واحد رودهن

کارآموزی

عنوان کار آموزی:
اجرای کارهای سخت افزاری
و شبکه

محل کار آموزی:

شرکت کارا سیستم

نام استاد :

نام دانشجو:

بهار ۹۳

صفحه عنوان

فهرست

چکیده:

من یک شبکه را با برنامه **word** پیاده سازی کردم.

این طراحی 6 روز طول کشید. در زیر توضیحی درباره شبکه داده شده;

سپس قسمتهای مختلف این طرح را معرفی کردم.

<< شبکه تعدادی از سیستمهای متصل به هم است که سرویسها و منابع خود را به اشتراک گذاشته و از طریق خط ارتباطی اشتراکی با هم مرتبط هستند. >>

پس یک شبکه به دو یا چند سیستم مجزا و چیزهایی برای به اشتراک گذاشتن داده‌ها نیاز دارد. سیستم‌های مجزا از طریق مسیر فیزیکی که محیط انتقام نام دارد به هم متصل می‌شوند. تمام سیستم‌های روی مسیر فیزیکی باید از قوانین مخابراتی مشترک برای دریافت و ارسال اطلاعات استفاده کنند. این قوانین پروتکل نام دارند .

- در ساده‌ترین حالت یک شبکه کامپیوتری از دو یا چند کامپیوتر تشکیل شده است که اطلاعات را روی محیط انتقال مشترک به اشتراک می‌گذارند .

Patch panel (تابلوهای تقسیم گسترش‌پذیر): این تابلوها به شکلهای مختلفی ساخته می‌شوندو بین کابلهایی که به هابها و همچنین کابلهایی که به رایانه‌ها وصل می‌شوند قرارمی‌گیرند. بعضی از این Patch panel ها تا ۹۶ پورت دارند و سرعت انتقال ۱۰۰ Mbps را پشتیبانی می‌کنند.

Router : یک مسیریاب برای بسته‌های (Packet) اطلاعات در شبکه است.

Rack (قفسه‌های توزیع): در شبکه‌های (Tp) بزرگ قفسه‌های توزیع می‌توانند فضای مناسبی را برای کابلها و هابها ایجاد نماید به طوری که فضای کف را اشغال نکند. این قفسه‌ها فضای خوبی برای تمرکز دادن و سازمان‌دهی شبکه‌ای هستند که تعدادی اتصالات دارد .

Hub: قطعه شبکه‌ای که بیش از پیش در شبکه‌ها وسیله‌ای استاندارد می‌شوند هاب است. هاب قطعه مرکزی در توپولوژی ستاره‌ای می‌باشد .

Ups: یک ترانزیستور که چند کار را انجام می‌دهد:

اول اینکه اگر برق قطع شود در کسر بسیار کوچکی از ثانیه برق اضطراری را وصل می‌کند طوری که کامپیوتر متوجه تغییر ولتاژ نشود.دوم اینکه نوسانات برق را تنظیم می‌کند.

.**Vpnline**: خط تلفنی که مستقیم است و احتیاج به شماره‌گیری ندارد و در صورتی که دکل مشکل پیدا کند از آن استفاده می‌شود .

کابل معمولی ۱ ـ ۱: طبق فرمول زیر ساخته می‌شود :

۱	۲	۳	۴	۵	۶	۷	۸
۱	۲	۳	۴	۵	۶	۷	۸

کابل کراس (Cross): برای وصل کردن دو کارت شبکه به یکدیگر و طبق فرمول زیر ساخته می‌شود:

۱	۲	۳	۴	۵	۶	۷	۸
۳	۶	۱	۴	۵	۲	۷	۸

Hp server: یک کامپیوتر است که کار مدیریت را برای بقیه کامپیوترها انجام می‌دهد .

در واقع یک سرور مادر است که بانک اطلاعاتی همه دستگاهها را در Hard آن سرور ذخیره می‌شود .

کیوسک: کامپیوترهایی که کاربر روی آن کار می‌کنند .

معرفی مختصر محل کارآموزی:

این مجتمع در تهران و در خیابان فردوسی واقع شده است فعا لیت های این مجتمع در زمینه های :

۱- Web Site Design

۲- خرید و فروش سخت افزار

۳- نصب و راه اندازی شبکه های کامپیوتری

شرحی بر فعالیت‌های انجام گرفته در طی دوره کارآموزی :

استاد گرامی، بنده تلاش کردم در طی این دوره با مفاهیم، نکات و تجاربی آشنا شوم که در صنعت و کار مورد استفاده قرار می‌گیرد و در دانشگاه مطلب کمتری راجع به آن‌ها عنوان می‌شود.

اگرچه ممکن است این مطالب ظاهری تئوری‌گونه به خود گرفته باشد ولی این‌ها ناشی از ساعت‌ها تجربه شخصی خودم و سال‌ها تجربه دیگران می‌باشد.

از جمله کارهای من ساختن یک شبکه کوچک متشکل از ۳ کامپیوتر بود. ابتدا باید یک سری سوکت آماده می‌کردم

که این سوکت‌ها همگی به **Hub switch** متصل بودند.

برای آماده کردن این سوکت‌ها احتیاج به کابل، کیستون، سوکت، سیم چین و پرس داریم. کابل استفاده شده Utp است و ۵ نوع دارد که من در اینجا از ۵ CAT استفاده کردم.

ابتدا کابلهایی به طول ۲ الی ۳ متر جدا نموده آنها را لخت نموده و می‌دیدم که ۸ رشته سیم که دو به دو بهم پیچیده شده بودند وجود داشت .

رنگ این سیمها عبارت بود از قهوه‌ای، سبز، آبی و نارنجی که هر یک با یک رشته سیم سفید به هم تابیده شده بودند.

برای اینکه سوکت‌ها درست کار کنند باید این رنگها به ترتیب خاصی کنار هم قرار می‌گرفتند که به وسیله کیستون این کار را انجام می‌دادیم. در روی کیستون دو گروه رنگی A و B درست کردم. در این گروه از چپ به راست باید سیم‌ها به این ترتیب کنار هم قرار می‌گرفتند:

قهوه‌ای، قهوه‌ای سفید ـ سبر، سبز سفید ـ آبی، آبی سفید ـ نارنجی و نارنجی سفید

سپس آنها را داخل سوکت فشار دادم و وسیله پرس و به وسیله فشار دست سر سیمها را که درون سوکت قرار داشت ثابت کردم به این ترتیب کابلها ساخته می‌شدند. سپس 3 کامپیوتر انتخاب کردم و به وسیله هر کدام از کابل‌های گفته شده سر هر کابل از یک سو به کارت شبکه (در پشت Case) و از سوی دیگر به hub switch وصل بود. سپس باید IPها را در کامپیوتر تنظیم می‌کردم

و پس از بالا آمدن برنامه win ابتدا روی Network Neighbor hood کلیک راست کرده و Properties را زده وارد configuration شده گزینه (Tcp/Ip) را انتخاب و سپس Properties را انتخاب می‌کنیم.

Sybnetmusk, IP و get way را تعیین می‌کنیم سپس برای شکل دهی شبکه این مراحل را طی می‌کنیم:

Stsrt → program →accessories →communication→
Network set up wizard → next

پس از گذراندن این مراحل گزینه Ignaredi را انتخاب می‌کنیم و سپس Next و از ۳ گزینه موجود در صفحه other را انتخاب و به صفحه بعدی رفته گزینه آخر را انتخاب می‌کنیم که گزینه دارای شکل نمایشی از شبکه مورد نظر ما می‌باشد که متناسب با نیازمان شبکه مورد نظر را انتخاب می‌کنیم و سپس Next را انتخاب و در صفحه بعدی work group را مشخص می‌کنیم و کار به اتمام می‌رسد.

امنیت شبکه‌های کامپیوتری

مهمترین وظیفه یک شبکه کامپیوتری فراهم سازی امکان برقراری ارتباط میان گره‌های آن در تمام زمانها و شرایط گوناگون است ;

بصورتی که برخی از محققین امنیت در یک شبکه را معادل استحکام و عدم بروز اختلاف در آن می‌دانند. یعنی؛ Security = Robustness + Fault Tolerance. هرچند از زاویه‌ای این تعریف می‌توانددرست باشد اما بهتر است اضافه کنیم که امنیت در یک شبکه

علاوه بر امنیت کارکردی به معنی خصوصی بودن ارتباطات نیز هست. شبکه‌ای که درست کار کند و مورد حمله ویروسها و عوامل خارجی قرار نگیرد اما در عوض تبادل اطلاعات میان دو نفر در ان توسط دیگران شنود شود ایمن نیست.

...

اما ببینیم که چه کسانی ـ فرد، دستگاه، نرم افزار و ... ـ می‌توانند امنیت ارتباط برقرار شده شما را تهدید کنند: هکر (Hacker)ها ، ویروس ها (Viruses)، کرم‌های شبکه (Worms) و ...

امنیت در شبکه یک امر بسیار ضروریست و جای یک سایت اطلاع رسانی در مورد امنیت شبکه بسیار خالی بود.«**امنیت در شبکه**» وارد گستره وب شد;

این سایت به همراه سایتهای سیمرغ، گفتگوی هارمونیک، مجله اینترنتی ورزش، بهترین‌های ایران و Oyax محصول داتیس پارس هست.

طراحی زیبا، ساختارا ساده و بدون پیچیدگی و زبانی عامه فهم از روشهای کاری این گروه می‌باشد. ورود سایت امنیت شبکه را به مدیران آن تبریک می‌گوییم.

امیدوارم فعالان توسعه محتوای فارسی در وب بیش از پیش موفق باشند و در آینده‌ای نزدیک با افزایش کاربران اینترنت، به جای سایتهای فال و طالع بینی، مخاطبین بیشتری جذب سایتهای با محتوای مفید گردند.

با کاربرد فایروال آشنا شویم ...

Firewall دستگاهی است در درون شبکه یک شرکت قرار می‌گیرد و شبکه را از محیط اینترنت و یا دسترسی های بیرونی ازوله می‌کند. فایروال با کنترل دسترسی‌ها به شبکه، به برخی درخواستها اجازه ورود به شبکه را داده و مانع ورود برخی دیگر درخواستها می‌شود. معمولاً برنامه‌ریزی و سیاستگذاری یک فایروال اینگونه است که کلیه دسترسی‌ها از بیرون به داخل شبکه شرکت از محیطی عبور می‌کند که کاملاً در حال کنترل و مونیتور کردن است;

این موضوع دقیقا 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 می‌کنند و یا شما را از x-Ray عبور می‌دهند .

اما از آنجایی که فایروالها اغلب به دلیل انجام تنظیمات نادرست خوب عمل نمی‌کنند، امروزه بسیاری از مدیران شرکت‌ها به آن‌ها اعتماد ندارند و عملکرد مثبت آن‌ها به هنگام بروز خطر یا حمله یک هکر را پنجاه پنجاه می‌دانند.

بعنوان مثال همانطور که می‌دانید یکی از مهم‌ترین منابع حملات شبکه‌ای از ناحیه کارکنان ناراضی شرکت‌ها است، این در حالی است که فایروال‌ها معمولاً طوری تنظیم می‌شوند که مراقبت شبکه را از تهدیدهای بیرونی به عهده بگیرند.

بنابراین یکی از مهمترین مواردی که مدیران یک سازمان باید آن را خوب درک کنند آن است که بدانند فایروالی که در شبکه شرکت نصب شده است چه محدودی راه پوشش امنیتی می‌دهد. همچنین مدیران شرکت‌ها باید بدانند که فایروال دستگاهی است که در

کنار سایر سیستم‌های امنیتی داخلی و خارجی می‌تواند بر استحکام امنیتی شبکه شما بیفزاید.در این حالت وب سرور در درون بشکه قرار دارد و امنیت شبکه بطور کامل توسط فایروال کنترل می‌شود اما ضعف وب سرور می‌تواند محل نفوذ هکرها باشد.

یک مثال کاربردی

بسیاری از شرکت‌های امروز دارای وب سرورهایی 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.

۱ـ بیرون فایروال:

انتخاب اول آن است که وب سرور را خارج از فایروال قرار دهید. در این حالت بنظر می‌رسد که شما سرور خود را مستقیماً بدون هیچ سیستم امنیتی روی اینترنت قرار داده‌اید. این محل برای وب سرور شما خطرناک است اما شاید تعجب کنید اگر بدانید که می‌تواند 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 می‌کند. اما دقت کنید که این حالت برای شبکه شما امنیت بیشتری دارد.

۲ـ درون فایروال و تحت حمایت آن : در این حالت شما وب سرور شرکت را در درون محدوده امنیتی فایروال یعنی شبکه شرکت قرار داده‌اید.

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 قاعدتا باید فقط به سرویس‌های درخواست صفات وب پاسخ بدهد

اما چنانچه هکری بتواند به نحوی به داخل این سرور رسوخ کند، به احتمال زیاد خواهد توانست از طریق پورت‌های مختلف وب سرور شما به قسمت‌های مختلف شبکه دسترسی پیدا کند. بخصوص اگر وب سرور شما برای اجرای برنامه‌ها مانند برنامه‌های 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

۳ـ میان دو فایروال :

این حالت ترکیبی است از دو موردی که تا کنون راجع به آن صحبت کردیم.

آشنایی با نکات تجربی هنگام انتخاب رمز عبور:

منزل مسکونی شما درب و پنجره‌هایی دارد که اغلب هنگام شب و یا در مواقعی که به مسافرت می‌روید آن‌ها را بسته و در شرایطی قفل‌هایی هم به آنها اضافه می‌کنید. یقیناً از یک کلید برای قفل همه دربها استفاده نمی‌کنید و هرگز کلیدها را در اختیار افراد ناآشنا نخواهید گذاشت.

همچنین کلیدها زیر فرش یا کنار باغچه حیاط مخفی نمی‌کنید. پس چرا با رمز عبور خود (**Password**) اینگونه رفتار می‌کنید؟

برای دسترسی به سرویسهای مختلف کامپیوتر و شبکه معمولاً برای شما رمزهای عبور مختلفی در نظر گرفته می‌شود;

و شما باید همانند کلید دربهای منزل از آنها محافظت کنید. برای یک لحظه به کلید ورودی منزل دقت کنید، بدون شک از بقیه کلیدها پیچیده‌تر و گرانتر است، بنابراین باید هنگام انتخاب رمز ورودی کامپیوتر خود موارد ایمنی را بیشتر رعایت کنید.

معمولاً شما می‌توانید password ورودی کامپیوتر خود را به هر اندازه که می‌خواهید پیچیده انتخاب کنید، اما دقت داشته باشید که باید بتوانید همواره به روشی آن را بخاطر بیاورید این روش نباید همانند گذاشتن کلید درب مورودی منزل زیر فرش جلوی درب یا کنار باغچه به گونه‌ای باشد که سارق به سادگی بتواند آن را پیدا کند. سارقان اینترنتی همانند سارقان منزل حرفه‌ای هستند بخصوص اگر با شما آشنایی داشته باشد. آنها با استفاده از تجاربی که دارند بسادگی گزینه‌هایی که می‌تواند ورود آنها به کامپیوتر شما را ممکن سازد حدس می‌زنند، بخصوص اگر با خصوصیات اخلاقی و زندگی شما آشنا باشند.

حتی امروزه روشهایی مانند جابجایی حرف o 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 می‌کنید و آن شامل ۶ حرف ، ۴ عدد و ۴ علامت است که همگی بصورت اتفاقی (random) انتخاب شده‌اند.

آیا بنظرشما این رمز می‌تواند برای شما مفید باشد؟ به احتمال زیاد نه چراکه در اینصورت خود شما مجبور خواهید بود برای به خاطر آوردن، آنرا جایی یادداشت کنید و این خطرناک‌ترین کارها است.

اگر مواردی که در زیر به آن‌ها اشاره می‌شود را رعایت کنید می‌توانید تقریباً مطمئن باشید که password کامپیوتر شما به این راحتی‌ها توسط یک سارق قابل حدث زدن نخواهد بود:

۱ـ رمز باید به اندازه کافی قوی باشد. در اینجا قوی بودن به معنای طولانی بودن رمز می‌باشد. هیچ اشکالی ندارد که حتی بیش از ۱۴ حرف هم باشد. انتخاب یک جمله نه به صورتی که معمولاً آن را می‌نویسیم می‌تواند گزینه مناسبی باشد .

۲ـ رمز باید یگانه باشد. گزینه‌هایی مانند ۱۲۳ یا test یا letmein یا my dog و .. گزینه‌هایی آشنا برای همگان است، هرگز از آنها استفاده نکنید.

برای گرفتن ایده به سراغ مواردی بروید که به فکر هیچ کس نمی‌رسد مثلاً نوع خاصی از یک مارماهی که در دریاهای سرد زندگی می‌کند راجع به این مارماهی مطالعه کنید و پس از شناخت آن در ارتباط با آن یک رمز انتخاب کنید و راجع به آن با هیچ کس صحبت نکنید .

۳ـ رمز باید کاربردی باشد. کاربردی به این معنای که به خاطر سپردن آن ممکن و ساده باشد. این اتفاق بارها رخ داده که کاربر رمز را به گونه‌ای انتخاب می‌کند که بعدها توانایی به یاد آوردن آن را ندارد لذا مجبور می‌شود آن را یادداشت کند .

۴ـ رمز باید طول عمر کوتاه داشته باشد. بازه زمانی تعویض رمز کاملاً به نوع کاربری کامپیوتر و موقعیت شغلی شما دارد .

اگر مسئولیت مهمی دارید و اطلاعات قیمتی در کامپیوتر خود نگهداری می‌کنید ترجیح بر آن است که در فاصله‌های کوتاه ـ مثلاً یک هفته ـ رمز خود را عوض کنید اگرنه حداقل هر یکی دو ماه رمز عبور خود را باید تغییر کنید .

آشنایی با اصول مهم مباحث امنیتی

تفکر امنیت در شبکه برای دستیابی به سه عامل مهم است که با یکدیگر مثلث امنیتی را تشکیل می‌دهد. این عوامل عبارتند از :

- رازداری و امانت داری (Confidentiality)

- یکپارچگی (Integrity)

- و در نهایت در دسترس بودن همیشگی (Availability).

این سه عامل (CIA) اصول اساسی امنیت اطلاعات ـ در شبکه و یا بیرون آن را تشکیل می‌دهند به گونه‌ای که تمامی تمهیدات لازمی که برای امنیت شبکه اتخاذ می‌شود و یا تجهیزاتی که ساخته می‌شوند همگی ناشی از نیاز به اعمال این پارامتر در محیط‌های نگاهداری و تبادل اطلاعات است.

Confidentiality: 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 می‌گردد و بطور خلاصه می‌توان آنرا اینگونه تعریف کرد:

ـ تغییرات در اطلاعات فقط باید توسط افراد یا پروسه‌های مشخص و مجاز انجام گیرد.ـ تغییرات بدون اجازه و بدون دلیل حتی توسط افراد یا پروسه‌های مجاز نباید صورت بگیرد.

ـ 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 می‌کند باید همزمان درون و برون سیستم از آن آگاه شوند.

Availability: ای نپارامتر ضمانت می‌کند که یک سیستم ـ مثلاً اطلاعاتی ـ همواره باید در دسترس باشد و بتواند کار خود را انجام دهد. بنابراین حتی اگر همه موارد ایمنی مدنظر باشد اما عواملی باعث خوابیدن سیستم شوند ـ مانند قطعبرق ـ از نظر یک سیستم امنتی این سیستم ایمن نیست.

اما جدای از مسائل بالا مفاهیم و پارامترهای دیگری نیز هستند که با وجود آنکه از همین اصول گرفته می‌شوند برای خود شخصیت جداگانه‌ای پیدا کرده‌اند. در این میان می‌توان به مفاهیمی نظیر Identification به معنی تقاضای شناسایی به هنگام دسترسی کاربر به سیستم،

Authentication: به معنی مشخص کردن هویت کاربر

Authorization: به معنی مشخص کردن میزان دسترسی کاربر به منابع

Accountability: به معنی قابلیت حسابرسی از عملکرد سیستم و ... اشاره کرد.

خدمات مهندسی و امنیت شبکه

مهندسان شبکه ،شبکه اینترنتی موسسات تجاری شما را چه کوچک و چه بزرگ راه اندازی و نگهداری می‌کند.

ما قادر هستیم به شما نشان دهیم که چگونه از شروع کار تا داشتن بیش از ۳۰ میلیون مشتری بر روی اینترنت پیشرفت خواهید کرد.

محدوده خدمات اینترنتی عبات است از:

راه‌اندازی ارتباطات نقطه به نقطه بر اساس فناوریهای روز نظیر xDSL، E1 و Wireless

طراحی و پیاده‌سازی شبکه‌های صنعتی در سطوح گوناگون

طراحی و پیاده‌سازی سیستمهای کابل کشی ساخت یافته UTP و فیبر نوری بر اساس آخرین استانداردها برای شبکه‌های محلی (LAN) و Enterprise LAN و ارائه راه حل‌های مبتنی بر تکنولوژی Fast-Ethernet ، Gigabit-Ethernet و ATM

ارائه روشهای مختلف دسترسی به اینترنت بر اساس خطوط اختصاصی پرسرعت، ارتباط ماهواره‌ای دوطرفه، VSAT و DVBپیاده‌سازی رده‌های مختلف ISP با ارائه راه حل بر اساس سیستم عاملهای مبتنی بر

UNIX (Solaris – FreeBSD , Linux) و همچنین سیستم عاملهای خانواده Microsoft،

نصب و پیکربندی سرویسهای مختلف ISP و Datacenter و ایجاد سیستمهای امنیتی و قابلیت کنترل ترافیک و تنظیم پهنای باند بین کاربران و سرویسهای مختلف

طراحی و پیاده سازی سرویسهای مختلف برای یکپارچه سازی شبکه ها مانند ارائه سرویس VOIP، ارائه سرویسهای صوتی ـ تصویری در شبکه

مستند سازی، آنالیز ساختار و مونیتورینگ ترافیک در شبکه‌های محلی و گسترده برای ارائه راهکارهای مناسب جهت بهبود وضعیت موجود، ارتقای سیستم و حذف گلوگاهها;

پیاده سازی سیستمهای امنیتی Firewall، VPN و IDS همچنین ارائه خدمات برای جلوگیری از حملات، تشخیص نفوذ و حمله کنندگان، امن کردن سیستمها و بازیابی (Recovery) سیستمها به وضعیت کاری قبل از حمله

طراحی و تولید محصولات سخت افزاری و نرم افزاری شبکه بر اساس نیازهای مشتریان داخلی اعم از Shapper , autodialler , network Monitor , BW , Modem Pool , DSL Router , Remote Access Servers , Firewall , Fax Server , Video/Voice Server , Cache Server

که برخی از این محصولات دارای مجوز از مراکزی چون سازمان پژوهشهای علمی صنعتی، مرکز توسعه صادرات ایران، صندوق حمایت از صنایع الکترونیک و سازمان مدیریت و برنامه ریزی کشور می‌باشد.

راه حل امنیتی مشکل آفرین در ویندوز xp

میلیونها شرکت کوچکه که از برنامه ویندوز استفاده می‌کنند پس از نصب برنامه کمکی کمپانی مایکروسافت برای حل مشکلات امنیتی بزرگ ویندوز xp با مشکلات تازه‌ای مواجه شده‌اند.

شرکت کانادایی استمتر یکس هشدار داده است که حدود ده درصد کامپیوترهای رومیزی پس از نصب این برنامه که ایکس پی (SP2) نام دارد، دچار مشکل شده‌اند.

این شرکت در بررسی‌های خود به این نتیجه رسیده است که شرکتهای کوچکه که معمولا از کامپیوترهای کهنه استفاده می‌کنند بیشتر دچار این مشکل می‌شوند.شرکتهایی هم که از نسخه‌های قدیمی برنامه‌های کامپیوتری استفاده می‌کنند یا به روایتهای کمتر شناخته شده از برنامه‌های مشهور متکی هستند با این مشکل روبرو خواهند شد.انتظار بی‌ثمر؟....

برنامه موسوم به آپدیت ایکس پی ۲ که کاربران مدتهاست منتظر آن بوده‌اند، در اواخر مات اوت به کاربران کامپیوتر عرضه شد.

این برنامه که مایکروسافت وعده ارائه آن را در سال ۲۰۰۳ داده بود، قرار است سیستم عامل ویندوز ایکس پی را از اینکه آماج حملات ویروس نویسان، نفوذگران بداندیش و تبهکار آن آشنا با فن آوری قرار بگیرد نجات دهد.

این نرم افزار، ویندوز ایکس پی را تغییر می‌دهد تا به کاربران امکان مدیریت برنامه ضد ویروس خود را با سهولیت بیشتری در دست بگیرند.

ایکس پی دو هسته مرکزی ویندوز را تغییر می‌دهد و راه نفذوذ مورد استفاده بدخواهان و برنامه نویسان دارای سوء نیست را می‌بندد. اما استفاده از خود این نرم افزار هم چندان بی درد سر نبوده است.مایکروسافت دریافته است که شصت برنامه که بیشتر آنها را خود این کمپانی ارائه کرده، پس از نصب ایکس پی دیگر به خوبی سابق کار نخواهند کرد.

مایکروسافت مهلت می‌خواهددر بعضی موارد تغییر تنظیمات ویندوز مشکلات را حل می‌کند اما در موارد دیگر اقدامات جدی‌تری مورد نیاز است...

مایکروسافت از بسیاری از مشتریان خود در شرکت‌های بزرگ خواسته است که نصب ایکس پی ۲ را به تعویق بیندازند تا شرکت سازنده نرم افزار ویندوز بتواند تعیین کند که چه برنامه‌هایی احتمالاً با این نرف افزار تازه سازگار نیستند.

اینک شرکت استمتریکس اطلاعاتی را از شرکتهای کوچک و بزرگ استفاده کننده از نرم افزارهای مایکروسافت جمع‌آوری کرده تا بتواند مقیاس مشکل پیش روی این شرکتها را بسنجد.

پیش بینی این شرکت آن است که ۱۰/۳ درصد از کامپیوترهای شرکت بزرگ با مشکل سازگاری برنامه‌های مختلف روبرو خواهند بود.

در مورد شرکتهای کوچکتر که کمتر از صد دستگاه کامپیوتر دارند، این میزان احتمالاً به 12 درصد خواهد رسید.

در این بررسی شرکتی هم بود که تا 60 درصد کامپیوترهایش دچار مشکل شوده بود.

مایکروسافت پاسخ و همکاری

بررسی استمستر نشان می‌دهد که هرچه نرم افزار نصب شده روی کامپیوتر کهنه‌تر باشد، احتمال دچار مشکل شدن آن بیشتر خواهد بود.

اما یک سخنگوی مایکروسافت در بریتانیا می‌گوید: «*تحقیقات خود ما نشان می‌دهد که اکثر برنامه‌ها کار خود را مثل روز اول انجام می‌دهند*».

او می‌افزاید: «اکثر مشکلات نرم افزاری که ما شاهد آن بودیم با مختصری تنظیم برطرف می‌شود».

او گفت که مایکروسافت با مشتریان شرکتی خود همکاری می‌کند تا کار نصب و تنظیمات بعداز نصب برنامه را راحت‌تر انجام بدهند.

امنیت شبکه‌های کامپیوتری

هکر اغلب سعی در آسیب رساندن به شبکه را دارد

مهمترین وظیفه یک شبکه کامپیوتری فراهم سازی امکان برقراری میان گره‌های آن در تمام زمانها و شرایط گوناگون است به صورتی که برخی از محققین امنیت در یک شبکه را معادل استحکام و عدم بروز اختلال در آن می‌دانند یعنی

Security=Robustness+Fault Tolerance. هرچند از زاویه‌ای این تعریف می‌تواند درست باشد اما بهتر است اضافه کنیم که امنیت در یک شبکه علاوه بر امنیت کارکردی به معنی خصوصی بودن ارتباطات نیز هست. شبکه‌ای 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 می‌خواهید با یک نفر در شبکه تبادل اطلاعات ـ بصورت email یا chat و ... ـ 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،

ـ تبادل اطلاعات شما را بشنود و یا از آن کپی زنده تهیه کند،

ـ با شبیه سازی کامپیوتر دوست شما، بعنوان او با شما تبادل اطلاعات کند،

ـ کامپیوتر شما یا دوستتان را از کار بیندازد،

ـ از منابع کامپیوتر شما برای مقاصد خود استفاده کند،

ـ برنامه مورد علاقه خود ـ یا یک تکه کد کوچک ـ را در کامپیوتر شما نصب کند،

ـ در مسیر ارتباطی میان شما و دوستتان اختلال بوجود آورد،

ـ با سوء استفاده از کامپیوتر شما به دیگران حمله کند،

ـ و بسیاری موارد دیگر ...

اما ببینیم که چه کسانی ـ فرد، دستگا، نرم افزار و ... ـ می‌توانند امنیت ارتباط برقرار شده شما را تهدید کنند.

هکر (Hacker)

در معنای لغوی به فردی گفته می‌شود که با ابزار به ساخت لوازم خانه (میز، مبل و ...) می‌پردازد. اما امروزه این اصطلاح بیشتر به افرادی اطلاق می‌شود که علاقمند به کشف رمز و راز برنامه های مختلف نصب شده روی کامپیوترها می‌باشند تا به این وسیله دانش و توانایی خود را بالا ببرند. اینگونه افراد معمولاً دانش زیادی از نحوه کار کامپیوتر و

سیستم‌های شبکه‌ای دارند و اغلب بطور غیرمجاز سعی در ورود به سیستم‌های اطلاعاتی یا کامپیوترهای شخصی افراد می‌کنند.

اما معنی عمومی‌تر 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 شبکه‌های کامپیوتری دیگران می‌شوند. قصد یا غرض این افراد از انجام اینکارها می‌تواند تمام مواردی باشد که در مطلب قبل امنیت در دنیای واقعی به آن اشاره کردیم، باشد. امروزه فعالیت این افراد در بسیار یاز کشورها در رده فعالیت‌های جنایی در نظر گرفته می‌شود.

ویروس (Virus)

همانطور که میدانید از لحاظ بیولوژیکی موجودات کوچکی که توانایی تکثیر در درون سلولهای زنده را دارند و اغلب باعث بروز بیماری‌هایی مانند سرماخوردگی، سرخک، هپاتیت و .. می‌شوند، ویروس نام دارند. ویروس‌ها عموماً با استفاده از

روشهای مختلف در جامعه انسانی ـ یا حیوانی ـ منتشر میشوند و در صورت عدم وجود کنترل و درمانها پزشکی خطرات جبران‌ناپذیری را به جامعه تحمیل می‌کنند.

با ایده‌برداری از همین روش یعنی زندگی در بدن یک میزبان و انتقال به هنگام تعامل میزبان با همسان خود، نرم‌افزارهای عموماً کوچکی تهیه شده است که می‌توانند در یک دستگاه کامپیوتر اجرا شوند و ضمن به خطر انداختن آن دستگاه به هنگام تبادل اطلاعات ـ به هر شکلی ـ با دیگر کامپیوترها خود را پخش کنند. این تبادل می‌تواند از طریق کپی کردن اطلاعات در روی دیسک باشد، یا اجرا برنامه‌های کامپیوتر و ...

کرم‌های شبکه (Worms):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 می‌شود.

اما در دنیای کامپیوتر و ارتباطات اینترنتی کرم به گونه‌ای از نرم افزارها گفته می‌شود که در گره‌های شبکه ـ مثلاً کامپیوتر ـ مستقر شده و می‌تواند علاوه بر زندگی و آسیب رسان به آن گره نسخه دیگری از خود را از طریق شبکه به سایر گره‌ها منتقل کند و آنها را نیز دچار مشکل سازد. بنابراین مشاهده می‌کنید که سرعت تولید مثل و انتشار یک کرم در شبکه بزرگ چه مقدار می‌تواند زیاد باشد.

کرم‌ها معمولاً علاوه بر آنکه باعث تخریب میزبان خود می‌شوند، با اشغال کردن فضای ارتباطی در شبکه، تاثیری چون ترافیک و کندی ارتباطات در شبکه را به همراه می‌آورند که این خود می‌تواند عوارض بعدی برای فعالیت سایر تجهیزات در شبکه و یا حتی بخش عمده‌ای از شبکه اینترنت شود.

امنیت شبکه چیست؟

یکی از مهم‌ترین فعالیت‌های مدیر شبکه، تضمین امنیت منابع شبکه است. دسترسی غیرمجاز به منابع شبکه و یا ایجاد آسیب عمدی یا غیرعمدی به اطلاعات، امنیت شبکه را مختل می‌کند. از طرف دیگر امنیت شبکه نباید آنچنان باشد که کارکرد عادی کاربران را مشکل سازد.

برای تضمین امنیت اطلاعات و منابع سخت افزاری شبکه، از دو مدل امنیت شبکه استفاده می‌شود. این مدل‌ها عبارتند از: امنیت در سطح اشتراک (Share-Level) و امنیت در سطح کاربر. (User-Level)

در مدل امنیت در سطح اشتراک، این عمل با انتساب اسم رمز یا Password برای هر منبع به اشتراک گذاشته تامین می‌شود. دسترسی به منابع مشترک فقط هنگامی برقرار می‌گردد که کاربر اسم رمز صحیح را برای منبع به اشتراک گذاشته شده را به درستی بداند.

به عنوان مثال اگر سندی قابل دسترسی برای سه کاربر باشد، می‌توان با نسبت دادن یک اسم رمز به این سند مدل امنیت در سطح Share-Level را پیاده سازی کرد. منابع شبکه را می‌توان در سطوح مختلف به اشتراک گذاشت. برای مثال در سیستم عامل ویندوز ۹۵ می‌توان دایرکتوری‌ها را بصورت فقط خواندنی (Read Only)، بر حسب اسم رمز یا به شکل کامل (Full) به اشتراک گذاشت از مدل امنیت در سطح Share-Level می‌توان برای ایجاد بانک‌های اطلاعاتی ایمن استفاده کرد.

در مدل دوم یعنی امنیت در سطح کاربران، دسترسی کاربران به منابع به اشتراک گذاشته شده با دادن اسم رمز به کاربران تامین می‌شود.

در این مدل کاربران در هنگام اتصال به شبکه باید اسم رمز و کلمه عبور را وارد نمایند. در اینجا سرور مسئول تعیین اعتبار اسم رمز و کلمه عبور است. سرور در هنگام دریافت درخواست کاربر برای دسترسی به منبع به اشتراک گذاشته شده،

به بانک اطلاعاتی خود مراجعه کرده و درخوات کاربر را رد یا قبول می‌کند.

تفاوت این دو مدل در آن است که مدل امنیت در سطح Share-Level، اسم رمز به منبع نسبت داده شده و در مدل دوم اسم رمز و کلمه عبور به کاربر نسبت داده می‌شود. بدیهی است که مدل امنیت در سطح کاربر بسیار مستحکم‌تر از مدل امنیت در سطح اشتراک است. بسیاری از کاربران به راحتی می‌توانند اسم رمز یک منبع را به دیگران بگویند. اما اسم رمز و کلمه عبور شخصی را نمی‌توان به سادگی به شخص دیگری منتقل کرد.

امنیت اینترنتی
Internet Security

امروزه مقوله امنیت برای تمامی سیستمهای عامل حتی لینوکس بسیار ضروری به نظر می‌رسد شرکتهای بزرگ سالانه مقادیر هنگفتی را خرج ایجاد امنیت در شبکه هایشان می‌کنند تا آنها را از خطر حمله هکرها د رامان نگه داردند ولی اشخاص حقیقی کمتر به این موضوع مهم توجه می‌کنند

و بیشتر هم مورد تهاجم واقع می‌شوند چون فکر می‌کنند اطلاعات مهمی که به درد هکرها بخورد را در اختیار ندارند لذا هکرها با آنها کاری ندارند.

ولی این طور نیست چون آنها بر عکس به دنبال قربانیانی می‌گردند که وارد سیستم آنها شوند و با نصب و اجرای برنامه‌های مخرب، به طور غیرمستقیم به سایتها حمله ور شده تا در صورت ردگیری امنیتی، رد شما به عنوان هکر روی اینترنت باقی بماند و سپس دستگیر و مجازات خواهید شد. مجازاتهای سنگینی که در دنیا برای هکرها در نظر گرفته شده

است آنقدر سنگین است که یک هکر باید دهها سال زندانی شود.سوال مهمی که در اینجا باقی می‌ماند اینست که چگونه برای سیستم یا شبکه می‌توان امنیت ایجاد کرد و راهها ینفوذ هکرها را به سیستم یا شبکه بست. از این رو قصد داریم در طی چندین بخش به مقوله امنیت شبکه‌های رایانه‌ای بپردازیم و راههای ایجاد امنیت در یک سیستم رایانه‌ای را توضیح دهیم تا ضمن آگاهی از این موارد، شخصاً بتوانید برای رایانه شخصی خود یک سیستم امنیتی مطمئن بسازید. امنیت در حالت کلی یک امر نسبی است و هیچگاه نمی‌توان ادعا کرد یک سیستم رایانه‌ای مطلقاً امن است و رخنه‌ای برای نفوذ در آن وجود ندارد. از طرفی هر روزه در اخبرا راینه‌ای اطلاع می‌یابیم که حفره‌های جدیدی در سیستم عامل ویندوز پیدا شده است

و این موضوع ما را هراسان می‌کند که به زودی قربانی یکی از حفره‌های ویندوز خواهیم شد!! با این حال آیا دست از کارهای روزمره و اینترنتی خود کشیده‌ایم؟ **خیر** و تاوان سنگین بی‌امنیتی در رایانه شخصی خود را هم بارها پرداخته‌اید و کمتر هم متوجه آن شده‌اید.

- معایب نداشتن امنیت در یک رایانه

یکی از راههای تشخیص وجود ویروس و یا اسبهای تروا در سیستم، کند شدن سیستم عامل به صورت ناگهانی و بدون علت مشخص است که باعث می‌شود هکرها و دیگر سودجویان به ریش ما بخندند و ما هم بدون اطلاع، فقط سیستم عامل [ویندوز، لینوکس، فدورا و ...] رایانه را عوض می‌کنیم و یا کل هارد دیسک را فرمت می‌کنید حال اگر فایلهای

مهمی مثل کپی اسناد فاکتورها برای یک شرکت، برخی عکسها برای یک طراح، فایلهای مالتی مدیا برای میکس کنندگان فیلم و غیره درون هارددیسک باشد آن وقت فاجعه‌ای تمام عیار برای این افراد پیش می‌آید که منجر به زیانهای فراوانی می‌گردد. تمام حرف من و دیگر کارشناسان به شما این است که «***قربانی بودن تا کی***؟ »

پس به فکر چاره باید بود.....ایجاد امنیت رایانه‌ای;

حالا که پی به اهمیت اطلاعات و زیانهای نبود امنیت رایانه‌ای بردید،

آشنایی با راههای ایجاد امنیت می‌تواند دردهای چندین ساله شما را درمان کند به شرط آنکه طبق نسخه دکتر عمل کنید و در این زمینه هم مانند بقیه موارد خود درمانی نکنید چون عواقب این کار، گاهی اوقات به مراتب بدتر از یک حمله ویروسی است.

همانطور که می‌دانیم زندگی روزمره انسانی، در دنیای فیزیکی غالبا با تهدیدهایی 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 نهایتاً 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 به جود آمده است خطرات و تهدید مهاجمان که با بکارگیری روشهای گوناگون در صدد 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 اطلاع رسانی و بخصوص اینترنت مبحث امنیت را میتوان از دو جنبه مورد بررسی قرار داد:

۱ـ امنیت سرویس دهندگان (Servers Security)

۲ـ 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 پایگاه‌هایی 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 ... می‌پردازیم.

با توجه به گسترش زمینه‌های گوناگون استفاده از اینترنت بخصوص تبالات بازرگانی و فعالیت‌های اقتصادی و علاقمندی شدید مهاجمان ;

به این نوع از تخریب‌ها در قدم اول سعی بر آنست که تا به بررسی مباحث مربوط به تهدیدات سرویس دهنگان وب (Web Servers) و انواع آن پرداخته شود.

همچنین ببینید

ـ بررسی انواع تهدیدها

ـ بررسی نقاط ضعف امنیتی شبکه‌های وب

ـ معرفی دو نرم افزار مفید

بررسی آماری حاکی از آن است که تهدیدهای عمومی سیستم‌های سرویس دهنده اینترنتی به شرح ذیل می‌باشد:

کپی‌برداری غیر مجاز و یا سرقت اطلاعات

در این مورد معمولاً 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 معمولاً با ایجاد لایه‌های دسترسی گوناگون امکان استفاده بانک‌های اطلاعاتی را برای مدیران و یا افراد مجاز مهیا نموده‌اند، لذا خطر حضور و نفوذ مهاجمان ودر 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 طبقه بندی 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 پایگاه‌های 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 این اخبار و تغییر اطلاعات سایتهای خبرگزاری‌ها و یا جعل اخبار و نهایتاً شایعه پراکنی از دیگر معضلات این مبحث از امنیت شبکه می‌باشد.

منتشر کردن اطلاعات :

انتشار اطلاعات طبقه‌شده دولتی، شخصی، اقتصادی و ... توسط مهاجمان از دیگر نگرانی‌های ویژه اداره‌کنندگان سیستم‌های اطلاعاتی است.

معمولاً این تهدیدها بر روی سایتهایی دیده می‌شوند که در آنها اطلاعات طبقه‌شدی سیاسی، علمی و اقتصادی و .. نگهداری می‌شوند.

همچون پایگاه اطلاعات مراکز ملی تحقیقات مراکز ملی تحقیقات فضایی و یا بانک‌های اطلاعاتی مربوط به سوابق امنیتی و موارد استراتژیک هر کشور.

تغییر در ساختار ظاهری پایگاه

در بسیار از مواقع دیده شده است، محتوای ظاهری سایتهای اینترنتی که در معرض بینندگان عام قرار دارد 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 عملاً استفاده از محتوای اصلی سایت را برای کاربران عمومی غیرممکن می‌سازند. در برخی موارد هم شاهد Redirect نمودن و یا جابه‌جایی 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 جبران‌ناپذیری 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 سازمانهایی 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 ویروسهای خطرناک و یا موجبات بوجود آمدن مشکلات عدیده برای سرویس دهندگان اطلاعاتی و یا استفاده کنندگان از پایگاه مذکور می‌گردند. امروزه شاید ساده‌ترین روش انتشار ویروس و ارسال همگانی آن جهت تخریب همین مورد باشد.

ایجاد دسترسی تعریف کاربران جدید و و تخریب نامحسوس

در بسیاری از شبکه‌هایی که در آنها با وفور کاربران مواجه هستیم و کنترل فرد فرد 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 موجود دارد.

بدیهی است در این شکل از خرابکاری‌های شبکه‌ای مخربین قادر خواهند بود بصورت نامحصوص کلیه تراکنش‌ها و فرآیندهای گوناگون موجود در سایت را مورد بازبینی قرار داده و از آن سوء استفاده نمایند کهاین عملیات با دسترسی به کد عبور مدیران شبکه به راحتی قاب لانجام است.

این فرآیند برای اداره کنندگان پایگاه‌های اطلاعاتی،

مشکلات عمده ای 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 برخورداند به طور مثال از تهدیدهای مربوط به سیتم‌های اقتصادی آنلاین می‌توان به موارد ذیل اشاره نمود:

۱ـ 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 پرتراکنش پس از نفوذ اقدام به تخلیه حساب و یا جابه‌جایی پول می‌نمایند.

۲ـ انجام معاملات صوری و غیرواقعی بصورت الکترونیکی :

جهت کسب اعتبارمعمولاً اعتبارات بانکی به حسابهایی تعلق می‌گیرد که داری گردش بالای کلان می‌باشند و اساساً 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 استفاده‌گران تامین می‌گردد.

۳ـ گشایش حسابهای بانکی غیرواقعی و انجام تراکنش‌های غیرحقیقی

نفوذگران در این زمینه سعی در ایجاد حسابهای جاری و یا ارزی غیرواقعی می‌نمایند و در آن‌ها همچون بند ۲ سعی درایجاد تراکنشهای مالی و نقل و انتقالات پول می‌نمایند. بدیهی است با در نظر گرفتن غیرواقعی بودن حساب‌ها پیگیری وضعیت صاحب حساب و یا کنترل آن و فرآیند اقتصادی قابل انجام نبوده و براحتی از آن سوء استفاده به عمل می‌آید.

۴ـ تغیر در اسناد مالی و بانکی و جعل :

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

۵ـ سوء استفاده از کارتهای اعتباری و انجام خرید و فروش مجازی :

همانطور که میدانیم استفاده از کارتهای اعتباری رایج، در جوامع مدرن بعنوان راه حلی مناسب جهت انجام فعالیت‌های اقتصادی کوچک و بزرگ بصورت همگانی مورد توجه و استفاده قرار می‌گیرد. بدیهی است در این مورد نیز مهاجمن با جعل و یا تولید شماره کارتهای اعتباری توسط نرم‌افزارهای مربوط 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.

۶ـ ارسال فرم سفارش کالا و یا رزرواسیون الکترونیکی بصورت غیرحقیقی :

در بسیار 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.

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 عدیده‌ای را ینز به همراه داشته است. در حقیقت هر یک از

طرفین (سرویس دهندگان و سرویس گیرندگان) با نگرانی‌های جدی مواجه هستند و در همین راستا، جهت ایمن سازی مراودات خود از یکدیگر انتظاراتی رامطرح می‌نمایند. ایجاد ایمنی و رفع هرگونه تهدید در انجام معاملات 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 صدمه زدن 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 سرویس دهنده و ایمنی مخابراتی از رئوس مطالب مورد توجه می‌باشند.

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 سایت‌ها از امکانات، محاسن و معایب و حفره‌های موجود در سیستم عامل مورد استفاده موجب می‌شود مبحث انجام تنظیمات

صحیح به دقت و درستی انجام نشده و به سادگی، زمینه جهت ورود غیرمجاز مهاجم مهیا شود. بسته نبودن Port های موجود در مجموعه سرویس‌های یک Server به لحاظ امنیتی بسیار خطرناک می‌باشد که در بسیاری از موارد به جهت عدم دقت مسئولین مربوطه، مسیر هموار جهت ورود مهاجمین (Hackers) بوجود می‌آورد.

2) وجود کاستی های فراوان در ساختار سیستم عامل‌ها

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 عاملهای Server دارای نقایص فراوانی به لحاظ حفظ امنیت می‌باشند که بدیهی است با گذشت زمان نقاط ضعفشان شناسایی و رفع می‌گردد.

3) اجازه استفاده از سرویس‌های گوناگون در Server

اجازه استفاده از سرویس‌های گوناگونی همچون TTP,IRC,FTP,TelNet و ... زمینه‌ساز هجوم‌های غیرمجاز فراوان در سرورها می‌باشد. در حقیقت هر یک از درگاههای ورودی مذکور (Port) 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.

4) 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 می‌گردد.

5) 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 برنامه‌های تهیه شده بصورت ASP نمونه‌ای از این موارد می‌باشد.

6) 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 نرم افزارهای Capture و یا ذخیره کننده Log 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. بر اساس 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 Log ثبت می‌شود و با کنترل و بررسی آن‌ها می‌توان اقدامات امنیتی و بازدارنده 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 مذکرو را افزایش می‌دهد.

7) 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 عملیات‌ها انجام شده و درصد محدود بروز خطر برای سرویس دهندگان موجب عدم کنترل عملکرد و تراکنش‌های اقتصادی کاربر می‌گردد. لذا هیچگاه نباید به عملکرد کاربران یک سایت اعتماد کامل داشت.

8) عدم وجود روشهای مناسب شناسایی کاربر

یکی دیگر از نقاط ضعف سرویس‌دهندگان عدم استفاده از روشهای مناسب شناسایی کاربران مجاز به استفاده از امکانات سیستم می‌باشد.

امروزه شایدعمده‌ترین روش شناسایی کاربر نام شناسایی (User Name) و کلمه عبور (Password) او باشد که براساس آمار یکی از مهمترین راههای سوء استفاده از سایت: به دست آوردن و استفاده از مورد ذکر شده می‌باشد.

در حقیقت نرم افزارهایی 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 می‌گیرند که خود موجب کاهش یورشهای احتمالی می‌گردد.

9) عدم استفاده از تدابیر امنیتی مناسب و نرم افزارهای Firewall و Proxy

با توجه به موارد ذکر شده در مباحث نقاط ضعف سیستم‌های عامل و پروتکل‌ها، وجود و استفاده از شیوه‌های نرم افزاری بازدارنده بسیار مورد توجه قرار گرفته است.

ایجاد و تهیه نرم افزارهایی که با لفظ دیواره آتش Firewall شناخته می‌شوند و نهایتاً نصب و استفاده از آن‌ها بر روی سرور و یا در مسیر حرت اطلاعات موجب کاهش احتمال یورش و نفوذ به حفره‌های موجود می‌گردد.

در حقیقت این نوع نرم افزارها بصورت یک سد محکم و یا یک فیلتر در مسیر کاربران واقع می‌گردد 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 می‌گردد تا شرکت‌های نرم افزاری در کوتاهترین زمان ممکن در بروز رسانی و رفع نواقص Firewall های خود اقدام نمایند و آنها را در مقابل تهدیدها آماده سازند.

10) 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 میهباشد. در حقیقت شیوه‌ای مرسوم که توسط مهاجمان مورد استفاده قرار می‌گیرد،

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 ویروس یاب و Firewall های مناسب از این نوع تهدیدها جلوگیری می‌نماید.

11) عدم محافظت از اطلاعات حساس

بسیاری از سرویس دهندگان جهت حفظ اطلاعات حساس خود اقدام به مخفی سازی encryption می‌نمایند. البته شکل ساده و تئوریکال قضیه، دور از دسترس قرار دادن اطلاعات است .

ولیکن روشهای گوناگون جهت انجام این مهم مورد استفاده قرار می‌گیرد 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 برابر حفره‌های عمومی موجود در سایت‌های وب داشت ولیکن طرح این سؤال که:

«چرا دیگران علاقمند به نفوذ و خرابکاری در سایت مطلوب ما هستند؟» بتواند درشناخت عوامل گوناگون و مطرح برای مهاجمین یاری‌رسان باشد. در نهایت همواره باید به خاطر داشت:

«ایمنی مطلوب امروز همواره بهتر از ایمنی کامل فرد است».

خلاصه اطلاعات کارآموزی

در طی این دوره کارآموزی با اطلاعاتی از جمله:

ـ اجزای شبکه‌های کامپیوتری مانند؛

Patch Panel-

Rooter-

Rack-

Hub-

UPS-

VPN Line-

انواع کابل‌ها و کیوسک

HP Server-

IRCERT-

نحوه انتخاب رمز عبور

اصول مهم امنیتی شبکه

و همچنین امنیت اینترنتی و مباحث مربوط به آن آشنا شدم.

و این دوره برای بنده تجربه‌ای گرانبها بود.

منابع :

مجله علمی ساصد

شماره گان

۵۷۵-۵۷۶-۵۷۷-۵۷۸-۵۷۹-۵۸۰