۱ امنیت و مدیریت ریسک

۱/۱ ریسک

احتمال رخداد و میزان تاثیر آن در صورت بروز است که از حاصلضرب احتمال در زیان حاصله در اثر بروز قابل محاسبه می باشد.

ریسک = احتمال رخداد * زیان حاصله

۱/۲ مدیریت ریسک

یکی از بحث های مهم مدیریتی, مدیریت ریسک است چرا که یک سیستم بدون هرگونه ریسک یک سیستم ایده آل است یا ممکن نیست و یا عملا هزینه انجام آن به اندازی زیاد است که انجام آن را غیر ممکن می سازد. در نتیجه هر مدیری باید قبل از اعمال ابزار های امنیتی اقدام به تخمین مسائل مختلف آن کند.

۱/۳ روش های تعامل با ریسک

عمومن چهار روش یا رویکرد جهت تعامل با ریسک وجود دارد:

۱/۳/۱ پذیرفتن ریسک

یا چشم پوشی و صرفنظر کردن از آن و ادامه بدون توجه به آن. در این روش عمومن پش از وقوع مشکل امنیتی اقدام به حل آن انجام می گردد و سیاست درمان به جای پیشگیری است.

۱/۳/۲ اجتناب از ریسک

در این روش اصولا به صورت علت و معلول به قضیه نگاه می شود. اگر عاملی باعث ریسک شود, خود عامل حذف شده و در نتیجه ریسک نیز برطرف می شود. بعنوان مثال ریسک در سرویس ایمیل و در نتیجه حذف سرویس ایمیل.

۱/۳/۳ محدود کردن و کنترل ریسک

در این روش سعی می شود که ریسک کنترل شود و دامنه عملکرد آن محدود گردد بطوریکه اگر مشکل پیش آمد یا دامنه اثر آن محدود و یا به راحتی قابل رفع باشد. مثل محدود کردن سرویس ایمیل به نداشتن پیوست فایل های اجرایی

۱/۳/۴ انتقال ریسک

در این روش مشکلات ناشی از بروز ریسک به یک مجموعه خارجی منتقل می شود بطوریکه آن مجموعه مسولیت رفع یا حل مشکل و یا جبران خسارت ناشی از وقوع آن را بر عهده بگیرد. یکی از روش های متداول در این مورد استفاده از خدمات بیمه می باشد.

۲ پروتکل های شبکه

برای تحلیل و فهم روش هایی که یک نفوذگر با بکارگیری آنها به شبکه حمله می کند باید یک دانش پایه از تکنولوژی های شبکه داشته باشیم تا مکانیزم های حملات را بهتر درک نماییم. در این راستا آشنایی با مجموعه قوانین و مقررات موجود در شبکه ها مفید خواهد بود.

برای جلوگیری از طراحی شبکه ها به صورت سلیقه ای و به تبع آن پیچیده تر شدن ارتباطات شبکه ای, سازمان جهانی استاندارد مدل ۷ لایه ای را برای ارتباطات شبکه ای ارائه نمود که این لایه هاعبارتند از:

۱. فیزیکی Physical
۲. اتصال داده Data Link
۳. شبکه Network
۴. انتقال Transport
۵. جلسه Session
۶. نمایش یا ارائه Presentation
۷. کاربرد Application

۲/۱ وظایف لایه های مختلف پروتکل OSI:

۲/۱/۱ لایه فیزیکی

وظیفه اصلی در این لایه انتقال بیت ها به صورت سیگنال های الکتریکی و ارسال ان بر روی کانال ارتباطی است. واحد اطلاعات در این لایه بیت است و برخی از پارامتر هایی که در این لایه مد نظر قرار می گیرند عبارتند از: (الف) ظرفیت کانال ارتباطی (ب) نرخ انتقال اطلاعات

۲/۱/۲ اتصال داده با پیوند داده

در این لایه با استفاده از مکانیزم های کشف و کنترل خطا فرآیندی صورت می گیرد تا اطلاعات بدون خطا و مطمئن به مقصد برسد. در این لایه اشکالات کشف شده اصلاح می گردد و در صورتیکه نتوان اطلاعات را اصلاخ نمود تدابیری اتخاذ می گردد تا اطلاعات مجددا ارسال شود. همچنین یکی دیگر از وظایف این لایه کنترل جریان ترافیک است و سعی می شود هماهنگی بین فرستنده و گیرنده کند بوجود آید. واحد اطلاعاتی در این لایه Frame است.

۲/۱/۳ لایه شبکه

از آنجایی که بین دو ماشین در شبکه مسیر های گوناگونی وجود دارد این لایه وظیفه دارد مسیر هدایت اطلاعات به مقصد درست را تعیین نماید. در این لایه تدابیری اندیشیده می شود تا از ازدحام و تداخل جلوگیری شود. واحد اطلاعاتی در این لایه Packet است.

۲/۱/۴ لایه انتقال

در این لایه بر اساس خدمات لایه های زیرین یک سرویس انتقال بسیار مطمئن ارائه می شود. همچنین تقسیم پیام های بزرگ به بسته های اطلاعاتی کوچک تر و بازسازی بسته هایاطلاعاتی و تشکیل یک پیام کامل از وظایف این لایه محسوب می شود. واحد اطلاعاتی در این لایه Segment است.

۲/۱/۵ لایه جلسه

وظیفه این لایه فراهم آوردن شرایط یک نشست (مانند ورود به سیستم از راه دور) می باشد. برخی از این وظایف عبارتند از: برقراری و مدیریت یک جلسه یا نشست, مشخص نمودن اعتبار پیام ها و اتمام جلسات و ...

۲/۱/۶ لایه نمایش

در این لایه وظایفی مانند فشرده سازی فایل ها, رمزگشایی و رمزنگاری اطلاعات, تبدیل کد های مختلف به یکدیگر و بعبارتی تمامی کارهایی که مربوط به چگونگی نمایش اطلاعات می باشد در این لایه انجام می شود.

۲/۱/۷ لایه کاربرد

در این لایه استاندارد مبادله پیام بین نرم افزار هایی که در اختیار کاربر بوده و به نحوی با شبکه در ارتباط هستند تعریف می شوند. این لایه شامل استاندارد هایی نظیر: انتقال نامه های الکترونیکی, دسترسی به بانک های اطلاعاتی از راه دور, مدیریت شبکه و مواردی این چنینی می باشد.

۲/۲ پروتکل TCP/IP

این مدل در کتاب های استاندارد دارای ۴ لایه می باشد که امروزه با توجه به مباحث امنیتی و تفکیک وظایف برخی از این پروتکل ها به تعداد این لایه ها اضافه گردیده است.

۲/۳ وظایف پروتکل TCP/IP

۲/۳/۱ لایه میزبان به شبکه یا Network Interface

در این لایه استاندارد های سخت افزاری و نرم افزاری و پروتکل های شبکه تعریف می شود. این لایه با مسائل فیزیکی, الکتریکی, مخابراتی, چگونگی عملکرد رابطه های شبکه و مدارد این چنینی درگیر است. این لایه وظیفه دارد هماهنگی بین این شبکه های مختلف را انجام دهد. پروتکل های لایه اول می توانند مبتنی بر ارسال بیت یا بایت باشند.

۲/۳/۲ لایه شبکه

مهم ترین وظیفه ی این لایه عبارتست از هدایت بسته ها از مبدا تا مقصد می باشد. ضمنن در این لایه سرویسی به منظور سالم رسیدن یا نرسیدن اطلاعات به مقصد وجود ندارد و به همین دلیل لایه های بالاتر وظایف این چنینی را بر عهده خواهند داشت.

۲/۳/۳ لایه انتقال

این لایه ارتباط ماشین های انتهایی را برقرار می کند و با سرویس هایی که ارائه می نماید یک ارتباط اتصال گرا(Connection Oriented [منظور از اتصال گرا و بدون اتصال مانند مخابرات و پست است]) و مطمئن برقرار خواهد شد.

۲/۳/۴ لایه کاربرد

در این لایه بر اساس خدمات لایه های زیرین سرویس های سطح بالایی برای ایجاد برنامه های کاربردی ارائه می شود که این خدمات در غالب پروتکل های استانداردی همانند موارد زیر در اختیار کاربران قرار می گیرد.

- پروتکل انتقال فایل یا FTP
- سرویس مدیریت پست الکترونیکی
- پروتکل انتقال صفحات فوق متنی یا HTTP

۳ فایروال ها

شبکه های امروزی از المان های مختلف تشکیل شده اند که بطور کلی می توان آنها را به قسمت های ذیل تقسیم کرد:

- تجهیزات غیر فعال (Passive):
  شامل کابل های ارتباطی, وک ها, پنل ها, و ... این المان ها برق مصرف نمی کنند و بستر مناسب برای سایر المان های شبکه فراهم می کنند.

- تجهیزات فعال (Active):
سوئیچ ها (تعدادی درگاه برای اتصال به درگاه شبکه فراهم می کنند), مسیر ده ها(مسیر دهی بسته های IP از داخل سازمان به بیرون سازمان و بر عکس را بر عهده دارند), سرور ها, تجهیزات امنیتی و ...

شبکه ها را می توان به لحاظ منطقی و با توجه به سطح امنیتی به طور کلی به سه قسمت تقسیم کرد:

- شبکه عمومی Public Network: همان شبکه بیرونی سازمان یا شرکت می باشد که اینترنت از این نوع است و در این نوع از شبکه امنیت حد اقل می باشد.
- شبکه نیمه خصوصی Semi Private Network (Intranet): بخشی از شبکه سازمان است که نیاز به دسترسی به آن از خارج سازمان وجود دارد. این نوع از شبکه معمولا دارای سطح امنیت متوسط است.
- شبکه خصوصی یا Private Network: شبکه داخلی سازمان که فقط از داخل سازمان قابل دسترسی است و حداکثر امنیت در آن وجود دارد.

فایروال ها مانعی هستند که ترافیک باید از آن عبور نماید. سیاست امنیتی فایروال, مشخص می کند چه ترافیکی مجار است از مسیری عبور کند. فیروال ها می توانند از ابزار های موثری برای حفاظت از سیستم محلی یا شبکه ای از سیستم ها در مقابل خطرات امنیتی مبتنی بر شبکه باشند.

ویژگی های فایروال ها:

- تمام ترافیک از داخل به خارج, و برعکس باید از فایروال عبور کند.
- فقط ترافیک مجاز که توسط سیاست امنیتی محلی تعریف می شود, اجازه عبور دارد.
- خود فایروال ها در مقابل رخنه کردن ایمن هستند.

فایروال ها به لحاظ نحوه عملکرد و امکاناتی که دارند به سه نوع کلی تقسیم می شوند:

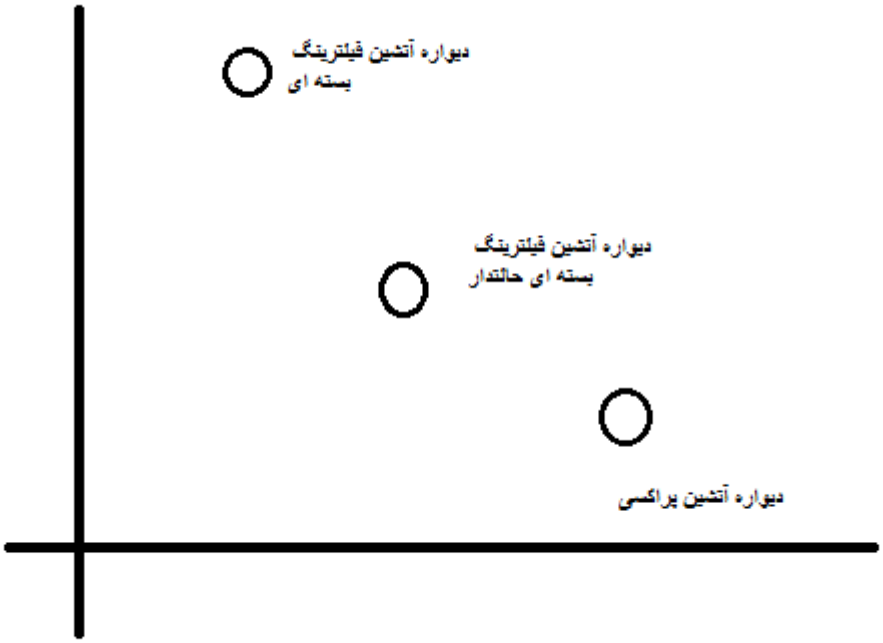
- دیواره آتشین فیلترینگ بسته ای (Packet Filtering Firewalls)

در این دیواره های آتشین که در لایه ۳ مدل OSI عمل می کنند, نحوه عملکرد با توجه به یک مجموعه قوانین مشخص می شوند

- دیواره های آتشین فیلترینگ بسته ای مبتنی بر حالت (Stateful Packet Filtering)

این دیواره های آتشین در لایه ۴ عمل می کنند و مفهوم اتصال را می فهمند و برای انواع اتصال ها تمرکز دارند. در مقایسه با نوع اول کندتر, پر هزینه تر, و پیچیدگی مدیریت بالاتری دارند.

- دیواره های آتشین پراکسی (Proxy Firewalls)
  - این نوع دیواره های آتشین در لایه ۷ مدل OSI عمل می کنند و به همین جهت به آنها دیواره های آتشین لایه کاربرد نیز می گویند.
  - این نوع دیواره های آتشین کندترین, گرانترین, و پیچیده ترین نوع به لحاظ ساختار و مدیریت هستند.



۳٫۱ معایب عمومی فایروال ها:

علیرغم فوایدی که دیواره های آتش برای ما دارند, معایبی نیز دارند:

۱. افزایش هزینه
در صورت اضافه کردن دیواره آتش ممکن است به سخت افزار یا نرم افزار جدیدی نیاز باشد.
۲. وابستگی به یک نقطه حساس:
معمولا موقعیت فایروال ها حساس بوده و در صورت ایجاد مشکل, کل خدمات شبکه تحت تاثیر قرار می گیرد.
۳. امکان ایجاد Back Door: چنانچه فایروال ها توسط نفوزگران مورد استفاده قرار بگیرند, خرابکاران مکانیزم هایی را در پشت فایروال ایجاد می کنند که مجددا می توانند از طریق آنها وارد شبکه شوند که می توانند در قالب نصب برنامه باشند.
۴. اگر در تنظیمات فایروال ها اشتباهاتی اعمال شود این به معنی قطع گروهی از سرویس ها و خدمات شبکه خواهد بود و میتواند خسارت زیادی وارد کند.

۴ رمزنگاری

برخلاف بسیاری از مباحث امنیتی که در آن میزان امن سازی بطور دقیق مشخص نیست, در رمز نگاری به دلیل ماهیت ریاضی آن ضریب امنیتی الگوریتم رمز نگاری قابل محاسبه و ارزیابی است.

برخی اصطلاحات در حوزه رمز نگاری:

- Plain Text: یا متن خام گفته شده که همان متن یا داده رمز نشده می باشد.
- Cipher Text: متن یا داده رمز شده که بطور مستقیم قابل فهم و خواندن نباشد.
- Decryption: به عملیات تبدیل Plain text به Cipher را گویند.
- Encryption: به عملیات تبدیل Cipher به Plain Text را گویند که عموما به کمک یک کلید و یک الگوریتم رمزنگاری انجام می شود.
- آنالیز رمز: به تلاش برای رمز گشایی بدون داشتن کلید و یا الگوریتم رمز با استفاده از روش هایی مثل فرکانس تکرار الگوهای رمز شده, روش های آنالیز آماری و آنالیز معنایی گویند.
- حمله Brute-Force-Attack: حمله ای با هدف رمز گشایی که در آن کلیه حالات ورودی آزمایش شده تا نهایتن رمز کشف شود را گویند. یک الگوریتم خوب رمزنگاری الگوریتمی است که تعداد حالات نیاز به تست خیلی زیاد باشد.

۴/۱ رمز نگاری جایگزینی یا Substitution Cipher:

یکی از ایده های رایج رمز نگاری جابجا کردن کاراکتر های اصلی با کاراکترها و یا عبارات دیگر جایگزین می کنند. یکی از روش های معروف در این زمینه روش سزار می باشد که در آن از یک جدول متناظر استفاده می شد به این ترتیب که هر کاراکتر با کاراکتر متناظر آن از لیست الفبا جایگزین می شد مانند زیر:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

حال عبارت زیر را رمز گذاری کنید:

CRYPTOGRAPHY

۴/۲ Vigenere Cipher

این الگوریتم از یک کلید انتخابی جهت کد گذاری استفاده می کند. به حروف A تا Z عددی از یک تا ۲۶ اختصاص می دهد. جهت کد گذاری عدد کاراکتر اصلی را با عدد کاراکتر کلید جمع کرده و کاراکتر متناظر حاصل جمع را پیدا می کند و در صورتی که حاصل جمع از ۲۶ بیشتر شود ۲۶ را از آن کسر میکند:

Plain Text: CRYPTOGRAPHY

KEY: WHITEWHITEWH

Cipher Text: …

در این روش از آنجا که کلید می تواند هر چیزی باشد روش خوبی می باشد اما با استفاده از روش های آنالیز رمز مثل بررسی آماری می توان آن را رمز گشایی کرد.

۴/۳ ابزار های اصلی رمزنگاری

۴/۳/۱ تولید اعداد تصادفی

در رمز نگاری اصولا نیاز داریم که کلید ها از اعداد تصادفی انتخاب شوند تا مهاجمان نتوانند با حدس زدن کلید ها اقدام به رمزگشایی کنند لذا به یک مولد مناسب جهت تولید اعداد تصادفی بسیار مهم است. دو روش برای تولید اعداد تصادفی در سیستم های کامپیوتری وجود دارند:

- اتفاده از توابع ریاضیاتی: که در این روش با یک فرمول ریاضی اقدام به تولید اعداد تصادفی می شود که معمولا از یک عدد تصادفی در این فرمول استفاده می شود.
- استفاده از یک پدیده تصادفی از خارج کامپیوتر که با بکار گیری آن با یک تابع ریاضیاتی اعداد تصادفی تولید می کنند. مانند: حرکات موس, شماره سریال قطعات متصل به سیستم, کلید های فشرده شده و ...

۴/۳/۲ رمزنگاری متقارن

در این رمزنگاری از یک کلید مشترک و مشابه برای زمان رمز کردن و رمزگشایی استفاده می شود. روش هایی را که توضیح دادیم از این نوع هستند مانند .Vigenere

هرچند که در این روش اگر کلید را درست انتخاب کنیم تعداد حالات ها آنقدر زیاد خواهد بود که سالیان زیادی طول می کشد تا مهاجمان بتوانند رمزگشایی کنند ولی با سرعت تکنولوژی و سیستم های کامپیوتری جدیدتر به راحتی قابل باز شدن هستند.

۴/۳/۲/۱ *انواع الگوریتم های متقارن (ادامه)*

- رمز جریانی Stream Cipher

بر این روش بر اساس جریان بایت های ورودی و یک کلید و با توجه به اطلاعات قبلی وارده داده به صورت سریال رمز نگاری می شود. این روش چون به صورت جریان اطلاعات ورودی کار می کند نیاز به طول مشخصی از داده ها جهت انجام عملیات رمز نگاری ندارد و اطلاعات ورودی را با هر طولی بدون نیاز به اضافه کردن بیت ها رمز می کنند.

- رمز بلوکه ایBlock Cipher

در این روش اطلاعات به صورت بلوک هایی با اندازه مشخص وارد الگوریتم شده و با یک کلید مشترک برای کد و دیکد کردن عملیات انجام می شود.

یک عیب الگوریتم این است که اگر یک بلوکه اطلاعات مشابه مستمرا تکرار شود مثلا یک جواب Yes که در یک بلوک ارسال شده این بلوک های مشابه, بلوک های کد شده مشابه تولید می کنند و تکرار آنها در ترافیک در حال تبادل احتمال تشخیص رمز اصلی بالا می رود.

۴/۳/۳ رمزنگاری نامتقارن Asymmetric Cryptocraphy

روش های رمز نگاری نا متقارن دارای ویژگی های عمومی زیر هستند:

- از یک کلید A برای رمز کردن و یک کلید B برای رمز گشایی استفاده میشود. به کلید رمز کردن A کلید عمومی یا Public Key و به کلید رمزگشایی B کلید خصوصی یا Private Key می گویند.
- خاصیت اصلی الگوریتم نامتقارن این است که اطلاعات تنها با کلید عمومی قابل کد شدن است که کلید عمومی در اختیار همه قرار میگیرد ولی تنها کلید خصوصی است که میتواند اطلاعات را رمزگشایی کند.

مراحل انجام الگوریتم رمزنگاری نامتقارن بصورت زیر می باشد:

۱. A یک کلید عمومی رمز کردن و یک کلید خصوصی تولید میکند و کلید عمومی را منتشر کرده و کلید خصوصی را نزد خود نگه می دارد.
۲. B کلید عمومی A را دریافت کرده و یک کلید متقارن برای تبادل اطلاعات با A تولید می کند و آن را با کلید عمومی A کد کرده برای A می فرستد.
۳. A کلید رمز شده با رمز عمومی خود را دریافت کرده با کلید خصوصی خود آن را رمز گشایی می کند و کلید متقارن را بدست می آورد. (تنها A است که میتواند کلید رمز شده را رمزگشایی کند)
۴. A و B هردو کلید متقارن در اختیار دارند و کلید به صورت امن تبادل شده است حال می توانند از این کلید متقارن جهت رمز نگاری استفاده شود.

۴/۳/۴ توابع Hash

یکی از ابزار های مهم رمز نگاری می باشد که دارای خصوصیات زیر است:

- توابعی هستند که اطلاعات با طول متغیر را دریافت کرده و یک اطلاعات با طول کوتاه که اصطلاحن Digest نامیده میشود تولید می کنند.
- توابع عمومن در زمان کمی عمل می کنند و سرعت اجرای آنها بسیار بالاست.
- به لحاظ عملیاتی طوری هستند که هیچ دو داده متفاوت Digest مشابه تولید نمی کنند.

برخی از کاربرد های متداول توابع Hash:

- ذخیره کردن کلمات عبور
- از توابع هش می توان برای پیاده سازی مکانیزم جامعیت اطلاعات (Integrity) استفاده کرد

۵ امضای دیجیتال

۶ پروتکل های امنیتی

۷ امنیت در سرویس های وب

۸ نفوذگران

یک مساله امنیتی مهم برای سیستم های شبکه ای, مهاجم یا تجاوز توسط کاربران یا نرم افزار است. تجاوز کاربران می تواند به شکل ورود غیر مجاز به ماشین یا در مورد کار غیر مجاز, به دست آوردن امتیاز ها یا کارایی فغالیت ها خارج از مجوز هایش باشد. سه دسته از نفوذگران عبارتند از:

- **نقاب زنان**: شخصی که مجوز استفاده از کامپیوتر را ندارد و از کنترل های دستیابی سیستم عبور می کند تا خودش را حساب کاربر قانونی جلوه دهد.
- **Misfeasor**: کاربر قانونی که به داده ها, برنامه ها, یا منابعی دسترسی دارد که این دستیابی برای او مجاز نیست یا برای این دستیابی ها مجاز هست ولی از امتیاز های خود بد استفاده می کند.
- **کاربر مخفی**: شخصی که کنترل سرپرستی را به سرقت می برد و از این کنترل برای فرار از نظارت و کنترل های دستیابی یا متوقف کردن کلکسیون نظارت استفاده می کند.

نقاب زنان احتمالن خارج از سیستم هستند. Misfreasor معمولن داخلی هستند و کاربر مخفی می تواند داخل یا خارج سیستم باشد.

هدف نفوذگر, دستیابی به سیستم با افزایش حدود مجوز های دستیابی در سیستم است. معملن این کار مستلزم این است که نفوذگر اطلاعاتی را به دست می آورد که می بایست حفاظت شوند. در بعضی موارد این اطلاعات به شکل کلمه عبور کاربر است. با دانستن کلمه عبور بعضی از کاربران, نفوذگران می تواند وارد سیستم شود و تمام مجوز های مخصوص کاربر را قانونی امتحان کند.

سیستم باید فایلی را نگهداری کند که یک کلمه عبور را به هر کاربر مجاز نسبت دهد. اگر چنین فایلی بدون حفاظت ذخیره شود, دستیابی به آن و پی بردن به کلمه های عبور آسان است. فایل کلمه عبور باید به یکی از روش های زیر حفاظت شود:

- **تابع یک طرفه یا برگشت ناپذیر**: سیستم فقط مقدار یک تابع را بر اساس کلمه عبور کاربر ذخیره می کند. وقتی کاربر کلمه عبور را ارائه می کند, سیستم آن کلمه عبور را تبدیل م یکند و آن را با مقدار ذخیره شده مقایسه می نماید. در عمل, سیستم معمولن تبدیل یک طرفه را اجرا می کند که در آن, کلمه عبور برای تولید کلید برای تابع یک طرفه به کار می رود و در آن خروجی با طول ثابت تولید می کند.
- **کنترل دستیابی**: دستیابی به فایل کلمه عبور برای یک یا چند حساب مهیا است.

بنا بر گزارشات داده شده, نفوذگران به اشکال مختلفی سعی در بدست آوردن رمز های عبور کاربران هستند که تعدادی از مهمترین آنها عبارتند از:

- تمام کلمه های عبور یک تا سه کاراکتری را امتحان می کنند.
- کلمه های موجود در دیکشنری آنلاین سیستم با لیستی از کلمه های عبور احتمالی
- اطلاعات راجع به کاربران از جمله نام والدین, تاریخ تولد و ...
- شماره تلفن کار, شماره های اجتماعی همچون کد ملی و ...
- استراق سمع بین کاربر راه دور و سیستم میزبان

تشخیص نفوذگری

ناگزیر بهترین سیستم جلوگیری از نفوذگری شکست خواهد خورد. خط دوم دفاعی سیستم, تشخیص نفوذگری است و در سال های اخیر موضوع موضوع تحقیقات مهمی است. این موضوع به دلیل چندین نکته, از جمله موارد مهم است:

- اگر نفوذگری سریعن تشخیص داده شود, نفوذگر شناسایی شده قبل از انجام هر نوع عمل تخریبی یا به خطر افتادن داده ه, می تواند از سیستم خارج شود. حتی اگر نفوذ گری در زمان شروع دتشخیص داده نشود, هرچه زودتر تشخیص داده شود, میزان خرابی کمتر خواهد بود و ترمیم سیستم بهتر صورت می گیرد.
- سیستم تشخیص نفوذگری موثر, می تواند به عنوان جلوگیری کننده ی نفوذگری عمل کند.
- تشخیص نفوذگری, برای جمع آوری داده ها درباره تکنیک نفوذگری به کار می رود. این اطلاعات می توانند امکان جلوگیری از نفوذگری را تقویت کنند.

روش های زیر را برای تشخیص نفوذگری مطرح کرده اند:

- **تشخیص نا هنجاری آماری**: شامل کلکسیونی از داده ها است که به رفتار کاربران مجاز در یک دوره ی زمانی مربوط می شود. سپس تست های آماری به رفتار مشاهده شده اعمال می شوند تا اطمینان حاصل شود که رفتار مربوط به کاربر مجاز نیست.
- **تشخیص قانونی**: شامل تلاش برای تعریف مجمو عه ای از قوانین است که می تواند تصمیم بگیرد که رفتار مربوط به نفوذگر است.

۹ نفوذگر ها و نرم افزار های مخرب

نرم افزار مغرض نرم افزاری است که بطور عمدی در سیستم قرار داده می شود تا اهداف مضری را برآورده کند.

ویروس قطعه نرم افزاری است که می تواند با اصلاح سایر برنامه ها به آنها ضربه بزند و در انواع گوناگون زیر می باشد:

- ویروس مقیم در حافظه
- ویروس سکتور راه انداز
- ویروس مخفی
- ویروس چند شکلی
- ویروس فراشکلی

حمله انکار سرویس DoS: تلاش برای جلوگیری از کاربران قانونی سرویس, از به کارگیری آن سرویس است.

نرم افزار های مغرض می توانند به دو دسته تقشسم شوند: آن هایی که نیاز به برنامه میزبان دارند و آنهایی که مستقل عمل می کنند. اولی اساسا بخشی از برنامه ها هستند که نمی توانند مستقل از برنامه کاربردی واقعی, سودمند یا سیستم عامل وجود داشته باشند. دومی برنامه های مستقلی هستند که می توانند توسط سیستم عامل زمانبندی و اجرا شوند. برنامه های zombie و کرم ها نمونه هایی از این دسته اند.

Backdoor: یک نقطه ورودی سری به برنامه ایست که اجازه می دهد افرادی که از در پشتی آگاه هستند بدون عبور از رویه های امنیتی عادی, به سیستم دستیابی داشته باشند. برنامه نویسیان چندین سال به طور قانونی از backdoor ها برای اشکال زدایی و تست برنامه ها استفاده کردند. این کار معمولن وقتی انجام می شود که برنامه نویس در حال نوشتن برنامه ایست که دارای رویه احراز هویت, یا تنظیمات طولانی است که از کاربر می خواهد مقادیر مختلفی را وارد نماید تا آن برنامه را اجرا کند. Backdoor ها وقتی خطرناک می شوند که برنامه نویسیان با استفاده از آن هادستیابی های غیر مجاز داشته باشند. پیاده سازی کنترل سیستم عامل برای backdoor ها دشوار است چون اندازه گیری امنیتی باید بر فعالیت های توسعه برنامه و به هنگام سازی نرم افزار تاکید کنند که عملن مشکل است.

برنامه ایست که دستیابی غیر مجاز به عملکردها را امکان پذیر می سازد.

بمب منطقی: یکی از قدیمی ترین انواع خطرات رایانه ایست و در واقع کدی است که در برنامه قانونی تعبیه می شود تا در اثر واقع شدن شرطی منفجر شود و دست به عملی بزند مثل ایجاد مشکل در صورت مواجه شدن با تاریخ خاصی. وقتی بمب منطقی منفجر شد, ممکن است داده ها را تغییر دهد یا کل داده یا فایل را حذف نماید, ماشین را متوقف سازد یا خرابی های دیگر را انجام دهد.

اسب های تراوا:یک برنامه مفید یا رویه فرمان است که شامل کد مخفی است و وقتی که فراخوانی می شود کار های مضر ناخواسته ای را انجام می دهد. برنامه های اسب تراوا می توانند برای انجام کار ها به طور غیر مستقیم به کار روند که کاربر غیر مجاز نمی تواند به طور مستقیم آن ها را انجام دهد. به عنوان مثال برای دستیابی به فایل های کاربران دیگر در سیستم اشتراکی, کاربر می تواند برنامه اسب تراوا را ایجاد کند که وقتی اجرا می شود, مجوز های فایل کاربر فراخوان را تغییر می دهد به طوری که این فایل ها توسط کاربران دیگر قابل خواندن است. انگیز متداول دیگر برای اسب تراوا تخریب داده هاست. بنظر می رسد که برنامه کار مفیدی را انجام می دهد (مانند ماشین حساب) اما ممکن است فایل های کاربر را حذف نماید.

Zombie: برنامه ایست که به طور سری یک کامپیوتر متصل به اینترنت را تحویل می گیرد و سپس با استفاده از آن حملاتی را تدارک می بیند که ردیابی خالق Zombie را دشوار می سازد. Zombie روی صد ها کامپیوتر متعلق به شخص ثالث غیر مشکوک قرار می گیرند و با ایجاد ترافیک زیاد استرنت, بر وب سایت علبه می کنند.

۱۰ ماهیت ویروس ها

کرم برنامه ایست که می تواند خودش را تکثیر کند و کپی هایی را از طریق اتصال های شبکه ای به کامپیوتر های دیگر بفرستد.

۱۱ امنیت برنامه های وب

هر برنامه كامپيوتري كه براي اجراء در محيط شبكه، طراحي و پياده سازي مي گردد ، مي بايست توجه خاصي به مقوله امنيت داشته باشد .برنامه هاي وب از زيرساخت شبكه (اينترانت ، اينترانت) براي ارائه خدمات خود به كاربران استفاده نموده و لازم است نحوه دستيابي كاربران به اين نوع از برنامه ها ، كنترل، و با توجه به سياست هاي موجود ، امكان دستيابي فراهم گردد .در ابتدا مي بايست كاربران شناسائي و پس از تائيد هويت آنان ، امكان دستيابي به برنامه با توجه به مجوزهاي تعريف شده ، فراهم گردد.

Authentication، فرآيندي است كه بر اساس آن كاربران شناسائي مي گردند و Authorization . ، فرآيند اعطاي دستيابي به كاربران با توجه به هويت آنان مي باشد . با تلفيق Authentication وAuthorization ، امكان ايمن سازي برنامه هاي وب در مقابل افراد مزاحم و غير مجاز ، فراهم مي گردد.

بطور كلی از سه روش عمده به منظور شناسائي كاربران و اعطاي مجوزهاي لازم در جهت دستيابي و استفاده از يک برنامه وب ، استفاده مي نمايد:

Windows Authentication

شناسائي و تائيد كاربران بر اساس ليست كاربران تعريف شده بر روي سرويس دهنده انجام خواهد شد. در ادامه با توجه به مجوزها و امتيازات نسبت داده شده به هر Account ، امكان دستيابي و يا عدم دستيابي به منابع موجود بر روي سرويس دهنده ، فراهم مي گردد.

Forms Authentication

در روش فوق ، كاربران به يک فرم وب Logon ، هدايت مي گردند . در ادامه ، اطلاعات مربوط به نام و رمز عبور آنان اخذ و فرآيند شناسائي و تائيد بر اساس يک ليست كاربران و يا از طريق يک بانک اطلاعاتي كه برنامه حمايت مي نمايد ، انجام خواهد شد.

Authentication Passport

در روش فوق ، كاربران جديد به يک سايت كه توسط مايكروسافت ميزبان شده است ، هدايت مي گردند .پس از ريجستر شدن كاربران ، امكان دستيابي آنان به چندين سايت ، فراهم خواهد شد.

۱۲ استراتژی حفاظت از اطلاعات در شبکه های کامپیوتری

اطلاعات در سازمان ها و موسسات مدرن، بمنزله شاهرگ حياتي محسوب مي گردد . دستيابي به اطلاعات و عرضه مناسب و سريع آن، همواره مورد توجه سازمان هائي است كه اطلاعات در آنها داراي نقشي محوري و سرنوشت ساز است . سازمان ها و موسسات مي بايست يک زير ساخت مناسب اطلاعاتي را براي خود ايجاد و در جهت انظباط اطلاعاتي در سازمان خود حركت نمايند . اگر مي خواهيم ارائه دهنده اطلاعات در عصر اطلاعات بوده و صرفا" مصرف كننده اطلاعات نباشيم ، در مرحله نخست مي بايست فرآيندهاي توليد ،عرضه و استفاده از اطلاعات را در سازمان خود قانونمد نموده و در مراحل بعد ، امكان استفاده از اطلاعات ذيربط را براي متقاضيان (محلي،جهاني) در سريعترين زمان ممكن فراهم نمائيم . سرعت در توليد و عرضه اطلاعات ارزشمند ، يكي از رموز موفقيت سازمان ها و موسسات در عصر اطلاعات است . پس از ايجاد انظباط اطلاعاتي، مي بايست با بهره گيري از شبكه هاي كامپيوتري زمينه استفاده قانونمند و هدفمند از اطلاعات را برای سایرین فراهم کرد.

امنیت اطلاعات در شبکه های کامپیوتری

به موازات حركت بسمت يک سازمان مدرن و مبتني بر تكنولوژي اطلاعات، مي بايست تدابير لازم در رابطه با حفاظت از اطلاعات نيز انديشيده گردد . مهمترين مزيت و رسالت شبكه هاي كامپيوتري ، اشتراک منابع سخت افزاري و نرم افزاري است . كنترل دستيابي و نحوه استفاده از منابع به اشتراک گذاشته شده ، از مهمترين اهداف يک سيستم امنيتي در شبكه است . با گسترش شبكه هاي كامپيوتري خصوصا" اينترنت ، نگرش نسبت به امنيت اطلاعات و ساير منابع به اشتراک گذاشته شده ، وارد مرحله جديدي شده است . در اين راستا ، لازم است كه هر سازمان براي حفاظت از اطلاعات ارزشمند ، پايبند به يک استراتژي خاص بوده و بر اساس آن سيستم امنيتي را اجراء و پياده سازي نمايد.

دشمنان، انگیزه ها، انواع عملیاتی

بمنظور دفاع موثر و مطلوب در مقابل حملات به اطلاعات و سيستم هاي اطلاعاتي ، يک سازمان مي بايست دشمنان، پتانسيل و انگيزه هاي آنان و انواع حملات را بدرستي براي خود آناليز تا از اين طريق ديدگاهي منطقي نسبت به موارد فوق ايجاد و در ادامه امكان برخورد مناسب با آنان فراهم گردد .اگر قصد تجويز دارو براي بيماري وجود داشته باشد ، قطعا" قبل از معاينه و آناليز وضعيت بيمار، اقدام به تجويز دارو براي وي نخواهد شد. در چنين مواري نمي توان براي برخورد با مسائل پويا از راه حل هاي مشابه و ايستا استفاده كرد .بمنظور ارائه راهكارهاي پويا و متناسب با مسائل متغير، لازم است در ابتدا نسبت به كالبد شكافي دشمنان ، انگيزه ها و انواع حملات ، شناخت مناسبي ايجاد گردد . دشمنان ، شامل سارقين اطلاعاتي ، مجرمان ،دزدان كامپيوتري ، شركت هاي رقيب و ... مي باشد.