن بسته اطلاعاتی و انجام پردازش های لازم بر روی آن را دارا خواهد بود. TCP/IP ، از یک مدل ارتباطی چهار لایه بمنظور ارسال اطلاعات از محلی به محل دیگر استفاده می نماید: Internet, Transprt, Applicatin و Netwrk Interface ، لایه های موجود در پروتکل TCP/IP می باشند.هر یک از پروتکل های وابسته به پشته TCP/IP ، با توجه به رسالت خود ، در یکی از لایه های فوق، قرار می گیرند. لایه Applicatin لایه Applicatin ، بالاترین لایه در پشته TCP/IP است .تمامی برنامه و ابزارهای کاربردی در این لایه ، با استفاده از لایه فوق، قادر به دستیابی به شبکه خواهند بود. پروتکل های موجود در این لایه بمنظور فرمت دهی و مبادله اطلاعات کاربران استفاده می گردند . HTTP و FTP دو نمونه از پروتکل ها ی موجود در این لایه می باشند. پروتکل HTTP(Hypertext Transfer Prtcl) . از پروتکل فوق ، بمنظور ارسال فایل های صفحات وب مربوط به وب ، استفاده می گردد . پروتکل FTP(File Transfer Prtcl) . از پروتکل فوق برای ارسال و دریافت فایل، استفاده می گردد . لایه Transprt لایه " حمل ، " قابلیت ایجاد نظم و ترتیب و تضمین ارتباط بین کامپیوترها و ارسال داده به لایه Applicatin (لایه بالای خود) و یا لایه اینترنت (لایه پایین خود) را بر عهده دارد. لایه فوق ، همچنین مشخصه منحصربفردی از برنامه ای که داده را عرضه نموده است ، مشخص می نماید. این لایه دارای دو پروتکل اساسی است که نحوه توزیع داده را کنترل می نمایند. TCP(Transmissin Cntrl Prtcl). پروتکل فوق ، مسئول تضمین صحت توزیع اطلاعات است . UDP(User Datagram Prtcl). پروتکل فوق ، امکان عرضه سریع اطلاعات بدون پذیرفتن مسئولیتی در رابطه با تضمین صحت توزیع اطلاعات را برعهده دارد . لایه اینترنت لایه" اینترنت،" مسئول آدرس دهی ، بسته بندی و روتینگ داده ها ، است. لایه فوق ، شامل چهار پروتکل اساسی است : IP(Internet Prtcl) .

پروتکل فوق ، مسئول آدرسی داده ها بمنظور ارسال به مقصد مورد نظر است . Address Resulatin Prtcl(ARP). پروتکل فوق ، مسئول مشخص نمودن آدرس Media Access Cntrl(MAC) آداپتور شبکه بر روی کامپیوتر مقصد است. Internet Cntrl Message Prtcl(ICMP) . پروتکل فوق ، مسئول ارائه توابع عیب یابی و گزارش خطاء در صورت عدم توزیع صحیح اطلاعات است . Internet Grup Managemant Prtcl(IGMP). پروتکل فوق ، مسئول مدیریت Multicasting در TCP/IP را برعهده دارد. لایه Netwrk Interface لایه " اینترفیس شبکه ، " مسئول استقرار داده بر روی محیط انتقال شبکه و دریافت داده از محیط انتقال شبکه است . لایه فوق ، شامل دستگاه های فیزیکی نظیر کابل شبکه و آداپتورهای شبکه است . کارت شبکه (آداپتور) دارای یک عدد دوازده رقمی مبنای شانزده (نظیر : B۵-۵۰-۰۴-۲۲-D۴-۶۶) بوده که آدرس MAC ، نامیده می شود. لایه " اینترفیس شبکه ، " شامل پروتکل های مبتنی بر نرم افزار مشابه لایه های قبل ، نمی باشد. پروتکل های Ethernet و Asynchrnus Transfer Mde(ATM) ، نمونه هائی از پروتکل های موجود در این لایه می باشند . پروتکل های فوق ، نحوه ارسال داده در شبکه را مشخص می نمایند. مشخص نمودن برنامه ها در شبکه های کامپیوتری ، برنامه ها ی متعددی در یک زمان با یکدیگر مرتبط می گردند. زمانیکه چندین برنامه بر روی یک کامپیوتر فعال می گردند ، TCP/IP ، می بایست از روشی بمنظور تمایز یک برنامه از برنامه دیگر، استفاده نماید. بدین منظور ، از یک سوکت (Scket) بمنظور مشخص نمودن یک برنامه خاص ، استفاده می گردد. آدرس IP برقراری ارتباط در یک شبکه ، مستلزم مشخص شدن آدرس کامپیوترهای مبداء و مقصد است (شرط اولیه بمنظور برقراری ارتباط بین دو نقطه ، مشخص بودن آدرس نقاط درگیر در ارتباط است) . آدرس هر یک از دستگاه های درگیر در فرآیند ارتباط ، توسط یک عدد منحصربفرد که IP نامیده می شود ، مشخص می گردند. آدرس فوق به هریک از کامپیوترهای موجود در شبکه نسبت داده می شود . ۱۰.۱.۱.۱۰ : IP ، نمونه ای در این زمینه است . پورت TCP/UDP پورت مشخصه ای برای یک برنامه و در یک کامپیوتر خاص است .پورت با یکی از پروتکل های لایه" حمل ("TCP و یا UDP) مرتبط و پورت TCP و یا پورت UDP ، نامیده می شود. پورت می تواند عددی بین صفر تا ۶۵۵۳۵ را شامل شود. پورت ها برای برنامه های TCP/IP سمت سرویس دهنده ، بعنوان پورت های" شناخته شده " نامیده شده و به اعداد کمتر از ۱۰۲۴ ختم و رزو می شوند تا هیچگونه تعارض و برخوردی با سایر برنامه ها بوجود نیاید. مثلا "برنامه سرویس دهنده FTP از پورت TCP بیست و یا بیست ویک استفاده می نماید. سوکت (Scket) سوکت ، ترکیبی از یک آدرس IP و پورت TCP ویا پورت UDP است . یک برنامه ، سوکتی را با مشخص نمودن آدرس IP مربوط به کامپیوتر و نوع سرویس (TCP برای تضمین توزیع اطلاعات و یا UDP) و پورتی که نشاندهنده برنامه است، مشخص می نماید. آدرس IP موجود در سوکت ، امکان آدرس دهی کامپیوتر مقصد را فراهم و پورت مربوطه ، برنامه ای را که داده ها برای آن ارسال می گردد را مشخص می نماید. در بخش دوم این مقاله به تشریح هر یک از پروتکل های موجود در پشته TCP/IP، خواهیم پرداخت . TCP/IP ،شامل شش پروتکل اساسی (TCP, UDP, IP, ICMP, IGMP ،ARP) و مجموعه ای از برنامه های کاربردی است. پروتکل های فوق، مجموعه ای از استانداردها ی لازم بمنظور ارتباط بین کامپیوترها و دستگاهها را در شبکه ، فراهم می نماید. تمامی برنامه ها و سایر پروتکل ها ی موجود در پروتکل TCP/IP ، به پروتکل های شش گانه فوق مرتبط و از خدمات ارائه شده توسط آنان استفاده می نمایند . در ادامه به تشریح عملکرد و جایگاه هر یک از پروتکل های اشاره شده ، خواهیم پرداخت . پروتکل TCP : لایه Transmissin Cntrl Prtcl (Transprt TCP) ، یکی از پروتکل های استاندارد TCP/IP است که امکان توزیع و عرضه اطلاعات (سرویس ها) بین صرفا "دو کامپیوتر ، با ضریب اعتماد بالا را فراهم می نماید. چنین ارتباطی (صرفا "بین دو نقطه) ، Unicast نامیده می شود . در ارتباطات با رویکرد اتصال گرا ، می بایست قبل از ارسال داده ، ارتباط بین دو کامپیوتر برقرار گردد . پس از برقراری ارتباط ، امکان ارسال اطلاعات برای صرفا "اتصال ایجاد شده ، فراهم می گردد .

ارتباطات از این نوع ، بسیار مطمئن می باشند ، علت این امر به تضمین توزیع اطلاعات برای مقصد مورد نظر برمی گردد . بر روی کامپیوتر مبداء ، TCP داده هائی که می بایست ارسال گردند را در بسته های اطلاعاتی (Packet) سازماندهی می نماید. در کامپیوتر مقصد ، TCP ، بسته های اطلاعاتی را تشخیص و داده های اولیه را مجددا "ایجاد خواهد کرد . ارسال اطلاعات با استفاده از TCP TCP ، بمنظور افزایش کارائی ، بسته های اطلاعاتی را بصورت گروهی ارسال می نماید . TCP ، یک عدد سریال (موقعیت یک بسته اطلاعاتی نسبت به تمام بسته اطلاعاتی ارسالی) را به هریک از بسته ها نسبت داده و از Acknwledgment بمنظور اطمینان از دریافت گروهی از بسته های اطلاعاتی ارسال شده ، استفاده می نماید. در صورتیکه کامپیوتر مقصد ، در مدت زمان مشخصی نسبت به اعلام وصول بسته های اطلاعاتی ، اقدام ننماید ، کامپیوتر مبداء ، مجددا "اقدام به ارسال اطلاعات می نماید. علاوه برافزودن یک دنباله عددی و Acknwledgment به یک بسته اطلاعاتی ، TCP اطلاعات مربوط به پورت مرتبط با برنامه ها ی مبداء و مقصد را نیز به بسته اطلاعاتی اضافه می نماید. کامپیوتر مبداء ، از پورت کامپیوتر مقصد بمنظور هدایت صحیح بسته های اطلاعاتی به برنامه مناسب بر روی کامپیوتر مقصد ، استفاده می نماید. کامپیوتر مقصد از پورت کامپیوتر مبداء بمنظور برگرداندن اطلاعات به برنامه ارسال کننده در کامپیوتر مبداء ، استفاده خواهد کرد . هر یک از کامپیوترهائی که تمایل به استفاده از پروتکل TCP بمنظور ارسال اطلاعات دارند ، می بایست قبل از مبادله اطلاعات ، یک اتصال بین خود ایجاد نمایند . اتصال فوق ، از نوع مجازی بوده و Sessin نامیده می شود .دو کامپیوتر درگیر در ارتباط ، با استفاده از TCP و بکمک فرآیندی با نام : Three-Way handshake ، با یکدیگر مرتبط و هر یک پایبند به رعایت اصول مشخص شده در الگوریتم مربوطه خواهند بود . فرآیند فوق ، در سه مرحله صورت می پذیرد : مرحله اول : کامپیوتر مبداء ، اتصال مربوطه را از طریق ارسال اطلاعات مربوط به Sessin ، مقداردهی اولیه می نماید (عدد مربوط به موقعیت یک بسته اطلاعاتی بین تمام بسته های اطلاعاتی و اندازه مربوط به بسته اطلاعاتی) مرحله دوم : کامپیوتر مقصد ، به اطلاعات Sessin ارسال شده ، پاسخ مناسب را خواهد داد . کامپیوتر مبداء ، از شرح واقعه بکمک Acknwledgment ارسال شده توسط کامپیوتر مقصد ، آگاهی پیدا خواهد کرد . پروتکل UDP : لایه User Datagram Prtcl (Transprt UDP) ، پروتکلی در سطح لایه" حمل "بوده که برنامه مقصد در شبکه را مشخص نموده و از نوع بدون اتصال است . پروتکل فوق، امکان توزیع اطلاعات با سرعت مناسب را ارائه ولی در رابطه با تضمین صحت ارسال اطلاعات ، سطح مطلوبی از اطمینان را بوجود نمی آورد . UDP در رابطه با داده های دریافتی توسط مقصد ، به Acknwledgment نیازی نداشته و در صورت بروز اشکال و یا خرابی در داده های ارسال شده ، تلاش مضاعفی بمنظور ارسال مجدد داده ها ، انجام نخواهد شد . این بدان معنی است که داده هائی کمتر ارسال می گردد ولی هیچیک از داده های دریافتی و صحت تسلسل بسته های اطلاعاتی ، تضمین نمی گردد .از پروتکل فوق ، بمنظور انتقال اطلاعات به چندین کامپیوتر با استفاده از Bradcast و یا Multicast ، استفاده بعمل می آید . پروتکل UDP ، در مواردیکه حجم اندکی از اطلاعات ارسال و یا اطلاعات دارای اهمیت بالائی نمی بانشد ، نیز استفاده می گردد. استفاده از پروتکل UDP در مواردی همچون Multicasting Streaming media ، (نظیر یک ویدئو کنفرانس زنده) و یا انتشار لیستی از اسامی کامپیوترها که بمنظور ارتباطات محلی استفاده می گردند ، متداول است . بمنظور استفاده از UDP ، برنامه مبداء می بایست پورت UDP خود را مشخص نماید دقیقا" مشابه عملیاتی که می بایست کامپیوتر مقصد انجام دهد . لازم به یادآوری است که پورت های UDP از پورت های TCP مجزا و متمایز می باشند (حتی اگر دارای شماره پورت یکسان باشند). پروتکل IP : لایه Internet Prtcl (Internet IP) ، امکان مشخص نمودن محل کامپیوتر مقصد در یک شبکه ارتباطی را فراهم می نماید. IP ، یک پروتکل بدون اتصال و غیرمطمئن بوده که اولین مسئولیت آن آدرس دهی بسته های اطلاعاتی و روتینگ بین کامپیوترهای موجود در شبکه است . با اینکه IP همواره سعی در توزیع یک بسته اطلاعاتی می نماید ، ممکن است یک بسته اطلاعاتی در زمان ارسال گرفتار مسائل متعددی نظیر : گم

شدن ، خرابی ، عدم توزیع با اولویت مناسب ، تکرار در ارسال و یا تاخیر، گردند.در چنین مواردی ، پروتکل IP تلاشی بمنظور حل مشکلات فوق را انجام نخواهد داد (ارسال مجدد اطلاعات درخواستی) .آگاهی از وصول بسته اطلاعاتی در مقصد و بازیافت بسته های اطلاعاتی گم شده ، مسئولیتی است که بر عهده یک لایه بالاتر نظیر TCP و یا برنامه ارسال کننده اطلاعات ، واگذار می گردد . عملیات انجام شده توسط IP می توان IP را بعنوان مکانی در نظر گرفت که عملیات مرتب سازی و توزیع بسته های اطلاعاتی در آن محل ، صورت می پذیرد .بسته ها ی اطلاعاتی توسط یکی از پروتکل های لایه حمل (TCP و یا UDP) و یا از طریق لایه " اینترفیس شبکه ، " برای IP ارسال می گردند . اولین وظیفه IP ، روتینگ بسته های اطلاعاتی بمنظور ارسال به مقصد نهائی است . هر بسته اطلاعاتی ، شامل آدرس IP مبداء (فرستنده) و آدرس IP مقصد (گیرنده) می باشد. در صورتیکه IP ، آدرس مقصدی را مشخص نماید که در همان سگمنت موجود باشد ، بسته اطلاعاتی مستقیما "برای کامپیوتر مورد نظر ارسال می گردد . در صورتیکه آدرس مقصد در همان سگمنت نباشد ، IP ، می بایست از یک روتر استفاده و اطلاعات را برای آن ارسال نماید.یکی دیگر از وظایف IP ، ایجاد اطمینان از عدم وجود یک بسته اطلاعاتی (بلاتکلیف !) در شبکه است . بدین منظور محدودیت زمانی خاصی در رابطه با مدت زمان حرکت بسته اطلاعاتی در طول شبکه ، در نظر گرفته می شود .عملیات فوق، توسط نسبت دادن یک مقدار Time T Live(TTL) به هر یک از بسته های اطلاعاتی صورت می پذیرد. TTL ، حداکثر مدت زمانی را که بسته اطلاعاتی قادر به حرکت در طول شبکه است را مشخص می نماید(قبل از اینکه بسته اطلاعاتی کنار گذاشته شود) . پروتکل ICMP : لایه Internet Cntrl Message Prtcl (Internet ICMP) ، امکانات لازم در خصوص اشکال زدائی و گزارش خطاء در رابطه با بسته های اطلاعاتی غیرقابل توزیع را فراهم می نماید. با استفاده از ICMP ، کامپیوترها و روترها که از IP بمنظور ارتباطات استفاده می نمایند ، قادر به گزارش خطاء و مبادله اطلاعاتی محدود در رابطه وضعیت بوجود آمده می باشند. مثلا "در صورتیکه IP ، قادر به توزیع یک بسته اطلاعاتی به مقصد مورد نظر نباشد ، ICMP یک پیام مبتنی بر غیرقابل دسترس بودن را برای کامپیوتر مبداء ارسال می دارد . با اینکه پروتکل IP بمنظور انتقال داده بین روترهای متعدد استفاده می گردد ، ولی ICMP به نمایندگی از TCP/IP ، مسئول ارائه گزارش خطاء و یا پیام های کنترلی است . تلاش ICMP ، در این جهت نیست که پروتکل IP را بعنوان یک پروتکل مطمئن مطرح نماید ، چون پیام های ICMP دارای هیچگونه محتویاتی مبنی بر اعلام وصول پیام (Acknwledgment) بسته اطلاعاتی نمی باشند . ICMP ، صرفا "سعی در گزارش خطاء و ارائه فیدبک های لازم در رابطه با تحقق یک وضعیت خاص را می نماید . پروتکل IGMP : لایه Internet Grup Internet IGMP) Managment Prtcl) ، پروتکلی است که مدیریت لیست اعضاء برای IP Multicasting ، در یک شبکه TCP/IP را بر عهده دارد . IP Multicasting، فرآیندی است که بر اساس آن یک پیام برای گروهی انتخاب شده از گیرندگان که گروه multicat نامیده می شوند ؛ ارسال می گردد . IGMP لیست اعضاء را نگهداری می نماید . پروتکل ARP : لایه Internet Address Reslutin Prtcl (ARP) ، پروتکلی است که مسئولیت مسئله " نام به آدرس "را در رابطه با بسته های اطلاعاتی خروجی (utging) ، برعهده دارد . ماحصل فرآیند فوق ، Mapping آدرس IP به آدرسMedia Access Cntrl(MAC) ، مربوطه است . کارت شبکه از آدرس MAC ، بمنظور تشخیص تعلق یک بسته اطلاعاتی به کامپیوتر مربوطه ، استفاده می نمایند . بدون آدرس های MAC ، کارت های شبکه ، دانش لازم در خصوص ارسال بسته های اطلاعاتی به لایه بالاتر بمنظور پردازش های مربوطه را دارا نخواهند بود . همزمان با رسیدن بسته های اطلاعاتی به لایه IP بمنظور ارسال در شبکه ، آدرس های MAC مبداء و مقصد به آن اضافه می گردد . ARP ، از جدولی خاص بمنظور ذخیره سازی آدرس های IP و MAC مربوطه ، استفاده می نماید. محلی از حافظه که جدول فوق در آنجا ذخیره می گردد ، ARP Cache نامیده می شود. ARP Cache هر کامپیوتر شامل mapping لازم برای کامپیوترها و روترهائی است که صرفا "بر روی یک سگمنت مشابه قرار دارند.

آشنایی با ملزومات شبکه

آشنایی با ملزومات شبکه حتما همه شما تا به حال تجربه ی اتصال به اینترنت را داشته اید و کم و بیش اطلاعاتی راجع به این موضوع دارید. برای آشنایی بیشتر شما نکاتی هر چند مختصر در مورد شبکه و قطعات مورد نیاز در آن خواهیم گفت. همان طور که می دانید اینترنت، متشکل از شبکه هایی است که هر یک ازطریق مسیرهایی به دیگری متصل هستند. این مسیرها تبادل اطلاعات را میسر می سازند. اتصال به اینترنت به معنی دستیابی به این مسیرها است. حال برای این که این شبکه ها که شامل هزاران کامپیوتر هستند بتوانند به درستی با هم در ارتباط باشند به وسایل و قطعات ویژه ای مثل هاب، تکرار کننده، مسیریاب و ... نیاز است. اما برای اینکه بدانید وظیفه هر یک از این وسیله ها چیست ادامه ی مطلب را بخوانید. کابل BUS: در شبکه های محلی اترنت اولیه برای ارتباط از کابل کواکسیال استفاده می شد. (این کابل ها همان کابل هایی هستند که برای اتصال آتن به تلویزیون استفاده می شوند و شما هم حتما دیده اید.) این کابل از یک کامپیوتر به کامپیوتر دیگر رفته و تمام دستگاه ها را به هم متصل می کند. بنابراین هر سیگنالی که در کابل Bus وجود دارد در تمام دستگاه ها قابل مشاهده است. این روش ساده ترین روش ایجاد شبکه ی کامپیوتری است. البته در ظاهر ساده به نظر می رسد اما در واقع پر از اشکال است. چون وقتی که تعداد سیستم ها زیاد می شود، کار کابل کشی بسیار پر زحمت است. تازه وقتی بخواهید دستگاهی را از مدار خارج کنید و یا یک دستگاه جدید به شبکه اضافه کنید مشکلات ظهور می کنند. البته امروزه به ندرت می توانید یک شبکه محلی LAN پیدا کنید که با کابل کواکسیال درست شده باشد. Hub: به طور خلاصه باید بگوییم هاب یک جعبه است که دارای تعدادی ورودی بنام پورت (Prt) می باشد. تعداد این ورودی ها بسته به تعداد کامپیوترهایی است که می خواهیم در یک شبکه باشند. مثلا-اگر در یک شرکت تمام کامپیوترها در شبکه باشند، در هر طبقه یک هاب قرار می دهند و تمام دستگاه های آن طبقه با کابل به هاب مورد نظر وصل می شوند که بعد هر کدام از این هاب ها به طریقی به کامپیوتر سرور متصل می شوند. اگر اطلاعاتی به داخل این جعبه آمد توسط کابل وارد تمام کامپیوترها می شود. شاید بگویید پس چه فرقی بین این روش و روش اولیه وجود دارد؟ در جواب باید گفت بزرگترین فرق در این است که شما می توانید هر زمان که بخواهید به راحتی یک کامپیوتر جدید را با اتصال به این جعبه به شبکه اضافه کنید و یا با خارج کردن کابل یک دستگاه از این جعبه آن را از شبکه خارج کنید بدون این که کل شبکه تحت تاثیر قراربگیرد. اکثر هاب ها یک چراغ نمایشگر دارند که نشان می دهد هر کابل به خوبی دستگاه را به شبکه متصل کرده است و یک چراغ دیگر وضعیتی را نشان می دهد که ۲ سیستم سعی می کنند در یک زمان اطلاعات را به اشتراک بگذارند و در نتیجه باعث تصادف داده ها (Data Cllisin) می شوند. به طور کلی هاب به دو دسته تقسیم می شود: ۱.Active: این نوع هاب، سیگنال هایی را که از درون آن می گذرند تقویت می کند. ۲.Passive: این هاب هیچ عمل تقویتی روی سیگنال انجام نمی دهد و صرفا آن را از خود عبور می دهد. در مسافرت های طولانی زیاد بودن طول کابل باعث ضعیف شدن سیگنال می شود و با تقویت آن، قدرت اولیه را به آن برمی گرداند. نوع دیگر از هاب ها وجود دارد که هوشمند نامیده می شود که به مسئول شبکه اجازه کنترل از راه دور اتصالات را می دهد. تکرار کننده(Repeater): این وسیله در واقع نوع خاصی Hub است که فقط دارای ۲ پورت است. کار آن تقویت سیگنال های بین دو شبکه یا سگمنت های یک شبکه که فاصله ی زیادی از هم دارند می باشد. مثل هاب های دارای ۲ نوع Passive و Active می باشد. نوع اول علاوه بر سیگنال هر چیز دیگری حتی نویز (Nise: امواج ناخواسته که به همراه سیگنال اصلی که دارای اطلاعات است می باشند. مثلا در امواج صوتی نویز باعث افت کیفیت صدا و شنیدن اصوات اضافه می شود) را هم تقویت می کند. اما تکرار کننده ی نوع اکتیو سیگنال را قبل از ارسال بازدید کرده و چیزهای اضافه را خارج می کند و مثلا-دیگر نویز را تقویت نمی کند. پل (Bridge): مثل تکرارکننده دارای ۲ پورت است و برای اتصال گروهی از

کامپیوترها به کار می رود. تفاوت آنها در این است که پل لیستی دارد که نشان می دهد در هر سمت چه کامپیوترهایی قرار دارند و به بسته هایی (در اینترنت و هر شبکه ای اطلاعات برای اینکه فرستاده شوند به قطعات کوچکتری تقسیم می شوند، هر قطعه را بسته می نامیم) که باید بطرف دیگر شبکه بروند اجازه ی عبور می دهد. سوئیچ (Switch): تقریبا مثل هاب است اما به جای ۲ پورت دارای چندین پورت است. درون خود یک جدولی دارد و نشان می دهد که جه سیستم هایی به هر پورت متصلند و بسته ها را به جایی که باید بروند می فرستد. برخلاف هاب سیگنال ها فقط به درون پورتی که باید بروند می روند نه به تمام پورت ها. جداول (و شبکه) باید به قدر کافی ساده باشند چرا که فقط یک مسیر ممکن برای هر بسته وجود دارد. اگر دقت کرده باشید متوجه خواهید شد که سوئیچ از هاب سریعتر است چون احتیاجی نیست که هر پورت کل ترافیک ارسال و دریافت اطلاعات را متحمل شود و فقط آنچه که مخصوص خود است را دریافت می کند. البته سوئیچ از پل هم سریعتر است و در ضمن گران تر از هر دوی آنها. بعضی از سوئیچ ها و پل ها می توانند برای اتصال شبکه هایی که پروتکل های فیزیکی مختلفی دارند استفاده شوند. مثلا برای اتصال شبکه های اترنت یا شبکه TkenRing. هر دوی این شبکه ها می توانند به اینترنت متصل شوند. در شبکه TkenRing اطلاعات بع صورت نشانه (Tken) هایی از یک کامپیوتر به کامپیوتر دیگر به صورت ستاره یا حلقه منتقل می شوند. شبکه اترنت را هم قبلا توضیح داده ایم. این قطعات به صورت ویژه هستند و در همه شبکه ها استفاده نمی شوند. مسیریاب (Ruter): مسیریاب از ۲ یا چند پورت برای ورود و خروج اطلاعات تشکیل شده است در واقع کنترل ترافیک به عهده آنها می باشد. مسیریاب را می توان مرتب کننده ی هوشمند بسته ها نامید. همان طور که از نامش پیدا است، بهترین مسیر را برای فرستادن قطعات به مقصد انتخاب می کند و چک می کند تا ببیند آیا بسته ها به مقصد رسیده اند یا نه. براساس مقصد داده ها، بسته ها از یک مسیریاب به مسیریاب دیگر از طریق بهترین راه فرستاده می شوند. این موضوع یاعث می شود تا به عنوان یک وسیله قدرتمند در شبکه های پیچیده مثل اینترنت استفاده شود. در واقع می توان اینترنت را به عنوان شبکه ای از مسیریاب ها توصیف کرد. انواع مسیریاب ها با جداول و پروتکل های مختلفی کار می کنند اما حداقل این که هر مسیریاب در اینترنت باید با پروتکل TCP/IP کار کند. Bruter: این وسیله ترکیبی از پل و مسیریاب می باشد/(Bridgt+Ruter). بسته های محلی می توانند از یک طرف شبکه به طرف دیگر با توجه به آدرس مقصد هدایت شوند حتی اگر از هیچ پروتکل ارسالی هم پیروی نکنند. بسته هایی که دارای پروتکل مناسب هستند می تواند طبق مسیر خود به دنیای خارج از شبکه محلی فرستاده شوند. دروازه (Gateway): دلیل اصلی پیچیدگی موضوع در وازه ها از این حقیقت ناشی می شود که این کلمه ۲ عملکرد مختلف را توصیف می کند. یک نوع آن، یک شبکه را به یک شبکه یا دستگاه های مختلف دیگر ارتباط می دهد. مثلا یک شبکه از کامپیوترهایی که به یک سیستم ابرکامپیوتر IBM متصل هستند. کاربرد معمولی آن در گره (Nde) یک شبکه می باشد که امکان دستیابی به اینترنت و یا کامپیوترهای دیگر دریک شبکه پیچیده LAN را می دهد. در شبکه هایی که بیش از یک دروازه وجود دارد معمولا- یکی از آنها به عنوان دروازه ی پیش فرض انتخاب می شود. قبلا- یک دروازه تقریبا شبیه به چیزی بود که ما امروزه مسیریاب می نامیم. سرور پراکسی (Prxy Server): این سیستم بین یک سرور و یک کامپیوتر Wrk Statin (یعنی کامپیوتری که به کامپیوتر اصلی یا همان سرور متصل است) برقرار است. ملموس ترین مثال در مورداینترنت، مرورگری که شما با آن کار می کنید است. این مرورگر ظاهرا در حال برقراری ارتباط با یک سرور خارج از وب است اما درواقع به یک سرورپراکسی محلی متصل است. شاید بگویید این کار چه مزیت دارد؟ مزیت اول: این سیستم باعث افزایش سرعت دسترسی به اینترنت می شود. چون سرور پراکسی صفحات وبی که قبلا باز شده اند را در حافظه ذخیره می کند، هنگامی که شما به این صفحات احتیاج دارید به جای اینکه آن را از سایت اصلی و از محلی دور پیدا کنید به راحتی وبه سرعت آنها را از این دستگاه برمی دارید. حال ببینیم نحوه ی کار به چه صورت است. وقتی شما در یک شبکه ی محلی مثلا شبکه ی شرکت می خواهید به یک سرویس دهنده در شبکه دسترسی داشته باشید، یک درخواست از کامپیوتر

شما به سرور پراکسی (سرویس دهنده ی پراکسی) فرستاده می شود. سرور پراکسی با سرور اصلی در اینترنت ارتباط برقرار می کند و سپس سرور پراکسی اطلاعات را از سرور اینترنت به کامپیوتر شما درون شبکه شرکت می فرستد و در ضمن یک کپی از این اطلاعات در سرور پراکسی ذخیره می شود. مزیت دوم: با کمی دقت می بینید که سرور پراکسی به عنوان یک واسطه بین شبکه ی اینترنت و شبکه ی شرکت شما عمل می کند. به عبارتی باعث امنیت در شبکه ی داخلی شرکت می شود. چون به جای اینکه چندین کامپیوتر در شبکه داخلی به اینترنت متصل باشند فقط یک سرور پراکسی با اینترنت در ارتباط است. امنیت شبکه از لحاظ ویروس و هک شدن... تا حدود زیادی تامین می شود. اما این چگونه انجام می شود؟ معمولا در شرکت ها برای محافظت از شبکه ی خود از دیواره های آتش (Firewalls) استفاده می کنند. دیواره های آتش به کاربر در شبکه امکان می دهند به اینترنت دسترسی داشته باشد، ولی جلوی هکرها و هر کس در اینترنت که می خواهد به شبکه آن شرکت دسترسی داشته باشد و باعث خسارت شود را می گیرند. دیواره های آتش مجموعه ای از سخت افزارها و نرم افزارهایی مثل مسیریاب ها، سرویس دهنده ها و نرم افزارهای مختلف هستند. انواع مختلفی دارند و بسته به کاربردشان می توانند ساده و یا پیچیده باشند.

فرستادن پیام در شبکه های LAN

برای این کار ابتدا وارد Cmmand Prmpt می شویم و در آن فرمان IPCNFIG را تایپ می کنیم. پس از چند لحظه در زیر همین قسمت تمام آی پی هایی که در آن لحظه به کامپیوتر شما یا به شبکه Lan داخلی متصل هستند نوشته می شود. برای مثال: ۱۹۲.۱۶۸.۰.۱ ۱۹۲.۱۶۸.۰.۲ و غیره... روش کار: برای شروع کار ابتدا یکی از آی بی ها را انتخاب می کنیم (سعی می کنیم تا صاحب آی پی مورد نظر از جنس مخالف باشد :D) و دستور زیر را برای آن آی پی می نویسیم: NET SEND IP MESSAGE که به ترتیب: NET SEND : دستور اولیه می باشد. IP : ای پی شخص مورد نظر. MESSAGE: پیغام مورد نظر می باشد. برای مثال : .....

آموزش راه اندازی شبکه خصوصی مجازی (VPN)

شبکه خصوصی مجازی یا VPN (Virtual Private Netwrk) در اذهان تصور یک مطلب پیچیده برای استفاده و پیاده کنندگان آن به وجود آورده است . اما این پیچیدگی ، در مطالب بنیادین و مفهومی آن است نه در پیاده سازی . این نکته را باید بدانید که پیاده سازی VPN دارای روش خاصی نبوده و هر سخت افزار و نرم افزاری روش پیاده سازی خود را داراست و نمی توان روش استانداردی را برای کلیه موارد بیان نمود . اما اصول کار همگی به یک روش است . مختصری درباره تئوری VPN مفهوم اصلی VPN چیزی جز برقراری یک کانال ارتباطی خصوصی برای دسترسی کاربران راه دور به منابع شبکه نیست . در این کانال که بین دو نقطه برقرار می شود ، ممکن است که مسیرهای مختلفی عبور کند اما کسی قادر به وارد شدن به این شبکه خصوصی شما نخواهد بود . گرچه می توان از VPN در هر جایی استفاده نمود اما استفاده آن در خطوط Dialup و Leased کار غیر ضروری است (در ادامه به دلیل آن پی خواهید برد). در یک ارتباط VPN شبکه یا شبکه ها می توانند به هم متصل شوند و از این طریق کاربران از راه دور به شبکه به راحتی دسترسی پیدا می کنند. اگر این روش از ارائه دسترسی کاربران از راه دور را با روش خطوط اختصاصی فیزیکی (Leased) مقایسه کنیم ، می بینید که ارائه یک ارتباط خصوصی از روی اینترنت به مراتب از هر روش دیگری ارزان تر تمام می شود . از اصول دیگری که در یک شبکه VPN در نظر گرفته شده بحث امنیت انتقال اطلاعات در این کانال مجازی می باشد . یک ارتباط VPN می تواند بین یک ایستگاه کاری و یک شبکه محلی و یا بین دو شبکه محلی صورت گیرد. در بین هر دو نقطه یک تونل ارتباطی برقرار می گردد و اطلاعات انتقال یافته در این کانال به صورت کد شده

حرکت می کنند ، بنابراین حتی در صورت دسترسی مزاحمان و هکرها به این شبکه خصوصی نمی توانند به اطلاعات رد و بدل شده در آن دسترسی پیدا کنند. جهت برقراری یک ارتباط VPN ، می توان به کمک نرم افزار یا سخت افزار و یا ترکیب هر دو ، آن را پیاده سازی نمود . به طور مثال اکثر دیواره های آتش تجاری و روترها از VPN پشتیبانی می کنند . در زمینه نرم افزاری نیز از زمان ارائه ویندوز NT ویرایش ۴ به بعد کلیه سیستم عامل ها دارای چنین قابلیتی هستند . در این مقاله پیاده سازی VPN بر مبنای ویندوز ۲۰۰۰ گفته خواهد شد . پیاه سازی VPN برای پیاده سازی VPN بر روی ویندوز ۲۰۰۰ کافیست که از منوی Prgram/AdministrativeTls/ ، گزینه Ruting and Remte Access را انتخاب کنید . از این پنجره گزینه VPN را انتخاب کنید . پس از زدن دکمه Next وارد پنجره دیگری می شوید که در آن کارت های شبکه موجود بر روی سیستم لیست می شوند . برای راه اندازی یک سرور VPN می بایست دو کارت شبکه نصب شده بر روی سیستم داشته باشید . از یک کارت شبکه برای ارتباط با اینترنت و از کارت دیگر جهت برقراری ارتباط با شبکه محلی استفاده می شود. در این جا بر روی هر کارت به طور ثابت IP قرار داده شده اما می توان این IPها را به صورت پویا بر روی کارت های شبکه قرار داد . در پنجره بعد نحوه آدرس دهی به سیستم راه دوری که قصد اتصال به سرور ما را دارد پرسیده می شود . هر ایستگاه کاری می تواند یک آدرس IP برای کار در شبکه محلی و یک IP برای اتصال VPN داشته باشد . در منوی بعد نحوه بازرسی کاربران پرسیده می شود که این بازرسی می تواند از روی کاربران تعریف شده در روی خود ویندوز باشد و یا آنکه از طریق یک سرویس دهنده RADIUS صورت گیرد در صورت داشتن چندین سرور VPN استفاده از RADIUS را به شما پیشنهاد می کنیم . با این روش کاربران ، بین تمام سرورهای VPN به اشتراک گذاشته شده و نیازی به تعریف کاربران در تمامی سرورها نمی باشد. پروتکل های استفاده شونده عملیاتی که در بالاـ انجام گرفت تنها پیکربندی های لازم جهت راه اندازی یک سرور VPN می باشد . اما (Remte Ruting Access RRAS (Service دارای دو پروتکل جهت برقراری تونل ارتباطی VPN می باشد. ساده ترین پروتکل آن PPTP (Pint t Pint Tunneling Prtcl) است ، این پروتکل برگرفته از PPP است که در سرویس های Dialup مورد استفاده واقع می شود ، در واقع PPTP همانند PPP عمل می کند . پروتکل PPTP در بسیاری از موارد کافی و مناسب است ، به کمک این پروتکل کاربران می توانند به روش های PAP (Passwrd Authenticatin Prtcl) و Chap (Challenge Handshake Authenticatin Prtcl) بازرسی شوند. جهت کد کردن اطلاعات می توان از روش کد سازی RSA استفاده نمود. PPTP برای کاربردهای خانگی و دفاتر و افرادی که در امر شبکه حرفه ای نیستند مناسب است اما در جایگاه امنیتی دارای پایداری زیادی نیست . پروتکل دیگری به نام L۲TP (Layer۲ Frwarding) به وسیله شرکت CISC ارائه شده که به لحاظ امنیتی بسیار قدرتمندتر است. این پروتکل با استفاده از پروتکل انتقال اطلاعات UDP (User Datagram Prtcl) به جای استفاده از TCP به مزایای زیادی دست یافته است . این روش باعث بهینه و ملموس تر شدن برای دیواره های آتش شده است ، اما باز هم این پروتکل در واقع چیزی جز یک کانال ارتباطی نیست . جهت حل این مشکل و هر چه بالاتر رفتن ضریب امنیتی در VPN شرکت مایکروسافت پروتکل دیگری را به نام IPSec (IP Security) مطرح نموده که پیکربندی VPN با آن کمی دچار پیچیدگی می گردد. اما در صورتی که پروتکل PPTP را انتخاب کرده اید و با این پروتکل راحت تر هستید تنها کاری که باید در روی سرور انجام دهید فعال کردن قابلیت دسترسی Dial in می باشد. این کار را می توانید با کلیک بر روی Remte Access Plices در RRAS انجام دهید و با تغییر سیاست کاری آن ، آن را راه اندازی کنید (به طور کلی پیش فرض سیاست کاری ، رد کلیه درخواست ها می باشد). دسترسی ایستگاه کاری از طریق VPN حالا که سرور VPN آماده سرویس دهی شده ، برای استفاده از آن باید بر روی ایستگاه کاری نیز پیکربندیهایی را انجام دهیم . سیستم عاملی که ما در این جا استفاده می کنیم ویندوز XP می باشد و روش پیاده سازی VPN را بر روی آن خواهیم گفت اما انجام این کار بر روی ویندوز ۲۰۰۰ نیز به همین شکل صورت می

گیرد . بر روی ویندوزهای ۹۸ نیز می توان ارتباط VPN را برقرار نمود ، اما روش کار کمی متفاوت است و برای انجام آن بهتر است به آدرس زیر مراجعه کنید : www.supprt.micrst.cm بر روی ویندوزهای XP ، یک نرم افزار جهت اتصال به VPN برای هر دو پروتکل PPTP و L۲TP وجود دارد. در صورت انتخاب هر کدام ، نحوه پیکربندی با پروتکل دیگر تفاوتی ندارد . راه اندازی VPN کار بسیار ساده ای است ، کافیست که بر روی Netwrk Cnnectin کلیک نموده و از آن اتصال به شبکه خصوصی از طریق اینترنت (Private Netwrk Thrugh Internet) را انتخاب کنید . در انجام مرحله بالا از شما یک اسم پرسیده می شود . در همین مرحله خواسته می شود که برای اتصال به اینترنت یک ارتباط تلفنی (Dialup) تعریف نمایید ، پس از انجام این مرحله نام و یا آدرس سرور VPN پرسیده می شود . مراحل بالا- تنها مراحلی است که نیاز برای پیکربندی یک ارتباط VPN بر روی ایستگاه های کاری می باشد . کلیه عملیات لازمه برای VPN به صورت خودکار انجام می گیرد و نیازی به انجام هیچ عملی نیست . برای برقراری ارتباط کافیست که بر روی آیکونی که بر روی میز کاری ایجاد شده دو بار کلیک کنید پس از وارد کردن کد کاربری و کلمه عبور چندین پیام را مشاهده خواهید کرد که نشان دهنده روند انجام برقراری ارتباط VPN است . اگر همه چیز به خوبی پیش رفته باشد می توانید به منابع موجود بر روی سرور VPN دسترسی پیدا کنید این دسترسی مانند آن است که بر روی خود سرور قرار گرفته باشید . ارتباط سایت به سایت (Site-t-Site VPN) در صورتی که بخواهید دو شبکه را از طریق یک سرور VPN دومی به یکدیگر وصل کنید علاوه بر مراحل بالا باید چند کار اضافه تر دیگری را نیز انجام دهید . جزئیات کار به پروتکلی که مورد استفاده قرار می گیرد . جهت این کار باید سرور را در پنجره RRAS انتخاب کرده و منوی خاص (Prperties) آن را بیاورید . در قسمت General مطمئن شوید که گزینه های LAN و Demand Dial انتخاب شده باشند (به طور پیش گزیده انتخاب شده هستند). هم چنین اطمینان حاصل کنید که پروتکل را که قصد روت (Rute) کردن آن را دارید فعال است . پس از مراحل بالا نیاز به ایجاد یک Demand Dial دارید ، این کار را می توانید با یک کلیک راست بر روی واسط روت (Ruting Interface) انجام دهید . در پنجره بعدی که ظاهر می شود باید برای این ارتباط VPN خود یک نام تعیین کنید این نام باید همان اسمی باشد که در طرف دیگر کاربران با آن به اینترنت متصل می شوند در صورتی که این مطلب را رعایت نکنید ارتباط VPN شما برقرار نخواهد شد . پس از این مرحله باید آدرس IP و یا نام دامنه آن را مشخص کنید و پس از آن نوع پروتکل ارتباطی را تعیین نمود . اما مرحله نهایی تعریف یک مسیر (Rute) بر روی سرور دیگر می باشد بدین منظور بر روی آن سرور در قسمت Demand Dial ، RRAS را انتخاب کنید و آدرس IP و ساب نت را در آن وارد کنید و مطمئن شوید که قسمت Use This t Initate Demand انتخاب شده باشد . پس از انجام مرحله بالا کار راه اندازی این نوع VPN به پایان می رسد . پایان همان طور که دیدید راه اندازی یک سرور VPN بر روی ویندوز ۲۰۰۰ تحت پروتکل PPTP کار ساده ای بود اما اگر بخواهید از پروتکل L۲TP/IPSec استفاده کنید کمی کار پیچیده خواهد شد . به خاطر بسپارید که راه اندازی VPN بار زیادی را بر روی پردازنده سرور می گذارد و هرچه تعداد ارتباطات VPNبیشتر باشد بار زیادتری بر روی سرور است که می توانید از یک وسیله سخت افزاری مانند روتر جهت پیاده سازی VPN کمک بگیرد . آموزش کامپیوتر :: آموزش شبکه و امنیت شبکه :: نمایش میزان Lad Averages و Uptime سرور با یک تگ ام تی! یکی از تگ های مفید و جالب ام تی که تقریبا محجور و دورافتاده، قرار گرفته است و من کمتر کسی را دیده ام که از آن استفاده کند، تگ MT Server Uptime می باشد. تگی که میزان دقیق Lad Averages سرور و همچنین مدت زمان دقیق Uptime بودن سرور را نشان می دهد. خب این همه گفتم تا این تگ را به شما معرفی کنم! شما هم اگر می خواهید در مورد سروری که سایتتان روی آن قرار دارد، این اطلاعات را کسب کنید، کافی است تگ زیر را هر جای صفحه که مایلید و یا در یک صفحه جدید قرار دهید.

آموزش کلیات امنیت شبکه

وقتی بحث امنیت شبکه پیش می اید ، مباحث زیادی قابل طرح و ارائه هستند ، موضوعاتی که هر کدام به تنهایی می توانند جالب ، پرمحتوا و قابل درک باشند ، اما وقتی صحبت کار عملی به میان می اید ، قضیه یک جورایی پیچیده می شود . ترکیب علم و عمل ، احتیاج به تجربه دارد و نهایت هدف یک علم هم ، به کار امدن ان هست . وقتی دوره تئوری امنیت شبکه را با موفقیت پشت سر گذاشتید و وارد محیط کار شدید ، ممکن است این سوال برایتان مطرح شود که " خب ، حالا از کجا شروع کنم ؟ اول کجا را ایمن کنم ؟ چه استراتژی را پیش بگیرم و کجا کار را تمام کنم " ؟ انبوهی از این قبیل سوالات فکر شما را مشغول می کند و کم کم حس می کنید که تجربه کافی ندارید و این البته حسی طبیعی هست . پس اگر این حس رو دارید و می خواهید یک استراتژی علمی – کاربردی داشته باشید ، تا انتهای این مقاله با من باشید تا قدم به قدم شما رو به امنیت بیشتر نزدیک کنم. همیشه در امنیت شبکه موضوع لایه های دفاعی ، موضوع داغی هست و نظرات مختلفی وجود دارد . عده ای فایروال را اولین لایه دفاعی می دانند ، بعضی ها هم Access List رو اولین لایه دفاعی می دانند ، اما واقعیت پنهان این هست که هیچکدام از اینها ، اولین لایه دفاعی نیستند . یادتون باشد که اولین لایه دفاعی در امنیت شبکه و حتی امنیت فیزیکی ، Plicy هست . بدون plicy ، لیست کنترل ، فایروال و هر لایه دیگر ، بدون معنی می شود و اگر بدون plicy شروع به ایمن کردن شبکه کنید ، محصول یک آبکش واقعی از کار در می اید . با این مقدمه ، و با توجه به این که شما plicy مورد نظرتان را کاملا تجزیه و تحلیل کردید و دقیقا می دانید که چه چیزی رو می خواهید و چی را احتیاج ندارید ، کار را شروع می کنیم . ما باید پنج مرحله رو پشت سر بگذاریم تا کارمان تمام بشود . این پنج مرحله عبارتند از : ۱– Inspectin (بازرسی) ۲– Prtectin (حفاظت) ۳– Detectin (ردیابی) ۴– Reactin (واکنش) ۵– Reflectin (بازتاب) در طول مسیر ، از این پنج مرحله عبور می کنیم ، ضمن اینکه ایمن کردن شبکه به این شکل ، احتیاج به تیم امنیتی دارد و یک نفر به تنهایی نمی تواند این پروسه رو طی کند و اگر هم بتواند ، خیلی طولانی می شود و قانون حداقل زمان ممکن را نقض می کند . ۱– اولین جایی که ایمن کردن رو شروع می کنیم ، ایمن کردن کلیه authenticatin های موجود هست . معمولا رایج ترین روش authenticatin که مورد استفاده قرار می گیرد ، استفاده از شناسه کاربری و کلمه رمز هست. مهمترین جاهایی که باید authenticatin را ایمن و محکم کرد عبارتند از : – کلمات عبور کاربران ، به ویژه مدیران سیستم . – کلمات عبور سوییچ و روتر ها (من روی سوییچ خیلی تاکید میکنم ، چون این device به صورت plug and play کار می کند ، اکثر مدیرهای شبکه از cnfig کردن ان غافل می شوند ، در حالی که می تواند امنیت خیلی خوبی به شبکه بدهد ، به مدیران امنیتی توصیه میکنم که حتما این device رو کنترل کنند) . – کلمات عبور مربوط به SNMP . – کلمات عبور مربوط به پرینت سرور . – کلمات عبور مربوط به محافظ صفحه نمایش . آنچه که شما در کلاسهای امنیت شبکه در مورد Accunt and Passwrd Security یاد گرفتید را اینجا به کار می برید . که من به خاطر طولانی نشدن بحث به انها اشاره نمیکنم . ۲– قدم دوم نصب و به روز کردن آنتی ویروس بر روی همه دسکتاپ ، سرور و میل سرورها هست . ضمن اینکه آنتی ویروس های مربوط به کاربران باید به طور اتوماتیک به روز رسانی بشود و آموزشهای لازم در مورد فایلهای ضمیمه ایمیل ها و راهنمایی لازم جهت اقدام صحیح در صورت مشاهده موارد مشکوک یا اضطراری به کاربران هم داده بشود . ۳ – مرحله سوم شامل نصب آخرین به روز رسانی های امنیتی سیستم عامل و سرویسهای موجود هست . در این مرحله علاوه بر کارهای ذکر شده ، کلیه سرورها و device ها و دسک تاپ ها با ابزار های شناسایی حفره های امنیتی بررسی می شوند تا علاوه بر شناسایی و رفع حفره های امنیتی ، سرویس های غیر ضروری هم شناسایی و غیرفعال بشوند . ۴–در این مرحله نوبت گروه بندی کاربران و اعطای مجوزهای لازم به فایلها و دایرکتوری ها میباشد . ضمن اینکه accunt های قدیمی هم باید غیر فعال شوند . گروه بندی و اعطای مجوز بر اساس یکی از سه مدل استاندارد Access Cntrl Techniques یعنی DAC , MAC یا RBAC

انجام می شود . بعد از پایان این مرحله ، یک بار دیگه امنیت سیستم عامل باید چک بشود تا چیزی فراموش نشده باشد . ۵- حالا نوبت device ها هست که معمولا شامل روتر ، سوییچ و فایروال می شود . بر اساس plicy موجود و توپولوژی شبکه ، این bx ها باید cnfig بشوند . تکنولوژی هایی مثل PAT , NAT و filtering و غیره در این مرحله مطرح می شود و بر همین اساس این مرحله خیلی مهم هست. حتی موضوع مهم IP Addressing که از وظایف مدیران شبکه هست می تواند مورد توجه قرار بگیرد تا اطمینان حاصل بشود که از حداقل ممکن برای IP Assign به شبکه ها استفاده شده است. ۶- قدم بعد تعیین استراژی backup گیری هست . نکته مهم که اینجا وجود دارد این هست که باید مطمئن بشویم که سیستم backup گیری و بازیابی به درستی کار می کند و بهترین حالت ممکن باشد . ۷- امنیت فیزیکی . اول از همه به سراغ UPS ها می رویم . باید چک کنیم که UPS ها قدرت لازم رو برای تامین نیروی الکتریکی لازم جهت کار کرد صحیح سخت افزار های اتاق سرور در زمان اضطراری رو داشته باشند . نکات بعدی شامل کنترل درجه حرارت و میزان رطوبت هست. همینطور ایمنی در برابر سرقت و آتش سوزی. سیستم کنترل حریق باید به شکلی باشد که به نیروی انسانی و سیستم های الکترونیکی آسیب وارد نکند . به طور کل آنچه که در مورد امنیت فیزیکی یاد گرفتید را در این مرحله به کار می برید . ۸- امنیت وب سرور یکی از موضوعاتی هست که روش باید وسواس داشته باشید. به همین دلیل در این قسمت کار ، مجددا و با دقت بیشتر وب سرور رو چک و ایمن می کنیم . در حقیقت ، امنیت وب رو اینجا لحاظ می کنیم . (اسکریپت های سمت سرویس دهنده رو هیچ وقت فراموش نکنید) ۹ - حالا نوبت چک ، تنظیم و تست سیستم های Auditing و Lgging هست . این سیستم ها هم می تواند بر پایه hst و هم بر پایه netwrk باشد . سیستم های رد گیری و ثبت حملات هم در این مرحله نصب و تنظیم می شوند. باید مطمئن شوید که تمام اطلاعات لازم ثبت و به خوبی محافظت می شود . در ضمن ساعت و تاریخ سیستم ها درست باشد ، مبادا که اشتباه باشه که تمام زحماتتان در این مرحله به باد میرود . و امکان پیگیری های قانونی در صورت لزوم دیگر وجود ندارد . ۱۰- ایمن کردن Remte Access با پروتکل ها و تکنولوژی های ایمن و Secure قدم بعدی رو تشکیل می دهد. در این زمینه با توجه به شرایط و امکانات ، ایمن ترین پروتکل و تکنولوژی ها رو به خدمت بگیرید . ۱۱ - نصب فایروال های شخصی در سطح hst ها ، لایه امنیتی مضاعفی به شبکه شما میدهد . پس این مرحله رو فراموش نکنید . ۱۲ - شرایط بازیابی در حالت های اضطراری رو حتما چک و بهینه کنید . این حالت ها شامل خرابی قطعات کامپیوتری ، خرابکاری کاربران عادی ، خرابی ناشی از بلایای طبیعی (زلزله - آتش سوزی - افتادن - سرقت - سیل و ...) و خرابکاری ناشی از نفوذ هکرها ، میباشد . استاندارد های warm site و ht site را در صورت امکان رعایت کنید. یادتون باشد که " همیشه در دسترس بودن اطلاعات ، " جز، قوانین اصلی امنیتی هست . ۱۳- و قدم آخر این پروسه که در حقیقت شروع یک جریان همیشگی هست ، عضو شدن در سایتها و بولتن های امنیتی و در جریان آخرین اخبار امنیتی قرار گرفتن هست . برای همه شما عزیزان آرزوی سلامتی و موفقیت را دارم .

دو شاخص مهم شبکه، پهنای باند و میزان تاخیر

پهنای باند از جمله واژه های متداول در دنیای شبکه های کامپیوتری است که به نرخ انتقال داده توسط یک اتصال شبکه و یا یک اینترفیس ، اشاره می نماید . این واژه از رشته مهندسی برق اقتباس شده است . در این شاخه از علوم ، پهنای باند نشان دهنده مجموع فاصله و یا محدوده بین بالاترین و پائین ترین سیگنال بر روی کانال های مخابراتی (باند) ، است. به منظور سنجش اندازه پهنای باند از واحد " تعداد بایت در ثانیه " و یا bps استفاده می شود . پهنای باند تنها عامل تعیین کننده سرعت یک شبکه از زاویه کاربران نبوده و یکی دیگر از عناصر تاثیرگذار" ، میزان تاخیر "در یک شبکه است که می تواند برنامه های متعددی را که بر روی شبکه اجراء می گردند، تحت تاثیر قرار دهد . پهنای باند چیست ؟ تولید کنندگان تجهیزات سخت افزاری شبکه در زمان ارائه

محصولات خود تبلیغات زیادی را در ارتباط با پهنای باند ، انجام می دهند . اکثر کاربران اینترنت نسبت به میزان پهنای باند مودم خود و یا سرویس اینترنت bradband دارای آگاهی لازم می باشند.پهنای باند، ظرفیت اتصال ایجاد شده را مشخص نموده و بدیهی است که هر اندازه ظرفیت فوق بیشتر باشد ، امکان دستیابی به منابع شبکه با سرعت بیشتری فراهم می گردد . پهنای باند ، ظرفیت تئوری و یا عملی یک اتصال شبکه و یا یک اینترفیس را مشخص نموده که در عمل ممکن است با یکدیگر متفاوت باشند . مثلا "یک مودم V.۹۰ پهنای باندی معادل ۵۶ kbps را در حالت سقف پهنای باند حمایت می نماید ولی با توجه به محدودیت های خطوط تلفن و سایر عوامل موجود، عملا "امکان رسیدن به محدوده فوق وجود نخواهد داشت . یک شبکه اترنت سریع نیز از لحاظ تئوری قادر به حمایت پهنای باندی معادل ۱۰۰Mbps است ، ولی عملا "این وضعیت در عمل محقق نخواهد شد (تفاوت ظرفیت تئوری پهنای باند با ظرفیت واقعی) . پهنای باند بالا- و bradband در برخی موارد واژه های" پهنای باند بالا- "و" bradband " به جای یکدیگر استفاده می گردند . کارشناسان شبکه در برخی موارد از واژه" پهنای باند بالا- " به منظور مشخص نمودن سرعت بالای اتصال به اینترنت استفاده می نمایند . در این رابطه تعاریف متفاوتی وجود دارد . این نوع اتصالات، پهنای باندی بین ۶۴Kbps تا ۳۰۰kbps و یا بیشتر را ارائه می نمایند . پهنای باند بالا- با bradband متفاوت است . Bradband ، نشاندهنده روش استفاده شده به منظور ایجاد یک ارتباط است در صورتی که پهنای باند ، نرخ انتقال داده از طریق محیط انتقال را نشان می دهد . اندازه گیری پهنای باند شبکه به منظور اندازه گیری پهنای باند اتصال شبکه می توان از ابزارهای متعددی استفاده نمود . برای اندازه گیری پهنای باند در شبکه های محلی (LAN) ، از برنامه هائی نظیر netpref و ttcp ، استفاده می گردد. در زمان اتصال به اینترنت و به منظور تست پهنای باند می توان از برنامه های متعددی استفاده نمود . تعداد زیادی از برنامه های فوق را می توان با مراجعه به صفحات وب عمومی استفاده نمود . صرفنظر از نوع نرم افزاری که از آن به منظور اندازه گیری پهنای باند استفاده می گردد ، پهنای باند دارای محدوده بسیار متغیری است که اندازه گیری دقیق آن امری مشکل است . تاخیر پهنای باند صرفا "یکی از عناصر تاثیر گذار در سرعت یک شبکه است . تاخیر(Latency) که نشاندهنده میزان تاخیر در پردازش داده در شبکه است ، یکی دیگر از عناصر مهم در ارزیابی کارآئی و سرعت یک شبکه است که دارای ارتباطی نزدیک با پهنای باند می باشد . از لحاظ تئوری سقف پهنای باند ثابت است . پهنای باند واقعی متغیر بوده و می تواند عامل بروز تاخیر در یک شبکه گردد . وجود تاخیر زیاد در پردازش داده در شبکه و در یک محدوده زمانی کوتاه می تواند باعث بروز یک بحران در شبکه شده و پیامد آن پیشگیری از حرکت داده بر روی محیط انتقال و کاهش استفاده موثر از پهنای باند باشد . تاخیر و سرویس اینترنت ماهواره ای دستیابی به اینترنت با استفاده از ماهواره به خوبی تفاوت بین پهنای باند و تاخیر را نشان می دهد . ارتباطات مبتنی بر ماهواره دارای پهنای باند و تاخیر بالائی می باشند . مثلا "زمانی که کاربری درخواست یک صفحه وب را می نمائید ، مدت زمانی که بطول می انجامد تا صفحه در حافظه مستقر گردد با این که کوتاه بنظر می آید ولی کاملا "ملموس است. تاخیر فوق به دلیل تاخیر انتشار است .علاوه بر تاخیر انتشار ، یک شبکه ممکن است با نوع های دیگری از تاخیر مواجه گردد . تاخیر انتقال (مرتبط با خصایص فیزیکی محیط انتقال) و تاخیر پردازش (ارسال درخواست از طریق سرویس دهندگان پروکسی و یا ایجاد hps بر روی اینترنت) دو نمونه متداول در این زمینه می باشند . اندازه گیری تاخیر در یک شبکه از ابزارهای شبکه ای متعددی نظیر ping و tracerute می توان به منظور اندازه گیری میزان تاخیر در یک شبکه استفاده نمود . برنامه های فوق فاصله زمانی بین ارسال یک بسته اطلاعاتی از مبداء به مقصد و برگشت آن را محاسبه می نمایند . به زمان فوق rund-trip ، گفته می شود . Rund-trip تنها روش موجود به منظور تشخیص و یا بدست آوردن میزان تاخیر در یک شبکه نبوده و در این رابطه می توان از برنامه های متعددی استفاده نمود . پهنای باند و تاخیر دو عنصر تاثیر گذار در کارائی یک شبکه می باشند .معمولا "از واژه (Quality f Service) QS به منظور نشان دادن وضعیت کارآئی یک شبکه استفاده می گردد که در آن دو

شاخص مهم پهنای باند و تاخیر مورد توجه قرار می گیرد.

گزارش شبکه از سال ۲۰۰۳

بررسی های یک شرکت تحقیقاتی در سال ۲۰۰۳ نشان میدهد که بیش از ۴۰ درصد مراکز مالی از این مسئله که سیستم های نرم افزاری آنها مورد حملات الکترونیکی قرار می گیرند ناراضی بوده و احساس عدم امنیت می کنند. از این میان حدود ۱۶ درصد حملات بیرونی، ۱۰ درصد حملات داخل سازمان و حدود ۱۴ درصد هر دو نوع حمله را اعلام کرده اند. حملات هکرها بسیار پیچیده و دقیق شده است بگونه ای که در سال ۲۰۰۳ حدود یک سوم از بانکها و موسسات مالی اعتباری، گزارش حمله به سیستم های کامپیوتری خود را ثبت کرده اند. اغلب مدیران و مشاوران این موسسات اعلام کرده اند که ترس بیشتر آنها از حملات داخل سازمانی می باشد، چرا که فردی که از داخل به سیستم های کامپیوتری حمله می کند، هم اطلاعات بیشتری راجع به سازمان دارد و هم به منابع بیشتری دسترسی دارد. در مقابل این ادعا برخی دیگر معتقد هستند که مشکل فقط خطر حملات داخلی نیست. یکی از این مدیران معتقد است که" : ما همه روزه شاهد حملات پیچیده تر، هوشمندانه تر و حرفه ای تر هستیم. این در حالی است که هر روز بر مقدار اطلاعات ما افزوده می شود و نگهداری از آنها دشوارتر است ".با توجه به این مسائل اتحادیه اروپا در صدد ایجاد استانداردهای امنیتی برای تبادل اطلاعات مانند استفاده از بستر کلید عمومی (Public Key Infrastructure) است. اما این کار بسیار دشوار است چرا که بنگاههای تجاری در اروپا در یک سطح از تکنولوژی قرار ندارند و بسیاری از آنها حتی توان ترمیم و اصلاح سیستم پس از یک مشکل داخلی یا فاجعه – مانند زلزله – را نیز ندارند. در مقابل، آمریکا در این صنعت از بلوغ بیشتری برخوردار است، بخصوص برنامه هایی که پس از ۱۱ سپتامبر در آن کشور اجرا شد، توانایی آنها را برای جلوگیری از حملات و احیانا "اصلاح سیستم ها پس از فجایع مختلف – طبیعی و تروریستی – بالا برده است. در حال حاضر بنظر می رسد که روزبروز با بیشتر شدن وابستگی تجارت، صنعت و ... به اینترنت و IT مسئله امنیت از جمله مواردی است که شرکت ها و سازمانها باید به آن بیش از پیش بها دهند. این بررسی ها همچنین نشان می دهد که در سال ۲۰۰۳ بطور متوسط حدود ۶ تا ۸ درصد هزینه IT به بالابردن امنیت شبکه ها تخصیص داشته است. کارشناسان IT معتقد هستند طی سالهای ۲۰۰۴ تا ۲۰۰۶ در تمامی شرکت های متوسط و بزرگ آمریکا و اروپا بدون شک شغل جدیدی با عنوان مدیر ارشد امینت (Chief Security fficer) یا مدیر ارشد امنیت اطلاعات (Chief Infrmatin Security fficer) وجود خواهد داشت. شرکت Delitte Tuche Thmatsu برای تهیه این تحلیل با ۱۷۵ متخصص رده بالای IT در شرکت های مختلف مصاحبه کرده است.

ورود به سیستم سرور ها

این یرنامه تحت داس کار میکنه منظورم داس ویندوز هستش با این برنامه میتونید تمامه اطلاعات از قبیل user های ISP به همراه پسوردهایشان و از اینجور چیزا رو دریافت کنید این برنامه رو از اینجا بگیر یه برنامه دیگه هم هست که شبیه همینه اینم میتونی از اینجا بگیری طریقه ی استفاده از این دو تا برنامه اینارو کپی کن تو دایرکتوری windws تو همون درایوی که ویندوزت رو کپی کردی در ویندوز xp و ۲۰۰۰ باید در دایرکتوری winnt کپی کنید بعد از کپی کردن باید بروید در داس و انها را اجرا کنید کافی است بعد از کپی کردن این فایل ها در دایکتوری های مخصوص خودشان داس را بالا آوردi واسمه انها را تایپ کرد حتما دایکتوری را در داس جایی مناسب بگزارید مثل این: C:/>nbtenum -a ip adress بعدش داس رو بالا میارین و مینویسین nbtenum مهم نیست تو کدوم درایو شما فقط بنویس خوب -] Usage: nbtenum [-v nbtenum [-h nbtenum [- q] [ip address | ip input file] [username] [passwrd nbtenum [-a] [ip address | ip input file]

[dictinary file nbtenum [-s] [ip address | ip input file] [dictinary file خوب بعدش این میاد اون دو تای بالا یی مهم نیستن Nbtenum -q ip adress رو بنویسید اطلاعات سیستم رو میده Nbtenum -a ip adress رو بنویسید یوزر های سیستم رو میده ولی بصورت ناشناس وارد میشه حالا اگه بنویسید nbtenum-a ip adress keivan ایتجا با نام keivan وارد میشه و پسورد رو خالی میذاره nbtenum -s ip adress keivan این هم تقریبا کار a- رو میکنه و زیاد فرق نمیکنه در اینجا یه نکته هستش که آدمو گیج میکنه ببینید : این برنامه یه فایل درست میکنه و اطلاعات رو در اون میذاره آدرس این فایل رو شما باید تایین کنید حالا چطوری؟؟؟؟ یه مثال اول میزنم C:nbtenum -a ipadress حالا این برنامه این فایل رو در درایو c میذاره شما اول که تو داس وارد میشید اون خودش یه آدرس پیش فرض داره مثل :C: D و یا غیره که شما باید خودتون تغییرش بدین

سرورهای پراکسی، شیوه عملکرد و کاربرد آنها

برای کنکاوش بیشتر پیرامون بحث فیلتر و امنیت سرورهای سرویس دهنده نیاز به کسب اطلاعات در مورد این نوع سرورها و کاربردهای مختلف آنهاباشیم. از این جهت در این مقاله به کلیاتی پیرامون خود سرورهای فیلتر کننده که نوع سرور پراکسی می باشند، می پردازیم. مفهوم عامه پراکسی ابتدا یک نگاه بندازیم به اینکه این سرورها چه کاربردی دارند و در حقیقت اصلا می خواهیم چکار کنیم. زمانیکه شما به اینترنت متصل می شوید، یک شخص با یک IP یعنی آدرس شما هستید در یک دنیای بزرگ. این شخص برای گرفتن اطلاعات مورد نظرش می تواند خودش بوسیله مرورگر خود یک درخواست بفرستد برای اطلاعات مورد نظرش و آنرا دریافت کرده و به نمایش بگذارد. حال برای آنکه واضح تر روشن شود اینطور فرض کنیم که شما (شخصی که خواهان اطلاعات است) قصد دارید یک نفر را بکُشید (فقط مثال است) برای این کار، اگر طبق روش قبل باشد، تفنگ خود (مرورگر اینترنتی) خود را گرفته و به قصد کشتن طرف مقابل (دریافت اطلاعات درخواستی) از آن استفاده می کنید. حال بهتر نیست که یک مامور (پلیس و یا کسی که حرفه ای باشد توی این کار) را اجیر کنید تا این کار را برای شما انجام دهد؟ آیا این ماموری که شما می فرستید، حرفه ای تر نیست، و کار را بهتر انجام نمی دهد؟ اینجاست که نقش پراکسی مشخص می شود. سرور پراکسی در حقیقت درخواست را از شما می گیرد - بازیابی اطلاعات درخواستی- (یا همان سفارش کشتن شخص مورد نظر) و آنرا خود بصورت حرفه ای انجام داده و از نتایج آن شما را مطلع می سازد. پراکسی از کجا بوجود آمد؟ در روزهای اول وِب، کاربرای خانگی بسیار معدود بودند و اکثر کاربران اینترنتی، دانشمندان و محققانی بودند که از طریق ارگان خود، دانشگاه و یا موسسه خود به اینترنت متصل بودند. پهنای باند در آن زمان بسیار محدود بود و زمینه اطلاعات نیز بسیار نبود. زمانیکه یکی از این سایتهای تحقیقاتی که اکثرا حاوی اطلاعات استاتیک و ثابت بودند، به روز می شدند اکثر کاربران این شبکه ها این صفحات را می آوردند. مدیران این شبکه ها برای به اشتراک گذاشتن اینترنت در کل گروه و همچنین صرفه جویی در پهنای باند محدود موجود از سرورهای پراکسی سود می بردند. این سرورها خود، یک بار درخواست برای صفحه مورد نظر را ارسال کرده و نسخه ای از آن را ذخیره می کردند و در دفعات بعد آن را در پاسخ به درخواست کاربران داخلی ارسال می کردند. با گذشت زمان و افزایش چشمگیر پهنای باند و همچنین نیاز کاربران خانگی از استفاده از سایر متد ها و پروتوکولها استفاده از پراکسی کم رنگ تر شده است. پراکسی های وب که ما در بالا بررسی کردیم عمده ترین کاربرد پراکسی ها می باشند. از این حرفها گذشته به یک سری از کاربردهای پراکسی بپردازیم. مخفی کردن مشخصات کاربر یکی از بیشترین کاربردهای سرورهای پراکسی این است که افرادی که در شبکه داخلی قرار دارند، یعنی کاربران پشت سرور از دید افرادی که در اینترنت قرار دارند محفوظ می مانند. همانند Netwrk Address Translatin یا NAT این قابلیت سرورهای پراکسی موجبات بوجود آمدن لایه ای امن و بین شبکه ای

می شود. این قابلیت سرور های پراکسی بر اساس مبنای کار این سرورهاست. با وجود این سرورها، تمامی دخواستهای کاربران داخلی طوری به سرور مقصد در اینترنت فرستاده می شود که گویی خود این سرور این اطلاعات را برای خود می خواهد. این خصوصیات سرورهای پراکسی از آنجا ناشی می شود که لایه انتقال داده ها transprt layer بین کاربران داخلی و سرورهای اینترنتی وجود ندارد. این خود موجب آن می شود که از طرف سرورهای اینترنتی و یا کاربران بر روی اینترنت نتوان ردگیری و یا حتی حمله به کاربران داخلی واقع در پشت سرورهای پراکسی کرد. این لایه انتقال یعنی اینکه هیچ پل ارتباطی بین کاربر درخواست کننده و سرور بیرون نیست کاربر سرور پراکسی را به عنوان همان سرور بیرونی قبول می کند و درست با آن همانطور برخورد می کند که انگار سرور بیرونی است. در همین حال سرور بیرون هم سرور پراکسی را یک کاربر می بیند و با آن به همان روال کار می کند که یک کاربر کار می کند. حال اگر کاربر مستقیما اطلاعات را از سرور بیرونی دریافت کند، سرور بیرونی باید بداند که به کی دارد اطلاعات می دهد و به همین دلیل مشخصات کاربر را کامل دریافت می کند. برای ارسال اطلاعات و پاسخ به درخواست هم راه ارتباطی مستقیمی بین این دو برقرار می شود. پس اگر این سرور می تواند با کاربر ارتباط داشته باشد، هکر ها و عوامل موزی هم می توانند این کار را انجام دهند. اما در صورتیکه از سرور پراکسی استفاده شود تمام مسیر افراد بیرونی برای ردیابی و اذیت به خود سرور پراکسی ختم می شود. خوب ممکن است پیش خود سوال کنید که این همه سرور توی ISP و یا ICP وجود دارند، کار آنها چیست؟ این سرورها و روترها و یا حتی فایرولها کارشان دوباره نویسی پاکتها می باشد. این سرورها با توجه به مقصد و مبدا پاکتها را طوری می نویسند که به مقصد برسند ولی خود، عامل مستقیم برای شما نمی شوند. البته راههایی نیز ابداع شده است که سرورهای پراکسی را بطور مخفی به کار گیرند این شرکتهای سرویس دهنده، اما بعنوان سرور پراکسی کاربرد نخواهند داشت. یک جلوه دیگر مخفی کردن کاربران، ویژگی استفاده چند کاربره از پراکسی ها در محلهایی می باشد که محدودیتهای ارتباطی وجود دارد. مثلا زمانیکه می خواهید از یک IP و یا یک خط ارتباطی چند دستگاه بطور همزمان ارتباط داشته باشند. در اینجاست که سرور پراکسی آن یک میزبان است که دنیای بیرون به رسمیت می شناسد و تمام کاربران داخلی با عنوان این پراکسی شناخته می شوند. از این جهت هم می باشد که سرورهای پراکسی کوچک خانگی هم از مشهوریت خاصی برخوردارند. آزمون ماهیت اطلاعات: منظور از این آزمون، تطبیق محتویات درخواست و پاسخ آن با استانداردهای تبیین شده برای پروتوکول مورد نظر می باشد. این بحث دو مزیت دارد اما اصلی ترین و مهمترین آن آزمونهایی می باشد که جلوگیری از explit و یا هک شدن هم کاربر و هم سرور را فراهم سازد. تطبیق اطلاعات دریافتی و ارسالی، به این معنی می باشد که موارد و یا دستوراتی که در بسیاری موارد از طریق درخواستهای غیر استاندارد به کاربران تحمیل می شود، را دریافت و آنها را در چارچوبی که طبق استاندارد های تعریف شده برای هر پروتوکول قرار می دهد، و در صورتیکه در این چارچوب قرار نگیرد، پاسخی مبتنی بر آن به درخواست کننده می فرستد. برای روشن تر شدن مطلب به بحثی پیرامون یک سرور می پردازیم. اکثر می دانیم sendmail –سندمیل – یک سرور پست الکترونیکی تحت سیستم عامل NIX می باشد. این سرور در نسخه های اول توسط کاربران هک می شد. سندمیل زمانی که پیامی را دریافت می کند، به مقدار سایزی که در ابتدای پیام (header) نوشته شده است از حافظه برای ذخیره آن جدا می کند. در صورتیکه سایز حقیقی پیام از سایزی که در پیام گفته شده بیشتر باشد، مابقی پیام به صورت برنامه ای اجرایی درون برنامه سندمیل اجرا شده و به هکر این اختیار را می دهد که از طریق آن دسترسی کامل به سرور داشته باشد. حال به مثالی ساده تر برای طرف کاربر می پردازیم. در مرورگرهای ابتدایی اینترنتی، در صورتیکه در سایتی، لینک®۰ ;با تعداد کاراکتر بیشتر از ۲۵۵ کاراکتر در سایت وجود داشته باشد و بر آن کلیک شود، مرورگر لینک را به ۲۵۵ کاراکتر تقلیل داده، سپس اجرا می کند. این بدان معنی است که آنچه از این تعداد کاراکتر فراتر باشد را مرورگر به عنوان یک دستور اجرا می کند. از این روش بسیاری از هکر ها برای دستیابی به کامپیوتر طرف و خرابکاری در آن زمان استفاده می کردند. این مثال و مثال قبل به روشنی خطر

اجرای دستورات پنهانی و دستیابی به رایانه ها را چه در سمت سرور و چه برای کاربران روشن می کند. آنچه تا بحال خواندیم برای روشن شدن چگونگی عمل این نوع روش نفوذ بود اما در اینجا اشاره ای به حجم و میزان خسارتی که از طریق این روش می تواند بر یک شبکه داشته باشد بپردازیم. مایکروسافت با بلوغ سرور IIS (Internet Infrmatin Server) خود در نسخه های ۴ و ۵ خود را در سرویس دهی اینترنتی مطرح کرد. این سرورها که صفحات اینترنتی را نمایش می دادند، در طول زمان بیشتر مضر برای مایکروسافت جلوه دادند تا سودمند. حتما سایتهای بسیاری را که توسط روش ابلاغ درخواستهای غیر استاندارد هک شده اند به گوشتان رسیده است. مهمترین نقاط ضعف IIS هم همین روش بود. یک هکر می توانست با ارسال متد پست (pst) به این سرور با تعداد کاراکتری بیش از آنچه که می تواند پردازش کند دسترسی کامل به سرور مذکور پیدا کند و یا با ارسال درخواستهایی نا مفهوم به ماجولهای IIS با DLL های مختلف که مهمترین آنها Search و Legacy Database بود. این روشهای هک چنان مرسوم شده بود که هکرها با نوشتن اسکریپتهای خودکار بر روی کامپیوترهای هک شده، هزاران سرور را در طول چند ساعت هک کنند. مایکروسافت هم که بسیاری از سرویسهای قابل ارائه خود را مبتنی بر این سرور طراحی کرده بود، مانند پلتفرم .NET بدلیل از دست دادن اعتبار IIS از دست داد و کمتر شرکتی مایل به استفاده از هیچیک از آنها می شد. برای مبارزه با این پدیده، مایکروسافت تعداد کثیری (صدها) update و بروزرسانی های آنی برای IIS در اختیار کاربران آن و شرکتها قرار داد. اما با وجود اسکریپتها و آگاهی از وجود ایرادات در نرم افزار زمانی که هزاران سرور بدان آلوده می شدند، روشی مناسب برای جلوگیری از آآن نبود. سرورهای پراکسی در این زمان موثر ترین راه حل جلوگیری و حل و فسخ این مشکل شناخته شده و بکار گرفته شدند. از این باب است که تمام سایتهای شرکت مایکروسافت پشت نوعی از این سرورها قرار دارند. حتی می بینیم که در مورد نرم افزار های امن از جمله آپاچی، خود این سرور ماجول پراکسی برای سایر وب سرورها دارد. روشی که در این مبحث بدان پرداختیم روشی، پیشگیرانه می باشد که در تمام دنیا از آن استفاده می شود و تطبیق متدها و درخواستها با استانداردها قبل از ارسال به سرور مقصد در حال حاضر استانداردی در راه اندازی سرورهای میزبانی امن می باشد.

راه اندازی utlk خانوادگی

ساده ترین راه برای به اشتراک گذاشتن یک نسخه از utlk ۲۰۰۳ تعیین کاربران مجزا در windws xp است. برای این منظور به cntrl panel رفته، گزینه users را کلیک کنید و سپس کاربر جدیدی را تعریف نمایید. هنگامی که از درون یک حساب مشخص ویندوز با utlk کار می کنید، تنها مجموعه اطلاعات مربوط به آن حساب را می بینید. utlk به گونه ای طراحی شده که اطلاعات خود را در فایل پوشه های مشخصی (.PST) هر کاربر نگهداری می کند. اما اگر بخواهید بعضی از اطلاعات را که در utlk ذخیره کرده اید با دیگران به اشتراک بگذارید چه باید بکنید؟ به عنوان مثال، بسیاری از خانواده ها تمایل دارند تقویمی برای فعالیت های دسته جمعی خود داشته باشند. در این حالت ، شما باید یک فایل پوشه های شخصی ثانوی ایجاد کنید. برای این منظور از منوی file گزینه new و سپس utlk datafile را انتخاب کنید. چون در حالت عادی، utlk فایل های اطلاعاتی خود را در چند فولدر زیر یکدیگر پنهان می کند، شاید بهتر باشد این فولدر را در مکانی که دسترسی به آن آسان تر باشد، مثلا" c:\utlk ایجاد کنید و فایل هایی را که می خواهید به اشتراک بگذارید در آنجا قرار دهید. هنگامی که این فایل را ایجاد کردید، باید به ازای هر نوع خاص از اطلاعات که می خواهید وارد کنید پوشه جدیدی بسازید. با کلیک راست روی بالاترین پوشه در مجموعه جدید فولدر های شخصی خود،گزینه new flder را انتخاب کرده و اسامی مورد نظر calendar ، Tasks ltems و نام هایی از این دست را از کادر موسوم flder cntains انتخاب کنید. در اینجا می توانید برای هر پوشه نام دلخواه مثلا" (shared calender) را برای جلوگیری از اشتباه تعریف کنید. برای این که همه افراد بتوانند از این پوشه های جدید استفاده

کنند می بایست از طریق حساب های خود وارد شده و فولدر جدید را با استفاده از chsing file و سپس pen و در نهایت utlk data file باز کنند. در این هنگام شما دو دسته پوشه در قاب navigatin خواهید دید. با کلیک روی نام هر پوشه می توانید محتویات آن را ببینید. هنگامی که پوشه های اشتراکی شما باز باشند،می توانید از آن ها مانند دیگر پوشه های utlk استفاده کنید. می توانید هر کدام از cntact ها را از پوشه اشتراکی به inbx خود منتقل و پیغامی برای او ایجاد کنید. همچنین می توانید پیغامی را به پوشه اشتراکی تماس ها منتقل کنید تا آدرس ایمیل فرستنده آن را به دست آورید. البته کماکان باید از پوشه های اولیه خود برای دریافت ایمیل استفاده کنید. بنابراین هنگامی که از پوشه های مشترک استفاده می کنید، دو دسته پوشه باز شده را خواهید دید. می توانید به utlk بگویید این پوشه های اشتراکی را به عنوان پوشه های پیش فرض شما در نظر بگیرد.اما در این حالت باید سرویس های ایمیل خود را به اشتراک بگذارید. اگر از کامپیوترهای دستی نظیر (palm) استفاده می کنید نمی توانید از نرم افزار موجود در دستگاه خود برای هماهنگ کردن پوشه های اشتراکی استفاده کنید. اما با استفاده از نرم افزارهایی چون Intellisync یا نسخه های جدید pcket mirrr می توانید دستگاه خود را با پوشه های شخصی اضافی هماهنگ کنید. بیشتر pcket pc های جدید قابلیت کار با همه پوشه های utlk را دارا می باشند و چنانچه دستگاه شما چنین قابلیتی ندارد می توانید از Intellisync برای این منظور استفاده کنید. اما به خاطر داشته باشید، که اگر افراد مختلفی کامپیوتر دستی خود را با آن دسته از پوشه ها که شما ایجاد کرده اید هماهنگ کنند مشکلات زیادی برای شما ایجاد می شود. در این شرایط احتمال بوجود آمدن خطا (errr) و بوجود آمدن رکوردهای همسان افزایش می یابد. شما می توانید از پوشه cntacts واقع در پوشه اشتراکی utlk ، به عنوان مرجع آدرس ها جهت ادغام نامه ها استفاده کنید. مراحل کار دقیقا" مطابق مراحلی است که از پوشه cntacts واقع در پوشه اولیه خود انجام می دادید. یعنی پوشه را باز کنید . گزینه Tls را انتخاب کنید. روی letters and mailings وسپس mail merge کلیک کرده و مراحل را دنبال کنید. اگر بخواهید از آدرس های موجود در utlk در wrd استفاده کنید، باید wrd را به گونه ای تنظیم کنید که بتوانید پوشه را ببینید. برای این منظور، با کلیک راست روی پوشه cntacts گزینه prperties را انتخاب کنید. دکمه utlk address bk را فشار دهید. سپس گزینه shw this flder as an address bk را علامت بزنید. با این کار، می توانید آدرس دلخواه را مستقیما" از پوشه اشتراکی utlk به یک سند در wrd منتقل کنید. کافیست دکمه Insert address را زده و پوشه مورد نظر را از لیست موجود در کادر محاوره name select انتخاب کنید. (اگر دکمه Insert address را به خط ابزار wrd اضافه نکرده اید،از منوی Tls و گزینه custmize می توانید این کار را انجام دهید. به خاطر داشته باشید طراحی utlk به گونه ای نیست که چندین کاربر بتوانید به طور همزمان به فایل های اطلاعاتی آن را به گونه ای طرح ریزی کرد که هر لحظه تنها یک کاربر به فایل اطلاعاتی utlk دسترسی داشته باشد تا از خرابی آن جلوگیری شود.

چگونه تنظیمات سیستم خود را به کامپیوتر های دیگر منتقل کنیم ؟

تنظیمات سیستم از قبیل تنظیمات User Accunts و سطح دسترسی و شناسه اینترنت و... کاری بسیار وقت گیر می باشد و اگر قرار باشد این گونه تنظیمات بر روی سیستم های زیادی اعمال شود انجام این عملیات مشکل و پر دردسر خواهد بود . اما چگونه و با چه ابزاری می توان تنظیمات یک سیستم را به سایر سیستم ها انتقال داد ؟ Files and Settings Transfer Wizard یکی از قابلیتهای پیشرفته و بسیار جالب ویندوز XP است که بدین منظور طراحی شده است . برای استفاده از این ابزار از طریق منوی START به منوی Accessries و بعد از آن به System Tls رفته و Files and Settings Transfer Wizard را انتخاب کنید با استفاده از Wizard آن عملیات لازم را انجام دهید حال می توان اطلاعات را بر روی CD یا Flppy و یا هارد دیسک و حتی کامپیوتری در شبکه قرار داد پس از ذخیره اطلاعات در محل مناسب به کامپیوتر جدید رفته و دو باره به همین

قسمت مراجعه کنید و مسیر فایلها را در اختیار آن قرار دهید در این حالت کلیه تنظیمات بر روی این سیستم نیز به صورت خود کار و سریع اعمال خواهد شد .

کامل ترین مرجع خطاهای مودم به فارسی

کامل ترین مرجع خطاهای مودم ۶۰۰ . اگر سیستم در حال شماره گیری باشد و دوباره شماره گیری نمایید این خطا نمایش داده می شود . ۶۰۱ . راه انداز Prt بی اعتبار می باشد . ۶۰۲ . Prt هم اکنون باز می باشد برای بسته شدن آن باید کامپیوتر را مجددا راه اندازی نمود. ۶۰۳ . بافر شماره گیری بیش از حد کوچک است . ۶۰۴ . اطلاعات نادرستی مشخص شده است . ۶۰۵ . نمی تواند اطلاعات Prt را تعیین کند . ۶۰۶ . Prt شناسایی نمی شود . ۶۰۷ . ثبت وقایع مربوط به مودم بی اعتبار می باشد . ۶۰۸ . راه انداز مودم نصب نشده است . ۶۰۹ . نوع راه انداز مودم شناسایی نشده است . ۶۱۰ . بافر ندارد . ۶۱۱ . اطلاعات مسیر یابی غیر قابل دسترس می باشد . ۶۱۲ . مسیر درست را نمی تواند پیدا نماید . ۶۱۳ . فشرده سازی بی اعتباری انتخاب شده است . ۶۱۴ . سرریزی بافر . ۶۱۵ . Prt پیدا نشده است . ۶۱۶ . یک درخواست ناهمزمان در جریان می باشد . ۶۱۷ .Prt. یا دستگاه هم اکنون قطع می باشد . ۶۱۸ . Prt باز نمی شود. (وقتی رخ می دهد که یک برنامه از Prt استفاده کند). ۶۱۹ . Prt قطع می باشد (وقتی رخ می دهد که یک برنامه از Prt استفاده کند). ۶۲۰ . هیچ نقطه پایانی وجود ندارد . ۶۲۱ . نمی تواند فایل دفتر راهنمای تلفن را باز نماید . ۶۲۲ . فایل دفتر تلفن را نمی تواند بارگذاری نماید . ۶۲۳ . نمی تواند ورودی دفتر راهنمای تلفن را بیابد . ۶۲۴ . نمی توان روی فایل دفتر راهنمای تلفن نوشت . ۶۲۵ . اطلاعات بی اساسی در دفتر راهنمای تلفن مشاهده می شود . ۶۲۶ . رشته را نمی تواند بارگذاری کند . ۶۲۷ . کلید را نمی تواند بیابد . ۲۸ . Prt قطع شد. ۶۲۹ . Prt بوسیله دستگاه راه دور قطع می شود. (درست نبودن راه انداز مودم با برنامه ارتباطی). ۶۳۰ . Prt به دلیل از کارافتادگی سخت افزار قطع می شود . ۶۳۱ . Prt توسط کاربر قطع شد. ۶۳۲ . اندازه ساختار داده اشتباه می باشد . ۶۳۳ . Prt هم اکنون مورد استفاده می باشد و برای Remte Access Dial-up پیکر بندی نشده است (راه انداز درستی بر روی مودم شناخته نشده است) . ۶۳۴ . نمی تواند کامپیوتر شما را روی شبکه راه دور ثبت نماید . ۶۳۵ . خطا مشخص نشده است . ۶۳۶ . دستگاه اشتباهی به Prt بسته شده است . ۶۳۷ . رشته (string) نمی تواند تغییر یابد . ۶۳۸ . زمان درخواست به پایان رسیده است . ۶۳۹ . شبکه ناهمزمان قابل دسترس نیست . ۶۴۰ . خطای NetBIS رخ داده است . ۶۴۱ . سرور نمی تواند منابع NetBIS مورد نیاز برای پشتیبانی سرویس گیرنده را بدهد . ۶۴۲ . یکی از اسامی NetBIS شما هم اکنون روی شبکه راه دور ثبت می گردد ، (دو کامپیوتر می خواهند با یک اسم وارد شوند) . ۶۴۳. Dial-up. adaptr در قسمت netwrk ویندوز وجود ندارد . ۶۴۴ . شما ppus پیغام شبکه را دریافت نخواهید کرد . ۶۴۵ . Authenticatin داخلی اشکال پیدا کرده است. ۶۴۶ . حساب در این موقع روز امکان lg n وجود ندارد . ۶۴۷ . حساب قطع می باشد . ۶۴۸ . اعتبار passwrd تمام شده است . ۶۴۹ . حساب اجازه Remte Access را (دستیابی راه دور) را ندارد . (به نام و کلمه عبور اجازه dial-up داده نشده است) . ۶۵۰ . سرور Remte Access (دستیابی راه دور) پاسخ نمی دهد . ۶۵۱ . مودم شما (یا سایر دستگاههای اتصال دهنده) خطایی را گزارش کرده است . (خطا از طرف مودم بوده است) . ۶۵۲ . پاسخ نا مشخصی از دستگاه دریافت می گردد . ۶۵۳ . Macr (دستورالعمل کلان). ماکرو خواسته شده توسط راه انداز در لیست فایل INF. موجود نمی باشد . ۶۵۴ . یک فرمان یا یک پاسخ در قسمت .INF دستگاه به یک ماکرو نامشخص اشاره می نماید . ۶۵۵ . دستور العمل (پیغام) در قسمت فایل .INF دستگاه مشاهده نمی شود . ۶۵۶ . دستورالعمل (ماکرو) (default ff) در فایل .INF. دستگاه شامل یک دستور العمل نامشخص می باشد . ۶۵۷ . فایل .INF. دستگاه نمی تواند باز شود . ۶۵۸ . اسم دستگاه در فایل .INF. دستگاه یا در فایل .INI رسانه بیش از حد طولانی می باشد . ۶۵۹ . فایل .INI. رسانه به نام ناشناخته یک دستگاه اشاره می

نماید . ۶۶۰ . فایل .INI رسانه برای این فرمان پاسخی را ندارد . ۶۶۱ . فایل .INF دستگاه فرمان را از دست داده است . ۶۶۲ . تلاش برای قرار دادن یک ماکرو لیست نشده در قسمت فایل .INF صورت نگرفته است. ۶۶۳ . فایل .INI رسانه به نوع ناشناخته یک دستگاه اشاره می نماید . ۶۶۴ . نمی تواند به حافظه اختصاص دهد . ۶۶۵ . Prt برای Remte Access (دستیابی راه دور) پیکر بندی نشده است. ۶۶۶ . مودم شما (یاسایر دستگاههای اتصال دهنده) در حال حاضر کار نمی کنند . ۶۶۷ . فایل .INI رسانه را نمی تواند بخواند . ۶۶۸ . اتصال از بین رفته است . ۶۶۹ . پارامتر به کار برده شده در فایل .INI رسانه بی اعتبار می باشد . ۶۷۰ . نمی تواند نام بخش را از روی فایل .INI رسانه بخواند . ۶۷۱ . نمی تواند نوع دستگاه را از روی فایل .INI رسانه بخواند . ۶۷۲ . نمی تواند نام دستگاه را از روی فایل .INI رسانه بخواند . ۶۷۳ . نمی تواند کاربر را از روی فایل .INI رسانه بخواند . ۶۷۴ . نمی تواند بیشترین حد اتصال BPS را از روی فایل .INI رسانه بخواند . ۶۷۵ . نمی تواند بیشترین حد BPS حامل را از روی فایل .INI رسانه بخواند . ۶۷۶ . خط اشغال می باشد . ۶۷۷ . شخص به جای مودم پاسخ می دهد . ۶۷۸ . پاسخی وجود ندارد . ۶۷۹ . نمی تواند عامل را پیدا نماید . ۶۸۰ . خط تلفن وصل نیست . ۶۸۱ . یک خطای کلی توسط دستگاه گزارش می شود . ۶۸۲ . Writing sectin name دچار مشکل می باشد. ۶۸۳ . Writing device type با مشکل روبرو شده است. ۶۸۴writing device name. ۶۸۴ با مشکل روبرو می باشد . ۶۸۵ . Writing maxcnnectbps مشکل دارد. ۶۸۶ . Writing maxcarrierBPS دچار مشکل می باشد. ۶۸۷ . Writing usage با مشکل مواجه است. ۶۸۸ . Writing default ff دچار مشکل می باشد. ۶۸۹ . Reading default ff با مشکل مواجه است. ۶۹۰ . فایل INI خالی ست . ۶۹۱ . دسترسی صورت نمی پذیرد زیرا نام و کلمه عبور روی دامین بی اعتبار می باشد ۶۹۲ . سخت افزار در درگاه یا دستگاه متصل شده از کار افتاده است . ۶۹۳ . Binary macr با مشکل مواجه می باشد . ۶۹۴ . خطای DCB یافت نشد . ۶۹۵ . ماشین های گفتگو آماده نیستند . ۶۹۶ . راه اندازی ماشین های گفتگو با مشکل روبرو می باشد . ۶۹۷ . Partial respnse lping با مشکل روبرو می باشد . ۶۹۸ . پاسخ نام کلیدی در فایل INF . دستگاه ، در فرمت مورد نظر نمی باشد . ۶۹۹ . پاسخ دستگاه باعث سر ریزی بافر شده است . ۷۰۰ . فرمان متصل به فایل INF . دستگاه بیش از حد طولانی می باشد . ۷۰۱ . دستگاه به یک میزان BPS پشتیبانی نشده توسط گرداننده cm تغییر می یابد . ۷۰۲ . پاسخ دستگاه دریافت می گردد زمانی که هیچکس انتظار ندارد . ۷۰۳ . در فعالیت کنونی مشکلی ایجاد شده است . ۷۰۴ . شماره اشتباه ۷۰۵ . callback . مشکل . ۷۰۶ . invalid auth state Invalid auth state دچار مشکل می باشد. ۷۰۷ . علامت خطایاب . ۷۰۸ X. ۲۵ . اعتبار حساب تمام شده است . ۷۰۹ . تغییر پسورد روی دامین با مشکل روبرو می باشد . ۷۱۰ . در زمان ارتباط با مودم شما خطاهای سری یش از حد اشباع شده مشاهده می گردد. ۷۱۱ . Rasman initializatin صورت نمی گیرد گزارش عملکرد را چک کنید ۷۱۲ . درگاه Biplex در حال اجرا می باشد . چند ثانیه منتظر شوید و مجددا شماره بگیرید . ۷۱۳ . مسیرهای ISDN فعال در خط اصلی قطع می باشد . ۷۱۴ . کانال های ISDN کافی برای ایجاد تماس تلفنی در دسترس نمی باشند . ۷۱۵ . به دلیل کیفیت ضعیف خط تلفن خطاهای فراوانی رخ می دهد . ۷۱۶ . پیکر بندی remte access IP غیر قابل استفاده می باشد . ۷۱۷ . آدرسهای IP در static pl remte access IP وجود ندارد . ۷۱۸ . مهلت بر قراری تماس PPP پایان پذیرفته است . ۷۱۹ . PPP توسط دستگاه راه دور پایان می یابد . ۷۲۰ . پروتکل های کنترلppp پیکر بندی نشده اند . ۷۲۱ . همتای PPP پاسخ نمی دهد . ۷۲۲ . بسته PPPبی اعتبار می باشد . ۷۲۳ . شماره تلفن از جمله پیشوند و پسوند بیش از حد طولا نی می باشد . ۷۲۴ . پروتکل IPXنمی تواند بر روی درگاه dial –ut نماید زیرا کامپیوتر یک مسیر گردان IPX می باشد . ۷۲۵ . IPX نمی تواند روی prt (درگاه) dial – in شود زیرا مسیر گردان IPX نصب نشده است . ۷۲۶ . پروتکل IPX نمی تواند برای dial – ut ، روی بیش از یک درگاه در یک زمان استفاده شود . ۷۲۷ . نمی توان به فایل TCPCFG . DLL دست یافت . ۷۲۸ . نمی تواند آداپتور IP متصل به remte access

را پیدا کند . ۷۲۹ . SLIP استفاده نمی شود مگر اینکه پروتکل IP نصب شود . ۷۳۰ . ثبت کامپیوتر کامل نمی باشد . ۷۳۱ . پروتکل پیکر بندی نمی شود . ۷۳۲ . توافق بین PPP صورت نگرفته است . ۷۳۳ . پروتکل کنترل PPP برای پروتکل این شبکه ، در سرور موجود نمی باشد . ۷۳۴ . پروتکل کنترل لینک PPP خاتمه یافته است . ۷۳۵ . آدرس مورد نیاز توسط سرور رد می شود . ۷۳۶ . کامپیوتر راه دور پروتکل کنترل را متوقف می نماید . ۷۳۷ . نقطه برگشت (LPBACK DETECTED) شناسایی شد . ۷۳۸ . سرور آدرس را مشخص نمی کند . ۷۳۹ . سرور راه دور نمی تواند از پسورد ENCRYPTED ویندوز NT استفاده نماید. ۷۴۰ . دستگاه های TAPI که برای remte access پیکر بندی می گردند به طور صحیح نصب و آماده نشده اند . ۷۴۱ . کامپیوتر محلی از encryptin پشتیبانی نمی نماید . ۷۴۲ . سرور راه دور از encryptin پشتیبانی نمی نماید . ۷۴۳ . سرور راه دور به encryptin نیاز دارد . ۷۴۴ . نمی تواند شماره شبکه IPX را استفاده نماید که توسط سرور راه دور در نظر گرفته شده است گزارش وقایع را باز بینی نمایید . ۷۴۵ . یک فایل مهم و ضروری آسیب دیده است . Dial – up netwrking را مجددا نصب نمایید . ۷۵۱ . شماره callback شامل یک کاراکتر بی اعتبار می باشد . کاراکترهای زیر فقط مجاز دانسته می شوند : ۰ .@ , – ,(,), Space, T, P, W تا۹ . ۷۵۲ . در زمان پر دازش script یک خطای نحوی صورت می گیرد . ۷۵۳ . اتصال نمی تواند قطع شود زیرا توسط مسیر گردان چند پروتکلی ایجاد شده است . ۷۵۴ . سیستم قادر به یافتن bundle چند انصالی نمی باشد . ۷۵۵ . سیستم قادر به اجرای شماره گیری خودکار نمی باشد زیرا این ورودی یک شماره گیر عادی را دارد . ۷۵۶ . این اتصال هم اکنون در شماره گیری می باشد . ۷۵۷ . خدمات دستیابی راه دور خود به خود آغاز نمی شوند اطلا عات بیشتری در گزارش وقایع در اختیار شما قرار می گیرد . ۷۵۸ . اشتراک اتصال اینترنت هم اکنون روی این اتصال میسر می گردد . ۷۶۰ . در زمان فراهم آوری امکانات مسیر یابی ، این خطا رخ می دهد . ۷۶۱ . در زمان فراهم شدن اشتراک اتصال اینترنت برای این اتصال این خطا ایجاد می گردد. ۷۶۳ . اشتراک اتصال اینترنت فعال نمی باشد . دو اتصال LAN و یا بیشتر به علاوه اتصالی که با این LANها مشترک شده است وجود دارد . ۷۶۴ . دستگاه کارت خوان smartcard نصب نیست . ۷۶۵ . اشتراک اتصال اینترنت میسر نمی باشد . اتصال LAN با آدرس IP در حال حاضر پیکر بندی می شود که برای آدرس گذاری اتوماتیک IP مورد نیاز می باشد . ۷۶۶ . سیستم نمی تواند هیچ گواهی ای را بیابد . ۷۶۷ . اشتراک اتصال اینترنت میسر نمی گردد اتصال LAN بر روی شبکه شخصی انتخاب می گردد که بیش از یک آدرس IP را پیکر بندی کرده است . اتصال LANرا با یک آدرسIP مجزا ، مجددا پیکر بندی نمایید قبل از اینکه اشتراک اتصال اینترنت صورت گیرد . ۷۶۸ . به دلیل رمز دار نکردن داده ها اتصال صورت نمی پذیرد . ۷۶۹ . مقصد مشخصی قابل دست یابی نمی باشد . ۷۷۰ . دستگاه راه دور تلا ش برای ایجاد اتصال را نمی پذیرد . ۷۷۱ . اقدامات اتصال صورت نمی گیرد زیرا شبکه اشغال می باشد . ۷۷۲ . سخت افزار شبکه کامپیوتر راه دور با نوع تلفن مورد نیاز سازگاری ندارد . ۷۷۳ . امکان ایجاد اتصال موثر نمی باشد زیرا شماره مقصد تغییر کرده است . ۷۷۴ . به دلیل از کار افتارگی موقت ، اتصال صورت نمی گیرد . ۷۷۵ . مکالمه تلفنی توسط کامپیوتر راه دور متوقف شد . ۷۷۶ .مکالمه تلفنی نمی تواند وصل گردد زیرا مقصد خواسته است که ویژگی را حفظ نماید . ۷۷۷ . اتصال صورت نمی گیرد زیرا مودم (یا سایر وسایل ارتباط دهنده) روی کامپیوتر راه دور دچار مشکل می باشند . ۷۷۸ . تایید هویت سرور غیر ممکن می باشد . ۷۷۹ . برای بر قراری dial – ut این اتصال باید از smartcard استفاده نمایید . ۷۸۰ . عمل انجام شده برای این اتصال بی اعتبار می باشد . ۷۸۱ . تلاش برای رمز گذاری (encryptin) صورت نمی گیرد زیرا گواهی معتبری یافت نمی گردد . ۷۸۲ . ترجمه آدرس شبکه (NAT) در حال حاضر به عنوان یک پروتکل مسیر یابی نصب می گردد و باید قبل از اینکه اشتراک اتصال اینترنت فراهم گردد حذف شود . ۷۸۳ . اشتراک اتصال اینترنت میسر نمی باشد . اتصال LAN که به عنوان شبکه شخصی انتخاب می گردد یا فراهم نمی شود و یا از شبکه قطع می باشد . لطفا قبل از فراهم شدن اشتراک اتصال اینترنت از اتصال آداپتور LAN مطمئن شوید . ۷۸۴ . در حالی که این اتصال

را در زمان lg n استفاده می کنید شما نمی توانید شماره بگیرید زیرا این اتصال برای استفاده از نام کاربری پیکر بندی شده است که متفاوت از نام کاربر روی smartcard می باشد . چنانچه بخواهید آنرا در زمان lg n استفاده نمایید باید برای استفاده از (username) روی کارت smart آنرا پیکربندی کنید . ۷۸۵ . در صورت استفاده از این اتصال در زمان lg n شما نمی توانید شماره گیری نمایید زیرا برای استفاده از یک smartcard پیکر بندی نشده است . چنانچه بخواهید آنرا در زمان lg n به کار ببرید باید امکانات این اتصال را تصحیح و آماده نمایید به طوری که smartcard استفاده نماید . ۷۸۶ . مبادرت به اتصال L۲TP صورت نمی پذیرد زیرا هیچ گواهینامه معتبری برای تصدیق (authenticatin) امنیت روی کامپیوتر شما وجود ندارد . ۷۸۷ . اتصال L۲TP غیر ممکن است زیرا لایه امنیتی نمی تواند کامپیوتر راه دور را authenticatin نماید . ۷۸۸ . تلاش برای ایجاد اتصال L۲TP بی نتیجه می باشد زیرا لایه امنیتی نمی تواند پارامترهای سازگار با کامپیوتر راه دور را فراهم نماید . ۷۸۹ . تلاش برای اتصال L۲TP فراهم نمی گردد زیرا لایه امنیتی با یک خطای پردازشی در طول سازگاری با کامپیوتر راه دور مواجه است . ۷۹۰ . تلاش برای اتصال L۲TP صورت نمی گیرد زیرا تایید گواهینامه بر روی کامپیوتر راه دور میسر نمی باشد . ۷۹۱ . اتصال L۲TP میسر نمی باشد زیرا خط مشی امنیتی (security plicy) برای اتصال یافت نمی شود . ۷۹۲ . اتصال L۲TP صورت نمی گیرد زیرا زمان توافق امنیتی به پایان رسیده است . ۷۹۳ . اتصال L۲TP میسر نمی گردد زیرا این خطا رخ می دهد در حالی که در مورد امنیت به توافق می رسند . ۷۹۴ . ویژگی RADIUS این کاربر PPP نمی باشد . ۷۹۵ . ویژگی RADIUS نوع تونلی برای این کاربر ، نادرست می باشد . ۷۹۶ . ویژگی RADIUS نوع خدمات برای این کار نه قالب بندی می شود و نه callback قالب بندی می شود . ۷۹۷ . مودم پیدا نشد . ۷۹۸ . گواهینامه ای شناسایی نمی شود که بتواند پروتکل قابل ارائه استفاده شود . ۷۹۹ . اشتراک اتصال اینترنت میسر نمی گردد زیرا دو IP شبیه به هم در شبکه وجود دارد . IC ها به میزبانی نیازمند می باشند که برای استفاده از ۱۹۲ ، ۱۶۸ ، ۰ ، ۱ پیکر بندی شده است . مطمئن شوید که هیچ سرویس گیرنده دیگری برای استفاده از ۱۹۲ ، ۱۶۸ ، ۰ ، ۱ پیکر بندی نشده است . ۸۰۰ . قادر به ایجاد اتصال VPN نمی باشد . سرویس دهنده VPN در دسترس نمی باشد و یا ممکن است پارامترهای امنیتی برای اتصال به درستی پیکربندی نشده باشند .

FTP Site و راه های ایمن سازی۱

FTP یا File Transfer Prtcl یکی از رایج ترین و قدیمی ترین سرویسهای موجود بر روی شبکه ها و همچنین اینترنت است که برای نقل و انتقال فایلها روی شبکه بکار می رود. در حال حاضر FTP روشی استاندارد و در دسترس است که جامعیت یافته است. FTP Site یکی از اعضای IIS ۵.۰ بوده وبه همراه Windws ۲۰۰۰ آمده است بصورت یک Service مستقل با کارایی و امکانات فراوان می باشد. بعضی از این امکانات آشکار بوده و برخی از آنها توسط سرپرست شبکه مورد استفاده قرار می گیرند البته بعدها سرویسهای وابسته ای نظیر VPN و SSH برای امنیت رواج یافته اند. در این نوشتار ده روش موجود در Windws ۲۰۰۰ توضیح داده خواهد شد تا به کمک آن بتوانید سایتهای FTP خود را بیش از پیش در اختیار گرفته ، ایمن نموده و کنترل نمائید. ۱- از دسترسیهای بی نام و نامشخص جلوگیری نمایید. در ابتدا و پس از فعال ساختن FTP، دسترسی ها بی نام به صورت پیش فرض در سیستم به وجود می آیند. به عبارتی هرکس بدون ثبت و Autenticatin قادر به استفاده از FTP Site خواهد بود. به غیر از موارد خاص از این خاصیت در اکثر اوقات استفاده غیر مجاز می شود. با حذف دسترسی Annymus که به معنای بی نام است و استفاده از کلمه عبور و Passwrd مختص کاربر قادر به کنترل دسترسی ها خواهیم بود. این عمل با تنظیم ACL یا (Access Cntrl List) روی FTP Hme Directry که در سیستم NTFS وجود دارد قابل انجام است. برای محدود کردن دسترسی های ناشناس به FTP ، گزینه مربوط به Allw Annymus Cnnectin در پنجره Security Accunts واقع

در FTP Prperty را بردارید. ۲- گزارشگیری را فعال نمایید با فعال شدن گزارشگیری شما از اینکه چه کسانی با کدام آدرس شبکه (IP) به سایت شما دسترسی یافته اند آگاهی خواهید یافت . مرور گزارشها شما را قادر می سازد ترافیک سایت را تشخیص داده و متوجه تهدیدهای امنیتی و مشکلات شوید. برای فعال ساختن گزارشگیری از Enable Lgging ، FTP Site را در صفحه Prperty فعال سازید. بااین عمل فایل های گزارش با فرمت خاص قابل مرور شدن و تجزیه تحلیل خواهند بود. ۳- ACL را مقاوم سازید برای تنظیم نه تنها لزوم دسترسی به FTP Directry با استفاده از محدودیت های موجود در ACL (در NTFS) و همچنین تنظیم آن است بلکه گروه های موجود در FTP باید از لحاظ حقوق و دسترسی تنظیم گردند. به عنوان مثال شما تنها می خواهید دسترسی Read,Write,List Flder را به این گروه بدهید بدون آنکه امکان اجرا (Execute) را فعال سازید لذا تنها سه گزینه فوق انتخاب می شود. ۴-FTP Site را بصورت یکطرفه (Blind Put) تنظیم نمایید. اگر تنها انتقال اطلاعات به سرور مدنظر بوده و نیاز به برداشت فایل از آن نباشد (به عبارتی انتقال اطلاعات یکطرفه است) به این حالت اصطلاحا Blind Put گفته می شود. به عبارتی امکان نوشتن (Write) را دارا می باشد بدون آنکه توانایی خواندن داشته باشد. این روش یکی از روش های کنترلی برای در اختیار گرفتن دسترسی کاربران می باشد. تنظیم Blind Put در FTP Site و مجوزهای NTFS صورت می پذیرد. شکل فوق روش حذف دسترسی خواندن رااز FTP Site نشان می دهد. ۵- فعال سازی ظرفیت حافظه مورد نیاز Windws ۲۰۰۰ به همراه ابزاری دستی برای تخصیص فضای دیسک (Disk Qutas) به بازار آمد. Disk Qutas بطور مؤثر قادر به تخصیص مقدار مشخصی فضای حافظه به کاربری خاص می باشد. مقدار پیش فرض معادل فضای کل دیسک (Partitin) است. با استفاده از این خاصیت شما قادر به کنترل و محدود کردن خطاهای احتمالی ناشی از کاربرها می باشید لذا سایت شما به سایتی غیر جذاب برای نفوذگران بدل خواهد شد. جهت فعال سازی Qutas در Prperty پارتیشن NTFS قادر به انجام این مهم خواهید شد. Qutas می تواند برای یک کاربر تنظیم شود و نمی تواند به یک گروه تخصیص یابد. مدیریت Quta برای هر کاربر تنظیم می شود و محدودیت باید روی هر User Accunt برای دسترسی به FTP تنظیم گردد.

آموزش کار با برنامه NetMeeting

برنامه NetMeeting می تواند از طریق اینترنت ارتباط بین افراد را انتخاب کند با داشتن تجهیزات کافی شما می توانید از اینتر نت به عنوان یک خط تلفن یک ابزار کنفرانس ویدئویی یک تابلوی اعلانات الکترونیکی یا حتی ابزاری برای استفاده مشترک از کلیپ بوردها استفاده کنید به همین دلایل است که نام این برنامه ملاقات در شبکه یا همان NetMeeting است برای استفاده کامل از امکانات این برنامه شما به یک مودم بسیار سریع یک دوربین ویدئویی وصل شده به کامپیوتر و تعدادی دستگاه دیگر نیاز دارد با این وجود در این تمرین شما از همان تجهیزاتی که قبلاً داشته اید استفاده خواهید کرد. برای کار در برنامه NetMeeting از مراحل زیر پیروی کنید: گزینه Micrsft NetMeeting / Internet EXplrer / Prgrams را انتخاب کنید هنگامی که برای اواین مرتبه وارد برنامه Micrsft NetMeetingمی شوید مجموعهای از صفحه تصویر ها را مشاهده می کنید که شما را قادر می سازند محیط کاری این برنامه را تعریف و آماده کنید برای ادامه کار روی دکمه Next کلیک کنید اگر می خواهید در هنگامی که مردم با شما تماس می گیرند بتوانند نام و آدرس شما را مشاهده کنند باید از یک سرور دایرکتوری استفاده کنید شما باید همان سرور دایرکتوری را انتخاب کنید که افراد دیگری که معمولاً با شما تماس می گیرند از آن استفاده می کنند روی دکمه NEXT کلیک کنید تا کار ادامه یابد اکنون شما باید نام و نام خانوادگی و آدرس پست الکترونی خود را وارد کنید مابقی اطلاعات خواسته شده اختیاری هستند برای ادامه کار روی دکمه Next کلیک کنید اکنون باید برای اطلاعات خود یک گروه تعیین کنید روی دکمه Next کلیک کنید پنجره Audi Tunning Wizard باز می شود برای انتخاب نوع ارتباطی که می

خواهید از آن استفاده کنید روی دکمه Next این پنجره کلیک کنید شما صوت و تصویر ارتباطی که برنامه NetMeeting باید در این هنگام نوع صحیح ارتباط خود را تعیین کنید زیرا این تعیین مستقیماً بر روی کیفیت می تواند برقرار کند تاثیر می گذارد برای ادامه کار روی دکمه Next کلیک کنید برای آنکه پارامتر هایی که تعیین کرده اید آزمایش شوند باید روی دکمه Start Recrding کلیک کنید با این کار باید آنقدر در میکروفون خود صحبت کنید تا زمان سنج نشان دهد که آزمایش تمام شده است برای ادامه کار روی دکمه Next کلیک کنید اکنون شما آماده کار در NetMeeting هستید برای آنکه پنجره برنامه NetMeeting نشان داده شود روی دکمه Finish کلیک کنید بسته به نوع ارتباطی که شما انتخاب کرده اید برنامه Cnnectin Wizardبا اینترنت ارتباط برقرار می کند برای آنکه پنجره New Call ظاهر شود روی دکمه Call کلیک کنید اطلاعات لازم برای دسترسی به شرکت خود را در مستطیل Address وارد کنید شما می توانید در این مستطیل ادرس پست الکترونیکی نام کامپیوتر ادرس شبکه کامپیوتری و یا شماره تلفن متصل به مودم خود را وارد کنید پس از آنکه تماس شما برقرار شد روی دکمه Hang Up کلیک کنید تا ارتباط قطع شود برای بستن برنامه NetMeeting روی دکمهClse کلیک کنید اگر از برنامه NetMeeting برای ارتباط تلفنی یا تصویری با دیگران در اینترنت استفاده می کنید شما می توانید قبل از برقراری تماس ابتدا یک یادداشت را از طریق پست الکترونیکی برای شخص مورد نظر خود بفرستید تا او بداند که چه موقع با وی تماس خواهید گرفت اگر از طریق ینترنت وصل شده اید این پیش بینی بسیار مهم است زیرا برای آنکه برنامه NetMeeting مودم به ارتباط مورد نظر را برقرار کند هر دو طرف مکالمه باید به اینترنت وصل شده باشند اگر به یک LAN متصل هسنید شما احتمالاً در خواهید یافت که این روش از روش مودم بسیار بهتر است زیرا شبکه های محلی عموماً دارای سرعت انتقال داده بیشتری نسبت به مودمها هستند بنابراین شما می داده های بیشتر و با کیفیت بالاتری را در زمان کوتاهتر نسبت به مودم از طریق یک LAN ارسال کنید.

الگوریتم RSA قسمت – ۱

الگوریتم RSA قسمت – ۱ Rivest , Shamir , Adleman در مطلب قبل راجع به کلیدهای عمومی و خصوصی برای کد کردن و پنهان سازی اطلاعات صحبت کردیم و در آنجا صحبت از الگوریتمی بنام RSA نمودیم. در این مطلب سعی میکنیم و با ذکر یک مثال ساده به تشریح این لگوریتم بپردازیم. از این الگوریتم برای تهیه کلید های مذکور، کد کردن اطلاعات، دی کد کردن یا آشکار سازی اطلاعات، تهیه امضاهای الکترونیکی و .... استفاده می شود. الگوریتم RSA پس از آنکه ران ریوست (Rn Rivest)، آدام شامیر (Adam Shamir) و لن ادلمن (Len Adleman) در سال ۱۹۷۷ آنرا بدست آوردند به این نام مشهور شد، هرچند تکنیک های اولیه آن پیشتر در سال ۱۹۷۳ توسط فردی بنام کلیفورد کوکس (Cliffrd Ccks) بدست آمده بود اما تا سال ۱۹۷۷ اولا- "الگورتیم کاملا- "محرمانه بود و ثانیا "به سادگی آنچه در زیر بیان خواهیم کرد نبود. تهیه کلید های عمومی و خصوصی بطور خلاصه روش کار برای تهیه کلیدها به شرح زیر است : ۱- دو عدد بزرگ (هر چه بزرگتر بهتر) اول به نام های p و q را انتخاب می کنیم، بهتر است این اعداد از لحاظ سایز نزدیک به یکدیگر باشند. ۲- عدد دیگری بنام n را معادل با حاصلضرب p در q تعریف می کنیم : ۳ n = p x q- عدد چهارم یعنی m را معادل حاصلضرب ۱-p در ۱-q تعریف می کنیم : m = (p-) ۴ x (q-۱) (۱- عدد e را که از m کوچکتر است آنگونه پیدا می کنیم که بزرگترین مقسوم علیه مشترک این دو یک باشد به عبارتی نسبت به هم اول باشند. ۵- عددی مانند d را پیدا کنید که باقیمانده حاصلضرب d در e تقسیم بر m مساوی عدد ۱ باشد، یعنی : ۱ = (d x e) md m حال پس از طی این مراحل شما می توانید از e و n بعنوان کلید عمومی و از d و n بعنوان کلید اختصاصی استفاده کنید. روش پنهان کردن و آشکار کردن برای کد کردن اطلاعات کافی است عدد منتصب به هر کاراکتر –

مثلا "ASCII – را که در اینجا M می نامیم در فرمول زیر قرار دهید و بجای ارسال آن عدد C = Me md n را ارسال کنید. در واقع دراینجا شما توانسته اید با کمک کلید عمومی، کاراکتر M را به C تبدیل کنید. حال گیرنده برای آشکار سازی کافی است عدد دریافتی یعنی C را با استفاده از کلید خصوصی به M تبدیل کند. برای اینکار کافی است از این فرمول استفاده کنید : M = Cd md n ، بنابراین شما با دریافت کاراکتر کد شده C و در دست داشتن کلید خصوصی توانسته اید کاراکتر اصلی را مشخص نمایید. صحبت راجع به علت عملکرد صحیح این کلیدها و بازگشت پذیری الگوریتم خارج از بحث این مطلب است، اما در نوشته بعدی سعی میکنیم با ذکر مثالی مطلب را با وضوح بیشتر تشریح کنیم. (ادامه دارد ...)

نکاتی راجع به انتخاب رمز عبور

منزل مسکونی شما درب و پنجره هایی دارد که اغلب هنگام شب و یا در مواقعی که به مسافرت می روید آنها را بسته و در شرایطی قفل هایی هم به آنها اضافه می کنید. یقینا "از یک کلید برای قفل همه دربها استفاده نمی کنید و هرگز کلید ها را در اختیار افراد نا آشنا نخواهید گذاشت. همچنین کلیدها زیر فرش یا کنار باغچه حیاط مخفی نمی کنید. پس چرا با رمز عبور خود (Passwrd) اینگونه رفتار میکنید؟ برای دسترسی به سرویسهای مختلف کامپیوتر و شبکه معمولآ برای شما رمزهای عبور مختلفی در نظر گرفته می شود و شما باید همانند کلید دربهای منزل از آنها محافظت کنید. برای یک لحظه به کلید وردی منزل دقت کنید، بدون شک از بقیه کلید ها پیچیده تر و گرانتر است، بنابراین باید هنگام انتخاب رمز ورودی کامپیوتر خود موارد ایمنی را بیشتر رعایت کنید. معمولآ شما می توانید passwrd ورودی کامپیوتر خود را به هر اندازه که می خواهید پیچیده انتخاب کنید، اما دقت داشته باشید که باید بتوانید همواره به روشی آنرا بخاطر بیاورید. این روش نباید همانند گذاشتن کلید درب وردی منزل زیر فرش جلوی درب یا کنار باغچه به گونه ای باشد که سارق به سادگی بتواند آنرا پیدا کند. سارقان اینترنتی همانند سارقان منزل حرفه ای هستند بخصوص اگر با شما آشنایی داشته باشند. آنها با استفاده از تجاربی که دارند بسادگی گزینه هایی که می تواند ورود آنها به کامپیوتر شما را ممکن سازد حدس می زنند، بخصوص اگر با خصوصیات اخلاقی و زندگی شما آشنا باشند. حتی امروزه روشهایی مانند جابجایی حرف با عدد صفر یا حرف S یا $ و ... برای همه سارقان شناخته شده و جزء اولین انتخابهای آنها است. فرض کنید یک رمز عبور انتخاب می کنید و آن شامل ۶ حرف، ۴ عدد و ۴ علامت است که همگی بصورت اتفاقی (randm) انتخاب شده اند. آیا بنظر شما این رمز می تواند برای شما مفید باشد؟ به احتمال زیاد نه چرا که در اینصورت خود شما مجبور خواهید بود برای به خاطر آوردن، آنرا جایی یادداشت کنید و این خطرناک ترین کارها است. اگر مواردی که در زیر به آنها اشاره می شود را رعایت کنید می توانید تقریبآ مطمئن باشید که passwrd کامپیوتر شما به این راحتی ها توسط یک سارق قابل حدث زدن نخواهد بود : ۱– رمز باید به اندازه کافی قوی باشد. در اینجا قوی بودن به معنای طولانی بودن رمز می باشد. هیچ اشکالی ندارد که حتی بیش از ۱۴ حرف هم باشد. انتخاب یک جمله نه بصورتی که معمولآ آنرا می نویسیم می تواند گزینه مناسبی باشد. ۲– رمز باید یگانه باشد. گزینه هایی مانند ۱۲۳ یا test یا letmein یا mydg و .. گزینه هایی آشنا برای همگان است، هرگز از آنها استفاده نکنید. برای گرفتن ایده به سراغ مواردی بروید که به فکر هیچ کس نمی رسد، مثلآ نوع خاصی از یک مارماهی که در دریاهای سرد زندگی می کند. راجع به این مارماهی مطالعه کنید و پس از شناخت آن در ارتباط با آن یک رمز انتخاب کنید و راجع به آن با هیچکس صحبت نکنید. ۳– رمز باید کاربردی باشد. کاربردی به این معنای که بخاطر سپردن آن ممکن و ساده باشد. این اتفاق بارها رخ داده که کاربر رمز را به گونه ای انتخاب می کند که بعدها توانایی به یاد آوردن آنرا ندارد لذا مجبور می شود آنرا جایی یادداشت کند. ۴– رمز باید طول عمر کوتاه داشته باشد. بازه زمانی تعویض رمز کاملآ به نوع کاربری کامپیوتر و موقعیت شغلی شما دارد. اگر مسئولیت مهمی دارید و اطلاعات قیمتی در کامپیوتر خود نگه داری میکنید ترجیح بر آن است که در

فاصله های کوتاه – مثلاً یک هفته – رمز خود را عوض کنید اگر نه حداقل هر یکی دو ماه رمز عبور خود را باید تغییر دهید.

شبکه و خوب، بد، زشت!!!

روزگاری استفاده از اینترنت شامل فعالیت های مفید اطلاع رسانی بود و با وجود آنکه مرزبندی مشخص و قوانین خاصی در آن تعریف نشده بود کسی حقوق کسی را پایمال نمی کرد، اما امروز اینگونه نیست. برای مثال روند توسعه سرویس ارسال و دریافت فایل را درنظر بگیرید که سالهای سال است در حال ارائه خدمت به نرم افزارها و کاربران اینترنتی است. خوب : شما بسادگی با استفاده از سرویس FTP می توانستید فایلهای مورد نیاز خود را از سایت شرکت های تولید کننده نرم افزار بردارید و یا اینکه با نصب یک نرم افزار FTP می توانستید فایلهای مورد علاقه خود را در اختیار دوستان و آشنایان قرار دهید. یکی از بهترین امکانات اینترنت که به شما اجازه می دهد محصولات الکترونیکی را به لحظه در اختیار مردم در سراسر جهان قرار دهید. بد : سرویس های انتقال فایل پیشرفت کردند و نرم افزارهای ساده FTP به موجوداتی که امکان به اشتراک گذاردن فایل برای افرادی که یکدیگر را نمیشناسند، تبدیل شدند. امروزه اغلب به آنها نرم افزارهای Peer t Peer برای File Sharing گفته می شود. خب خیلی جای اشکال نیست اما با این روش بتدریج کاربران شروع به در اختیار یکدیگر گذاشتن نرم افزارها، موسیقی، اطلاعات و ... بدون رعایت موارد قانونی کپی رایت کردند. زشت : اما موضوع به همین جا ختم نمی شود. امروزه با نصب بسیاری از این نوع نرم افزارهای File Sharing شما درب های بسیاری را برای ورود افراد نا آشنا به کامپیوتر خود باز گذاشته اید. کسانی که از کامپیوتر شما برای ذخیره فایلهای بزرگ خود استفاده می کنند و یا خدای ناکرده از آن برای دسترسی به سایر کامپیوتر های شبکه. بنابراین دقت کنید! اگر به اینترنت از طریق خطوط پر سرعت – مثلا "ADSL – بصورت دائمی متصل هستید، آیا تاکنون متوج شده اید که به ناگاه کامپیوتر شما کند می شود؟ اگر ساده نگر باشید می گویید" این کامپیوتر دیگر قدیمی شده باید آنرا ارتقاء دهم "و یا در نهایت تصمیم به انجام عملیات پاکسازی دیسک و defragmentain می کنید. اما خیلی از اوقات مشکل شما این نیست. سودجویانی هستند که با استفاده از همین نرم افزارهای File Sharing اقدام به نگهداری فیلم، موسیقی و ... بر روی کامپیوتر شما می کنند، بدن آنکه شما متوجه شوید. شاید در لحظه ای که کامپیوتر شما کند می شود آنها در حال مصرف کردن منابع کامپیوتر شما هستند؟ همواره اینرا باید بدانید که اگر از کامپیوتر شرکت استفاده می کنید و چنین نرم افزاری را در آن نصب می کنید، در مقابل شرکت مسئولیت دارید و ممکن است کل شبکه شرکت را با اینکار خود به خطر بیندازید. متاسفانه کار به جایی رسیده که کنترل درگاه های ورودی و خروجی کامپیوتر را نمی توان به دست هر نوع نرم افزار ویروس یاب عادی سپرد، چرا که خود این نرم افزار ممکن است درگاه ورودی برای سوء استفاده کنندگان باشد. بنابراین بخصوص هنگامی که از نرم افزارهای File Sharing استفاده می کنید همواره از ویروس یاب های معتبر برای کنترل رفتار و عملکرد برنامه های موجود در کامپیوتر خود استفاده کنید.

اصول مهم مباحث امنیتی شبکه

اصول مهم امنیت اطلاعات : تفکر امنیت در شبکه برای دستیابی به سه عامل مهم است که با یک دیگر مثلث امنیتی را تشکیل می دهند. این عوامل عبارتند از راز داری و امانت داری (Cnfidentiality) ، یکپارچگی (Integrity) و در نهایت در دسترس بودن همیشگی (Availability). این سه عامل (CIA) اصول اساسی امنیت اطلاعات – در شبکه و یا بیرون آن – را تشکیل می دهند بگونه ای که تمامی تمهیدات لازمی که برای امنیت شبکه اتخاذ میشود و یا تجهیزاتی که ساخته می شوند، همگی ناشی از نیاز به اعمال این سه پارامتر در محیط های نگهداری و تبادل اطلاعات است. Cnfidentiality : به معنای آن است که اطلاعات فقط در دسترس کسانی قرار گیرد که به آن نیاز دارند و اینگونه تعریف شده است. بعنوان مثال از دست دادن این خصیصه امنیتی

معادل است با بیرون رفتن قسمتی از پرونده محرمانه یک شرکت و امکان دسترسی به آن توسط مطبوعات. Integrity : بیشتر مفهومی است که به علوم سیستمی باز می گردد و بطور خلاصه می توان آنرا اینگونه تعریف کرد: – تغییرات در اطلاعات فقط باید توسط افراد یا پروسه های مشخص و مجاز انجام گیرد. – تغییرات بدون اجاز و بدون دلیل حتی توسط افراد یا پروسه های مجاز نباید صورت بگیرد. – یکپارچگی اطلاعات باید در درون و بیرون سیستم حفظ شود. به این معنی که یک داده مشخص چه در درون سیستم و چه در خارج آن باید یکسان باشد و اگر تغییر می کند باید همزمان درون و برون سیستم از آن آگاه شوند. Availability : این پارامتر ضمانت می کند که یک سیستم – مثلا "اطلاعاتی – همواره باید در دسترس باشد و بتواند کار خود را انجام دهد. بنابراین حتی اگر همه موارد ایمنی مد نظر باشد اما عواملی باعث خوابیدن سیستم شوند – مانند قطع برق – از نظر یک سیستم امنیتی این سیستم ایمن نیست. اما جدای از مسائل بالا- مفاهیم و پارامترهای دیگری نیز هستند که با وجود آنکه از همین اصول گرفته می شوند برای خود شخصیت جداگانه ای پیدا کرده اند. در این میان می توان به مفاهیمی نظیر Identificatin به معنی تقاضای شناسایی به هنگام دسترسی کاربر به سیستم، Authenticatin به معنی مشخص کردن هویت کاربر، Authrizatin به معنی مشخص کردن میزان دسترسی کاربر به منابع، Accuntability به معنی قابلیت حسابرسی از عملکرد سیستم و ... اشاره کرد.

پنج استراتژی برای بهبود امنیت دسترسی از راه دور

مدیریت دسترسی از راه دور به اطلاعات نیاز به تخصص و تجربه زیاد دارد، کاربری که قصد ارتباط از راه دور با یک شبکه را دارد ممکن است خود به اینترنت متصل باشد و به هیچ وجه مشخص نیست که از طریق کامپیوتر او چه کسانی بخواهند بدون اجازه وارد شبکه مورد نظر وی شوند. مسئله ورود ویروس ها و کرم های اینترنتی نیز مشکل دیگری است که باید به آن توجه شود. در اینجا به پنج نکته بسیار مهم برای دسترسی از راه دور به یک شبکه اشاره خواهیم داشت، که لازم است مدیران برای اجرای آنها برنامه ریزی لازم را انجام دهند. ۱ – سیاست اجرایی کنترل نرم افزار داشته باشید. باید برای کاربرانی که قصد دسترسی به اطلاعات شبکه از راه دور را دارند، سیاست های دقیقی برای داشتن نرم افزارهای خاص در کامپیوترشان تعریف کنید. بعنوان مثال ممکن است از کاربران بخواهید نرم افزارهای آنتی ویروس (antivirus) یا ضد جاسوسی (anti-spyware) خاصی را به روش مشخص در کامپیوتر خود نصب کرده باشند. بهترین راه آن است که هنگامی که قرار است به کارمند یا کاربر خود دسترسی لازم را بدهید، آموزشهای لازم را به همراه یک جزوه به او ارائه کنید. باید مطمئن شوید که کاربر اصول و قوانین ارتباط با شبکه شما را رعایت می کند. ۲ – امنیت دروازه ارتباطی در شبکه را جدی بگیرید. از یکی از شرکت هایی که ارائه دهنده راهکارهای امنیتی هستند بخواهید که دروزاه ورود کاربران از راه دور به شبکه شرکت را بدقت تحلیل کنند و جوانب امنیتی لازم را در آن اعمال کنند. حتی ممکن است آنها پیشنهاد دهند که کاربران همگی از طریق کانالهای VPN به شبکه متصل شوند که در اینصورت باید این کار انجام شود. ۳ – در سطح شرکت قوانین امنیتی را توسعه داده ، لازم الاجرا کنید. این قوانین باید توسط همه استفاده کنندگان از شبکه شرکت حتی آنها که در داخل شرکت هستند اجرا شود. بعنوان مثال اعمالی مانند File Sharing در یک دایرکتوری می تواند جزو خطرناکترین فعالیت ها از دید امنیتی باشد که باید محدود شود. ۴ – امکان ثبت عملکردها (Lgging) و گزارش گیری را باید داشته باشید. کلیه اطلاعات (منظور lg ها است) بخصوص مربوط به دسترسی از خارج به داخل شبکه و در صورت امکان عملکردهای داخلی باید ثبت شود. یک مدیر هشیار شبکه، هر روز با گزارشهایی که از شبکه می گیرد رفتار آنرا بررسی می کند و در صورتی که مورد غیر عادی در آن ببینید کنجکاو شده و به بررسی دقیق مسئله می پردازد. بطور مرتب امنیت شبکه خود را باید مرور کنید. هر یک یا دو ماه در میان باید با مشاهده گزارشهای تهیه شده از عملکرد قبلی سیستم، سیاست های

شبکه را بطور جدی مرور کنید و آنها را بهبود کیفی ببخشید. خطر دسترسی از راه دور به شبکه را جدی بگیرید...

کلیدهای امنیتی جدید و رمزهای یک دقیقه ای !

دو شرکت بزرگ تولید کننده محصولات امنیتی اینترنتی، در ژانویه سال ۲۰۰۵ گونه های جدید سیستم های" شناسه عبور "خود را ارائه کردند. این سیستم ها از نسخه های قبلی که معمولا "در دسته کلید کاربر قرار گرفته می شد کوچکتر بوده و به آسانی با اتصال به پورت USB قابلیت کنترل شناسه های عبوری کاربر در نرم افزارهای مختلف را دارا است. از سالها پیش با ارائه این سیستم ها دیگر استفاده از روشهای سنتی username و passwrd برای شناسایی کاربران برای دسترسی به سرویسهای اطلاعاتی، سخت افزارها و ... در اینترنت و شبکه های محلی بتدریج کمرنگتر شد. در گونه های اولیه از این سیستم ها، شرکت های متخصص در امنیت اطلاعات با ارائه محصولات کوچکی همانند آنچه که در شکل اول مشاهده می کنید، دستگاه سخت افزاری کوچکی را ساختند که با کمک آن شما می توانید برای کاربران خود رمزعبوری کاملا "متغییر تهیه کنید، بگونه ای که کاربر بدون داشتن این سخت افزار عملا "نمی تواند به سیستم مورد نظر lgin نماید. روش کار بر اساس الگوریتم های پیچیده ریاضی و هماهنگی میان کلید الکترونیک با سروی است که تصدیق هویت شما را بعهده دارد است. کلید در هر بازه زمانی – مثلا" یک دقیقه – یک رمز عبوری برای شناسه شما تولید می کند و از طرف دیگر سرور با آگاهی از اینکه در این لحظه تنها چه رمزی را می تواند از شما بپذیرد، فقط رمز ارائه شده از کلید را قبول می کند. دقت کنید که کلید و سرور تشخیص هویت قبلا "از لحاظ زمانی با یکدیگر هماهنگ شده اند و در صورت ایجاد اختلاف میان ساعت دو دستگاه، پس از هر بار ورود به سیتسم سرور خود را از لحاظ زمانی با کلید هماهنگ می کند و نیز در صورت لزوم از کاربر می خواهد که رمز بعدی – که حداکثریک دقیقه بعد توسط کلید اعلام خواهد شد – را به سیستم وارد کند. تحت این شرایط سرور مطمئن می شود که شخصی که تمایل به ورود به سیستم را دارد، کیلد مخصوص را در دست داشته و نمی خواهد بصورت دزدی وارد شود. نمونه جدید کلید های الکترونیک برای پورت USB همانطور که مشاهده می کنید در این سیستم شما حتی با مشاهده کردن کلید و حفظ کردن یک کد رمز نمی توان بعدا "در موقعیت مناسب از آن استفاده کرد چرا که رمزی که در هر لحظه مشاهده می شود فقط حد اکثر یک دقیقه اعتبار دارد و پس از آن دیگر قابل استفاده نخواهد بود. لازم به ذکر است که سرور تصدیق کننده هویت می تواند از ترکیب این رمز با رمز شخصی کاربر استفاده کند. به این ترتیب با گم شدن کلید، شخص یابنده باز نمی تواند از آن برای سوء استفاده، بهربرداری نماید. گونه های جدید چه امتیازی دارند؟ در نسخه های جدید از این سخت افزارها، امکان اتصال آنها به پورتهای USB فراهم آمده است و علاوه بر آن دستگاه های جدید از لحاظ حجمی حدود ۳۵ درصد کوچکتر از گونه های قبلی ساخته شده اند. داخل این دستگاه های کوچک یک میکروکنترلر کوچک قرار دارد که به آن امکان می دهد تا هفت شناسه و سه جفت username/passwrd مختلف را مدیریت نماید. برخی از انواع این دستگاههای مشخص کننده هویت دارای ۱۲۸ یا ۲۵۶ مگابایت حافظه امن هستند و امکاناتی نظیر نگهداری کدهای رمز یکبار مصرف، کلید های خصوصی، کاربری ای شبیه به کارتهای اعتباری و ... را نیز به مصرف کننده می دهند. جالب است بدانید که مقامات یکی از این شرکتهای سازنده کدهای رمز اعلام کرده اند که در سه ماه آخر سال ۲۰۰۴ توانسته اند بیش از ۲۰ میلیون از این دستگاه های" شناسه عبور "را بفروش برسانند. همچنین گزارشها و آمارهای بدست آمده نشان می دهد که در سال ۲۰۰۳ حدود ۳۵ درصد از کاربران حرفه ای اینترنت بیان داشته بودند که از username/passwrd بعنوان یک روش نا امن برای دسترسی به اطلاعات استفاده نمی کنند، حال آنکه در سال ۲۰۰۵ تعداد این افراد به حدود ۵۳ درصد رسیده است.

IPSec چیست ؟

اگر با ویندوز ۲۰۰۰ بصورت جدی کار کرده باشید، حتما "متوجه شدید که یکی از مزایای خوب آن وجود پروتکلی بنام IPSec در آن است. این پروتکل برای این منظور طراحی شده که بتواند بسته (Packet) های اطلاعاتی TCP/IP را توسط کلید عمومی (همان روش PKC) رمز کند تا در طول مسیر، امکان استفاده غیر مجاز از آنها وجود نداشته باشد. به بیان دیگر کامپیوتر مبدا" بسته اطلاعاتی TCP/IP عادی را بصورت یک بسته اطلاعاتی IPSec بسته بندی (Encapsulate) می کند و برای کامپیوتر مقصد ارسال میکند. این بسته تا زمانی که به مقصد برسد رمز شده است و طبیعتا "کسی نمی تواند از محتوای آنها اطلاع بدست آورد. باوجود آنکه بنظر سیستم ساده ای می آید اما باید راجع به آن مطالب بیشتری بدانید. بدیهی ترین نکته آن است که استفاده از این پروتکل زمان نقل و انتقال اطلاعات را بیشتر می کند چرا که هم حجم اطلاعات بیشتر می شود و هم زمانی برای رمز کردن و رمزگشایی. بنابراین بهتر آن است که جز در موارد خاص که علاقه ندارید کسی در شبکه فعالیت های شما را متوجه شود از این پروتکل استفاده کنید. بخصوص که شما می توانید با تعریف سیاست هایی به Windws بگویید که در چه مواردی از آن استفاده کند و در چه مواردی نه. IPSec Plicy شما می توانید با دادن یک سری دستورالعمل ها به Windws، او را تعلیم دهید که تحت چه شرایطی از IPSec استفاده کند. تحت این شرایط شما در واقع مشخص می کنید که ترافیک کدام گروه از IP ها باید توسط IPSec انجام شود و کدامیک نشود برای این منظور معمولا "از روش فیلتر کردن IP استفاده می شود. فهرست خاصی از IP های فیلتر شده که شما تهیه می کنید می تواند مرجعی برای استفاده از پروتکل IPSec برای ویندوز باشد. بدیهی است برای انجام اینکار علاوه بر آشنایی با ویندوز، شما باید تا اندازه ای با شبکه ای که به آن متصل هستید آشنا بوده و اطلاعات اولیه ای را داشته باشید. برای این منظور باید از کنسول مدیریتی ویندزو (Micrsft Management Cnsle) استفاده کرده و از snap-in های مربوط به IPSec برای تعریف سیاست های نامبرده شده استفاده کنید.

شکستن الگوریتم RSA

آیا متنی که توسط الگوریتم RSA بصورت رمز شده و مخفی درآمده است قابل شکسته شدن است؟ این سئوالی است که اغلب راجع به همه روشهای رمز کردن اطلاعات پرسیده می شود. واقعیت آن است که همه روشهای رمز کردن قابل شکستن است، اما نکته مهم آن است که در چه مدت زمان و با چه امکاناتی این اطلاعات باید رمزگشایی شوند. در ارتباط با الگوریتم RSA باید گفت روشهای محدودی برای شکستن متن رمز شده توسط آن وجود دارد که در اینجا به مواردی از آن اشاره می کنیم. تجزیه n به عوامل اول اولین روش آن است که بتوان کلید خصوصی را حدس زد و یا پیدا کرد، در این صورت هکر می تواند تمامی متن های تهیه شده با کلید عمومی را رمزگشایی کند و بخواند و یا می تواند از امضای الکترونیک صاحب کلید استفاده کند. فرض را بر این می گذاریم که فردی که قصد حدس زدن کلید خصوصی را دارد، از جمله افرادی است که کلید عمومی را دارا است. در این حالت او n و e را در دسترس دارد. (برای یادآوری به مطلب الگوریتم RSA قسمت ? - مراجعه کنید.) حال اولین قدم برای این آقای هکر آن است که بتواند از روی عدد n عاملهای p و q را حدث بزند. این مشکلترین قسمت کار است که محاسبات ریاضی و بررسی های انجام داده شده نشان می دهد اگر عدد n مثلا "۱۵۵ رقم داشته باشد (RSA-۱۵۵) در آن صورت با قوی ترین کامپیوتر های موجود بیش از ۷ ماه زمان لازم است تا بتوان عوامل اول تشکیل دهنده n را مشخص کرد. الگوریتم های ریاضی بدست آمده نشان می دهد که اعداد بزرگ اگر عوامل اول کوچکتری داشته باشند، ساده تر تجزیه می شوند تا اعداد بزرگی که عوامل اول بزرگتری دارند. نکته بسیار جالب آن است که هرچقدر هم که توانایی و سرعت کامپیوتر ها برای تجزیه

یک عدد بزرگ بالاتر رود شما می توانید در هنگام استفاده از RSA با پیشنهاد کلید بزرگتر (انتخاب اعدد p و q بزرگتر) کار تجزیه n را برای کامپیوترهای جدید، بسیار دشوارتر سازید. بدست آوردن روش موثر برای محاسبه ریشه e ام با توجه به روش رمز کردن شما با داشتن کلید عمومی (n و e) و استفاده از فرمول C = Me md n می توانید حروف را رمز کنید. اما با نگاهی به فرمول می توان دریافت که کافی است شما بتوانید ریشه e ام C md n را بدست آورید در آن صورت شما می توانید به عدد m نزدیک شوید و کاراکتر اولیه برسید. نکته مهم آن است که شما در اینجا کلیدای را کشف نکرده اید و فقط توانسته اید کاراکتر را بدست آورید، ضمن آنکه بنظر نمی رسد که در حال حاضر کسی از این روش برای رمز گشایی استفاده کند چرا که به مراتب دشوار تر از روش اول است. این روش فقط برای مواردی که e عدد کوچک باشد کاربرد آزمایشگاهی و آموزشی دارد و در رمزکردن های معمولی به هیچ وجه مورد استفاده موفقیت آمیز حتی در زمانهای طولانی ندارد. حدس زدن پیام برای باز کردن رمز پیامهایی که با الگوریتم RSA رمز شده اند، روشهای محاسبه ریاضی عملا "راه به جایی نمی برند، این است که در مواردی که متن کوچک باشد شاید حدس زدن متن اصلی ساده ترین روش برای رمزگشایی باشد. ارسال پیام های کوتاه دو یا سه کلمه ای و تشخیص ساده آنها توسط هکر می تواند به او کمک کند که از روی پیام رمزگشایی شده کلید خصوصی شما را حدس بزند. در این گونه موارد کافی است تعداد زیادی کلمات یا بیت های اتفاقی (Randm) در انتهای پیام بگذارید تا هکر نتواند پیام شما را حدس بزند.

الگوریتم RSA قسمت – ۲

با توجه به روشی که در مطلب قبل ارائه کردیم در اینجا بعنوان نمونه مثالی از نحوه تعریف کلید های عمومی و خصوصی خواهیم آورد. اما برای سادگی محاسبات از اختیار کردن اعداد بزرگ دوری خواهیم کرد و توجه شما را به این نکته جلب می کنیم که هرچقدر اعداد اولیه بزرگتر باشند احتمال شکستن رمز در مدت زمان محدود ناچیزتر می شود. ۱– ابتدا باید دو عدد اول بزرگ انتخاب کنیم که در اینجا از اعداد ساده و هم اندازه ای مانند ۱۱ و ۳ استفاده می کنیم. پس q=۳ ۲ , p=۱۱– حاصلضرب p در q که همان n است را به اینصورت خواهیم داشت : n = ۱۱ X ۳ = ۳۳ ۳– حاصلضرب p–۱ در q–۱ که همان m است را به اینصورت خواهیم داشت : m = ۱۰ X ۲ = ۲۰ ۴– برای انتخاب عدد e که نسبت به m=۲۰ اول باشد و کمتر از آن هم باشد ساده ترین گزینه یعنی عدد ۳ را انتخاب می کنیم. ۵– برای یافتن عدد d که در رابطه md m = ۱ (d x e) صادق باشد اعداد ۱,۲,۳,۴,۵ و ... را امتحان می کنیم، بنظر می رسد که عدد ۷ برای اینکار مناسب باشد چرا که ۷X۳=۲۱ باقیمانده ای معادل ۱ بر m=۲۰ دارد. حال می توانیم از زوج (۳۳,۳) بعنوان کلید عمومی و از زوج (۳۳,۷) بعنوان کلید خصوصی استفاده کنیم. حال اگر از فرمول هایی که در مطلب قبل برای کد کردن و آشکار سازی استفاده کنیم برای اعداد ۱ تا ۱۶۳۲ به جدول زیر خواهیم رسید. : m

۲۳ ۲۲ ۲۱ ۲۰ ۱۹ ۱۸ ۱۷ : m ۴ ۹ ۵ ۱۹ ۱۲ ۱۱ ۱۰ ۳ ۱۷ ۱۳ ۱۸ ۲۶ ۳۱ ۲۷ ۱ ۸ ۰ : c ۱۶ ۱۵ ۱۴ ۱۳ ۱۲ ۱۱ ۱۰ ۹ ۸ ۷ ۶ ۵ ۴ ۳ ۲ ۱ ۰

۳۲ ۲۵ ۶ ۲ ۷ ۱۵ ۲۰ ۱۶ ۳۰ ۲۳ ۲۲ ۲۱ ۱۴ ۲۸ ۲۴ ۲۹ : c ۳۲ ۳۱ ۳۰ ۲۹ ۲۸ ۲۷ ۲۶ ۲۵ ۲۴ بنابراین هم اکنون شما یک جدول تبدیل کد دارید که با کمک کلید عمومی اعداد صفر تا ۳۲ را به اعدادی کد شده و در همین رنج تبدیل کرده اید. اما اگر دقت کنید تعدادی از اعداد دقیقا "به همان عدد خود تبدیل شده اند که به اینها uncncealed یا مخفی نشده گفته می شود. اولآ باید بدانیم که ۰ و ۱ همواره به همین اعداد تبدیل می شوند و مطلب دیگر اینکه اگر رنج دو عدد اول ابتدایی را بزرگ در نظر بگیریم دیگر مشکلی پیش نخواهد آمد. حال کافی است فرض کنیم C=۴ ، B=۳ ، A=۲ و ... Z=۲۷ و جملات مربوطه را کد نماییم. دقت کنید که معمولا "از ۰ و ۱ برای کدینگ استفاده نمی شود.

SSL چیست؟

Secure scket Layer یا SSL پرتکلی است که بوسیله Netscape برای انتقال پرونده های خصوصی روی اینترنت بوجود آمده است. SSL توسط یک کلید شخصی کار می کند، تا اطلاعات انتقالی در اینترنت را برای شما پنهان کند. هر دو مرورگر اینترنت اکسپلورر و نت اسکیپ از SSL پشتیبانی می کنند. و بسیاری از سایتهای از این پروتکل استفاده می کنند، تا از اطلاعات محرمانه کاربران (مانند اطلاعات کارت اعتباری) نگهداری کنند. آدرس سایتهایی که نیاز به SSL دارند باید به صورت https به جای http باشد. یک پرتکل دیگر برای انتقال مطمئن اطلاعات روی شبکه جهانی وب secure http یا s-http است. به طوریکه SSL یک ارتباط مطمئن بین یک کاربر و سرور ایجاد می کند. و هر اطلاعاتی را می توان با آن منتقل کرد. ولی s-http طراحی شده است تا پیام های شخصی را به طور ایمن انتقال دهد. بنابراین SSL و s-http را می توان به عنوان مکمل یکدیگر در نظر گرفت، تا رقیب یکدیگر. هر دو پرتکل بوسیله IETF (که مخفف Internet Engineering Task Frce است) به عنوان استاندارد تصویب شده

راه اندازی یک سرور مجازی لینوکس

همزمان با رشد سریع اینترنت و خدمات آنلاین، هر روز بر حجم پردازش سرویس دهنده ها و تعداد درخواست های کاربران افزوده می شود. اما حداکثر توان کاری هر سرویس دهنده اندازه ای دارد که بیشتر از آن نمی تواند به در خواست ها جواب دهد و به صورت معمول سرویس دهی کند. برای خروج از این وضعیت یک مدیر سرویس دهنده، چندین راه حل دارد: جایگزینی سرورهایی با قدرت پردازش بیشتر و یا افزایش تعداد سرویس دهنده های موجود. اما این کار شاید هزینه بسیار زیادی را به سیستم تحمیل کند. به طوری که عملا اجرای آن غیرممکن خواهد بود. در این شرایط ، شاید برپا سازی یک سرویس دهنده مجازی بر پایه مفاهیم کلاستر و تقسیم سرویس ها میان چندین سرویس دهنده، یکی از مؤثرترین راهکارهایی باشد که می توان برای افزایش قدرت سرویس دهنده به کاربست. کلاستر سازی این قابلیت را فراهم می کند که با افزودن یک سرور مجازی به سیستم ، در خواست های سرویس میان چند سرویس دهنده تقسیم شود و از وارد آمدن فشار اضافی بریک سرویس دهنده و نهایتا مختل شدن سرویس دهی شبکه جلوگیری به عمل آید. در این نوشتار، به برپاسازی و پیکربندی یک سرور مجازی لینوکس در یک شبکه، که شامل چندین سرویس دهنده مختلف، مانند سروی دهنده وب، ایمیل و FTP است نگاهی می اندازیم. مفهوم کلاستر کلاسترها یکی از جذاب ترین مفاهیمی هستند که در بحث های پردازش موازی و سرویس دهنده مطرح می شوند. به طور عام ، مفهوم کلاسترها به یک مجموعه از کامپیوترها اطلاق می شود که با اشتراک قدرت پردازشی یکدیگر، توان بیشتری را برای انجام دادن امور پردازشی محوله فراهم می کنند. یک کلاستر شامل چندین ماشین است که در یک شبکه محلی پرسرعت به هم متصل شده و با استفاده از یک برنامه زمانبندی و هماهنگ سازی میان ماشین های شبکه، امور پردازشی را انجام می دهند. گونه ای از این کلاسترها موسوم به lad-balancing cluster وظیفه موازنه کردن ترافیک شبکه را میان ماشین های شبکه بر عهده دارند. هدف این نوشتار نیز پیاده سازی چنین کلاستری است که بتواند با تقسیم کردن درخواست های سرویس ارسالی از کاربران یک شبکه میان چند سرویس دهنده ، از تراکم حجم کاری بر روی یک سرویس دهنده بکاهد. طرح ریزی کلاستر کلاستر شامل یک سرور مجازی مبتنی بر سیستم عامل لینوکس و تعدادی سرور فیزیکی خواهد بود که با استفاده از یک سوئیچ ، با هم در ارتباط هستند . هدف شبکه، ارائه سرویس هایی مانند وب و ایمیل به کاربران است. کاربران از طریق یک بستر شبکه ای، مانند اینترنت، با سرور مجازی ارتباط دارند. سرورهای فیزیکی می توانند بر هر سیستم عاملی مبتنی باشند. وظیفه سرور مجازی لینوکس ، بااستفاده

از آدرس های IP، کاهش فشار حجم درخواست های ارسالی به یک سرور فیزیکی و تقسیم درخواست ها میان چند سرور موجود در شبکه است. در واقع می توان گفت که سرور مجازی ، نقش یک رابط را میان کاربران شبکه و سرورهای فیزیکی شبکه ایفا می کند که در این میان، امکان همزمانی پردازش های بیشتری از درخواست ها با استفاده از یک آدرس IP فراهم می شود. هنگامی که سرور مجازی یک درخواست را از کاربر دریافت می کند، براساس یک الگوریتم زمانبندی ، درخواست کاربر را به سرور فیزیکی مربوطه تحویل می دهد. سپس سرور فیزیکی داده های مورد تقاضا را برای سرور مجازی به درخواست کاربر جواب خواهد داد. در این میان، سرویس دهنده حقیقی همان سرورهای فیزیکی هستند که آدرس IP آن ها توسط سرور مجازی تغییر یافته است. سرور مجازی از دو رابط شبکه استفاده می کند: یک رابط برای برقراری ارتباط با کاربران و دسترسی کاربران به شبکه ، و رابط دوم جهت ارتباط با شبکه محلی و سرورهای فیزیکی . راه اندازی یک کلاستر با این ساختار، قابلیت هرگونه تغییر، حذف یا افزودن سرورهای فیزیکی را برای مدیر شبکه فراهم می کند. بازسازی هسته لینوکس لینوکس شامل هسته نسخه ۲.۴.۲۸ و نسخه های بالاتر، از کلاسترهای سرور مجازی یا LVS پشتیبانی می کنند. پس اگر از نسخه های پایین تر استفاده می شود، باید با اضافه کردن ماجول LVS مجددا هسته را کامپایل و بازسازی کنید. این بسته به صورت رایگان از نشانی http://www.linuxvirtualserver.rg قابل دریافت است . چون در سایت برای نسخه های مختلف هسته، بسته های مختلفی ارائه شده ، لازم است شماره بسته متناسب با نسخه هسته لینوکس سیستم بررسی شود. بسته دریافتی از سایت را در شاخه usr/src/ کپی کنید و دستورات زیر را اجرا نمایید: -ipvs-۲.۴.۲۱-linux./ Gunzip cd/usr/scr/linux ۱.۰.۱۰.patch.gz Patch-p۱<.../linux-۲.۴.۲۱-ipvs-۱.۰.۱۰.patch دستور خط اول ، موقعیت خط فرمان را به زیرشاخه×linux منتقل می کند. در خط دوم ، با استفاده از ابزار GUNZIP ، بسته دریافت شده از سایت پروژه از حالت فشرده خارج شده و در خط سوم این بسته، به هسته اضافه شده است . پس از اضافه شدن بسته به هسته، باید مجددا هسته کامپایل شود. یعنی در دایرکتوری ×usr/src/linux دستورات زیر اجرا شوند: Make mrprper Make ldcnfig Make menucnfig با اجرای دستور آخر، یک منو با چندین زیرشاخه اجرا خواهدشد. برای فعال کردن سرور مجازی از شاخه Netwrking ptins، گزینه IP:Virtual Server Cnfiguratin را انتخاب نمایید و آدرس سرور مجازی را تنظیم کنید: IPVS (۱۶)]×[Ipvirtual server debugging virtual server supprt(EXPERIMENTAL) cnnectin table size(the Nith pwer f۲) ---IPVS scheduler Rund-rbin scheduling < M >weighted rund-rbin scheduling < M >least-cnnectin scheduling scheduling < M >weighted least-cnnectin scheduling < M >lcality-based least-cnnectin scheduling < M >lcality-based least-cnnectin with replicatin scheduling < M >destinatin hashing scheduling < M >surce hashing scheduling < M >shrtest expected delay scheduling < M >never queue scheduling ---IPVS applicatin helper FTP prtcl helper قبل از خروج از menucnfig، باید تغییرات ذخیره شوند. برای ساختن تمامی ماجول های جدید کرنل، دستور زیر اجرا می شود: make dep&&make bzlmage &&make mdules && make mdulesinstall پس از اجرای دستور بالا، زیر شاخه جدیدی به نام bzlmage در دایرکتوری /usr/src/linux×/arch/i۳۸۶/bt ساخته می شود و تصویر هسته کامپایل شده در این شاخه قرار می گیرد. برای اتمام پیکربندی هسته، باید این تصویر در شاخهbt/ کپی شده و فایل های پیکربندی بوت لودرهای سیستم نیز بروز رسانی شوند. نصب ابزار IPT و IPVsadm در گام بعدی ، پس از بازسازی هسته لینوکس، برای پیکربندی سرور مجازی ، باید بسته های IPTable و IPVsadm نصب شوند. IPTable ابزاری برای راه اندازی ساختار یک فایروال

مبتنی بر فیلتر بسته های IPV۴ و NAT در هسته لینوکس است. بااستفاده از این ابزار، آدرس های IPهای مجازی برای سرورهای فیزیکی تعریف می شوند. IPVsadm نیز یک ابزار برای مدیریت سرور مجازی لینوکس، تنظیم الگوریتم زمانبندی تقسیم درخواست ها و قوانین ارسال درخواست های کاربران به سرورهای فیزیکی است. بسته نصب IPTable به همراه اکثر توزیع ها ارائه می شود و می توان از طریق برنامه مدیریت بسته های توزیع لینوکس به راحتی آن را نصب کرد. بسته rpm نصب ابزار IPVsadm نیز از سایت پروژه LVS قابل دریافت است. پس از نصب این دو ابزار، لازم است که گزینه IP frwarding برای سرور لینوکس فعال شود. برای این منظور، فایل etc/sysctl.cnf/ را در یک ویرایشگر متنی بازکرده و گزینه زیر را با ارزش ۱ مقداردهی کنید: net.ipv۴.ipfrward=۱ اکنون کافی است با استفاده از دستور start، سرویس IPTable برای ارسال بسته های IP سرورهای فیزیکی به آدرس کاربران شبکه فعال شود: service iptables start فعال کردن IP masquerading برای تنظیم آدرس IP سرورهای فیزیکی در سرور مجازی لینوکس، باید به این نکته توجه شود که eth۰ برای کارت شبکه ارتباطی با شبکه اینترنت و eth۱ برای کارت شبکه محلی تعریف شوند. در ادامه برروی سرور مجازی، دستورات زیر اجرا شوند: iptables-t nat-P PSTRUTING DRP iptables-t nat-A PSTRUTING- eth۰-j MASQUERDE در خط اول ، با تعریف یک قانون برای IPTables، یک سطح خارجی امنیتی برای شبکه تعریف می شود. DRP این اختیار را به IRTables می دهد که هرگونه بسته IP که از ruleهای تعریفی تبعیت نمی کند، از شبکه حذف شود و در نتیجه هر آدرس IP جعلی یا ساختگی را نمی توان برای شبکه تنظیم کرد. خط دوم، جدول NAT را برای آدرس دهی شبکه داخلی میان سرورهای فیزیکی با سرور مجازی و کارت شبکه eth۰ فعال می کند. پیکربندی سرور مجازی لینوکس با IPVsadm در گام بعدی، با استفاده از ابزار IPVsadm سرور مجازی تنظیم می شود. برای شروع باید به هریک از ماشین های شبکه یک آدرس IP اختصاص داده شود. برای سرورهای فیزیکی شبکه محلی، یک بازه آدرس دهی مانند ۱۰.۰.۰.۰ تا ۲۵۵.۲۵۵.۲۵۵.۰ انتخاب شده و از یک شماره Subnet Musk استفاده می شود. از سرور مجازی به عنوان دروازه برای سرورهای فیزیکی استفاده می شود. ماشین های کلاینت با آدرس های IP اختصاص یافته توسط سرویس دهنده اینترنت با سرور مجازی در ارتباط خواهند بود. یکی از دو سرور یک سرویس دهنده HTTP است که برای آن آدرس ۱۰.۰.۰.۲ تعریف می شود و سرور دوم که یک سرویس دهنده FTP است، با ۱۰.۰.۰.۳ آدرس دهی می شود. آدرس ۱۰.۰.۰.۱ به عنوان پیش فرض دروازه برای ارتباط با سرور مجازی انتخاب می شود و برای ارتباط سرور مجازی انتخاب می شود و برای ارتباط سرور مجازی با شبکه اینترنت آدرس IP عمومی ۶۱.۱۶.۱۳۰.۱۰۰ منظور می گردد. اکنون با ابزار IPVsadm، آدرس های تخصیص داده شده برای سرور مجازی تعریف می شوند: Ipvsadm-A-t ۱۶۱.۱۶۱۳۰.۱۰۰:۸۰-s wlc ipvsadm-A-۱۶۱.۱۶.۱۳۰.۱۰۰:۲۱-s wrr در فرامین بالا wlc و wrr دو الگوریتم مدیریت ترافیک سرور مجازی برای پورت های ۸۰ و ۲۱ هستند. غیر از این دو، الگوریتم های زمانبندی قابل تعریف دیگری نیز وجود دارد که برای آشنایی با آن ها می توانید به صفحات man این برنامه مراجعه کنید. برای تعریف سرورهای فیزیکی ، دستورات بالا- به صورت زیر اجرا می شوند: ipvsadm-a-t ۱۶۱.۱۶۱۳۰.۱۰۰:۸۰-r ۱۰.۰.۰.۳:۸۰-m ipvsadm-a-t ۱۶۱.۱۶.۱۳۰.۱۰۰:۸۰-r ۱۰.۰.۰.۲:۸۰-m-w۲ ipvsadm-a-t ۱۶۱.۱۶.۱۳۰.۱۰۰:۲۱-r ۱۰.۰.۰.۳:۲۱-m البته همیشه ترافیک پورت ۸۰ بیشتر از ترافیک پورت FTP خواهدبود. بدین خاطر آدرس IP شماره ۱۰.۰.۰.۳ برای پورت ۸۰ نیز تعریف شده است. در این حالت، سرور مجازی با استفاده از الگوریتم های زمانبندی خود، می تواند بار ترافیکی این پورت را بر روی دو سرور فیزیکی تقسیم کند، با دادن ارزش دو توسط آرگومان m- به آدرس ۱۰.۰.۰۲، سرور مجازی خواهد فهمید که این پورت بر روی آدرس دیگری نیز تعریف شده است. نتیجه گیری برای آزمایش درستی عملکرد شبکه، می توان با استفاده از ماشین های کلاینت، درخواست هایی را برای سرور مجازی فرستاد و نتیجه را مشاهده کرد. اگر به صورت همزمان چندین درخواست را

از چند ماشین کلاینت ارسال کنید، خواهید دید برخی درخواست ها به وسیله سرویس دهنده FTP پردازش شده اند و آدرس IP متفاوتی میان درخواست های رسیده برروی ماشین های کلاینت وجود دارد. راه اندازی یک سرور مجازی با مشخصات بالا جوابگوی یک کلاستر با تعداد محدودی سرویس دهنده است. برای شبکه هایی که از تعداد زیادی سرویس دهنده استفاده می کنند، به راه اندازی چند سرور مجازی، تنظیمات پیشرفته جدول NAT، و سرویس DNS نیاز خواهید داشت.

امنیت شبکه های کامپیوتری

مهمترین وظیفه یک شبکه کامپیوتری فراهم سازی امکان برقراری ارتباط میان گره های آن در تمام زمانها و شرایط گوناگون است بصورتی که برخی از محققین امنیت در یک شبکه را معادل استحکام و عدم بروز اختلال در آن می دانند. یعنی Security=Rbustness+Fault Tlerance . هر چند از زاویه ای این تعریف می تواند درست باشد اما بهتر است اضافه کنیم که امینت در یک شبکه علاوه بر امنیت کارکردی به معنی خصوصی بودن ارتباطات نیز هست. شبکه ای که درست کار کند و مورد حمله ویروسها و عوامل خارجی قرار نگیرد اما در عوض تبادل اطلاعات میان دو نفر در آن توسط دیگران شنود شود ایمن نیست. فرض کنید می خواهید با یک نفر در شبکه تبادل اطلاعات – بصورت email یا chat و ... – داشته باشید، در اینصورت مصادیق امنیت در شبکه به این شکل است : هیچ کس (فرد یا دستگاه) نباید بتواند – وارد کامپیوتر شما و دوستتان شود، – تبادل اطلاعات شما را بشنود و یا از آن کپی زنده تهیه کند، – با شبیه سازی کامپیوتر دوست شما، بعنوان او با شما تبادل اطلاعات کند، – کامپیوتر شما یا دوستتان را از کار بیندازد، – از منابع کامپیوتر شما برای مقاصد خود استفاده کند، – برنامه مورد علاقه خود – یا یک تکه کد کوچک – را در کامپیوتر شما نصب کند، – در مسیر ارتباطی میان شما و دوستتان اختلال بوجود آورد، – با سوء استفاده از کامپیوتر شما به دیگران حمله کند، – و بسیاری موارد دیگر ... اما ببینیم که چه کسانی – فرد، دستگاه، نرم افزار و ... – می توانند امنیت ارتباط برقرار شده شما را تهدید کنند. هکر (Hacker) در معنای لغوی به فردی گفته می شود که با ابزار به ساخت لوازم خانه (میز، مبل و ...) می پردازد. اما امروزه این اصطلاح بیشتر به افرادی اطلاق می شود که علاقمند به کشف رمز و راز برنامه های مختلف نصب شده روی کامپیوترها می باشند تا به این وسیله دانش و توانایی خود را بالا ببرند. اینگونه افراد معمولا "دانش زیادی از نحوه کار کامپیوتر و سیستم های شبکه ای دارند و اغلب بطور غیر مجاز سعی در ورود به سیستم های اطلاعاتی یا کامپیوتر های شخصی افراد می کنند. اما معنی عمومی تر این لغت امروزه از موارد بالا نیز فراتر رفته و به افرادی گفته میشود که برای خرابکاری و یا سرقت اطلاعات و ... وارد کامپیوترها یا شبکه های کامپیوتری دیگران می شوند. قصد یا غرض این افراد از انجام اینکار ها می تواند تمام مواردی باشد که در مطلب قبل امنیت در دنیای واقعی به آن اشاره کردیم، باشد. امروزه فعالیت این افراد در بسیاری از کشورها در رده فعالیت های جنایی در نظر گرفته می شود. ویروس (Viruse) همانطور که میدانید از لحاظ بیولوژیکی موجودات کوچکی که توانایی تکثیر در درون سلولهای زنده را دارند و اغلب باعث بروز بیماری ها مانند سرما خوردگی، سرخک، هپاتیت و ... می شوند، ویروس نام دارند. ویروس ها عموما "با استفاده از روشهای مختلف در جامعه انسانی – یا حیوانی – منتشر میشوند و در صورت عدم وجود کنترل و درمانها پزشکی خطرات جبران ناپذیری را به جامعه تحمیل می کنند. با ایده برداری از همین روش یعنی زندگی در بدن یک میزبان و انتقال به هنگام تعامل میزبان با همسان خود، نرم افزارهای عموما" کوچکی تهیه شده است که می توانند در یک دستگاه کامپیوتر اجرا شوند و ضمن به خطر انداختن کار آن دستگاه به هنگام تبادل اطلاعات – به هر شکلی – با دیگر کامپیوتر ها خود را پخش کنند. این تبادل می تواند از طریق کپی کردن اطلاعات در روی دیسک باشد، یا اجرا برنامه های کامپیوتر و ... کرم های شبکه (Wrms) همانطور که میدانید حیوانات کوچک، باریک و درازی که بدنی نرم دارند و اغلب در روی زمین، درختان و گیاهان یا حتی زیر خاک زندگی کرده و از برگ گیاهان، حشرات و ... تغذیه

میکنند، کرم نامیده می شود. اما در دنیای کامپیوتر و ارتباطات اینترنتی کرم به گونه ای از نرم افزارها گفته می شود که در گره های شبکه – مثلا "کامپیوتر – مستقر شده و می تواند علاوه بر زندگی و آسیب رسان به آن گره نسخه دیگری از خود را از طریق شبکه به سایر گره ها منتقل کند و آنها را نیز دچار مشکل سازد. بنابراین مشاهده می کنید که سرعت تولید مثل و انتشار یک کرم در شبکه بزرگ چه مقدار می تواند زیاد باشد. کرم ها معمولا "علاوه بر آنکه باعث تخریب میزبان خود می شوند، با اشغال کردن فضای ارتباطی در شبکه، تاثیری چون ترافیک و کندی ارتباطات در شبکه را به همراه می آورند که این خود می تواند عوارض بعدی برای فعالیت سایر تجهیزات در شبکه و یا حتی بخش عمده ای از شبکه اینترنت شود.

کد و رمز Public Key Cryptgraphy – Encryptin

در سال ۱۹۷۶ وایتفیلد دیف (Whitfield Diffie) و مارتین هلمن (Martin Hellman) دانشجویان دانشگاه استنفورد، یکی از کاربردی ترین روشهای کد کردن اطلاعات را اختراع و به ثبت رساندند. در این روش که به روش کدینگ نا متقارن (asymmetric encryptin) نیز معروف است از دو کلید برای کد کردن اطلاعات استفاده می شود. (در روشهای قدیمی تر از یک کلید استفاده می شد که به آن symmetric encryptin گفته می شد.) آنها مقاله خود را در یکی از شماره های سال ۱۹۷۶ مجله IEEE که با عنوان Transactins n Infrmatin Thery منتشر شده بود به چاپ رساندند که خیلی زود انقلابی در صنعت Cryptgraphy (پنهان سازی اطلاعات) در دنیا بوجود آورد. Public Key Cryptgraphy یا PKC به معنی استفاده از کلید عمومی برای کد کردن و پنهان کردن اطلاعات است. در این روش هر کاربر برای کد کردن و یا باز کردن کد دو کلید در اختیار دارد، یکی کلید عمومی (Public) و یکی کلید خصوصی (Private). خاصیت این روش آن است که هر کدام از این کلید ها می تواند اطلاعاتی را که کلید دیگر کد و مخفی کرده است به حالت اصل در بیاورند. هر چند از لحاظ ریاضی کلید های Public و Private با یکدیگر ارتباط دارند اما تقریبا "محال است که کسی بتواند حتی با تجهیزات فوق العاده مدرن و صرف وقت زیاد با داشتن یکی از کلیدها، دیگری را تشخیص دهد. در واقع می توان گفت که با توجه به سطح دانش کنونی و دستگاه های کامپیوتری موجود، الگوریتم کدینگ و ارتباط میان کلیدها تقریبا "غیر قابل شکستن است. روش کار اینگونه است که هر کاربر دو کلید در دست خود دارد که یکی را در اختیار همه دوستان و اطرافیان برای خواند مطالبی که او کد کرده است قرار می دهد، این همان کلید عمومی یا Public است. حال کافی است که او برای ارسال مطالب به دیگران مطالب را با کلید خصوصی خود کد یا مخفی سازی نماید. دیگران به راحتی می توانند مطالب او را با کلید Public ای که از وی دارند با حالت اولیه بازگردانند (Decrypt) و آنها را مطالعه کنند. و یا اگر کسی بخواهد برای شما یک مطلب کد شده بفرستد با کلید Public شما آنرا کد می کند و این تنها شما و فقط شما هستید که می توانید آنرا با کلید Private خود باز کنید و به محتوای اصلی دسترسی داشته باشید. اساس استفاده از این روش کدینگ یا مخفی سازی اطلاعات به الگوریتم مشهوری بنام Rivest Shamir Adleman یا RSA بر می گردد که در آینده راجع به آن صحبت خواهیم کرد.

SSL چیست ؟

از لحاظ لغوی مخفف Secure Sckets Layer می باشد و در واقع یکی از پروتکل های انتقال اطلاعات روی وب است. این پروتکل توسط کمپانی Netscape برای اولین بار به منظور انتقال اطلاعات بصورت امن بین دونقطه در اینترنت تهیه شد و پس از مدتی علاوه بر مرورگر Netscape Navigatr و خانواده آن، مرورگر Internet Explrer نیز از آن استفاده کرد. در این روش تبادل اطلاعات میان مرورگر و سایتی که در حال مرور شدن است، بوسیله کلید های خصوصی (private key) کد

می شود و چنانچه در طول مسیر اطلاعات شنود شود، قابل استفاده نخواهد بود. بنابراین بخوبی می توان از این پروتکل برای کاربردهای تجاری استفاده کرد. در حال حاضر بسیاری از وب سایت ها علاوه بر پروتکل معمول http از SSL نیز حمایت می کنند و شما می توانید برای دسترسی امن به اطلاعات این سایت ها از طریق یک لینک SSL ، از https استفاده کنید. اما پس از معرفی SSL پروتکل دیگری بنام S-HTTP یا همان Secure HTTP برای همین منظور تعریف شد. این پروتکل برای استفاده ایمن از وب می باشد و فرقی که SSL با آن دارد در این است که SSL فقط میان دو نقطه یعنی مبدا و مقصد تعریف می شود. هر دوی این پروتکل ها توسط اداره IEFT (Internet Engineering Task Frce) بعنوان استاندارد تعریف شده اند.

آنتی ویروس چیست؟

انسان در طول زندگی و به هنگام رشد بتدریج یاد میگیرد که برای سالم زیستن باید مسائل خاصی را رعایت کند و هرگاه که نکته جدیدی می آموزد سعی می کند علاوه بر دانسته های قدیم آنرا نیز رعایت کند. مسئله امنیت شبکه یا کامپیوتر نیز چنین حالتی دارد. شما باید بتدریج با آشنا شدن مسائل مختلف امنیتی همه آنها را مد نظر داشته باشید. امنیت کامپیوتر در منزل شما یک موضوع ساده نیست که بخواهید از آن به راحتی بگذرید. موارد زیادی هست که باید به مرور زمان و کسب تجربه آنها را بیاموزید و در دستور کار خود قرار دهید. سعی خواهیم کرد در مطالبی که بتدریج ارائه میشود به مهمترین این موارد اشاره کنیم. استفاده از آنتی ویروس اگر یکنفر زنگ درب منزل شما را به صدا درآورد و بخواهد وارد منزل شما شود و به شما جنسی را به زور بفروشد، یا بخواهد از تلفن منزل شما استفاده کند و ... بدون شک شما بفکر فرو می روید که آیا به او چنین اجازه ای را بدهید که وارد منزل شود یا نه؟ اگر این فرد یکی از همسایه ها یا آشنایان باشد، به عبارتی شما شناخت مثبت لازم از او را داشته باشید به احتمال زیاد به او چنین اجازه ای را خواهید داد در غیر اینصورت بعید است که چنین کاری را انجام دهید. همچنین شما آموزشهای لازم را به فرزندان یا سایر افراد خانواده را خواهید داد تا در نبود شما رعایت این موارد امنیتی را بکنند و بدانند چه تیپ افرادی را به منزل راه دهند و کدام دسته را راه ندهند. یک نرم افزار Anti Virus که به اختصار آنرا AV می نامیم، به همین صورت رفتار می کند. نرم افزارهای AV با مشاهده و بررسی محتوای فایل ها به دنبال الگوهای آشنای ویروسها یا کرم های اینترنتی می گردند. در صورت مشاهده این الگوها که به آن Virus Signature گفته می شود، از ورود آن به کامپیوتر شما و اجرا شدن جلوگیری می کنند و یا به شما هشدار لازم را می دهند و از شما دستور میگیرند که آیا فایل را حذف کنند و یا سعی در اصلاح آن نمایند. شرکتهای سازنده آنتی ویروس با آمدن ویروسهای جدید، الگوهای نرم افزاری آنها را کشف و جمع آوری می کنند و به همین علت اغلب لازم است تا این نرم افزارها هر چندگاهی به روز (Update) شوند تا الگوهای جدید ویروسها را بشناسند. ویروسها باهوش هستند روشهای بسیاری وجود دارد که توسط آن برنامه های مختلفی که حامل ویروس هستند، نظاره گر رفتار کامپیوتر شما میشوند. شما در حال نگاه کردن به یک فیلم روی اینترنت هستید، یا در حال خواندن یک نامه و بسیاری کارهای عادی دیگر ... و بدون آنکه بدانید در همان زمان شما به ویروسی اجازه دادید تا کامپیوتر شما را بررسی و تحلیل کند. بسیاری از اوقات هنگامی که شما آنها را شناسایی می کنید و از بین می برید، خبر ندارید که ویروس برای ورود مجدد و فعال شدن در کامپیوتر شما قبلا "چاره لازم را اندیشیده است و راه های دیگری (Backdrs) برای حمله مجدد به کامپیوتر یا شبکه شما ایجاد کرده است. ویروسها چگونه وارد کامپیوتر شما می شوند راه های مختلفی برای رسیدن ویروس ها به کامپیوتر شما وجود دارد، مانند فلاپی دیسک، CD، مشاهده وب سایت، email، اجرای فایل های dwnlad شده و ... بنابراین لازم است که تمامی این موارد به هنگام استفاده مورد کنترل یک AV قرار گیرد. به بیان دیگر هنگامی که میخواهید برنامه ای را از روی یک CD را اجرا کنید و یا email ای را باز کنید باید آنها را توسط یک AV کنترل کنید. فراموش نکنید که شما همواره مراقب منزل خود هستید و دقت می کنید که درب

منزل و پنجره ها هنگام شب یا هنگامی که در منزل نیستید باز نباشند. به همین ترتیب باید همواره وضعیت قسمت های مختلف کامپیوتر خود را کنترل کنید. اینکه اندازه فایلهای شما عادی باشد یا نه، اینکه مثلا "فایل جدیدی به کامپیوتر شما اضافه نشده باشد و بسیاری موارد دیگر که بتدریج می توانید آنها را یاد بگیرید. اما یک AV بسادگی می تواند هر موقع که شما اراده کنید تمام سیستم شما را کنترل کند و شما را از عدم وجود ویروس در کامپیوتر مطمئن سازد. DURCH تست یک نرم افزار مناسب AV معمولا "باید بتواند به نیازهای زیر پاسخ دهد : ۱- تست Demand : باید بتواند هنگامی که می خواهید به یک فایل یا صفحه اینترنتی یا یک mail دسترسی داشته باشید، آنرا کنترل کند. ۲- تست Update : به این معنی که AV باید بتواند در بازه های زمانی مشخص بانک اطلاعاتی خود که شامل الگوهای (Signatures) ویروس ها است را بروز کند. ۳- تست Respnd : اینکه نرم افزار آنتی ویروس بتواند تمامی رفتارهای منطقی در برخورد با یک ویروس را از خود نشان دهد. فایل کثیف را دوباره سازی و تمیز کند و یا آنرا حذف نماید. ۴- تست Check : باید بتواند تمام فایلها از نوع مختلف را که میتوانند محلی برای پنهان شدن ویروس باشند را کنترل کند. ۵- تست Heuristics : به این معنی که نرم افزار AV شما باید با وجود نداشتن الگوی همه ویروسها، بتواند تشخیص خطر دهد و به شما هشدار دهد که" با وجود آنکه مطمئن نیستم اما احتمالآ مسئله مشکوکی در کامپیوتر شما وجود دارد ".این کنترل نیاز به آن دارد که نرم افزار AV از هوش بالایی برخوردار باشد.

با کاربرد فایروال آشنا شویم

Firewall دستگاهی است در درون شبکه یک شرکت قرار می گیرد و شبکه را از محیط اینترنت و یا دسترسی های بیرونی ایزوله می کند. فایروال با کنترل دسترسی ها به شبکه، به برخی از درخواستها اجازه ورود به شبکه را داده و مانع ورود برخی دیگر درخواستها می شود. معمولآ- برنامه ریزی و سیاستگذاری یک فایروال اینگونه است که کلیه دسترسی ها از بیرون به داخل شبکه شرکت از محیطی عبور می کند که کاملآ- در حال کنترل و مونیتور کردن است. این موضوع دقیقآ همانند قسمتی است که شما هنگام ورود به یک ساختمان مهم باید از آن عبور کنید که در آن نیروهای امنیتی شما را بازرسی بدنی می کنند و یا شما را از X-Ray عبور می دهند. اما از آنجایی که فایروالها اغلب به دلیل انجام تنظیمات نادرست خوب عمل نمی کنند، امروزه بسیاری از مدیران شرکت ها به آنها اعتماد ندارند و عملکرد مثبت آنها به هنگام بروز خطر یا حمله یک هکر را پنجاه پنجاه می دانند. بعنوان مثال همانطور که می دانید یکی از مهمترین منابع حملات شبکه ای از ناحیه کارکنان ناراضی شرکت ها است، این در حالی است که فایروال ها معمولآ طوری تنظیم می شوند که مراقبت شبکه را از تهدیدهای بیرونی به عهده بگیرند. بنابراین یکی از مهمترین مواردی که مدیران یک سازمان باید آنرا خوب درک کنند آن است که بدانند فایروالی که در شبکه شرکت نصب شده است چه محدوده ای راه پوشش امنیتی می دهد. همچنین مدیران شرکت ها باید بدانند که فایروال دستگاهی است که در کنار سایر سیستم های امنیتی داخلی و خارجی می تواند بر استحکام امنیتی شبکه شما بیفزاید. در این حالت وب سرور در درون شبکه قرار دارد و امنیت شبکه بطور کامل توسط فایروال کنترل می شود اما ضعف وب سرور می تواند محل نفوذ هکرها باشد. یک مقال کاربردی بسیاری از شرکت های امروز دارای وب سرور هایی هستند که اطلاعات مورد نظر خود را از طریق آن در اختیار کارکنان و یا مشتریان خود قرار میدهند. خب چنانچه شبکه شما از نعمت وجود یک فایروال برخوردار باشد بنظر شما وب سرور را باید در کجای شبکه قرار داد. ۱ - بیرون فایروال انتخاب اول آن است که وب سرور را خارج از فایروال قرار دهید. در این حالت بنظر می رسد که شما سرور خود را مستقیمآ بدون هیچ سیستم امنیتی روی اینترنت قرار داده اید. این محل برای وب سرور شما خطرناک است اما شاید تعجب کنید اگر بدانید که می تواند مفید هم باشد. چرا؟ در این حالت چنانچه یکی از سارقین یا هکرهای اینترنتی بتواند از ضعف وب سرور شما استفاده کند و بخواهد وارد شبکه شما شود با دیواری بنام فایروال برخورد می کند. اما دقت کنید

که این حالت برای شبکه شما امنیت بیشتری دارد. ۲ – درون فایروال و تحت حمایت آن در این حالت شما وب سرور شرکت را در درون محدوده امنیتی فایروال یعنی شبکه شرکت قرار داده اید. لذا باید به فایروال بگویید که برای درخواست کنندگان سرویس وب، پروتکل http را اجازه عبور دهد و نه چیز دیگر. در این حالت وب سرور شما قاعدتآ باید فقط به سرویس های درخواست صفحات وب پاسخ بدهد اما چنانچه هکری بتواند به نحوی به داخل این سرور رسوخ کند، به احتمال زیاد خواهد توانست از طریق پورت های مختلف وب سرور شما به قسمت های مختلف شبکه دسترسی پیدا کند. بخصوص اگر وب سرور شما برای اجرای برنامه ها مانند برنامه های CGI آماده باشد. در اینجا ترکیبی از دو حالت قبل را داریم و شبکه و وب سرور در محدوده کنترل امنیتی دو فایروال قرار دارند ۳ – میان دو فایروال این حالت ترکیبی است از دو موردی که تا کنون راجع به آن صحبت کردیم. به شکل نگاه کنید کاملآ واضح است که در این حالت هم شبکه و هم وب سرور از امنیت لازم که توسط فایروالها بوجود می آید بهره خواهند برد.

روزگاری اینترنت قابل اعتماد بود!

اولین نقطه برای شروع به ایمن کردن کامپیوتر خود آن است که درک درستی از اینترنت و نحوه کار آن داشته باشید. چرا که اگر بدانید اینترنت چگونه کار میکند به سادگی می توانید راه حل های امنیتی را ارزیابی کرده، انتخاب و اجرا کنید. اساس بنیان اینترنت بر اعتماد بود ما معمولا "به چشمان خود خیلی اعتماد داریم، وقایعی را که می بینیم به مراتب بیش از آنچه می شنویم برای ما ارزش و اعتبار دارد. همچنین وقتی نوشته های روی یک بسته دارو را می خوانیم به آن اعتماد می کنیم، به حرفهای پدر و مادر اعتماد داریم و ... چرا؟ برای آنکه همه مواردی را که برشماردیم دارای پشتوانه قابل قبول و معتبر هستند. اما هرگز به نوشته های دست خط روی یک کاغذ اهمیت خاصی نمی دهیم چرا که ممکن است هر فردی آنرا تهیه کرده باشد. اگر به سالهای ۱۹۶۰ برگردیم، هنگامی که کامپیوتر ها بسیار گرانقیمت و البته کند بودند، متوجه می شویم که در آن دوران، برخلاف وجود این دو عیب به ظاهر بزرگ، کاربرد کامپیوترها و شبکه های کامپیوتری بسیار درست و بجا بود و نیز به دلیل گرانی قیمت، این ابزار در دست دولت، سازمانها و شرکت های معتبر و بزرگ بود. اما شما بهتر از ما می دانید که امروز دیگر اینگونه نیست. یک مثال آیا این تا بحال برای شما اتفاق افتاده که پست چی نامه ای را برای شما بیاورد و محتویات آن چیزی نباشد که با توجه به نام و آدرس فرستنده روی پاکت شما انتظار دارید؟ به احتمال زیاد اینگونه نبوده است؟ چرا که جابجایی نامه های پستی در انحصار شرکت های معتبر است و نیز ارسال آنها بعنوان Spam هزینه و دردسر بسیار دارد و ارسال کننده به سختی و با هزینه قابل توجه میتواند بعنوان دوست و آشنا برای شما نامه ارسال کند و داخل آن اطلاعات مورد نظر خود را قرار دهد. لذا عملا "ارزش انجام اینکار وجود ندارد. اما همانطور که احتمالا- "تابحال متوجه شدید در اینترنت اینگونه نیست. امروزه دسترسی به اینترنت و داشتن سایت یا سرورهای ارسال و دریافت email با هزینه اندک قابل تهیه است. لذا هر شخصی می تواند به تنهایی توانایی هایی را که روزی در انحصار شرکت های بزرگ و معتبر بود داشته باشد و در عرض کمتر از چند دقیقه هزاران نفر را مورد تعرض اطلاعاتی قرار دهد. علاوه بر آن بسیاری از متخصصان اینترنت با استفاده از ضعف تکنولوژی های اینترنت میتوانند بهنگام تبادل بسته های اطلاعات در اینترنت در آنها تغییراتی دهند که در نهایت باعث رسیدن اطلاعت غلط – و مورد علاقه تغییر دهند – به دست مشتری خواهد شد. بنابراین همانگونه که توجه میکنید بستر تبادل اطلاعات اینترنت که روزی بر پایه اعتماد درست شده بود امروزه قابل اعتماد نیست.

دیدار با یک Link Spammer

Link Spammeer به افرادی گفته می شود که بدون اجازه با قرار دادن لینک در سایت دیگران مانند نوشتن توضیح

(Cmment) در وبلاگ ها و یا با هر روشی که بتوانند به توزیع لینک های سایتهای مشتریان خود – که اغلب نا مربوط و بی خاصیت هستند – در اینترنت فعالیت میکنند. سم (Sam) یکی از این افرا است که در یک آپارتمان نسبتا "بزرگ در شهر لندن زندگی می کند و تقریبا "در تمام طول شبانه روز کارش همین است که گفتیم. در ابتدا بنظر می رسید که اینکار را برای تفریح انجام می دهد اما پس از کمی صحبت متوجه شدیم که موضوع به این سادگی ها هم نیست. او یک برنامه نویس حرفه ای در زمینه LWP ، Perl و PHP هست که اولین کار خود را در ۱۳ سالگی، که یک قسمت از برنامه ای برای یک شرکت تولید کننده بازی های کامپیوتری بود نوشت. او هم اکنون ۳۲ سال دارد و بصورت حرفه ای به کار Link Spamming مشغول است. خب برای چه و چگونه اینکار را انجام می دهی؟ آیا کار تو شبیه به email spammer ها هست؟ دسامبر سال ۲۰۰۳ بود که گوگل در سیستم خود تغییراتی داد که به Flrida Update معروف شد. گوگل الگوریتم ارزیاب سایتها و صفحات اینترنتی را تغییر داد، تا شاید بتواند از اینکه سایت های فامیل یا حتی آنها که پول بیشتر دارند همدیگر را تقویت کنند جلوگیری کند. بنابراین اگر شما یک مجموعه بزرگ از لینک ها داشتید (Link Farm) که مقصد آنها هم به اعضای همین مجموعه لینک داشت، گوگل شما را محکوم می کرد و امتیاز سایت شما را پایین می آورد و حتی ممکن بود شما را از بانک اطلاعاتی خود بیرون بیندازد. لذا ما Link Spammer ها که قبلا "نام بهتری به ما اطلاق می شد – یعنی Search Engine ptimiser – باید راه حلی برای بالا بردن امتیاز و Rank مشتری های خود پیدا می کردیم. گوگل علاقه زیادی به وبلاگها دارد چرا که محتوی آنها خیلی سریع عوض می شود. خب چه جایی بهتر از اینجا برای معرفی و دادن لینک به سایت های مشتری های ما. البته Cmment Spamming قبل از آپدیت فلوریدا هم وجود داشت اما بعد از آن بعنوان یک راهکار اساس برای ما SE ها مطرح شد. تجربه من نشان می دهد که فتو بلاگها اهداف بهتری هستند چرا که مشتریان بیشتری دارند و معمولا "همه می توانند آنجا Cmment بگذارند. حقیقت موضوع را هم بخواهید برنامه نویسی آن کار دشواری نیست و بسادگی با ابزارهایی که هست می توان برنامه ساده ای برای اینکار نوشت، پس از آن احتیاج به یک لیست از وبلاگ ها داریم، که با یک جستجو روی لغاتی مانند Wrdpress یا Mvable Type یا Blger می توانی هزارها نام وبلاگ و سایت پیدا کنی. آنها صلاحیت زیادی دارند افرادی مانند سم زیاد هستند و باید گفت خیلی بالاتر از یک Link Spammer هستند. او می گوید : وقتی یک سیستم مدیریت محتوای (CMS) جدید به بازار ارائه می شود و مردم شروع به استفاده از آن می کنند، کمتر از یکساعت طول می کشد که بتوان سیستمی نوشت که در آن بطور خودکار Cmment بگذارد. چیزی حدود ۲۰۰ خط Script برای اینکار کافی است. نکته مهم آن است که آنرا نباید با PC خودتان انجام دهید چرا که به احتمال زیاد ISP شما متوجه خواهد شد و سرویستان را محدود و یا حتی قطع خواهد کرد. حتی اگر ISP شما متوجه نشود، اگر آدرس IP شما ثابت باشد، به احتمال زیاد صاحب سایت یا وبلاگ IP شما را بلاک میکند و جلوی قرار دادن کامنت را میگیرد. بنابراین باید از صدها هزار پراکسی های آزادی (pen Prxies) که در اینترنت هست استفاده کرد. جالب هست که بسیاری از این پراکسی ها برای استفاده شرکتهای مختلف از اینترنت درست شده اند که بخاطر تنظیمات غلط – که احتمالا "برای آنها سخت هم هست – معمولا "همه می توانند از آنها استفاده کنند! من شخصا "از حدود ۲۰۰ ؛ ۳۰۰ پراکسی برای نوشتن Cmment در سایت ها یا وبلاگ ها استفاده می کنم. معمولا "هم سعی می کنم آنها را در نوشته های آخر قرار ندهم چرا که صاحب سایت زودتر و راحتتر متوجه می شود. دقت کنید برای من مهم آن است که گوگل لینک به سایت مشتری من را در صفحه یک سایت دیگر ببیند. همین و بس، بخصوص که صفحات جدید هنوز توسط گوگل ایندکس نشده است. اما مهمترین دلیل سم برای انجام اینکار : شاید باور نکنید اما این سایت هایی که من برایشان کار میکنم هرکدام بین ۱۰۰ تا ۲۰۰ هزار پوند در ماه درآمد دارند، که جزئی از این درآمد آنها نصیب من می شود. این مهمترین دلیلی است که من اینکار را انجام میدهم. چرا بجای اینکار مشتریهای تو نمیخواهند به گوگل رسما "آگهی بدهند؟ تجربه من و بسیاری از محققان رفتار اینترت شناسی نشان می

دهد که این روش یعنی رسیدن به هدف از طریق مسیرهای طبیعی - یعنی نه از یکجا مثلا- "گوگل - بیش از شش برابر بازده بیشتری داره نسبت به همان هزینه ای که برای گوگل یا هر جستجوگر دیگه ای میکنید. پرداخت بر اساس کلیک که اغلب جستجوگرها اینگونه محاسبه می کنند بسیار هزینه بر هست. اما مسائل اخلاقی چطور؟ شما از فضا ، منابع و پهنای باند مردم استفاده میکنید؟ تا هنگامی که قانونی برای منع اینکار نباشد انجام می دهیم. چرا که بنظر من وقتی صاحب یک سایت برای نوشته های خود اجازه قرار دادن Cmment را میگذارد، ما می توانیم برویم و آنجا Cmment بگذاریم.

به امنیت شبکه خود فکر می کنید؟

کمی فکر کنید ! در محدوده فعالیت های شخصی شما باید به کامپیوتر خود به چشم منزل یا آپارتمانی که در آن زندگی میکنید نگاه کنید. تمامی فعالیت هایی را که بصورت عادت برای ایمن نگاه داشتن و حفظ کردن منزل انجام می دهید را مرور کنید. کامپیوتر منزل شما و فایلها و اطلاعات داخل آن همانند خانه و اسباب زندگی شما است. برخی از آنها گران قیمت و با ارزش و برخی کم ارزش تر هستند. شما هنگام خروج از منزل درب ها و پنجره ها را می بندید و آنها را قفل می کنید. حتی اگر لوازم گران قیمت و یا اسناد مهم داشته باشید آنها را درون یک گاوصندوق قرار می دهید یا حتی برای منزل خود سیستم امنیتی مانند دزدگیر نصب می کنید. اگر بیشتر فکر کنید متوجه می شود که موضوع کمی مهمتر از موارد مطرح شده در بالا- است. بعنوان یک مثال، شما خوب می دانید که اگر کنار پنجره بلند صحبت کنید یقینا "ممکن است کسی که در بیرون منزل ایستاده و یا یکی از همسایه ها صحبت های شما را گوش کند. یا حتی هنگامی که همه خانواده در منزل هستند و می خواهید صحبت خصوصی با دوستان داشته باشید درب اطاق را می بندید و آرام با تلفن صحبت میکنید. حتی ممکن است برای جلوگیری از شنود مکالمه توسط دیگران یک خط تلفن برای خود جداگانه تهیه کنید! پس چرا؟ بله، پس چرا وقتی در منزل اینگونه رفتار می کنید و مراقب بسیاری از موارد امنیتی هستید کامپیوتر منزل خود را بی خیال رها می کنید و بدون فکر به کمک آن با دوستان چت می کنید یا تبادل email و ... انجام می دهید و خرید اینترنتی میکنید ؟ آیا هیچ فکر کردید که ممکن است افرادی نه در خانه شما بلکه در نقاط دوری از دنیا در کمین باشند تا از اطلاعات شما استفاده کنند؟ چرا برای درب منزل خود سه قفل ایمنی و یک سیستم دزدگیر تهیه می کنید اما برای برنامه های مهم رمز های ساده ای چون hell، ۱۲۳، test و ... انتخاب می کنید؟ آیا می دانید این رمزها و بسیار رمزهای مشکل تر از این موارد، بسادگی قابل حدث زدن می باشند؟ چرا اصولا "علاقه ای به به روز رسانی Patch ها یا Service Pack های نرم افزارهای مختلف روی کامپیوتر خود ندارید؟ و یا هر بار که S از شما تقاضا می کند که آیا مایل هستید آخرین تغییرات S را dwnlad کنید، آنرا cancel می کنید؟ این موضوع وقتی مهمتر می شود که شما بجای یک کامپیوتر یک شبکه داشته باشید، در آنصورت باید بیشتر فکر کنید و حتی از مشاورین متخصص یا و شرکت های با تجربه برای حل مشکلات امنیتی شبکه خود یا شرکت خود استفاده کنید.

Intruder – میهمانان ناخوانده علاقمند به کامپیوتر شما

ممکن است هم اکنون میهمانی ناخوانده در کامپیوتر شما حضور داشته باشد! Intruders، این اصطلاح به مزاحمین و افرادی گفته می شود که بدون اجازه و یا به حالت سر زده وارد منزل مردم می شوند. امروزه تعداد زیادی از این افراد وجود دارند که بدون اجازه خیال ورود به کامپیوترهای متصل به شبکه را دارند. اما چرا؟ برای آنکه این ا فراد می خواهند از چیزهایی که شما در کامپیوتر خود ذخیر کرده اید استفاده کنند. آنها به دنبال شماره کردیت کارت (Cerdit Card Number)، اطلاعات و شماره حساب بانکی و ... خلاصه هر آنچه که ممکن است شما در کامپیوتر خود ذخیره کرده باشید هستند. Intruder ها با سرقت این

اطلاعات می توانند بجای شما از آنها استفاده کنند. اما موضوع فقط به پول ختم نمی شود، آنها ممکن است حتی از هارد دیسک شما برای نگهداری و ذخیره اطلاعات خود استفاده کنند و یا از پردازشگر قوی کامپیوتر شما! شاید باور نکنید ولی اگر ارتباط پرسرعت با اینترنت داشته باشید آنها از آن برای dwnlad کردن اطلاعات مورد نظر خود استفاده می کنند و یا کامپیوتر شما را بازیچه ای برای حمله به سایر کامپیوتر های موجود در اینترنت قرار می دهند. دقت کنید که هرچقدر آنها از تعداد بیشتری کامپیوتر برای حمله – مثلا- "به یک بانک – استفاده کنند، کشف حمله و یا حتی پیدا کردن خاطی برای ماموران قانونی بسیار دشوارتر و سخت تر خواهد بود. اما چرا Intruder ها به به کامپیوترهای خانگی علاقه نشان می دهند؟ دلیل آن بسیار ساده است، چرا که کامپیوترهای خانگی معمولا "دارای سیستم های حفاظتی محکم نیستند و بسادگی قابل دسترسی آنها می باشند. بخصوص هنگامی که شما دسترسی به اینترنت پر سرعت داشته باشید و کامپیوتر شما همواره روشن باشد، دیگر وقت آنها را تلف نیز نخواهید کرد. حملات این میهمانان سرزده معمولا "با موفقیت توام است، چرا که تقریبا "تمام صاحبان کامپیوترهای خانگی از لزوم ایمن کردن کامپیوتر خود با خبر نیستند. آنها اینگونه فکر می کنند که چون کامپیوتر در خانه است پس کسی نمی تواند آنرا سرقت کند یا مورد سوء استفاده قرار دهد. در صورتی که اتصال کامپیوتر به اینترنت بدون رعایت موارد امنیتی مانند آن است که شما درب و پنجره منزل خود را همواره باز بگذارید. اما یک میهمان ناخوانده (Intruder) چگونه وارد کامپیوتر شما می شود؟ معمولا "آنها با ارسال یک email حاوی ویروس ماجرا آغاز می شود. شما با خواندن این نامه ویروس را در کامپیوتر خود فعال می کنید و درب آنرا به روی میهنمان ناخوانده باز می کنید. در موارد دیگر آنها ممکن است از ضعف سایر برنامه هایی که مورد اطمینان شما هستند استفاده کنند مانند مرورگر اینترنت، یا نرم افزار چت و ... در هر صورت موضوع آن است که آقای Intruder برای اولین بار به طریقی وارد کامپیوتر شود. پس از آن یک یا چند نرم افزار را بصورت مخفیانه در کامپیوتر شما نصب می کند تا به این وسیله به او امکان استفاده از منابع کامپیوتر شما را بدهد. حتی پس از آنکه احیانا "شما متوجه حضور این میهمان شوید و راه های ورودی او را ببندید، Intruder باز هم مسیرهایی را برای ورود خود به کامپیوتر شما از پیش درست کرده اند تا در مواقع لزوم از آن استفاده کنند. به این مسیر ها اغلب درب های پشتی یا Backdrs گفته می شود. فراموش نکنید که مهمترین شرط داشتن امنیت در شبکه – یا حتی در دنیای واقعی – آن است که بدانیم به چه برنامه، email، سایت و ... – و یا چه افرادی – اطمینان کنیم.

چگونه دو رایانه را به یکدیگر متصل کنیم؟

با آمدن رایانه های جدید افراد بسیاری تمایل به خرید آنها پیدا می کنند پس از خرید یک رایانه جدید و سریعتر مدل قدیمی رایانه در گوشه ای انداخته میشود .بعضی از اشخاص از رایانه های لپ تاپ استفاده می کنند و می خواهند آن را با رایانه شخصی شبکه کنند . وصل کردن دو رایانه به هم از ساده ترین مباحث شبکه به حساب می آید . پس از ساخت شبکه علاوه بر امکان انتقال اطلاعات از این طریق شما می توانید از یک امکان لذت بخش دیگر نیز استفاده کنید .با شبکه شدن دو رایانه شما می توانید بازیهای مختلفی را تحت شبکه خانگی خودتان بازی کنید و از آن لذت ببرید . برای شبکه کردن دو رایانه شما احتیاج به سخت افزار شبکه روی هر دو سیستم و به مقدار لازم کابل شبکه دارید. بساری از مادربورد های جدید خودشان دارای پورت شبکه هستند .اما اگر مادربورد شما دارای سخت افزار شبکه نیست باید کارت شبکه را برای هر دو سیستم تهیه کنید انواع معمولی کارت های شبکه قیمت های بسیار مناسبی دارندو در تمام فروشگاهها نیز پیدا می شوند .به جز کارت شبکه شما باید به اندازه فاصله دو رایانه کابل شبکه خریداری کنید در موقع خرید اری کابل شبکه باید حتما به فروشنده گوشزد کنید که کابل را برای اتصال تنها دو رایانه می خواهید. این مساله باعث می شود که فروشنده برای نصب فیشهای دو سر کابل رشته های آن را به نحو خاصی که مخصوص اتصال دو رایانه است دو رایانه است مرتب کند . حتما می دانید برای شبکه کردن بیش از دو رایانه احتیاج به سخت

افزارهـای دیگری مثل سیسـتم ارتباط مرکزی یا هاب HUB نیاز می باشـد .نحوه چیده شدن رشـته های کابل شـبکه برای اتصال به HAB و شـبکه کردن بیش از دو رایانه متفاوت می باشد. پس از خرید این وسایل حالا باید شـما کارتهای شـبکه را روی سیستم ها نصب کنید این کارتها معمولا با استفاده از درایورهای خودشان به راحتی نصب می شوند بعد از نصب کارت های شبکه در قسمت Netwrk Cnnectins ویندوز شـما گزینه ای با عنوان Lcal Area Cnnectins اضـافه می شود حالا کابل را به کارت های شبکه دو رایانه وصل کنیـد و هر دو رایانه را تحت ویـنـدوز XP روشن نماییـد .در این مرحله برای درست کردن شـبکه روی گزینه MY Cmputer هر دو رایـانه کلیک راست کرده و گزینه Prperties را انتخاب نمایید .حالا به قسـمت Cmputer Name بروید هر دو رایانه باید دارای Wrkgrup یکسـانی باشـند .برای یکسان کردن آنها روی گزینه Change کلیک کرده و سپس اسـمی را برای Wrkgrup هر دو رایـانه وارد نماییـد.حتما دقت نماییـد که Cmputer Name هـای هر دو رایانه بایـد متفاوت باشـد . حالاـ روی هر دو رایـانه بـه قسـمت Netwrk Cnnectins برویـد و روی Lcal Area Cnnectins کلیک کنیـد و Prperties را انتخاب کنیـد و در پنجره باز شده دنبال خطی با عنوان Prtcl TCP/internet بگردید این خط را انتخاب نموده و روی گزینه Prperties کلیک نمایید معمولاگزینه btain Autmatically an ip Address به عنوان پیش فرض انتخاب شده است .شـما گزینه Use The Fllwing ip Address را انتخاب کنیـد ، در قسـمت ip Address یکی از رایـانه IP را ۱۹۲.۱۶۸.۰.۱ و در رایـانه دیگر ۱۹۲.۱۶۸.۰.۲ وارد نموده ، در قسـمت Subnet Mask هر دو رایانه این مقـدار را وارد نماییـد : ۲۵۵.۲۵۵.۲۵۵.۰ حالا دیگر کار شـبکه شـدن رایانه ها تمام شـده است هر دو رایانه را برای اطمینان مجـددا راه اندازی کنید . به یاد داشـته باشـید که درایو ها و پوشه هایی را که می خواهید در هر رایانه روی شـبکه قرار بگیرد را باید Share کنید برای این کار : روی درایو ها و پوشه ها کلیک راست کرده و گزینه Prperties را انتخاب کنید در قسمت Sharing این پنجره شما باید گزینه share this flder را انتخاب کنید .

آشنائی با انواع اتصال کامپیوتر ها در شبکه

ارایش و نحوه بهم پیوستن وسایل مختلف شبکه را Tplgy می گویند. سه نوع توپولوژی اصلی وجود دارد : Bus گذرگاه Star ستاره Ring حلقه Bus توپولوژی گـذرگاه این توپولوژی شامـل یـک خط ارتباطی که به صورت یک خط مرتب می شود و همه گره ها به یک خط ارتباطی وصل می شوند این شـبکه دوسـر آزاد و متمایز دارد همه گره ها دستیابی یکسانی بر شـبکه دارند وقتی یک پیام بخواهـد بین دوگره حرکت کند تمام گره های موجود در شـبکه پیام را می خوانند تا ببینند که پیام مربوط به آنهاست یا نه این پیـام به کـامپیوتر مورد نظر که رسـید آن را گرفته و پردازش می کنـد در حالیکه سایر گره ها آن را نادیـده می گیرنـد در یک شبکه کوچـک اینروش به خـوبی کـار می کنـد ولی در شـبکه هـای بزرگ که مسیرهای طولاـنی نیز دارد این روش جـواب خوبی نمیدهد و قطع شدن کابل در هر نقطه از شـبکه باعث از کار افتادن کل شـبکه می شود Ring توپولوژی حلقه این توپولوژی شکل یک دایره را به خود می گیرد هر گره با گره بعـدی خود وابسـته است پیامهای ارسالی از هر گره در طول حلقه می چرخد تا به گره مورد نظر برسـد پیام فقط در یک جهت حرکت می کنـد. روی توپولوژی حلقه شـبکه های Peer t peer خوب کار می کننـد. با توجه به اینکه گره مسـتقیمآ به گره کناری خود وصل می شود اگر یک کامپیوتر از کار بیفتـد کل شـبکه نیز از کار می افتـد. تعداد گرههای هر حلقه معمولاًمحدود است توسعه این شبکه محدود بوده و برای افزایش یک گره به شبکه باید کل شبکه از کار انداخته شود. Star توپولوژی ستاره توپولوژی شکل ستاره به خود می گیرد هر گره با یک گره مرکزی وابسته است پیامهای ارسالی از هر گره توسط یک گره مرکزی به گره مورد نظر می رسد

آموزش کلیات امنیت شبکه

آموزش کلیات امنیت شبکه وقتی بحث امنیت شبکه پیش می اید ، مباحث زیادی قابل طرح و ارائه هستند ، موضوعاتی که هر کدام به تنهایی می توانند جالب ، پرمحتوا و قابل درک باشند ، اما وقتی صحبت کار عملی به میان می اید ، قضیه یک جورایی پیچیده می شود . ترکیب علم و عمل ، احتیاج به تجربه دارد و نهایت هدف یک علم هم ، به کار امدن ان هست . وقتی دوره تئوری امنیت شبکه را با موفقیت پشت سر گذاشتید و وارد محیط کار شدید ، ممکن است این سوال برایتان مطرح شود که "" خب ، حالا از کجا شروع کنم ؟ اول کجا را ایمن کنم ؟ چه استراتژی را پیش بگیرم و کجا کار را تمام کنم "" ؟ انبوهی از این قبیل سوالات فکر شما را مشغول می کند و کم کم حس می کنید که تجربه کافی ندارید و این البته حسی طبیعی هست . پس اگر این حس رو دارید و می خواهید یک استراتژی علمی - کاربردی داشته باشید ، تا انتهای این مقاله با من باشید تا قدم به قدم شما رو به امنیت بیشتر نزدیک کنم. همیشه در امنیت شبکه موضوع لایه های دفاعی ، موضوع داغی هست و نظرات مختلفی وجود دارد . عده ای فایروال را اولین لایه دفاعی می دانند ، بعضی ها هم Access List رو اولین لایه دفاعی می دانند ، اما واقعیت پنهان این هست که هیچکدام از اینها ، اولین لایه دفاعی نیستند . یادتون باشد که اولین لایه دفاعی در امنیت شبکه و حتی امنیت فیزیکی ، Plicy هست . بدون plicy ، لیست کنترل ، فایروال و هر لایه دیگر ، بدون معنی می شود و اگر بدون plicy شروع به ایمن کردن شبکه کنید ، محصول یک آبکش واقعی از کار در می اید . با این مقدمه ، و با توجه به این که شما plicy مورد نظرتان را کاملا تجزیه و تحلیل کردید و دقیقا می دانید که چه چیزی رو می خواهید و چی را احتیاج ندارید ، کار را شروع می کنیم . ما باید پنج مرحله رو پشت سر بگذاریم تا کارمان تمام بشود . این پنج مرحله عبارتند از : ۱- Inspectin (بازرسی) ۲- Prtectin (حفاظت) ۳- Detectin (ردیابی) ۴- Reactin (واکنش) ۵- Reflectin (بازتاب) در طول مسیر ، از این پنج مرحله عبور می کنیم ، ضمن اینکه ایمن کردن شبکه به این شکل ، احتیاج به تیم امنیتی دارد و یک نفر به تنهایی نمی تواند این پروسه رو طی کند و اگر هم بتواند ، خیلی طولانی می شود و قانون حداقل زمان ممکن را نقض می کند . ۱- اولین جایی که ایمن کردن رو شروع می کنیم ، ایمن کردن کلیه authenticatin های موجود هست . معمولا رایج ترین روش authenticatin که مورد استفاده قرار می گیرد ، استفاده از شناسه کاربری و کلمه رمز هست. مهمترین جاهایی که باید authenticatin را ایمن و محکم کرد عبارتند از : - کلمات عبور کاربران ، به ویژه مدیران سیستم . - کلمات عبور سوییچ و روتر ها (من روی سوییچ خیلی تاکید میکنم ، چون این device به صورت plug and play کار می کند ، اکثر مدیرهای شبکه از cnfig کردن ان غافل می شوند ، در حالی که می تواند امنیت خیلی خوبی به شبکه بدهد ، به مدیران امنیتی توصیه میکنم که حتما این device رو کنترل کنند) . - کلمات عبور مربوط به SNMP . - کلمات عبور مربوط به پرینت سرور . - کلمات عبور مربوط به محافظ صفحه نمایش . آنچه که شما در کلاسهای امنیت شبکه در مورد Accunt and Passwrd Security یاد گرفتید را اینجا به کار می برید . که من به خاطر طولانی نشدن بحث به انها اشاره نمیکنم . ۲- قدم دوم نصب و به روز کردن آنتی ویروس بر روی همه دسکتاپ ، سرور و میل سرورها هست . ضمن اینکه آنتی ویروس های مربوط به کاربران باید به طور اتوماتیک به روز رسانی بشود و آموزشهای لازم در مورد فایلهای ضمیمه ایمیل ها و راهنمایی لازم جهت اقدام صحیح در صورت مشاهده موارد مشکوک یا اضطراری به کاربران هم داده بشود . ۳ - مرحله سوم شامل نصب آخرین به روز رسانی های امنیتی سیستم عامل و سرویسهای موجود هست . در این مرحله علاوه بر کارهای ذکر شده ، کلیه سرورها و device ها و دسک تاپ ها با ابزار های شناسایی حفره های امنیتی بررسی می شوند تا علاوه بر شناسایی و رفع حفره های امنیتی ، سرویس های غیر ضروری هم شناسایی و غیرفعال بشوند . ۴-در این مرحله نوبت گروه بندی کاربران و اعطای مجوزهای لازم به فایلها و دایرکتوری ها میباشد . ضمن اینکه accunt های قدیمی هم باید غیر فعال شوند . گروه بندی و اعطای مجوز بر اساس یکی از سه مدل استاندارد Access Cntrl Techniques یعنی DAC , MAC یا

RBAC انجام می شود . بعد از پایان این مرحله ، یک بار دیگه امنیت سیستم عامل باید چک بشود تا چیزی فراموش نشده باشد . ۵- حالا نوبت device ها هست که معمولا شامل روتر ، سوییچ و فایروال می شود . بر اساس plicy موجود و توپولوژی شبکه ، این bx ها باید cnfig بشوند . تکنولوژی هایی مثل NAT , PAT و filtering و غیره در این مرحله مطرح می شود و بر همین اساس این مرحله خیلی مهم هست. حتی موضوع مهم IP Addressing که از وظایف مدیران شبکه هست می تواند مورد توجه قرار بگیرد تا اطمینان حاصل بشود که از حداقل ممکن برای IP Assign به شبکه ها استفاده شده است. ۶- قدم بعد تعیین استراژی backup گیری هست . نکته مهم که اینجا وجود دارد این هست که باید مطمئن بشویم که سیستم backup گیری و بازیابی به درستی کار می کند و بهترین حالت ممکن باشد . ۷- امنیت فیزیکی . اول از همه به سراغ UPS ها می رویم . باید چک کنیم که UPS ها قدرت لازم رو برای تامین نیروی الکتریکی لازم جهت کار کرد صحیح سخت افزار های اتاق سرور در زمان اضطراری رو داشته باشند . نکات بعدی شامل کنترل درجه حرارت و میزان رطوبت هست. همینطور ایمنی در برابر سرقت و آتش سوزی. سیستم کنترل حریق باید به شکلی باشد که به نیروی انسانی و سیستم های الکترونیکی آسیب وارد نکند . به طور کل آنچه که در مورد امنیت فیزیکی یاد گرفتید را در این مرحله به کار می برید . ۸- امنیت وب سرور یکی از موضوعاتی هست که روش باید وسواس داشته باشید. به همین دلیل در این قسمت کار ، مجددا و با دقت بیشتر وب سرور رو چک و ایمن می کنیم . در حقیقت ، امنیت وب رو اینجا لحاظ می کنیم . (اسکریپت های سمت سرویس دهنده رو هیچ وقت فراموش نکنید) ۹ - حالا نوبت چک ، تنظیم و تست سیستم های Auditing و Lgging هست . این سیستم ها هم می تواند بر پایه hst و هم بر پایه netwrk باشد . سیستم های رد گیری و ثبت حملات هم در این مرحله نصب و تنظیم می شوند. باید مطمئن شوید که تمام اطلاعات لازم ثبت و به خوبی محافظت می شود . در ضمن ساعت و تاریخ سیستم ها درست باشد ، مبادا که اشتباه باشه که تمام زحماتتان در این مرحله به باد میرود . و امکان پیگیری های قانونی در صورت لزوم دیگر وجود ندارد . ۱۰- ایمن کردن Remte Access با پروتکل ها و تکنولوژی های ایمن و Secure قدم بعدی رو تشکیل می دهد. در این زمینه با توجه به شرایط و امکانات ، ایمن ترین پروتکل و تکنولوژی ها رو به خدمت بگیرید . ۱۱ - نصب فایروال های شخصی در سطح hst ها ، لایه امنیتی مضاعفی به شبکه شما میدهد . پس این مرحله رو فراموش نکنید . ۱۲ - شرایط بازیابی در حالت های اضطراری رو حتما چک و بهینه کنید . این حالت ها شامل خرابی قطعات کامپیوتری ، خرابکاری کاربران عادی ، خرابی ناشی از بلایای طبیعی (زلزله - آتش سوزی - افتادن - سرقت - سیل و ...) و خرابکاری ناشی از نفوذ هکرها ، میباشد . استاندارد های warm site و ht site را در صورت امکان رعایت کنید. یادتون باشد که "" همیشه در دسترس بودن اطلاعات ، "" جز، قوانین اصلی امنیتی هست . ۱۳- و قدم آخر این پروسه که در حقیقت شروع یک جریان همیشگی هست ، عضو شدن در سایتها و بولتن های امنیتی و در جریان آخرین اخبار امنیتی قرار گرفتن هست . برای همه شما عزیزان آرزوی سلامتی و موفقیت را دارم .

آشنایی با مفاهیم NAT

قبل از اینکه نگاهی عمیق به مقوله NAT داشته باشیم می بایست بدانیم که عملکرد NAT چگونه است. بسته به نوع استفاده ، NAT روشهای پیاده سازی مختلفی دارد ولی همه آنها دارای یک مفهوم می باشند. NAT بسیار متداول شده تا آنجایی که در قابلیت پشتیبانی از آن در اکثر دستگاه ها نظیر ruter, firewall و... قرارداده شده است ویا حداقل یک نوع از این تکنولوژی را پشتیبانی می کنند. NAT تنها مختص شبکه هایی که به اینترنت متصل هستند محدود نمی شوند ،بلکه شما از این تکنولوژی می توانید بین شبکه های محلی خود نیز استفاده کنید ولی چون اکثر سازمانها درجهت ارتباط با اینترنت از این روش استفاده می کنند ما نیز به بررسی همین نوع استفاده می پردازیم. مفهوم NAT بسیار ساده و به این صورت است که یک دستگاه (مثل کامپیوتر یا

مسیریاب)به عنوان دروازه ورود به اینترنت عمل می کند و با این کار آدرس های ایستگاه های کاری را به آدرس دستگاهی که NAT روی آن فعال است ترجمه می کند ،به بیان دیگر NAT روی دستگاهی که به اینترنت وصل شده فعال می شود و ایستگاه های کاری و به طور کلی شبکه شما را از دید اینترنت پنهان می دارد. از سوی دیگر اینترنت شبکه شما را به صورت یک دستگاه ساده می بیند که به اینترنت متصل می باشد. NAT روی شبکه تغییر ایجاد نمی کند و نیازی به تنظیمات دوباره روی ایستگاه های کاری نیست فقط ایستگاه های کاری می بایست آدرس دروازه خروجی از شبکه را که همان آدرس دستگاهی است که NAT روی آن فعال شده را بدانند. همانطوری که دیده می شود شبکه با چهار ایستگاه کاری و یک مسیریاب جهت اتصال به اینترنت داریم .تمام ایستگاه های کاری دارای آدرس محلی گروه C می باشند. NAT چگونه کار می کند ؟ سه روش کلی برای اجرای NAT وجود دارد اگر چه قاعده کلی برای هر روش یکی است .همانطوری که در شکل های بالا نشان داده شد ،ترافیک ارسالی از سمت ایستگاه های کاری از درون یک روتر به اینترنت وارد می شوند و عملیات NAT را روی بسته ها انجام می دهد و به مقصد می فرستد. هربسته ای که روی کارت شبکه محلی مسیریاب دریافت می شود توسط روتر عملیات جابجایی آدرس محلی با آدرس اینترنتی انجام می شود و سپس بسته ها ارسال می شود. یک ایستگاه کاری از داخل شبکه یک بسته اطلاعاتی را به آدرس مقصد ۱۳۵.۲۵۰.۲۴.۱۰ می فرستد ، این بسته اطلاعاتی از داخل دروازه خروجی گذشته وبه اینترنت می رسد. عملیات NAT روی بسته ارسالی به روش زیر ارسال می گردد : بسته اطلاعاتی اصلی پس از رسیدن به مسیریاب آدرس مبداء آن از ۱۹۲.۱۶۸.۰.۱۲ به ۲۰۳.۳۱.۲۲۰.۱۳۴ تغییر پیدا می کند سپس روتر این اطلاعات را در حافظه خود و در NAT-Table نگهداری می کند و به این طریق است که بسته هایی هم که از اینترنت ارسال می شوند ،مقصد خود را تشخیص می دهند.

آشنایی با سوئیچ شبکه

سوئیچ شبکه از مجموعه ای کامپیوتر (گره) که توسط یک محیط انتقال (کابلی بدون کابل) بیکدیگر متصل می گردند ، تشکیل شده است. در شبکه از تجهیزات خاصی نظیر هاب و روتر نیز استفاده می گردد. سوئیچ یکی از عناصر اصلی و مهم در شبکه های کامپیوتری است . با استفاده از سوئیچ ، چندین کاربرقادربه ارسال اطلاعات از طریق شبکه در یک لحظه خواهند بود. سرعت ارسال اطلاعات هر یک از کاربران بر سرعت دستیابی سایر کاربران شبکه تاثیر نخواهد گذاشت . سوئیچ همانند روتر که امکان ارتباط بین چندین شبکه را فراهم می نماید ، امکان ارتباط گره های متفاوت (معمولا "کامپیوتر) یک شبکه را مستقیما "با یکدیگر فراهم می نماید. شبکه ها و سوئیچ ها دارای انواع متفاوتی می باشند.. سوئیچ هائی که برای هر یک از اتصالات موجود در یک شبکه داخلی استفاده می گردند ، سوئیچ های LAN نامیده می شوند. این نوع سوئیچ ها مجموعه ای از ارتباطات شبکه را بین صرفا "دو دستگاه که قصد ارتباط با یکدیگر را دارند ، در زمان مورد نظر ایجاد می نماید. مبانی شبکه عناصر اصلی در یک شبکه کامپیوتری بشرح زیر می باشند: شبکه . شبکه شامل مجموعه ای از کامپیوترهای متصل شده (با یک روش خاص)، بمنظور تبادل اطلاعات است . گره . گره ، شامل هر چیزی که به شبکه متصل می گردد ، خواهد بود.(کامپیوتر ، چاپگر و ...) سگمنت. سگمنت یک بخش خاص از شبکه بوده که توسط یک سوئیچ ، روتر و یا Bridge از سایر بخش ها جدا شده است . ستون فقرات . کابل اصلی که تمام سگمنت ها به آن متصل می گردند. معمولا "ستون فقرات یک شبکه دارای سرعت بمراتب بیشتری نسبت به هر یک از سگمنت های شبکه است . مثلا "ممکن است نرخ انتقال اطلاعات ستون فقرات شبکه ۱۰۰ مگابیت در ثانیه بوده در صورتیکه نرخ انتقال اطلاعات هر سگمنت ۱۰ مگابیت در ثانیه باشد. توپولوژی . روشی که هر یک از گره ها به یکدیگر متصل می گردند را گویند. کارت شبکه . هر کامپیوتر از طریق یک کارت شبکه به شبکه متصل می گردد.در اکثر کامپیوترهای شخصی ، کارت فوق از نوع اترنت بوده (دارای سرعت ۱۰ و یا ۱۰۰ مگابیت در ثانیه) و در یکی از اسلات های موجود روی برد اصلی سیستم ، نصب

خواهد شد. آدرس MAC . آدرس فیزیکی هر دستگاه (کارت شبکه) در شبکه است. آدرس فوق یک عدد شش بایتی بوده که سه بایت اول آن مشخص کننده سازنده کارت شبکه و سه بایت دوم ، شماره سریال کارت شبکه است . Unicast . ارسال اطلاعات توسط یک گره با آدرس خاص و دریافت اطلاعات توسط گره دیگر است . Multicast . یک گره ، اطلاعاتی را برای یک گروه خاص (با آدرس مشخص) ارسال می دارد.دستگاههای موجود در گروه ، اطلاعات ارسالی را دریافت خواهند کرد. Bradcast . یک گره اطلاعاتی را برای تمام گره های موجود در شبکه ارسال می نماید. استفاده از سوئیچ در اکثر شبکه های متداول ، بمنظور اتصال گره ها از هاب استفاده می شود. همزمان با رشد شبکه (تعداد کاربران ، تنوع نیازها ، کاربردهای جدید شبکه و ...) مشکلاتی در شبکه های فوق بوجود می آید : - Scalability . در یک شبکه مبتنی بر هاب ، پهنای باند بصورت مشترک توسط کاربران استفاده می گردد. با توجه به محدود بودن پهنای باند ، همزمان با توسعه، کارآئی شبکه بشدت تحت تاثیر قرار خواهد گرفت . برنامه های کامپیوتر که امروزه بمنظور اجراء بر روی محیط شبکه ، طراحی می گردنند به پهنای باند مناسبی نیاز خواهند داشت . عدم تامین پهنای باند مورد نیازبرنامه ها ، تاثیر منفی در عملکرد آنها را بدنبال خواهد داشت . -Latency . به مدت زمانی که طول خواهد کشید تا بسته اطلاعاتی به مقصد مورد نظر خود برسد ، اطلاق می گردد. با توجه به اینکه هر گره در شبکه های مبتنی بر هاب می بایست مدت زمانی را در انتظار سپری کرده (ممانعت از تصادم اطلاعات) ، بموازات افزایش تعداد گره ها در شبکه ، مدت زمان فوق افزایش خواهد یافت . در این نوع شبکه ها در صورتیکه یکی از کاربران فایل با ظرفیت بالائی را برای کاربر دیگر ارسال نماید ، تمام کاربران دیگر می بایست در انتظاز آزاد شدن محیط انتقال بمنظور ارسال اطلاعات باشند. بهرحال افزایش مدت زمانی که یک بسته اطلاعاتی به مقصد خود برسد ، هرگز مورد نظر کاربران یک شبکه نخواهد بود. - Netwrk Failure . در شبکه های مبتنی بر هاب ، یکی از دستگاههای متصل شده به هاب قادر به ایجاد مسائل و مشکلاتی برای سایر دستگاههای موجود در شبکه خواهد بود. عامل بروز اشکال می تواند عدم تنظیم مناسب سرعت (مثلا "تنظیم سرعت یک هاب با قابلیت ۱۰ مگابیت در ثانیه به ۱۰۰ مگابیت در ثانیه) و یا ارسال بیش از حد بسته های اطلاعاتی از نوع Bradcast ، باشد. - Cllisins . در شبکه های مبتنی بر تکنولوژی اترنت از فرآینده خاصی با نام CSMA/CD بمنظور ارتباط در شبکه استفاده می گردد. فرآیند فوق نحوه استفاده از محیط انتقال بمنظور ارسال اطلاعات را قانونمند می نماید. در چنین شبکه هائی تا زمانیکه بر روی محیط انتقال ترافیک اطلاعاتی باشد ، گره ای دیگر قادر به ارسال اطلاعات نخواهد بود. در صورتیکه دو گره در یک لحظه اقدام به ارسال اطلاعات نمایند ، یک تصادم اطلاعاتی ایجاد و عملا "بسته های اطلاعاتی ارسالی توسط هر یک از گره ها نیز از بین خواهند رفت . هر یک از گره های مربوطه (تصادم کننده) می بایست بمدت زمان کاملا "تصادفی در انتظار باقی مانده و پس از فراهم شدن شرایط ارسال ، اقدام به ارسال اطلاعات مورد نظر خود نمایند. هاب مسیر ارسال اطلاعات از یک گره به گره دیگر را به حداقل مقدار خود می رساند ولی عملا "شبکه را به سگمنت های گسسته تقسیم نمی نماید. سوئیچ بمنظور تحقق خواسته فوق عرضه شده است . یکی از مهمترین تفاوت های موجود بین هاب و سوئیچ ، تفسیر هر یک از پهنای باند است . تمام دستگاههای متصل شده به هاب ، پهنای باند موجود را بین خود به اشتراک می گذارند.در صورتیکه یک دستگاه متصل شده به سوئیچ ، دارای تمام پهنای باند مختص خود است. مثلا "در صورتیکه ده گره به هاب متصل شده باشند ، (در یک شبکه ده مگابیت درثانیه) هر گره موجود در شبکه بخشی از تمام پهنای باند موجود (ده مگابیت در ثانیه) را اشغال خواهد کرد. (در صورتیکه سایر گره ها نیز قصد ارتباط را داشته باشند) . در سوئیچ ، هر یک از گره ها قادر به برقراری ارتباط با سایر گره ها با سرعت ده مگابیت در ثانیه خواهد بود. در یک شبکه مبتنی بر سوئیچ ، برای هر گره یک سگمنت اختصاصی ایجاد خواهد شد. سگمنت های فوق به یک سوئیچ متصل خواهند شد. در حقیقت سوئیچ امکان حمایت از چندین (در برخی حالات صدها) سگمنت اختصاصی را دارا است . با توجه به اینکه تنها دستگاه های موجود در هر سگمنت سوئیچ و گره می باشند ، سوئیچ قادر به انتخاب اطلاعات ، قبل از رسیدن

به سایر گره ها خواهد بود. در ادامه سوئیچ، فریم های اطلاعاتی را به سگمنت مورد نظر هدایت خواهد کرد. با توجه به اینکه هر سگمنت دارای صرفا "یک گره می باشد ، اطلاعات مورد نظر به مقصد مورد نظر ارسال خواهند شد. بدین ترتیب در شبکه های مبتنی بر سوئیچ امکان چندین مبادله اطلاعاتی بصورت همزمان وجود خواهد داشت . با استفاده از سوئیچ ، شبکه های اترنت بصورت full-duplex خواهند بود. قبل از مطرح شدن سوئیچ ، اترنت بصورت half-duplex بود. در چنین حالتی داده ها در هر لحظه امکان ارسال در یک جهت را دارا می باشند . در یک شبکه مبتنی بر سوئیچ ، هر گره صرفا "با سوئیچ ارتباط برقرار می نماید (گره ها مستقیما "با یکدیگر ارتباط برقرار نمی نمایند) . در چنین حالتی اطلاعات از گره به سوئیچ و از سوئیچ به گره مقصد بصورت همزمان منتقل می گردند. در شبکه های مبتنی بر سوئیچ امکان استفاده از کابل های بهم تابیده و یا فیبر نوری وجود خواهد داشت . هر یک از کابل های فوق دارای کانکتورهای مربوط به خود برای ارسال و دریافت اطلاعات می باشند. با استفاده از سوئیچ ، شبکه ای عاری از تصادم اطلاعاتی بوجود خواهد آمد. انتقال دو سویه اطلاعات در شبکه های مبتنی بر سوئیچ ، سرعت ارسال و دریافت اطلاعات افزایش می یابد. اکثر شبکه های مبتنی بر سوئیچ بدلیل قیمت بالای سوئیچ ، صرفا "از سوئیچ به تنهائی استفاده نمی نمایند. در این نوع شبکه ها از ترکیب هاب و سوئیچ استفاده می گردد. مثلا "یک سازمان می تواند از چندین هاب بمنظور اتصال کامپیوترهای موجود در هر یک از دپارتمانهای خود استفاده و در ادامه با استفاده از یک سوئیچ تمام هاب ها(مربوط به هر یک از دپارتمانها) بیکدیگر متصل می گردد. تکنولوژی سوئیچ ها سوئیچ ها دارای پتانسیل های لازم بمنظور تغییر روش ارتباط هر یک از گره ها با یکدیگر می باشند. تفاوت سوئیچ با روتر چیست ؟ سوئیچ ها معمولا "در لایه دوم (Data layer) مدل SI فعالیت می نمایند.در لایه فوق امکان استفاده از آدرس های MAC (آدرس ها ی فیزیکی) وجود دارد. روتر در لایه سوم (Netwrk) مدل SI فعالیت می نمایند. در لایه فوق از آدرس های IP ر IPX و یا Appeltalk استفاده می شود. (آدرس ها ی منطقی) . الگوریتم استفاده شده توسط سوئیچ بمنظور اتخاذ تصمیم در رابطه با مقصد یک بسته اطلاعاتی با الگوریتم استفاده شده توسط روتر ، متفاوت است . یکی از موارد اختلاف الگوریتم های سوئیچ و هاب ، نحوه برخورد آنان با Bradcast است . مفهوم بسته های اطلاعاتی از نوع Bradcast در تمام شبکه ها مشابه می باشد. در چنین مواردی ، دستگاهی نیاز به ارسال اطلاعات داشته ولی نمی داند که اطلاعات را برای چه کسی می بایست ارسال نماید. بدلیل عدم آگاهی و دانش نسبت به هویت دریافت کننده اطلاعات ، دستگاه مورد نظر اقدام به ارسال اطلاعات بصورت bradcast می نماید. مثلا "هر زمان که کامپیوتر جدید ویا یکدستگاه به شبکه وارد می شود ، یک بسته اطلاعاتی از نوع Bradcast برای معرفی و حضور خود در شبکه ارسال می دارد. سایر گره ها قادر به افزودن کامپیوتر مورد نظر در لیست خود و برقراری ارتباط با آن خواهند بود. بنابراین بسته های اطلاعاتی از نوع Bradcast در مواردیکه یک دستگاه نیاز به معرفی خود به سایر بخش های شبکه را داشته و یا نسبت به هویت دریافت کننده اطلاعات شناخت لازم وجود نداشته باشند ، استفاده می گردند. هاب و یا سوئیچ ها قادر به ارسال بسته ای اطلاعاتی از نوع Bradcast برای سایر سگمنت های موجود در حوزه Bradcast می باشند. روتر عملیات فوق را انجام نمی دهد. در صورتیکه آدرس یکدستگاه مشخص نگردد ، روتر قادر به مسیریابی بسته اطلاعاتی مورد نظر نخواهد بود. ویژگی فوق در مواردیکه قصد جداسازی شبکه ها از یکدیگر مد نظر باشد ، بسیار ایده آل خواهد بود. ولی زمانیکه هدف مبادله اطلاعاتی بین بخش های متفاوت یک شبکه باشد ، مطلوب بنظر نمی آید. سوئیچ ها با هدف برخورد با مشکل فوق عرضه شده اند. سوئیچ های LAN بر اساس تکنولوژی packet-switching فعالیت می نمایند. سوئیچ یک ارتباط بین دو سگمنت ایجاد می نماید. بسته های اطلاعاتی اولیه در یک محل موقت (بافر) ذخیره می گردند ، آدرس فیزیکی (MAC) موجود در هدر خوانده شده و در ادامه با لیستی از آدرس های موجود در جدول Lkup (جستجو) مقایسه می گردد. در شبکه های LAN مبتنی بر اترنت ، هر فریم اترنت شامل یک بسته اطلاعاتی خاص است . بسته اطلاعاتی فوق شامل یک عنوان (هدر) خاص و شامل اطلاعات مربوط به آدرس فرستنده و

گیرنده بسته اطلاعاتی است . سوئیچ های مبتنی بر بسته های اطلاعاتی بمنظور مسیریابی ترافیک موجود در شبکه از سه روش زیر استفاده می نمایند. Cut-Thrugh Stre-and-frward Fragment-free سوئیچ های Cut-thrugh ، بلافاصله پس از تشخیص بسته اطلاعاتی توسط سوئیچ ، آدرس MAC خوانده می شود. پس از ذخیره سازی شش بایت اطلاعات که شامل آدرس می باشند ، بلافاصله عملیات ارسال بسته های اطلاعاتی به گره مقصد آغاز می گردد. (همزمان با دریافت سایر بسته های اطلاعاتی توسط سوئیچ) . با توجه به عدم وجود کنترل های لازم در صورت بروز خطاء در روش فوق ، سوئیچ های زیادی از روش فوق استفاده نمی نمایند. سوئیچ های stre-and-frward ، تمام بسته اطلاعاتی را در بافر مربوطه ذخیره و عملیات مربوط به بررسی خطاء (CRC) و سایر مسائل مربوطه را قبل از ارسال اطلاعات انجام خواهند داد. در صورتیکه بسته اطلاعاتی دارای خطاء باشد ، بسته اطلاعاتی دور انداخته خواهد شد. .در غیراینصورت ، سوئیچ با استفاده از آدرس MAC ، بسته اطلاعاتی را برای گره مقصد ارسال می نماید. اغلب سوئیچ ها از ترکیب دو روش گفته شده استفاده می نمایند. در این نوع سوئیچ ها از روش cut-thrugh استفاده شده و بمحض بروز خطاء از روش stre-and-frward استفاده می نمایند. یکی دیگر از روش های مسیریابی ترافیک در سوئیچ ها که کمتر استفاده می گردد ، fragment-free است . روش فوق مشابه cut-thrugh بوده با این تفاوت که قبل از ارسال بسته اطلاعاتی ۶۴ بایت آن ذخیره می گردد. سوئیچ های LAN دارای مدل های متفاوت از نقطه نظر طراحی فیزیکی می باشند. سه مدل رایج در حال حاضر بشرح زیر می باشند: - Shared memry . این نوع از سوئیچ ها تمام بسته های اطلاعاتی اولیه در بافر مربوط به خود را ذخیره می نمایند. بافر فوق بصورت مشترک توسط تمام پورت های سوئیچ (اتصالات ورودی و خروجی) استفاده می گردد. در ادامه اطلاعات مورد نظر بکمک پورت مربوطه برای گره مقصد ارسال خواهند شد. -Matrix . این نوع از سوئیچ ها دارای یک شبکه(تور) داخلی ماتریس مانند بوده که پورت های ورودی و خروجی همدیگر را قطع می نمایند. زمانیکه یک بسته اطلاعاتی بر روی پورت ورودی تشخیص داده شد ، آدرس MAC آن با جدول lkup مقایسه تا پورت مورد نظر خروجی آن مشخص گردد. در ادامه سوئیچ یک ارتباط را از طریق شبکه و در محلی که پورت ها همدیگر را قطع می کنند ، برقرار می گردد. - Bus Architecture . در این نوع از سوئیچ ها بجای استفاده از یک شبکه (تور) ، از یک مسیر انتقال داخلی (Bus) استفاده و مسیر فوق با استفاده از TDMA توسط تمام پورت ها به اشتراک گذاشته می شود. سوئیچ های فوق برای هر یک از پورت ها دارای یک حافظه اختصاصی می باشند. Transparent Bridging اکثر سوئیچ های LAN مبتنی بر اترنت از سیستم ی با نام transparent bridging برای ایجاد جداول آدرس lkup استفاده می نمایند. تکنولوژی فوق امکان یادگیری هر چیزی در رابطه با محل گره های موجود در شبکه ، بدون حمایت مدیریت شبکه را فراهم می نماید. تکنولوژی فوق داری پنج بخش متفاوت است : Learning Flding Filtering Frwarding Aging نحوه عملکرد تکنولوژی فوق بشرح زیر است : - سوئیچ به شبکه اضافه شده و تمام سگمنت ها به پورت های سوئیچ متصل خواهند شد. - گره A بر روی اولین سگمنت (سگمنت A) ، اطلاعاتی را برای کامپیوتر دیگر (گره B) در سگمنت دیگر (سگمنت C) ارسال می دارد. - سوئیچ اولین بسته اطلاعاتی را از گره A دریافت می نماید. آدرس MAC آن خوانده شده و آن را در جدول Lkup سگمنت A ذخیره می نماید. بدین ترتیب سوئیچ از نحوه یافتن گره A آگاهی پیدا کرده و اگر در آینده گره ای قصد ارسال اطلاعات برای گره A را داشته باشد ، سوئیچ در رابطه با آدرس آن مشکلی نخواهد داشت . فرآیند فوق را Learning می گویند. - با توجه به اینکه سوئیچ دانشی نسبت به محل گره B ندارد ، یک بسته اطلاعاتی را برای تمام سگمنت های موجود در شبکه (بجز سگمنت A که اخیرا "یکی از گره های موجود در آن اقدام به ارسال اطلاعات نموده است .) فرآیند ارسال یک بسته اطلاعاتی توسط سوئیچ ، بمنظور یافتن یک گره خاص برای تمام سگمنت ها ، Flding نامیده می شود. - گره B بسته اطلاعاتی را دریافت و یک بسته اطلاعاتی را بعنوان Acknwledgement برای گره A ارسال خواهد کرد. - بسته اطلاعاتی ارسالی توسط گره B به سوئیچ می

رسـد. در این زمـان ، سوئیـچ قادر به ذخیره کردن آدرس MAC گره B در جدول Lkup سگمنت C می باشـد. با توجه به اینکه سوئیچ از آدرس گره A آگاهی دارد ، بسته اطلاعاتی را مستقیما "برای آن ارسال خواهد کرد. گره A در سگمنتی متفاوت نسبت به گره B قرار دارد ، بنابراین سوئیـچ می بایست بمنظور ارسال بسته اطلاعاتی دو سـگمنت را به یکدیگر متصل نمائید. فرآیند فوق Frwarding نامیده می شود. – در ادامه بسته اطلاعاتی بعدی از گره A بمنظور ارسال برای گره B به سوئیچ می رسد ، با توجه به اینکه سوئیچ از آدرس گره B آگاهی دارد ، بسته اطلاعاتی فوق مستقیما "برای گره B ارسال خواهد شد. – گره C اطلاعاتی را از طریـق سوئیـچ برای گره A ارسـال می دارد. سوئیـچ آدرس MAC گره C را در جـدول Lkup سگمنت A ذخیره می نمایـد ، سوئیـچ آدرس گره A را دانسـته و مشـخص می گردد کـه دو گره A و C در یـک سـگمنت قرار دارنـد. بنـابراین نیازی به ارتباط سگمنت A با سگمنت دیگر بمنظور ارسال اطلاعات گره C نخواهد بود. بدین ترتیب سوئیچ از حرکت بسته های اطلاعاتی بین گره های موجود در یک سـگمنت ممانعت می نمایـد. فرآینـد فوق را Filtering می گوینـد. – Learning و Flding ادامه یافته و بموازات آن سوئیچ ، آدرس های MAC مربوط به گره ها را در جداول Lkup ذخیره می نماید. اکثر سوئیچ ها دارای حافظه کافی بمنظور ذخیره سازی جداول Lkup می باشند. بمنظور بهینه سازی حافظه فوق ، اطلاعات قدیمی تر از جداول فوق حذف تا فرآیند جسـتجو و یافتن آدرس ها در یک زمان معقول و سـریعتر انجام پـذیرد. بـذین منظور سوئیچ ها از روشـی با نام aging استفاده می نمایند. زمانیکه یک Entry برای یک گره در جـدول Lkup اضـافه می گردد ، به آن یـک زمان خاص نسـبت داده می شود. هر زمـان که بسـته ای اطلاعـاتی از طریق یک گره دریافت می گردد ، زمان مورد نظر بهنگام می گردد. سوئیـچ دارای یک یک تایمر قابل پیکربندی بوده که با عث می شود، Entry های موجود در جدول Lkup که مدت زمان خاصـی از آنها استفاده نشده و یا به آنها مراجعه ای نشده است ، حذف گردند . با حذف Entry های غیرضروری ، حافظه قابل استفاده برای سایر Entry ها بیشتر می گردد. در مثال فوق ، دو گره سـگمنت A را به اشتراک گذاشـته و سگمنت های A و D بصورت مسـتقل می باشند. در شبکه های ایـده آل مبتنی بر سوئیـچ ، هر گره دارای سـگمنت اختصاصـی مربوط بخود است . بـدین ترتیب امکـان تصـادم حـذف و نیـازی به عملیات Filtering نخواهد بود. فراوانی و آشـفتگی انتشار در شـبکه های با توپولوژی ستاره (Star) و یا ترکیب Bus و وStar یکی از عناصـر اصلی شبکه که می تواند باعث از کار افتادن شبکه گردد ، هاب و یا سوئیچ است . Spanning tress بمنظوری پیشـگیری از مسئله " آشفتگی انتشار "و سایر اثرات جانبی در رابطه با Lping شرکت DEC پروتکلی با نام –Spanning(STP tree Prtcl) را ایجـاد نموده است . پروتکل فوق با مشـخصه ۸۰۲.۱d توسط موسسه IEEE اسـتاندارد شده است . Spanning tree از الگـوریتم Spanning–tree algritm(STA) اسـتفاده می نمایـد. الگوریتم فوق بررسـی خواهد کرد آیا یک سوئیچ دارای بیش از یـک مسیر برای دستیابی به یک گره خاص است . در صورت وجود مسیرهای متعـدد ، بهترین مسیر نسبت به سایر مسیرها کدام است ؟ نحوه عملیات STP بشـرح زیر است : – به هر سوئیچ ، مجموعه ای از مشـخصه ها (ID) نسبت داده می شود. یکی از مشـخصه ها برای سوئیچ و سایر مشـخصه ها برای هر یک از پورت ها استفاده می گردد. مشخصه سوئیچ ، Bridge(BID ID) نامیـده شـده و دارای هشت بـایت است . دو بـایت بمنظور مشـخص نمودن اولویت و شـش بایت برای مشـخص کردن آدرس MAC استفاده می گردد. مشخصه پورت ها ، شانزده بیتی است . شش بیت بمنظور تنظیمات مربوط به اولویت و ده بیت دیگر برای اختصاص یک شـماره برا ی پورت مورد نظر است . – برای هر مسیر یک Path Cst محاسبه می گردد. نحوه محاسبه پارامتر فوق بر اساس استانداردهای ارائه شده توسط موسسه IEEE است . بمنظور محاسبه مقادر فوق ، ۱.۰۰۰ مگابیت در ثانیه (یک گیگابیت در ثانیه) را بر پهنای باند سگمنت متصل شده به پورت ، تقسیم می نمایند. بنابراین یک اتصال ۱۰ مگابیت در ثانیه ، دارای Cst به میزان ۱۰۰ است (۱.۰۰۰ تقسیم بر ۱۰) . بمنظور هماهنگ شدن با افزایش سـرعت شبکه های کامپیوتری استاندارد Cst نیز اصلاح می گردد. جـدول زیر مقادیر جدید STP Cst را نشان می دهـد. (مقدار Path cst می تواند یک مقدار دلخواه بوده که توسـط

مدیریت شبکه تعریف و مشخص می گردد) – هر سوئیچ فرآیندی را بمنظور انتخاب مسیرهای شبکه که می بایست توسط هر یک از سگمنت ها استفاده گردد ، آغاز می نمایند. اطلاعات فوق توسط سایر سوئیچ ها و با استفاده از یک پروتکل خاص با نام Bridge prtcl data units(BPUD) به اشتراک گذاشته می شود. ساختار یک BPUDبشرح زیر است ? : Rt BID . پارامتر فوق BID مربوط به Rt Bridge جاری را مشخص می کند ?. Path Cst t Bridge . مسافت rt bridge را مشخص می نماید. مثلا- "در صورتیکه داده از طریق طی نمودن سه سگمنت با سرعتی معادل ۱۰۰ مگابیت در ثانیه برای رسیدن به Rt bridge باشد ، مقدار cst بصورت (۱۹+۱۹+۰=۳۸) بدست می آید. سگمنتی که به Rt Bridge متصل است دارای Cst معادل صفر است? . Sender BID . مشخصه BID سوئیچ ارسال کننده BPDU را مشخص می کند?. Prt ID . پورت ارسال کننده BPDU مربوط به سوئیچ را مشخص می نماید. تمام سوئیچ ها بمنظور مشخص نمودن بهترین مسیر بین سگمنت های متفاوت ، بصورت پیوسته برای یکدیگر BPDUارسال می نمایند. زمانیکه سوئیچی یک BPDU را (از سوئیچ دیگر) دریافت می دارد که مناسبتر از آن چیزی است که خود برای ارسال اطلاعات در همان سگمنت استفاده کرده است ، BPDU خود را متوقف (به سایر سگمنت ها ارسال نمی نماید) و از BPDU سایر سوئیچ ها بمنظور دستیابی به سگمنت ها استفاده خواهد کرد. – یک Rt bridge بر اساس فرآیندهای BPDU بین سوئیچ ها ، انتخاب می گردد. در ابتدا هر سوئیچ خود را بعنوان Rt در نظر می گیرد. زمانیکه یک سوئیچ برای اولین بار به شبکه متصل می گردد ، یک BPDU را بهمراه BID خود که بعنوان Rt BID است ، ارسال می نماید. زمانیکه سایر سوئیچ ها BPDU را دریافت می دارند ، آن را با BID مربوطه ای که بعنوان Rt BID ذخیره نموده اند، مقایسه می نمایند. در صورتیکه Rt BID جدید دارای یک مقدار کمتر باشد ، تمام سوئیچ ها آن را با آنچیزی که قبلا "ذخیره کرده اند، جایگزین می نمایند. در صورتیکه Rt BID ذخیره شده دارای مقدار کمتری باشد ، یک BPDU برای سوئیچ جدید بهمراه BID مربوط به Rt BID ارسال می گردد. زمانیکه سوئیچ جدید BPDU را دریافت می دارد ، از Rt بودن خود صرفنظر و مقدار ارسالی را بعنوان Rt BID در جدول مربوط به خود ذخیره خواهد کرد. – با توجه به محل Rt Bridge ، سایر سوئیچ ها مشخص خواهند کرد که کدامیک از پورت های آنها دارای کوتاهترین مسیر به Rt Bridge است . پورت های فوق، Rt Prts نامیده شده و هر سوئیچ می بایست دارای یک نمونه باشد. – سوئیچ ها مشخص خواهند کرد که چه کسی دارای پورت های designated است . پورت فوق ، اتصالی است که توسط آن بسته های اطلاعاتی برای یک سگمنت خاص ارسال و یا از آن دریافت خواهند شد. با داشتن صرفا "یک نمونه از پورت های فوق ، تمام مشکلات مربوط به Lping برطرف خواهد شد. – پورت های designated بر اساس کوتاهترین مسیر بین یک سگمنت تا rt bridge انتخاب می گردند. با توجه به اینکه Rt bridge دارای مقدار صفر برای path cst است ، هر پورت آن بمنزله یک پورت designated است . (مشروط به اتصال پورت مورد نظر به سسگمنت) برای سایر سوئیچ ها، Path Cst برای یک سگمنت بررسی می گردد. در صورتیکه پورتی دارای پایین ترین path cst باشد ، پورت فوق بمنزله پورت designated سگمنت مورد نظر خواهد بود. در صورتیکه دو و یا بیش از دو پورت دارای مقادیر یکسان path cst باشند ، سوئیچ با مقادر کمتر BID اتخاب می گردد. – پس از انتخاب پورت designatedبرای سگمنت شبکه ، سایر پورت های متصل شده به سگمنت مورد نظر بعنوان nn- designated prt در نظر گرفته خواهند شد. بنابراین با استفاده از پورت های designated می توان به یک سگمنت متصل گردید. هر سوئیچ دارای جدول BPDU مربوط به خود بوده که بصورت خودکار بهنگام خواهد شد. بدین ترتیب شبکه بصورت یک spanning tree بوده که rr bridge که بمنزله ریشه و سایر سوئیچ ها بمنزله برگ خواهند بود. هر سوئیچ با استفاده از Rt Prts قادر به ارتباط با rt bridge بوده و با استفاده از پورت های designated قادر به ارتباط با هر سگمنت خواهد بود. روترها و سوئیچینگ لایه سوم همانگونه که قبلا "اشاره گردید ، اکثر سوئیچ ها در لایه دوم مدل SI فعالیت می نمایند (Data Layer) . اخیرا "برخی از

تولیدکنندگان سوییچ، مدلی را عرضه نموده اند که قادر به فعالیت در لایه سوم مدل SI است . (Netwrk Layer) . این نوع سوئیچ ها دارای شباهت زیادی با روتر می باشند. زمانیکه روتر یک بسته اطلاعاتی را دریافت می نماید ، در لایه سوم بدنبال آدرس های مبداء و مقصد گشته تا مسیر مربوط به بسته اطلاعاتی را مشخص نماید. سوئیچ های استاندارد از آدرس های MAC بمنظور مشخص کردن آدرس مبداء و مقصد استفاده می نمایند.(از طریق لایه دوم) مهمترین تفاوت بین یک روتر و یک سوئیچ لایه سوم ، استفاده سوئیچ های لایه سوم از سخت افزارهای بهینه بمنظور ارسال داده با سرعت مطلوب نظیر سوئیچ های لایه دوم است. نحوه تصمیم گیری آنها در رابطه با مسیریابی بسته های اطلاعاتی مشابه روتر است . در یک محیط شبکه ای LAN ، سوئیچ های لایه سوم معمولا "دارای سرعتی بیشتر از روتر می باشند. علت این امر استفاده از سخت افزارهای سوئیچینگ در این نوع سوئیچ ها است . اغلب سوئیچ های لایه سوم شرکت سیسکو، بمنزله روترهائی می باشند که بمراتب از روتر ها سریعتر بوده (با توجه به استفاده از سخت افزارهای اختصاصی سوئیچینگ) و دارای قیمت ارزانتری نسبت به روتر می باشند. نحوه Pattern matching و caching در سوئیچ های لایه سوم مشابه یک روتر است . در هر دو دستگاه از یک پروتکل روتینگ و جدول روتینگ، بمنظور مشخص نمودن بهترین مسیر استفاده می گردد. سوئیچ های لایه سوم قادر به برنامه ریزی مجدد سخت افزار بصورت پویا و با استفاده از اطلاعات روتینگ لایه سوم می باشند و همین امر باعث سرعت بالای پردازش بسته های اطلاعاتی می گردد. سوئیچ های لایه سوم ، از اطلاعات دریافت شده توسط پروتکل روتینگ بمنظور بهنگام سازی جداول مربوط به Caching استفاده می نمایند. همانگونه که ملاحظه گردید ، در طراحی سوئیچ های LAN از تکنولوژی های متفاوتی استفاده می گردد. نوع سوئیچ استفاده شده ، تاثیر مستقیم بر سرعت و کیفیت یک شبکه را بدنبال خواهد داشت .

سیستم عامل شبکه چیست؟

سیستم عامل شبکه چیست؟ نرم افزاری است که به کامپیوتر امکان استفاده از منابع نرم افزاری وسخت افزاری را داده و عملیات سیستم را تحت کنترل دارد. سیستم عاملهای Ds , windws ۳.۱ به کامپیوتر امکان استفاده از منابع خوش را می دهد و سیستم عاملهای Netware , Windws NT , Windws ۹۵ به کامپیوتر امکان استفاده وبه اشتراک گذاشتن منابع دیگر کامپیوتر های روی شبکه را می دهد بهر حال سیستم عامل شبکه کلیه عملیات سیستم را تحت شبکه نظرات داشته و کنترل می کند.

آموزش راه اندازی و تنظیم یک شبکه LAN کوچک

اگر در محیط کار یا منزل خود با بیش از یک کامپیوتر سروکار دارید احتمالا به فکر افتاده اید که آنها را به یکدیگر متصل کرده و یک شبکه کوچک کامپیوتری راه بیا ندازید . با اتصال کامپیوتر ها به یکدیگرمیتوانید چاپگرتان را بین همه انها به اشتراک بگذارید از طریق یکی از کامپیوتر ها که به اینترنت وصل است بقیه را نیز به اینترنت متصل کنید از هر یک از کامپیوتر ها به فایل های خود از جمله عکس ها اهنگ ها و اسنادتان دسترسی پیدا کنید به بازی هایی بپردازید که نه چند بازیکن با چند کامپیوتر نیاز دارند وبلاخره این که که خروجی وسایلی چون DVD PLAYER یا وب کم را به سایر کامپیوتر ها ارسال کنید . در این مقاله ضمن معرفی روش های مختلف اتصال کامپیوتر ها به یکدیگر انخام تنضیمات دستی را برای بهره بردن از حد اقل مزایای یک شبکه کامپیو تری به شما نشان می دهیم . ذکر این نکته هم لازم است که قسمت اصلی این مقاله به نصب نرم افزار اختصاص دارد اما در انتهای مطلب در خصوص ساختار شبکه و مسائل فیزیکی ان هم توضیهاتی داده ایم روشهای اتصال: برای اتصال کامپیوتر هایی که در فاصله ای نه چندان دور از یکدیگر قرار دارند راههای مختلفی وجود دارد که عبارتند از : سیم کشی دیتا به صورت تو کار در حین ساخت ساختمان که امروز بسیار متداول است . ذر این روش همان گونه که برای برق ساختمان از قبل نقشه می کشند

و مثلا جای کلید ها و پریز ها را مشخص می کنند برای شبکه کامپیوتری هم نقشه کشی و سیم کشی می کنند . قرار دادن سیم ها در کف اتاق و اتصال کامپیوتر هایی که در یک اتاق قرار دارند . استفاده از فناوری بی سیم ساتفاده از سیم کشی برق داخل ساختمان استفاده از سیم کشی تلفن داخل ساختمان هر یک روش ها مزایا و معایب خاص خود را دارند اما برای به اشتراک گذاشتن چاپگر فایل ها و اینتر نت باید کامپیوتر ها را به نحو صحیح و مناسبی تنظیم و آماده کنید و فرق نمی کند که کدام روش را انتخاب کرده باشید به همین دلیل کار را از همین نقطه شروع می کنیم از آنجا که ویندوز های اکس پی و ۹۸ پر استفاده ترین ویندوز ها در منازل و دفاتر کوچک هستند نحوه اشتراک گذاری منابع در این دو ویندوز را مورد بحث قرار می دهیم هر چند مورد سایر ویندوز ها مفاهیم تغییر نمی کند گام های اولیه : برای راه اندازی شبکه در منزل خود این سه کار را باید انجام دهیم : ۱انتخاب فناوری مناسب شبکه که مورد نظر ما در این مقاله اترنت استاندارد است ۲خرید و نصب سخت افزار مناسب این کار، که اصلی ترین آنها کارت شبکه برای هر یک از این کامپیوتر ها و یک هاب – سوییچ است ۳تنظیم و آماده سازی سیستم ها به نحوی که بتوانند همدیگر را ببینند و با یکدیگر صحبت کنند از این سه مرخله قدم سوم از همه مهم تر است . ویندوز اکس پی قسمتی به نام NETWRK SETUP WIZARD دارد که تنظیمات شبکه را برای شما انجام می دهد . به غیر از این متخصصان هستند که در ازای دریافت دستمزد ، شبکه شما را در محل راه می اندازند . نام گذاری کامپیوتر ها به اشتراک گذاشتن چاپگر ها فایل ها و اتصالات اینترنتی ،اساسی ترین کارهایی هستند که این افراد برای شما انجام می دهند . اما اگر با مشکلی مواجه بشوید یا تنظیمات کامپیوتر تان بهم بخورد ، باید بتوانید خودتان شبکه را تنظیم کنید . کلا بد نیست مفاهیم و اصول راه اندازی یک شبکه کامپیوتری را بدانید تا به هنگام ضرورت خودتان بتوانید دست به کار شوید . به طور کلی کار هایی که باید انجام دهید تا یک شبکه ((مرده)) را ((زنده)) کنید و به بهره برداری از ان بپر دازید ، از این قرار است : نام گذاری کامپیوتر دادن آدرس IP به اشتراک گذاشتن فایل ها به اشتراک گذاشتن چاپگر انجام تنظیمات امنیتی به اشتراک گذاشتن اتصال اینترنت نام گذاری کامپیوتر: بعد از نصب سخت افزار های مورد نیاز برای راه اندازی شبکه ، نیاز به نوبت به نصب نرم افزار های آن می رسد. در اولین قدم باید برای تکتک کامپیوتر های موجود در شبکه خود اسمی منحصر به فرد و غیر تکراری انتخاب کنید . علاوه بر اسم کامپیوتر اسم گروه کاری یا WRK GRUP هم مهم است . تمام کامپیوتر های یک شبکه باید عضو یک گروه کاری باشند . ویندوز اکس پی : برای نام گذاری کامپیوتر در ویندوز اکس پی این مراحل را دنبال کنید : ۱-پنجره cntrl panel را باز کنید ۲-اگر حالت نمایش آیکون ها به صورت کلاسیک نیست روی لینک classic new کلیک کنید .در این حالت بر نامه system را اجرا کنید . ۳- در کادر محاوره ظاهر شده صفحه cmputer name را انتخاب کنید ۴-همان طور که ملا حظه می کنید کامپیوتر یک اسم کامل دارد و یک گروه کاری . روی دکمه chang کلیک کنید تا کادر محاوره بعدی ظاهر شود . ۵-در کادر اول اسمی را تایپ کنید که می خواهید به کامپیوتر تان اختصاص دهید . این اسم هر چیزی می تواند باشد ، فقط نباید تکراری باشد . مثلا اسم کامپیونر اول را pc ۱ بگذارید . ۶-در کادر دوم اسمی را که می خواهید به گروه کاری خود اختصاص دهید وارد کنید .مثلا My ffice یا My Hme یا هر چیز دیگر . حتی خود Wrk Grup هم بد نیست . ۷- در پایان K و دوباره K را بزنید . اگر ویندوز خواست ری استارت کند قبول کنید . ویندوز ۹۸ برای نام گذاری کامپیوتر در ویندوز ۹۸ این مراحل را دنبال کنید: ۱-با کلیک راست روی آیکون Netwrk Neighbrhd روی دسکتاپ گزینه ، prperties را انتخاب کنید . ۲-در کادر محاوره ظاهر شده ، به صفحه identificatin بروید . ۳-در کادر اول ، اسم کامپیوتر و در کادر دوم اسم گروه کاری مورد نظر را بنویسید . بعد از تنظیم نام برای تک تک کامپیوتر ها و گذاشتن یک اسم برای کروه کاری تمام آنها ، کامپیوتر ها را دارای هویت کرده و در یک گروه جای داده اید . حالا نوبت به دادن آدرس IP میرسد . آدرس IP آدرس IP نشانی هر کامپیوتر در شبکه است . کامپیوتر از طریق این نشانی است که یکدیگر را در شبکه پیدا می کنند . در هر شبکه آدرس IP هر کامپیوتر باید منحصر به فرد و

غیر تکراری باشد . در باره IP و آدرس دهی از این طریق ، زیاد میتوان صحبت کرد ، اما از آنجا که در این مقاله قصد پرداختن به تئوری را نداریم بلا فاصله دست به کار می شویم . فقط ذکر این نکته را زروری میدانیم که آدرس IP در واقع یک شماره چهار قسمتی است . هر قسمت عددی از ۰ تا ۲۵۵ است که با علامت نقطه از قسمت بعدی جدا می شود . مثلا ۱۹۲.۱۶۸.۰.۱ یک آدرس IP است . مفهوم دیگر Subnet Mask است ، که توضیح آن هم از حوصله این مقاله خارج است . فقط این را قبول کنید که در یک شبکه کوچک ، subnet mask را به صورت ۲۵۵.۲۵۵.۲۵۵.۰ تایین می کنیم . در یک شبکه کوچک ، برای تمام کامپیوتر ها سه قسمت اول آدرس IP را یکسان می گیریم و فقط قسمت چهارم را برای هر کامپیوتر عدد متفاوتی را در نظر می گیریم . مثلاـ در کامپیوتر اول آدرس ۱۹۲.۱۶۸.۰.۱ و برای کامپیوتر دوم آدرس ۱۹۲.۱۶۸.۰.۲ را می نویسیم و به همین ترتیب ذر بقیه کامپیوتر ها قسمت چهارم آدرس IP را عدد متفاوتی را می دهیم .

Active Directry چیست

از جمله امکانات قدرتمند Windws ۲۰۰۰ Advanced server است . Active Directry امکان مدیریت کاربران و کامپیوترها و گروها و بطور کلی تمامی عناصر موجود در یک شبکه را فراهم می کند (البته نباید اینگونه تصور نمود که Active Directry تمامی مشکل یک مدیر شبکه را حل می نماید) با استفاده از قابلیتهای Active Directry می توان مشخص کرد کدام User با کدام Cmputer تحت کدام Dmaine به چه کاری بپردازد یعنی میزان دسترسی آن به منابع موجود در شبکه چه مقدار باشد .و تا چه میزان در این کار اختیار داردو اجازه دسترسی دارد. مثلا("امکان نوشتن یا جابجا نمودن و حتی امکان دسترسی به دیگر کاربران – دادن – و خود در چه سطحی از مدیریت نمودن شبکه قرار بگیرد.)با استفاده از قابلیت Active Directry در Windws ۲۰۰۰ Advanced Server مدیریت شبکه بسیار آسان است . چند نکته مهم در استفاده از Active Directry : ۱. اولین عاملی که باید در Active Directry مد نظر داشت این است که فایل سیستم ما باید از نوع NTFS باشد تا امکان استفاده از Active Directry را داشته باشیم. ۲. صحت تنظیمات کارت شبکه و پروتکل کامپیوترمورد نظر نیز کنترل شود. ۳. IP Address را دستی تنظیم و قبل از آن DNS SERVER را Cnfighr می نمائیم. ۴. بهتر است که در شبکه Clinte های خود را از خانواده Windws NT (XP , ۲۰۰۰ Pr , NT Wrk Staitin باشد (در اینصورت به بهترین وجه می توان امنیت شبکه و کامپیوتر های آن را تامین نمود) ۱.۱ : Physical Cnnectin r Physical Tplgy.اتصال فیزیکی ۲.۲ lgical Cnnectin.اتصال منطقی اتصال فیزیکی در یک شبکه چگونگی اتصال کامپیوترها و سخت افزارهای موجود در یک شبکه را از نظر فیزیکی مورد بحث قرار می دهد و اتصال منطقی نحوه رفتار کامپیوترهای موجود در شبکه را مورد بحث قرار می دهد. ساختار شبکه های کامپیوتری: شبکه های کامپیوتری از نظر ساختار به دو دسته تقسیم می شوند. ۱)Bradcast Pint t Pint Netwr(۲ Netwrk در اتصال Bradcast Netwrk هر کامپیوتر توسط Nd کابل شبکه خود همواره باید یا بطور مستقیم به کامپیوتر دیگر متصل بوده و یا توسط یک رسانه Media همانندHub به کامپیوتر دیگر متصل شود. در این روش کامپیوتر پیغام دهنده packet اطلاعات خود را در کل رسانه رها می نماید با این توضیح که نام و آدرس کامپیوتر پیغام گیرنده را هم به همراه آن ارسال می کند. این packet به همه کامپیوترها رسیده و تنها توسط کامپیوتری دریافت و خوانده می شود که آدرس و نام کامپیوتری که همراه با packet ارسال شده است – با آن همخوانی داشته باشد. در این ساختار علاوه بر اینکه ترافیک شبکه زیاد بوده و باعث کم شدن سرعت کارکرد شبکه می شود امنیت آن نیز از سطح مطلوبی برخوردار نیست زیرا packet اطلاعات که ممکن است محرمانه هم باشد در سطح شبکه پخش شده و به همه کامپیوترها می رسد. این ساختار از پیچیدگی کمتری برخوردار بوده و هزینه تهیه سخت افزارهای لازم برای راه اندازی آن کم است. در اتصال Pint t Pint

Netwrk دریافت و ارسال packet ها در شبکه توسط ابزاری هوشمند کنترل می شود بگونه ای که packet اطلاعاتی که برای یک کامپیوتر مشخص ارسال می گردد تنها به سمت همان کامپیوتر ارسال شده و دیگر کامپیوترها امکان دسترسی به آن را ندارند از طرف دیگر بدلیل اینکه این بسته اطلاعاتی در کل شبکه منتشر نمی شود ترافیک شبکه بطور قابل ملاحظه ای پایین آمده و امنیت درسطح شبکه بالا می رود. اینگونه شبکه ها به دلیل داشتن ابزاری چون سوئیچ های هوشمند گران تر از نوع قبل می باشد.

دسترسی سریع به شبکه

دسترسی سریع به شبکه PAP چیست؟ PAP مخفف عبارت Private Access Prvider است و منظور آن تامین کننده ارتباطات خصوصی است. در سال گذشته وزارت ارتباطات و فن آوری اطلاعات به تعدادی از شرکت های خصوصی مجوز داده است تا با استفاده از شبکه فیبر نوری شرکت های مخابرات استانی، به ایجاد شبکه ارتباطی پرسرعت برای کاربران بپردازند. به این شرکت ها اصطلاحا PAP گفته می شود. آنها با نصب تجهیزات لازم ارتباطات سیمی یا بی سیم را برای کاربران تامین می کنند. با استفاده از چنین بستری می توان امکان دسترسی پر سرعت به اینترنت را فراهم کرد. همچنین از این شبکه می توان برای ایجاد اینترنت های داخلی، شبکه های سازمانی و بین سازمانی و راه اندازی راه کارهای جامع الکترونیکی استفاده کرد. در واقع شرکت های PAP می توانند با ایجاد این بستر قوی و مناسب، محیطی را آماده کنند که اطلاعات و خدمات مختلف الکترونیکی براحتی و با سرعت مناسب در اختیار کاربران قرار گیرد. صحبت هایی که در حال حاضر در رسانه ها و اخبار درباره ارائه اینترنت پرسرعت و با استفاده از فن آوری DSL مطرح می گردد، در راستای کار همین شرکتهاست. برای کسب اطلاعات بیشتر در این مورد می توانید به سایت سازمان ارتباطات رادیویی در نشانی http://www.tra.ir مراجعه کنید .

آشنایی با Netstat

این دستور که با سویچ های دیگری هم استفاده میشه یکی از دستورایی هست که همه هکر ها اول باهاش آشنا میشن.که با تایپ این دستور شما متوجه آی پی سیستمها و پورتهایی که با آنها در ارتباط هستید میشوید و مشاهده میکنید که چه پورتهایی Listening و یا Established هستن این باعث میشود اگر پورتی مخصوص یک تروجن مثل ۲۷۳۷۴ که پورت اصلی Subv هست در سیستم شما باز بود شما متوجه این پورت باز بروی سیستمتان بشوید. اگر در قسمت Freign Address هم یک آی پی بوسیله پورتی به سیستم شما وصل بود شما به سرعت متوجه می شوید که یک نفر با آن آیپی در سیستم شماست ، پس این راهیست که متوجه گردید سیستمتان آسیب پذیر است یا نه ، برای مثال من با تایپ دستور Netstat در Ms-Ds پس از اتصال به اینتر نت نتایج زیر را گرفتم : C:\WINDWS>netstat Active Cnnectins Prt Lcal Address Freign Address State TCP Midia:۱۴۵۴ cs۳۳.msg.sc۵.yah.cm:۵۰۵۰ ESTABLISHED TCP Midia:۱۴۸۸ ۶۳.۱۲۳.۴۴.۲۲۲:۸۰ ESTABLISHED TCP Midia:۱۴۹۱ pi۱.vip.sc۵.yah.cm:۸۰ TIME_WAIT TCP Midia:۱۴۹۷ ۶۴.۱۸۷.۵۴.۲۳:۸۰ ESTABLISHED TCP Midia:۱۴۹۸ ۶۴.۱۸۷.۵۴.۲۳:۸۰ ESTABLISHED همانطور که ملاحظه میکنید این دستور گاهی اوقات اسم صاحب سیستم کلاینتی که شما با آن در ارتباط هستید را نیز میدهد و چون اینجا من با کسی در PM نبودم اسم کسی را نمیبینید ولی اگر کسی با من چت کند و دستور Netstat را اجرا کند اسم را میبیند و متوجه میشود که Midia صاحب آن سیستم کلاینتی می باشدکه در حال چت کردن با آن است و همچنین در این قسمت مشخص است که من با پورت ۵۰۵۰ با یاهو مسنجر ارتباط برقرار کرده ام و نیز نتایجی که در زیر Lcal Address مشخص است اطلاعاتی درباره خود من می باشد . و نتایجی که در Freign Address بدست میاد مشخص میکند که ما با چه سرور یا کلاینتی در

ارتباط هستیم . که در سطر پنجم مثال بالا یعنی ۶۳.۱۲۳.۴۴.۲۲۲:۸۰ آیپی سایت یاهو میباشد و مشخص میکند که من در سایت یاهو بوده و به وسیله پورت ۸۰ که پورت Http میباشد با این وب سرور ارتباط برقرار کرده ام و در قسمت Status هم مشخص میشود که شما با چه پورتهایی Established هستید یعنی ارتباط برقرار کرده و وصل هستید و چه پورتهایی Listening یا منتظر Request و در حال شنیدن می باشید ، بنابراین با دستور Netstat می شود یک عمل مانیتورینگ از تمام آیپی ها – پورتها و ماشینهایی که شما با آنها در ارتباط هستید گرفت . دستور Help : Netstat/? برنامه Netstat را معرفی میکند و سویچ های که ازش میتوان استفاده کرد و در مقابل هر سویچ در مورد کار آن توضیح مختصری میدهد. دستور Netstat –n : با این دستور میتوان آیپی و پورت سیستمی که شما با آن در ارتباط هستید را بدست آورد . برای مثال وقتی شما با یک نفر در یاهو مسنجر چت میکنید پورت ???? روی سیستم pen هست چون یاهو از پورت ???? استفاده میکند پس با تایپ netstat –n خواهید داشت: Active Cnnectins Prt Lcal Address Freign Address State TCP ۲۱۷.۲۱۹.۲۲۳.۲۱:۱۴۲۵ ۶۴.۲۴۲.۲۴۸.۱۵:۸۰ ESTABLISHED TCP ۲۱۷.۲۱۹.۲۲۳.۲۱:۱۴۳۱ ۲۱۶.۱۳۶.۱۷۵.۲۲۶:۵۰۵۰ TIME_WAIT TCP ۲۱۷.۲۱۹.۲۲۳.۳۸:۵۱۰۱ ۲۱۷.۲۱۹.۲۲۳.۲۱:۱۴۳۷ ESTABLISHED همانطور که ملاحظه میکنید من در این لحظه با آیپی ۲۱۷.۲۱۹.۲۲۳.۳۸ در حال چت کردن بودم که اشتراکش هم از رایان روش بوده (مثل خودم)و آی پی خود نیز پروتکلی که ما بوسیله آن با یک سیستم ارتباط برقرار کردیم Prt مشخص میشود در قسمت Lcal Address من هم TCPارتباط برقرار شده است. دستور Netstat –na : با تایپ کردن این دستور در MS-DS Prmpt تمام پورتهایی که داده ها و بسته ها را میفرستند مشخص میشود ، نشان " na " در تمام دستورات به معنی نمایش همه پورتها و لیست کردن آدرسهای شبکه و شماره فرمها در یک قالب عددی می باشد ، برای مثال من با تایپ این فرمان در MS-DS این نتایج را گرفتم : – C:\WINDWS>netstat na Active Cnnectins Prt Lcal Address Freign Address State TCP ۰.۰.۰.۰:۱۹۵۴ ۰.۰.۰.۰:۰ LISTENING TCP ۲۱۷.۲۱۹.۲۲۳.۲۱:۱۹۵۴ ۲۰۷.۴۶.۱۰۶.۲۱:۱۸۶۳ LISTENING TCP ۰.۰.۰.۰:۵۱۰۱ ۰.۰.۰.۰:۰ ESTABLISHED TCP ۲۱۷.۲۱۹.۲۲۳.۲۱:۱۹۷۱ ۲۱۶.۱۳۶.۲۲۵.۳۶:۵۰۵۰ ESTABLISHED TCP ۲۱۷.۲۱۹.۲۲۳.۲۱:۲۰۳۱ ۶۳.۱۲۱.۱۰۶.۷۴:۸۰ TIME_WAIT TCP ۱۲۷.۰.۰.۱:۱۰۲۵ ۰.۰.۰.۰:۰ LISTENING : UDP ۰.۰.۰.۰:۱۹۵۸ : UDP ۶۴.۱۱۰.۱۴۸.۵۹:۱۳۸ : UDP ۶۴.۱۱۰.۱۴۸.۵۹:۱۳۷ : UDP ۶۴.۱۱۰.۱۴۸.۵۹:۹ خب میبینید که پورتهای باز روی سیستم من لیست شده است. مثل ۱۹۵۴–۱۹۷۱–۲۰۳۱ دستور Netstat –a : این دستور نیز مثل دستور Netstat –an یا –na عمل میکنه فقط فرقش در اینه که این دستور پورتها را با معادل اسمیشان نشان میدهد ، برای مثال پورت ۱۳۹ را با معادل اسمیش یعنی Netbis نشان میدهد و همچنین مانند دستور Netstat اسم صاحب سیستم را پرینت میکند .(این دستور برای تست کردن نقطه ضعفها و پورتهای باز در سیستم های خودمان بسیار مفید میباشد و اگر سیستم آلوده به تروجن بود میشود از این دستورها و کلاً برنامه Netstat این موضوع را فهمید ، پس آنهایی که سوال میکنند ما چگونه بفهمیم سیستم خودمان آلوده به تروجن هست یا نه ، استفاده از این دستور و کلاً دستورات Netstat میتواند خیلی به آنها کمک کند) دستور Netstat –p xxx : منظور از xxx یعنی آن پروتکلی که شما در نظر دارید که میتواند TCP و UDP باشد. دستور Netstat –e : این دستور نیز یکی از دستورات Netstat است که آماری از ارتباطها و بسته ها و شماره های ارسال و ذخیره بسته ها و داده ها را نشان میدهد .(این دستور بیشتر برای ویندوزهای ۹۸ , me و همینطور مودمهایی که آمار بسته ها را نمیدهند خوب و مفید است چون در ویندوز ۲۰۰۰ – XP– قسمتی از این آمار براحتی در اختیار User قرار میگیرد ، و شما میتونید با استفاده از این دستور ترافیک ISP و شبکه را ببینید و همینطور برنامه هایی که در حال دانلود هستند را چک کنید و یا اگر بسته ای در ارسالش مشکلی پیش بیاد میتوانید در قسمت Errrs مشاهده کنید ، ...) دستور Netstat –r : این دستور توسط کاربران معمولی اینترنت زیاد بکار گرفته نمیشود چون درک

بعضی از گزینه هاش برای کاربران عادی دشوار ، بحرحال این دستور جزییات دقیقی مثل آدرس Gateway - Interface Metric -Netmask , ... درباره آدرس آی پی شما در شبکه میدهد ، همچنین در ویندوزهای۸ ۹ - ME کار دستور Netstat -a را هم انجام میدهد

امنیت شبکه: چالشها و راهکارها

امنیت شبکه: چالشها و راهکارها چکیده این مقاله به طور کلی به چالشها و راهکارها در امنیت شبکه می‌پردازد. در ابتدای مقاله به مباحثی چون: امنیت شبکه‌های اطلاعاتی و ارتباطی، اهمیت امنیت شبکه، سابقهٔ امنیت شبکه، پیدایش جرایم رایانه‌ای، طبقه‌بندی جرایم رایانه‌ای، و راهکارهایی که برای این چالش پیشنهاد شده است از جمله کنترل دولتی، کنترل سازمانی، کنترل فردی، تقویت اینترانتها، وجود یک نظام قدرتمند و کار گسترده فرهنگی برای آگاهی کاربران و فایروالها پرداخته می‌شود. در آخر نیز به مسأله «اینترنت و امنیت فرهنگی در ایران» و چالشهایی که در این زمینه مطرح گردیده پرداخته شده و برای رفع این مشکل پیشنهاداتی نیز ارائه گردیده است. ۱. مقدمه اینترنت یک شبکهٔ عظیم اطلاع‌رسانی و یک بانک وسیع اطلاعاتی است که در آینده نزدیک دسترسی به آن برای تک‌تک افراد ممکن خواهد شد. کارشناسان ارتباطات، بهره‌گیری از این شبکه را یک ضرورت در عصر اطلاعات می‌دانند. این شبکه که از هزاران شبکه کوچکتر تشکیل شده، فارغ از مرزهای جغرافیایی، سراسر جهان را به هم مرتبط ساخته است. طبق آخرین آمار بیش از شصت میلیون رایانه از تمام نقاط جهان در این شبکهٔ گسترده به یکدیگر متصل شده‌اند که اطلاعات بی‌شماری را در تمامی زمینه‌ها از هر سنخ و نوعی به اشتراک گذاشته‌اند. گفته می‌شود نزدیک به یک میلیارد صفحه اطلاعات با موضوعات گوناگون از سوی افراد حقیقی و حقوقی روی این شبکه قرار داده شده است. این اطلاعات با سرعت تمام در بزرگراههای اطلاعاتی بین کاربران رد و بدل می‌شود و تقریباً هیچ گونه محدودیت و کنترلی بر وارد کردن یا دریافت کردن داده‌ها اعمال نمی‌شود. حمایت از جریان آزاد اطلاعات، گسترش روزافزون فنآوری اطلاعات و بسترسازی برای اتصال به شبکه‌های اطلاع‌رسانی شعار دولتهاست. این در حالی است که گستردگی و تنوع اطلاعات آلوده روی اینترنت، موجب بروز نگرانی در بین کشورهای مختلف شده است. انتشار تصاویر مستهجن، ایجاد پایگاههایی با مضامین پورنوگرافی و سایتهای سوءاستفاده از کودکان و انواع قاچاق در کشورهای پیشرفته صنعتی بخصوص در خاستگاه این شبکهٔ جهانی یعنی آمریکا، کارشناسان اجتماعی را بشدت نگران کرده، به گونه‌ای که هیأت حاکمه را مجبور به تصویب قوانینی مبنی بر کنترل این شبکه در سطح آمریکا نموده است. هشدار، جریمه و بازداشت برای برپاکنندگان پایگاههای مخرب و فسادانگیز تدابیری است که کشورهای مختلف جهان برای مقابله با آثار سوء اینترنت اتخاذ کرده‌اند. ترس و بیم از تخریب مبانی اخلاقی و اجتماعی، ناشی از هجوم اطلاعات آلوده و مخرب از طریق اینترنت، واکنشی منطقی است، زیرا هر جامعه‌ای چارچوبهای اطلاعاتی خاص خود را دارد و طبیعی است که هر نوع اطلاعاتی که این حد و مرزها را بشکند می‌تواند سلامت و امنیت جامعه را به خطر اندازد. علی‌الرغم وجود جنبه‌ای مثبت شبکههای جهانی، سوء استفاده از این شبکه‌های رایانه‌ای توسط افراد بزهکار، امنیت ملی را در کشورهای مختلف با خطر روبرو ساخته است. از این رو بکارگیری فیلترها و فایر والهای مختلف برای پیشگیری از نفوذ داده‌های مخرب و مضر و گزینش اطلاعات سالم در این شبکه‌ها رو به افزایش است. خوشبختانه با وجود هیاهوی بسیاری که شبکهٔ اینترنت را غیرقابل کنترل معرفی می‌کند، فناوری لازم برای کنترل این شبکه و انتخاب اطلاعات سالم روبه گسترش و تکامل است. ۲. امنیت شبکه‌های اطلاعاتی و ارتباطی ۲-۱: اهمیت امنیت شبکه چنانچه به اهمیت شبکه‌های اطلاعاتی (الکترونیکی) و نقش اساسی آن دریافت اجتماعی آینده پی برده باشیم، اهمیت امنیت این شبکه‌ها مشخص می‌گردد. اگر امنیت شبکه برقرار نگردد، مزیتهای فراوان آن نیز به خوبی حاصل نخواهد شد و پول و تجارت الکترونیک، خدمات به کاربران خاص، اطلاعات شخصی، اطلاعاتی عمومی و نشریات الکترونیک همه و همه در معرض

دستکاری و سوءاستفاده‌های مادی و معنوی هستند. همچنین دستکاری اطلاعات- به عنوان زیربنای فکری ملت‌ها توسط گروههای سازماندهی شده بین‌المللی، به نوعی مختل ساختن امنیت ملی و تهاجم علیه دولت‌ها و تهدیدی ملی محسوب می‌شود. برای کشور ما که بسیاری از نرم‌افزارهای پایه از قبیل سیستم عامل و نرم‌افزارهای کاربردی و اینترنتی، از طریق واسطه‌ها و شرکتهای خارجی تهیه می‌شود، بیم نفوذ از طریق راههای مخفی وجود دارد. در آینده که بانکها و بسیاری از نهادها و دستگاههای دیگر از طریق شبکهٔ به فعالیت می‌پردازند، جلوگیری از نفوذ عوامل مخرب در شبکه بصورت مسئله‌ای استراتژیک درخواهد آمد که نپرداختن به آن باعث ایراد خساراتی خواهد شد که بعضاً جبران‌ناپذیر خواهد بود. چنانچه یک پیغام خاص، مثلاً از طرف شرکت مایکروسافت، به کلیه سایتهای ایرانی ارسال شود و سیستم عاملها در واکنش به این پیغام سیستمها را خراب کنند و از کار بیندازند، چه ضررهای هنگفتی به امنیت و اقتصاد مملکت وارد خواهد شد؟ نکته جالب اینکه بزرگترین شرکت تولید نرم‌افزارهای امنیت شبکه، شرکت چک پوینت است که شعبهٔ اصلی آن در اسرائیل می‌باشد. مسأله امنیت شبکهٔ برای کشورها، مسأله‌ای استراتژیک است؛ بنابراین کشور ما نیز باید به آخرین تکنولوژیهای امنیت شبکه مجهز شود و از آنجایی که این تکنولوژیها به صورت محصولات نرم‌افزاری قابل خریداری نیستند، پس می‌بایست محققین کشور این مهم را بدست بگیرند و در آن فعالیت نمایند. امروزه اینترنت آنقدر قابل دسترس شده که هرکس بدون توجه به محل زندگی، ملیت، شغل و زمان میتواند به آن راه یابد و از آن بهره ببرد. همین سهولت دسترسی آن را در معرض خطراتی چون گم شدن، ربوده شدن، مخدوش شدن یا سوءاستفاده از اطلاعات موجود در آن قرار می‌دهد. اگر اطلاعات روی کاغذ چاپ شده بود و در قفسه‌ای از اتاقهای محفوظ اداره مربوطه نگهداری می‌شد، برای دسترسی به آنها افراد غیرمجاز می‌بایست از حصارهای مختلف عبور می‌کردند، اما اکنون چند اشاره به کلیدهای رایانه‌ای برای این منظور کافی است. ۲-۲: سابقه امنیت شبکه اینترنت در سال ۱۹۶۹ بصورت شبکه‌های بنام آرپانت که مربوط به وزارت دفاع آمریکا بود راه‌اندازی شد. هدف این بود که با استفاده از رایانه‌های متصل به هم، شرایطی ایجاد شود که حتی اگر، بخشهای عمده‌ای از سیستم اطلاعاتی به هر دلیلی از کار بیفتد، کل شبکه بتواند به کار خود ادامه دهد، تا این اطلاعات حفظ شود. از همان ابتدا، فکر ایجاد شبکه، برای جلوگیری از اثرات مخرب حملات اطلاعاتی بود. در سال ۱۹۷۱ تعدادی از رایانه‌های دانشگاهها و مراکز دولتی به این شبکه متصل شدند و محققین از این طریق شروع به تبادل اطلاعات کردند. با بروز رخدادهای غیرمنتظره در اطلاعات، توجه به مسأله امنیت بیش از پیش اوج گرفت. در سال ۱۹۸۸، آرپانت برای اولین بار با یک حادثه امنیتی سراسری در شبکه، مواجه شد که بعداً، «کرم موریس» نام گرفت. رابرت موریس که یک دانشجو در نیویورک بود، برنامه‌هایی نوشت که می‌توانست به یک رایانه‌ای دیگر راه یابد و در آن تکثیر شود و به همین ترتیب به رایانه‌های دیگر هم نفوذ کند و بصورت هندسی تکثیر شود. آن زمان ۸۸۰۰۰ رایانه به این شبکه وصل بود. این برنامه سبب شد طی مدت کوتاهی ده درصد از رایانه‌های متصل به شبکه در آمریکا از کار بیفتد. به دنبال این حادثه، بنیاد مقابله با حوادث امنیتی (IRST) شکل گرفت که در هماهنگی فعالیتهای مقابله با حملات ضد امنیتی، آموزش و تجهیز شبکه‌ها و روشهای پیشگیرانه نقش مؤثری داشت. با رایج‌تر شدن و استفاده عام از اینترنت، مسأله امنیت خود را بهتر و بیشتر نشان داد. از جمله این حوادث، اختلال در امنیت شبکه، WINK/ILS WRM در سال ۱۹۸۹، Sniff packet در سال ۱۹۹۴ بود که مورد اخیر از طریق پست الکترونیک منتشر می‌شد و باعث افشای اطلاعات مربوط به اسامی شماره رمز کاربران می‌شد. از آن زمان حملات امنیتی- اطلاعاتی به شبکه‌ها و شبکه جهانی روزبه‌روز افزایش یافته است. گرچه اینترنت در ابتدا، با هدف آموزشی و تحقیقاتی گسترش یافت، امروزه کاربردهای تجاری، پزشکی، ارتباطی و شخصی فراوانی پیدا کرده است که ضرورت افزایش ضریب اطمینان آن را بیش از پیش روشن نموده است. ۳- جرائم رایانه‌ای و اینترنتی ویژگی برجسته فناوری اطلاعات، تأثیری است که بر تکامل فناوری ارتباطات راه دور گذاشته و خواهد گذاشت. ارتباطات کلاسیک همچون انتقال صدای انسان، جای خود را، به مقادیر وسیعی از داده‌ها، صوت، متن، موزیک، تصاویر ثابت و متحرک داده است. این تبادل و

تکامل نه تنها بین انسانها بلکه مابین انسانها و رایانه‌ها، و همچنین بین خود رایانه‌ها نیز وجود دارد. استفاده وسیع از پست الکترونیک، و دستیابی به اطلاعات از طریق وب‌سایتهای متعدد در اینترنت نمونه‌هایی از این پیشرفتها می‌باشد که جامعه را بطور پیچیده‌ای دگرگون ساخته‌اند. سهولت در دسترسی و جستجوی اطلاعات موجود در سیستمهای رایانه‌ای توأم با امکانات عملی نامحدود در مبادله و توزیع اطلاعات، بدون توجه به فواصل جغرافیایی، منجر به رشد سرسام‌آور مقدار اطلاعات موجود در آگاهی که می‌توان از آن بدست آورد، شده است. این اطلاعات موجب افزایش تغییرات اجتماعی و اقتصادی پیش‌بینی نشده گردیده است. اما پیشرفتهای مذکور جنبهٔ خطرناکی نیز دارد که پیدایش انواع جرایم و همچنین بهره‌برداری از فناوری جدید در ارتکاب جرایم بخشی از آن به شمار می‌رود. بعلاوه عواقب و پیامدهای رفتار مجرمانه می‌تواند خیلی بیشتر از قبل و دور از تصور باشد چون که محدودیتهای جغرافیایی یا مرزهای ملی آن را محدود نمی‌کنند. فناوری جدید مفاهیم قانونی موجود را دچار چالشهایی ساخته است. اطلاعات و ارتباطات راه دور به راحت‌ترین وجه در جهان جریان پیدا کرده و مرزها دیگر موانعی بر سر این جریان به شمار نمی‌روند. جنایتکاران غالباً در مکانهایی به غیر از جاههایی که آثار و نتایج اعمال آنها ظاهر می‌شود، قرار دارند. سوءاستفاده گسترده مجرمین، به ویژه گروههای جنایتکار سازمان نیافته از فناوری اطلاعات سبب گشته است که سیاستگذاران جنایی اغلب کشورهای جهان با استفاده از ابزارهای سیاست جنایی درصدد مقابله با آنها برآیند. تصویب کنوانسیون جرایم رایانه‌ای در اواخر سال ۲۰۰۱ و امضای آن توسط ۳۰ کشور پیشرفته، تصویب قوانین مبارزه با این جرایم توسط قانون‌گذاران داخلی و تشکیل واحدهای مبارزه با آن در سازمان پلیس بیشتر کشورهای پیشرفته و تجهیز آنها به جدیدترین سخت‌افزارها و نرم‌افزارهای کشف این گونه جرایم و جذب و بکارگیری بهترین متخصصین در واحدهای مذکور، بخشی از اقدامات مقابله‌ای را تشکیل می‌دهد. ۳-۱: پیدایش جرایم رایانه‌ای در مورد زمان دقیق پیدایش جرم رایانه‌ای نمی‌توان اظهارنظر قطعی کرد. این جرم زائیده تکنولوژی اطلاعاتی و انفورماتیکی است، بنابراین بطور منظم بعد از گذشت مدت کوتاهی از شیوع و کاربرد تکنولوژی اطلاعات، باب سوءاستفاده نیز قابل طرح است. شیوع استعمال این تکنولوژی و برابری کاربران آن حداقل در چند کشور مطرح جهان بصورت گسترده، امکان بررسی اولین مورد را دشوار می‌سازد. در نهایت آن چه مبرهن است اینکه در جامعه آمریکا رویس موجب شد برای اولین بار اذهان متوجه سوءاستفاده‌های رایانه‌ای شود. ۳-۲: قضیه رویس: آلدون رویس حسابدار یک شرکت بود. چون به گمان وی، شرکت حق او را پایمال کرده بود، بنابراین با تهیه برنامه‌ای، قسمتی از پولهای شرکت را اختلاس کرد. انگیزهٔ رویس در این کار انتقام‌گیری بود. مکانیزم کار بدین گونه بود که شرکت محل کار وی یک عمده‌فروش میوه و سبزی بود. محصولات متنوعی را از کشاورزان می‌خرید و با استفاده از تجهیزات خود از قبیل کامیونها، انبار و بسته‌بندی و سرویس‌دهی به گروههای فروشندگان، آنها را عرضه می‌کرد. به دلیل وضعیت خاص این شغل، قیمتها در نوسان بود و ارزیابی امور تنها می‌توانست از عهدهٔ رایانه برآید تا کنترل محاسبات این شرکت عظیم را عهده‌دار شود. کلیه امور حسابرسی و ممیزی اسناد و مدارک و صورت حسابها به صورت اطلاعات مضبوط در نوارهای الکترونیکی بود. رویس در برنامه‌ها، دستورالعمل‌های اضافی را گنجانده بود و قیمت کالاها را با ظرافت خاصی تغییر می‌داد. با تنظیم درآمد اجناس وی مبلغی را کاهش می‌داد و مبالغ حاصله را به حسابهای مخصوص واریز می‌کرد. بعد در زمانهای خاص چکی به نام یکی از هفده شرکت جعلی و ساختگی خودش صادر و مقداری از مبالغ را برداشت می‌کرد. بدین ترتیب وی توانست در مدت ۶ سال بیش از یک میلیون دلار برداشت کند. اما او بر سر راه خودش مشکلی داشت و آن این بود که مکانیسمی برای توقف عملکرد سیستم نمی‌توانست بیندیشد. بنابراین در نهایت خود را به مراجع قضایی معرفی و به جرم خود اعتراض کرد و به مدت ده سال به زندان محکوم شد. از این جا بود که مبحث جدیدی به نام جرم رایانه‌ای ایجاد شد. ۳-۳: تعریف جرم رایانه‌ای تاکنون تعریفهای گوناگونی از جرم رایانه‌ای از سوی سازمانها، متخصصان و برخی قوانین ارائه شده که وجود تفاوت در آنها بیانگر ابهامات موجود در ماهیت و تعریف این جرائم است. جرم رایانه‌ای یا جرم در فضای

مجازی (سایر جرایم) دارای دو معنی و مفهوم است. در تعریف مضیق، جرم رایانه‌ای صرفاً عبارت از جرایمی است که در فضای سایبر رخ می‌دهد. از این نظر جرایمی مثل هرزه‌نگاری، افترا، آزار و اذیت سوءاستفاده از پست الکترونیک و سایر جرایمی که در آنها رایانه به عنوان ابزار و وسیله ارتکاب جرم بکار گرفته می‌شود، در زمرهٔ جرم رایانه‌ای قرار نمی‌گیرند. در تعریف موسع از جرم رایانه‌ای هر فعل و ترک فعلی که در اینترنت یا از طریق آن یا با اینترنت یا از طریق اتصال به اینترنت، چه بطور مستقیم یا غیرمستقیم رخ می‌دهد و قانون آن را ممنوع کرده و برای آن مجازات در نظر گرفته شده است جرم رایانه‌ای نامیده می‌شود. براین اساس اینگونه جرایم را می‌توان به سه دسته تقسیم نمود: دسته اول: جرایمی هستند که در آنها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شوند. مانند سرقت، تخریب و غیره دسته دوم: جرایمی هستند که در آنها رایانه به عنوان ابزار وسیله توسط مجرم برای ارتکاب جرم بکار گرفته می‌شود. دسته سوم: جرایمی هستند که می‌توان آنها را جرایم رایانه‌ای محض نامید. این نوع از جرایم کاملاً با جرایم کلاسیک تفاوت دارند و در دنیای مجازی به وقوع می‌پیوندند اما آثار آنها در دنیای واقعی ظاهر می‌شود. مانند دسترسی غیرمجاز به سیستم‌های رایانه‌ای. ۳-۴: طبقه‌بندی جرایم رایانه‌ای طبقه‌بندی‌های مختلفی از جرایم رایانه‌ای توسط مراجع مختلف انجام گرفته است. برای آشنایی شما با آنها موارد مهم بشرح زیر اکتفا می‌شود. ۳-۴-۱: طبقه‌بندی ECDB در سال ۱۹۸۳ «او.ای.سی.دی.بی» مطالعه امکان پذیری اعمال بین‌المللی و هماهنگی قوانین کیفری را به منظور حل مسئله جرم یا سوءاستفاده‌های رایانه‌ای متعهد شد. این سازمان در سال ۱۹۸۶ گزارشی تحت عنوان جرم رایانه‌ای، تحلیل سیاستهای قانونی منتشر ساخت که به بررسی قوانین موجود و پیشنهادهای اصلاحی چند کشور عضو پرداخته و فهرست حداقل سوءاستفاده‌هایی را پیشنهاد کرده بود که کشورهای مختلف باید با استفاده از قوانین کیفری، مشمول ممنوعیت و مجازات قرار دهند. بدین گونه اولین تقسیم‌بندی از جرایم رایانه‌ای در سال ۱۹۸۳ ارائه شد و طی آن پنج دسته اعمال را مجرمانه تلقی کرد و پیشنهاد کرد در قوانین ماهوی ذکر شود. این پنج دسته عبارتند از: الف: ورود، تغییر، پاک کردن و یا متوقف‌سازی داده‌های رایانه‌ای و برنامه‌های رایانه‌ای که بطور ارادی با قصد انتقال غیرقانونی وجوه یا هر چیز باارزش دیگر صورت گرفته باشد. ب: ورود، تغییر، پاک کردن، و یا متوقف‌سازی داده‌های رایانه‌ای و برنامه‌های رایانه‌ای که بصورت عمدی و به قصد ارتکاب جعل صورت گرفته باشند. یا هرگونه مداخله دیگر در سیستمهای رایانه‌ای که بصورت عمدی و با قصد جلوگیری از عملکرد سیستم رایانه‌ای و یا ارتباطات صورت گرفته باشد. ج: ورود، تغییر، پاک کردن و متوقف‌سازی داده‌های رایانه‌ای و یا برنامه‌های رایانه‌ای. د: تجاوز به حقوق انحصاری مالک یک برنامهٔ رایانه‌ای حفاظت شده با قصد بهره‌برداری تجاری از برنامه‌ها و ارائه آن به بازار. ه- دستیابی یا شنود در یک سیستم رایانه‌ای و یا ارتباطی که آگاهانه و بدون کسب مجوز از فرد مسئول سیستم مزبور یا تخطی از تدابیر امنیتی و چه با هدف غیر شرافتمندانه و یا موضوع صورت گرفته باشد. ۳-۴-۲: طبقه‌بندی شورای اروپا: کمیتهٔ منتخب جرایم رایانه‌ای شورای اروپا، پس از بررسی نظرات «او ای سی دی.بی» و نیز بررسیهای حقوقی- فنی دو لیست تحت عناوین لیست حداقل و لیست اختیاری را به کمیته وزراء پیشنهاد داد و آنان نیز تصویب کردند. این لیستها بدین شرح هستند: الف: کلاهبرداری رایانه‌ای ب: جعل رایانه‌ای ج: خسارت زدن به داده‌های رایانه‌ای یا برنامه‌های رایانه‌ای د: دستیابی غیرمجاز ه: ایجاد مجدد و غیرمجاز یک برنامهٔ رایانه‌ای حمایت شده - ایجاد مجدد غیرمجاز یک توپوگرافی. - لیست اختیاری الف: تغییر داده‌های رایانه‌ای و یا برنامه‌های رایانه‌ای ب: جاسوسی رایانه‌ای ج: استفاده غیرمجاز از رایانه د: استفاده غیرمجاز از برنامهٔ رایانه‌ای حمایت شده. ۳-۴-۳: طبقه‌بندی اینترپول: سالهاست که اینترپول در مبارزه با جرایم مرتبط با فناوری اطلاعات فعال می‌باشد. این سازمان با بهره‌گیری از کارشناسان و متخصصین کشورهای عضو اقدام به تشکیل گروههای کاری در این زمینه کرده است. رؤسای واحدهای مبارزه با جرایم رایانه‌ای کشورهای باتجربه عضو سازمان در این گروه کاری گردهم آمده‌اند. گروههای کاری منطقه‌ای در اروپا، آسیا، آمریکا و آفریقا مشغول به کارند. و زیر نظر کمیتهٔ راهبردی جرایم فناوری اطلاعات، مستقر در دبیرخانهٔ کل اینترپول فعالیت می‌نمایند. گروه کاری اروپایی اینترپول با حضور

کارشناسان هلند، اسپانیا، بلژیک، فنلاند، فرانسه، آلمان، ایتالیا، سوئد و انگلیس در سال ۱۹۹۰ تشکیل شد. این گروهها هر سال سه بار تشکیل جلسه می‌دهند و در ژانویه سال ۲۰۰۱ سی‌امین گردهمایی آن در دبیرخانه کل تشکیل گردید. تهیه کتابچهٔ راهنمای پی‌جویی جرایم رایانه‌ای، کتاب و سی‌دی راهنمای جرایم رایانه‌ای، تشکیل دوره‌های آموزشی برای نیروهای پلیس در طول ۵ سال گذشته، تشکیل سیستم اعلام خطر که مرکب از سیستمهای پاسخگوی شبانه‌روزی، نقاط تماس دائمی شبانه‌روزی، تبادل پیام بین‌المللی در قالب فرمهای استاندارد در زمینهٔ جرایم رایانه‌ای واقعه می‌باشد و انجام چندین پروژه تحقیقاتی پیرامون موضوعات مرتبط با جرایم رایانه‌ای از جمله اقدامات گروه کاری مذکور می‌باشد. گروه کار آمریکایی جرایم مرتبط با تکنولوژی اطلاعات مرکب از کارشناسان و متخصصین کشورهای کانادا، ایالات متحده، آرژانتین، شیلی، کلمبیا، جامائیکا و باهاماست. گروه کاری آفریقایی جرایم مرتبط با تکنولوژی اطلاعات مرکب از کارشناسان آفریقای جنوبی، زیمبابوه، نامبیا، تانزانیا، اوگاندا، بوتسوانا، سوازیلند، زنگبار، لسوتو و رواندا در ژوئن سال ۱۹۹۸ تشکیل گردید. آنها کارشان را با برگزاری یک دوره آموزشی آغاز نمودند و دومین دوره آموزشی آنها با مساعدت مالی سفارتخانه‌های انگلیس برگزار شد. گروه کاری جنوب اقیانوس آرام، و آسیا در نوامبر سال ۲۰۰۰ در هند تشکیل شد و کارشناسانی از کشورهای استرالیا، چین، هنگ کنگ، هند، ژاپن، نپال، و سریلانکا عضو آن هستند. این گروه کاری با الگو قرار دادن کمیته راهبردی جرایم مربوط به فناوری اطلاعات به منظور ایجاد و هماهنگی میان اقدامات گروههای کاری منطقه‌ای در محل دبیرخانه کل اینترپول تشکیل گردیده است. سازمان پلیس جنایی بین‌المللی جرایم رایانه‌ای را به شرح زیر طبقه‌بندی کرده است: ۱: دستیابی غیرمجاز ۱-۱: نفوذغیرمجاز ۱-۲: شنود غیرمجاز ۱-۳: سرقت زمان رایانه ۲: تغییر داده‌های رایانه‌ای ۲-۱: بمب منطقی ۲-۲: اسب تروا ۲-۳: ویروس رایانه‌ای ۲-۴: کرم رایانه‌ای ۳: کلاه‌برداری رایانه‌ای ۳-۱: صندوقهای پرداخت ۳-۲: جعل رایانه‌ای ۳-۳: ماشینهای بازی ۳-۴: دستکاریها در مرحله ورودی/ خروجی ۳-۵: ابزار پرداخت (نقطه فروش) ۳-۶: سوءاستفاده تلفنی ۴: تکثیر غیرمجاز ۴-۱: بازیهای رایانه‌ای ۴-۲: نرم‌افزارهای دیگر ۴-۳: توپوگرافی نیمه هادی ۵: سابوتاژ رایانه‌ای ۵-۱: سخت‌افزار ۵-۲: نرم‌افزار ۶: سایر جرائم رایانه‌ای ۶-۱: سیستمهای تابلوی اعلانات الکترونیک ۶-۲: سرقت اسرار تجاری ۶-۳: سایر موضوعات قابل تعقیب ۳-۴-۴: طبقه‌بندی در کنوانسیون جرایم سایبرنتیک این کنوانسیون در اواخر سال ۲۰۰۱ به امضای ۳۰ کشور پیشرفته رسیده است و دارای وظایف زیر می‌باشد: هماهنگ کردن ارکان تشکیل دهنده جرم در حقوق جزای ماهوی داخلی کشورها و مسائل مربوطه در بخش جرایم سایبراسپیس. الف: فراهم آوردن اختیارات لازم آیین دادرسی کیفری داخلی برای پی‌جویی و تعقیب چنین جرائمی علاوه بر جرایم دیگر که با استفاده از سیستمهای رایانه‌ای ارتکاب می‌یابند. ب: تدوین سیستم سریع و مؤثر همکاری بین‌المللی ج: کنوانسیون بین‌المللی جرایم رایانه‌ای بوداپست (۲۰۰۱) جرم را موارد زیر تعریف نموده است: - نفوذ غیرمجاز به سیستمهای رایانه‌ای - شنود غیرمجاز اطلاعات و ارتباطات رایانه‌ای - اخلال در داده‌های رایانه‌ای - اخلال در سیستمهای رایانه‌ای - جعل رایانه‌ای - کلاه‌برداری رایانه‌ای - سوءاستفاده از ابزارهای رایانه‌ای - هرزه‌نگاری کودکان - تکثیر غیرمجاز نرم‌افزارهای رایانه‌ای و نقض حقوق ادبی و هنری ۳-۵: شش نشانه از خرابکاران شبکه‌ای ۱: در صورت نفوذ یک خرابکار به شبکهٔ شما ممکن است حساب بانکی‌تان تغییر کند. ۲: خرابکاران شبکه‌ای آن قدر تلاش می‌کنند تا بالاخره موفق به ورود به اینترانت شما شوند. لازم به ذکر است که در برخی موارد در صورتیکه یک خرابکار بتواند به حساب بانکی شما نفوذ کند فایل آن بطور خودکار بسته نمی‌شود. ۳: گاهی اوقات خرابکاران برای نفوذ به یک رایانه ناچارند کد جدیدی به آن وارد کنند. برای این کار لازم است رایانه دوباره راه‌اندازی شود. بنابراین راه‌اندازیهای مجدد رایانه که بطور غیرمنتظره انجام می‌شود، می‌تواند نشانه‌ای از نفوذ خرابکاران شبکه‌ای به رایانه شما باشد. ۴: بعضی اوقات خرابکاران شبکه‌ای تنها با حذف بخشهایی از یک فایل می‌توانند راه نفوذ خود در آن را مخفی نگه دارند. بنابراین قسمتهای حذف شده از یک فایل می‌تواند نشان‌دهندهٔ مسیر نفوذ خرابکاران شبکه‌ای به یک فایل از رایانه باشد. ۵: گاهی با این که انتظار می‌رود ارتباط بین دو رایانه از طریق شبکه، در زمانهایی

مشخص، بسیار کم باشد ترافیک زیادی در آن مسیر ملاحظه می‌شود. چه بسا خرابکاران شبکه‌ای در حال تلاش برای نفوذ به آن سیستمها باشند و همین امر موجب ترافیک سنگین بین آنها شود. ۶: بخشهایی در سیستم هر شرکت وجود دارد که جدا از بقیه سیستم بوده و تنها افراد معدودی به آن دسترسی دارند، گاهی می‌توان خرابکاران شبکه‌ای را در چنین بخشهایی پیدا کرد. ۴: راهکارهای امنیتی شبکه ۴-۱: کنترل دولتی علاوه بر بهره‌گیری از امکانات فنی، روشهای کنترل دیگری نیز برای مهار اینترنت پیشنهاد شده است. در این روش، سیاست کلی حاکم بر کشور اجازه دسترسی به پایگاههای مخرب و ضد اخلاقی را نمی‌دهد و دولت شبکه‌های جهانی را از دروازه اتصال و ورود به کشور با فیلترهای مخصوص کنترل می‌کند. ۴-۲: کنترل سازمانی روش دیگر کنترل سازمانی است که معمولاً سازمان، اداره یا تشکیلاتی که مسئولیت سرویس‌دهی و اتصال شهروندان را به اینترنت به عهده می‌گیرند، خود موظف به کنترل شبکه و نظارت بر استفاده صحیح از آن می‌شود تا با الزامات قانونی و اخلاقی تواماً انجام این وظیفه را تضمین کند. ۴-۳: کنترل فردی کنترل فردی روش دیگری است که قابل انجام است. در این نوع کنترل تمام تضمینهای اجرایی، درون فردی است و شخص با بهره‌گیری از وجدان فردی و مبانی اخلاقی و تعهد دینی، مراقبتهای لازم را در ارتباط با شبکه‌های جهانی به عمل آورد. این اعتقاد و فرهنگ در محدودهٔ خانواده نیز اعمال می‌شود و چه بسا اطرافیان را نیز تحت تأثیر قرار دهد. البته شیوهٔ اخیر در صورتی ممکن خواه بود که واگذاری خط اشتراک IP پس از شناسایی کامل افراد و با ملاحظه خصوصیات اخلاقی آنان انجام پذیرد. در غیر این صورت تصور اعمال چنین کنترلی از سوی تک تک افراد جامعه صرفاً در حد آرزو باقی خواهد ماند. آرزویی که نمی‌تواند بسیاری از تأثیرات سوء این شبکه را از بین ببرد و آن را بسوی شبکه سالم سوق دهد. ۴-۴: تقویت اینترانت‌ها از سوی دیگر تقویت شبکه‌های داخلی که به اینترانت معروف است می‌تواند نقش بسزایی در کاهش آلودگیهای فرهنگی و اطلاعاتی اینترنت یاری کند. قرار دادن اطلاعات مفید اینترنت به صورت ناپیوسته و روی شبکه‌های داخلی یا اینترانتها، علاوه بر ارائهٔ خدمات و اطلاع‌رسانی سالم، پس از چندی، بایگانی غنی و پرباری از انواع اطلاعات فراهم آمده از چهار گوشه جهان را در اختیار کاربران قرار می‌دهد که با افزایش اطلاعات داخلی و یا روزآمد کردن آن، به عنوان زیربنای اطلاعاتی کشور قابل طرح می‌باشد. به هر حال سرعت بالا و هزینه کم در استفاده از اینترانتها، دو عامل مورد توجه کاربران به شبکه‌های داخلی است که به نظر نمی‌رسد محمل مناسبی برای اطلاعات گزینش شده اینترنت باشد. ۴-۵: وجود یک نظام قانونمند اینترنتی مورد دیگر که کارشناسان از آن به عنوان پادزهر آسیبهای اینترنتی از قبیل تهاجم فرهنگی، اطلاعات نادرست و یا پیامدهای ضد اخلاقی نام می‌برند، وجود یک نظام قانونمند اینترنتی در جامعه است که ادارهٔ آن از سوی یک متولی قدرتمند و کاردان می‌تواند اینترنت سرکش و افسار گسیخته را مهار کند و از آن به نحو شایسته بهره‌برداری نماید. این نظام اگر با یک نظام حقوقی و دادرسی جامع و عمیق توأم باشد، موارد تخلف و سوءاستفاده از این ابزار به راحتی قابل تشخیص و پیگیری قضایی خواهد بود. در این صورت امکان سوءاستفاده و تأثیرپذیری از فرهنگهای بیگانه که عموماً مغایر با اصول اخلاقی ماست، به طرز چشمگیری کاهش می‌یابد. ۴-۶: کار گسترده فرهنگی برای آگاهی کاربران اما بهترین روش، کار گستردهٔ فرهنگی، برای آگاهی کاربران است. کافی است که آنها آگاه شوند که گرایش و ارتباط با پایگاههای غیرمتعارف جز ضلالت و تباهی ثمره‌های ندارد. باید تقوای درونی و اعتقادات دینی کاربران را رشد داد و آنها را تقویت کرد. بنابراین بهترین بارو (فایروال) برای ممانعت از خطرات اینترنت و جلوگیری از تأثیر ابعاد منفی آن، وجدان درونی و ایمان هر نسل است که بخشی از این ایمان را علمای دین باید در وجود نسل جوان و انسانهای این عصر بارور سازند. ۴-۷: فایروالها در حقیقت فایروال یا بارو شبکه‌های کوچک خانگی و شبکه‌های بزرگ شرکتی را از حملات احتمالی رخنه‌گرها (هکرها) و وب سایتهای نامناسب و خطرناک حفظ می‌کند و مانع و سدی است که متعلقات و دارایهای شما را از دسترس نیروهای متخاصم دور نگاه می‌دارد. بارو یک برنامه یا وسیله سخت‌افزاری است که اطلاعات ورودی به سیستم رایانه و شبکه‌های اختصاصی را تصفیه می‌کند. اگر یک بسته اطلاعاتی ورودی به وسیلهٔ فیلترها نشان‌دار شود،

اجازه ورود به شبکه و رایانه کاربر را نخواهد داشت. به عنوان مثال در یک شرکت بزرگ بیش از صد رایانه وجود دارد که با کارت شبکه به یکدیگر متصل هستند. این شبکهٔ داخلی توسط یک یا چند خط ویژه به اینترنت متصل است. بدون استفاده از یک بارو تمام رایانه‌ها و اطلاعات موجود در این شبکه برای شخص خارج از شبکه قابل دسترسی است و اگر این شخص راه خود را بشناسد می‌تواند یک یک رایانه‌ها را بررسی و با آنها ارتباط هوشمند برقرار کند. در این حالت اگر یک کارمند خطایی را انجام دهد و یک حفره امنیتی ایجاد شود، رخنه‌گرها می‌توانند وارد سیستم شده و از این حفره سوء استفاده کنند. اما با داشتن یک بارو همه چیز متفاوت خواهد بود. باروها روی خطوطی که ارتباط اینترنتی برقرار می‌کنند، نصب می‌شوند و از یک سری قانونهای امنیتی پیروی می‌کنند. به عنوان مثال یکی از قانونهای امنیتی شرکت می‌تواند به صورت زیر باشد: از تمام پانصد رایانه موجود در شرکت فقط یکی اجازه دریافت صفحات ftp را دارد و بارو باید مانع از ارتباط دیگر رایانه‌ها از طریق ftp شود. این شرکت می‌تواند برای وب سرورها و سرورهای هوشمند و غیره نیز چنین قوانینی در نظر بگیرد. علاوه بر این، شرکت می‌تواند نحوهٔ اتصال کاربران- کارمندان به شبکه اینترنت را نیز کنترل کند به عنوان مثال اجازه ارسال فایل از شبکه به خارج را ندهد. در حقیقت با استفاده از بارو یک شرکت می‌تواند نحوهٔ استفاده از اینترنت را تعیین کند. باروها برای کنترل جریان عبوری در شبکه‌ها از سه روش استفاده می‌کنند: ۱:Packet Filtering یک بسته اطلاعاتی با توجه به فیلترهای تعیین شده مورد تحلیل و ارزیابی قرار می‌گیرند. بسته‌هایی که از تمام فیلترها عبور می‌کنند به سیستمهای موردنیاز فرستاده شده و بقیه بسته‌ها رد می‌شوند. ۲: Prxy Services اطلاعات موجود در اینترنت توسط بارو اصلاح می‌شود و سپس به سیستم فرستاده می‌شود و بالعکس. ۳: Stateful Inspectin این روش جدید محتوای هر بسته با بسته‌های اطلاعاتی ویژه‌ای از اطلاعات مورد اطمینان مقایسه می‌شوند. اطلاعاتی که باید از درون بارو به بیرون فرستاده شوند، با اطلاعاتی که از بیرون به درون ارسال می‌شود، از لحاظ داشتن خصوصیات ویژه مقایسه می‌شوند و در صورتی که با یکدیگر ارتباط منطقی داشتن اجازه عبور به آنها داده می‌شود و در غیر اینصورت امکان مبادلهٔ اطلاعات فراهم نمی‌شود. ۴-۸: سیاست‌گذاری ملی در بستر جهانی واقعیت این است که بدون ملاحظه چند الگوی ملی در برخورد با اینترنت نمی‌توان از سیاست‌گذاری مبتنی بر فهم جهانی سخن گفت. لذا معرفی اجمالی چند نمونه که با سه رویکرد تحول‌گرا، ثبات‌گرا، و اعتدال‌گرا تناسب بیشتری دارند ضروری است. ۴-۸-۱: الگوی آمریکایی اینترنت در آمریکا هم به عنوان تهدید امنیتی و هم به عنوان بزرگترین فرصت ملی تلقی می‌شود. کاخ سفید در پنجم ژانویه سال ۲۰۰۰ بیانیه‌ای را تحت عنوان «استراتژی امنیت ملی در قرن جدید» منتشر کرد. در این بیانیه ضمن برشمردن منافع حیاتی آمریکا، از اینترنت به عنوان مهمترین ابزار دیپلماسی مردمی نام برده شده است. پیشرفت جهانی تکنولوژیهای آزاد و اطلاع‌رسانی چون اینترنت توانایی شهروندان و مؤسسات را برای تأثیرگذاری بر سیستمهای دولتها تا حد غیرقابل تصوری بالا برده است. دیپلماسی مردمی یعنی تلاش برای انتقال اطلاعات و پیامهایمان به مردم جهان یکی از ابعاد مهم استراتژی امنیت ملی ماست. برنامه‌ریزی ما باید به گونه‌ای باشد که توانایی ما را برای اطلاع‌رسانی و تأثیرگذاری بر ملل کشورهای دیگر در جهت منافع آمریکا تقویت کند و گفتگوی میان شهروندان و مؤسسات آمریکایی را با نظائرشان در دیگر کشورها توسعه ببخشد. توسعهٔ اینترنت در داخل و استفاده از آن برای تأثیرگذاری بر دیگران بخش مهمی از سیاستهای استراتژیک آمریکاست. افزایش جرایم رایانه‌ای در آمریکا از جمله حمله به سایتهای Amazn و yah، ریس FBI را واداشت تا در فوریه ۲۰۰۰ از کنگره بخواهد ۳۷ میلیون دلار به بودجه ۱۰۰ میلیون دلاری وزارت دادگستری برای مبارزه با جرایم رایانه‌ای بیفزاید و کلینتون در همان ماه درخواست یک بودجه ۹ میلیون دلاری برای تأسیس مرکز امنیت ملی، مشارکت شرکتهای اینترنتی و تجارت الکترونیک علیه حمله‌کنندگان به سایتهای رایانه‌ای را به کنگره ارائه داد. ۴-۸-۲: الگوی فلسطین اشغالی این کشور در فاصله سال ۱۹۹۴ تا ۲۰۰۰ تبدیل به یک غول صنعت اینترنت شده است این کشور در سطح داخلی چنین سیاستهایی اتخاذ کرده است: - اختصاص ۳٪ از GDP کشور معادل ۹۰ میلیارد دلار به تحقیق و توسعه در زمینه تکنولوژی

پیشرفته – آموزش مهارتهای پیشرفته رایانه‌ای در دوران سربازی و تداوم آموزش در دوران خدمت احتیاط. تولید Checkpint با پیشینه و ریشه در کاربردهای نظامی و به عنوان یکی از قابل اطمینان‌ترین و پرفروشترین باروهای جهان که کشورهای عربی نیز به آن متکی هستند، یکی از سیاستهای جهانی کشور مذکور است. ۴–۸–۳: الگوی چینی چین رسماً اعلام کرده است به دنبال برقراری توازن میان جریان آزاد اطلاعات و صیانت فرهنگ و ارزشهای اجتماعی خود می‌باشد. پیتر پیت معاون شرکت دولتی اینترنت چین گفته است: ما علاقه به قمار، پورنوگرافی و موارد حساسیت برانگیز سیاسی نداریم اما حتی با محتوای فیلتر شده، اینترنت را تنها و مهمترین نیرویی می‌دانیم که درهای چین را بر روی دنیا می‌گشاید راه تغییرات اقتصادی را هموار می‌کند. در اجرای این استراتژی چین اقدامات زیر را انجام داده است: – سرمایه‌گذاری عظیم در صنایع الکترونیک، مخابرات و رایانه – اقدامات وسیع و سازمان یافته برای تکثیر، شکستن قفل و شبیه‌سازی نرم‌افزارها و برنامه‌های کاربردی رایانه‌ای و تقویت صنعت عظیم نرم‌افزار در چین – تأسیس شرکت دولتی اینترنت چین و انحصار ورود اینترنت به کشور از طریق این شرکت – همکاری شرکت با غولهای اینترنتی آمریکا برای ایجاد خدمات مبتنی بر وب با استانداردهای کیفی AQL و استانداردهای اخلاقی و قانونی چین – جلب همکاری AQL و Netscape برای تولید یک پویشگر اینترنت به زبان چینی – هزینه عظیم برای فیلتر کردن محتوای نامناسب اخلاقی و سیاسی در اینترنت ۴–۸–۴: الگوی کشورهای عربی حاشیه خلیج فارس تقریباً در تمام کشورهای حاشیه خلیج فارس کنترل قوی دولتی بر محتوا و توزیع اطلاعات وجود دارد. این کنترلها به علل مذهبی، سیاسی و فشارهای داخلی صورت می‌گیرد. روش اصلی کنترل اطلاعات الکترونیک، در این کشورها انحصار مخابرات در شرکتهای دولتی است. یکی از پیامدهای اصلی این کنترل دولتی تأخیر در رسیدن اینترنت و کندی در همه‌گیر شدن آن در این کشورهاست. در کشورهای عربی منطقه خلیج فارس دولت و بخش دانشگاهی عامل گسترش اینترنت نبوده‌اند، در عوض تجارت آزاد و بازرگانان خارجی مقیم، بیشترین مشتاقان و کاربران اینترنت را تشکیل می‌دهند. در واقع هیچ شخص، سازمان، و تجارت مدنی نمی‌تواند بدون اتکاء به وب و اینترنت در رقابت جهانی برای دسترسی به منابع طبیعی و اقتصادی خلیج فارس به بقاء خود ادامه دهد. اقتصاد وابسته و ادغام منطقه در اقتصاد جهانی، اتصال به اینترنت را گریزناپذیر می‌کند. بازار مصرف اینترنت در کشورهای عربی خلیج فارس، اساساً تجاری است. کشورهای خلیج فارس از نظر سیاستگذاری در مورد اینترنت روی یک طیف قرار دارند که یک طرف آن عراق و طرف دیگر آن یمن و قطر است. عراق تاکنون رسماً به اینترنت متصل نشده است و مودمهای شخصی را ممنوع کرده است. از طرف دیگر یمن و قطر با حذف هرگونه کنترلی بر روی اینترنت و سرمایه‌گذاری برای گسترش زیر ساختها به منافع اینترنت بیشتر از خطرات آن بها داده‌اند. کویت با برخورداری از سیستم مخابراتی کاملاً پذیرفته در سال ۱۹۹۴ ارائه خدمات عمومی اینترنت را آغاز کرد. وزارت مخابرات کویت امتیاز ISP را ابتدا به گلف نت و سپس به یک کمپانی دیگر واگذار کرد. گلف نت از طریق ماهواره Sprint به آمریکا متصل است. دانشجویان کویتی بدون هیچ گونه هزینه به اینترنت دسترسی دارند عمان به واسطه جبران عقب ماندگی نسبی از دیگر کشورهای خلیج فارس، بازسازی سیستم مخابراتی را در اولویتهای خود قرار داده است. در چارچوب یک طراحی ملی برای زیرساختها و خدمات مخابراتی GT سازمان عمومی مخابرات طرحی را برای سال ۲۰۰۰ ارائه کرد که در آن امکان دسترسی به هر اطلاعی در هر زمانی در هر کجا و به هر شکل برای دولت و بخش خصوصی پیش‌بینی شده‌اند. GT در سال ۱۹۹۵ یک مناقصه بین‌المللی را برای ISP اعلام کرد. در این مناقصه Sprint آمریکا برگزیده شد و علاوه بر ایجاد سایت، اداره آن را به مدت ۵ سال تعهد کرد. دسترسی عمومی به اینترنت از دسامبر ۱۹۹۶ فراهم شد و کاربری تجاری آن به سرعت توسعه یافت. قطر مدرن‌ترین شبکهٔ مخابراتی منطقه را ایجاد کرده است و انحصار مخابرات دولتی توسط Qtel اعمال می‌شود که تنها ISP کشور را دارا می‌باشد، ولی بررسیهایی به منظور خصوصی‌سازی، ولی به صورت غیررقابتی در حال انجام است. دولت در کنار اینترنت، یک سیستم اطلاعاتی ژئوفیزیکی را با اهداف توسعه بخشی عمومی و خصوصی به سرعت توسعه داده است ولی آموزش عالی و

دانشگاه بهره چندانی از آن نبرده‌اند. قطر تنها کشور حاشیه خلیج فارس است که خود را منطقه فارغ از سانسور اطلاعات معرفی کرده و هیچ‌گونه کنترلی بر محتوای اینترنت اعمال نمی‌کند. تنها حساسیت دولت مسأله پورنوگرافی است که با استفاده از باروها تا حدی کنترل می‌شود. امارات متحده عربی از سال ۱۹۹۵ ارزان قیمت‌ترین و نظارت شده‌ترین خدمات اینترنت منطقه را ارائه می‌کند و نسبت به جمعیت دارای بیشترین تعداد رایانه متصل به اینترنت است. دولت و بخش تجاری و دانشگاهها همه پشتیبان اینترنت هستند و از آن به خوبی بهره‌برداری می‌کنند. وزارت مخابرات با راه‌اندازی چند پراکسی سرور گران قیمت تمام تبادلات داده‌ها را فیلتر و کنترل می‌کند. در عین حال امارات شاهد بیشترین مباحثات افکار عمومی درباره خطرات استفاده از اینترنت بوده است. عربستان سعودی بزرگترین و محافظه‌کارترین کشور منطقه است و به موارد غیراخلاقی و فعالیتهای تبعیدیان خارج نشین بسیار حساس است. هنوز اینترنت در سعودی توسعهٔ چندانی پیدا نکرده است و دسترسی عمومی در اینترنت همگانی نشده است، اما برخی از بخشهای دولتی، پزشکی و دانشگاهی از طریق یک اتصال ماهواره‌ای به آمریکا از خدمات اینترنت استفاده می‌کنند. سعودی گران‌ترین طرح مطالعاتی در مورد کاربردها و استلزامات اینترنت را به مدت دو سال پیگیری کرد و در نتیجه روش مدیریت کاملاً ـ متمرکز برای ورود اینترنت به کشور و کنترل کل ورودی توسط یک باروی ملی برای جلوگیری از دسترسی به محتوای نامناسب از طرف دولت پذیرفته شد. ۵- اینترنت و امنیت فرهنگی ایران در بحبوحه جنگ نگرشها، این واقعیت را نباید از نظر دور داشت که در حال حاضر اینترنت در ایران نقش بسیار مهمی از لحاظ امنیت فرهنگی ایفاء می‌کند. از نظر علمی افزایش توانایی دسترسی دانشجویان، اساتید، و محققان ایرانی به منابع الکترونیک و تماسهای علمی با دانشمندان دیگر کشورها کاملاً مرهون اینترنت دانشگاهیان است. از نظر افزایش توان کسب آگاهیهای سیاسی و اجتماعی و دریافت آراء مختلف و امکان گفتگو نمی‌توان نقش اینترنت را انکار کرد. امروزه سایتهای مختلف ایرانی با تشکیل گروههای مباحثاتی بسیار جدید در مورد مسائل جهانی و ملی عرضه وسیعی را برای آگاهی جویی و اعلام نظرهای تخصصی و عمومی فراهم کرده‌اند (سیک، ۱۹۹۹). پیگیری نظرسنجی‌های اینترنتی در مورد انتخاب مجلس ششم، انتخاب رئیس مجلس، فایده یا ضرر ارتباط با آمریکا، انتخاب مهمترین شخصیت قرن اخیر ایران، نشان می‌دهد که اینترنت برای ایرانیان امکانات کاملاًمساعدی برای ابراز آزادانه عقاید و مشارکت سیاسی و فرهنگی فراهم آورده است. حتی برخی احزاب و داوطلبان نمایندگی برای تبلیغات انتخاباتی خود، از اینترنت استفاده کرده‌اند. به این ترتیب می‌توان نقش مهمی برای اینترنت در گسترش آزادیها و مشارکت سیاسی و دمکراسی فرهنگی قائل شد. ۵-۱: معیارهای امنیت فرهنگی در سیاستگذاری برای تحلیل فرآیند سیاستگذاری در مورد اینترنت در ایران، پاسخ به سؤالاتی در مورد آزادی بیان، کنترل جریان اطلاعات، قوانین مربوط و در یک بیان نظریه هنجاری حاکم بر رسانه‌های جدید ضروری است. این سؤالات به ۵ حیطه اصلی قابل تحلیل است: حق ارتباط خصوصی حق ارتباط ناشناس حق رمزگذاری در ارتباط معافیت کانال ارتباطی از مسئولیت محتوی دسترسی عمومی و ارزان با توجه به تحقیق محسنیان راد (۱۳۷۶) نظریه حاکم بر رسانه‌های مرسوم در ایران در سال ۱۳۷۶، آمیزه‌ای از نظریه مسئولیت اجتماعی، توسعهٔ بخش و ایدئولوژیک بوده است. تغییرات سیاسی سال ۷۶ به بعد نقش نظریه مسئولیت اجتماعی را تقویت کرده است. ولی در مورد اینترنت وضع کاملاً متفاوت است و حاکمیت تئوری آزادی‌گرا بر دسترسی و انتشار از طریق اینترنت کاملاً ـ ملموس است. تا اواخر نیمه اول سال ۱۳۸۰، دولت هیچ گونه نظارت و دخالت ملموسی در مورد آن نداشته است. زیرا: ۱. قوانین مربوط به مطبوعات که عمده‌ترین قانون در حوزهٔ محدوده محدودیتهای آزادی بیان است شامل گفتار روی شبکه نمی‌شود. ۲. افراد، سازمانها و شرکتها امکان دسترسی به سرویس دهندگان اینترنت را از طریق خطوط تلفن دارند. ۳. برای دسترسی به اینترنت هیچ گونه مجوز دولتی لازم نیست. ۴. دسترسی به اینترنت با پست یا پست الکترونیک نیاز به هیچ گونه تأییدی از طرف هیچ سازمان دولتی ندارد. ۵. هیچ دستورالعمل یا بخشنامه‌ای وجود ندارد که سرویس دهندگان را موظف کند اطلاعات مربوط به مشترکان، کاربران و محتوای داده‌های تبادل شده را به سازمانهای دولتی ارائه دهند. ۶. هیچ قانون یا دستورالعملی برای

منع رمزگذاری محتوای داده‌های مبادله شده وجود ندارد. ۷. هیچ قانونی وجود ندارد که سرویس‌دهندگان ملزم به کنترل محتوا نماید. ۸. هیچ سیاست و اقدام مشخصی در مورد سانسور یا بلوک کردن سایتها، گروههای مباحثاتی و آدرسهای پست الکترونیکی وجود ندارد و ایران فاقد یک بارو و سیستم فیلترینگ ملی و مرکزی است. ۹. هیچ قانونی وجود ندارد که سرویس‌دهندگان را مسئول محتوای سایتهای روی سرویس بداند. ۱۰. کافه‌های اینترنتی به سرعت در حال رشد است و هیچ قانون خاصی برای نحوهٔ تأسیس و نحوهٔ اداره وجود ندارد، این کافه‌ها تابع قانون اماکن عمومی هستند. ۱۱. خدمات اینترنت در ایران به سرعت ارزان شده است و دولت برای دسترسیهای دانشگاهی سوبسید قابل ملاحظه‌ای را پذیرفته است. سیاست گسترش فیبر نوری و افزایش ظرفیت تبادل بین‌المللی داده‌ها از سیاستهای جاری دولت است. ۵-۲: مشکلات فعلی سیاستگذاری در امنیت فرهنگی و اینترنت در جریان سیاستگذاری برای اینترنت در کشور ما موانع جدی وجود دارد. این موانع را می‌توان به شرح زیر مرتب کرد: ۱. فقدان استراتژی فرهنگی کلان در مورد صنایع فرهنگی جدید ۲. فقدان سیاست ملی مخابراتی - روشن نبودن اولویت‌بندی در مورد گسترش تلفن ثابت، همراه و مخابرات داده‌ها - روشن نبودن میزان ظرفیت دولت در پذیرش مشارکت بخش خصوصی در وارد کردن و توزیع اینترنت ۳. فقدان سیاست روشن گمرکی در مورد مجاز یا ممنوع بودن واردات تجهیزات، دریافت و ارسال ماهواره‌ای برای خدمات اینترنت ۴. وجود رقابت تخریبی میان ارگانهای عمومی متولی اینترنت در کشور از جمله فیزیک نظری، شرکت مخابرات، صدا و سیما ۵. فقدان سیاست ملی اطلاع‌رسانی علی‌الرغم تشکیل شورای عالی اطلاع‌رسانی این شورا به سیاست‌گذاری تفصیلی و اعلام شده‌ای در زمینهٔ اطلاع‌رسانی دست نیافته است. وجود مدعیان و متولیان متعدد در مدیریت ملی اطلاعات و عدم تفکیک وظایف آنها موجب کندی و بلکه عقب‌ماندگی جدی ایران در تولید و سازماندهی اطلاعات الکترونیک شده است. امروزه به علت عدم سازماندهی اطلاعات علمی کشور، دسترسی به کتابخانه کنگرهٔ آمریکا بسیار ساده‌تر و مفیدتر از دسترسی به کتابخانه‌های ملی، مجلس و دانشگاه تهران است. ۶. فقدان سیاستهای نظارتی و امنیتی هم اکنون بایستی روشن شود که مسئول حفاظت از داده‌های موجود در سامانه‌های نظامی، امنیتی، اقتصادی کشور کیست؟ چه سازمانی مسئول جلوگیری، پیشگیری و پیگیری حملات الکترونیکی و نقش امنیت سامانه‌های ملی است؟ چه سازمانی متولی سیاستگذاری و تعیین موارد ممنوعه در تبادل داده‌ها است؟ کدام سازمان مسئول نظارت بر کیفیت فرهنگی و محتوای سایتهای تولیدشده و قابل دسترس در کشور است؟ ۵-۳: ملاحظات فرهنگی در سیاستگذاری به نظر می‌رسد ملاحظات اساسی فرهنگی در سیاستگذاری آتی در مورد اینترنت در ایران به شرح زیر می‌باشد: - گسترش اینترنت در کشور ایران باید به گونه‌ای باشد که به خلاقیت‌گستری مدد رسانده، نه اینکه موجبات خلاقیت‌زدایی را فراهم آورد. سیاستگذاری در مورد توسعه اینترنت نباید به توسعه مصرف یا باز تولید محتوای آن محدود شود

فایروال چیست؟

مدلهای TCP/IP , SI چیستند؟ دانستن این که یک فایروال چگونه کار می کند به شما کمک می کند که روابط لایه های شبکه را بهتر متوجه شوید طراحان شبکه یک ساختار هفت لایه ای برای شبکه تعیین کرده اند که هر لایه مسئولیت خاص خود را دارا می باشد این لایه ها شبکه را قادر می سازند که پروتکلهای شبکه را با لایه های سخت افزاری همگام کنند در یکشبکه معین یک پروتکل تا لایه بالایی سخت افزار بیشتر نمی تواند وارد شود زیرا لایه سخت افزار جدای از لایه پروتکل می باشد به همین صورت که یک کابل فیزیکی نمی تواند بیشتر از لایه یک حرکت کند TCP /IP قدیمی تر از مدل SI است اما استاندارد این دو شبیه به هم نیست در TCP /IP۴ لایه اول دقیقا مطابق مدل SI هستند فایروالها در لایه های مختلف فعالیت می کنند تا بتوانند از ضوابط مختلفی برای مصدور کردن ترافیک استفاده کنند پایین ترین لایه ای که فایروالها در آن کار می کنند لایه سوم است که در مدل SI لایه شبکه و در TCP /IP لایه IP می باشد کار این لایه مسیر یابی و ارسال بسته ها به مقصد می باشد در این لایه فایروال

میتواند تشخیص دهد که بسته از چه مبدا ای آمده است اما نمی تواند محتویات بسته و یا اینکه بسته به چه بسته های دیگری وابسته است را مشخص کندفایروال در لایه ترانسپورت راجع به بسته کمی بیشتر اطلاعات دارد و قادر است که اجازه یا عدم اجازه دسترسی با قوانین و ضوابط در سطوح بالاتری را صادر کند در لایه نرم افزار فایروال قدرت بسیار زیادی در صدور مجوز ها برای بسته ها دارد و مشکل وقتی پدیدار می شود که تابع فایروال در داخل شبکه در سطح بالاتری نسبت به لایه برنامه ها قرار گیرد که این هیچ الزامی ندارد و کارکردن فایروال در سطوح پایینی شبکه باعث امنیت بیشتر آن می شود اگر یک نفوذ گر نتواند سه مرحله قبل را متعلق به دخود کند مسلما نمی تواند کنترل سیستم عامل را در دست بگیرد فایروالهای جدید و پیشرفته کل ترافیک شبکه را در خود ذخیره کرده و اجازه نمی دهند که آنها مستقیما به شبکه TCP / IP دسترسی پیدا کنند و این کار را برای یک نفوذ گر جهت نفوذ به سیستم و باز کردن درب پشتی برای نفوذ بعدی مشکل می نماید

آموزش شبکه LAN

آموزش شبکه LAN LAN چیست؟ شبکه چیست شبکه مجموعه‌ای از سرویس دهنده‌ها و سرویس گیرنده‌های متعددی می‌باشد که‌به یکدیگر متصل هستند. در این بین سرویس دهنده‌ها (server) نقش سرویس دهنده و خدمات دهی وسرویس گیرنده‌ها (Client) نقش سرویس گیرنده یا همان مشتری را بازی می‌کنند. انواع شبکه شبکه‌ها را می‌توان به دو دسته‌ی «شبکه‌های محلی LAN و شبکه‌های بزرگ‌تر از آن WAN) تقسیم کرد. شبکه‌های محلی Lcal Area Netwrk این نوع شبکه‌ها به شبکه‌های((LAN) معروف هستند. شبکه های محلی معمولا میزبان ۲ تا ۲۰کامپیوتر و در غالب Wrk Grup میباشند. سرعت این نوع شبکه بسیار زیاد است (معمولا ۱۰۰MB Per Sec) و می توان حجم داده های بالا را در مدت بسیار کم انتقال داد. شبکه‌های گسترده Wide Area Netwrk این نوع شبکه ها به شبکه های WAN معروف هستند. این شبکه ها بزرگتر از شبکه های LAN و اغلب برای امور عمومی از آن استفاده می شود. ازجمله این شبکه ها میتوان شبکه های VAN و یا شبکه های بزرگتر مانند Internet و.. را نام برد. سرعت انتقال داده ها در این نوع شبکه ها نسبت به LAN (در ایران) بسیار ناچیز میباشد. این سرعت به خاطر استفاده از خطوط ۵۶K است. البته می توان با استفاده از خطوط DSL یا ISDN و یا بی سیم Wire Less سرعت این ارتباط را به اندازه ۵۱۲ k , ۲۵۶ k, ۱۲۸K یا بالاتر افزایش داد. Internet Prtcl: IP IP یک عدد ۳۲ بیتی (bit) است که پس از اتصال به شبکه ... , LAN , Internet) به ما متعلق می‌گیرد. شکل کلی IP را می توان به صورت http://www.xxx.yyy.zzz در نظر گرفت که با هر بار اتصال به اینترنت به صورت Dial Up این عدد تغییر می کند. به عنوان مثال در حال حاضر IP ما ۲۱۳.۱۵۵.۵۵.۱۰۴ است اما در اتصال بعدی ممکن است این عدد به ۲۱۳.۱۵۵.۵۵.۲۰ تغییر کند. IP چه کاربردی دارد؟ IP به عنوان یک شناسنامه در شبکه است و کاربردهای بسیاری دارد .برای توصیف کامل IP نیاز به شرح TCP/IP است که بعدا به آن اشاره خواهیم کرد. همان طور که در جامعه شناسنامه وسیله ای برای احراز هویت ماست و بدون آن جزو آن جامعه محسوب نمی شویم ، IP نیز وسیله ای برای شناسایی ما در شبکه است و امکان اتصال به شبکه بدون آن وجود ندارد. به طور مثال هنگامی که در شبکه مشغول چت (Chat) هستیم ، کامپیوتر شما دارای یک IP می باشد. و جملاتی را که شما تایپ می کنید به وسیله مسیر یابها (Ruter) مسیر یابی (Ruting) شده و به کامپیوتر شخص مقابل میرسند و متنی را هم که شخص مقابل تایپ میکند روی IP شما فرستاده می شود. خط فرمان در ویندوز چیست؟ خط فرمان یا همان" Cmmand Prmpt "در ویندوز نوعی شبیه ساز سیستم عامل Ds در ویندوز است که فایلهای اجرایی" exe,cm "در آن اجرا می شود. خط فرمان ویندوز دستورات بسیار زیاد و کاربردی دارد که به مرور زمان انها را خواهیم آموخت. دسترسی به خط فرمان در ویندوز: دسترسی به خط فرمان به دو روش میسر است. روش اول : روی Start Menu کلیک کرده و گزینه Run را انتخاب می کنیم . سپس در پنجره ظاهر شده اگر ویندوز

شما ME/۹۸ باشد عبارت" Cmmand "و اگر XP/۲۰۰۰/۲۰۰۳ باشد عبارت" CMD "را تایپ می کنیم هم اکنون محیط Cmmand Prmpt در جلوی شما قرار دارد! روش دوم : با طی کردن مسیر Start> Prgrams>Accessries و کلیک کردن برروی Cmmand Prmpt این محیط برای شما باز میشود. ادامه مبحث IP : چگونه IPخود را بدست آوریم : برای بدست آوردن IP خود در سیستم عامل ویندوز کافی است همان طور که در بالا توضیح داده شد به محیط Cmmand Prmpt رفته و عبارت " IPCNFIG " را تایپ کنیم. به طور مثال پس از اجرای دستور به نتایج زیر می رسید : Windws IP Cnfiguratin ۰ Ethernet adapter: IP Address. . . . . : ۲۱۳.۱۵۵.۵۵.۲۳۲ Subnet Mask . . . . . : ۲۱۳.۱۵۵.۵۵.۲۳۲ Default Gateway . . . . . : ۲۵۵.۲۵۵.۲۵۵.۰ فعلا تنها به سطر IP Address که با رنگ قرمز مشخص شده است توجه کنید (Default Gateway و Subnet Mask) بعدا برسی خواهد شد. ملاحظه میکنید که IP ما۲۱۳.۱۵۵.۵۵.۲۳۲ است. آدرسهای IP به چند دسته تقسیم می شوند؟ آدرسهای IP به پنج کلاس A,B,C,D,E تقسیم می شوند. از بین این کلاسها تنها کلاسهای A,B,C کاربرد دارند که به شرح آنها می پردازیم . کلاس A : تمام IP هایی که www آنها (در درس قبل شکل کلی IP را به صورت http://www.xxx.yyy.zzz معرفی کردیم) بین ۱ تا ۱۲۶ است ، جزو کلاس A محسوب می شوند. به عنوان مثال : ۱۱۲.۱۰.۵۷.۱۳ یک IP کلاس A است. این کلاس ویژه پایگاهای بزرگ اینترنتی است. کلاس B : تمام IP هایی که WWW آنها بین ۱۲۸ تا ۱۹۱ می باشد را شامل می شود. مانند IP ی ۱۷۲.۱۵۵.۵۵.۷۳ که جزو کلاس B است. کلاس C : این کلاس تمام IP هایی که WWW آنها بین ۱۹۲ تا ۲۲۳ است را شامل می شود: مانند ۲۱۳.۱۳۳.۵۲.۱۳۸ که جزو کلاس C محصوب می شود. تحلیل IP : همان طور که گفته شد IP یک عدد ۳۲ بیتی است. هم اکنون این گفته را کاملتر شرح داده و مطلب را بازتر می کنیم/ درک این قسمت از مطلب نیازمند دانستن مفاهیم Bit و Byte است . این در حقیقت واحدهای اندازه گیری حافظه کامپیوتر هستند که در پایین آنها را شرح می دهیم : BIT: به کوچکترین واحد اندازه گیری حافظه کامپیوتری می گویند. Byte : به مجموع ۸ بیت ، یک بایت می گویند. بنابر این نتیجه می گیریم ۳۲ بیت همان ۴ بایت در مبنای اعشاری (مبنای ۱۰) است و برای این که کامپیوتر اعداد را در مبنای ۲ در نظر می گیرد آن را به صورت Binary (مبنای ۲) می نویسیم. برای اینکه این مفاهیم را بهتر متوجه شوید آنها را در جدول برسی می کنیم. IP از چند قسمت تشکیل شده است؟ IP از دو قسمت Net ID و Hst ID تشکیل شده است و مقادیر بیت ها در این دو قسمت در کلاسهای مختلف IP متفاوت است. Net ID در واقع شناسه شبکه و Hst ID شناسه میزبان در IP است. بررسی Net ID در کلاساهی مختلف: Net ID در کلاس A به صورت http://www.۰.۰.۰ یعنی تنها www را شامل می شود. در کلاس B به صورت : http://www.xxx.۰.۰ است یعنی http://www.xxx در واقع Net Id می باشد. و در کلاس C به صورت : http://www.xxx.yyy.۰ است یعنی NetID .. این رودیگه باید فهمیده باشید چیه) ; کلاس A : در کلاس Net ID : A هشت بیت است و Hst ID آن ۲۴ بیت که مجموعا ۳۲ بیت می شود. این کلاس می تواند ۱۶.۷۷۷.۱۴ میزبان (Hst) داشته باشد یعنی ۱۶.۷۷۷.۱۴ IP که زیر مجموعه آن قرار می گیرند. به عنوان مثال http://www.۴۴.۴.۱۳ که ۴۴.۴.۱۳ یکی از میزبان ها (Hst) می باشد. کلاس B : در کلاس NetID : B از هشت بیت به شانزده بیت افزایش می یابد و فضا را برای hst ID کمتر می کند، به همین دلیل IP های زیر مجموعه آن به ۵۶.۵۳۴ کاهش می یابد. به عنوان مثال http://www.xxx.۵۵.۱۳۷ : IP که ۵۵.۱۳۷ یکی از میزبانهاست . کلاس NetID : C باز هم بزرگتر شده و از ۱۶ بیت در کلاس B به بیست و چهار افزایش می یابد و Hst ID به کوچکترین مقدار خود یعنی هشت بیت می رسد. این کلاس تنها ۲۴۲ IP را پشتیبانی می کند. به عنوان مثال http://www.xxx.yyy.۹۳ که در آن ۹۳ یکی از میزبانهاست. نکات مهم درس : ۱- سعی کنید بیشتر در محیط Cmmand Prmpt کار کنید تا به آن عادت کرده و دست خود را در اجرای دستورات سریع تر کنید. سرعت در اجرای دستورات هنگام Hack کردن بخصوص Client بسیار مهم است. ۲- با

کمی دقت حتما متوجه می شوید که IP ای که www آن ۱۲۷ باشد در هیچ یک از کلاسهای مطرح شده وجود ندارد. در حقیقت IP ی ۱۲۷.۰.۰.۱ از قبل برای کامپیوتر خودمان رزرو شده و به آن Lcal Hst می گویند. ۳- هنگامی که به صورت Dial Up به اینترنت متصل می شوید معمولا IP کلاس C به شما تعلق می گیرد. ۴- توصیه و پیشنهاد برای استفاده از Cmmand Line ویندوز ۲۰۰۰ یا XP است.

محاسبات شبکهای چیست؟

محاسبات شبکهای چیست؟ در محاسبات شبکهای چندین پردازشگر به طور همزمان و جداگانه محاسبه خاصی را انجام میدهند. به گزارش بخش خبر شبکه فن آوری اطلاعات ایران، به نقل از ایلنا، امروزه در بسیاری از محافل اطلاعاتی و مراکز IT صحبت از محاسبات شبکهای یا GRID CMPUTING است ؛ اما این اصطلاح هنوز برای بسیاری از کاربران ناشناخته باقی مانده است. محاسبات شبکهای در سادهترین حالت ممکن, به معنی فعالیت مشترک پردازندههای چندگانه بر روی ماشینهای چندگانه است و هدف آن افزایش توان محاسباتی در زمینههایی است که توان بسیار بالای CPU را میطلبد. در محاسبات شبکهای سرورهای چندگانهای با هم ارتباط دارند که از سیستمعاملها و نرمافزارهای مشابهی استفاده میکند. به کمک محاسبات شبکهای, میتوان کارهای محاسباتی را به طور همزمان به کمک چندین پردازشگر انجام داد. در مواردی که نتیجه محاسبات خیلی حساس است و دقت آن سرنوشتساز است, دهها و گاهی هزاران پردازشگر به طور همزمان یک محاسبه را انجام میدهند. بعد از انجام محاسبات نتایج کار همه پردازشگرها با هم مقایسه میشود تا میزان دقت محاسبات تعیین شود.

تجهیزات و پیکربندی یک شبکه Wireless

تجهیزات و پیکربندی یک شبکه Wireless سخت افزار مورد نیاز به منظور پیکربندی یک شبکه بدون کابل به ابعاد شبکه مورد نظر بستگی دارد . علیرغم موضوع فوق ، در این نوع شبکه ها اغلب و شاید هم قطعا "به یک access pint و یک اینترفیس کارت شبکه نیاز خواهد بود . در صورتی که قصد ایجاد یک شبکه موقت بین دو کامپیوتر را داشته باشید ، صرفا "به دو کارت شبکه بدون کابل نیاز خواهید داشت . Access Pint چیست ؟ سخت افزار فوق ، به عنوان یک پل ارتباطی بین شبکه های کابلی و دستگاههای بدون کابل عمل می نماید . با استفاده از سخت افزار فوق ، امکان ارتباط چندین دستگاه به منظور دستیابی به شبکه فراهم می گردد .access pint می تواند دارای عملکردی مشابه یک روتر نیز باشد . در چنین مواردی انتقال اطلاعات در محدوده وسیعتری انجام شده و داده از یک access pint به access pint دیگر ارسال می گردد . یک نمونه دستگاه access pint کارت شبکه بدون کابل هر یک از دستگاههای موجود بر روی یک شبکه بدون کابل ، به یک کارت شبکه بدون کابل نیاز خواهند داشت . یک کامپیوتر Laptp ، عموما "دارای یک اسلات PCMCIA است که کارت شبکه درون آن قرار می گیرد . کامپیوترهای شخصی نیز به یک کارت شبکه داخلی که معمولا "دارای یک آنتن کوچک و یا آنتن خارجی است ، نیاز خواهند داشت .آنتن های فوق بر روی اغلب دستگاهها ،اختیاری بوده و افزایش سیگنال بر روی کارت را بدنبال خواهد داشت . یک نمونه کارت شبکه بدون کابل پیکربندی یک شبکه بدون کابل به منظور پیکربندی یک شبکه بدون کابل از دو روش متفاوت استفاده می گردد : روش Infrastructure : به این نوع شبکه ها، hsted و یا managed نیز گفته می شود . در این روش از یک و یا چندین access pint (موسوم به gateway و یا روترهای بدون کابل) که به یک شبکه موجود متصل می گردند ، استفاده می شود . بدین ترتیب دستگاههای بدون کابل، امکان استفاده از منابع موجود بر روی شبکه نظیر چاپگر و یا اینترنت را بدست می آورند . روش Ad-Hc : به این نوع شبکه ها ، unmanaged و یا peer t peer نیز گفته می شود

. در روش فوق هر یک از دستگاهها مستقیما "به یکدیگر متصل می گردند.مثلا "یک شخص با دارا بودن یک دستگاه کامپیوتر laptp مستقر در محوطه منزل خود می تواتند با کامپیوتر شخصی موجود در منزل خود به منظور دستیابی به اینترنت ، ارتباط برقرار نماید . پس از تهیه تجهیزات سخت افزاری مورد نیاز به منظور ایجاد یک شبکه بدون کابل ، در ادامه می بایست تمامی تجهیزات تهیه شده را با هدف ایجاد و سازماندهی یک شبکه به یکدیگر متصل تا امکان ارتباط بین آنان فراهم گردد . قبل از نصب و پیکربندی یک شبکه بدون کابل ، لازم است به موارد زیر دقت نمائید : تهیه درایورهای مربوطه از فروشنده سخت افزار و کسب آخرین اطلاعات مورد نیاز فاصله بین دو کامپیوتر می بایست کمتر از یکصد متر باشد . هر یک از کامپیوترهای موجود می بایست بر روی یک طبقه مشابه باشند . استفاده از تجهیزات سخت افزاری مربوط به یک تولید کننده ، دارای مزایا و معایبی است . در این رابطه پیشنهاد می گردد لیستی از ویژگی های هر یک از سخت افزارهای مورد نیاز عرضه شده توسط تولید کنندگان متعدد تهیه شود تا امکان مقایسه و اخذ تصمیم مناسب، فراهم گردد . مراحل لازم به منظور نصب یک شبکه (فرضیات : ما دارای یک شبکه کابلی موجود هستیم و قصد پیاده سازی یک شبکه بدون کابل به منظور ارتباط دستگاههای بدون کابل به آن را داریم) : اتصال access pint به برق و سوکت مربوط به شبکه اترنت پیکربندی access pint (معمولا "از طریق یک مرورگر وب) تا امکان مشاهده آن توسط شبکه موجود فراهم گردد . نحوه پیکربندی access pint بستگی به نوع آن دارد. پیکربندی مناسب کامپیوترهای سرویس گیرنده به منظور ارتباط با access pint (در صورتی که تمامی سخت افزارهای شبکه بدون کابل از یک تولید کننده تهیه شده باشند ، عموما "با تنظیمات پیش فرض هم می توان شبکه را فعال نمود . به هر حال پیشنهاد می گردد همواره به راهنمای سخت افزار تهیه شده به منظور پیکربندی بهینه آنان ، مراجعه گردد) .

WAP چیست؟

سیستمی است که در آن پرو تکل ارتباطی و محیط برنامه نویسی جهت پیاده سازی سیستم های پیاده سازی سیستم های اطلاعاتی مبتنی بر وب روی گوشی های تلفن همراه ارایه می شود . پروتکل ارتباطی پروتکل ارتباطی که در حال حاضر در اینترنت برای دیدن صفحات وب استفاده می شود HTTP است .(البته در سطح شبکه اینترنت برای فعالیت های متفاوت پروتکل های متفاوتی در سطح لایه Applicatin استفاده می شود ولی پروتکلی که جهت دیدن سایت ها از آن استفاده می شود HTTP است) . وقتی آدرس سایتی را به اینترنت اکسپلورر می دهید تا صفحه مربوط به آن سایت را ببینند ، در پشت پرده ، اینترنت اکسپلورر بسته ای را حاوی اطلاعاتی جهت در خواست صفحه آن سایت است به اینترنت می فرستد . اطلاعات این بسته به فرمتی است که در پروتکل HTTP تعریف شده است . با این توصیف ، وقتی صحبت از تلفن همراه می شود در نگاه اول مساله حل شده است و فقط کافی است این بار تلفن همراه شما چنین بسته ای ساخته و به اینترنت بفرستد . ولی این کار برای یک تلفن همراه شدنی نیست . زیرا بسته هایی که در پروتکل HTTP ساخته می شوند حجم زیادی دارند و لذا لازم است فرستنده دارای حافظه مناسبی باشد . در حالی که تلفن همراه از نظر حافظه بسیار محدود است (البته به تازگی گروهی از تلفن های همراه با نام Smart phne وارد بازار شده اند که از نظر حافظه نسبت به انواع قدیمی تر بسیار قوی تر ند .) همچنین جهت پردازش بسته هایی که با پروتکل HTTP ارسال و دریافت می شوند ، نیاز به پردازشگری قوی تر از آن چه که در یک تلفن همراه وجود دارد ، می باشد . لذا جهت ورود تلفن همراه ، به دنیای اینترنت ضروری است با توجه به قابلیت های یک تلفن همراه پروتکل ویژه ای طراحی شود. این پروتکل WAP نام دارد . البته WAP فراتر از یک پروتکل ساده در لایه Applicatin می باشد و بهتر است به آن پشته پروتکل WAP (Prtcl Stack) بگوییم . پشته پروتکل WAP دارای شش لایه می باشد و یک ارتباط cnnectin less را در دنیای تلفن های همراه ایجاد می کند . در این جا اشاره مختصری به کار هر یک از لایه ها می کنیم . ۱ :Bearer Layer- معادل همان لایه فیزیکی در TCP/IP

می باشد ولی این بار محیط ارتباطی wireless است و لذا پروتکل های دیگری در این لایه استفاده می شود . ۲ :WDP- این لایه در واقع همان UDP است . به عبارت دیگر فعالیت و ساختاری مانند پروتکل UDP در لایه انتقال TCP/IP دارد . ۳- WTLS: لایه ای است که امنیت ارتباطات را فراهم می کند . در این لایه از پروتکل SSL استفاده می شود . ۴- WTP : این لایه مدیریت در خواست ها و پاسخ ها را بر عهده دارد . ۵-WSP : همانند لایه sessin در Si می باشد ، با تفاوت های مختصری جهت بهینه سازی . ۶- WAE : همانند لایه Applicatin در TCP/IP می باشد . در واقع تمام برنامه هایی که پیاده سازی می شوند در این لایه قراردارند و کاربر تلفن همراه و برنامه نویس WAP ، هر دو، با لایه ارتباط برقرار می کنند . مشکل عدم توانایی تلفن همراه جهت استفاده از پروتکل HTTP با طراحی پشته پرو تکلی جدید ی با در نظر گرفتن محدودیت های تلفن همراه حل شد . ولی استفاده از این پروتکل مشکل جدیدی را ایجاد می کند . که ضروری است تدبیر خاصی برای حل آن اندیشیده شود . دو پروتکل متفاوت ، دو دنیای متفاوت فرض کنید تصمیم داریم که با استفاده از تلفن همراه به اینترنت وصل شویم و از اطلاعات موجود در اینترنت استفاده کنیم . برای این کار ضروریست تلفن همراه با زبانی (یا پروتکل) که در حال حاضر در اینترنت استفاده می شود (HTTP) صحبت کند ولی همان طور که اشاره شد این امر امکان پذیر نمی باشد . راه حل مشکل استفاده از یک مترجم می باشد ، مترجمی که پروتکل تلفن های همراه (WAP) را به پروتکل وب کنونی (HTTP) و برعکس ترجمه کند. این مترجم اصطلاحا WAP gatewavay نامیده می شود. WAPgateway در واقع یک نرم افزار است که بین این دو شبکه قرار می گیرد و وقتی که در خواست صفحه خاصی از تلفن همراه ارسال می شود ، WAP gateway این در خواست را گرفته و به در خواستی با فرمت HTTP تبدیل کرده و به اینترنت می فرستد و در ادامه پس از دریافت پاسخ از web server مربوطه ، پاسخ را به فرمت پروتکل WAP تبدیل کرده و به تلفن همراه بر می گرداند .WAP gaterway می تواند در شبکه مخابراتی و یا در شبکه ISP و یا در شبکه خودتان قرارگیرد . در حال حاضر شرکت های مختلف به گونه های متفاوتی از WAP gaterway را ارائه کرده اند . توجه کنید که برخی از تولید کنندگان قابلیت های RAS را هم به خود اضافه کرده اند تا به نصب RAS server و تنظیم آن وجود نداشته باشد . Brwser تا این جا پروتکل ارتباطی و نحوه ارتباط با اینترنت مشخص شد . مشکل دیگری که وجود دارد عدم وجود Brwser یا مرورگر در تلفن همراه نمی تواند از IEکه درPC استفاده می شود استفاده کند برای حل این مشکل ، تولید کنندگان گوشی در قسمتی از RM دستگاه یک micr brwser قرار داده اند که در واقع کاری شبیه به اینترنت اکسپلورر ویندوز می کند . البته در چند سال آینده این ریز مرورگرها روی سیم کارت قرار خواهند گرفت که این امر جهت راحتی در پیاده سازی سیستم های WAP می گیرد . (همان طور که در حال حاضر ممکن است یک مرورگر صفحه ای را به گونه خاصی نمایش دهد و مرورگر دیگری به شکل دیگر، دردنیای تلفن های همراه هم مرورگر های مختلفی وجود دارد . محتویات سایت محتویات سایت های اینترنتی که در اینترنت اکسپلورر مشاهده می کنید با زبان HTML و یا XML و .... نوشته می شوند . اینترنت اکسپلوررمحتویات یک فایل HTML را خوانده و آن را تفسیر می کند و به صورتی که لازم است نمایش می دهد با این وصف ، ریز مرورگر هم لازم است صفحات HTML را گرفته و تفسیرکرده و نمایش دهد . ولی این کار عملی نیست . اولا جهت نمایش یک صفحه HTML، صفحه نمایش بزرگی لازم است که تلفن همراه ندارد . ثانیا حجم فایل های HTML زیادتر ازآن است که دریک تلفن همراه معمولی قرار گیرد . ثالثا جهت پردازش Tag های HTML نیاز پردازندهای قوی تراز آنچه که در تلفن همراه موجود است می باشد . طراحان WAP با ارایه زبانی مانند HTML ولی مناسب برای یک تلفن همراه این مشکل را حل کردند . یعنی به زبانی به نام (WML (Wireless Markup lamguage هم به زبانی به نام WML Script ایجاد شده است . برای تبدیل کدهای HTML به WML نیز نرم افزارهای دیگری ساخته شده است ولیکن عملکرد آن ها چندان مطلوب نبوده است . لذا اگر قصد دارید سایتی را جهت استفاده تلفن های همراه پیاده سازی کنید بهتر است از همان ابتدا صفحات WML را خودتان

بنویسید (WML بسیار شبیه به HTML است) و روی web server تان قراردهید . اگر با ASP.NET آشنایی کافی دارید می توانید با استفاده از امکاناتی که مایکرو سافت در VS.NET جهت تولید سایت برای PDAها قرار داده است سایت خود را پیاده سازی کنید . البته در VS.NET مفاهیمی غیر از آنچه که در WML خواهید دید نیز مطرح می شود . در مورد web server هم می توانید از Iis مایکرو سافت استفاده کنید و فقط تنظیمات خاصی را روی آن باید انجام دهید . دنیای WAP مفاهیم ومسایل دیگری هم دارد که در این جا مطرح نشدند ولی امیدوارم این مقاله دید اولیه ای را جهت وارد شدن به این وادی به شماداده باشد

SSL چیست؟

Secure Scket Layer , یا همان SSL یک تکنولوژی استاندارد و به ثبت رسیده برای تامین ارتباطی امن مابین یک وب سرور و یک مرورگر اینترنت است. این ارتباط امن از تمامی اطلاعاتی که ما بین وب سرور و مرورگر اینترنت (کاربر) انتقال میابد , محافظت میکند تا در این انتقال به صورت محرمانه و دست نخورده باقی بماند. SSL یک استاندارد صنعتی است و توسط ملیونها وب سایت در سراسر جهان برای برقراری امنتیت انتقال اطلاعات استفاده میشود. برای اینکه یک وب سایت بتواند ارتباطی امن از نوع SSL را داشته باشد نیاز به یک گواهینامه SSL دارد. زمانیکه شما میخواهید SSL را بر روی سرور خود فعال کنید سؤالات متعددی در مورد هویت سایت شما (مانند آدرس سایت) و همین طور هویت شرکت شما (مانند نام شرکت و محل آن) از شما پرسیده میشود. آنگاه سرور دو کلید رمز را برای شما تولید میکند , یک کلید خصوصی (Private Key) و یک کلید عمومی (Public Key). کلید خصوصی به این خاطر , این نام را گرفته است , چون بایستی کاملاـ محرمانه و دور از دسترس دیگران قرارگیرد. اما در مقابل نیازی به حفاظت از کلید عمومی نیست و این کلید در قالب یک فایل درخواست گواهینامه یا Certificate Signing Request که به اختصار آنرا CSR مینامیم قرارداده میشود که حاوی مشخصات سرور و شرکت شما بصورت رمز است. آنگاه شما باسیتی که این کد CSR را برای صادرکننده گواهینامه ارسال کنید. در طول مراحل سفارش یک SSL مرکز صدور گواهینامه درستی اطلاعات وارد شده توسط شما را بررسی و تایید میکند و سپس یک گواهینامه SSL برای شما تولید کرده و ارسال میکند. وب سرور شما گواهینامه SSL صادر شده را با کلید خصوصیتان در سرور و بدور از دسترس سایرین مطابقت میدهد. سرور شما آنگاه امکان برقراری ارتباط امن را با کاربران خود در هر نقطه دارد. نمایش قفل امنیت SSL پیچیده گیهای یک پروتکل SSL برای کاربران شما پوشیده است لیکن مرورگر اینترنت آنها در صورت برقراری ارتباط امن , وجود این ارتباط را توسط نمایش یک قفل کوچک در پایین صفحه متذکر میشود. و در هنگامی که شما روی قفل کوچک زرد رنگی که در پایین صفحه IE نمایش داده میشود دوبار کلیک میکنید باعث نمایش گواهینامه شما به همراه سایر جزئیات می شود. گواهینامه های SSL تنها برای شرکتها و اشخاص حقیقی معتبر صادر میشوند. به طور مثال یک گواهینامه SSL شامل اطلاعاتی در مورد دامین , شرکت , آدرس , شهر , استان , کشور و تاریخ ابطال گواهینامه و همینطور اطلاعاتی در مورد مرکز صدور گواهینامه که مسؤول صدور گواهینامه میباشد. زمانیکه یک مرورگر اینترنت به یک سایت از طریق ارتباط امن متصل میشود , علاوه بر دریافت گواهینامه SSL (کلید عمومی) , پارامترهایی را نظیر تاریخ ابطال گواهینامه , معتبر بودن صادرکننده گواهینامه و مجاز بودن سایت به استفاده از این گواهینامه نیز بررسی میکند و هرکدام از موارد که مورد تایید نباشد به صورت یک پیغام اخطار به کاربر اعلام میدارد.

آشنائی با پروتکل DNS

آشنائی با پروتکل DNS DNS از کلمات Dmain Name System اقتباس و یک پروتکل شناخته شده در عرصه شبکه های کامپیوتری خصوصا "اینترنت است . از پروتکل فوق به منظور ترجمه اسامی کامپیوترهای میزبان و Dmain به آدرس های IP استفاده می گردد. زمانی که شما آدرس http://www.src.ir را در مرورگر خود تایپ می نمائید ، نام فوق به یک آدرس IP و بر اساس یک درخواست خاص (query) که از جانب کامپیوتر شما صادر می شود ، ترجمه می گردد . تاریخچه DNS DNS ، زمانی که اینترنت تا به این اندازه گسترش پیدا نکرده بود و صرفا "در حد و اندازه یک شبکه کوچک بود ، استفاده می گردید . در آن زمان ، اسامی کامپیوترهای میزبان به صورت دستی در فایلی با نام HSTS درج می گردید . فایل فوق بر روی یک سرویس دهنده مرکزی قرار می گرفت . هر سایت و یا کامپیوتر که نیازمند ترجمه اسامی کامپیوترهای میزبان بود ، می بایست از فایل فوق استفاده می نمود . همزمان با گسترش اینترنت و افزایش تعداد کامپیوترهای میزبان ، حجم فایل فوق نیز افزایش و امکان استفاده از آن با مشکل مواجه گردید (افزایش ترافیک شبکه). با توجه به مسائل فوق ، در سال ۱۹۸۴ تکنولوژی DNS معرفی گردید . پروتکل DNS DNS ، یک" بانک اطلاعاتی توزیع شده " است که بر روی ماشین های متعددی مستقر می شود (مشابه ریشه های یک درخت که از ریشه اصلی انشعاب می شوند) . امروزه اکثر شرکت ها و موسسات دارای یک سرویس دهنده DNS کوچک در سازمان خود می باشند تا این اطمینان ایجاد گردد که کامپیوترها بدون بروز هیچگونه مشکلی ، یکدیگر را پیدا می نمایند . در صورتی که از ویندوز ۲۰۰۰ و اکتیو دایرکتوری استفاده می نمائید، قطعا "از DNS به منظور ترجمه اسامی کامپیوترها به آدرس های IP ، استفاده می شود . شرکت مایکروسافت در ابتدا نسخه اختصاصی سرویس دهنده DNS خود را با نام (WINS Windws Internet Name Service طراحی و پیاده سازی نمود . سرویس دهنده فوق مبتنی بر تکنولوژی های قدیمی بود و از پروتکل هائی استفاده می گردید که هرگز دارای کارائی مشابه DNS نبودند . بنابراین طبیعی بود که شرکت مایکروسافت از WINS فاصله گرفته و به سمت DNS حرکت کند . از پروتکل DNS در مواردی که کامپیوتر شما اقدام به ارسال یک درخواست مبتنی بر DNS برای یک سرویس دهنده نام به منظور یافتن آدرس Dmain می نماید ، استفاده می شود .مثلا "در صورتی که در مرورگر خود آدرس http://www.src.ir را تایپ نمائید ، یک درخواست مبتنی بر DNS از کامپیوتر شما و به مقصد یک سرویس دهنده DNS صادر می شود . ماموریت درخواست ارسالی ، یافتن آدرس IP وب سایت سخاروش است . پروتکل DNS و مدل مرجع SI پروتکل DNS معمولا "از پروتکل UDP به منظور حمل داده استفاده می نماید . پروتکل UDP نسبت به TCP دارای verhead کمتری می باشد. هر اندازه verhead یک پروتکل کمتر باشد ، سرعت آن بیشتر خواهد بود . در مواردی که حمل داده با استفاده از پروتکل UDP با مشکل و یا بهتر بگوئیم خطاء مواجه گردد ، پروتکل DNS از پروتکل TCP به منظور حمل داده استفاده نموده تا این اطمینان ایجاد گردد که داده بدرستی و بدون بروز خطاء به مقصد خواهد رسید . فرآیند ارسال یک درخواست DNS و دریافت پاسخ آن ، متناسب با نوع سیستم عامل نصب شده بر روی یک کامپیوتر است .برخی از سیستم های عامل اجازه استفاده از پروتکل TCP برای DNS را نداده و صرفا "می بایست از پروتکل UDP به منظور حمل داده استفاده شود . بدیهی است در چنین مواردی همواره این احتمال وجود خواهد داشت که با خطاهائی مواجه شده و عملا" امکان ترجمه نام یک کامپیوتر و یا Dmain به آدرس IP وجود نداشته باشد . پروتکل DNS از پورت ۵۳ به منظور ارائه خدمات خود استفاده می نماید . بنابراین یک سرویس دهنده DNS به پورت ۵۳ گوش داده و این انتظار را خواهد داشت که هر سرویس گیرنده ای که تمایل به استفاده از سرویس فوق را دارد از پورت مشابه استفاده نماید . در برخی موارد ممکن است مجبور شویم از پورت دیگری استفاده نمائیم . وضعیت فوق به سیستم عامل و سرویس دهنده DNS نصب شده بر روی یک کامپیوتر بستگی دارد. ساختار سرویس دهندگان نام دامنه ها در اینترنت امروزه بر روی اینترنت میلیون ها سایت با اسامی Dmain ثبت شده وجود دارد . شاید این سوال برای شما تاکنون مطرح شده باشد که این اسامی چگونه سازماندهی می شوند ؟ ساختار DNS بگونه ای طراحی

شده است که یک سرویس دهنده DNS ضرورتی به آگاهی از تمامی اسامی Dmain ریجستر شده نداشته و صرفا "میزان آگاهی وی به یک سطح بالاتر و یک سطح پائین تر از خود محدود می گردد . internic ، مسئولیت کنترل دامنه های ریشه را برعهده داشته که شامل تمامی Dmain های سطح بالا می باشد (در شکل فوق به رنگ آبی نشان داده شده است) . در بخش فوق تمامی سرویس دهندگان DNS ریشه قرار داشته و آنان دارای آگاهی لازم در خصوص دامنه های موجود در سطح پائین تر از خود می باشند (مثلا "micrsft.cm) . سرویس دهندگان DNS ریشه مشخص خواهند کرد که کدام سرویس دهنده DNS در ارتباط با دامنه های micrsft.cm و یا Cisc.cm می باشد . هر dmain شامل یک Primary DNS و یک Secndary DNS می باشد . Primary DNS ، تمامی اطلاعات مرتبط با Dmain خود را نگهداری می نماید. Secndary DNS به منزله یک backup بوده و در مواردی که Primary DNS با مشکل مواجه می شود از آن استفاده می گردد . به فرآیندی که بر اساس آن یک سرویس دهنده Primary DNS اطلاعات خود را در سرویس دهنده Secndary DNS تکثیر می نماید ، Zne Transfer گفته می شود . امروزه صدها وب سایت وجود دارد که می توان با استفاده از آنان یک Dmain را ثبت و یا اصطلاحا "ریجستر نمود . پس از ثبت یک Dmain ، امکان مدیریت آن در اختیار شما گذاشته شده و می توان رکوردهای منبع (RR) را در آن تعریف نمود. Supprt, www و Ruters ، نمونه هائی از رکوردهای منبع در ارتباط با دامنه Cisc.cm می باشد. به منظور ایجاد Subdmain می توان از یک برنامه مدیریتی DNS استفاده نمود . www و یا هر نوع رکورد منبع دیگری را می توان با استفاده از اینترفیس فوق تعریف نمود . پس از اعمال تغییرات دلخواه خود در ارتباط با Dmain ، محتویات فایل های خاصی که بر روی سرویس دهنده ذخیره شده اند نیز تغییر نموده و در ادامه تغییرات فوق به سایر سرویس دهندگان تائید شده اطلاع داده می شود . سرویس دهندگان فوق ، مسئولیت Dmain شما را برعهده داشته و در ادامه تمامی اینترنت که به این سرویس دهندگان DNS متصل می شوند از تغییرات ایجاد شده آگاه و قادر به برقراری ارتباط با هر یک از بخش های Dmain می گردند. مثلا "در صورتی که قصد ارتباط با Supprt.Cisc.cm را داشته باشید، کامپیوتر شما با سرویس دهنده DNS که مسئولیت مدیریت دامنه های Cm. را دارد ، ارتباط برقرار نموده و سرویس دهنده فوق اطلاعات لازم در خصوص دامنه Cisc.cm را در اختیار قرار خواهد داد . در نهایت سرویس دهنده DNS مربوط به Cisc.cm (سرویس دهنده فوق ، تمامی اطلاعات مرتبط با دامنه Cisc.cm را در خود نگهداری می نماید) ، آدرس IP کامپیوتر مربوط به Supprt.Cisc.cm را مشخص نموده تا امکان برقراری ارتباط با آن فراهم گردد .

آشنایی با ملزومات شبکه

حتما همه شما تا به حال تجربه ی اتصال به اینترنت را داشته اید و کم و بیش اطلاعاتی راجع به این موضوع دارید. برای آشنایی بیشتر شما نکاتی هر چند مختصر در مورد شبکه و قطعات مورد نیاز در آن خواهیم گفت. همان طور که می دانید اینترنت، متشکل از شبکه هایی است که هر یک ازطریق مسیرهایی به دیگری متصل هستند. این مسیرها تبادل اطلاعات را میسر می سازند. اتصال به اینترنت به معنی دستیابی به این مسیرها است. حال برای این که این شبکه ها که شامل هزاران کامپیوتر هستند بتوانند به درستی با هم در ارتباط باشند به وسایل و قطعات ویژه ای مثل هاب، تکرار کننده، مسیریاب و ... نیاز است. اما برای اینکه بدانید وظیفه هر یک از این وسیله ها چیست ادامه ی مطلب را بخوانید. کابل BUS: در شبکه های محلی اترنت اولیه برای ارتباط از کابل کواکسیال استفاده می شد. (این کابل ها همان کابل هایی هستند که برای اتصال آتن به تلویزیون استفاده می شوند و شما هم حتما دیده اید.) این کابل از یک کامپیوتر به کامپیوتر دیگر رفته و تمام دستگاه ها را به هم متصل می کند. بنابراین هر سیگنالی که در کابل Bus وجود دارد در تمام دستگاه ها قابل مشاهده است. این روش ساده ترین روش ایجاد شبکه ی کامپیوتری است. البته در

ظاهر ساده به نظر می رسد اما در واقع پر از اشکال است. چون وقتی که تعداد سیستم ها زیاد می شود، کار کابل کشی بسیار پر زحمت است. تازه وقتی بخواهید دستگاهی را از مدار خارج کنید و یا یک دستگاه جدید به شبکه اضافه کنید مشکلات ظهور می کنند. البته امروزه به ندرت می توانید یک شبکه محلی LAN پیدا کنید که با کابل کواکسیال درست شده باشد. Hub: به طور خلاصه باید بگوییم هاب یک جعبه است که دارای تعدادی ورودی بنام پورت (Prt) می باشد. تعداد این ورودی ها بسته به تعداد کامپیوترهایی است که می خواهیم در یک شبکه باشند. مثلا اگر در یک شرکت تمام کامپیوترها در شبکه باشند، در هر طبقه یک هاب قرار می دهند و تمام دستگاه های آن طبقه با کابل به هاب مورد نظر وصل می شوند که بعد هر کدام از این هاب ها به طریقی به کامپیوتر سرور متصل می شوند. اگر اطلاعاتی به داخل این جعبه آمد توسط کابل وارد تمام کامپیوترها می شود. شاید بگویید پس چه فرقی بین این روش و روش اولیه وجود دارد؟ در جواب باید گفت بزرگترین فرق در این است که شما می توانید هر زمان که بخواهید به راحتی یک کامپیوتر جدید را با اتصال به این جعبه به شبکه اضافه کنید و یا با خارج کردن کابل یک دستگاه از این جعبه آن را از شبکه خارج کنید بدون این که کل شبکه تحت تاثیر قراربگیرد. اکثر هاب ها یک چراغ نمایشگر دارند که نشان می دهد هر کابل به خوبی دستگاه را به شبکه متصل کرده است و یک چراغ دیگر وضعیتی را نشان می دهد که ۲ سیستم سعی می کنند در یک زمان اطلاعات را به اشتراک بگذارند و در نتیجه باعث تصادف داده ها (Data Cllisin) می شوند. به طور کلی هاب به دو دسته تقسیم می شود: ۱.Active: این نوع هاب، سیگنال هایی را که از درون آن می گذرند تقویت می کند. ۲.Passive: این هاب هیچ عمل تقویتی روی سیگنال انجام نمی دهد و صرفا آن را از خود عبور می دهد. در مسافرت های طولانی زیاد بودن طول کابل باعث ضعیف شدن سیگنال می شود و با تقویت آن، قدرت اولیه را به آن برمی گرداند. نوع دیگر از هاب ها وجود دارد که هوشمند نامیده می شود که به مسئول شبکه اجازه کنترل از راه دور اتصالات را می دهد. تکرار کننده(Repeater): این وسیله در واقع نوع خاصی Hub است که فقط دارای ۲ پورت است. کار آن تقویت سیگنال های بین دو شبکه یا سگمنت های یک شبکه که فاصله ی زیادی از هم دارند می باشد. مثل هاب های دارای ۲ نوع Passive و Active می باشد. نوع اول علاوه بر سیگنال هر چیز دیگری حتی نویز (Nise: امواج ناخواسته که به همراه سیگنال اصلی که دارای اطلاعات است می باشند. مثلا در امواج صوتی نویز باعث افت کیفیت صدا و شنیدن اصوات اضافه می شود) را هم تقویت می کند. اما تکرار کننده ی نوع اکتیو سیگنال را قبل از ارسال بازدید کرده و چیزهای اضافه را خارج می کند و مثلا دیگر نویز را تقویت نمی کند. پل (Bridge): مثل تکرارکننده دارای ۲ پورت است و برای اتصال گروهی از کامپیوترها به کار می رود. تفاوت آنها در این است که پل لیستی دارد که نشان می دهد در هر سمت چه کامپیوترهایی قرار دارند و به بسته هایی (در اینترنت و هر شبکه ای اطلاعات برای اینکه فرستاده شوند به قطعات کوچکتری تقسیم می شوند، هر قطعه را بسته می نامیم) که باید بطرف دیگر شبکه بروند اجازه ی عبور می دهد. سوئیچ (Switch): تقریبا مثل هاب است اما به جای ۲ پورت دارای چندین پورت است. درون خود یک جدولی دارد و نشان می دهد که جه سیستم هایی به هر پورت متصلند و بسته ها را به جایی که باید بروند می فرستد. برخلاف هاب سیگنال ها فقط به درون پورتی که باید بروند می روند نه به تمام پورت ها. جداول (و شبکه) باید به قدر کافی ساده باشند چرا که فقط یک مسیر ممکن برای هر بسته وجود دارد. اگر دقت کرده باشید متوجه خواهید شد که سوئیچ از هاب سریعتر است چون احتیاجی نیست که هر پورت کل ترافیک ارسال و دریافت اطلاعات را متحمل شود و فقط آنچه که مخصوص خود است را دریافت می کند. البته سوئیچ از پل هم سریعتر است و در ضمن گران تر از هر دوی آنها. بعضی از سوئیچ ها و پل ها می توانند برای اتصال شبکه هایی که پروتکل های فیزیکی مختلفی دارند استفاده شوند. مثلا برای اتصال شبکه های اترنت یا شبکه TkenRing. هر دوی این شبکه ها می توانند به اینترنت متصل شوند. در شبکه TkenRing اطلاعات بع صورت نشانه (Tken) هایی از یک کامپیوتر به کامپیوتر دیگر به صورت ستاره یا حلقه منتقل می شوند. شبکه اترنت را هم قبلا توضیح داده ایم. این قطعات به صورت

ویژه هستند و در همه شبکه ها استفاده نمی شوند. مسیریاب (Ruter): مسیریاب از ۲ یا چند پورت برای ورود و خروج اطلاعات تشکیل شده است در واقع کنترل ترافیک به عهده آنها می باشد. مسیریاب را می توان مرتب کننده ی هوشمند بسته ها نامید. همان طور که از نامش پیدا است، بهترین مسیر را برای فرستادن قطعات به مقصد انتخاب می کند و چک می کند تا ببیند آیا بسته ها به مقصد رسیده اند یا نه. براساس مقصد داده ها، بسته ها از یک مسیریاب به مسیریاب دیگر از طریق بهترین راه فرستاده می شوند. این موضوع یاعث می شود تا به عنوان یک وسیله قدرتمند در شبکه های پیچیده مثل اینترنت استفاده شود. در واقع می توان اینترنت را به عنوان شبکه ای از مسیریاب ها توصیف کرد. انواع مسیریاب ها با جداول و پروتکل های مختلفی کار می کنند اما حداقل این که هر مسیریاب در اینترنت باید با پروتکل TCP/IP کار کند. Bruter: این وسیله ترکیبی از پل و مسیریاب می باشد/(Bridgt+Ruter). بسته های محلی می توانند از یک طرف شبکه به طرف دیگر با توجه به آدرس مقصد هدایت شوند حتی اگر از هیچ پروتکل ارسالی هم پیروی نکنند. بسته هایی که دارای پروتکل مناسب هستند می تواند طبق مسیر خود به دنیای خارج از شبکه محلی فرستاده شوند. دروازه (Gateway): دلیل اصلی پیچیدگی موضوع در وازه ها از این حقیقت ناشی می شود که این کلمه ۲ عملکرد مختلف را توصیف می کند. یک نوع آن، یک شبکه را به یک شبکه یا دستگاه های مختلف دیگر ارتباط می دهد. مثلا یک شبکه از کامپیوترهایی که به یک سیستم ابرکامپیوتر IBM متصل هستند. کاربرد معمولی آن در گره (Nde) یک شبکه می باشد که امکان دستیابی به اینترنت و یا کامپیوترهای دیگر دریک شبکه پیچیده LAN را می دهد. در شبکه هایی که بیش از یک دروازه وجود دارد معمولا یکی از آنها به عنوان دروازه ی پیش فرض انتخاب می شود. قبلا یک دروازه تقریبا شبیه به چیزی بود که ما امروزه مسیریاب می نامیم. سرور پراکسی (Prxy Server): این سیستم بین یک سرور و یک کامپیوتر Wrk Statin (یعنی کامپیوتری که به کامپیوتر اصلی یا همان سرور متصل است) برقرار است. ملموس ترین مثال در مورداینترنت، مرورگری که شما با آن کار می کنید است. این مرورگر ظاهرا در حال برقراری ارتباط با یک سرور خارج از وب است اما درواقع به یک سرورپراکسی محلی متصل است. شاید بگویید این کار چه مزیت دارد؟ مزیت اول: این سیستم باعث افزایش سرعت دسترسی به اینترنت می شود. چون سرور پراکسی صفحات وبی که قبلا باز شده اند را در حافظه ذخیره می کند، هنگامی که شما به این صفحات احتیاج دارید به جای اینکه آن را از سایت اصلی و از محلی دور پیدا کنید به راحتی وبه سرعت آنها را از این دستگاه برمی دارید. حال ببینیم نحوه ی کار به چه صورت است. وقتی شما در یک شبکه ی محلی مثلا شبکه ی شرکت می خواهید به یک سرویس دهنده در شبکه دسترسی داشته باشید، یک درخواست از کامپیوتر شما به سرور پراکسی (سرویس دهنده ی پراکسی) فرستاده می شود. سرور پراکسی با سرور اصلی در اینترنت ارتباط برقرار می کند و سپس سرور پراکسی اطلاعات را از سرور اینترنت به کامپیوتر شما درون شبکه شرکت می فرستد و در ضمن یک کپی از این اطلاعات در سرور پراکسی ذخیره می شود. مزیت دوم: با کمی دقت می بینید که سرور پراکسی به عنوان یک واسطه بین شبکه ی اینترنت و شبکه ی شرکت شما عمل می کند. به عبارتی باعث امنیت در شبکه ی داخلی شرکت می شود. چون به جای اینکه چندین کامپیوتر در شبکه داخلی به اینترنت متصل باشند فقط یک سرور پراکسی با اینترنت در ارتباط است. امنیت شبکه از لحاظ ویروس و هک شدن... تا حدود زیادی تامین می شود. اما این چگونه انجام می شود؟ معمولا در شرکت ها برای محافظت از شبکه ی خود از دیواره های آتش (Firewalls) استفاده می کنند. دیواره های آتش به کاربر در شبکه امکان می دهند به اینترنت دسترسی داشته باشد، ولی جلوی هکرها و هر کس در اینترنت که می خواهد به شبکه آن شرکت دسترسی داشته باشد و باعث خسارت شود را می گیرند. دیواره های آتش مجموعه ای از سخت افزارها و نرم افزارهایی مثل مسیریاب ها، سرویس دهنده ها و نرم افزارهای مختلف هستند. انواع مختلفی دارند و بسته به کاربردشان می توانند ساده و یا پیچیده باشند.

شبکه اترنت (Ethernet) چیست؟

دستیابی به اطلاعات با روش های مطمئن و با سرعت بالا یکی از رموز موفقیت هر سازمان و موسسه است . طی سالیان اخیر هزاران پرونده و کاغذ که حاوی اطلاعات با ارزش برای یک سازمان بوده ، در کامپیوتر ذخیره شده اند. با تغذیه دریائی از اطلاعات به کامپیوتر ، امکان مدیریت الکترونیکی اطلاعات فراهم شده است . کاربران متفاوت در اقصی نقاط جهان قادر به اشتراک اطلاعات بوده و تصویری زیبا از همیاری و همکاری اطلاعاتی را به نمایش می گذارند. شبکه های کامپیوتری در این راستا و جهت نیل به اهداف فوق نقش بسیار مهمی را ایفاء می نمایند.اینترنت که عالی ترین تبلور یک شبکه کامپیوتری در سطح جهان است، امروزه در مقیاس بسیار گسترده ای استفاده شده و ارائه دهندگان اطلاعات ، اطلاعات و یا فرآورده های اطلاعاتی خود را در قالب محصولات تولیدی و یا خدمات در اختیار استفاده کنندگان قرار می دهند. وب که عالی ترین سرویس خدماتی اینترنت می باشد کاربران را قادر می سازد که در اقصی نقاط دنیا اقدام به خرید، آموزش ، مطالعه و ... نمایند. با استفاده از شبکه، یک کامپیوتر قادر به ارسال و دریافت اطلاعات از کامپیوتر دیگر است . اینترنت نمونه ای عینی از یک شبکه کامپیوتری است . در این شبکه میلیون ها کامپیوتر در اقصی نقاط جهان به یکدیگر متصل شده اند.اینترنت شبکه ای است مشتمل بر زنجیره ای از شبکه های کوچکتراست . نقش شبکه های کوچک برای ایجاد تصویری با نام اینترنت بسیار حائز اهمیت است . تصویری که هر کاربر با نگاه کردن به آن گمشده خود را در آن پیدا خواهد کرد. در این بخش به بررسی شبکه های کامپیوتری و جایگاه مهم آنان در زمینه تکنولوژی اطلاعات و مدیریت الکترونیکی اطلاعات خواهیم داشت . شبکه های محلی و شبکه های گسترده تاکنون شبکه های کامپیوتری بر اساس مولفه های متفاوتی تقسیم بندی شده اند. یکی از این مولفه ها " حوزه جغرافیائی " یک شبکه است . بر همین اساس شبکه ها به دو گروه عمده Lcal area netwrk(LAN) و Wide area netwrk(WAN) تقسیم می گردند. در شبکه های LAN مجموعه ای از دستگاه های موجود در یک حوزه جغرافیائی محدود، نظیر یک ساختمان به یکدیگر متصل می گردند . در شبکه های WAN تعدادی دستگاه که از یکدیگر کیلومترها فاصله دارند به یکدیگر متصل خواهند شد. مثلا "اگر دو کتابخانه که هر یک در یک ناحیه از شهر بزرگی مستقر می باشند، قصد اشتراک اطلاعات را داشته باشند، می بایست شبکه ای WAN ایجاد و کتابخانه ها را به یکدیگر متصل نمود. برای اتصال دو کتابخانه فوق می توان از امکانات مخابراتی متفاوتی نظیر خطوط اختصاصی (Leased) استفاده نمود. شبکه های LAN نسبت به شبکه های WAN دارای سرعت بیشتری می باشند. با رشد و توسعه دستگاههای متفاوت مخابراتی میزان سرعت شبکه های WAN ، تغییر و بهبود پیدا کرده است . امروزه با بکارگیری و استفاده از فیبر نوری در شبکه های LAN امکان ارتباط دستگاههای متعدد که در مسافت های طولانی نسبت بیکدیگر قرار دارند، فراهم شده است . اترنت در سال ۱۹۷۳ پژوهشگری با نام " Metcalfe "در مرکز تحقیقات شرکت زیراکس، اولین شبکه اترنت را بوجود آورد. هدف وی ارتباط کامپیوتر به یک چاپگر بود. وی روشی فیزیکی بمنظور کابل کشی بین دستگاههای متصل بهم در اترنت ارائه نمود. اترنت در مدت زمان کوتاهی بعنوان یکی از تکنولوژی های رایج برای برپاسازی شبکه در سطح دنیا مطرح گردید. همزمان با پیشرفت های مهم در زمینه شبکه های کامپیوتری ، تجهیزات و دستگاه های مربوطه، شبکه های اترنت نیز همگام با تحولات فوق شده و قابلیت های متفاوتی را در بطن خود ایجاد نمود. با توجه به تغییرات و اصلاحات انجام شده در شبکه های اترنت ،عملکرد و نحوه کار آنان نسبت به شبکه های اولیه تفاوت چندانی نکرده است . در اترنت اولیه، ارتباط تمام دستگاه های موجود در شبکه از طریق یک کابل انجام می گرفت که توسط تمام دستگاهها به اشتراک گذاشته می گردید. پس از اتصال یک دستگاه به کابل مشترک ، می بایست پتانسیل های لازم بمنظور ایجاد ارتباط با سایر دستگاههای مربوطه نیز در بطن دستگاه وجود داشته باشد (کارت شبکه) . بدین ترتیب امکان گسترش شبکه بمنظور استفاده از دستگاههای جدید براحتی انجام و نیازی به اعمال تغییرات بر روی دستگاههای موجود در شبکه نخواهد بود. اترنت یک تکنولوژی محلی (LAN) است. اکثر شبکه های اولیه در حد و اندازه یک

ساختمان بوده و دستگاهها نزدیک به هم بودند. دستگاههای موجود بر روی یک شبکه اترنت صرفا "قادر به استفاده از چند صد متر کابل بیشترنبودند.اخیرا "با توجه به توسعه امکانات مخابراتی و محیط انتقال، زمینه استقرار دستگاههای موجود در یک شبکه اترنت با مسافت های چند کیلومترنیز فراهم شده است . پروتکل پروتکل در شبکه های کامپیوتری به مجموعه قوانینی اطلاق می گردد که نحوه ارتباطات را قانونمند می نماید. نقش پروتکل در کامپیوتر نظیر نقش زبان برای انسان است . برای مطالعه یک کتاب نوشته شده به فارسی می بایست خواننده شناخت مناسبی از زبان فارسی را داشته باشد. بمنظور ارتباط موفقیت آمیز دو دستگاه در شبکه می بایست هر دو دستگاه از یک پروتکل مشابه استفاده نمایند. اصطلاحات اترنت شبکه های اترنت از مجموعه قوانین محدودی بمنظور قانونمند کردن عملیات اساسی خود استفاده می نمایند. بمنظور شناخت مناسب قوانین موجود لازم است که با برخی از اصطلاحات مربوطه در این زمینه بیشتر آشنا شویم : Medium (محیط انتقال) . دستگاههای اترنت از طریق یک محیط انتقال به یکدیگر متصل می گردند. Segment (سگمنت) . به یک محیط انتقال به اشتراک گذاشته شده منفرد "، سگمنت " می گویند. Nde (گره) . دستگاههای متصل شده به یک Segment را گره و یا " ایستگاه " می گویند. Frame (فریم) . به یک بلاـک اطلاعات که گره ها از طریق ارسال آنها با یکدیگر مرتبط می گردند، اطلاق می گردد فریم ها مشابه جملات در زبانهای طبیعی (فارسی، انگلیسی ...) می باشند. در هر زبان طبیعی برای ایجاد جملات، مجموعه قوانینی وجود دارد مثلا "یک جمله می بایست دارای موضوع و مفهوم باشد. پروتکل های اترنت مجموعه قوانین لازم برای ایجاد فریم ها را مشخص خواهند کرد .اندازه یک فریم محدود بوده (دارای یک حداقل و یک حداکثر) و مجموعه ای از اطلاعات ضروری و مورد نیار می بایست در فریم وجود داشته باشد. مثلا "یک فریم می بایست دارای آدرس های مبداء و مقصد باشد. آدرس های فوق هویت فرستنده و دریافت کننده پیام را مشخص خواهد کرد. آدرس بصورت کاملا "اختصاصی یک گره را مشخص می نماید.(نظیر نام یک شخص که بیانگر یک شخص خاص است) . دو دستگاه متفاوت اترنت نمی توانند دارای آدرس های یکسانی باشند. یک سیگنال اترنت بر روی محیط انتقال به هر یک از گره های متصل شده در محیط انتقال خواهد رسید. بنابراین مشخص شدن آدرس مقصد، بمنظوردریافت پیام نقشی حیاتی دارد. مثلا "در صورتیکه کامپیوتر B (شکل بالاـ) اطلاعاتی را برای چاپگر C ارسال می دارد کامپیوترهای A و D نیز فریم را دریافت و آن را بررسی خواهند کرد. هر ایستگاه زمانیکه فریم را دریافت می دارد، آدرس آن را بررسی تا مطمئن گردد که پیام برای وی ارسال شده است یا خیر؟ در صورتیکه پیام برای ایستگاه مورد نظر ارسال نشده باشد، ایستگاه فریم را بدون بررسی محتویات آن کنار خواهد گذاشت (عدم استفاده). یکی از نکات قابل توجه در رابطه با آدرس دهی اترنت، پیاده سازی یک آدرس Bradcast است . زمانیکه آدرس مقصد یک فریم از نوع Bradcast باشد، تمام گره های موجود در شبکه آن را دریافت و پردازش خواهند کرد. CSMA/CD تکنولوژی CSMA/CD (carrier-sense multiple access with cllisin detectin) مسئولیت تشریح و تنظیم نحوه ارتباط گره ها با یکدیگررا برعهده دارد. با اینکه واژه فوق پیچیده بنظر می آید ولی با تقسیم نمودن واژه فوق به بخش های کوچکتر، می توان با نقش هر یک از آنها سریعتر آشنا گردید.بمنظور شناخت تکنولوژی فوق مثال زیر را در نظر بگیرید : فرض کنید سگمنت اترنت، مشابه یک میز ناهارخوری باشد. چندین نفر (نظیر گره) دور تا دور میز نشسته و به گفتگو مشغول می باشند. واژه multiple access (دستیابی چندگانه) بدین مفهوم است که : زمانیکه یک ایستگاه اترنت اطلاعاتی را ارسال می دارد تمام ایستگاههای دیگر موجود (متصل) در محیط انتقال ، نیز از انتقال اطلاعات آگاه خواهند شد.(.نظیر صحبت کردن یک نفر در میز ناهار خوری و گوش دادن سایرین). فرض کنید که شما نیز بر روی یکی از صندلی های میز ناهار خوری نشسته و قصد حرف زدن را داشته باشید، در همان زمان فرد دیگری در حال سخن گفتن است در این حالت می بایست شما در انتظار اتمام سخنان گوینده باشید. در پروتکل اترنت وضعیت فوق carrier sense نامیده می شود.قبل از اینکه ایستگاهی قادر به ارسال اطلاعات باشد می بایست گوش خود را بر روی محیط انتقال گذاشته

و بررسی نماید که آیا محیط انتقال آزاد است ؟ در صورتیکه صدائی از محیط انتقال به گوش ایستگاه متقاضی ارسال اطلاعات نرسد، ایستگاه مورد نظر قادر به استفاده از محیط انتقال و ارسال اطلاعات خواهد بود. Carrier-sense multiple access شروع یک گفتگو را قانونمند و تنظیم می نماید ولی در این رابطه یک نکته دیگر وجود دارد که می بایست برای آن نیز راهکاری اتخاذ شود.فرض کنید در مثال میز ناهار خوری در یک لحظه سکوتی حاکم شود و دو نفر نیز قصد حرف زدن را داشته باشند.در چنین حالتی در یک لحظه سکوت موجود توسط دو نفر تشخیص و بلافاصله هر دو تقریبا "در یک زمان یکسان شروع به حرف زدن می نمایند.چه اتفاقی خواهد افتاد ؟ در اترنت پدیده فوق را تصادم (Cllisin) می گویند و زمانی اتفاق خواهد افتاد که دو ایستگاه قصد استفاده از محیط انتقال و ارسال اطلاعات را بصورت همزمان داشته باشند. در گفتگوی انسان ها ، مشکل فوق را می توان بصورت کاملا "دوستانه حل نمود. ما سکوت خواهیم کرد تا این شانس به سایرین برای حرف زدن داده شود.همانگونه که در زمان حرف زدن من، دیگران این فرصت را برای من ایجاد کرده بودند! ایستگاههای اترنت زمانیکه قصد ارسال اطلاعات را داشته باشند، به محیط انتقال گوش فرا داده تا به این اطمینان برسند که تنها ایستگاه موجود برای ارسال اطلاعات می باشند. در صورتیکه ایستگاههای ارسال کننده اطلاعات متوجه نقص در ارسال اطلاعات خود گردند ،از بروز یک تصادم در محیط انتقال آگاه خواهند گردید. در زمان بروز تصادم ، هر یک از ایستگاههای مربوطه به مدت زمانی کاملا "تصادفی در حالت انتظار قرار گرفته و پس از اتمام زمان انتظار می بایست برای ارسال اطلاعات شرط آزاد بودن محیط انتقال را بررسی نمایند! توقف تصادفی و تلاش مجدد یکی از مهمترین بخش های پروتکل است . محدودیت های اترنت یک شبکه اترنت دارای محدودیت های متفاوت از ابعاد گوناگون (بکارگیری تجهیزات) است .طول کابلی که تمام ایستگاهها بصورت اشتراکی از آن بعنوان محیط انتقال استفاده می نمایند یکی از شاخص ترین موارد در این زمنیه است . سیگنال های الکتریکی در طول کابل بسرعت منتشر می گردند. همزمان با طی مسافتی، سیگنال ها ضعیف می گردند. وجود میدان های الکتریکی که توسط دستگاههای مجاور کابل نظیرلامپ های فلورسنت ایجاد می گردد ، باعث تلف شدن سیگنال می گردد. طول کابل شبکه می بایست کوتاه بوده تا امکان دریافت سیگنال توسط دستگاه های موجود در دو نقطه ابتدائی و انتهائی کابل بصورت شفاف و با حداقل تاخیر زمانی فراهم گردد. همین امر باعث بروز محدودیت در طول کابل استفاده شده، می گردد پروتکل CSMA/CD امکان ارسال اطلاعات برای صرفا "یک دستگاه را در هر لحظه فراهم می نماید، بنابراین محدودیت هائی از لحاظ تعداد دستگاههائی که می توانند بر روی یک شبکه مجزا وجود داشته باشند، نیز بوجود خواهد آمد. با اتصال دستگاه های متعدد (فراوان) بر روی یک سگمنت مشترک، شانس استفاده از محیط انتقال برای هر یک از دستگاه های موجود بر روی سگمنت کاهش پیدا خواهد کرد. در این حالت هر دستگاه بمنظور ارسال اطلاعات می بایست مدت زمان زیادی را در انتظار سپری نماید . تولید کنندگان تجهیزات شبکه دستگاه های متفاوتی را بمنظور غلبه بر مشکلات و محدودیت گفته شده ، طراحی و عرضه نموده اند. اغلب دستگاههای فوق مختص شبکه های اترنت نبوده ولی در سایر تکنولوژی های مرتبط با شبکه نقش مهمی را ایفاء می نمایند. تکرارکننده (Repeater) اولین محیط انتقال استفاده شده در شبکه های اترنت کابل های مسی کواکسیال بود که Thicknet (ضخیم) نامیده می شوند. حداکثر طول یک کابل ضخیم ۵۰۰ متر است . در یک ساختمان بزرگ ، کابل ۵۰۰ متری جوابگوی تمامی دستگاه های شبکه نخواهد بود. تکرار کننده ها با هدف حل مشکل فوق، ارائه شده اند. . تکرارکننده ها ، سگمنت های متفاوت یک شبکه اترنت را به یکدیگر متصل می کنند. در این حالت تکرارکننده سیگنال ورودی خود را از یک سگمنت اخذ و با تقویت سیگنال آن را برای سگمنت بعدی ارسال خواهد کرد. بدین ترتیب با استفاده از چندین تکرار کننده و اتصال کابل های مربوطه توسط آنان ، می توان قطر یک شبکه را افزایش داد. (قطر شبکه به حداکثر مسافت موجود بین دو دستگاه متمایز در شبکه اطلاق می گردد) Bridges و سگمنت شبکه های اترنت همزمان با رشد (بزرگ شدن) دچار مشکل تراکم می گردند. در صورتیکه تعداد زیادی ایستگاه به یک سگمنت متصل گردند، هر یک

دارای ترافیک خاص خود خواهند بود . در شرایط فوق ، ایستگاههای متعددی قصد ارسال اطلاعات را دارند ولی با توجه به ماهیت این نوع از شبکه ها در هر لحظه یک ایستگاه شانس و فرصت استفاده از محیط انتقال را پیدا خواهد کرد. در چنین وضعیتی تعداد تصادم در شبکه افزایش یافته و عملا "کارآئی شبکه افت خواهد کرد. یکی از راه حل های موجود بمنظور برطرف نمودن مشکل تراکم در شبکه تقسیم یک سگمنت به چندین سگمنت است . با این کار برای تصادم هائی که در شبکه بروز خواهد کرد، دامنه وسیعتری ایجاد می گردد.راه حل فوق باعث بروز یک مشکل دیگر می گردد: سگمنت ها قادر به اشتراک اطلاعات با یکدیگر نخواهند بود. بمنظور حل مشکل فوق، Bridges در شبکه اترنت پیاده سازی شده است . Bridge دو و یا چندین سگمنت را به یکدیگر متصل خواهد کرد. بدین ترتیب دستگاه فوق باعث افزایش قطر شبکه خواهد شد. عملکرد Bridge از بعد افزایش قطر شبکه نظیر تکرارکننده است ، با این تفاوت که Bridge قادر به ایجاد نظم در ترافیک شبکه نیز خواهد بود . Bridge نظیر سایر دستگاههای موجود در شبکه قادر به ارسال و دریافت اطلاعات بوده ولی عملکرد آنها دقیقا "مشابه یک ایستگاه نمی باشد. Bridge قادر به ایجاد ترافیکی که خود سرچشمه آن خواهد بود، نیست (نظیر تکرارکننده) .Bridge صرفا "چیزی را که از سایر ایستگاهها می شنود ، منعکس می نماید. (Bridge قادر به ایجا د یک نوع فریم خاص اترنت بمنظور ایجاد ارتباط با سایر Bridge ها می باشند) همانگونه که قبلا "اشاره گردید هر ایستگاه موجود در شبکه تمام فریم های ارسال شده بر روی محیط انتقال را دریافت می نماید.(صرفنظر ازاینکه مقصد فریم همان ایستگاه باشد و یا نباشد.) Bridge با تاکید بر ویژگی فوق سعی بر تنظیم ترافیک بین سگمنت ها دارد. همانگونه که در شکل فوق مشاهده می گردد Bridge دو سگمنت را به یکدیگر متصل نموده است . در صورتیکه ایستگاه A و یا B قصد ارسال اطلاعات را داشته باشند Bridge نیز فریم های اطلاعاتی را دریافت خواهد کرد. نحوه برخورد Bridge با فریم های اطلاعاتی دریافت شده به چه صورت است؟ آیا قادر به ارسال اتوماتیک فریم ها برای سگمنت دوم می باشد؟ یکی ازاهداف استفاده از Bridge کاهش ترافیک های غیرضروری در هر سگمنت است . در این راستا، آدرس مقصد فریم ، قبل از هر گونه عملیات بر روی آن، بررسی خواهد شد. در صورتیکه آدرس مقصد، ایستگاههای A و یا B باشد نیازی به ارسال فریم برای سگمنت شماره دو وجود نخواهد داشت . در این حالت Bridge عملیات خاصی را انجام نخواهد داد. نحوه برخورد Bridge با فریم فوق مشابه فیلتر نمودن است . درصورتیکه آدرس مقصد فریم یکی از ایستگاههای C و یا D باشد و یا فریم مورد نظر دارای یک آدرس از نوع Bradcast باشد ، Bridge فریم فوق را برای سگمنت شماره دو ارسال خواهد کرد. با ارسال و هدایت فریم اطلاعاتی توسط Bridge امکان ارتباط چهار دستگاه موجود در شبکه فراهم می گردد. با توجه به مکانیزم فیلتر نمودن فریم ها توسط Bridge ، این امکان بوجود خواهد آمد که ایستگاه A اطلاعاتی را برای ایستگاه B ارسال و در همان لحظه نیز ایستگاه C اطلاعاتی را برای ایستگاه D ارسال نماید.بدین ترتیب امکان برقراری دو ارتباط بصورت همزمان بوجود آمده است . روترها : سگمنت های منطقی با استفاده از Bridge امکان ارتباط همزمان بین ایستگاههای موجود در چندین سگمنت فراهم می گردد. Bridge در رابطه با ترافیک موجود در یک سگمنت عملیات خاصی را انجام نمی دهد. یکی از ویژگی های مهم Bridge ارسالی فریم های اطلاعاتی از نوع Bradcast برای تمام سگمنت های متصل شده به یکدیگر است. همزمان با رشد شبکه و گسترش سگمنت ها، ویژگی فوق می تواند سبب بروز مسائلی در شبکه گردد. زمانیکه تعداد زیادی از ایستگاه های موجود در شبکه های مبتنی بر Bridge ، فریم های Bradcast را ارسال می نمایند، تراکم اطلاعاتی بوجود آمده بمراتب بیشتر از زمانی خواهد بود که تمامی دستگاهها در یک سگمنت قرار گرفته باشند. روتر یکی از دستگاههای پیشرفته در شبکه بوده که قادر به تقسیم یک شبکه به چندین شبکه منطقی مجزا است . روتر ها یک محدوده منطقی برای هر شبکه ایجاد می نمایند. روترها بر اساس پروتکل هائی که مستقل از تکنولوژی خاص در یک شبکه است، فعالیت می نمایند. ویژگی فوق این امکان را برای روتر فراهم خواهد کرد که چندین شبکه با تکنولوژی های متفاوت را به یکدیگر مرتبط نماید. استفاده از روتر در

شبکه های محلی و گسترده امکان پذیراست . وضعیت فعلی اترنت از زمان مطرح شدن شبکه های اترنت تاکنون تغییرات فراوانی از بعد تنوع دستگاه های مربوطه ایجاد شده است . در ابتدا از کابل کواکسیال در این نوع شبکه ها استفاده می گردید.امروزه شبکه های مدرن اترنت از کابل های بهم تابیده و یا فیبر نوری برای اتصال ایستگاه ها به یکدیگر استفاده می نمایند. در شبکه های اولیه اترنت سرعت انتقال اطلاعات ده مگابیت در ثانیه بود ولی امروزه این سرعت به مرز ۱۰۰و حتی ۱۰۰۰ مگابیت در ثانیه رسیده است . مهمترین تحول ایجاد شده در شبکه های اترنت امکان استفاده از سوئیچ های اترنت است .سگمنت ها توسط سوئیچ به یکدیگر متصل می گردند. (نظیر Bridge با این تفاوت عمده که امکان اتصال چندین سگمنت توسط سوئیچ فراهم می گردد) برخی از سوئیچ ها امکان اتصال صدها سگمنت به یکدیگر را فراهم می نمایند. تمام دستگاههای موجود در شبکه، سوئیچ و یا ایستگاه می باشند . قبل از ارسال فریم های اطلاعاتی برا ی هر ایستگاه ، سوئیچ فریم مورد نظر را دریافت و پس از بررسی، آن را برای ایستگاه مقصد مورد نظر ارسال خواهد کرد . عملیات فوق مشابه Bridge است ، ولی در مدل فوق هر سگمنت دارای صرفا "یک ایستگاه است و فریم صرفا "به دریافت کننده واقعی ارسال خواهد شد. بدین ترتیب امکان برقراری ارتباط همزمان بین تعداد زیادی ایستگاه در شبکه های مبتنی بر سوئیچ فراهم خواهد شد. همزمان با مطرح شدن سوئیچ های اترنت مسئله Full-duplex نیز مطرح گردید. Full-dulex یک اصطلاح ارتباطی است که نشاندهنده قابلیت ارسال و دریافت اطلاعات بصورت همزمان است . در شبکه های اترنت اولیه وضعیت ارسال و دریافت اطلاعات بصورت یکطرفه (half-duplex) بود.در شبکه های مبتنی بر سوئیچ، ایستگاهها صرفا "با سوئیچ ارتباط برقرار کرده و قادر به ارتباط مستقیم با یکدیگر نمی باشند. در این نوع شبکه ها از کابل های بهم تابیده و فیبر نوری استفاده و سوئیچ مربوطه دارای کانکتورهای لازم در این خصوص می باشند.. شبکه های مبتنی بر سوئیچ عاری از تصادم بوده و همزمان با ارسال اطلاعات توسط یک ایستگاه به سوئیچ ، امکان ارسال اطلاعات توسط سوئیچ برای ایستگاه دیگر نیز فراهم خواهد شد. اترنت و استاندارد ۸۰۲.۳ شاید تاکنون اصطلاح ۸۰۲.۳ را در ارتباط با شبکه های اترنت شنیده باشید . اترنت بعنوان یک استاندارد شبکه توسط شرکت های : دیجیتال، اینتل و زیراکس (DIX) مطرح گردید. در سال ۱۹۸۰ موسسه IEEE کمیته ای را مسئول استاندار سازی تکنولوژی های مرتبط با شبکه کرد. موسسه IEEE نام گروه فوق را ۸۰۲ قرار داد. (عدد ۸۰۲ نشاندهنده سال و ماه تشکیل کمیته استاندارسازی است) کمیته فوق از چندین کمیته جانبی دیگر تشکیل شده بود . هر یک از کمیته های فرعی نیز مسئول بررسی جنبه های خاصی از شبکه گردیدند. موسسه IEEE برای تمایز هر یک از کمیته های جانبی از روش نامگذاری : X۸۰۲.X استفاده کرد. X یک عدد منصر بفرد بوده که برای هر یک از کمیته ها در نظر گرفته شده بود . گروه ۸۰۲.۳ مسئولیت استاندارد سازی عملیات در شبکه های CSMA/CD را برعهده داشتند. (شبکه فوق در ابتدا DIX Ethernet نامیده می شد) اترنت و ۸۰۲.۳ از نظر فرمت داده ها در فریم های اطلاعاتی با یکدیگر متفاوت می باشند. تکنولوژی های متفاوت شبکه متداولترین مدل موجود در شبکه های کامپیوتری(رویکرد دیگری از اترنت) توسط شرکت IBM و با نام Tken ring عرضه گردید. در شبکه های اترنت بمنظور دستیابی از محیط انتقال از فواصل خالی (Gap) تصادفی در زمان انتقال فریم ها استفاده می گردد. شبکه های Tken ring از یک روش پیوسته در این راستا استفاده می نمایند. در شبکه های فوق ، ایستگاه ها از طریق یک حلقه منطقی به یکدیگر متصل می گردند. فریم ها صرفا "در یک جهت حرکت و پس از طی طول حلقه ، فریم کنار گذاشته خواهد شد. روش دستیابی به محیط انتقال برای ارسال اطلاعات تابع CSMA/CD نخواهد بود و از روش Tken passing استفاده می گردد. در روش فوق در ابتدا یک Tken (نوع خاصی از یک فریم اطلاعاتی) ایجاد می گردد . Tken فوق در طول حلقه می چرخد . زمانیکه یک ایستگاه قصد ارسال اطلاعات را داشته باشد، می بایست Tken را در اختیار گرفته و فریم اطلاعاتی خود را بر روی محیط انتقال ارسال دارد. زمانیکه فریم ارسال شده مجددا "به ایستگاه ارسال کننده برگشت داده شد (طی نمودن مسیر حلقه)، ایستگاه فریم خود را حذف و یک Tken جدید را ایجاد وآن را بر روی حلقه قرار خواهد داد. در اختیار گرفتن

Tken شرط لازم برا ی ارسال اطلاعات است . سرعت ارسال اطلاعات در این نوع شبکه ها چهار تا شانزده مگابیت در ثانیه است . اترنت با یک روند ثابت همچنان به رشد خود ادامه می دهد. پس از گذشت حدود سی سال ازعمر شبکه های فوق استانداردهای مربوطه ایجاد و برای عموم متخصصین شناخته شده هستند و همین امر نگهداری و پشتیبانی شبکه های اترنت را آسان نموده است . اترنت با صلابت بسمت افزایش سرعت و بهبود کارآئی و عملکرد گام بر می دارد.

شبکه گیگابایتی چیست؟

شبکه های متصل با سیم نیز در کنار شبکه های بی سیم در حال پیشرفت اند. این پیشرفت باعث شده تا کامپیوترهای رو میزی بتوانند با سرعت ۱۰۰۰ مگابایت بر ثانیه به یکدیگر متصل شوند. چندی است که نسل تازه ای از شبکه های متصل با سیم با نام Eethernet گیگا بیتی زیر سایه و درهیاهوی شبکه های بی سیم متولد شده. این استاندارد که که طراحی آن از حدود ۶ سال پیش آغاز شده بود سرانجام به بار نشست و سرعت آن چهار برابر پر سرعت ترین شبکه بی سیم کنونی است. کنترل کننده های Ethernet گیگا بایتی کم کم جای خود را روی بردهای اصلی بازکرده و جای کنترل کننده های Fast Ethernet را با سرعت ۱۰۰ مگا بیت بر ثانیه می گیرند. آزمایش های نشان داده اند که سرعت شبکه های Ethernet گیگا بیتی در عمل به ۹۰ مگا بیت بر ثانیه می رسد. این میزان برابر است با ده برابر سرعت Fast Ethernet. آهنگ انتقال در Ethernet گیگابیتی در حال حاضر از هر سخت دیسکی بیشتر است. بنا براین هنگام کار با فایل های ویدئویی یا CAD که روی کامپیوتر های سرویس دهنده ذخیره شده اند، شبکه سرعت کار را کاهش نمی دهد. هر چه سریعتر، هر چه ارزانتر با گسترش کنترل کننده های گیگابیتی، در خواست برای سوئیچ های مناسب نیز رو به افزایش است. قیمت این دستگاه ها هم به طور همزمان رو به کاهش است به طوری که یک سوئیچ گیگا بیتی با ۸ درگاه سال گذشته حدود ۲۰۰۰ یورو پایین آمده. Ethernet گیگا بیتی با سرعت زیادی که دارد برای انتقال داده ها روی شبکه های محلی هم بسیار مناسب است. دستگاه های Ethernet گیگا بیتی اگر چه با گونه های پیشین یعنی Fast Ethernet و Ethernet مگا بیتی سازگارند اما برای بهره مندی از بیشترین سرعت باید از هر ۴ زوج سیم استفاده کرد. افزون بر این از یک مدولاسیون پنج سطحی نیز استفاده می شود. همه اینها به این معنی است که روی هر زوج سیم و در هر تپش با بسامد ۱۰۰ مگا هرتز بیش از دو بیت منتقل می شود. در نتیجه بیش از یک گیگابیت بر ثانیه فرستاده می شود که بخشی از این پهنای باند اضافی برای رمز گذاری داده ها با شیوه Trellis به کار می رود. داده هایی که در این شیوه به جریان داده های اضافه می شود پایداری و ایمنی این شبکه ها را افزایش می دهد. کابل ها یکسان نیستند برای بهره مندی از بیشترین سرعت، باید کابل ها را کمی پیچیده تر ساخت. کابل های ۴ رشته ای Cat۵ که در Fast Ethernet در فاصله های کوتاه به کار می روند در Ethernet گیگا بیتی قابل استفاده نیستند و سرعت این دستگاه ها را تا حد Fast Ethernet کاهش می دهند. جالب است بدانید که در سخت افزار گیگا بیتی تفاوتی میان درگاه های Uplink و Dwnlink وجود ندارند. هر دستگاه طرف مقابل را شناسایی کرده و بسته به اینکه در سمت دیگر یک کارت شبکه یا یک سوئیچ قرار داشته باشد خود را تنظیم می کند. کابل های هشت رشته ای هم از نظر کیفیت با هم تفاوت دارند. قیمت کابل های Cat۶ به طور نظری امکان استفاده از بسامد ۳۰۰ مگا هرتز را فراهم می کند و آهنگ انتقال آن در مقایسه با Cat۵ روی هر جفت سیم سه برابر است. طول کابل Cat۶ حداکثر ۱۰۰ متر است که در صورت استفاده از یک سوئیچ می توان دو دستگاه کامپیوتر به فاصله ۲۰۰ متر را به یکدیگر متصل کرد. اما در این کابل ها در مقایسه با Cat۵ ویژگی آبشاری (Cascading) بسیار محدودتر شده به طوری که به جای امکان استفاده از پنج سوئیچ پشت سر هم (که فاصله را به ۶۰۰ متر می رسانند) تنها می توان از دو سوئیچ استفاده کرد که حداکثر فاصله را به ۳۰۰ متر محدود می کند. بنا براین در ساختمان های بزرگ برای استفاده از کابل های Cat۶ وجود Ruter لازم است. در صورت افزایش

فاصله (برای نمونه میان دو ساختمان) باید به جای کابل های مسی، کابل های فیبر نوری را به کار برد. در این کابل های فیبر نوری Single Mde، فاصله می تواند تا پنج کیلومتر افزایش یابد. این را هم بگوییم که تجهیزات استفاده از فیبر نوری بیش از ده برابر تجهیزات کابل Cat۵ قیمت دارند. سرعت بسیار بالا برای کامپیوترهای شخصی بد نیست فاصله های زیاد را به حال خود گذاشته و کمی کاربرد شبکه های گیگابیتی را در کامپیوترهای شخصی بررسی کنیم. پهنای باندی که این شبکه ها فراهم می کنند برخی تغییرات را در سخت افزار کامپیوترهای شخصی ایجاب می کند. کارت شبکه گیگا بیتی در حالت دو طرفه کامل (Full Duplex) کار می کند. یعنی می تواند همزمان داده را فرستاده و دریافت کند که این آهنگ انتقال ۱۸۰ مگابایت در ثانیه را به دست می دهد در حالی که پهنای باند گذرگاه PCI تنها ۱۳۳ مگابایت برثانیه است. البته اگر در سیستم کارت PCI دیگری مانند کارت صوتی یا کنترل کننده RAID وجود داشته باشد این پهنای باند ۱۳۳ مگابایتی باز هم کاهش یافته و باقیمانده آن دراختیار کارت شبکه قرار می گیرد. بنابراین بی دلیل نیست که کارت های شبکه ویژه کامپیوتر های سرویس دهنده که با معماری ۶۴ بیتی ساخته می شوند پهنای باند ۵۳۳ یا حتی ۱۰۶۶ مگابیتی دارند. در مقابل، بیشتر کارت های شبکه یک پارچه با برد اصلی از نظر آهنگ انتقال داده با کارت های شبکه PCI تفاوتی ندارند چون آنها نیز به درگاه PCI کند متصل اند. تنها راه حل اینتل در سری تراشه های i۸۶۵ و i۸۷۵ با نام CSA) Cmmunicatins Streaming Architecture) است که این گلوگاه را تقریبا برطرف کرده. در این شیوه، کنترل کننده شبکه از طریق یک مسیر اختصاصی با آهنگ انتقال ۲۶۶ مگابایت بر ثانیه به سری تراشه متصل می شود. در نتیجه، بخش های دیگر نمی توانند سرعت آن را پایین بیاورند. بد نیست در اینجا اشاره کنیم که این کنترل کننده های اینتل در عمل به سرعت ۱۵۰ مگا بایت بر ثانیه دست پیدا می کنند در حالی که کنترل کننده های یکپارچه با برد اصلی مانند Bradcm ،۳Cm یا VIA آن هم بدون وجود کارت های PCI دیگری حتی تا نصف پایین می آید. آنچه که در این میان بسیار عجیب است اینست که برخی شرکت های سازنده برد اصلی هیچ تمایلی به بهره برداری از این فناوری اینتل ندارند و با وجود تراشه های سری تراشه های i۸۷۵، i۸۶۵ روی محصولاتسان باز هم آنها را با کنترل کننده های Bradcm مجهز می کنند. استانداردسازی سری تراشه های که در آینده به بازار می آیند این مشکل را برطرف می کنند چون نه تنها گذرگاه پر سرعت PCI Experss را با خود دارند بلکه کنترل کننده شبکه گیگابایتی نیز با آنها یکپارچه شده. به نظر نمی رسد که Ethernet بتواند در بخش کامپیوترهای شخصی به سرعت های بالاتر دست پیدا کند. اگر چه همین حالا- نیز استاندارد ۱۰ Ethernet گیگابایتی تعریف شده و دستگاه های سخت افزاری آن در دست ساخت هستند اما برای بهره مندی از سرعت بالای آن چاره به جز رفتن به سراغ کابل های فیبر نوری نیست. اگر روش های تشخیص خطا یا اندازه Packet در پروتکل Ethernet تغییر نکنند در شبکه های ۱۰ Ethernet گیگابایتی حداکثر می توان از کابل های مسی به طول ۱۰ متر استفاده کرد که برای پیاده سازی عملی شبکه ها بسیار کوتاه است.

Prxy Server چیست ؟

Prxy Server نرم افزاری است که در یک شبکه حد واسط بین اینترنت و کاربران واقع می شود. فلسفه ایجاد Prxy Server قراردادن یک خط اینترنت در اختیار تعداد بیش از یک نفر استفاده کننده در یک شبکه بوده است ولی بعدها امکانات و قابلیتهایی به Prxy Server افزوده شد که کاربرد آن را فراتر از به اشتراک نهادن خطوط اینترنت کرد . بطور کلی Prxy Server ها در چند مورد کلی استفاده می شوند . یک کاربرد Prxy Server ها ، همان به اشتراک گذاشتن یک خط اینترنت برای چند کاربر است که باعث کاهش هزینه و کنترل کاربران و همچنین ایجاد امنیت بیشتر می شود . کاربرد دوم Prxy Serverها ، در سایتهای اینترنتی به عنوان Firewall می باشد . کاربرد سوم که امروزه از آن بسیار استفاده می شود ، Caching اطلاعات است . با توجه

به گران بودن هزینه استفاده از اینترنت و محدود بودن پهنای باند ارتباطی برای ارسال و دریافت اطلاعات ، معمولا "نمی توان به اطلاعات مورد نظر در زمان کم و با سرعت مطلوب دست یافت . امکان Caching اطلاعات ، برای کمک به رفع این مشکل در نظر گرفته شده است . Prxy Server ، سایتهایی را که بیشتر به آنها مراجعه می شود را دریک حافظه جداگانه نگاه می دارد. به این ترتیب برای مراجعه مجدد به آنها نیازی به ارتباط از طریق اینترنت نیست بلکه به همان حافظه مخصوص رجوع خواهد شد . این امر باعث می گردد از یک طرف زمان دسترسی به اطلاعات کمتر شده و از سوی دیگر چون اطلاعات از اینترنت دریافت نمی شود ، پهنای باند محدود موجود با اطلاعات تکراری اشغال نشود . بخصوص آنکه معمولا "تغییرات در یک Website محدود به یک یا دو صفحه می باشد و گرفتن اطلاعات از اینترنت بدون Caching به معنای گرفتن کل سایت می باشد حال آنکه با استفاده از Prxy Server و امکان Caching اطلاعات ، میتوان تنها صفحات تغییر کرده را دریافت کرد ویژگیهای Prxy Server ویژگی اول : با استفاده از Prxy Server می توان از اکثر پروتکلهای موجود در شبکه های محلی در محدوده نرم افزارهای کاربردی در شبکه های LAN مرتبط با اینترنت استفاده کرد . Prxy Server پروتکلهای پر کاربرد شبکه های محلی مانند IPX/SPX (مورد استفاده در شبکه های ناول) ، NETBEUI (مورد استفاده در شبکه های LAN با تعداد کاربران کم) و TCP/IP (مورد استفاده در شبکه های Intranet) را پشتیبانی می کند. با این ترتیب برای اینکه بتوان از یک نرم افزار کاربردی شبکه LAN که مثلا "با پروتکل IPX/SPX روی ناول نوشته شده ، روی اینترنت استفاده کرد نیازی نیست که قسمتهای مربوط به ارتباط با شبکه که از Functin Call های API استفاده کرده را به Functin Call های TCP/IP تغییر داد بلکه Prxy Server خود این تغییرات را انجام داده و می توان به راحتی از نرم افزاری که تا کنون تحت یک شبکه LAN با ناول کار می کرده است را در شبکه ای که مستقیما "به اینترنت متصل است ، استفاده کرد . همین ویژگی درباره سرویسهای اینترنت مانند , Pp۳ , IRC RealAudi , Gpher , Telnet , FTP و . . . وجود دارد . به این معنا که هنگام پیاده سازی برنامه با یک سرویس یا پروتکل خاص ، محدودیتی نبوده و کدی در برنامه برای ایجاد هماهنگی نوشته نمی شود . ویژگی دوم : با Cache کردن اطلاعاتی که بیشتر استفاده می شوند و با بروز نگاه داشتن آنها ، قابلیت سرویسهای اینترنت نمایان تر شده و مقدار قابل توجهی در پهنای باند ارتباطی صرفه جویی می گردد. ویژگی سوم : Prxy Server امکانات ویژه ای برای ایجاد امنیت در شبکه دارد . معمولا "در شبکه ها دو دسته امنیت اطلاعاتی مد نظر است . یکی آنکه همه کاربران شبکه نتوانند از همه سایتها استفاده کنند و دیگر آنکه هر کسی نتواند از روی اینترنت به اطلاعات شبکه دسترسی پیدا کند . با استفاده از Prxy Server نیازی نیست که هر Client بطور مستقیم به اینترنت وصل شود در ضمن از دسترسی غیرمجاز به شبکه داخلی جلوگیری می شود . همچنین می توان با استفاده از SSL (Secure Sckets Layers) امکان رمز کردن داده ها را نیز فراهم آورد. ویژگی چهارم : Prxy Server بعنوان نرم افزاری که می تواند با سیستم عامل شما مجتمع شود و همچنین با IIS (Internet Infrmatin Server) سازگار می باشد، استفاده می گردد. خدمات Prxy Server Prxy Server سه سرویس در اختیار کاربران خود قرار می دهد: ۱-Web Prxy Service : این سرویس برای Web Publishing یا همان ایجاد Web Site های مختلف درشبکه LAN مفید می باشد . برای این منظور قابلیت مهم Reverse Prxing در نظر گرفته شده است . Reverse Prxing امکان شبیه سازی محیط اینترنت درمحیط داخل می باشد. به این ترتیب فرد بدون ایجاد ارتباط فیزیکی با اینترنت می تواند برنامه خود را همچنان که در محیط اینترنت عمل خواهد کرد، تست کرده و مورد استفاده قرا دهد. این قابلیت در بالا بردن سرعت و کاهش هزینه تولید نرم افزارهای کاربردی تحت اینترنت موثر است. ۲-Winsck Prxy Service : منظور، امکان استفاده از API Callهای Winsck در Windws است . در Functin Call ، Windws های مورد استفاده در سرویسهای اینترنت مانند Gpher ، FTP ، Telnet و . . . ، تحت عنوان Winsck Prtcls معرفی شده اند. در حقیقت برای استفاده از این

سرویسها در نرم افزارهای کاربردی نیازی نیست که برنامه نویس چگونگی استفاده از این سرویسها را پیش بینی کند. ۳-Scks Prxy Service : این سرویس، سرویس Scks ۴.۳a را پشتیبانی می کند که در واقع زیر مجموعه ای از Winsck می باشد و امکان استفاده از Http ۱.۰۲ و بالاتر را فراهم می کند. به این ترتیب می توان در طراحی Website خارج از ، Firewall Security ایجاد کرد. معیارهای موثر در انتخاب ۱ Prxy Server- سخت افزار مورد نیاز : برای هر چه بهتر شدن توانمندیهای Prxy Server ، باید سخت افزار آن توانایی تحمل بار مورد انتظار را داشته باشد . ۲- نوع رسانه فیزیکی برای ارتباط با اینترنت : راه حلهای مختلفی برای اتصال به شبکه اینترنت وجود دارد . ساده ترین راه ، استفاده از مودم و خطوط آنالوگ می باشد . راه دیگر استفاده از ISDN و خطوط دیجیتال است که هم احتیاج به تبدیل اطلاعات از آنالوگ به دیجیتال و برعکس در ارسال و دریافت اطلاعات ندارد و هم از سرعت بالاتری برخوردار است . روش دیگر استفاده از خط های T۱/E۱ با ظرفیت انتقال گیگا بایت می باشد . پیشنهاد می شود که در شبکه های با کمتر از ۲۵۰ کاربر از ISDN و از ۲۵۰ کاربر به بالا از T۱/E۱ استفاده شود . (البته در ایران به علت عدم وجود خطوط ISDN و کمبود خطوط T۱/E۱ این استانداردها کمتر قابل پیاده سازی هستند.) ۳- هزینه ارتباط با اینترنت : دو عامل موثر در هزینه اتصال به اینترنت ، پهنای باند و مانایی ارتباط می باشد . هر چه مرورگرهای اینترنتی بیشتر و زمان استفاده بیشتر باشد ، هزینه بالاتر خواهد بود . با توجه به اینکه Prxy Server می تواند با Caching اطلاعات این موارد را بهبود بخشد ، بررسی این عامل می تواند در تعیین تعداد Prxy های مورد استفاده موثر باشد . ۴- نوع و نحوه مدیریت سایت : این عامل نیز در تعیین تعداد Prxyها موثر است . مثلا "اگر در شبکه ای مشکل راهبری وجود داشته باشد ، با اضافه کردن تعداد Prxyها ، مشکل راهبری نیز بیشتر خواهد شد . ۵- پروتکل های مورد استفاده : Prxy Server ها معمولا" از پروتکلهای TCP/IP و یا IPX/SPX برای ارتباط با Client ها استفاده می کنند . بنابراین برای استفاده از Prxy باید یکی از این پروتکل ها را در شبکه استفاده کرد . پیشنهاد می شود در شبکه های کوچک با توجه به تعداد کاربرها Prxy Server و Web Server روی یک کامپیوتر تعبیه شوند و در شبکه های متوسط یا بزرگ تعدادserver Prxyها بیش از یکی باشد .

کلیات امنیت شبکه

وقتی بحث امنیت شبکه پیش می اید ، مباحث زیادی قابل طرح و ارائه هستند ، موضوعاتی که هر کدام به تنهایی می توانند جالب ، پرمحتوا و قابل درک باشند ، اما وقتی صحبت کار عملی به میان می اید ، قضیه یک جورایی پیچیده می شود . ترکیب علم و عمل ، احتیاج به تجربه دارد و نهایت هدف یک علم هم ، به کار امدن ان هست . وقتی دوره تئوری امنیت شبکه را با موفقیت پشت سر گذاشتید و وارد محیط کار شدید ، ممکن است این سوال برایتان مطرح شود که " خب ، حالا از کجا شروع کنم ؟ اول کجا را ایمن کنم ؟ چه استراتژی را پیش بگیرم و کجا کار را تمام کنم " ؟ انبوهی از این قبیل سوالات فکر شما را مشغول می کند و کم کم حس می کنید که تجربه کافی ندارید و این البته حسی طبیعی هست . پس اگر این حس رو دارید و می خواهید یک استراتژی علمی – کاربردی داشته باشید ، تا انتهای این مقاله با من باشید تا قدم به قدم شما رو به امنیت بیشتر نزدیک کنم. همیشه در امنیت شبکه موضوع لایه های دفاعی ، موضوع داغی هست و نظرات مختلفی وجود دارد . عده ای فایروال را اولین لایه دفاعی می دانند ، بعضی ها هم Access List رو اولین لایه دفاعی می دانند ، اما واقعیت پنهان این هست که هیچکدام از اینها ، اولین لایه دفاعی نیستند . یادتون باشد که اولین لایه دفاعی در امنیت شبکه و حتی امنیت فیزیکی ، Plicy هست . بدون plicy ، لیست کنترل ، فایروال و هر لایه دیگر ، بدون معنی می شود و اگر بدون plicy شروع به ایمن کردن شبکه کنید ، محصول یک آبکش واقعی از کار در می اید . با این مقدمه ، و با توجه به این که شما plicy مورد نظرتان را کاملا تجزیه و تحلیل کردید و دقیقا می دانید که چه چیزی رو می خواهید و چی را احتیاج ندارید ، کار را شروع می کنیم . ما باید پنج مرحله رو پشت سر بگذاریم تا کارمان تمام

بشود . این پنج مرحله عبارتند از : ۱- Inspectin (بازرسی) ۲- Prtectin (حفاظت) ۳- Detectin (ردیابی) ۴- Reactin (واکنش) ۵- Reflectin (بازتاب) در طول مسیر ، از این پنج مرحله عبور می کنیم ، ضمن اینکه ایمن کردن شبکه به این شکل ، احتیاج به تیم امنیتی دارد و یک نفر به تنهایی نمی تواند این پروسه رو طی کند و اگر هم بتواند ، خیلی طولانی می شود و قانون حداقل زمان ممکن را نقض می کند . ۱- اولین جایی که ایمن کردن رو شروع می کنیم ، ایمن کردن کلیه authenticatin های موجود هست . معمولا رایج ترین روش authenticatin که مورد استفاده قرار می گیرد ، استفاده از شناسه کاربری و کلمه رمز هست. مهمترین جاهایی که باید authenticatin را ایمن و محکم کرد عبارتند از : - کلمات عبور کاربران ، به ویژه مدیران سیستم . - کلمات عبور سوییچ و روتر ها (من روی سوییچ خیلی تاکید میکنم ، چون این device به صورت plug and play کار می کند ، اکثر مدیرهای شبکه از cnfig کردن ان غافل می شوند ، در حالی که می تواند امنیت خیلی خوبی به شبکه بدهد ، به مدیران امنیتی توصیه میکنم که حتما این device رو کنترل کنند) . - کلمات عبور مربوط به SNMP . - کلمات عبور مربوط به پرینت سرور . - کلمات عبور مربوط به محافظ صفحه نمایش . آنچه که شما در کلاسهای امنیت شبکه در مورد Accunt and Passwrd Security یاد گرفتید را اینجا به کار می برید . که من به خاطر طولانی نشدن بحث به انها اشاره نمیکنم . ۲- قدم دوم نصب و به روز کردن آنتی ویروس بر روی همه دسکتاپ ، سرور و میل سرورها هست . ضمن اینکه آنتی ویروس های مربوط به کاربران باید به طور اتوماتیک به روز رسانی بشود و آموزشهای لازم در مورد فایلهای ضمیمه ایمیل ها و راهنمایی لازم جهت اقدام صحیح در صورت مشاهده موارد مشکوک یا اضطراری به کاربران هم داده بشود . ۳ - مرحله سوم شامل نصب آخرین به روز رسانی های امنیتی سیستم عامل و سرویسهای موجود هست . در این مرحله علاوه بر کارهای ذکر شده ، کلیه سرورها و device ها و دسک تاپ ها با ابزار های شناسایی حفره های امنیتی بررسی می شوند تا علاوه بر شناسایی و رفع حفره های امنیتی ، سرویس های غیر ضروری هم شناسایی و غیرفعال بشوند . ۴-در این مرحله نوبت گروه بندی کاربران و اعطای مجوزهای لازم به فایلها و دایرکتوری ها میباشد . ضمن اینکه accunt های قدیمی هم باید غیر فعال شوند . گروه بندی و اعطای مجوز بر اساس یکی از سه مدل استاندارد Access Cntrl Techniques یعنی DAC , MAC یا RBAC انجام می شود . بعد از پایان این مرحله ، یک بار دیگه امنیت سیستم عامل باید چک بشود تا چیزی فراموش نشده باشد . ۵- حالا نوبت device ها هست که معمولا شامل روتر ، سوییچ و فایروال می شود . بر اساس plicy موجود و توپولوژی شبکه ، این bx ها باید cnfig بشوند . تکنولوژی هایی مثل NAT , PAT و filtering و غیره در این مرحله مطرح می شود و بر همین اساس این مرحله خیلی مهم هست. حتی موضوع مهم IP Addressing که از وظایف مدیران شبکه هست می تواند مورد توجه قرار بگیرد تا اطمینان حاصل بشود که از حداقل ممکن برای IP Assign به شبکه ها استفاده شده است. ۶- قدم بعد تعیین استراژی backup گیری هست . نکته مهم که اینجا وجود دارد این هست که باید مطمئن بشویم که سیستم backup گیری و بازیابی به درستی کار می کند و بهترین حالت ممکن باشد . ۷- امنیت فیزیکی . اول از همه به سراغ UPS ها می رویم . باید چک کنیم که UPS ها قدرت لازم رو برای تامین نیروی الکتریکی لازم جهت کار کرد صحیح سخت افزار های اتاق سرور در زمان اضطراری رو داشته باشند . نکات بعدی شامل کنترل درجه حرارت و میزان رطوبت هست. همینطور ایمنی در برابر سرقت و آتش سوزی. سیستم کنترل حریق باید به شکلی باشد که به نیروی انسانی و سیستم های الکترونیکی آسیب وارد نکند . به طور کل آنچه که در مورد امنیت فیزیکی یاد گرفتید را در این مرحله به کار می برید . ۸- امنیت وب سرور یکی از موضوعاتی هست که روش باید وسواس داشته باشید. به همین دلیل در این قسمت کار ، مجددا و با دقت بیشتر وب سرور رو چک و ایمن می کنیم . در حقیقت ، امنیت وب رو اینجا لحاظ می کنیم . (اسکریپت های سمت سرویس دهنده رو هیچ وقت فراموش نکنید) ۹ - حالا نوبت چک ، تنظیم و تست سیستم های Auditing و Lgging هست . این سیستم ها هم می تواند بر پایه hst و هم بر پایه netwrk باشد .

سیستم های رد گیری و ثبت حملات هم در این مرحله نصب و تنظیم می شوند. باید مطمئن شوید که تمام اطلاعات لازم ثبت و به خوبی محافظت می شود . در ضمن ساعت و تاریخ سیستم ها درست باشد ، مبادا که اشتباه باشه که تمام زحماتتان در این مرحله به باد میرود . و امکان پیگیری های قانونی در صورت لزوم دیگر وجود ندارد . ۱۰- ایمن کردن Remte Access با پروتکل ها و تکنولوژی های ایمن و Secure قدم بعدی رو تشکیل می دهد. در این زمینه با توجه به شرایط و امکانات ، ایمن ترین پروتکل و تکنولوژی ها رو به خدمت بگیرید . ۱۱ - نصب فایروال های شخصی در سطح hst ها ، لایه امنیتی مضاعفی به شبکه شما میدهد . پس این مرحله رو فراموش نکنید . ۱۲ - شرایط بازیابی در حالت های اضطراری رو حتما چک و بهینه کنید . این حالت ها شامل خرابی قطعات کامپیوتری ، خرابکاری کاربران عادی ، خرابی ناشی از بلایای طبیعی (زلزله - آتش سوزی - افتادن - سرقت - سیل و ...) و خرابکاری ناشی از نفوذ هکرها ، میباشد . استاندارد های warm site و ht site را در صورت امکان رعایت کنید. یادتون باشد که " همیشه در دسترس بودن اطلاعات ، " جز، قوانین اصلی امنیتی هست . ۱۳- و قدم آخر این پروسه که در حقیقت شروع یک جریان همیشگی هست ، عضو شدن در سایتها و بولتن های امنیتی و در جریان آخرین اخبار امنیتی قرار گرفتن هست . برای همه شما عزیزان آرزوی سلامتی و موفقیت را دارم . مهدی قاسمی عضو گروه امنیتی آشیانه http://www.ashiyane.cm/ هفته قبل : مقدمات امنیت شبکه همانطور که میدانیم زندگی روزمره انسانی، در دنیای فیزیکی غالبا با تهدیدهائی از سوی مهاجمان، متجاوزان و قانون شکنان مواجه بوده است و برنامه‌ریزان و مدیران جوامع با اتخاذ تدابیر و با بکارگیری نیروهای سازمان یافته در پی مبارزه با تهدیدهای مذکور و محافظت از جان و منافع انسانی و نهایتا ایجاد امنیت در جامعه می‌باشند. طبیعی است با الزام حضور و ورود انسانها به دنیای مدرن ارتباطات و اینترنت (که توسط متخصصان علوم ارتباطات و رایانه بوجود آمده است) خطرات و تهدید مهاجمان که با بکارگیری روشهای گوناگون درصدد ایجاد اختلال، انهدام و یا وارد آوردن صدمه هستند، همواره وجود خواهد داشت. به همین جهت مبحث امنیت و ایجاد آن در دنیای الکترونیکی ارتباطات، جایگاه ویژه‌ای را در محافل گوناگون علمی فن‌آوری اطلاعات بدست آورده است. حال در خصوص شبکه‌های اطلاع‌رسانی و بخصوص اینترنت مبحث امنیت را میتوان از دو جنبه مورد بررسی قرار داد : امنیت سرویس دهندگان (Servers Security) امنیت کاربران یا استفاده کنندگان (Client Security) که در هر دو مورد با تهدیدهای بسیار جدی از سوی مهاجمان و مخربین «Hackers) مواجه هستیم. در حقیقت در این بخش سعی بر این است تا به بررسی جوانب گوناگون امنیت همچون بررسی انواع خطرات و تهدیدهای موجود با در نظر گرفتن زمینه‌های مورد علاقه مخربین، بررسی حفره‌ها و روشهای نفوذ و نحوه تخریب، بیان و معرفی نمونه پایگاه هایی که مورد یورش و تهاجم واقع شده‌اند، بررسی روشهای رویاروئی و مقابله با تهدیدها و خطرات، شناخت نرم‌افزارهای مرتبط و موجود در زمینه حفاظت و امنیت شبکه و ... می پردازیم . با توجه به گسترش زمینه‌های گوناگون استفاده از اینترنت بخصوص تبادلات بازرگانی و فعالیتهای اقتصادی و علاقمندی شدید مهاجمان به این نوع از تخریب ها در قدم اول سعی بر آنست تا به بررسی مباحث مربوط به تهدیدات سرویس دهندگان وب (Web Servers) و انواع آن پرداخته شود . ادامه ..... در ادامه بحث امنیت شبکه‌های وب، به بررسی عوامل تضعیف سرویس دهندگان وب و علل مهیا شدن زمینه نفوذ و تهاجم به سایت‌ها، بخصوص مراکز فعالیت‌های اقتصادی خواهیم پرداخت. همانطور که می‌دانیم ایجاد امکان مراودات الکترونیکی در اینترنت با احتساب مزایا و محاسن بیشمار خود، مشکلات عدیده ای را نیز به همراه داشته است. در حقیقت هر یک از طرفین (سرویس دهندگان و سرویس گیرندگان) با نگرانی های جدی مواجه هستند و در همین راستا، جهت ایمن‌سازی مراودات خود از یکدیگر انتظاراتی را مطرح می‌نمایند. ایجاد ایمنی و رفع هرگونه تهدید در انجام معلامات و یا تراکنش‌های اقتصادی، و نیز قانونمند و مطمئن بودن فعالیت و مخفی ماندن اطلاعات مربوطه به آن بعنوان توقعات مشتریان مطرح می‌شود و در مقابل فعالیت همراه با دقت کاربر، عدم انجام اعمال خلاف قوائد و قوانین شبکه و مراودات الکترونیکی و نهایتاً اجتناب از تخریب و یا صدمه‌زدن به سایت از

انتظارات سرویس دهندگان می‌باشد. در عین حال هر دو طرف از واسطه انتقال دهنده اطلاعات که همانا سیستم‌های مخابراتی هستند توقع جلوگیری از استراق اطلاعات و ... را خواهند داشت. در حقیقت در مباحث مربوط به امنیت شبکه، ایمنی کاربر، ایمنی سرویس‌دهنده و ایمنی مخابراتی از رئوس مطالب مورد توجه می‌باشند.

آشنایی با سوئیچ شبکه

آشنایی با سوئیچ شبکه سوئیچ شبکه از مجموعه ای کامپیوتر (گره) که توسط یک محیط انتقال (کابلی بدون کابل) بیکدیگر متصل می گردند ، تشکیل شده است. در شبکه از تجهیزات خاصی نظیر هاب و روتر نیز استفاده می گردد. سوئیچ یکی از عناصر اصلی و مهم در شبکه های کامپیوتری است . با استفاده از سوئیچ ، چندین کاربرقادربه ارسال اطلاعات از طریق شبکه در یک لحظه خواهند بود. سرعت ارسال اطلاعات هر یک از کاربران بر سرعت دستیابی سایر کاربران شبکه تاثیر نخواهد گذاشت . سوئیچ همانند روتر که امکان ارتباط بین چندین شبکه را فراهم می نماید ، امکان ارتباط گره های متفاوت (معمولا "کامپیوتر) یک شبکه را مستقیما "با یکدیگر فراهم می نماید. شبکه ها و سوئیچ ها دارای انواع متفاوتی می باشند.. سوئیچ هائی که برای هر یک از اتصالات موجود در یک شبکه داخلی استفاده می گردند ، سوئیچ های LAN نامیده می شوند. این نوع سوئیچ ها مجموعه ای از ارتباطات شبکه را بین صرفا "دو دستگاه که قصد ارتباط با یکدیگر را دارند ، در زمان مورد نظر ایجاد می نماید. مبانی شبکه عناصر اصلی در یک شبکه کامپیوتری بشرح زیر می باشند: شبکه . شبکه شامل مجموعه ای از کامپیوترهای متصل شده (با یک روش خاص)، بمنظور تبادل اطلاعات است . گره . گره ، شامل هر چیزی که به شبکه متصل می گردد ، خواهد بود.(کامپیوتر ، چاپگر و ...) سگمنت. سگمنت یک بخش خاص از شبکه بوده که توسط یک سوئیچ ، روتر و یا Bridge از سایر بخش ها جدا شده است . ستون فقرات . کابل اصلی که تمام سگمنت ها به آن متصل می گردند. معمولا "ستون فقرات یک شبکه دارای سرعت بمراتب بیشتری نسبت به هر یک از سگمنت های شبکه است . مثلا- "ممکن است نرخ انتقال اطلاعات ستون فقرات شبکه ۱۰۰ مگابیت در ثانیه بوده در صورتیکه نرخ انتقال اطلاعات هر سگمنت ۱۰ مگابیت در ثانیه باشد. توپولوژی . روشی که هر یک از گره ها به یکدیگر متصل می گردند را گویند. کارت شبکه . هر کامپیوتر از طریق یک کارت شبکه به شبکه متصل می گردد.در اکثر کامپیوترهای شخصی ، کارت فوق از نوع اترنت بوده (دارای سرعت ۱۰ و یا ۱۰۰ مگابیت در ثانیه) و در یکی از اسلات های موجود روی برد اصلی سیستم ، نصب خواهد شد. آدرس MAC . آدرس فیزیکی هر دستگاه (کارت شبکه) در شبکه است. آدرس فوق یک عدد شش بایتی بوده که سه بایت اول آن مشخص کننده سازنده کارت شبکه و سه بایت دوم ، شماره سریال کارت شبکه است . Unicast. ارسال اطلاعات توسط یک گره با آدرس خاص و دریافت اطلاعات توسط گره دیگر است . Multicast . یک گره ، اطلاعاتی را برای یک گروه خاص (با آدرس مشخص) ارسال می دارد.دستگاههای موجود در گروه ، اطلاعات ارسالی را دریافت خواهند کرد. Bradcast . یک گره اطلاعاتی را برای تمام گره های موجود در شبکه ارسال می نماید. استفاده از سوئیچ در اکثر شبکه های متداول ، بمنظور اتصال گره ها از هاب استفاده می شود. همزمان با رشد شبکه (تعداد کاربران ، تنوع نیازها ، کاربردهای جدید شبکه و ...) مشکلاتی در شبکه های فوق بوجود می آید : - Scalability . در یک شبکه مبتنی بر هاب ، پهنای باند بصورت مشترک توسط کاربران استفاده می گردد. با توجه به محدود بودن پهنای باند ، همزمان با توسعه، کارآئی شبکه بشدت تحت تاثیر قرار خواهد گرفت . برنامه های کامپیوتر که امروزه بمنظور اجراء بر روی محیط شبکه ، طراحی می گردند به پهنای باند مناسبی نیاز خواهند داشت . عدم تامین پهنای باند مورد نیازبرنامه ها ، تاثیر منفی در عملکرد آنها را بدنبال خواهد داشت . -Latency . به مدت زمانی که طول خواهد کشید تا بسته اطلاعاتی به مقصد مورد نظر خود برسد ، اطلاق می گردد. با توجه به اینکه هر گره در شبکه های مبتنی بر هاب می بایست مدت زمانی را در انتظار سپری کرده (ممانعت از

تصادم اطلاعات) ، بموازات افزایش تعداد گره ها در شبکه ، مدت زمان فوق افزایش خواهد یافت . در این نوع شبکه ها در صورتیکه یکی از کاربران فایل با ظرفیت بالائی را برای کاربر دیگر ارسال نماید ، تمام کاربران دیگر می بایست در انتظاز آزاد شدن محیط انتقال بمنظور ارسال اطلاعات باشند. بهرحال افزایش مدت زمانی که یک بسته اطلاعاتی به مقصد خود برسد ، هرگز مورد نظر کاربران یک شبکه نخواهد بود. - Netwrk Failure . در شبکه های مبتنی بر هاب ، یکی از دستگاههای متصل شده به هاب قادر به ایجاد مسائل و مشکلاتی برای سایر دستگاههای موجود در شبکه خواهد بود. عامل بروز اشکال می تواند عدم تنظیم مناسب سرعت (مثلا "تنظیم سرعت یک هاب با قابلیت ۱۰ مگابیت در ثانیه به ۱۰۰ مگابیت در ثانیه) و یا ارسال بیش از حد بسته های اطلاعاتی از نوع Bradcast ، باشد. - Cllisins . در شبکه های مبتنی بر تکنولوژی اترنت از فرآینده خاصی با نام CSMA/CD بمنظور ارتباط در شبکه استفاده می گردد. فرآیند فوق نحوه استفاده از محیط انتقال بمنظور ارسال اطلاعات را قانونمند می نماید. در چنین شبکه هائی تا زمانیکه بر روی محیط انتقال ترافیک اطلاعاتی باشد ، گره ای دیگر قادر به ارسال اطلاعات نخواهد بود. در صورتیکه دو گره در یک لحظه اقدام به ارسال اطلاعات نمایند ، یک تصادم اطلاعاتی ایجاد و عملا" بسته های اطلاعاتی ارسالی توسط هر یک از گره ها نیز از بین خواهند رفت . هر یک از گره های مربوطه (تصادم کننده) می بایست بمدت زمان کاملا "تصادفی در انتظار باقی مانده و پس از فراهم شدن شرایط ارسال ، اقدام به ارسال اطلاعات مورد نظر خود نمایند. هاب مسیر ارسال اطلاعات از یک گره به گره دیگر را به حداقل مقدار خود می رساند ولی عملا "شبکه را به سگمنت های گسسته تقسیم نمی نماید. سوئیچ بمنظور تحقق خواسته فوق عرضه شده است . یکی از مهمترین تفاوت های موجود بین هاب و سوئیچ ، تفسیر هر یک از پهنای باند است . تمام دستگاههای متصل شده به هاب ، پهنای باند موجود را بین خود به اشتراک می گذارند.در صورتیکه یک دستگاه متصل شده به سوئیچ ، دارای تمام پهنای باند مختص خود است. مثلا "در صورتیکه ده گره به هاب متصل شده باشند ، (در یک شبکه ده مگابیت درثانیه) هر گره موجود در شبکه بخشی از تمام پهنای باند موجود (ده مگابیت در ثانیه) را اشغال خواهد کرد. (در صورتیکه سایر گره ها نیز قصد ارتباط را داشته باشند) . در سوئیچ ، هر یک از گره ها قادر به برقراری ارتباط با سایر گره ها با سرعت ده مگابیت در ثانیه خواهد بود. در یک شبکه مبتنی بر سوئیچ ، برای هر گره یک سگمنت اختصاصی ایجاد خواهد شد. سگمنت های فوق به یک سوئیچ متصل خواهند شد. در حقیقت سوئیچ امکان حمایت از چندین (در برخی حالات صدها) سگمنت اختصاصی را دارا است . با توجه به اینکه تنها دستگاه های موجود در هر سگمنت سوئیچ و گره می باشند ، سوئیچ قادر به انتخاب اطلاعات ، قبل از رسیدن به سایر گره ها خواهد بود. در ادامه سوئیچ، فریم های اطلاعاتی را به سگمنت مورد نظر هدایت خواهد کرد. با توجه به اینکه هر سگمنت دارای صرفا "یک گره می باشد ، اطلاعات مورد نظر به مقصد مورد نظر ارسال خواهند شد. بدین ترتیب در شبکه های مبتنی بر سوئیچ امکان چندین مبادله اطلاعاتی بصورت همزمان وجود خواهد داشت . با استفاده از سوئیچ ، شبکه های اترنت بصورت full-duplex خواهند بود. قبل از مطرح شدن سوئیچ ، اترنت بصورت half-duplex بود. در چنین حالتی داده ها در هر لحظه امکان ارسال در یک جهت را دارا می باشند . در یک شبکه مبتنی بر سوئیچ ، هر گره صرفا "با سوئیچ ارتباط برقرار می نماید (گره ها مستقیما "با یکدیگر ارتباط برقرار نمی نمایند) . در چنین حالتی اطلاعات از گره به سوئیچ و از سوئیچ به گره مقصد بصورت همزمان منتقل می گردند. در شبکه های مبتنی بر سوئیچ امکان استفاده از کابل های بهم تابیده و یا فیبر نوری وجود خواهد داشت . هر یک از کابل های فوق دارای کانکتورهای مربوط به خود برای ارسال و دریافت اطلاعات می باشند. با استفاده از سوئیچ ، شبکه ای عاری از تصادم اطلاعاتی بوجود خواهد آمد. انتقال دو سویه اطلاعات در شبکه های مبتنی بر سوئیچ ، سرعت ارسال و دریافت اطلاعات افزایش می یابد. اکثر شبکه های مبتنی بر سوئیچ بدلیل قیمت بالای سوئیچ ، صرفا "از سوئیچ به تنهائی استفاده نمی نمایند. در این نوع شبکه ها از ترکیب هاب و سوئیچ استفاده می گردد. مثلا- "یک سازمان می تواند از چندین هاب بمنظور اتصال کامپیوترهای موجود در هر

یک از دپارتمانهای خود استفاده و در ادامه با استفاده از یک سوئیچ تمام هاب ها(مربوط به هر یک از دپارتمانها) بیکدیگر متصل می گردد. تکنولوژی سوئیچ ها سوئیچ ها دارای پتانسیل های لازم بمنظور تغییر روش ارتباط هر یک از گره ها با یکدیگر می باشند. تفاوت سوئیچ با روتر چیست ؟ سوئیچ ها معمولا "در لایه دوم (Data layer) مدل SI فعالیت می نمایند.در لایه فوق امکان استفاده از آدرس های MAC (آدرس ها ی فیزیکی) وجود دارد. روتر در لایه سوم (Netwrk) مدل SI فعالیت می نمایند. در لایه فوق از آدرس های IP ر IPX و یا Appeltalk استفاده می شود. (آدرس ها ی منطقی) . الگوریتم استفاده شده توسط سوئیچ بمنظور اتخاذ تصمیم در رابطه با مقصد یک بسته اطلاعاتی با الگوریتم استفاده شده توسط روتر ، متفاوت است . یکی از موارد اختلاف الگوریتم های سوئیچ و هاب ، نحوه برخورد آنان با Bradcast است . مفهوم بسته های اطلاعاتی از نوع Bradcast در تمام شبکه ها مشابه می باشد. در چنین مواردی ، دستگاهی نیاز به ارسال اطلاعات داشته ولی نمی داند که اطلاعات را برای چه کسی می بایست ارسال نماید. بدلیل عدم آگاهی و دانش نسبت به هویت دریافت کننده اطلاعات ، دستگاه مورد نظر اقدام به ارسال اطلاعات بصورت bradcast می نماید. مثلا "هر زمان که کامپیوتر جدید ویا یکدستگاه به شبکه وارد می شود ، یک بسته اطلاعاتی از نوع Bradcast برای معرفی و حضور خود در شبکه ارسال می دارد. سایر گره ها قادر به افزودن کامپیوتر مورد نظر در لیست خود و برقراری ارتباط با آن خواهند بود. بنابراین بسته های اطلاعاتی از نوع Bradcast در مواردیکه یک دستگاه نیاز به معرفی خود به سایر بخش های شبکه را داشته و یا نسبت به هویت دریافت کننده اطلاعات شناخت لازم وجود نداشته باشند ، استفاده می گردند. هاب و یا سوئیچ ها قادر به ارسال بسته ای اطلاعاتی از نوع Bradcast برای سایر سگمنت های موجود در حوزه Bradcast می باشند. روتر عملیات فوق را انجام نمی دهد. در صورتیکه آدرس یکدستگاه مشخص نگردد ، روتر قادر به مسیریابی بسته اطلاعاتی مورد نظر نخواهد بود. ویژگی فوق در مواردیکه قصد جداسازی شبکه ها از یکدیگر مد نظر باشد ، بسیار ایده آل خواهد بود. ولی زمانیکه هدف مبادله اطلاعاتی بین بخش های متفاوت یک شبکه باشد ، مطلوب بنظر نمی آید. سوئیچ ها با هدف برخورد با مشکل فوق عرضه شده اند. سوئیچ های LAN بر اساس تکنولوژی packet-switching فعالیت می نمایند. سوئیچ یک ارتباط بین دو سگمنت ایجاد می نماید. بسته های اطلاعاتی اولیه در یک محل موقت (بافر) ذخیره می گردند ، آدرس فیزیکی (MAC) موجود در هدر خوانده شده و در ادامه با لیستی از آدرس های موجود در جدول Lkup (جستجو) مقایسه می گردد. در شبکه های LAN مبتنی بر اترنت ، هر فریم اترنت شامل یک بسته اطلاعاتی خاص است . بسته اطلاعاتی فوق شامل یک عنوان (هدر) خاص و شامل اطلاعات مربوط به آدرس فرستنده و گیرنده بسته اطلاعاتی است . سوئیچ های مبتنی بر بسته های اطلاعاتی بمنظور مسیریابی ترافیک موجود در شبکه از سه روش زیر استفاده می نمایند. Cut-Thrugh Stre-and-frward Fragment-free سوئیچ های Cut-thrugh ، بلافاصله پس از تشخیص بسته اطلاعاتی توسط سوئیچ ، آدرس MAC خوانده می شود. پس از ذخیره سازی شش بایت اطلاعات که شامل آدرس می باشند ، بلافاصله عملیات ارسال بسته های اطلاعاتی به گره مقصد آغاز می گردد. (همزمان با دریافت سایر بسته های اطلاعاتی توسط سوئیچ) . با توجه به عدم وجود کنترل های لازم در صورت بروز خطاء در روش فوق ، سوئیچ های زیادی از روش فوق استفاده نمی نمایند. سوئیچ های stre-and-frward ، تمام بسته اطلاعاتی را در بافر مربوطه ذخیره و عملیات مربوط به بررسی خطاء (CRC) و سایر مسائل مربوطه را قبل از ارسال اطلاعات انجام خواهند داد. در صورتیکه بسته اطلاعاتی دارای خطاء باشد ، بسته اطلاعاتی دور انداخته خواهد شد. .در غیراینصورت ، سوئیچ با استفاده از آدرس MAC ، بسته اطلاعاتی را برای گره مقصد ارسال می نماید. اغلب سوئیچ ها از ترکیب دو روش گفته شده استفاده می نمایند. در این نوع سوئیچ ها از روش cut-thrugh استفاده شده و بمحض بروز خطاء از روش stre-and-frward استفاده می نمایند. یکی دیگر از روش های مسیریابی ترافیک در سوئیچ ها که کمتر استفاده می گردد ، fragment-free است . روش فوق مشابه cut-thrugh بوده با این تفاوت که قبل از ارسال

بسته اطلاعاتی ۶۴ بایت آن ذخیره می گردد. سوئیچ های LAN دارای مدل های متفاوت از نقطه نظر طراحی فیزیکی می باشند. سه مدل رایج در حال حاضر بشرح زیر می باشند: - Shared memry . این نوع از سوئیچ ها تمام بسته های اطلاعاتی اولیه در بافر مربوط به خود را ذخیره می نمایند. بافر فوق بصورت مشترک توسط تمام پورت های سوئیچ (اتصالات ورودی و خروجی) استفاده می گردد. در ادامه اطلاعات مورد نظر بکمک پورت مربوطه برای گره مقصد ارسال خواهند شد. -Matrix . این نوع از سوئیچ ها دارای یک شبکه(تور) داخلی ماتریس مانند بوده که پورت های ورودی و خروجی همدیگر را قطع می نمایند. زمانیکه یک بسته اطلاعاتی بر روی پورت ورودی تشخیص داده شد ، آدرس MAC آن با جدول lkup مقایسه تا پورت مورد نظر خروجی آن مشخص گردد. در ادامه سوئیچ یک ارتباط را از طریق شبکه و در محلی که پورت ها همدیگر را قطع می کنند ، برقرار می گردد. - Bus Architecture . در این نوع از سوئیچ ها بجای استفاده از یک شبکه (تور) ، از یک مسیر انتقال داخلی (Bus) استفاده و مسیر فوق با استفاده از TDMA توسط تمام پورت ها به اشتراک گذاشته می شود. سوئیچ های فوق برای هر یک از پورت ها دارای یک حافظه اختصاصی می باشند. Transparent Bridging اکثر سوئیچ های LAN مبتنی بر اترنت از سیستم ی با نام transparent bridging برای ایجاد جداول آدرس lkup استفاده می نمایند. تکنولوژی فوق امکان یادگیری هر چیزی در رابطه با محل گره های موجود در شبکه ، بدون حمایت مدیریت شبکه را فراهم می نماید. تکنولوژی فوق داری پنج بخش متفاوت است : Learning Flding Filtering Frwarding Aging نحوه عملکرد تکنولوژی فوق بشرح زیر است : - سوئیچ به شبکه اضافه شده و تمام سگمنت ها به پورت های سوئیچ متصل خواهند شد. - گره A بر روی اولین سگمنت (سگمنت A) ، اطلاعاتی را برای کامپیوتر دیگر (گره B) در سگمنت دیگر (سگمنت C) ارسال می دارد. - سوئیچ اولین بسته اطلاعاتی را از گره A دریافت می نماید. آدرس MAC آن خوانده شده و آن را در جدول Lkup سگمنت A ذخیره می نماید. بدین ترتیب سوئیچ از نحوه یافتن گره A آگاهی پیدا کرده و اگر در آینده گره ای قصد ارسال اطلاعات برای گره A را داشته باشد ، سوئیچ در رابطه با آدرس آن مشکلی نخواهد داشت . فرآیند فوق را Learning می گویند. - با توجه به اینکه سوئیچ دانشی نسبت به محل گره B ندارد ، یک بسته اطلاعاتی را برای تمام سگمنت های موجود در شبکه (بجز سگمنت A که اخیرا "یکی از گره های موجود در آن اقدام به ارسال اطلاعات نموده است .) فرآیند ارسال یک بسته اطلاعاتی توسط سوئیچ ، بمنظور یافتن یک گره خاص برای تمام سگمنت ها ، Flding نامیده می شود. - گره B بسته اطلاعاتی را دریافت و یک بسته اطلاعاتی را بعنوان Acknwledgement برای گره A ارسال خواهد کرد. - بسته اطلاعاتی ارسالی توسط گره B به سوئیچ می رسد. در این زمان ، سوئیچ قادر به ذخیره کردن آدرس MAC گره B در جدول Lkup سگمنت C می باشد. با توجه به اینکه سوئیچ از آدرس گره A آگاهی دارد ، بسته اطلاعاتی را مستقیما "برای آن ارسال خواهد کرد. گره A در سگمنتی متفاوت نسبت به گره B قرار دارد ، بنابراین سوئیچ می بایست بمنظور ارسال بسته اطلاعاتی دو سگمنت را به یکدیگر متصل نمائید. فرآیند فوق Frwarding نامیده می شود. - در ادامه بسته اطلاعاتی بعدی از گره A بمنظور ارسال برای گره B به سوئیچ می رسد ، با توجه به اینکه سوئیچ از آدرس گره B آگاهی دارد ، بسته اطلاعاتی فوق مستقیما "برای گره B ارسال خواهد شد. - گره C اطلاعاتی را از طریق سوئیچ برای گره A ارسال می دارد. سوئیچ آدرس MAC گره C را در جدول Lkup سگمنت A ذخیره می نماید ، سوئیچ آدرس گره A را دانسته و مشخص می گردد که دو گره A و C در یک سگمنت قرار دارند. بنابراین نیازی به ارتباط سگمنت A با سگمنت دیگر بمنظور ارسال اطلاعات گره C نخواهد بود. بدین ترتیب سوئیچ از حرکت بسته های اطلاعاتی بین گره های موجود در یک سگمنت ممانعت می نماید. فرآیند فوق را Filtering می گویند. - Learning و Flding ادامه یافته و بموازات آن سوئیچ ، آدرس های MAC مربوط به گره ها را در جداول Lkup ذخیره می نماید. اکثر سوئیچ ها دارای حافظه کافی بمنظور ذخیره سازی جداول Lkup می باشند. بمنظور بهینه سازی حافظه فوق ، اطلاعات قدیمی تر از جداول فوق حذف تا فرآیند

جستجو و یافتن آدرس ها در یک زمان معقول و سریعتر انجام پذیرد. بدین منظور سوئیچ ها از روشی با نام aging استفاده می نمایند. زمانیکه یک Entry برای یک گره در جدول Lkup اضافه می گردد ، به آن یک زمان خاص نسبت داده می شود. هر زمان که بسته ای اطلاعاتی از طریق یک گره دریافت می گردد ، زمان مورد نظر بهنگام می گردد. سوئیچ دارای یک یک تایمر قابل پیکربندی بوده که با عث می شود، Entry های موجود در جدول Lkup که مدت زمان خاصی از آنها استفاده نشده و یا به آنها مراجعه ای نشده است ، حذف گردند . با حذف Entry های غیرضروری ، حافظه قابل استفاده برای سایر Entry ها بیشتر می گردد. در مثال فوق ، دو گره سگمنت A را به اشتراک گذاشته و سگمنت های A و D بصورت مستقل می باشند. در شبکه های ایده آل مبتنی بر سوئیچ ، هر گره دارای سگمنت اختصاصی مربوط بخود است . بدین ترتیب امکان تصادم حذف و نیازی به عملیات Filtering نخواهد بود. فراوانی و آشفتگی انتشار در شبکه های با توپولوژی ستاره (Star) و یا ترکیب Bus و وStar یکی از عناصر اصلی شبکه که می تواند باعث از کار افتادن شبکه گردد ، هاب و یا سوئیچ است . Spanning tress بمنظوری پیشگیری از مسئله " آشفتگی انتشار "و سایر اثرات جانبی در رابطه با Lping شرکت DEC پروتکلی با نام STP(Spanning-tree Prtcl) را ایجاد نموده است . پروتکل فوق با مشخصه ۸۰۲.۱d توسط موسسه IEEE استاندارد شده است . Spanning tree از الگوریتم STA(Spanning-tree algritm) استفاده می نماید. الگوریتم فوق بررسی خواهد کرد آیا یک سوئیچ دارای بیش از یک مسیر برای دستیابی به یک گره خاص است . در صورت وجود مسیرهای متعدد ، بهترین مسیر نسبت به سایر مسیرها کدام است ؟ نحوه عملیات STP بشرح زیر است : - به هر سوئیچ ، مجموعه ای از مشخصه ها (ID) نسبت داده می شود. یکی از مشخصه ها برای سوئیچ و سایر مشخصه ها برای هر یک از پورت ها استفاده می گردد. مشخصه سوئیچ ، BID(Bridge ID) نامیده شده و دارای هشت بایت است . دو بایت بمنظور مشخص نمودن اولویت و شش بایت برای مشخص کردن آدرس MAC استفاده می گردد. مشخصه پورت ها ، شانزده بیتی است . شش بیت بمنظور تنظیمات مربوط به اولویت و ده بیت دیگر برای اختصاص یک شماره برا ی پورت مورد نظر است . - برای هر مسیر یک Path Cst محاسبه می گردد. نحوه محاسبه پارامتر فوق بر اساس استانداردهای ارائه شده توسط موسسه IEEE است . بمنظور محاسبه مقادر فوق ، ۱.۰۰۰ مگابیت در ثانیه (یک گیگابیت در ثانیه) را بر پهنای باند سگمنت متصل شده به پورت ، تقسیم می نمایند. بنابراین یک اتصال ۱۰ مگابیت در ثانیه ، دارای Cst به میزان ۱۰۰ است (۱.۰۰۰ تفسیم بر ۱۰) . بمنظور هماهنگ شدن با افزایش سرعت شبکه های کامپیوتری استاندارد Cst نیز اصلاح می گردد. جدول زیر مقادیر جدید STP Cst را نشان می دهد. (مقدار Path cst می تواند یک مقدار دلخواه بوده که توسط مدیریت شبکه تعریف و مشخص می گردد) - هر سوئیچ فرآیندی را بمنظور انتخاب مسیرهای شبکه که می بایست توسط هر یک از سگمنت ها استفاده گردد ، آغاز می نمایند. اطلاعات فوق توسط سایر سوئیچ ها و با استفاده از یک پروتکل خاص با نام Bridge prtcl data units(BPUD) به اشتراک گذاشته می شود. ساختار یک BPUDبشرح زیر است : Rt BID . پارامتر فوق BID مربوط به Rt Bridge جاری را مشخص می کند. Path Cst t Bridge . مسافت rt bridge را مشخص می نماید. مثلا "در صورتیکه داده از طریق طی نمودن سه سگمنت با سرعتی معادل ۱۰۰ مگابیت در ثانیه برای رسیدن به Rt bridge باشد ، مقدار cst بصورت (۱۹+۱۹+۰=۳۸) بدست می آید. سگمنتی که به Rt Bridge متصل است دارای Cst معادل صفر است . Sender BID. مشخصه BID سوئیچ ارسال کننده BPDU را مشخص می کند. Prt ID . پورت ارسال کننده BPDU مربوط به سوئیچ را مشخص می نماید. تمام سوئیچ ها بمنظور مشخص نمودن بهترین مسیر بین سگمنت های متفاوت ، بصورت پیوسته برای یکدیگر BPDUارسال می نمایند. زمانیکه سوئیچی یک BPDU را (از سوئیچ دیگر) دریافت می دارد که مناسبتر از آن چیزی است که خود برای ارسال اطلاعات در همان سگمنت استفاده کرده است ، BPDU خود را متوقف (به سایر سگمنت ها اراسال نمی نماید) و از BPDU سایر سوئیچ ها بمنظور دستیابی به سگمنت ها استفاده خواهد کرد. - یک Rt bridge بر اساس

فرآیندهای BPDU بین سوئیچ ها ، انتخاب می گردد. در ابتدا هر سوئیچ خود را بعنوان Rt در نظر می گیرد. زمانیکه یک سوئیچ برای اولین بار به شبکه متصل می گردد ، یک BPDU را بهمراه BID خود که بعنوان Rt BID است ، ارسال می نماید. زمانیکه سایر سوئیچ ها BPDU را دریافت می دارند ، آن را با BID مربوطه ای که بعنوان Rt BID ذخیره نموده اند، مقایسه می نمایند. در صورتیکه Rt BID جدید دارای یک مقدار کمتر باشد ، تمام سوئیچ ها آن را با آنچیزی که قبلا "ذخیره کرده اند، جایگزین می نمایند. در صورتیکه Rt BID ذخیره شده دارای مقدار کمتری باشد ، یک BPDU برای سوئیچ جدید بهمراه BID مربوط به Rt BID ارسال می گردد. زمانیکه سوئیچ جدید BPDU را دریافت می دارد ، از Rt بودن خود صرفنظر و مقدار ارسالی را بعنوان Rt BID در جدول مربوط به خود ذخیره خواهد کرد. – با توجه به محل Rt Bridge ، سایر سوئیچ ها مشخص خواهند کرد که کدامیک از پورت های آنها دارای کوتاهترین مسیر به Rt Bridge است . پورت های فوق، Rt Prts نامیده شده و هر سوئیچ می بایست دارای یک نمونه باشد. – سوئیچ ها مشخص خواهند کرد که چه کسی دارای پورت های designated است . پورت فوق ، اتصالی است که توسط آن بسته های اطلاعاتی برای یک سگمنت خاص ارسال و یا از آن دریافت خواهند شد. با داشتن صرفا "یک نمونه از پورت های فوق ، تمام مشکلات مربوط به Lping برطرف خواهد شد. – پورت های designated بر اساس کوتاهترین مسیر بین یک سگمنت تا rt bridge انتخاب می گردند. با توجه به اینکه Rt bridge دارای مقدار صفر برای path cst است ، هر پورت آن بمنزله یک پورت designated است . (مشروط به اتصال پورت مورد نظر به سسگمنت) برای سایر سوئیچ ها، Path Cst برای یک سگمنت بررسی می گردد. در صورتیکه پورتی دارای پایین ترین path cst باشد ، پورت فوق بمنزله پورت designated سگمنت مورد نظر خواهد بود. در صورتیکه دو و یا بیش از دو پورت دارای مقادیر یکسان path cst باشند ، سوئیچ با مقادر کمتر BID اتخاب می گردد. – پس از انتخاب پورت designatedبرای سگمنت شبکه ، سایر پورت های متصل شده به سگمنت مورد نظر بعنوان nn -designated prt در نظر گرفته خواهند شد. بنابراین با استفاده از پورت های designated می توان به یک سگمنت متصل گردید. هر سوئیچ دارای جدول BPDU مربوط به خود بوده که بصورت خودکار بهنگام خواهد شد. بدین ترتیب شبکه بصورت یک spanning tree بوده که بمنزله rr bridge ریشه و سایر سوئیچ ها بمنزله برگ خواهند بود. هر سوئیچ با استفاده از Rt Prts قادر به ارتباط با rt bridge بوده و با استفاده از پورت های designated قادر به ارتباط با هر سگمنت خواهد بود. روترها و سوئیچینگ لایه سوم همانگونه که قبلا "اشاره گردید ، اکثر سوئیچ ها در لایه دوم مدل SI فعالیت می نمایند (Data Layer) . اخیرا "برخی از تولیدکنندگان سوییچ، مدلی را عرضه نموده اند که قادر به فعالیت در لایه سوم مدل SI است . (Netwrk Layer) . این نوع سوئیچ ها دارای شباهت زیادی با روتر می باشند. زمانیکه روتر یک بسته اطلاعاتی را دریافت می نماید ، در لایه سوم بدنبال آدرس های مبداء و مقصد گشته تا مسیر مربوط به بسته اطلاعاتی را مشخص نماید. سوئیچ های استاندارد از آدرس های MAC بمنظور مشخص کردن آدرس مبداء و مقصد استفاده می نمایند.(از طریق لایه دوم) مهمترین تفاوت بین یک روتر و یک سوئیچ لایه سوم ، استفاده سوئیچ های لایه سوم از سخت افزارهای بهینه بمنظور ارسال داده با سرعت مطلوب نظیر سوئیچ های لایه دوم است. نحوه تصمیم گیری آنها در رابطه با مسیریابی بسته های اطلاعاتی مشابه روتر است . در یک محیط شبکه ای LAN ، سوئیچ های لایه سوم معمولا "دارای سرعتی بیشتر از روتر می باشند. علت این امر استفاده از سخت افزارهای سوئیچینگ در این نوع سوئیچ ها است . اغلب سوئیچ های لایه سوم شرکت سیسکو، بمنزله روترهائی می باشند که بمراتب از روتر ها سریعتر بوده (با توجه به استفاده از سخت افزارهای اختصاصی سوئیچینگ) و دارای قیمت ارزانتری نسبت به روتر می باشند. نحوه Pattern matching و caching در سوئیچ های لایه سوم مشابه یک روتر است . در هر دو دستگاه از یک پروتکل روتینگ و جدول روتینگ، بمنظور مشخص نمودن بهترین مسیر استفاده می گردد. سوئیچ های لایه سوم قادر به برنامه ریزی مجدد سخت افزار بصورت پویا و با استفاده از اطلاعات روتینگ لایه

سوم می باشند و همین امر باعث سرعت بالای پردازش بسته های اطلاعاتی می گردد. سوئیچ های لایه سوم ، از اطلاعات دریافت شده توسط پروتکل روتینگ بمنظور بهنگام سازی جداول مربوط به Caching استفاده می نمایند. همانگونه که ملاحظه گردید ، در طراحی سوئیچ های LAN از تکنولوژی های متفاوتی استفاده می گردد. نوع سوئیچ استفاده شده ، تاثیر مستقیم بر سرعت و کیفیت یک شبکه را بدنبال خواهد داشت .

محاسبات شبکهای چیست؟

در محاسبات شبکهای چندین پردازشگر به طور همزمان و جداگانه محاسبه خاصی را انجام میدهند. به گزارش بخش خبر شبکه فن آوری اطلاعات ایران، به نقل از ایلنا، امروزه در بسیاری از محافل اطلاعاتی و مراکز IT صحبت از محاسبات شبکهای یا GRID CMPUTING است ؛ اما این اصطلاح هنوز برای بسیاری از کاربران ناشناخته باقی مانده است. محاسبات شبکهای در سادهترین حالت ممکن, به معنی فعالیت مشترک پردازندههای چندگانه بر روی ماشینهای چندگانه است و هدف آن افزایش توان محاسباتی در زمینههایی است که توان بسیار بالای CPU را میطلبد. در محاسبات شبکهای سرورهای چندگانهای با هم ارتباط دارند که از سیستمعاملها و نرمافزارهای مشابهی استفاده میکنند. به کمک محاسبات شبکهای, میتوان کارهای محاسباتی را به طور همزمان به کمک چندین پردازشگر انجام داد. در مواردی که نتیجه محاسبات خیلی حساس است و دقت آن سرنوشتساز است, دهها و گاهی هزاران پردازشگر به طور همزمان یک محاسبه را انجام میدهند. بعد از انجام محاسبات نتایج کار همه پردازشگرها با هم مقایسه میشود تا میزان دقت محاسبات تعیین شود.

شبکه اترنت چیست؟

شبکه اترنت (Ethernet) چیست؟ دستیابی به اطلاعات با روش های مطمئن و با سرعت بالا یکی از رموز موفقیت هر سازمان و موسسه است . طی سالیان اخیر هزاران پرونده و کاغذ که حاوی اطلاعات با ارزش برای یک سازمان بوده ، در کامپیوتر ذخیره شده اند. با تغذیه دریائی از اطلاعات به کامپیوتر ، امکان مدیریت الکترونیکی اطلاعات فراهم شده است . کاربران متفاوت در اقصی نقاط جهان قادر به اشتراک اطلاعات بوده و تصویری زیبا از همیاری و همکاری اطلاعاتی را به نمایش می گذارند. شبکه های کامپیوتری در این راستا و جهت نیل به اهداف فوق نقش بسیار مهمی را ایفاء می نمایند.اینترنت که عالی ترین تبلور یک شبکه کامپیوتری در سطح جهان است، امروزه در مقیاس بسیار گسترده ای استفاده شده و ارائه دهندگان اطلاعات ، اطلاعات و یا فرآورده های اطلاعاتی خود را در قالب محصولات تولیدی و یا خدمات در اختیار استفاده کنندگان قرار می دهند. وب که عالی ترین سرویس خدماتی اینترنت می باشد کاربران را قادر می سازد که در اقصی نقاط دنیا اقدام به خرید، آموزش ، مطالعه و ... نمایند. با استفاده از شبکه، یک کامپیوتر قادر به ارسال و دریافت اطلاعات از کامپیوتر دیگر است . اینترنت نمونه ای عینی از یک شبکه کامپیوتری است . در این شبکه میلیون ها کامپیوتر در اقصی نقاط جهان به یکدیگر متصل شده اند.اینترنت شبکه ای است مشتمل بر زنجیره ای از شبکه های کوچکتراست . نقش شبکه های کوچک برای ایجاد تصویری با نام اینترنت بسیار حائز اهمیت است . تصویری که هر کاربر با نگاه کردن به آن گمشده خود را در آن پیدا خواهد کرد. در این بخش به بررسی شبکه های کامپیوتری و جایگاه مهم آنان در زمینه تکنولوژی اطلاعات و مدیریت الکترونیکی اطلاعات خواهیم داشت . شبکه های محلی و شبکه های گسترده تاکنون شبکه های کامپیوتری بر اساس مولفه های متفاوتی تقسیم بندی شده اند. یکی از این مولفه ها " حوزه جغرافیائی " یک شبکه است . بر همین اساس شبکه ها به دو گروه عمده LAN(Lcal area netwrk) و WAN(Wide area netwrk) تقسیم می گردند. در شبکه های LAN مجموعه ای از دستگاه های موجود در یک حوزه جغرافیائی محدود،

نظیر یک ساختمان به یکدیگر متصل می گردند . در شبکه های WAN تعدادی دستگاه که از یکدیگر کیلومترها فاصله دارند به یکدیگر متصل خواهند شد. مثلا "اگر دو کتابخانه که هر یک در یک ناحیه از شهر بزرگی مستقر می باشند، قصد اشتراک اطلاعات را داشته باشند، می بایست شبکه ای WAN ایجاد و کتابخانه ها را به یکدیگر متصل نمود. برای اتصال دو کتابخانه فوق می توان از امکانات مخابراتی متفاوتی نظیر خطوط اختصاصی (Leased) استفاده نمود. شبکه های LAN نسبت به شبکه های WAN دارای سرعت بیشتری می باشند. با رشد و توسعه دستگاههای متفاوت مخابراتی میزان سرعت شبکه های WAN ، تغییر و بهبود پیدا کرده است . امروزه با بکارگیری و استفاده از فیبر نوری در شبکه های LAN امکان ارتباط دستگاههای متعدد که در مسافت های طولانی نسبت بیکدیگر قرار دارند، فراهم شده است . اترنت در سال ۱۹۷۳ پژوهشگری با نام " Metcalfe "در مرکز تحقیقات شرکت زیراکس، اولین شبکه اترنت را بوجود آورد. هدف وی ارتباط کامپیوتر به یک چاپگر بود. وی روشی فیزیکی بمنظور کابل کشی بین دستگاههای متصل بهم در اترنت ارائه نمود. اترنت در مدت زمان کوتاهی بعنوان یکی از تکنولوژی های رایج برای برپاسازی شبکه در سطح دنیا مطرح گردید. همزمان با پیشرفت های مهم در زمینه شبکه های کامپیوتری ، تجهیزات و دستگاه های مربوطه، شبکه های اترنت نیز همگام با تحولات فوق شده و قابلیت های متفاوتی را در بطن خود ایجاد نمود. با توجه به تغییرات و اصلاحات انجام شده در شبکه های اترنت ،عملکرد و نحوه کار آنان نسبت به شبکه های اولیه تفاوت چندانی نکرده است . در اترنت اولیه، ارتباط تمام دستگاه های موجود در شبکه از طریق یک کابل انجام می گرفت که توسط تمام دستگاهها به اشتراک گذاشته می گردید. پس از اتصال یک دستگاه به کابل مشترک ، می بایست پتانسیل های لازم بمنظور ایجاد ارتباط با سایر دستگاههای مربوطه نیز در بطن دستگاه وجود داشته باشد (کارت شبکه) . بدین ترتیب امکان گسترش شبکه بمنظور استفاده از دستگاههای جدید براحتی انجام و نیازی به اعمال تغییرات بر روی دستگاههای موجود در شبکه نخواهد بود. اترنت یک تکنولوژی محلی (LAN) است. اکثر شبکه های اولیه در حد و اندازه یک ساختمان بوده و دستگاهها نزدیک به هم بودند. دستگاههای موجود بر روی یک شبکه اترنت صرفا "قادر به استفاده از چند صد متر کابل بیشترنبودند.اخیرا "با توجه به توسعه امکانات مخابراتی و محیط انتقال، زمینه استقرار دستگاههای موجود در یک شبکه اترنت با مسافت های چند کیلومترنیز فراهم شده است . پروتکل پروتکل در شبکه های کامپیوتری به مجموعه قوانینی اطلاق می گردد که نحوه ارتباطات را قانونمند می نماید. نقش پروتکل در کامپیوتر نظیر نقش زبان برای انسان است . برای مطالعه یک کتاب نوشته شده به فارسی می بایست خواننده شناخت مناسبی از زبان فارسی را داشته باشد. بمنظور ارتباط موفقیت آمیز دو دستگاه در شبکه می بایست هر دو دستگاه از یک پروتکل مشابه استفاده نمایند. اصطلاحات اترنت شبکه های اترنت از مجموعه قوانین محدودی بمنظور قانونمند کردن عملیات اساسی خود استفاده می نمایند. بمنظور شناخت مناسب قوانین موجود لازم است که با برخی از اصطلاحات مربوطه در این زمینه بیشتر آشنا شویم : Medium (محیط انتقال) . دستگاههای اترنت از طریق یک محیط انتقال به یکدیگر متصل می گردند. Segment (سگمنت) . به یک محیط انتقال به اشتراک گذاشته شده منفرد "، سگمنت " می گویند. Nde (گره) . دستگاههای متصل شده به یک Segment را گره و یا " ایستگاه " می گویند. Frame (فریم) . به یک بلاک اطلاعات که گره ها از طریق ارسال آنها با یکدیگر مرتبط می گردند، اطلاق می گردد فریم ها مشابه جملات در زبانهای طبیعی (فارسی، انگلیسی ...) می باشند. در هر زبان طبیعی برای ایجاد جملات، مجموعه قوانینی وجود دارد مثلا "یک جمله می بایست دارای موضوع و مفهوم باشد. پروتکل های اترنت مجموعه قوانین لازم برای ایجاد فریم ها را مشخص خواهند کرد .اندازه یک فریم محدود بوده (دارای یک حداقل و یک حداکثر) و مجموعه ای از اطلاعات ضروری و مورد نیار می بایست در فریم وجود داشته باشد. مثلا "یک فریم می بایست دارای آدرس های مبداء و مقصد باشد. آدرس های فوق هویت فرستنده و دریافت کننده پیام را مشخص خواهد کرد. آدرس بصورت کاملا "اختصاصی یک گره را مشخص می نماید.(نظیر نام یک شخص که بیانگر یک

شخص خاص است) . دو دستگاه متفاوت اترنت نمی توانند دارای آدرس های یکسانی باشند. یک سیگنال اترنت بر روی محیط انتقال به هر یک از گره های متصل شده در محیط انتقال خواهد رسید. بنابراین مشخص شدن آدرس مقصد، بمنظوردریافت پیام نقشی حیاتی دارد. مثلا "در صورتیکه کامپیوتر B (شکل بالا) اطلاعاتی را برای چاپگر C ارسال می دارد کامپیوترهای A و D نیز فریم را دریافت و آن را بررسی خواهند کرد. هر ایستگاه زمانیکه فریم را دریافت می دارد، آدرس آن را بررسی تا مطمئن گردد که پیام برای وی ارسال شده است یا خیر؟ در صورتیکه پیام برای ایستگاه مورد نظر ارسال نشده باشد، ایستگاه فریم را بدون بررسی محتویات آن کنار خواهد گذاشت (عدم استفاده). یکی از نکات قابل توجه در رابطه با آدرس دهی اترنت، پیاده سازی یک آدرس Bradcast است . زمانیکه آدرس مقصد یک فریم از نوع Bradcast باشد، تمام گره های موجود در شبکه آن را دریافت و پردازش خواهند کرد. CSMA/CD تکنولوژی CSMA/CD)carrier-sense multiple access with cllisin detectin) مسئولیت تشریح و تنظیم نحوه ارتباط گره ها با یکدیگررا برعهده دارد. با اینکه واژه فوق پیچیده بنظر می آید ولی با تقسیم نمودن واژه فوق به بخش های کوچکتر، می توان با نقش هر یک از آنها سریعتر آشنا گردید.بمنظور شناخت تکنولوژی فوق مثال زیر را در نظر بگیرید : فرض کنید سگمنت اترنت، مشابه یک میز ناهارخوری باشد. چندین نفر (نظیر گره) دور تا دور میز نشسته و به گفتگو مشغول می باشند. واژه multiple access (دستیابی چندگانه) بدین مفهوم است که : زمانیکه یک ایستگاه اترنت اطلاعاتی را ارسال می دارد تمام ایستگاههای دیگر موجود (متصل) در محیط انتقال ، نیز از انتقال اطلاعات آگاه خواهند شد.(.نظیر صحبت کردن یک نفر در میز ناهار خوری و گوش دادن سایرین). فرض کنید که شما نیز بر روی یکی از صندلی های میز ناهار خوری نشسته و قصد حرف زدن را داشته باشید، در همان زمان فرد دیگری در حال سخن گفتن است در این حالت می بایست شما در انتظار اتمام سخنان گوینده باشید. در پروتکل اترنت وضعیت فوق carrier sense نامیده می شود.قبل از اینکه ایستگاهی قادر به ارسال اطلاعات باشد می بایست گوش خود را بر روی محیط انتقال گذاشته و بررسی نماید که آیا محیط انتقال آزاد است ؟ در صورتیکه صدائی از محیط انتقال به گوش ایستگاه متقاضی ارسال اطلاعات نرسد، ایستگاه مورد نظر قادر به استفاده از محیط انتقال و ارسال اطلاعات خواهد بود. Carrier-sense multiple access شروع یک گفتگو را قانونمند و تنظیم می نماید ولی در این رابطه یک نکته دیگر وجود دارد که می بایست برای آن نیز راهکاری اتخاذ شود.فرض کنید در مثال میز ناهار خوری در یک لحظه سکوتی حاکم شود و دو نفر نیز قصد حرف زدن را داشته باشند.در چنین حالتی در یک لحظه سکوت موجود توسط دو نفر تشخیص و بلافاصله هر دو تقریبا "در یک زمان یکسان شروع به حرف زدن می نمایند.چه اتفاقی خواهد افتاد ؟ در اترنت پدیده فوق را تصادم (Cllisin) می گویند و زمانی اتفاق خواهد افتاد که دو ایستگاه قصد استفاده از محیط انتقال و ارسال اطلاعات را بصورت همزمان داشته باشند. در گفتگوی انسان ها ، مشکل فوق را می توان بصورت کاملا "دوستانه حل نمود. ما سکوت خواهیم کرد تا این شانس به سایرین برای حرف زدن داده شود.همانگونه که در زمان حرف زدن من، دیگران این فرصت را برای من ایجاد کرده بودند! ایستگاههای اترنت زمانیکه قصد ارسال اطلاعات را داشته باشند، به محیط انتقال گوش فرا داده تا به این اطمینان برسند که تنها ایستگاه موجود برای ارسال اطلاعات می باشند. در صورتیکه ایستگاههای ارسال کننده اطلاعات متوجه نقص در ارسال اطلاعات خود گردند ،از بروز یک تصادم در محیط انتقال آگاه خواهند گردید. در زمان بروز تصادم ، هر یک از ایستگاههای مربوطه به مدت زمانی کاملا "تصادفی در حالت انتظار قرار گرفته و پس از اتمام زمان انتظار می بایست برای ارسال اطلاعات شرط آزاد بودن محیط انتقال را بررسی نمایند! توقف تصادفی و تلاش مجدد یکی از مهمترین بخش های پروتکل است . محدودیت های اترنت یک شبکه اترنت دارای محدودیت های متفاوت از ابعاد گوناگون (بکارگیری تجهیزات) است .طول کابلی که تمام ایستگاهها بصورت اشتراکی از آن بعنوان محیط انتقال استفاده می نمایند یکی از شاخص ترین موارد در این زمنیه است . سیگنال های الکتریکی در طول کابل بسرعت منتشر می گردند. همزمان با

طی مسافتی، سیگنال ها ضعیف می گردند. وجود میدان های الکتریکی که توسط دستگاههای مجاور کابل نظیرلامپ های فلورسنت ایجاد می گردد ، باعث تلف شدن سیگنال می گردد. طول کابل شبکه می بایست کوتاه بوده تا امکان دریافت سیگنال توسط دستگاه های موجود در دو نقطه ابتدائی و انتهائی کابل بصورت شفاف و با حداقل تاخیر زمانی فراهم گردد. همین امر باعث بروز محدودیت در طول کابل استفاده شده، می گردد پروتکل CSMA/CD امکان ارسال اطلاعات برای صرفا "یک دستگاه را در هر لحظه فراهم می نماید، بنابراین محدودیت هائی از لحاظ تعداد دستگاههائی که می توانند بر روی یک شبکه مجزا وجود داشته باشند، نیز بوجود خواهد آمد. با اتصال دستگاه های متعدد (فراوان) بر روی یک سگمنت مشترک، شانس استفاده از محیط انتقال برای هر یک از دستگاه های موجود بر روی سگمنت کاهش پیدا خواهد کرد. در این حالت هر دستگاه بمنظور ارسال اطلاعات می بایست مدت زمان زیادی را در انتظار سپری نماید . تولید کنندگان تجهیزات شبکه دستگاه های متفاوتی را بمنظور غلبه بر مشکلات و محدودیت گفته شده ، طراحی و عرضه نموده اند. اغلب دستگاههای فوق مختص شبکه های اترنت نبوده ولی در سایر تکنولوژی های مرتبط با شبکه نقش مهمی را ایفاء می نمایند. تکرارکننده (Repeater) اولین محیط انتقال استفاده شده در شبکه های اترنت کابل های مسی کواکسیال بود که Thicknet (ضخیم) نامیده می شوند. حداکثر طول یک کابل ضخیم ۵۰۰ متر است . در یک ساختمان بزرگ ، کابل ۵۰۰ متری جوابگوی تمامی دستگاه های شبکه نخواهد بود. تکرار کننده ها با هدف حل مشکل فوق، ارائه شده اند. . تکرارکننده ها ، سگمنت های متفاوت یک شبکه اترنت را به یکدیگر متصل می کنند. در این حالت تکرارکننده سیگنال ورودی خود را از یک سگمنت اخذ و با تقویت سیگنال آن را برای سگمنت بعدی ارسال خواهد کرد. بدین ترتیب با استفاده از چندین تکرار کننده و اتصال کابل های مربوطه توسط آنان ، می توان قطر یک شبکه را افزایش داد. (قطر شبکه به حداکثر مسافت موجود بین دو دستگاه متمایز در شبکه اطلاق می گردد) Bridges و سگمنت شبکه های اترنت همزمان با رشد (بزرگ شدن) دچار مشکل تراکم می گردند. در صورتیکه تعداد زیادی ایستگاه به یک سگمنت متصل گردند، هر یک دارای ترافیک خاص خود خواهند بود . در شرایط فوق ، ایستگاههای متعددی قصد ارسال اطلا عات را دارند ولی با توجه به ماهیت این نوع از شبکه ها در هر لحظه یک ایستگاه شانس و فرصت استفاده از محیط انتقال را پیدا خواهد کرد. در چنین وضعیتی تعداد تصادم در شبکه افزایش یافته و عملا "کارآئی شبکه افت خواهد کرد. یکی از راه حل های موجود بمنظور برطرف نمودن مشکل تراکم در شبکه تقسیم یک سگمنت به چندین سگمنت است . با این کار برای تصادم هائی که در شبکه بروز خواهد کرد، دامنه وسیعتری ایجاد می گردد.راه حل فوق باعث بروز یک مشکل دیگر می گردد: سگمنت ها قادر به اشتراک اطلاعات با یکدیگر نخواهند بود. بمنظور حل مشکل فوق، Bridges در شبکه اترنت پیاده سازی شده است . Bridge دو و یا چندین سگمنت را به یکدیگر متصل خواهد کرد. بدین ترتیب دستگاه فوق باعث افزایش قطر شبکه خواهد شد. عملکرد Bridge از بعد افزایش قطر شبکه نظیر تکرارکننده است ، با این تفاوت که Bridge قادر به ایجاد نظم در ترافیک شبکه نیز خواهد بود . Bridge نظیر سایر دستگاههای موجود در شبکه قادر به ارسال و دریافت اطلاعات بوده ولی عملکرد آنها دقیقا "مشابه یک ایستگاه نمی باشد. Bridge قادر به ایجاد ترافیکی که خود سرچشمه آن خواهد بود، نیست (نظیر تکرارکننده) .Bridge صرفا "چیزی را که از سایر ایستگاهها می شنود ، منعکس می نماید. (Bridge قادر به ایجا د یک نوع فریم خاص اترنت بمنظور ایجاد ارتباط با سایر Bridge ها می باشند) همانگونه که قبلا "اشاره گردید هر ایستگاه موجود در شبکه تمام فریم های ارسال شده بر روی محیط انتقال را دریافت می نماید.(صرفنظر ازاینکه مقصد فریم همان ایستگاه باشد و یا نباشد.) Bridge با تاکید بر ویژگی فوق سعی بر تنظیم ترافیک بین سگمنت ها دارد. همانگونه که در شکل فوق مشاهده می گردد Bridge دو سگمنت را به یکدیگر متصل نموده است . در صورتیکه ایستگاه A و یا B قصد ارسال اطلاعات را داشته باشند Bridge نیز فریم های اطلاعاتی را دریافت خواهد کرد. نحوه برخورد Bridge با فریم های اطلاعاتی دریافت شده به چه صورت است؟ آیا قادر به ارسال اتوماتیک فریم ها

برای سگمنت دوم می باشد؟ یکی ازاهداف استفاده از Bridge کاهش ترافیک های غیرضروری در هر سگمنت است . در این راستا، آدرس مقصد فریم ، قبل از هر گونه عملیات بر روی آن، بررسی خواهد شد. در صورتیکه آدرس مقصد، ایستگاههای A و یا B باشد نیازی به ارسال فریم برای سگمنت شماره دو وجود نخواهد داشت . در این حالت Bridge عملیات خاصی را انجام نخواهد داد. نحوه برخورد Bridge با فریم فوق مشابه فیلتر نمودن است . درصورتیکه آدرس مقصد فریم یکی از ایستگاههای C و یا D باشد و یا فریم مورد نظر دارای یک آدرس از نوع Bradcast باشد ، Bridge فریم فوق را برای سگمنت شماره دو ارسال خواهد کرد. با ارسال و هدایت فریم اطلاعاتی توسط Bridge امکان ارتباط چهار دستگاه موجود در شبکه فراهم می گردد. با توجه به مکانیزم فیلتر نمودن فریم ها توسط Bridge ، این امکان بوجود خواهد آمد که ایستگاه A اطلاعاتی را برای ایستگاه B ارسال و در همان لحظه نیز ایستگاه C اطلاعاتی را برای ایستگاه D ارسال نماید.بدین ترتیب امکان برقراری دو ارتباط بصورت همزمان بوجود آمده است . روترها : سگمنت های منطقی با استفاده از Bridge امکان ارتباط همزمان بین ایستگاههای موجود در چندین سگمنت فراهم می گردد. Bridge در رابطه با ترافیک موجود در یک سگمنت عملیات خاصی را انجام نمی دهد. یکی از ویژگی های مهم Bridge ارسالی فریم های اطلاعاتی از نوع Bradcast برای تمام سگمنت های متصل شده به یکدیگر است. همزمان با رشد شبکه و گسترش سگمنت ها، ویژگی فوق می تواند سبب بروز مسائلی در شبکه گردد. زمانیکه تعداد زیادی از ایستگاه های موجود در شبکه های مبتنی بر Bridge ، فریم های Bradcast را ارسال می نمایند، تراکم اطلاعاتی بوجود آمده بمراتب بیشتر از زمانی خواهد بود که تمامی دستگاهها در یک سگمنت قرار گرفته باشند. روتر یکی از دستگاههای پیشرفته در شبکه بوده که قادر به تقسیم یک شبکه به چندین شبکه منطقی مجزا است . روتر ها یک محدوده منطقی برای هر شبکه ایجاد می نمایند. روترها بر اساس پروتکل هائی که مستقل از تکنولوژی خاص در یک شبکه است، فعالیت می نمایند. ویژگی فوق این امکان را برای روتر فراهم خواهد کرد که چندین شبکه با تکنولوژی های متفاوت را به یکدیگر مرتبط نماید. استفاده از روتر در شبکه های محلی و گسترده امکان پذیراست . وضعیت فعلی اترنت از زمان مطرح شدن شبکه های اترنت تاکنون تغییرات فراوانی از بعد تنوع دستگاه های مربوطه ایجاد شده است . در ابتدا از کابل کواکسیال در این نوع شبکه ها استفاده می گردید.امروزه شبکه های مدرن اترنت از کابل های بهم تابیده و یا فیبر نوری برای اتصال ایستگاه ها به یکدیگر استفاده می نمایند. در شبکه های اولیه اترنت سرعت انتقال اطلاعات ده مگابیت در ثانیه بود ولی امروزه این سرعت به مرز ۱۰۰و حتی ۱۰۰۰ مگابیت در ثانیه رسیده است . مهمترین تحول ایجاد شده در شبکه های اترنت امکان استفاده از سوئیچ های اترنت است .سگمنت ها توسط سوئیچ به یکدیگر متصل می گردند. (نظیر Bridge با این تفاوت عمده که امکان اتصال چندین سگمنت توسط سوئیچ فراهم می گردد) برخی از سوئیچ ها امکان اتصال صدها سگمنت به یکدیگر را فراهم می نمایند. تمام دستگاههای موجود در شبکه، سوئیچ و یا ایستگاه می باشند . قبل از ارسال فریم های اطلاعاتی برا ی هر ایستگاه ، سوئیچ فریم مورد نظر را دریافت و پس از بررسی، آن را برای ایستگاه مقصد مورد نظر ارسال خواهد کرد . عملیات فوق مشابه Bridge است ، ولی در مدل فوق هر سگمنت دارای صرفا "یک ایستگاه است و فریم صرفا "به دریافت کننده واقعی ارسال خواهد شد. بدین ترتیب امکان برقراری ارتباط همزمان بین تعداد زیادی ایستگاه در شبکه های مبتنی بر سوئیچ فراهم خواهد شد. همزمان با مطرح شدن سوئیچ های اترنت مسئله Full-duplex نیز مطرح گردید. Full-dulex یک اصطلاح ارتباطی است که نشاندهنده قابلیت ارسال و دریافت اطلاعات بصورت همزمان است . در شبکه های اترنت اولیه وضعیت ارسال و دریافت اطلاعات بصورت یکطرفه (half-duplex) بود.در شبکه های مبتنی بر سوئیچ، ایستگاهها صرفا "با سوئیچ ارتباط برقرار کرده و قادر به ارتباط مستقیم با یکدیگر نمی باشند. در این نوع شبکه ها از کابل های بهم تابیده و فیبر نوری استفاده و سوئیچ مربوطه دارای کانکتورهای لازم در این خصوص می باشند.. شبکه های مبتنی بر سوئیچ عاری از تصادم بوده و همزمان با ارسال اطلاعات توسط یک ایستگاه به سوئیچ ، امکان ارسال اطلاعات توسط سوئیچ برای ایستگاه دیگر نیز فراهم

خواهد شد. اترنت و استاندارد ۸۰۲.۳ شاید تاکنون اصطلاح ۸۰۲.۳ را در ارتباط با شبکه های اترنت شنیده باشید . اترنت بعنوان یک استاندارد شبکه توسط شرکت های : دیجیتال، اینتل و زیراکس (DIX) مطرح گردید. در سال ۱۹۸۰ موسسه IEEE کمیته ای را مسئول استاندار سازی تکنولوژی های مرتبط با شبکه کرد. موسسه IEEE نام گروه فوق را ۸۰۲ قرار داد. (عدد ۸۰۲ نشاندهنده سال و ماه تشکیل کمیته استاندارسازی است) کمیته فوق از چندین کمیته جانبی دیگر تشکیل شده بود . هر یک از کمیته های فرعی نیز مسئول بررسی جنبه های خاصی از شبکه گردیدند. موسسه IEEE برای تمایز هر یک از کمیته های جانبی از روش نامگذاری : X۸۰۲.X استفاده کرد. X یک عدد منصر بفرد بوده که برای هر یک از کمیته ها در نظر گرفته شده بود . گروه ۸۰۲.۳ مسئولیت استاندارد سازی عملیات در شبکه های CSMA/CD را برعهده داشتند. (شبکه فوق در ابتدا DIX Ethernet نامیده می شد) اترنت و ۸۰۲.۳ از نظر فرمت داده ها در فریم های اطلاعاتی با یکدیگر متفاوت می باشند. تکنولوژی های متفاوت شبکه متداولترین مدل موجود در شبکه های کامپیوتری(رویکرد دیگری از اترنت) توسط شرکت IBM و با نام Tken ring عرضه گردید. در شبکه های اترنت بمنظور دستیابی از محیط انتقال از فواصل خالی (Gap) تصادفی در زمان انتقال فریم ها استفاده می گردد. شبکه های Tken ring از یک روش پیوسته در این راستا استفاده می نمایند. در شبکه های فوق ، ایستگاه ها از طریق یک حلقه منطقی به یکدیگر متصل می گردند. فریم ها صرفا "در یک جهت حرکت و پس از طی طول حلقه ، فریم کنار گذاشته خواهد شد. روش دستیابی به محیط انتقال برای ارسال اطلاعات تابع CSMA/CD نخواهد بود و از روش Tken passing استفاده می گردد. در روش فوق در ابتدا یک Tken (نوع خاصی از یک فریم اطلاعاتی) ایجاد می گردد . Tken فوق در طول حلقه می چرخد . زمانیکه یک ایستگاه قصد ارسال اطلاعات را داشته باشد، می بایست Tken را در اختیار گرفته و فریم اطلاعاتی خود را بر روی محیط انتقال ارسال دارد. زمانیکه فریم ارسال شده مجددا "به ایستگاه ارسال کننده برگشت داده شد (طی نمودن مسیر حلقه)، ایستگاه فریم خود را حذف و یک Tken جدید را ایجاد وآن را بر روی حلقه قرار خواهد داد. در اختیار گرفتن Tken شرط لازم برا ی ارسال اطلاعات است . سرعت ارسال اطلاعات در این نوع شبکه ها چهار تا شانزده مگابیت در ثانیه است . اترنت با یک روند ثابت همچنان به رشد خود ادامه می دهد. پس از گذشت حدود سی سال ازعمر شبکه های فوق استانداردهای مربوطه ایجاد و برای عموم متخصصین شناخته شده هستند و همین امر نگهداری و پشتیبانی شبکه های اترنت را آسان نموده است . اترنت با صلابت بسمت افزایش سرعت و بهبود کارآئی و عملکرد گام بر می دارد.

شبکه گیگابایتی چیست؟

شبکه گیگابایتی چیست؟ شبکه های متصل با سیم نیز در کنار شبکه های بی سیم در حال پیشرفت اند. این پیشرفت باعث شده تا کامپیوترهای رو میزی بتوانند با سرعت ۱۰۰۰ مگابایت بر ثانیه به یکدیگر متصل شوند. چندی است که نسل تازه ای از شبکه های متصل با سیم با نام Eethernet گیگا بیتی زیر سایه و درهیاهوی شبکه های بی سیم متولد شده. این استاندارد که که طراحی آن از حدود ۶ سال پیش آغاز شده بود سرانجام به بار نشست و سرعت آن چهار برابر پر سرعت ترین شبکه بی سیم کنونی است. کنترل کننده های Ethernet گیگا بایتی کم کم جای خود را روی بردهای اصلی بازکرده و جای کنترل کننده های Fast Ethernet را با سرعت ۱۰۰ مگا بیت بر ثانیه می گیرند. آزمایش های نشان داده اند که سرعت شبکه های Ethernet گیگا بیتی در عمل به ۹۰ مگا بیت بر ثانیه می رسد. این میزان برابر است با ده برابر سرعت Fast Ethernet. آهنگ انتقال در Ethernet گیگابیتی در حال حاضر از هر سخت دیسکی بیشتر است. بنا براین هنگام کار با فایل های ویدئویی یا CAD که روی کامپیوتر های سرویس دهنده ذخیره شده اند، شبکه سرعت کار را کاهش نمی دهد. هر چه سریعتر، هر چه ارزانتر با گسترش کنترل کننده های گیگابیتی، در خواست برای سوئیچ های مناسب نیز رو به افزایش است. قیمت این دستگاه ها هم به طور همزمان رو به

کاهش است به طوری که یک سوئیچ گیگا بیتی با ۸ درگاه سال گذشته حدود ۲۰۰۰ یورو پایین آمده. Ethernet گیگا بیتی با سرعت زیادی که دارد برای انتقال داده ها روی شبکه های محلی هم بسیار مناسب است. دستگاه های Ethernet گیگا بیتی اگر چه با گونه های پیشین یعنی Fast Ethernet و Ethernet مگا بیتی سازگارند اما برای بهره مندی از بیشترین سرعت باید از هر ۴ زوج سیم استفاده کرد. افزون بر این از یک مدولاسیون پنج سطحی نیز استفاده می شود. همه اینها به این معنی است که روی هر زوج سیم و در هر تپش با بسامد ۱۰۰ مگا هرتز بیش از دو بیت منتقل می شود. در نتیجه بیش از یک گیگابیت بر ثانیه فرستاده می شود که بخشی از این پهنای باند اضافی برای رمز گذاری داده ها با شیوه Trellis به کار می رود. داده هایی که در این شیوه به جریان داده های اضافه می شود پایداری و ایمنی این شبکه ها را افزایش می دهد. کابل ها یکسان نیستند برای بهره مندی از بیشترین سرعت، باید کابل ها را کمی پیچیده تر ساخت. کابل های ۴ رشته ای Cat۵ که در Fast Ethernet در فاصله های کوتاه به کار می روند در Ethernet گیگا بیتی قابل استفاده نیستند و سرعت این دستگاه ها را تا حد Fast Ethernet کاهش می دهند. جالب است بدانید که در سخت افزار گیگا بیتی تفاوتی میان درگاه های Uplink و Dwnlink وجود ندارند. هر دستگاه طرف مقابل را شناسایی کرده و بسته به اینکه در سمت دیگر یک کارت شبکه یا یک سوئیچ قرار داشته باشد خود را تنظیم می کند. کابل های هشت رشته ای هم از نظر کیفیت با هم تفاوت دارند. قیمت کابل های Cat۶ به طور نظری امکان استفاده از بسامد ۳۰۰ مگا هرتز را فراهم می کند و آهنگ انتقال آن در مقایسه با Cat۵ روی هر جفت سیم سه برابر است. طول کابل Cat۶ حداکثر ۱۰۰ متر است که در صورت استفاده از یک سوئیچ می توان دو دستگاه کامپیوتر به فاصله ۲۰۰ متر را به یکدیگر متصل کرد. اما در این کابل ها در مقایسه با Cat۵ ویژگی آبشاری (Cascading) بسیار محدودتر شده به طوری که به جای امکان استفاده از پنج سوئیچ پشت سر هم (که فاصله را به ۶۰۰ متر می رسانند) تنها می توان از دو سوئیچ استفاده کرد که حداکثر فاصله را به ۳۰۰ متر محدود می کند. بنا براین در ساختمان های بزرگ برای استفاده از کابل های Cat۶ وجود Ruter لازم است. در صورت افزایش فاصله (برای نمونه میان دو ساختمان) باید به جای کابل های مسی، کابل های فیبر نوری را به کار برد. در این کابل های فیبر نوری Single Mde، فاصله می تواند تا پنج کیلومتر افزایش یابد. این را هم بگوییم که تجهیزات استفاده از فیبر نوری بیش از ده برابر تجهیزات کابل Cat۵ قیمت دارند. سرعت بسیار بالا برای کامپیوترهای شخصی بد نیست فاصله های زیاد را به حال خود گذاشته و کمی کاربرد شبکه های گیگابیتی را در کامپیوترهای شخصی بررسی کنیم. پهنای باندی که این شبکه ها فراهم می کنند برخی تغییرات را در سخت افزار کامپیوترهای شخصی ایجاب می کند. کارت شبکه گیگا بیتی در حالت دو طرفه کامل (Full Duplex) کار می کند. یعنی می تواند همزمان داده را فرستاده و دریافت کند که این آهنگ انتقال ۱۸۰ مگابایت در ثانیه را به دست می دهد در حالی که پهنای باند گذرگاه PCI تنها ۱۳۳ مگابایت برثانیه است. البته اگر در سیستم کارت PCI دیگری مانند کارت صوتی یا کنترل کننده RAID وجود داشته باشد این پهنای باند ۱۳۳ مگابایتی باز هم کاهش یافته و باقیمانده آن دراختیار کارت شبکه قرار می گیرد. بنابراین بی دلیل نیست که کارت های شبکه ویژه کامپیوتر های سرویس دهنده که با معماری ۶۴ بیتی ساخته می شوند پهنای باند ۵۳۳ یا حتی ۱۰۶۶ مگابیتی دارند. در مقابل، بیشتر کارت های شبکه یک پارچه با برد اصلی از نظر آهنگ انتقال داده با کارت های شبکه PCI تفاوتی ندارند چون آنها نیز به درگاه PCI کند متصل اند. تنها راه حل اینتل در سری تراشه های i۸۶۵ و i۸۷۵ با نام CSA) Cmmunicatins Streaming Architecture) است که این گلوگاه را تقریبا برطرف کرده. در این شیوه، کنترل کننده شبکه از طریق یک مسیر اختصاصی با آهنگ انتقال ۲۶۶ مگابایت بر ثانیه به سری تراشه متصل می شود. در نتیجه، بخش های دیگر نمی توانند سرعت آن را پایین بیاورند. بد نیست در اینجا اشاره کنیم که این کنترل کننده های اینتل در عمل به سرعت ۱۵۰ مگا بایت بر ثانیه دست پیدا می کنند در حالی که کنترل کننده های یکپارچه با برد اصلی مانند ۳Cm، Bradcm یا VIA آن هم بدون وجود کارت های PCI دیگری حتی تا نصف پایین می آید. آنچه که در این

میان بسیار عجیب است اینست که برخی شرکت های سازنده برد اصلی هیچ تمایلی به بهره برداری از این فناوری اینتل ندارند و با وجود تراشه های سری تراشه های i۸۷۵، i۸۶۵ روی محصولاتسان باز هم آنها را با کنترل کننده های Bradcm مجهز می کنند. استانداردسازی سری تراشه های که در آینده به بازار می آیند این مشکل را برطرف می کنند چون نه تنها گذرگاه پر سرعت PCI Experss را با خود دارند بلکه کنترل کننده شبکه گیگابایتی نیز با آنها یکپارچه شده. به نظر نمی رسد که Ethernet بتواند در بخش کامپیوترهای شخصی به سرعت های بالاتر دست پیدا کند. اگر چه همین حالا نیز استاندارد ۱۰ Ethernet گیگابایتی تعریف شده و دستگاه های سخت افزاری آن در دست ساخت هستند اما برای بهره مندی از سرعت بالای آن چاره به جز رفتن به سراغ کابل های فیبر نوری نیست. اگر روش های تشخیص خطا یا اندازه Packet در پروتکل Ethernet تغییر نکنند در شبکه های ۱۰ Ethernet گیگابایتی حداکثر می توان از کابل های مسی به طول ۱۰ متر استفاده کرد که برای پیاده سازی عملی شبکه ها بسیار کوتاه است.

شایعه حمله لینوکس در شبکه منتشر شد

شایعه حمله لینوکس در شبکه منتشر شد یک آگهی امنیتی جعلی که به نظر می آید از طرف Red Hat آمده است به کاربران لینوکس درباره یک حفره امنیتی بسیار بسیار بحرانی هشدار داد. به گزارش بخش خبر شبکه http://www.IRITN.cm ، به نقل از eWeek، این آگهی امنیتی که اواخر روز جمعه در اینترنت منتشر شد به کاربران لینوکس درباره یک حفره امنیتی بسیار بسیار بحرانی که می تواند سیستم ها را به خطر بیاندازد و به مهاجم اجازه دسترسی به سیستم اصلی بدهد را منتشر کرد. این پیام و Patch آن تنها یک پیام فریب آمیز برای کاربران لینوکس بود. به گفته این آگهی امنیتی جعلی، این آسیب پذیری در پکیجی از یوتیلتی های اصلی سیستم کشف شد این آسیب پذیری فایل های روی سیستم را دستکاری می کند. این آگهی جعلی درباره انتشار مشکلاتی در نسخه های ۲/۷ تا ۰/۹ Red Hat و ۱,۲Fedra Cre و دیگر برنامه ها هشدار داد. در عین حال در این آگهی آمده بود که ایستگاه های BSD و Slaris توسط این آسیب پذیری آلوده نشده است.

آشنایی با ترمینال های شبکه

در این مقاله درباره ی ترمینال های کامپیوتری که برای اتصال به شبکه استفاده می شوند، انواع آنها، مقایسه آنها با یکدیگر و پروتکل های ارتباطی مورد استفاده، مطالبی را خواهید آموخت. واژه های کلیدی: Thin- ترمینال Thick(Fat)- پروتکل RDP- پروتکل ۱ I- انواع ترمینال های شبکه احتمالا اصطلاح نرم افزارهای کاربردی تحت شبکه را شنیده اید. این نرم افزارها از دو قسمت تشکیل شده اند، قسمتی از نرم افزار که بر روی سرور نصب می شود و قسمتی از نرم افزار که بر روی سرور نصب می شود. در این نرم افزارها، بخشی از پردازش داده ها توسط پردازنده سرور و بخش دیگر توسط پردازنده کامپیوتر کاربر اجرا می شود. هر چقدر سهم کامپیوتر کاربر در اجرای نرم افزار کاهش یابد، به سخت افزار کمتری در آن احتیاج است. نوع خاصی از کامپیوترها وجود دارند که تمام بار پردازش داده ها را به پردازنده سرور محول می کنند. این کامپیوترها را ترمینال Thin می نامند. تنها وظیفه ی این ترمینال ها این است که اطلاعات ورودی کاربر را توسط کی برد و ماوس دریافت کرده و آنها را به برنامه کاربردی بر روی سرور منتقل کنند و نتایج حاصل از اجرا برنامه را که قرار است روی صفحه نمایش نشان داده شود، به مانیتور کاربر منتقل نماید. به همین دلیل گاهی این ترمینال ها را ترمینال های گنگ می نامند. شبکه هایی که در آن نرم افزارها تماما بر روی سرور اجرا می شوند شبیه سیستم های Mainframe و Minicmputer هستند که کاربران توسط ترمینال ها به آنها متصل می شوند. از آنجایی که این ترمینال ها پردازش مهمی را انجام نمی دهند و فقط داده های ورودی را به سمت سرور فرستاده و داده

هی خروجی را از سرور دریافت می کنند، احتیاج به پردازنده ی پیشرفته ای ندارند و یک پردازنده ی ساده نیز می تواند در این ترمینال ها مورد استفاده قرار بگیرد. ازمعروف ترین ترمینال های Thin به محصولات Wysee و HP می توان اشاره کرد. در مقابل ترمینال های Thin، ترمینال های Thick قرار دارند که بخش عمده ی پردازش یا تمام پردازش را بر روی کاربران انجام می دهند. ترمینال های Thick همان کامپیوترهای شخصی PC هستند که به شبکه متصل شده اند. در کشورما برای اتصال به اتصال به شبکه و اجرا نرم افزارها معمولا- از ترمینال های Thick استفاده می شود. با استفاده از نرم افزارها می توان یک ترمینال از نوع Thick را به یک ترمینال Thin تبدیل کرد. مثلا با استفاده از نرم افزار Telnet که در سیستم عامل ویندوز وجود دارد می توانیم به یک کامپیوتر دیگر متصل شده ونرم افزارهای نصب شده بر روی آن کامپیوتر را اجرا کنیم. نرم افزار PCAnywhere نیز دارای این قابلیت است که یک کامپیوتر شخصی را به یک ترمینال Thin تبدیل کند. وقتی یک PC را به یک ترمینال Thin تبدیل می کنیم مثل این است که فقط از کی برد، ماوس و مانیتور آن کامپیوتر استفاده می کنیم. سرور شبکه ای که در آن ترمینال های Thin وجود دارد، باید سیستم عاملی با ویژگی چند کاربری (امکان اتصال چند کاربر به طور هم زمان و اجرای نرم افزارهای کاربردی بر روی آن) داشته باشید. از جمله این سیستم عامل ها به Windws ۲۰۰۰ Server و Linux می توان اشاره کرد. برنامه Teminal Service در Windws ۲۰۰۰ و نسخه جدیدتر آن در Windws ۲۰۰۳، امکان اتصالات کاربران ترمینال های Thin به سرور و مدیریت آنها را فراهم می آورد. همچنین این نرم افزار می تواند یک PC را به یک ترمینال Thin تبدیل کند. ۲- مقایسه ترمینال ها Thin و Thick استفاده از ترمینال های Thin به جای استفاده از PC برای کاربران شبکه، هزینه ی خرید سخت افزارهای شبکه را کاهش می دهد و مدیریت کاربران را آسان می کند. اکنون این سوال مطرح می شود که آیا بهتر نیست در پیاده سازی یک شبکه به جای استفاده از PC به عنوان ایستگاه کاری، از ترمینال های Thin استفاده کرد؟ در این قسمت ترمینال های Thin با ترمینال های Thick مقایسه می کنیم. ترمینال های Thin دارای قابلیت های جالبی هستند. ترمینال های Thin سبکتر از PC ها هستند و فضای کمتری را در محیط اشغال می کنند. چون در ترمینال Thin تمام پردازش های لازم بر روی سرور انجام می شود، در آن احتیاج به نرم افزار و سخت افزار کمتر و ساده تری می باشد. معمولا- ترمینال Thin دارای دیسک سخت نیست و سیستم عامل ساده ی آن بر روی RM یا Flash Memry قرار دارد. مدیریت ایستگاه های کاری شبکه ای که از ترمینال های Thin تشکیل شده، آسان است و مدیر شبکه می تواند تمام ایستگاه های کاری را از پشت کامپیوتر سرور مدیریت کند. به این نوع مدیریت ایستگاه های کاری که از یک نقطه ی شبکه، می توان تنظیمات ایستگاه های کاری را انجام داد، مدیریت مرکزی می گویند. به همین دلیل در بعضی از کافی نت ها از ترمینال های Thin استفاده می شوند. معمولا ترمینال Thin، درایو فلاپی و CD-RM ندارد و احتمال آلوده شدن آن به ویروس کمتر است. به دلیال اینکه در ترمینال Thin قطعات مکانیکی متحرک مانند دیسک سخت وجود ندارد، سرو صدای کمتری نسبت به PC ها دارد و از آنها می توان در مکان هایی که دارای آلودگی ذرات هستند، استفاده کرد. چون در ترمینال های Thin قطعات کمتری به کار رفته است و نیز در این ترمینال ها از قطعات مکانیکی استفاده نمی شود، دیرتر خراب می شوند. همچنین این ترمینال ها توان الکتریکی کمتری مصرف می کنند. ترمینال های Thin معمولا ارزانتر از یک PC هستند و استفاده از ترمینال Thin می تواند در بعضی موارد تا ۵۰ درصد از هزینه های کل شبکه را کاهش دهد. ترمینال های Thick نیز دارای مزایای مخصوص به خود هستند. اگر شما چندین کامپیوتر قدیمی در اختیار دارید که بدون استفاده هستند، می توانید از آنها به عنوان ترمینال Thick استفاده کنید و مقدار قابل توجهی در هزینه ها صرفه جویی کنید. ترمینال های Thick به طور مستقل نیز قابل استفاده هستند و اگر سرور شبکه از کار بیافتد، کاربران می توانند به کار خود ادامه دهند. اما اگر در یک شبکه با ترمینال های Thin، سرور شبکه از کار بیافتد، ترمینال ها بدون استفاده خواهند بود. لذا وجود یک سرور پشتیبان در شبکه هایی با ترمینال های Thin، بسیار ضروری است. به ترمینال های Thick می توان تجهیزات جانبی

مانند Scanner و Webcam متصل کرد و قابلیت های آنها را افزایش داد. در شبکه هایی که از ترمینال های Thin استفاده می کنند چون به طور همزمان بر روی سرور چندین نرم افزار اجرا می شود، باید سرور دارای تجهیزات سخت افزاری و نرم افزاری پیشرفته ای باشد. اما سرور شبکه هایی با ترمینال های Thick می تواند یک سرور معمولی باشد. در شبکه هایی با ترمینال های Thin حجم زیادی از داده ها بین ترمینال و سرور انتقال داده می شود که عمده این داده ها، اطلاعات صفحه نمایش است. انتقال این حجم از داده ها پهنای باند زیادی از شبکه را اشغال می کند. بنابراین سرعت این شبکه ها باید زیاد باشد اما برای ترمینال های Thick، سرعت شبکه های معمولی نیز کفایت می کند. بنابراین پاسخ به این سوال که آیا در شبکه ها باید از ترمینال های Thin استفاده کرد یا از ترمینال های Thick، به این بستگی دارد که در شبکه چه کاری می خواهیم انجام دهیم و تجهیزات فعلی در دسترس کدامند؟ ۳- پروتکل های انتقال داده ها بین ترمینال Thin و سرور انتقال داده ها بین ترمینال Thin و سرور با رعایت مقرراتی (پروتکل) انجام می گیرد. اولین و قدیمی ترین پروتکل استفاده شده پروتکل Telnet است. این پروتکل فقط می تواند اطلاعات متنی را انتقال دهد. پروتکل Telnet یک پروتکل استاندارد است که اطلاعات فنی آن در سند RFC۸۵۴ وجود دارد. ازاین پروتکل برای یافتن اشکالات بعضی برنامه ها مانند Mail Server استفاده می شود. برای مدیریت روترها نیز از این پروتکل می توان استفاده کرد زیرا مدیریت روترها معمولا با ارسال فرمان های متنی انجام می شود. در حال حاضر با توجه به اینکه تقریبا اکثر نرم افزارها دارای رابط گرافیکی هستند از پروتکل های دیگری که برای انتقال تصاویر مناسب است، استفاده می شود که معروفترین آنها پروتکل ICA و پروتکل RDP است. پروتکل ICA متعلق به شرکت Citrix و پروتکل RDP متعلق به شرکت Micrsft است. ترمینال های Thin که در بازار به فروش می رسند یکی از این دو پروتکل یا هر دوی آنها را به کار می برند. اخیرا ویژگی های جالبی به این پروتکل ها اضافه شده است. استفاده بهتر از پهنای باند، نمایش تصاویر با تعداد رنگ بیشتر(۶۵۵۳۶ رنگ) و فشرده سازی داده هایی که در شبکه ارسال می شوند، از جمله این موارد است. همچنین نسخه های جدید این پروتکل ها می توانند از پورت ها و درایوهای یک PC مانند پورت ها و درایوهای سرور استفاده کنند. قابلیت توزیع بار از دیگر ویژگی های جالب نسخه های جدید این پروتکل ها است. با این قابلیت می توانیم چندین سرور یکسان را در شبکه نصب کنیم و پردازش داده های کاربران را بین آنها توزیع نماییم در حالی که از دید کاربران در این شبکه یک سرور بیشتر دیده نمی شود. به این ترتیب سرعت پردازش داده ها افزایش می یابد. این پروتکل ها دارای مزایایی نسبت به یکدیگر هستند که در هنگام خرید ترمینال Thin باید به آن توجه کرد. نرم افزارهای پروتکل ICA گران قیمت تر از پروتکل RDP است ولی قابلیت هایی که پروتکل ICA ارائه می دهد بیشتر از RDP می باشد. معمولا- پروتکل RDP دنباله رو پروتکل ICA است یعنی نسخه های جدید پروتکل RDP ویژگی های نسخه های قبلی پروتکل ICA را پیاده سازی کرده اند. با پروتکل ICA می توانیم کامپیوترهایی با سیستم عامل لینوکس، ویندوز یا مکینتاش را به سرور متصل کنیم ولی پروتکل RDP فقط سیستم عامل ویندوز را می تواند به سرور متصل کند. پروتکل RDA فقط با پروتکل TCP/IP کار می کند ولی پروتکل ICA با NetBEUI و IPX/SPX نیز می توانند داده ها را منتقل نماید

مقدمه ای بر مفاهیم تست نفوذپذیری

برای آشنایی بیشتر شما با این مباحث توضیحاتی برای شما ارائه شده است که در بخش های زیر می آید: ۱- تست نفوذپذیری چیست ؟ ۲- چرا شما به آن نیاز دارید ؟ ۳- یک سرویس را انتخاب کنید. ۴- ره آوردهای مختلف تست نفوذپذیری ۵- در ازای پولتان چه چیزی به دست می آورید ؟ ۱-تعریف : تست نفوذپذیری چیست ؟ تست نفوذپذیری رویه ای است که درآن میزان امنیت اطلاعات سازمان شما مورد ارزیابی قرار می گیرد. یک تیم مشخص با استفاده از تکنیک های هک یک حمله واقعی را شبیه

سازی می کنند تا به این وسیله سطح امنیت یک شبکه یا سیستم را مشخص کنند. تست نفوذپذیری به یک سازمان کمک می کند که ضعف های شبکه و ساختارهای اطلاعتی خود را بهتر بشناسد و در صدد اصلاح آنها بر آید. این امر به یک سازمان کمک می کند تا در زمینه تشخیص، توانایی پاسخ و تصمیم مناسب در زمان خود، بر روی امنیت نیروها و شبکه خود یک ارزیابی واقعی داشته باشد. نتیجه این تست یک گزارش می باشد که برای اجرایی شدن و بازرسی های تکنیکی مورد استفاده قرار می گیرد. ۲- چرا تست نفوذپذیری؟ چرا شما به آن نیاز دارید؟ دلایل مختلفی وجود دارد که یک سازمان تست نفوذپذری را انتخاب می کند. این دلایل می تواند از مسایل تکنیکی تا مسایل تجاری طبقه بندی گردند. اما برخی از عمومی ترین مسایل آن به صورت زیر می باشد : - مشخص کردن خطرات و ریسک هایی که سرمایه های اطلاعاتی سازمان شما با آنها مواجهه می شوند. در اصل شما می توانید با ریسک های اطلاعاتی خود آشنا شوید و سپس برای آنها به مقدار مورد نیاز هزینه کنید. - کاهش هزینه های امنیتی سازمان شما : با مشخص کردن نقاط ضعف و آسیب پذیری های سیستم های اطلاعاتی خود به مقدار قابل توجهی از هزینه های صرف شده برای امنیت، می کاهید ، زیرا که ممکن است آسیب پذیری ها و ضعف هایی در زیرساخت های تکنولوژیکی و یا ضعف های طراحی و پیاده سازی وجود داشته باشد که در تست نفوذپذیری مشخص می شوند. - ضمانت و آسودگی خاطر را برای سازمان شما به ارمغان می آورد – یک ارزیابی دقیق و کامل از امنیت سازمان شما ، کل سیاستها (Plicy) ، روالها، طراحی و پیاده سازی آن را پوشش می دهد. - دستیابی و نگهداری گواهینامه ها (HIPAA ، BSvv۹۹ و ...) - بهترین رویه برای تست آیین نامه های صنایع و قوانین حاکم بر آن ۳- یک سرویس را انتخاب کنید: چه تفاوتی بین انواع تست های مختلف وجود دارد؟ الف) تست نفوذپذیری بیرونی(External Penetratin Testing) : یکی از عمومی ترین ره آوردهای تست نفوذپذیری می باشد. این تست روی سرور ها، زیر ساخت های شبکه و زیر ساختهای نرم افزارهای سازمان انجام می گیرد. این تست ممکن است بدون دریافت هیچگونه اطلاعاتی از سازمان مورد نظر صورت گیرد (جعبه سیاه – Black Bx) یا با دریافت کلیه اطلاعات توپولوژیکی و محیطی صورت گیرد (جعبه شفاف – Crystal Bx). این تست ابتدا با استفاده از اطلاعات عمومی و در دسترس از سازمان مورد نظر شروع می شود و سپس با شناسایی میزبانها و سرور های شبکه هدف و تجزیه و تحلیل آن ادامه پیدا می کند. در ادامه رفتارهای ابزارهای امنیتی مانند مسیریابها و دیواره های آتش تجزیه و تحلیل می گردند. آسیب پذیری های موجود برای هر میزبان شبکه مشخص و بازبینی می گردند و دلایل آن نیز مشخص می شود. ب) ارزیابی امنیتی داخلی (Internal Security Assessment) : روالی مانند تست بیرونی دارد اما یک دید کامل تری نسبت به مسایل امنیتی سازمان ارائه می دهد. این تست عموما از شبکه های Access Pint و بازدید و مرور دوباره قسمتهای فیزیکی و منطقی شبکه انجام می گیرد. برای نمونه ممکن است لایه های شبکه، DMZ درون شبکه و شبکه های شرکاء که با شبکه شما مرتبط می باشند نیز مورد بررسی و تست قرار گیرد. پ) ارزیابی امنیتی برنامه های کابردی (Applicatin Security Assessment) این تست روی تمامی برنامه های کاربردی اختصاصی و غیر اختصاصی سازمان هدف انجام می گیرد و در طی آن تمامی خطرات این برنامه ها مشخص می شود. برای مثال نباید این برنامه ها، پتانسیل این را داشته باشند که اطلاعات حساس سازمان را در معرض عموم قرار دهند. این ارزیابی مهم و حیاتی می باشد و در طی آن باید بدانیم که اولا؛ این برنامه های کاربردی ، نرم افزارها و سرور های شبکه را در معرض خطر قرار نمی دهند. دوم اینکه یک کاربر خرابکار نمی تواند به داده های حیاتی دسترسی داشته باشد و آنها را تغییر دهد یا خراب کند. حتی در شبکه هایی که دارای زیر ساختهای قوی و قدرتمندی می باشند، یک برنامه کاربردی ناقص و آسیب پذیر می تواند کل شبکه را در معرض خطر قرار دهد. ت) ارزیابی امنیتی شبکه های بیسیم و دسترسی های از راه دور (Remte Access) در اصل ارزیابی خطرهایی می باشد که سیستم های سیار را در بر دارد. کار در خانه، با پهنای باند بالا از طریق اینترنت، استفاده از شبکه های بیسیم ۸۰۲.۱۱ و تکنولوژی های دسترسی از راه دور را به صورت گسترده ای افزایش داده است. طراحی و معماری امن

اینگونه شبکه ها بسیار مهم و حیاتی می باشد و باید از ریسک ها و خطرهای آنها به صورت کاملی آگاه شویم. ث) مهندسی اجتماعی (Scial Engineering) اشاره دارد به نفوذ هایی که از راه های غیر تکنیکی انجام می شود. این بخش به طور کلی روی ارتباطات افراد و کارکنان سازمان تکیه دارد و مشخص می کند چگونه مسایل انسانی سازمان می توانند مسایل امنیتی آن را در معرض خطر قرار دهند و باعث شکسته شدن برخی روال های امنیتی گردند. مهندسی اجتماع با استفاده از ایجاد روابط قابل اعتماد و دوستانه با اشخاص سازمان و با نمایش قصد کمک به طرف مقابل، اطلاعات حساس امنیتی از جمله کلمات رمز و نام کاربری او را دریافت می کند. موارد دیگر نیز به «آشغال گردی» موسوم است که در آن با جستجو در آشغالهای سازمان مورد نظر، به دنبال اطلاعات حساس و مهم می گردند. همچنین مسایل روان شناختی افراد برای حدس زدن کلمات رمز و ... نیز جزو این بخش از کار می باشد. ۴- انواع ره آوردهای مختلف : تست جعبه سیاه (Black Bx) و تست جعبه سفید (White Bx) تست نفوذپذیری به دو صورت مختلف می تواند انجام گیرد: «جعبه سیاه» (بدون دریافت هیچگونه دانش اولیه برای تست) و «جعبه سفید » (دریافت کلیه اطلاعات زیر ساختی برای تست) معمولاـ شرکت هایی که کار تست نفوذپذیری را انجام می دهند از شما می خواهند که یکی از موارد فوق را انتخاب کنید. اما تست جعبه سیاه به نظر بهترین انتخاب می باشد ، زیرا که یک شبیه سازی حقیقی از حمله یک هکر را پیاده سازی می کند. این یک ایده بسیار جالبی می باشد اما به طور دقیقی درست نیست. اولا اینگونه فرض کردیم که هکر هیچگونه اطلاعاتی از سیستم های شما ندارد ، که همیشه اینگونه نیست! اگر به طور واقعی یک هکر ، سازمان شما را هدف قرار دهد اینگونه نیست که هیچگونه اطلاعاتی از سیستم ها و شبکه داخلی سازمان نداشته باشد (فرض کنید هکر یکی از کارکنان سازمان شما باشد). البته در هر کدام از این موارد باید خطاهایی را نیز به صورت پیش فرض قبول کنیم. در اصل باید اینگونه فرض کرد که هکر اطلاعات کاملی از سیستم های شما را دارد زیرا که اگر امنیت شما بر اساس پنهان کردن طراحی شبکه باشد بنابراین از لحاظ امنیتی شبکه شما هیچ وقت نباید قابل لمس باشد که این غیر ممکن است! دوم اینکه بر خلاف یک تست کننده شبکه، یک هکر از لحاظ زمانی محدود نیست و محدودیت هایی که برای یک تست کننده وجود دارد برای یک هکر وجود ندارد. به عنوان مثال یک مهاجم ممکن است زمان زیادی (بعضی مواقع بیش از یک سال) را صرف کند تا یک آسیب پذیری را در سیستمی پیدا کند و توسط آن به شبکه نفوذ کند. سوالی که در اینجا مطرح می شود این است که این تست چه مقدار هزینه در بردارد؟ در تست جعبه سیاه مهم آن است که تیم تست کننده باید به مقدار قابل توجهی زمان صرف شناسایی شبکه هدف کند. این زمان ممکن است حتی بیش از زمانی باشد که صرف تست آسیب پذیری ها می گردد. اینگونه نیست که بگوییم تست جعبه سیاه هیچ هزینه ای در برندارد ، حتما هزینه هایی را در بر دارد. این مساله خیلی مهم است که تست کننده اطلاعاتی را درباره سیستم هایی که ممکن است توسط افراد دیگر مورد سوءاستفاده قرار گیرد را به دست آورد. پس حتما در تست جعبه سیاه باید زمان بیشتری برای انجام تست در نظر گرفت. ۵- در ازای پولتان چه چیزی به دست می آورید ؟ تست نفوذپذیری در اصل یک تجزیه و تحلیل اصولی برای تعین میزان امنیت سازمان شما می باشد. یک پروژه کامل ممکن است کلیه موارد مشخص شده در زیر را در بر گیرد: Netwrk Security • Netwrk Surveying • Prt Scanning • System Identificatin • Services Identificatin • Vulnerability Research & Verificatin • Applicatin Testing & Cde Review • Ruter Testing • Firewall Testing • Intrusin Detectin System Testing • Trusted Systems Testing • Passwrd Cracking • Denial f Service Testing • Cntainment Measures Testing Infrmatin Security • Dcument Grinding • Cmpetitive Intelligence Scuting • Privacy Review Scial Engineering • Request Testing • Guided Suggestin Testing • Trust Testing Wireless Security • Wireless Netwrks Testing • Crdless Cmmunicatins Testing • Privacy Review •

Infrared Systems Testing Cmmunicatins Security • PBX Testing • Vicemail Testing • FAX review • Mdem Testing Physical Security • Access Cntrls Testing • Perimeter Review • Mnitring Review • Alarm Respnse Testing • Lcatin Review • Envirnment Review بنابراین برای انجام کامل تست نیاز به صرف وقت کافی می باشد. گوهر و ارزش تست نفوذپذیری به گزارشی می باشد که در انتها دریافت می کنید. این گزارش باید در بخش های مختلفی آماده شود حتی این گزارش باید برای مدیران قابل فهم باشد و از طرفی باید گزارش برای کسانی که در بخش امنیتی سازمان شما و یا در بخش های تکنیکی و گواهینامه های امنیتی فعالیت دارند نیز کاربرد داشته باشد. هیئت مدیره سازمان نیاز دارد که از خطرات موجود و راه حل های ممکن آن به دور از مسایل تکنیکی آگاه شود. مدیران تکنیکی نیاز دارند که دید بازتری نسبت به وضعیت موجود داشته باشند که البته این دسته از افراد نیز ، نیازی به کلیه جزییات ندارند. ولی مدیران سیستم ها و مدیران شبکه باید از آسیب پذیری های هر سیستم به صورت جزیی و دقیق اطلاعات کاملی داشته باشند. البته این گزارش ها برای سازمانهای مختلف می تواند متفاوت باشد. در بعضی مواقع از چند صفحه تا چند صد صفحه گزارش می تواند تغییر داشته باشد.

پیاده سازی الگوریتم Dijkstra

Include Include Include include include include include Using namespace std; Typedef map > graph; class DistancePair public: DistancePair(unsigned int ds, string &dt) : distance(ds), destinatin(dt) bl peratr>(cnst DistancePair &right) cnst return distance > right.distance; string getDestinatin() cnst return destinatin; unsigned int getDistance() cnst return distance; private: unsigned int distance; string destinatin; vid dijkstra(graph &cityMap, string start, map &distances) pririty_queue, greater > que; que.push(DistancePair(۰,start)); while(!que.empty()) { int distance = que.tp().getDistance(); string city = que.tp().getDestinatin(); que.pp(); if(distances.cunt(city) == ۰) { distances[city] = distance; map::iteratr start, stp; start = cityMap[city].begin(); stp = cityMap[city].end(); while(start != stp) { unsigned int destDistance = (start).secnd; string destCity = (start).first; que.push(DistancePair(distance + destDistance, destCity)); start++; vid buildCityMap(graph &cityMap) { cityMap["A"]["B"] = ۷; cityMap["A"]["C"] = ۴; cityMap["A"]["D"] = ۶; cityMap["A"]["E"] = ۱; cityMap["C"]["B"] = ۲; cityMap["C"]["D"] = ۵; cityMap["D"]["B"] = ۳; cityMap["E"]["D"] = ۱; int main() graph cityMap; buildCityMap(cityMap); map distances; dijkstra(cityMap, "A", distances); map::iteratr start, stp; start = distances.begin(); stp = distances.end(); while(start != stp) { cut << ();(start).first << " " << (start).secnd << endl; start++; getchar

محاسبات شبکه ای چیست؟

در محاسبات شبکه ای چندین پردازشگر به طور همزمان و جداگانه محاسبه خاصی را انجام می دهند. به گزارش بخش خبر شبکه

فن آوری اطلاعات ایران، به نقل از ایلنا، امروزه در بسیاری از محافل اطلاعاتی و مراکز IT صحبت از محاسبات شبکه ای یا GRID CMPUTING است ؛ اما این اصطلاح هنوز برای بسیاری از کاربران ناشناخته باقی مانده است. محاسبات شبکه ای در ساده ترین حالت ممکن, به معنی فعالیت مشترک پردازنده های چندگانه بر روی ماشین های چندگانه است و هدف آن افزایش توان محاسباتی در زمینه هایی است که توان بسیار بالای CPU را می طلبد. در محاسبات شبکه ای سرورهای چندگانه ای با هم ارتباط دارند که از سیستم عامل ها و نرم افزارهای مشابهی استفاده می کند. به کمک محاسبات شبکه ای, می توان کارهای محاسباتی را به طور همزمان به کمک چندین پردازشگر انجام داد. در مواردی که نتیجه محاسبات خیلی حساس است و دقت آن سرنوشت ساز است, ده ها و گاهی هزاران پردازشگر به طور همزمان یک محاسبه را انجام می دهند. بعد از انجام محاسبات نتایج کار همه پردازشگرها با هم مقایسه می شود تا میزان دقت محاسبات تعیین شود.

آموزش HyperTerminal

۵۰۰۰۵ارسال فایلها بدون استفاده از اینترنت HyperTerminal برنامه ای است که توسط آن می توانید با استفاده از خطوط تلفن (و بدون نیاز به اینترنت) فایلهایی را از هر نوع به دوستانتان ارسال و یا از آنها فایلهایی را دریافت نمایید. شاید شما هم مانند من از ارسال فایلها توسط ابزار ذخیره سازی (مانند CD، دیسک و...) خسته شده اید در این قسمت قصد داریم به بررسی یکی از قابلیتهای جذاب و کمتر شناخته شده ویندوز که توانایی بالایی در ارسال و دریافت فایلهای مختلف به نام Hyper Terminal بپردازیم. HyperTerminal چیست؟ HyperTerminal برنامه ای است که توسط آن می توانید با استفاده از خطوط تلفن (و بدون نیاز به اینترنت) فایلهایی را از هر نوع به دوستانتان ارسال و یا از آنها فایلهایی را دریافت نمایید. در صورت کار با این برنامه در بسیاری از موارد شما دیگر نیازی به استفاده از اینترنت نخواهید داشت، بنابراین قادرید در هزینه های اتصال به اینترنت تا حد زیادی صرفه جویی کنید. برنامه Hyper Terminal به صورتی کاملاً ـ ساده و آسان طراحی گردیده به صورتی که شما با چند بار کار کردن با آن می توانید با نحوه کار کاملاً آشنا گردید. نکته: برای استفاده از HyperTerminal شما به امکانات خاص نیاز ندارید فقط کافی است که کامپیوتر شما و فردگیرنده به یک مودم مجهز باشد تا شما از طریق خط تلفن فایل مورد نظرتان را ارسال و یا دریافت نمایید. نحوه استفاده از Hyper Terminal برای فعال نمودن HyperTerminal در ویندوز xp به روی کلید Start کلیک نموده و از منوی کشویی ظاهر شده به ترتیب Accessries < All prgrams < Hyper Terminal< Cmmunicatins را انتخاب کنید تا پنجره Cnnectin Descriptin در روی صفحه نمایش ظاهر گردد. در کادر فوق یک نام را برای اتصال وارد کرده و از قسمت Icn یک آیکون را به دلخواه انتخاب نموده و بر روی کلید K کلیک کنید. در پنجره Cnnect T از منوی کشویی regin / Cuntry کشور محل سکونت خود (که در اینجا IRAN را باید انتخاب نمایید مگر اینکه خارج از ایران زندگی می کنید)، AreaCde کد کشور، phnenumber شماره تلفن تماس و از منوی CnnectUsing ابزار مورد استفاده (که در این جا مودم می باشد) را انتخاب کرده و برروی کلید K کلیک نمایید. نکته: در قسمت phne number شما باید شماره تلفن شخصی که می خواهید برای او فایل مورد نظرتان را ارسال کنید را وارد نمایید. در پنجره Cnnect شما کافی است بر روی کلید Dial کلیک کنید تا شماره گیری انجام گیرد. در این مرحله در صورتی که می خواهید تغییری در شماره تلفن تماس و یا محل سکونت خود دهید کافی است برروی کلیدهای Mdify یا Dialing prperties کلیک کرده و در کادرهای محاوره ای ظاهر شده تغییرات مورد نظر را اعمال نمایید. بعد از چند لحظه شماره گیری توسط مودم انجام می شود. تنظیماتی که فرد گیرنده باید انجام دهد برای دریافت یک فایل از طریق HyperTerminal فقط کافی است در پنجره اصلی برنامه از منوی Call گزینه Wait Fr a Call را انتخاب نمایید. بعد از چند لحظه شما می توانید فایلهای ارسالی را

دریافت کنید. ارسال فایلها بعد از اینکه در پنجره Cnnect تنظیمات مربوطه را انجام دادید و توسط شماره گیری به شماره مربوطه متصل شدید. برای مشخص کردن فایلهای ارسالی از منوی Transfer گزینه Send File را انتخاب کنید تا کادر محاوره ای Send File در روی صفحه نمایش ظاهر گردد. در کادر محاوره ای ظاهر شده برای انتخاب فایل مورد نظرتان بر روی کلید Brwse کلیک کنید تا کادر محاوره ای Select File t Send در روی صفحه نمایش ظاهر گردد. در کادر محاوره ای فوق شما کافی است فایل مورد نظرتان را انتخاب نموده و بر روی کلید pen کلیک نمایید و در کادر محاوره ای Send file بر روی کلید Send کلیک کنید تا عمل ارسال انجام پذیرد. ارسال پیغام به صورت متن بعد از اینکه به شماره مورد نظرتان متصل شدید در پنجره اصلی برنامه Hyper Terminal شما به صورت مستقیم می توانید متن مورد نظرتان را تایپ نمایید. متن تایپی در این قسمت برای دوست شما که به کامپیوتر او توسط برنامه Hyper Terminal متصل شدید نیز قابل مشاهده می باشد. مشخص کردن محلی برای ذخیره سازی فایلهای دریافتی شما به سادگی می توانید محلی را برای ذخیره سازی فایلهای دریافتی از طریق برنامه را به صورت پیش فرض تعریف نمایید. برای این منظور از منوی Transfer گزینه Receive File را انتخاب نمایید تا کادر محاوره ای مربوطه در روی صفحه نمایش ظاهر گردد. در کار محاوره ای فوق شما با کلیک نمودن کلید Brwse می توانید محلی را برای ذخیره سازی فایل دریافتی تعیین نمایید. ذخیره سازی اتصال بعد از برقراری ارتباط از طریق برنامه Hyper Terminal، شما می توانید اتصال فوق را برای استفاده مجدد ذخیره نمایید. برای این منظور از منوی کشویی File گزینه Save را انتخاب کنید. با این کار اتصال شما با اسمی که شما برای آن مشخص نموده اید ذخیره می گردد، برای برقراری اتصال برای دفعات آتی، در زیر منوی Accessries < All Prgrams < Start HyperTerminal Cmmunicatins کافی است به روی نام اتصال فقط کلیک کنید. قطع نمودن اتصال بعد از اینکه فایل های موردنظرتان را برای دوستانتان ارسال کردید و یا از آنها دریافت کردید، برای قطع نمودن اتصال به روی گزینه Discnnect کلیک نمایید تا اتصال شما قطع گردد. نوار ابزار برنامه Hyper Terminal در نوار ابزار برنامه HyperTerminal مجموعه دستورات پراستفاده به صورت آیکونهایی در دسترس شما قرار گرفته است. در صورتی که نوار ابزار برنامه در زیر نوار منوها وجود نداشت از زیر منوی View گزینه TlBar را انتخاب کنید

با Dhcp بیشتر آشنا شوید

تمامی پروتکل های شبکه به هر یک از کامپیوترهای موجود در شبکه، یک مشخصه (آدرس) منحصر بفرد را نسبت می دهند پروتکل IPX ، آدرس فوق را بصورت اتوماتیک و توسط ایستگاه کاری نسبت و منحصر بفرد بودن آن تضمین خواهد شد. پروتکل NetBEUI از یک نام NetBIS شانزده بیتی استفاده می نماید . پروتکل TCP/IP از یک آدرس IP ، استفاده می نماید. در نسخه های اولیه پیاده سازی شده TCP/IP ، از پروتکل فوق بمنظور اتصال تعداد اندکی از کامپیوترها استفاده می گردید و ضرورتی به وجود یک مرکز متمرکز بمنظور اختصاص اطلاعات آدرس دهی IP ، احساس نمی گردید. بمنظور حل مشکل مدیریت صدها و یا هزاران آدرس IP در یک سازمان ، DHCP پیاده سازی گردید. هدف سرویس فوق ، اختصاص آدرس های IP بصورت پویا و در زمان اتصال یک کامپیوتربه شبکه است . با وجود یک سرویس دهنده DHCP در شبکه ، کاربران شبکه قادر به اخذ اطلاعات مربوط به آدرس دهی IP می باشند . وضعیت فوق ، برای کاربرانی که دارای یک Laptp بوده و تمایل به اتصال به شبکه های متعدد را داشته باشند ، ملموس تر خواهد بود چراکه با برای ورود به هر یک از شبکه ها و استفاده از منابع موجود ، ضرورتی به انجام تنظیماتی خاص در رابطه با آدرس دهی IP وجود نخواهد داشت . سرویس دهنده DHCP ، علاوه براختصاص اطلاعات پایه IP نظیر : یک آدرس IP و Subnet mask ، قادر به ارائه سایر اطلاعات مربوط به

پیکربندی پروتکل TCP/IP برای سرویس گیرندگان نیز می باشد . آدرس Gateway پیش فرض ، سرویس دهنده DNS ، نمونه هائی در این زمینه می باشند. DHCP ویندوز ۲۰۰۰ (نسخه های سرویس دهنده) با سرویس دهنده DNS(Dmain Name System) ، در ارتباط خواهد بود. ویژگی فوق ، به یک سرویس دهنده DHCP اجازه می دهد که با یک سرویس دهنده پویای DNS ویندوز ۲۰۰۰ (DDNS) ، مرتبط و اطلاعات ضروری را با وی مبادله نماید . سرویس دهنده DHCP ویندوز ۲۰۰۰ ، قادر به ارائه پویای آدرس IP و Hst name بصورت مستقیم برای یک سرویس دهنده DDNS است . DHCP ، مسئولیت ارائه اطلاعات آدرس های IP سرویس گیرندگان را برعهده دارد . بمنظور اخذ اطلاعات آدرس دهی IP ، سرویس گیرنده می بایست یک lease را از سرویس دهنده DHCP دریافت نماید.زمانیکه سرویس دهنده DHCP ، اطلاعات آدرسی دهی IP را به یک سرویس گیرنده DHCP نسبت (اختصاص) می دهد ، سرویس گیرنده DHCP مالکیت آدرس IP را نخواهد داشت .در چنین حالتی ، سرویس دهنده DHCP همچنان مالکیت آدرس IP را بر عهده داشته و سرویس گیرنده اطلاعات فوق را اجاره و بصورت موقت و بر اساس یک بازه زمانی در اختیار خواهد داشت . می توان یک آدرس IP را بمنزله یک قطعه زمین در نظر گرفت که بصورت اجاره ای در اختیار سرویس گیرنده قرار گرفته و لازم است قبل از سررسید مدت قرارداد! نسبت به تمدید آن اقدام گردد.در صورت عدم تمدید ، سرویس گیرنده قادر به حضور درشبکه نخواهد بود. دراین مقاله قصد نداریم به بررسی فرآیند اختصاص IP توسط سرویس دهنده به سرویس گیرنده پرداخته و مراحل چهارگانه (Discver, ffer, Request, Acknwledgement) را تشریح نمائیم ! DHCP ، یکی از استانداردهای پروتکل TCP/IP بوده که باعث کاهش پیچیدگی و عملیات مدیریتی در ارتباط با آدرس های IP سرویس گیرندگان در شبکه می گردد . در این راستا سرویس دهنده DHCP ، بصورت اتوماتیک عملیات اختصاص آدرس های IP و سایر اطلاعات مرتبط با TCP/IP را در اختیار کاربرانی قرار می دهد که امکان DHCP-client آنان فعال شده باشد . بصورت پیش فرض ، کامپیوترهائی که بر روی آنان ویندوز ۲۰۰۰ اجراء می گردد ، سرویس گیرندگان DHCP-Enabled خواهند بود.

چگونگی بدست گرفتن مدیریت کابل

مدیریت کابل به ندرت در راس کارهای واجب مدیر یک شبکه معمولی قرار دارد. بعد از اتمام کارها، اگر همه چیز درست کار کند، دیگر چه کسی اهمیت می دهد که آیا کابل کشی شبکه یک بشقاب ماکارونی به نظر می رسد یا نه، اینطور نیست؟ اشتباه همین جاست. این امر مادامی صحیح است که همه فعالیتها به صورت دلچسبی انجام گیرد و شما بتوانید بدون مدیریت کابل زندگی کنید. وقتی شروع به تغییر بعضی موارد می کنید یا به طور معنی دارتر، وقتی که بعضی کارها غلط از آب در می آیند و احتیاج به شروع ردیابی دارید، بزودی از ناقص بودن تشکیلاتتان افسوس می خورید. در اینجا ۱۰ ترفند وجود دارد که سبب می شود جعبه سیم کشی تان در محل بهتری قرار گیرد. کدرنگ رنگ، کابلهای شما را کد گذاری می کند. چه شما سیمهای کانکتور خورده خودتان را درست کنید یا آنها را به طور آماده از یک فروشنده بخرید، به هر حال به صورت یک تعداد رنگ در دسترس می باشند. اغلب چنین نصب و راه اندازی هایی را، در جایی که از UTP fld-wiring شبیه به هم استفاده می نمایید، به منظور راه اندازی انواع مختلفی از سرویس ها می یابید. مانند: ISDN، تلفن و شبکه، که برای هر کدام رنگهای متفاوتی استفاده می شود و اگر کابلهای شبکه crss-ver دارید، رنگهای مختلف دیگری استفاده می کنید و یا اگر شما مثلا، آبی را برای سر سیمهای LAN، قرمز را برای تلفن، خاکستری را برای ISND و نارنجی پاستیلی را برای Crss-ver شبکه استفاده می کنید متوجه خواهید شد که بیش از این نمی توانید اشتباهی تلفن کسی را بیرون بکشید چون روی کابل اشتباهی عمل کرده اید. طول صحیح اگر شما یک سیم کانکتور خورده به طول یک فوت احتیاج دارید، از یک سیم Patch به طول یک فوت استفاده نمائید نه به طول ۶ فوت.

و عکس این مطلب، شما باید سعی کنید به جای داشتن باری از سیم های نقطه به نقطه فقط در کنار rack سیمهایی که به سمت بالا و پایین می روند داشته باشید، پس یک اتصال مستقیم ایجاد نکنید فقط به خاطر اینکه یک کابل شیک و تر و تمیزتر در دستتان دارید و برایتان زحمتی ندارد که بروید و یک کابل بلندتر تهیه کنید. اتصالات بدون گیر حتی اگر کابلهایتان را به طور منظم در گوشه های rack مرتب کنید، بعضی وقتها مجبورخواهید بود تا سیمها را از دسته سیمها بیرون بکشید. بنابراین سعی کنید همیشه اتصالات بدون گیر snagless بخرید تا بتوانید کابل را از دسته کابلها بدون پاره کردن نوار پلاستیکی بیرون بکشید البته هزینه آن کمی زیاد است، (نواری که آن را وقتی متصل است در پورت نگه می دارد.) در آخر کار از خودتان تشکر خواهید کرد. پورت های برچسب خورده این امر بی معنی به نظر می رسد، ولی همیشه پورت های خود را برچسب بزنید. هیچ چیز رنج آورتر از پیدا کردن سر یک patch در بین ۲۴ سوکت نیست. یعنی همانجایی که فقط یک سر در انتهای هر کدام برچسب خورده است. چون شما برای شمردن پورت ها ساعتها از عمرتان را صرف می کنید و آنها را مجددا وصل می نمائید زیرا آنها را در درگاه اشتباهی جای داده اید. دستگاه های برچسب خورده همچنین باید همه سوئیچها، روترها، مودم ها، سرورها، دسک تاپ ها و نظایر این ها را برچسب بزنید. در نتیجه شما می دانید که کدام کابل ها را به چه دستگاه هایی وصل می کنید. این امر نیز نامفهوم به نظر می رسد مخصوصا اگر شما فقط یک یا دو سرور دارید. این امر مانع شما از انجام یک کار نادرست، مانند جداساختن اشتباه سرور از شبکه LAN می سازد. کابل های برچسب خورده جایی که کابل های طولانی می کشید، در فواصل مکرر و معینی آنها را بر چسب بزنید. در نتیجه می توانید به سرعت آنها را شناسایی کنید بویژه اگر شما فیبر تیره یا سیمهای مسی می کشید که به زودی مورد استفاده قرار نمی گیرند. یک روز ممکن است شما مجبور شوید تا روکش فیبری سر سیمها را تعویض نمائید و اگر انتهای تمام آن کابلهای شبیه به هم به طرز خوبی برچسب خورده باشد، از خودتان تشکر خواهید کرد. تهیه مستندات طرح بندی کابل هایتان را ثبت کرده و بنویسید. بر طبق حالتهای قانون Sd (Sd`s Law States) بعضی چیزها وقتی شما نیستید مختل خواهد شد و اگر بتوانید از پای تلفن به کسی بگوئید که احتیاج به جابجا کردن کابل سبز از پورت ۲۴ به پورت ۹۵ دارید، از اینکه خود را به سختی به محل کار برسانید تا اکثر وظایف بدیهی پشتیبانی را انجام دهید، صرفه جویی خواهید نمود. نرم افزارهای پیگیری دارایی اگر شما شبکه بزرگی دارید، به خرید نرم افزار تخصصی که موجودی IT شما را به همراه زیربنای کابل کشی پیگری می نماید، توجه داشته باشید. مخصوصا برای نصب و راه اندازی های بزرگ، توانایی توجه به یک تاریچه تغییرات و شاید مجموعه ای از وقایع می تواند مفید باشد. آزمایش کننده کابل یک آزمایش کننده مابل بخرید و هر زمان که نصب یا جابجایی و حذف کابلی را انجام می دهید یک آزمایش سریع روی آن انجام دهید. سیمهای patch در حالتهای خاصی در کشوهای میز گیر می کنند و یا زیر صندلی های چرخ دار له می شوند و یا ضربه شدیدی می خورند، پس یک آزمایش ۵ ثانیه ای در هر زمان که تغییری ایجاد می کنید ممکن است به شما کمک کند تا یک سیم معیوب را شناسایی کنید و از یک حادثه بد در شرف وقوع جلوگیری نمائید. همیشه غیر از شما، حداقل یک نفر دیگر هم وجود دارد که به امور شبکه توجه داشته باشد، هر شخصی باید در محدوده خط مشی مدیریت کابل خود عمل نماید. دقیقا یک وصله غیر هماهنگ، تصادفی و بدون سند همه چیز را به طور کامل بیهوده و بی معنی ارائه می دهد.

دیواره های آتش (Firewall) چیستند؟

دیواره آتشین (Fire wall) سیستمی است بین کاربران یک شبکه محلی و یک شبکه بیرونی (مثل اینترنت) که ضمن نظارت بر دسترسی ها، در تمام سطوح، ورود و خروج اطلاعات را تحت نظر دارد. بر خلاف تصور عموم کاربری این نرم افزارها صرفاً در جهت فیلترینگ سایت ها نیست. برای آشنایی بیشتر با نرم افزارهای دیواره های آتشین، آشنایی با طرز کار آنها شاید مفیدترین راه

باشد. در وهله اول و به طور مختصر می توان گفت بسته های TCP/IP قبل و پس از ورود به شبکه وارد دیواره آتش می شوند و منتظر می مانند تا طبق معیارهای امنیتی خاصی پردازش شوند. حاصل این پردازش احتمال وقوع سه حالت است- ?: اجازه عبور بسته صادر می شود- ?. بسته حذف می شود- ?.بسته حذف می شود و پیام مناسبی به مبدا ارسال بسته فرستاده می شود •. ساختار و عملکرد با این توضیح، دیواره آتش محلی است برای ایست بازرسی بسته های اطلاعاتی به گونه ای که بسته ها براساس تابعی از قواعد امنیتی و حفاظتی پردازش شده و برای آنها مجوز عبور یا عدم عبور صادر شود. همانطور که همه جا ایست بازرسی اعصاب خردکن و وقت گیر است دیواره آتش نیز می تواند به عنوان یک گلوگاه باعث بالا رفتن ترافیک، تاخیر، ازدحام و بن بست شود. از آنجا که معماری TCP/IP به صورت لایه لایه است (شامل ? لایه: فیزیکی، شبکه، انتقال و کاربردی) و هر بسته برای ارسال یا دریافت باید از هر ? لایه عبور کند بنابراین برای حفاظت باید فیلدهای مربوطه در هر لایه مورد بررسی قرار گیرند. بیشترین اهمیت در لایه های شبکه، انتقال و کاربرد است چون فیلد مربوط به لایه فیزیکی منحصر به فرد نیست و در طول مسیر عوض می شود. پس به یک دیواره آتش چند لایه نیاز داریم. سیاست امنیتی یک شبکه مجموعه ای از قواعد حفاظتی است که بنابر ماهیت شبکه در یکی از سه لایه دیواره آتش تعریف می شوند. کارهایی که در هر لایه از دیواره آتش انجام می شود عبارت است از- ?: تعیین بسته های ممنوع (سیاه) و حذف آنها یا ارسال آنها به سیستم های مخصوص ردیابی (لایه اول دیواره آتش- ?) بستن برخی از پورت ها متعلق به برخی سرویس ها مثل FTP، Telnet و... (لایه دوم دیواره آتش- ?) تحلیل برآیند متن یک صفحه وب یا نامه الکترونیکی یا .... (لایه سوم دیواره آتش •••) در لایه اول فیلدهای سرآیند بسته IP مورد تحلیل قرار می گیرد: آدرس مبدأ: برخی از ماشین های داخل یا خارج شبکه حق ارسال بسته را ندارند، بنابراین بسته های آنها به محض ورود به دیواره آتش حذف می شود. آدرس مقصد: برخی از ماشین های داخل یا خارج شبکه حق دریافت بسته را ندارند، بنابراین بسته های آنها به محض ورود به دیواره آتش حذف می شود. IP آدرس های غیرمجاز و مجاز برای ارسال و دریافت توسط مدیر مشخص می شود. شماره شناسایی یک دیتا گرام تکه تکه شده: بسته هایی که تکه تکه شده اند یا متعلق به یک دیتا گرام خاص هستند حذف می شوند. زمان حیات بسته: بسته هایی که بیش از تعداد مشخصی مسیریاب را طی کرده اند حذف می شوند. بقیه فیلدها: براساس صلاحدید مدیر دیواره آتش قابل بررسی اند. بهترین خصوصیت لایه اول سادگی و سرعت آن است چرا که در این لایه بسته ها به صورت مستقل از هم بررسی می شوند و نیازی به بررسی لایه های قبلی و بعدی نیست. به همین دلیل امروزه مسیریاب هایی با قابلیت انجام وظایف لایه اول دیواره آتش عرضه شده اند که با دریافت بسته آنها را غربال کرده و به بسته های غیرمجاز اجازه عبور نمی دهند. با توجه به سرعت این لایه هر چه قوانین سختگیرانه تری برای عبور بسته ها از این لایه وضع شود بسته های مشکوک بیشتری حذف می شوند و حجم پردازش کمتری به لایه های بالاتر اعمال می شود. در لایه دوم فیلدهای سرآیند لایه انتقال بررسی می شوند: شماره پورت پروسه مبدأ و مقصد: با توجه به این مسئله که شماره پورت های استاندارد شناخته شده اند ممکن است مدیر دیواره آتش بخواهد مثلاً سرویس FTP فقط برای کاربران داخل شبکه وجود داشته باشد بنابراین دیواره آتش بسته های TCP با شماره پورت ?? و ?? که قصد ورود یا خروج از شبکه را داشته باشند حذف می کند و یا پورت ?? که مخصوص Telnet است اغلب بسته است. یعنی بسته هایی که پورت مقصدشان ?? است حذف می شوند. کدهای کنترلی: دیواره آتش با بررسی این کدها به ماهیت بسته پی می برد و سیاست های لازم برای حفاظت را اعمال می کند. مثلاً ممکن است دیواره آتش طوری تنظیم شده باشد که بسته های ورودی با SYN=۱ را حذف کند. بنابراین هیچ ارتباط TCP از بیرون با شبکه برقرار نمی شود. فیلد شماره ترتیب و Acknwledgement: بنابر قواعد تعریف شده توسط مدیر شبکه قابل بررسی اند. در این لایه دیواره آتش با بررسی تقاضای ارتباط با لایه TCP، تقاضاهای غیرمجاز را حذف می کند. در این مرحله دیواره آتش نیاز به جدولی از شماره پورت های غیرمجاز دارد. هر چه قوانین سخت گیرانه تری برای عبور بسته ها از این لایه وضع شود و پورت های بیشتری بسته شوند بسته های مشکوک

بیشتری حذف می شونـد و حجم پردازش کمتری به لایه سوم اعمال می شود. در لایه سوم حفاظت براساس نوع سرویس و برنامه کاربردی صورت می گیرد: در این لایه برای هر برنامه کاربردی یک سری پردازش های مجزا صورت می گیرد. بنابراین در این مرحله حجم پردازش ها زیاد است. مثلاً فرض کنید برخی از اطلاعات پست الکترونیکی شما محرمانه است و شما نگران فاش شدن آنها هستید. در اینجا دیواره آتش به کمک شما می آید و برخی آدرس های الکترونیکی مشکوک را بلوکه می کند، در متون نامه ها به دنبال برخی کلمات حساس می گردد و متون رمزگذاری شده ای که نتواند ترجمه کند را حذف می کند. یا می خواهید صفحاتی که در آنها کلمات کلیدی ناخوشایند شما هست را حذف کند و اجازه دریافت این صفحات به شما یا شبکه شما را ندهد.

•انواع دیواره های آتش دیواره های آتش هوشمند: امروزه حملات هکرها تکنیکی و هوشمند شده است به نحوی که با دیواره های آتش و فیلترهای معمولی که مشخصاتشان برای همه روشن است نمی توان با آنها مقابله کرد. بنابراین باید با استفاده از دیواره های آتش و فیلترهای هوشمند با آنها مواجه شد. از آنجا که دیواره های آتش با استفاده از حذف بسته ها و بستن پورت های حساس از شبکه محافظت می کنند و چون دیواره های آتش بخشی از ترافیک بسته ها را به داخل شبکه هدایت می کنند، (چرا که در غیر این صورت ارتباط ما با دنیای خارج از شبکه قطع می شود)، بنابراین هکرها می توانند با استفاده از بسته های مصنوعی مجاز و شناسایی پورت های باز به شبکه حمله کنند. بر همین اساس هکرها ابتدا بسته هایی ظاهراً مجاز را به سمت شبکه ارسال می کنند. یک فیلتر معمولی اجازه عبور بسته را می دهد و کامپیوتر هدف نیز چون انتظار دریافت این بسته را نداشته به آن پاسخ لازم را می دهد. بنابراین هکر نیز بدین وسیله از باز بودن پورت مورد نظر و فعال بودن کامپیوتر هدف اطمینان حاصل می کند. برای جلوگیری از آن نوع نفوذها دیواره آتش باید به آن بسته هایی اجازه عبور دهد که با درخواست قبلی ارسال شده اند. حال با داشتن دیواره آتشی که بتواند ترافیک خروجی شبکه را برای چند ثانیه در حافظه خود حفظ کرده و آن را موقع ورود و خروج بسته مورد پردازش قرار دهد می توانیم از دریافت بسته های بدون درخواست جلوگیری کنیم. مشکل این فیلترها زمان پردازش و حافظه بالایی است که نیاز دارند. اما در عوض ضریب اطمینان امنیت شبکه را افزایش می دهند. دیواره های آتش مبتنی بر پروکسی: دیواره های آتش هوشمند فقط نقش ایست بازرسی را ایفا می کنند و با ایجاد ارتباط بین کامپیوترهای داخل و خارج شبکه کاری از پیش نمی برد. اما دیواره های آتش مبتنی بر پروکسی پس از ایجاد ارتباط فعالیت خود را آغاز می کند. در این هنگام دیواره های آتش مبتنی بر پروکسی مانند یک واسطه عمل می کند، به نحوی که ارتباط بین طرفین به صورت غیرمستقیم صورت می گیرد. این دیواره های آتش در لایه سوم دیواره آتش عمل می کنند، بنابراین می توانند بر داده های ارسالی در لایه کاربرد نیز نظارت داشته باشند. دیواره های آتش مبتنی بر پروکسی باعث ایجاد دو ارتباط می شود - ?: ارتباط بین مبدا و پروکسی - ? ارتباط بین پروکسی و مقصد حال اگر هکر بخواهد ماشین هدف در داخل شبکه را مورد ارزیابی قرار دهد در حقیقت پروکسی را مورد ارزیابی قرار داده است و نمی تواند از داخل شبکه اطلاعات مهمی به دست آورد. دیواره های آتش مبتنی بر پروکسی به حافظه بالا و CPU بسیار سریع نیاز دارند و از آنجایی که دیواره های آتش مبتنی بر پروکسی باید تمام نشست ها را مدیریت کنند گلوگاه شبکه محسوب می شوند. پس هرگونه اشکال در آنها باعث ایجاد اختلال در شبکه می شود. اما بهترین پیشنهاد برای شبکه های کامپیوتری استفاده همزمان از هر دو نوع دیواره آتش است. با استفاده از پروکسی به تنهایی بارترافیکی زیادی بر پروکسی وارد می شود. با استفاده از دیواره های هوشمند نیز همانگونه که قبلاً تشریح شد به تنهایی باعث ایجاد دیواره نامطمئن خواهد شد. اما با استفاده از هر دو نوع دیواره آتش به صورت همزمان هم بار ترافیکی پروکسی با حذف بسته های مشکوک توسط دیواره آتش هوشمند کاهش پیدا می کند و هم با ایجاد ارتباط واسط توسط پروکسی از خطرات احتمالی پس از ایجاد ارتباط جلوگیری می شود.

کاربرد پورت های شبکه

پورت ۱۳: نام دیگر اون daytime است و کارش هم اینه که زمان و تاریخ رو در اون کامپیوتر به ما می‌ده. این پورت اصولا خیلی سر راسته. فقط کافیه که بهش وصل شیم تا اطلاعاتشون بیرون بریزه. البته این پورت رو خیلی از کامپیوترها بسته است. (یادتون باشه که وقتی می‌توان با یه پورت کار کرد که باز باشد). حالا- می‌خوایم با پورت ?? از ip شماره ۱۹۴.۲۲۵.۱۸۴.۱۳ صحبت کنم. یکی از این دو دستور را می‌نویسم: ۱۳ ۱۹۴.۲۲۵.۱۸۴.۱۳ telnet البته در آن دستورات به جای عدد ?? می‌توان معادلش را نوشت که daytime است. و جواب می‌شنوم: ۱۱:۳۵:۳۳ ۱۰/۵/۲۰۰۲ AM بله، با این پورت ارتباط برقرار کردیم و اطلاعاتش رو دریافت کردیم. این اطلاعات معمولا به درد این می‌خورد که مکان جغرافیایی اون کامپیوتر را حدس بزنیم (البته اگر زمان اون کامپیوتر صحیح باشد). به عنوان مثال این کامپیوتر خاص در ایران است چون ساعتش همزمان با ایران است. پورت ۲۵: برای ارسال E-mail به‌کار می‌رود. این پورت از پروتکل SMTP برای این کار استفاده می‌کند. نکته مهم آن است که این پروتکل توانایی خواندن E-mail را ندارد و فقط می‌تواند E-mail بفرستد. حالا سوالی که پیش می‌آید که چه برنامه‌هایی روی سرور پورت ?? را باز می‌کند؟ همان‌طور که گفتم، SMTP فقط یک پروتکل است (نه یک برنامه) و از نظر لغوی مخفف عبارت Simple Mail Transfer Prtcl است. برنامه‌ای که پورت ?? را باز می‌کند تا بتوان از طریق آن E-mail ارسال کنیم، SMTP Server می‌گویند. SMTP Server یک عبارت کلی است، برای این نوع برنامه‌ها. حالا- خود SMTP Server انواع مختلف دارد که مشهورترین‌هایشان، ESMTP MAIL Service، SendMail، SMail و ... هستند. نکته مهم این است که تفاوت زیادی نیست که سرور مورد نظر ما از کدامیک از این نرم‌افزارها استفاده می‌کند، زیرا اصول کار با آنها یکی است. برای صحبت کردن با پورت ?? اول باید یک Server پیدا کنیم که پورت ?? در آن باز باشد (اگرچه در اکثر سرورها پورت ?? باز است). بعد باید طبق معمول از telnet یا nc برای ارتباط استفاده کنیم ۲۱:این پورت برای فایل های به اشتراک گذاشته شدست شما توسط این پورت میتونید به فایل های به اشتراک گذاشته شده به صورت زیر دسترسی پیدا کنید ftp:// شما باید به جای x ای پی را وارد کنید البته اگه ویندوز زیر ۲۰۰۰ باشه کامپیوتر دیگه تو دست شماست البته شما سعی کنید هیچ وقت فایلی رو در ویندوز زیرxp به اشتراک نزارید(share) پورت ۸۰ پورت ?? یکی از مهم‌ترین پورت‌هاست. دنیای وب (صفحات اینترنتی) بر اساس همین پورت کار می‌کنه. توضیح اینکه وقتی به یه سایت وصل می‌شیم و صفحه وب را درخواست می‌کنیم، در واقع مرورگر اینترنتی به پورت ?? اون کامپیوتر وصل می‌شه و اطلاعات رو می‌گیره (البته بعد از گرفتن اطلاعات اون رو تفسیر می‌کنه و به صورت یه صفحه نشون می‌ده – دقت کنید که اطلاعات در واقع به صورت یک سری تگ HTML است). حالا ما می‌خواهیم با پورت ?? یک کامپیوتر صحبت کنیم ولی به کمک telnet و nc. اول باید یه cnnectin (اتصال) با پورت ?? برقرار کنیم (مثلا برای سایت htmail.cm باید بنویسم): nc –v http://www.htmail.cm ۸۰ telnet http://www.htmail.cm ۸۰ پس اول باید یکی از دستورات بالا را استفاده کنیم. من همیشه توصیه‌ام استفاده از nc بوده و خواهد بود. حالا باید شروع به صحبت با پورت ?? کنیم. من فعلا- دو تا جمله براتون می‌گم و بقیه‌اش بمونه واسه بعد. دقت کنید که موقع کار با پورت ?? با تلنت (نه nc) دستوراتی که ما می‌نویسیم، نمایش داده نمی‌شود ولی کار می‌کنه- ?. اولین جمله اینه: GET / HTTP/۱.۰ و بعدش دوتا Enter به فاصله‌ها دقت کنید. دو طرف / ی که بعد از GET است، فاصله وجود دارد. این جمله به پورت ?? می‌گه که هرچی در header داره، نشون بده. و جواب می‌شنوم: -HTTP/۱.۰ ۳۰۲ Mved Temprarily Server: Micrsft-IIS/۵.۰ Date: Thu, ۰۵ Dec ۲۰۰۲ ۱۲:۰۲:۵۱ GMT Lcatin: http://lc۲.law۵.htmail.passprt.cm/cgi-bin/lgin X-Cache: MISS frm cache۵.neda.net.ir Cnnectin: clse- ? دومین جمله اینه: / GET what/ever و بعدش دوتا Enter به فاصله‌ها دقت کنید. این دستور باعث میشه که هر چی داره، رو کنه. البته توجه کنید که ما

مسیر را مشخص نکردیم. بعدها در مورد این مسیر مشخص کردن صحبت خواهم کرد. این حالت که بدون مسیر است خیلی وقت‌ها کار نمی‌کنه (مثل همین مثال !!) گاهی پیش می‌آد که یک سری دستورات خاص را همیشه باید پشت سرهم به یه پورت خاص بفرستیم و بخواهیم در وقت صرفه‌جویی کنیم. مثلا همین جمله GET / HTTP/۱.۰ و دو Enter پشت سرهم که همیشه استفاده می‌کنیم. در این موارد می‌توان این دستورات را در یک فایل تایپ کرد (همراه با Enter ها که باید موقع نوشتن حتما بزنید) و بعد مثلاـ با نام yah.txt ذخیره کنید و بعد یکی از دستورات زیر را بنویسیم: yah.txt>nc-v http://www.yah.cm ۸۰ http://iritn.cm/index.php?actin=shw&type=news&id=۴۸۲۳ آموزش کامپیوتر :: آموزش اکسل :: آموزش Excel – بخش دوم

در ادامه سعی در بررسی کاستی‌های مجموعه خواهیم نمود

۱)عدم نصب صحیح سیستم عامل‌های اصلی شبکه

یکی از اصلی‌ترین دلائل بروز حمله به سایت‌های اینترنتی حفره‌های موجود در نرم‌افزارهای سیستم عامل به جهت عدم نصب اصولی و تکنیکی آنها می‌باشد. در حقیقت عدم شناخت و آگاهی کافی برخی از مسئولین سایت ها از امکانات، محاسن و معایب و حفره‌های موجود در سیستم عامل مورد استفاده موجب می شود مبحث انجام تنظیمات صحیح به دقت و درستی انجام نشده و به سادگی، زمینه جهت ورود غیر مجاز مهاجم مهیا شود. بسته نبودن Prt های موجود در مجموعه سرویسهای یک Server به لحاظ امنیتی بسیار خطرناک می باشد که در بسیاری از موارد به جهت عدم دقت مسئولین مربوطه، مسیر هموار جهت ورود مهاجمین «Hackers» بوجود می‌آورد.

۲)وجود کاستی‌های فراوان در ساختار سیستم عامل‌ها

متأسفانه علیرغم پیشرفت‌های شگرف دنیای سیستم عامل‌ها، متأسفانه علاوه بر مشکل عدم آگاهی نسبی برخی از متخصصین شبکه، وجود مشکلات بنیادی در بدنه نرم افزارهای Server نیز عامل ضعف دیگری برای آنها به شمار می‌رود. در حقیقت بسیاری از سیستم عامل های Server دارای نقایص فراوانی به لحاظ حفظ امنیت می‌باشند که بدیهی است با گذشت زمان نقاط ضعفشان شناسایی و رفع می گردد.

۳)اجازه استفاده از سرویس‌های گوناگون در Server

اجازه استفاده از سرویس‌های گوناگونی همچون TelNet , FTP , IRC , HTTP و ... زمینه‌ساز هجوم‌های غیر مجاز فراوان در سرورها می‌باشد. در حقیقت هر یک از درگاههای ورودی مذکور (prts) ، مسیری هموار جهت نفوذهای غیرمجاز به داخل سرورها می‌باشد که می‌بایست با توجه به شرایط مورد نیاز کاربران در آنها محدودیت‌های لازم اعمال گردد و یا در صورت عدم توجیه امنیتی مناسب برای حضور هر یک، از آنها صرف نظر شود.

۴)وجود مشکلات امنیتی در پروتکل‌ها

اتصال شبکه‌ها در اینترنت معمولاً با استفاده از پروتکل TCP/IP انجام می‌پذیرد. در همین راستا اجازه استفاده از امکانات HTTP بر روی TCP/IP با توجه به گستردگی سرویس‌های آن مورد توجه قرار گرفته است و لذا وجود حفره‌های فراوان و بسترسازی

مناسب برای مهاجمین در این پروتکل مشهور، موجبات پدید آمدن اختلالات امنیتی فراوان در شبکه می گردد.

۵)عدم رعایت تدابیر امنیتی در نرم‌افزارهای نصب شده بر روی سرور

معمولاً سرویس دهندگان وب جهت سهولت دسترسی و یا انجام امور کاربران و مشتریان خود اقدام به نصب نرم‌افزارهای کاربردی بر روی سیستم خود می‌نمایند که غالباً فاقد تدابیر ملزوم امنیتی می‌باشند. لذا بررسی و پیش‌بینی اقدامات تأمین در نصب و استفاده از این نوع برنامه‌ها بسیار پراهمیت به نظر می‌رسد. بطور مثال برنامه های تهیه شده بصورت ASP نمونه‌ای از این موارد می‌باشد.

۶)عدم استفاده از گزارش فعالیت‌های سیستم و یا کنترل عملکرد کاربران

یکی از مسائلی که باید مورد توجه سرویس دهندگان وب قرار گیرد، نصب و راه‌اندازی نرم‌افزارهای Capture و یا ذخیره کننده Lg بر روی سرور می‌باشد. حضور این نوع از قابلیت‌ها بر روی سرور موجب می‌شود تا حرکات مشکوک و خزنده و در عین حال دور از فعالیت‌های معمول روزانه، ثبت و مورد بررسی قرار گیرد. براساس شواهد موجود، مهاجمین قبل از انجام مأموریت اصلی خود، به بررسی وضعیت سرورها پرداخته و جنبه‌های مختلف و امکانات آنها را مورد بررسی قرار می‌دهند. این نوع حرکات در فایلهای Lg ثبت می‌شود و با کنترل و بررسی آنها می‌توان اقدامات امنیتی و باز دارنده مناسب قبل از حمله اصلی را اعمال نمود. متأسفانه با توجه به کثرت مشتریان و کاربران وب، کنترل گزارشهای سیستم برای مسئولین شبکه امری بس مشکل و خسته کننده به نظر آمده و نهایتاً احتمال بروز مشکلات مذکور را افزایش می‌دهد.

۷)اعتماد به عملکرد مشتری

یکی دیگر از کاستی‌های سرویس دهندگان در ارائه سرویس‌های آنلاین اعتماد به عملکرد قانونی و صحیح کاربران می‌باشد. در حقیقت همین ذهنیت موجب عدم کنترل کاربران خواهد بود. البته زمینه این مشکل مشابه مورد ششم این مبحث است اما در اینجا تراکم عملیات‌های انجام شده و درصد محدود بروز خطر برای سرویس دهندگان موجب عدم کنترل عملکرد و تراکنش‌های اقتصادی کاربر می گردد. لذا هیچگاه نباید به عملکرد کاربران یک سایت اعتماد کامل داشت.

۸)عدم وجود روشهای مناسب شناسایی کاربر

یکی دیگر از نقاط ضعف سرویس دهندگان، عدم استفاده از روشهای مناسب شناسایی کاربران مجاز به استفاده از امکانات سیستم می‌باشد. امروزه شاید عمده‌ترین روش شناسایی کاربرنام شناسایی «User name» و کلمه عبور «Passwrd» او باشد، که براساس آمار یکی از مهمترین راههای سوءاستفاده از سایت‌ها به دست آوردن و استفاده از مورد ذکر شده می‌باشد. در حقیقت نرم‌افزارهائی که به همین جهت (به دست آوردن و یا حدس زدن کلمه عبور) تهیه شده‌اند، به سادگی می‌توانند احتمالات گوناگون کلمات عبور را در زمان بسیار کوتاهی بر روی سرورها بررسی نموده و مقصود را به سرعت بیابند. در این راستا پیش‌بینی امکانات لازم جهت ایجاد کلمات عبور پیچیده بر روی سرورها از تدابیری است که می‌تواند احتمال بروز اختلال از این طریق را به حداقل برساند. در حقیقت کاربران ملزم به استفاده از کلمات عبوری باشند که به لحاظ ساختاری نتوان به سادگی به آنها دست یافت. البته در محافل و انجمن‌های علمی امنیت کامپیوتر و شبکه‌ها ، در این زمینه استانداردهایی تعیین شده است که هم اکنون در سایتهای مشهور مورد استفاده قرار می گیرند که خود موجب کاهش یورشهای احتمالی می گردد.

۹)عدم استفاده از تدابیر امنیتی مناسب و نرم‌افزارهای Firewall و Prxy

با توجه به موار ذکر شده در مباحث نقاط ضعف سیستم‌های عامل و پروتوکل‌ها، وجود و استفاده از شیوه‌های نرم‌افزاری بازدارنده بسیار مورد توجه قرار گرفته است. ایجاد و تهیه نرم‌افزارهایی که با لفظ دیواره آتش Firewall شناخته می‌شوند و نهایتاً نصب و استفاده از آنها بر روی سرور و یا در مسیر حرکت اطلاعات موجب کاهش احتمال یورش و نفوذ به حفره‌های موجود می گردد. در حقیقت این نوع نرم‌افزارها بصورت یک سد محکم و یا یک فیلتر در مسیر کاربران واقع می گردد و بطور دقیق نحوه عملکرد و مسیر حرکت کاربران و نحوه نقل و انتقالات اطلاعات را کنترل می‌نمایند. بدیهی است با توجه به پیشرفت تکنیک‌های یورش در بعضی مواقع شاهد پشت سر گذاشتن Firewall ها نیز می‌باشیم و همین موارد موجب می گردد تا شرکت‌های نرم‌افزاری در کوتاهترین زمان ممکن در به روز رسانی و رفع نواقص Firewall های خود اقدام نمایند و آنها را در مقابل تهدیدها آماده سازند.

۱۰)عدم شناخت کافی از صحت اطلاعات دریافتی (عدم کنترل اطلاعات)

یکی دیگر از نقاط ضعف موجود در سرویس دهندگان، عدم کنترل اطلاعات دریافتی و ارسالی از سوی کاربران می‌باشد. در حقیقت شیوه‌ای مرسوم که توسط مهاجمان مورد استفاده قرار می گیرد، ارسال Script و یا برنامه‌های پس از نفوذ بر روی سرورها می‌باشد که پس از دریافت‌های مذکور، مهاجم به سهولت قابلیت تخریب، تغییر و نهایتاً ایجاد اختلال در سایت را خواهد داشت. نصب ویروس‌یاب و Firewall های مناسب از این نوع تهدیدها جلوگیری می‌نماید.

۱۱)عدم محافظت از اطلاعات حساس

عدم محافظت از اطلاعات حساس

بسیاری از سرویس دهندگان جهت حفظ اطلاعات حساس خود اقدام به مخفی‌سازی encryptin می‌نمایند. البته شکل ساده و تئوریکال قضیه، دور از دسترس قرار دادن اطلاعات است ولیکن روشهای گوناگون جهت انجام این مهم مورد استفاده قرار می گیرد که با توجه به اهمیت آن در آینده به آن پرداخته خواهد شد. عناوین یازده گانه مطروحه، حاکی از اهم نقطه ضعف‌های موجود در سرویس دهندگان وب بوده و سعی در بررسی حفره‌های عمومی موجود در سایت‌های وب داشت ولیکن طرح این سئوال که: " چرا دیگران علاقمند به نفوذ و خرابکاری در سایت مطلوب ما هستند؟" بتواند در شناخت عوامل گوناگون و مطرح برای مهاجمین یاری رسان باشد.در نهایت همواره باید به خاطر داشت: " ایمنی مطلوب امروز، همواره بهتر از ایمنی کامل فرداست" بررسی های آماری حاکی از آن است که تهدیدهای عمومی سیستم های سرویس دهنده اینترنتی به شرح ذیل می باشد :

کپی‌برداری غیرمجاز و یا سرقت اطلاعات

در این مورد، معمولا مهاجمان سعی در کپی‌برداری و یا سرقت از اطلاعاتی می‌نمایند که دارای طبقه‌بندی اطلاعاتی است. با عنایت به اینکه غالب مراکز استراتژیک و سازمانهای گسترده اقدام به مکانیزه نمودن فرآیند نگهداری از اسناد و مدارک و انجام امور اداری روزانه خود نموده‌اند (همچون وزارتخانه‌ها، سازمانهای اقتصادی، مراکز نظامی و یا اطلاعاتی و ...) لذا معمولا- با ایجاد لایههای دسترسی گوناگون امکان استفاده از بانک‌های اطلاعاتی را برای مدیران و یا افراد مجاز مهیا نموده‌اند، لذا خطر حضور و نفوذ مهاجمان و در پی آن خطر سرقت اطلاعات و کپی‌برداری از آنها همواره نگران کننده خواهد بود و از عمده مشکلات امنیتی شبکه‌های وب می‌باشد. در حقیقت مهاجمین با استفاده از دسترسی کاربران مجاز و با دسترسی به کدهای ایشان، به اطلاعات

طبقه‌بندی شده و با ارزش دست یافته و بدینوسیله اقدام به سرقت اطلاعات می‌نمایند.

ایجاد تغییر و دستکاری در اطلاعات

این مورد در برخی از سیستم‌های مالی و اقتصادی، و نیز در پایگاه های اطلاعاتی رسمی دیده شده است. نفوذ و دستکاری اطلاعات موجود بر روی شبکه‌های بانکی با در نظر گرفتن گستره فعالیت این نوع از شبکه‌ها، منافع اقتصادی مطلوبی را برای مهاجمان به دنبال داشته است. دستکاری بانک‌های اطلاعاتی ادارات پلیس و یا مراکز امنیتی در این راستا بسیار زیانبار جلوه می‌نموده است. دستکاری در اخبار و تغییر اطلاعات سایتهای خبرگزاری‌ها و یا جعل اخبار و نهایتا شایعه پراکنی از دیگر معضلات این مبحث از امنیت شبکه می‌باشد.

منتشر کردن اطلاعات

انتشار اطلاعات طبقه‌بندی شده دولتی، شخصی، اقتصادی و... توسط مهاجمان از دیگر نگرانی‌های ویژه اداره کنندگان سیستم‌های اطلاعاتی است. معمولا این تهدیدها بر روی سایتهائی دیده می‌شوند که در آنها اطلاعات طبقه‌بندی شده سیاسی، علمی و اقتصادی و ... نگهداری می‌شوند. همچون پایگاه اطلاعات مراکز ملی تحقیقات فضایی و یا بانک‌های اطلاعاتی مربوط به سوابق امنیتی و موارد استراتژیک هر کشور.

تغییر در ساختار ظاهری پایگاه

در بسیاری از مواقع دیده شده است، محتوای ظاهری سایتهای اینترنتی که در معرض بینندگان عام قرارداد بصورت ناگهانی و بدون آگاهی مدیران آن سایت تغییر نموده است. بدین ترتیب که مهاجمان صفحات اصلی ایستگاه را با صفحات دیگری جابه‌جا نموده و عملا استفاده از محتوای اصلی سایت را برای کاربران عمومی غیرممکن می‌سازند. در برخی موارد هم شاهد Redirect نمودن و یا جابه‌جائی خودکار کاربر از سایت مذکور به سایتهای دیگر می‌باشیم.

تخریب پایگاههای اطلاعاتی

در مواقعی دیده شده است مهاجمان پس از نفوذ به سیستم باعث انهدام بانک‌های اطلاعاتی موجود در آن گردیده و خسارات جبران ناپذیری را به سازمانهای مربوط وارد می‌آورند. در بسیاری از موارد دیده شده است. جبران خسارت وارده بسیار مشکل و حتی غیر ممکن می‌نماید. مراکزی همچون سازمانهای ثبت احوال و اسناد، ادارات پلیس و یا سازمانهائی که دارای آرشیوهای رایانه‌ای و الکترونیکی می‌باشند مورد علاقه شدید مهاجمان واقع میگردند.

ارسال و انتشار ویروس

در این زمینه نیز، مهاجمان و مخربین با ارسال نامه‌های الکترونیکی و یا فایلهای آلوده به ویروس ها خطرناک و یا موجبات بوجود آمدن مشکلات عدیده برای سرویس دهندگان اطلاعاتی و یا استفاده کنندگان از پایگاه مذکور می گردند . امروزه شاید ساده ترین روش انتشار ویروس و ارسال همگانی آن جهت تخریب ،همین مورد باشد .

ایجاد دسترسی، تعریف کاربران جدید وتخریب نامحسوس

در بسیاری از شبکه‌هایی که در آنها با وفور کاربران مواجه هستیم و کنترل فردفرد افراد برای مسئولین پایگاه قابل انجام نمی‌باشد (همچون سرویس دهندگان Free-Email و یا ارائه کنندگان خدمات اینترنت ISP) همواره خطر نفوذ و ایجاد سطوح دسترسی جدید و یا کاربران مجازی وجود دارد. بدیهی است در این شکل از خرابکاری‌های شبکه‌ای، مخربین قادر خواهند بود بصورت نامحسوس کلیه تراکنش‌ها و فرآیندهای گوناگون موجود در سایت را مورد بازبینی قرار داده و از آن سوءاستفاده نمایند که این عملیات با دسترسی به کد عبور مدیران شبکه به راحتی قابل انجام است. این فرآیند برای اداره کنندگان پایگاه‌های اطلاعاتی، مشکلات عمده‌ای را با توجه به مسئولیت قانونی ایشان در قبال پایگاه مربوطه به دنبال خواهد داشت.

تهدیدهای مربوط به سایتهای فعال در امور مالی و اقتصادی

در خصوص مسائل امنیتی قابل ذکر است بعضی از ایستگاههای اینترنتی با در نظر گرفتن نوع فعالیت از تهدیدهای ویژه برخوردارند . بطور مثال از تهدیدهای مربوط به سیستم ها ی اقتصادی آنلاین می توان به موارد ذیل اشاره نمود : ورود و نفوذ به سیستمهای بانکی و برداشت‌های غیرمجاز مالی از حسابهای پرتراکنش لازم به ذکر است مهاجمین با در نظر گرفتن شرایط پیچیده حسابهای پر تراکنش پس از نفوذ اقدام به تخلیه حساب و یا جابه‌جائی پول می‌نمایند.

انجام معاملات صوری و غیرواقعی بصورت الکترونیکی جهت کسب اعتبار

معمولاـ اعتبارات بانکی به حسابهائی تعلق می گیرد که دارای گردش بالای کلان می‌باشند و اساسا با در نظر گرفتن اینکه گردش‌های مالی مناسب با انجام معاملات و تنظیم قراردادهای مطلوب با ارقام بالا بوجود می‌آید، لذا با استفاده از سیستم عقد قراردادهای الکترونیکی و ایجاد پرونده‌های مالی غیرواقعی در بانک اطلاعاتی بانکهای بزرگ، مطلوب سوء استفاده گران تامین می گردد.

گشایش حسابهای بانکی غیرواقعی و انجام تراکنش‌های غیرحقیقی

نفوذگران در این زمینه سعی در ایجاد حسابهای جاری و یا ارزی غیر واقعی می نمایند و در آنها همچون بند ۲ سعی در ایجاد تراکنشهای مالی و نقل و انتقالات پول می نمایند . بدیهی است با در نظر گرفتن غیر واقعی بودن حسابها، پیگیری وضعیت صاحب حساب و یا کنترل آن و فرایند اقتصادی قابل انجام نبوده و براحتی از آن سوء استفاده به عمل می آید .

تغییر در اسناد مالی و بانکی و جعل

در این مورد، مهاجمین با نفوذ به سیستم‌های مالی سعی در ایجاد تغییر در حسابها نموده و معمولا مدارک مهم را مورد تهاجم قرار می‌دهند. بدیهی است در این شکل از تخریب نیز منافع مالی سرشاری برای نفوذگران تامین میگردد.

سوءاستفاده از کارتهای اعتباری و انجام خرید و فروش‌های مجازی

همانطور که میدانیم استفاده از کارتهای اعتباری رایج، در جوامع مدرن بعنوان راه‌حلی مناسب جهت انجام فعالیت‌های اقتصادی کوچک و بزرگ بصورت همگانی مورد توجه و استفاده قرار می گیرد. بدیهی است در این مورد نیز مهاجمین با جعل و یا تولید شماره کارتهای اعتباری توسط نرم‌افزارهای مربوطه سعی در استفاده از حسابهای دیگران در خرید و انجام معاملات الکترونیکی می‌نمایند. که این مبحث را در آینده با توجه به اهمیت آن بیشتر مورد بررسی قرار خواهیم داد.

ارسال فرم سفارش کالا و یا رزرواسیون الکترونیکی بصورت غیرحقیقی

در بسیاری از سایتهای اینترنتی مربوط به فعالیتهای فرهنگی همچون سینماها و سالنهای تئاتر و یا آژانس‌های مسافرتی شاهد استفاده از امکان رزرواسیون بلیت هستیم. استفاده از این امکان همواره با مشکلاتی همچون رزرواسیون غیرحقیقی، خرید عمده بلیت بصورت غیرواقعی و ایجاد اختلال در عملکرد روزانه مراکز مذکور مواجه بوده است. البته مشکلاتی که در این راستا وجود دارد نیز بصورت جامع‌تر مورد بررسی قرار خواهد گرفت. با توجه به رشد روز افزون حملات مخرب شبکه ای، رعایت موارد امنیتی برای تک تک کاربران اینترنت لازم و ضروری به نظر می رسد. استفاده از نرم افزارهائی که به سادگی و حتی با کمترین میزان اطلاعات و توسط کاربران آماتور، می توانند موجب پدید آمدن اختلالات فراوان در شبکه و سیستم های شخصی شوند، نگرانی های بسیار جدی را بوجود می آورد. همانطور که می دانیم در طراحی سیستم عامل Windws XP، امکاناتی جهت پیشگیری از این نوع حملات پیش بینی شده است و موجبات پدید آمدن اطمینان خاطر نسبی کاربر در هنگام استفاده از شبکه بوجود آمده است. ولیکن در کنار سیستم عامل فوق، نرم افزارهایی با عنوان عمومی Firewall جهت جلوگیری از تهاجم های احتمالی مخربین شبکه مورد استفاده قرار می گیرند که خوشبختانه قابلیت نصب بر روی اکثر سیستم ها را نیز دارا می باشند. بهره جویی از این شیوه نه تنها عامل مؤثری برای حفاظت از سرویس دهندگان گوناگون اینترنت «Server» می باشد، بلکه کاربران معمولی را نیز در حفظ و نگهداری از سیستم های شخصی یاری می دهد. در همین راستا جهت برقراری امنیت نسبی در سیستم های شخصی کابران اینترنت، نرم افزارهای گوناگون و متنوعی را به بازار عرضه شده اند که از مشهورترین آنها می توان به PCCillin و Nrtn Persnal Firewall اشاره نمود. در حقیقت عملکرد کلی این نرم فزارها ایجاد یک مانع نسبتاً محکم بر سر راه مهاجمین شبکه ای است که به سادگی روی سیستم های شخصی و یا سرورها نصب شده و مورد استفاده واقع می شوند. PCCillin این نرم افزار در حقیقت یک ویروس یاب بسیار قوی است که دارای الحاقیه Firewall نیز می باشد.این نرم افزار ضمن کنترل ورود و خروج اطلاعات و برقراری امنیت در سیستم،از سلامت آنها نیز به لحاظ وجود ویروس و یا عدم آن اطمینان حاصل می کند و قابلیت update نمودن آن نیز برای کاربر فراهم شده است . Nrtn PFW این نرم افزار امنیتی بسیار قوی (Nrtn Persnal Firewall) مشابه نرم افزار PCCILLIN دارای قابلیت های فراوانی در زمینه برقراری امنیت در سیستم های کامپیوتری می باشد و کنترل کلیه فرآیندهای تبادل اطلاعات در زمان استفاده با توجه به اینکه متد و روشهای نفوذ مهاجمین با پیشرفت فن آوری و نرم افزارها، سریعاً متحول شده و تغییر می نماید، لذا در نرم افزار مذکور امکان Live Update جهت آماده سازی و محیا کردن تدابیر لازم جهت برابری و رویاروئی با حملات جدید از طریق سایت مرکزی شرکت تولید کننده نرم افزار فوق فراهم شده است.لذا در زمانهائیکه نیاز به تغییر بانک و update کردن آن باشد، هشدار لازم به کاربر داده خواهد شد و درپی آن عملیات به روز رسانی به سادگی با Dwnlad کردن فایلهای مورد نیاز انجام خواهد پذیرفت. امکان جالب دیگری که در این نرم افزار پیش بینی شده است، قابلیت Track نمود مهاجم در هنگام حمله بر سیستم می باشد. مفهوم عملکرد این است که می توان شهر ـ محل ISP و نام آن و IP اختصاص داده شده به سیستم فرد مهاجم توسط ISP را به دست آورد. این فرایند در پیگیری و شناسائی فرد مذکور مفید جلوه می نماید. بدیهی است، استفاده از برنامه فوق، مقابله نسبتاً مفیدی در برابر حملات مبتنی بر Trjan ها و Script و... شکل میدهد و موجبات بسته ماندن گذراههای قابل استفاده مهاجمین را پدید می آورد. لازم به ذکر است، نرم افزار فوق قابلیت استفاده در هر نوع شبکه (lan,.... - wan) را نیز دارا است. استفاده همزمان نرم افزار فوق با Nrtn Antivirus (که جهت کنترل و نابودی ویروسهای کامپیوتری بکار می رود) جهت ایمن سازی نسبی کامپیوترها بسیار مفید به نظر می آید. البته مبحث قابلیت های نرم افزارهای مطروحه بسیار گسترده بوده و کاربردهای گوناگونی در آنها پیش بینی شده است، که در این مقال سعی در معرفی کلی

آنها بوده است.

درباره مرکز تحقیقات رایانه‌ای قائمیه اصفهان

بسم الله الرحمن الرحیم جاهِدُوا بِأَمْوالِکُمْ وَ أَنْفُسِکُمْ فی سَبیلِ اللَّهِ ذلِکُمْ خَیْرٌ لَکُمْ إِنْ کُنْتُمْ تَعْلَمُونَ (سوره توبه آیه ۴۱) با اموال و جانهای خود، در راه خدا جهاد نمایید؛ این برای شما بهتر است اگر بدانید حضرت رضا (علیه السّلام): خدا رحم نماید بنده‌ای که امر ما را زنده (و برپا) دارد ... علوم و دانشهای ما را یاد گیرد و به مردم یاد دهد، زیرا مردم اگر سخنان نیکوی ما را (بی آنکه چیزی از آن کاسته و یا بر آن بیافزایند) بدانند هر آینه از ما پیروی (و طبق آن عمل) می کنند بنادر البحار-ترجمه و شرح خلاصه دو جلد بحار الانوار ص ۱۵۹ بنیانگذار مجتمع فرهنگی مذهبی قائمیه اصفهان شهید آیت الله شمس آبادی (ره) یکی از علمای برجسته شهر اصفهان بودند که در دلدادگی به اهلبیت (علیهم السلام) بخصوص حضرت علی بن موسی الرضا (علیه السلام) و امام عصر (عجل الله تعالی فرجه الشریف) شهره بوده و لذا با نظر و درایت خود در سال ۱۳۴۰ هجری شمسی بنیانگذار مرکز و راهی شد که هیچ وقت چراغ آن خاموش نشد و هر روز قوی تر و بهتر راهش را ادامه می دهند. مرکز تحقیقات قائمیه اصفهان از سال ۱۳۸۵ هجری شمسی تحت اشراف حضرت آیت الله حاج سید حسن امامی (قدس سره الشریف) و با فعالیت خالصانه و شبانه روزی تیمی مرکب از فرهیختگان حوزه و دانشگاه، فعالیت خود را در زمینه های مختلف مذهبی، فرهنگی و علمی آغاز نموده است. اهداف :دفاع از حریم شیعه و بسط فرهنگ و معارف ناب ثقلین (کتاب الله و اهل البیت علیهم السلام) تقویت انگیزه جوانان و عامه مردم نسبت به بررسی دقیق تر مسائل دینی، جایگزین کردن مطالب سودمند به جای بلوتوث های بی محتوا در تلفن های همراه و رایانه ها ایجاد بستر جامع مطالعاتی بر اساس معارف قرآن کریم و اهل بیت علیهم السّلام با انگیزه نشر معارف، سرویس دهی به محققین و طلاب، گسترش فرهنگ مطالعه و غنی کردن اوقات فراغت علاقمندان به نرم افزار های علوم اسلامی، در دسترس بودن منابع لازم جهت سهولت رفع ابهام و شبهات منتشره در جامعه عدالت اجتماعی: با استفاده از ابزار نو می توان بصورت تصاعدی در نشر و پخش آن همت گمارد و از طرفی عدالت اجتماعی در تزریق امکانات را در سطح کشور و باز از جهتی نشر فرهنگ اسلامی ایرانی را در سطح جهان سرعت بخشید. از جمله فعالیتهای گسترده مرکز : الف)چاپ و نشر ده ها عنوان کتاب، جزوه و ماهنامه همراه با برگزاری مسابقه کتابخوانی ب)تولید صدها نرم افزار تحقیقاتی و کتابخانه ای قابل اجرا در رایانه و گوشی تلفن سهمراه ج)تولید نمایشگاه های سه بعدی، پانوراما ، انیمیشن ، بازیهای رایانه ای و ... اماکن مذهبی، گردشگری و... د)ایجاد سایت اینترنتی قائمیه www.ghaemiyeh.com جهت دانلود رایگان نرم افزار های تلفن همراه و چندین سایت مذهبی دیگر ه)تولید محصولات نمایشی، سخنرانی و ... جهت نمایش در شبکه های ماهواره ای و)راه اندازی و پشتیبانی علمی سامانه پاسخ گویی به سوالات شرعی، اخلاقی و اعتقادی (خط ۲۳۵۰۵۲۴) ز)طراحی سیستم های حسابداری ، رسانه ساز ، موبایل ساز ، سامانه خودکار و دستی بلوتوث، وب کیوسک ، SMS و... ح)همکاری افتخاری با دهها مرکز حقیقی و حقوقی از جمله بیوت آیات عظام، حوزه های علمیه، دانشگاهها، اماکن مذهبی مانند مسجد جمکران و ... ط)برگزاری همایش ها، و اجرای طرح مهد، ویژه کودکان و نوجوانان شرکت کننده در جلسه ی)برگزاری دوره های آموزشی ویژه عموم و دوره های تربیت مربی (حضوری و مجازی) در طول سال دفتر مرکزی: اصفهان/خ مسجد سید/ حد فاصل خیابان پنج رمضان و چهارراه وفائی / مجتمع فرهنگی مذهبی قائمیه اصفهان تاریخ تأسیس: ۱۳۸۵ شماره ثبت : ۲۳۷۳ شناسه ملی : ۱۰۸۶۰۱۵۲۰۲۶ وب سایت: www.ghaemiyeh.com ایمیل: Info@ghaemiyeh.com فروشگاه اینترنتی: www.eslamshop.com تلفن ۲۵-۲۳۵۷۰۲۳- (۰۳۱۱) فکس ۲۳۵۷۰۲۲ (۰۳۱۱) دفتر تهران ۸۸۳۱۸۷۲۲ (۰۲۱) بازرگانی و فروش ۰۹۱۳۲۰۰۰۱۰۹ امور کاربران ۲۳۳۳۰۴۵(۰۳۱۱) نکته قابل توجه اینکه بودجه این مرکز؛ مردمی ، غیر دولتی و غیر انتفاعی با همت عده ای خیر اندیش اداره و تامین گردیده و لی جوابگوی حجم رو به

رشد و وسیع فعالیت مذهبی و علمی حاضر و طرح های توسعه ای فرهنگی نیست، از اینرو این مرکز به فضل و کرم صاحب اصلی این خانه (قائمیه) امید داشته و امیدواریم حضرت بقیه الله الاعظم عجل الله تعالی فرجه الشریف توفیق روزافزونی را شامل همگان بنماید تا در صورت امکان در این امر مهم ما را یاری نمایندانشاالله. شماره حساب ۶۲۱۰۶۰۹۵۳ ، شماره کارت :۶۲۷۳-۵۳۳۱-۳۰۴۵-۱۹۷۳و شماره حساب شبا : IR۹۰-۰۱۸۰-۰۰۰۰-۰۰۰۰-۰۶۲۱-۰۶۰۹-۵۳به نام مرکز تحقیقات رایانه ای قائمیه اصفهان نزد بانک تجارت شعبه اصفهان – خیابان مسجد سید ارزش کار فکری و عقیدتی الاحتجاج - به سندش، از امام حسین علیه السلام -: هر کس عهده دار یتیمی از ما شود که محنتِ غیبت ما، او را از ما جدا کرده است و از علوم ما که به دستش رسیده، به او سهمی دهد تا ارشاد و هدایتش کند، خداوند به او می‌فرماید: «ای بنده بزرگوار شریک کننده برادرش! من در کَرَم کردن، از تو سزاوارترم. فرشتگان من! برای او در بهشت، به عدد هر حرفی که یاد داده است، هزار هزار، کاخ قرار دهید و از دیگر نعمت‌ها، آنچه را که لایق اوست، به آنها ضمیمه کنید». التفسیر المنسوب إلی الإمام العسکری علیه السلام: امام حسین علیه السلام به مردی فرمود: «کدام یک را دوست‌تر می‌داری: مردی اراده کشتن بینوایی ضعیف را دارد و تو او را از دستش می‌رَهانی، یا مردی ناصبی اراده گمراه کردن مؤمنی بینوا و ضعیف از پیروان ما را دارد، امّا تو دریچه‌ای [از علم] را بر او می گشایی که آن بینوا، خود را بِدان، نگاه می‌دارد و با حجّت‌های خدای متعال، خصم خویش را ساکت می‌سازد و او را می‌شکند؟». [سپس] فرمود: «حتماً رهاندن این مؤمن بینوا از دست آن ناصبی. بی گمان، خدای متعال می‌فرماید: «و هر که او را زنده کند، گویی همه مردم را زنده کرده است»؛ یعنی هر که او را زنده کند و از کفر به ایمان، ارشاد کند، گویی همه مردم را زنده کرده است، پیش از آن که آنان را با شمشیرهای تیز بکشد». مسند زید: امام حسین علیه السلام فرمود: «هر کس انسانی را از گمراهی به معرفت حق، فرا بخواند و او اجابت کند، اجری مانند آزاد کردن بنده دارد».