سیستمهای امنیتی و روالها در پنج لایه مختلف در محیط فناوری اطلاعات متمرکز میگردد.(رویکرد لایه بندی شده برای امنیت شبکه)

1-پیرامون(محیط) 2- شبکه 3- میزبان 4- برنامه کاربردی 5- داده

Work factor (ضریب عملکرد)

میزان تلاش مورد نیاز توسط یک نفوذگر بمنظور تحت تاثیر قرار دادن یک یا بیشتر ،از سیستمها و ابزارهای امنیتی

ضریب عملکرد بالا=سختی بیشتر برای نفوذ به شبکه

سطح 1 :امنیت پیرامون

- اولین خط دفاعی نسبت به بیرون شبکه
-ناحیه ای است که شبکه به پایان میرسد و اینترنت آغاز میشود.
- پیرامون شامل یک یا چند فایروال و مجموعه ای از سروهای بشدت کنترل شده است که در بخش DMZ قرار میگیرند.

DMZ=Demilitaraized Zone

DMZ معمولا شامل وب سرورها ،مدخل ایمیلها ،آنتی ویروسها و سرورهایDNS میباشد که باید در معرض اینترنت قرار گیرند.

FW:Firewall

در لبه شبکه(محلی که به بیرون ودرون پیرامون شبکه متصل است قرار میگیرد)

وظائف فایروال:

1- کنترل ترافیک :با سنجیدن مبداء و مقصد تمام ترافیکهای وارد شونده و خارج شونده(عبور ترافیک مجاز)

2- تبدیل آدرس: تبدیل IP داخلی به آدرسهای قابل رویت در اینترنت

3- نقطه پایانی VPN :نقطه پایانی تونلهای VPN

AV:Antivirus

- در ناحیه DMZ نصب میگردد و محتوی ایمیلهای وارد شونده و خارج شونده را با دیتابیس خود چک میکند و ویروسهای آلوده را مسدود کرده و آنها را قرنطینه میکند و به دریافت کنندگان و مدیران شبکه انتقال میدهد.

VPN Virtual Private Network

- یک شبکه اختصاصی مجازیست که از رمز نگاری سطح بالا برای ارتباط امن ابزارهای دور از همدیگر با استفاده از یک تونل رمز شده استفاده میکند.
- VPN میتواند در یک مسیر یاب بر پایهVPN ،فایروال و یا یک سرور در ناحیه DMZ پایان پذیرد.

مزایای سطح پیرامون:

این تکنولوژیها سالهاست که در دسترس هستند بنابراین آشنایی با با نیازهای عملیاتی آن زیاد میباشد و ضمنا پیلده سازی آن آسان و توام با توجیه اقتصادی هستند.

معایب سطح پیرامون:

-چون این سیستمها تقریبا پایه ای هستند و مدتهاست در دسترس میباشند ،هکرها راه حلهای دور زدن آن را بیشتر نشان داده اند

- آنتی ویروسها نمیتوانند ویروسهایی را که در دیتا بیس خود نمیشناشند و یا داخل فایل رمز گذاری شده باشد را شناسایی کنند

- در حالت VPN کلیدهای رمز نگاری و گروههای کاربری باید بصورت مداوم مدیریت شوند.

سطح 2 :امنیت شبکه

- سطح شبکه به lan و wan داخلی اشاره دارد

Intrusion Detection System:IDS سیستمهای تشخیص نفوذ

Intrusion Prevention System:IPS سیستمهای جلوگیری از نفوذ

- ابزارهای IPS,IDS ترافیک گذرنده در شبکه را با جزئیات بیشتر نسبت به فایروال تحلیل میکنند با تطبیق دادن هر بسته اطلاعات با پایگاه دادهای از مشخصات حملات شناخته شده

- ابزارهای IDS مسئولین It را از وقوع یک حمله مطلع میسازند.

- ابزارهای IPS علاوه برعملی که IDS انجام میدهد بصورت خودکار ترافیک آسیب رسان را مسدود میکنند.

- بیشتر IPSها در هسته خود یک IDS دارند.

مدیریت آسیب پذیری(تخمین آسیب پذیری در گذشته)

- شبکه را برای آسیب پذیریها پیمایش میکنند.

- روند مرمت آسیب پذیری یافته شده را مدیریت میکند.

سیستمهای مدیریت آسیب پذیری (VA) معمولا پایگاه داده ای از قوانینی را نگهداری میکنند که آسیب پذیریهای شناخته شده برای گستره ای از ابزارها و برنامه های شبکه را مشخص میکنند که در کل روند بازسازی را مدیریت میکنند.

تابعیت امنیتی کاربر انتهایی:

این روشها تضمین میکند کاربران انتهایی استانداردهای امنیتی تعریف شده را قبل از اینکه اجازه دسترسی به شبکه داشته باشند رعایت کرده اند

این عمل جلوی حمله به شبکه از داخل خود شبکه را از طریق سیستمهای نا امن کارمندان و ابزارهای VPN و RAS میگیرد

آزمایشهایی که بر روی سیستمهای انتهایی انجام میگردد عبارتند از:

1- نرم افزار مورد نیاز مانند سرویس پکها ،آنتی ویروسهای بروز شده و غیره

2- کاربردهای ممنوع مانند اشتراک فایل و نرم افزارهای جاسوسی

کنترل دسترسی – تایید هویت

- کنترل دسترسی نیازمند تایید هویت کاربرانی است که به شبکه دسترسی دارند–هم کاربران و هم ابزارها باید با ابزار کنترل دسترسی در سطح شبکه کنترل شوند.

- معمولا تراکنشهای تایید هویت در مقابل دید کاربر اتفاق میافتد

مزایای سطح 2 (شبکه):

- IPS,IDS تجزیه و تحلیل عمیقتری را بعهده دارند ،بنابراین سطح بالاتری از محافظت را ارائه میکنند.

- حملاتی که داخل ترافیک قانونی شبکه وجود دارند و از فایروال عبور کرده اند مشخص خواهند شد.

- سیستمهای مدیریت آسیب پذیری روند آسیبپذیری شبکه را بصورت خودکار استخراج میکنند که بصورت دستی امکان ناپذیر است.

- روشهای تابعیت امنیتی کاربر انتهایی سطح بالایی از کنترل بر روی ابزاری را میدهد که بصورت سنتی کنترل کمی بر روی آن وجود خواهد داشت

هکرها بیشتر بدنبال بهره برداری از نقاط انتهایی برای داخل شدن به شبکه هستند که برنامه امنیتی کاربران انتهایی این درهای پشتی خطرناک به شبکه را میبندد.(وجود تهدید هایی مانند sasser,my doom.sobig)

معایب سطح 2 (شبکه):

- IDS ها تمایل به تولید تعداد زیادی علائم هشدار غلط دارند که بعنوان false positive شناخته میشوند.

- مدیران IDS ممکن است با توجه به مورد بالا حساسیت خود را نسبت به اطلاعات تولید شده توسط سیستم را از دست بدهند.

- IDS باید بصورت پیوسته مورد بررسی واقع شود و برای الگوهای مورد استفاده و آسیب پذیریهای کشف شده در محیط شبکه تنظیم گردند که میزان بالایی از منابع اجرایی را مصرف میکند.

- بسیاری از روشهای امنیتی کاربران انتهایی نیاز به نصب یک عامل در هر نقطه انتهایی دارد که مقدار قابل توجهی بار کاری اجرایی به نصب و نگهداری اضافه میکند.

- پیاده سازی یک سیستم یکپارچه در یک شبکه ممکن است دشوار باشد.

- استفاده از چند محصول مختلف برای امنیت سطح شبکه ممکن است آسیب پذیریهای بیشتری را در شبکه بوجود آورد.

سطح 3 امنیت میزبان:

سطح میزبان مربوط به ابزارهای منفرد مانند سرورها ،کامپیوترهای شخصی،سوئیچها،روترها و غیره در شبکه است.

- هر دستگاه تعدادی پارامتر قابل تنظیم دارد که اگر به نادرستی تنظیم شود میتواند سوراخ امنیتی نفوذ پذیری ایجاد کند.این پارامترها شامل تنظیمات رجیستری ،سرویسها،توابع عملیاتی روی خود ابزار یا وصله های سیستم عامل یا نرم افزارهای مهم میشود.

IDS در سطح میزبان:

- برای مشخصات عملیاتی بخصوصی از ابزار میزبان تنظیم میگردد.

VA (تخمین آسیبپذیری در سطح میزبان:

- دقت آن بالاست و کمترین نیاز را به منابع میزبتن دارد.

تابعیت امنیتی کاربر انتهایی:

- میزبان را برای عملیات زیان رسان و آلودگیها بررسی میکند و همچنین به روز بودن فایروالها و آنتی ویروسها

کنترل دسترسی –تصدیق هویت:

- دسترسی به ابزار تنها توسط کاربران مجاز صورت پذیرد.

مزایای سطح 3 میزبان:

این تکنولوژیها در سطح میزبان حفاظت بالایی ایجاد میکنند و دقت و پاسخ بالای آن به مدیران اجازه میدهد به سرعت مشخص کنند کدام تنظیمات ابزار نیاز به روزرسانی برای تضمین عملیات امن دارند.

معایب سطح 3 میزبان:

- مدیریت سیستمهای سطح میزبان میتواند بسیار زمان بر باشد.

- سیستمها نیاز به نمایش و بروز رسانی مداوم دارند

- با تعداد زیادی ابزار امنیتی در سطح میزبان تعداد هشدارها و علائم اشتباه میتواند بسیار زیاد باشد.

- اغلب نصبشان مشکل است

سطح 4 امنیت برنامه های کاربردی:

بیشتر برنامه نویسان در موقع تولید کد به امنیت توجه ندارند و باید یک استراتژی امنیتی جامع برای هر برنامه تحت شبکه اعمال شود.

پوشش محافظ برنامه:(فایر وال سطح برنامه)

- تضمین میکند تقاضا های وارد شونده و خارج شونده برای برنامه مورد نظر مجاز هستند.
- یک پوشش بر روی سرورهای مختلف که برای کاربر شفاف است نصب میشود و با درجه بالایی با سیستم یکپارچه میگردد
- پوشش محافظ برنامه برای عملکرد مورد انتظار سیستم میزبان تنظیم میگردد بعنوان مثال یک پوشش بر روی سرور ایمیل به این منظور پیکره بندی میگردد تا جلوی اجرای خودکار برنامه ها توسط ایمیلهای وارد شونده را بگیرد.

کنترل دسترسی – تصدیق هویت:

- تنها کاربران مجاز اجازه دسترسی به برنامه را دارند.

تعیین صحت ورودی:

- ورود دیتا برای فیلد معین مثلا تنها ورودی در برنامه قابل پذیرش است که فقط پنج کاراکتر عددیست.
- کلید واژه ها را باید فیلتر کرد ،مثلا عبارات مربوط به فرمانها مانندinsert بررسی ودر صورت نیاز مسدود گردد.

مزایا سطح 4 برنامه:

ابزارهای امنیتی سطح برنامه امنیت کلی را تقویت میکند و سطح بالاتری از جوابگویی را بعلت قابل ردیابی بودن ثبت ابزارها فراهم میکند

معایب سطح 4 برنامه:

پیاده سازی جامع سطح برنامه میتواند پر هزینه باشد.

سطح 5 امنیت داده:

امنیت سطح دیتا ترکیبی از سیاست امنیتی و رمزنگاری را در بر میگیرد.

سیاست سازمانی میگوید چه کسی به دیتا دسترسی دارد و کدام کاربران مجاز میتوانند آن را دستکاری کنند.

رمزنگاری:

این طرح ها در سطح دیتا و برنامه و سیستم عامل پیاده سازی میشوند و تقریبا تمام طرحها شامل کلیدهای رمز نگاری و رمز گشایی هستند و کاربرانی مجاز هستند که این کلیدها را داشته باشند.RSA-PGP-PKI

کنترل دسترسی – تصدیق هویت:

- تنها کاربران مجاز اجازه دسترسی به دیتا را دارند.

مزایا سطح 5 دیتا:

- یک مانع نهایی و موثر برای محافظت از اطلاعات خصوصی و دارایی دیجیتال را فراهم میکند.

معایب سطح 5 دیتا:

- بار اضافی برای رمزنگاری و رمز گشایی دیتا ایجاد میشود که میتواند تاثیرات زیادی را در کارائی بگذارد و بار اجرایی زیادی را برای سازمانهای بزگ یا در حال رشد دارد.

دفاع در مقابل تهدیدها و حملات معمول

حملات به وب سرور:

- از دستکاریهای ساده در صفحات گرفته تا در اختیار گرفتن سیستم از راه دور و حملاتDOS نمونه آن code red,Nimda

باز پخش ایمیلها بصورت غیر مجاز:

-هرزنامه spam و دستکاریهای میزبان دور که یک کنترل در سطح سیستم است و به حمله کننده اختیاراتی برابر با مدیر محلی سیستم میدهد.

فراهم بودن سرویسهای اینترنتی غیر مجاز:

- توانایی بکار گیری یک وب سرور یا سرویس اینترنتی که ریسک افشای سحوی اطلاعات را بالا میبرد.

تشخیص فعالیت ویروس:

- ضد ویروس برای تشخیص ویروس است نه فعالیت ویروسی بنابراین استفاده اIDS بسیار مناسب است.
- استفاده از یک فایروال در ترکیب با آنتی ویروس برای محافظت و استفاده از5 سطح لایه امنیتی میتواند بطور نسبی جلوی تهدیدات را بگیرد.

تشخیص نفوذ:intrusion detection

عبارت است از پردازه تشخیص تلاشهایی که جهت دسترسی غیر مجاز به یک شبکه یا کاهش کارائی آن انجام میشود و در2 مرحله انجام میشود.

1- اطمینان از اینکه الگوی عمومی فعالیتهای خطرناک ،تشخیص داده شده است.

2- اطمینان از اینکه با حوادث مشخصی که در طبقه بندی مشترک حملات نمیگنجد به سرعت رفتار میشود.

انواع حملات شبکه ای با توجه به طریقه حمله (چگونگی انجام حمله)

حملات از کار انداختن سرویس:

- حجم بالایی از درخواست ارائه خدمات به سرور فرستاده میشود تا امکان خدمات رسانی را از آن بگیرد.

حملات دسترسی به شبکه:

- امکان دسترسی غیر مجاز به منابع شبکه مانند حملاتDOS که از شبکه بعنوان مبداء حملات در جهت عدم شناسایی استفاده میکنند.

حملات دسترسی به شبکه به دو گروه تقسیم میشود.

1- دسترسی به داده:

- نفوذگر میتواند یک کاربر داخلی یا یک فرد خارج از مجموعه باشد . فوذ گر با افزایش امتیاز دسترسی به شکل غیر مجاز به اطلاعات محرمانه طبقه بندی شده دسترسی پیدا میکند این روش به تعدیل امتیاز معروف است Privilege Escalation

2- دسترسی به سیستم:

- نفوذگر به منابع سیستم و دستگاهها دسترسی پیدا میکند این دسترسی میتواند شامل اجرای برنامه ها برروی سیستم و بکارگیری منابع آن در جهت اجرای دستورات حمله کننده باشد.

- نفوذ گر میتواند به تجهیزات شبکه مانند پرینتر ،دوربین و.....دسترسی پیدا کند.

نفوذگر قبل از حمله از شناسایی reconnaissance جهت یافتن حفره های امنیتی و نقاط ضعف شبکه استفاده میکند.

انواع حملات شبکه ای با توجه به حمله کننده:

2- حملات انجام شده توسط افراد غیر معتمد (خارجی)

3- حملات انجام شده توسط هکرهای بی تجربه

4- حملات انجام شده توسط هکرهای با تجربه

- با توجه به شناخت دقیق از شبکه ابزارهایی تولید میکنند که عمدتا گروه اول از آن استفاده میکنند.

پردازه تشخیص نفوذ: **IDS**

1- IDS مبتنی بر خلاف قواعد آماری

- مثلا چند بار یک دستور مشخص توسط یک کاربر در یک تماس با یک میزبان host اجراء میشود.

2- IDS مبتنی بر امضاء یا تطبیق الگو

- منظور از امضاء مجموعه قواعدی است که یک حمله در حال انجام را تشخیص میدهد–اگر ترافیک در حال عبور با الگوی موجود در امضاء تطبیق پیدا کند پیغام اخطار تولید میشود و علاوه بر آگاه کردن مدیذان شبکه اتصال با هکر را باز آغازی میکند و با کمک فایروال و انجام عملیات کنترل دسترسی با نفوذ بیشتر مقابله میکند.

پردازه پیشگیری از نفوذ: **IPS**

ایده اینست که تمام حملات علیه هر بخش از محیط محافظت شده توسط روشهای بکارگرفته شده ناکام بماند ،این روشها میتوان تمام بسته های شبکه را بگیرند و نیت آنها را مشخص کنند.

IPS versus IDS

- یک IPS یا سیستم پیشگیری مانند یک محافظ امنیتی در مدخل یک اجتماع خصوصی عمل میکند که بر پایه بعضی گواهی ها قوانین یا سیاست های از پیش تعیین شده اجازه عبور میدهد.

- یک IDS یا سیستم تشخیص مانند یک اتوموبیل گشت زنی در میان اجتماع عمل میکند که فعالیتها را به نمایش میگذارد و دنبال موقعیتهای غیر عادی میگردد و بدون توجه به قدرت امنیت در مدخل به گشت زنیهای خود در سیستم ادامه میدهد و بررسیهای خود را انجام میدهد

- IPS به بعضی از موارد مشکوک به حمله اجازه عبور میدهد تا احتمال تشخیص غلط (false positive) کاهش یابد.
- IDS بدون تاثیر گذاشتن روی معماریهای محاسباتی شبکه ای به کارخود ادامه میدهد و روشهای آن با هوشمندی همراه هستند.

وظائف IDS (تشخیص موارد)

- حملات شناخته شده از طریق امضاء ها و قوانین
- تغییرات در حجم و جهت ترافیک با استفاده از قوانین پیچیده و تحلیل آماری
- تغییرات الگوی ترافیک ارتباطی با استفاده از تحلیل جریان
- تشخیص فعالیت های غیر عادی با استفاده از تحلیل انحراف معیار
- تشخیص فعالیت مشکوک با استفاده از تکنیکهای آماری و تحلیل جریان

روشهای بر اساس خلاف قاعده ممکن است تشخیص صد در صد صحیح نباشد و این روشها برای تصمیم گیری مسدود سازی بر اساس سیاست مناسب نیستند

وظائف IPS

- روشهای IPS باید طبیعت قطعی(deterministic) داشته باشند تا باعث عدم تشخیص حملهfalse negative و ریسک بی مورد در محیط شبکه نشود.
- هدف نهایی ، یک سیستم کامل است که نه تشخیص غلط حمله false positive که از بازذهی شبکه میکاهد و نه false negative اتفاق افتد.
- مسدود کردن برنامه های ناخواسته و حملات اسب تراوای فعال علیه شبکه ها و برنامه های اختصاصی با استفاده از قوانین قطعی و لیستهای کنترل دسترسی
- تشخیص بسته های دیتای متعلق به حمله با استفاده از فیلترهای بسته ای داده ای سرعت بالا
- تشخیص سوء استفاده از پرتکل و دستکاری پرتکل شبکه با استفاده از بازسازی هوشمند
- تشخیص DOS/DDOS مانند طغیان SYN و ICMP با استفاده از الگوریتمهای فیلترینگ بر پایه حد آستانه
- سوء استفاده از برنامه ها و دستکاریهای پرتکل حملات شناخته شده و شناخته نشده علیهsmtp,dns,ftp,http و غیره با استفاده از قوانین پرتکل برنامه ها و امضاء ها

حملات *DOS* Denial of service

مهاجم باعث ممانعت دستیابی کاربران تایید شده به اطلاعات و یا سرویسهای خاص میشود ومانند سلب دستیابی به سایتهای ایمیل ،وب سایتها، account های on line

- متداولترین نوع حملات DOS زمانی اتفاق می افتد که مهاجم اقدام به ایجاد یک سیلاب اطلاعاتی در شبکه نماید.بدین شکل که چون هر سرویس دهنده در لحظه قادر به پاسخگویی به حجم محدودی از درخواستها میباشد مهاجم با ارسال درخواستهای متعد سیلاب گونه باعث افزایش حجم عملیات سرویس دهنده میشود و عملا سرویس از کار میافتد.

Spam

مهاجم با ارسال پیام الکترونیکی ناخواسته به سرویس دهنده پست الکترونیکی حمله میکند و عملا امکان در یافت ایمیل معتبر را از account مجاز سلب مینماید.

حملات *DDOS* Distributed Denial of service

در یک تهاجم DDOS مهاجم از یک کامپیوتر میزبان برای تهاجم بر علیه کامپیوتر دیگری استفاده میکند ،مهاجمان با استفاده از نقاط آسیب پذیر یک host و بدست گرفتن کنترل آن به حملات از طریق آن کامپیوتر به جاهای دیگر شبکه استفاده میکنند که در حالت پیشرفته ممکن است از چندین کامپیوتر بعنوان تهاجمDOS استفاده شود.

***نحوه پیشگیری از حملات* DOS,DDOS,SPAM**

- نصب و نگهداری نرم افزار آنتی ویروس
- نصب و پیکره بندی فایر وال
- تبعیت از مجموعه سیاستهای خاص در خصوص توزیع و ارائه آدرس ایمیل خود به دیگران

چگونه از وقوع حملات DOS و یا DDOS آگاه شویم.

- کاهش سرعت و یا کارائی شبکه بطور غیر معمول
- عدم دسترسی به یک سایت خاص بدون دلایل فنی
- عدم دسترسی به هر سایتی بدون دلایل فنی
- افزایش محسوس حجم نامه های الکترونیکی ناخواسته دریافتی
- پس از و قوع حمله موضوع با مدیر شبکه و در نهایت مرکز ارائه دهنده خدمات اینترنتISP تماس گرفته شود.

منابع تشکیل دهنده اینترنت به نوعی محدود و مصرف شدنی هستند بنابراین سعی میشود با مصرف کردن مقدار قابل توجهی از منابع(پهنای باند)باعث کاهش تاثیر حمله DOS شد.

امنیت اینترنت تا حد زیادی وابسته به تمام عوامل است بدین صورت که با ارتباط اینترنت در معرض بسیاری از انواع حمله قرار میگیریم بدون توجه به اینکه تا چه حدی امنیت را در شبکه خود برقرار کرده ایم

استفاده از جعل IP توسط حملات پیشرفته DOS چالش جدی را ایجاد کرده است.

در حملات DOS با استفاده از تعداد زیادی بسته به یک مقصد از طریق چندین منبع آلوده باعث مصرف زیاد پهنای باند شبکه میشود که چنین حملاتی به عنوان طغیان بسته شناخته میشود. **Packet Flooding**

***طغیان* TCP:**

- رشته ای از بسته های TCP با پرچمهای Flag متفاوت به آدرس IP قربانی ارسال میگردد پرچمهایSYN,ACK,RST بیشتر استفاده میشود.

***طغیان* UDP:**

***طغیان* ICMP:**

روش جعل IP

- یا برای پنهان کردن منبع واقعی یک رشته بسته استفاده میشود و یا با جعل IP منبع بسته های زیادی به سایت واسط فرستاده میشود تا باعث شود پاسخ ها بسمت قربانی ارسال گردد.

پورتهای منبع و مقصد:

- ابزار حمله طغیان tcp یا udp گاهی اوقات پورت منبع یا مقصد را تغییر میدهند تا واکنش توسط فیلتر کردن بسته را مشکل تر کنند.

مقادیر Ip Header دیگر:

- در بسته های tcp/ip فقط مقدار ip مبداء و مقصد در header ثابت است با تغییر دادن خواص بسته ها از طریق دستکاری header نفوذ گر کار خود را انجام میدهد.

روشهای حمله DOS

حمله Smurf: **(Icmp flood)**

با استفاده از تقاضای اکو ICM (ping) وتغییر آدرس منبع تقاضای اکو به ip قربانی (بعنوان آدرس برگشت) کلیه ماشینهای ناحیه پاسخ آدرس اکو را به قربانی می فرستند و طی یک طغیان ماشین قربانی از کار خواهد افتاد.

این روش از روش مصرف پهنای باند استفاده میکند بعنوان مثال حمله کننده با پهنای باند پایین 56k میتواند سیستم قربانی با پهنای باند T1 را از کار بیاندازد

حمله Fraggle : (تقویت بسته **UDP** ***)***

روش کار مانند smurf است ولی از بسته های اکو udp استفاده میشود و عمومیت smurf را بعلت کمتر استفاده شدن پرتکل udp در شبکه را ندارد

حمله **SYN Flood:**

این روسش برای ایجاد حمله DOS بر اساس قحطی منابع عمل میکند در این روش برای برقراری ارتباط حمله کننده بجای یک تقاضای SYN به سرور چند تقاضای SYN به سرور قربانی با آدرسهای منبع جعلی بعنوان آدرس برگشت می فرستد و چون چنین آدرسهایی وجود ندارند کلاینت ACK را از طریق سرور دریافت نمیکند و زمان انتظار سرور بعد از مدتی به پایان میرسد بدین شکل منابع سرور در صورت ازدیاد این حالت مصرف خواهد شد.

حمله **DNS:**

در نسخه های اولیه BIND حمله کننده اطلاعات DNS غلط که میتواند باعث تغییر مسیر درخواست میشود ارسال میکند. در حقیقت حافظه نهان سرور DNS که در حال استفاده از عملیات بازگشت برای جستجوی یک ناحیه بود مسموم میشد و کاربر قانونی را بسمت شبکه مورد نظر حمله کننده یا یک شبکه دیگر هدایت میکرد.

روشهای حمله **DOS.DDOS**

Stecheldraht,TFN,TFN2K,Trinoo

حمله **Trinoo:**

در اصل از برنامه های master/slave است که با یکدیگر برای حمله طغیان udp بر علیه کامپیوتر قربانی در 3 مرحله هماهنگ میشوند

1- حمله کننده با استفاده از میزبان هک شده لیستی از سیستمهایی که میتوانند هک شوند بصورت خودکار جمع آوری میکنند.

2- به محض آمادگی لیست اسکریپتها برای هک کردن و تبدیل آنها به اربابان masters یا شیاطین daemons اجراء میشوند.

- یک ارباب میتواند چندین شیاطین راکنترل کند و شیاطین میزبانان هک شده ای هستند که طغیان udp را روی ماشین قربانی انجام میدهند.

3- حمله کننده فرمانی را به میزبانان master صادر میکند و حمله انجام میشود

- این اربابان به هر شیطانی دستور میدهند که حمله DOS را علیه آدرس IP مشخصی آغاز کنند و با انجام تعداد زیادی حمله DOS یک حمله DDOS شکل میگیرد.

حمله **TFN (Tribal Flood Ntwork) :**

همانند Trinoo در اصل از برنامه های master/slave است که با یکدیگر برای حمله طغیان SYN بر علیه کامپیوتر قربانی هماهنگ میشوند

- شیاطین TFN قادر به انجام حملات بسیار متنوع تری شامل طغیان ICMP ،طغیان SYN ،و حملات Smurf هستند.

حمله **TFN2K :**

1- با جعل آدرسهای ip اجرا میشوند تا باعث کشف مشکلتر منبع حمله شوند.

2- از شکافهای امنیتی سیستم عامل نیز استفاده میکنند.

3- نیازی به اجرای فرمان با وارد شدن به client ها ندارند و میتوانند روی واسطهای مختلفی مانند Tcp,Udp صورت پذیرند.

دفاع در برابر حملات Smurf یا Fraggle:

1- تنظیم روتر برای بستن تمام بسته های خارج شونده از شبکه که آدرس مبداء متناقض با زیر شبکه داخلی دارند.

2- تنظیم روتر در جهت اینکه به بسته های ICMP منتشر شده به شبکه خود اجازه عبور ندهد یعنی در داخل شبکه Ping انجام میشود ولی از بیرون بداخل Ping نمیشود.

3- برقراری ارتباط(تماس) با شبکه بالا دستی (احتمالا ISP) برای بهینه تر کردن جلوگیری از نفوذ.

دفاع در برابر حملات طغیان SYN

بجای تخصیص یک ارتباط کامل یک شی که فضای زیادی را در حافظه ایجاد میکند از یک رکورد کوچک Mincro-record استفاده گردد.پیاده سازی SYN های کوچکتر تنها 16 بایت فضا اشغال میکنند.

نوعی از طغیان کوکی SYN است که هر طرف ارتباط یک شماره توالی خودش را دارد sequence number در پاسخ به یک SYN سیستم مورد حمله واقع شده یک شماره توالی مخصوص از ارتباط را ایجاد میکند که کوکی است و سپس همه چیز را فراموش میکند یا به عبارتی حافظه خارج میکند و بعدا از طریق کوکی میتواند اطلاعات را بازیابی کند

برای حل مشکل بالا از کوکی های RST استفاده میشود روش بدین صورت است که سرور یک ACK/SYN اشتباه به کلاینت ارسال میکند و کلاینت باید یک بسته RST تولید کند تا به سرور بگویید چیزی اشتباه است و در این هنگام سرور میفهمد که کلاینت معتبر است.

کاستن زمان انقضاء (time out)در پشته های TCP (Stack) برای آزاد کردن یک ارتباط نیز یک راه حل است .تکنیک دیگر قطع بعضی از ارتباطات بصورت انتخابی است.

دفاع علیه حملات DNS:

1- دفاع از سرور اصلی Root server با بکآپ گرفتن و آبدیت پایگاه اصلی و استفاده از سرور اصلی با استفاده از آدرسهای anycast که باعث میشود سیستمها در شبکه های مختلف بعنوان یک سرور بنظر برسند.

2- تفکیک DNS (دسترسیهای جداگانه از DNS برای مشتریان داخلی و خارجی)

دفاع علیه حملات DDOS:

1- استفاده از روش سیاه چاله که تمام ترافیکهای داخلی و خارجی مسدود شده و دور ریخته میشوند و ایراد آن اینست که سیستم off-line میشود

2- تنظیم روترها و فایروالها برای فیلتر کردن ping و پرتکلهای غیر ضروری-روتر ها معمولا در مقابل حمله جعل شده پیچیده تر و حملات در سطح application با استفاده از آدرس ip معتبر ،بی تاثیر هستند.

3- استفاده از IDS ها بهمراه فایر وال ها

4- پیکره بندی مناسب application های سرویس دهنده(سرورها) بعنوان مثال یک application از چه منابعی میتواند استفاده کند وچگونه به تقاضای کلاینت پاسخ دهد.

5- استفاده از ابزار تخفیف (کنترل کننده با ترافیک شبکه)

6- خرید پهنای باند زیاد برای مقبله با تهدیدات

روشهایی که نفوذگران برای برای ورود به کامپیوتر و صدمه زدن به آن استفاده میکنند عبارتند از:

1- برنامه های اسب تروا : روشی برای گول زدن قربانی است تا برنامه های درپشتی را نصب نمایند

2- برنامه های پشتی و برنامه های مدیریت از راه دور :استفاده از ابزارهایی مانند **Subseven,Netbus,BackOrifice**

3- عدم پذیرش سرویس **:DOS** استفاده از آخرین وصله های امنیتی

4- وساطت برای یک حمله دیگر **:DDOS** عموما از برنامه های اسب تروا برای ایجاد یک عامل استفاده میشود

5- اشتراکهای ویندوزی حفاظت نشده **:On** شدن سرویس windows share یا سرویسهای point to point

6- کدهای قابل انتقال :بستن امکان اجرای کدهای سیار (قابل احراء) در کامپیوتر

7- اسکریپتهای **Cross-Site**: صفحات تبلیغاتی که همراه یک سایت باز میشود مانندصفحات خبری،فرم های محاوره ای و بحثهای on-line

8- ایمیلهای جعلی : ایمیل به ظاهر متعلق به منبع معتبر است و چیزی مانند رمز یا...را میخواهد

9- ویروسهای داخل ایمیل : باز نکردن ایمیلهای ناشناخته

10- پسوندهای مخفی فایل **Love-Letter-For-YOU ⟶ Love-Letter-For-YOU.txt.exe**

11- سرویس گیرندگان چت : آلوده شدن بعلت سرویسهای دو طرفه در چت

12- شنود بسته های اطلاعات : برنامه ای است که دیتا را از اطلاعاتی که در حال انتقال در روی شبکه است در اختیار میگیرد عموما کاربران dialup و DSL

کوکی چیست:

کوکی بخش کوچکی از اطلاعات با فرمت فایل متنی فرستاده شده توسط وب سرور برای ذخیره در مرورگر است تا بعدا بتواند از طریق آن مرورگر دوباره خوانده شود.

در داخل دایرکتوری مرور گر ثبت میگردد و در هنگام اجراء در Ram قرار میگیرد.

ابزارهای مهمی برای نگهداشتن state روی وب هستند مثلا مراجعه قبلی بوده است یا خیر

بیشتر کوکی ها بعد از خارج شدن از مرور گر ازبین میروند مگر از نوع ماندگار باشند که تاریخ انقضاء دارند.

بعضی اوقات از کوکی برای رد گیری عادات یک وبگرد استفاده میشود.

نت اسکیپ تمام کوکیهای ماندگارش را دریک فایل cookie.txt ذخیره میکند که قابل ویرایش است

در IE کوکیها بصورت جداگانه ذخیره میشود و در داخل شاخه cookie قرار دارند.

از کوکی برای ذخیره کلمات عبور و شناسه هایی برای تنظمات شخصی در صفحات وب استفاده میشود

از کوکیها برای بدست آوردن علائق کاربران در سایتهای تجاری نیز استفاده میشود.

کوکیها یا کوکیهای شخص اول هستند که از وب سایتی نشات میگیرد یا به آن فرستاده میشود که در حال مشاهده آن هستیم

کوکیهای شخص ثالث از وب سایت متفاوت از آنی که مشاهده میکنیم نشات میگرد بطور مثال تبلیغات وب سایتهای شخص ثالث

کوکیها امکان انتقال اطلاعات شخصی را به سایتهای ثانویه دارند که خوشایند نیست

کوکیها فقط آنچه را که به آنها گفته میشوند میدانند.

از کوکیها برای اهداف غیر اخلاقی توسط شنود بسته های اطلاعاتی توسط بعضی افراد استفاده میشود.

مرور گرهای جدید اجازه نحوه کار با کوکیها را به کاربر میدهد–در صورت تایید کوکی ثبت گردد.

چند مورد وجود دارد که ایجاد کننده یک وب سایت میتواند انجام دهد.

- مطمئن شود که کوکیها کمترین اطلاعات خصوصی را دارند.
- مطمئن شود که اطلاعات حساس درون کوکیها همیشه رمز نگاری میشود.

بیشتر سایتهای استفاده کننده از کوکی اطلاعات زیر را نیز لحاظ میکنند.

- اطلاعات لازم برای دادن اجازه به فرد
- ساعت و تاریخ
- تاریخ انقضاء
- کد **MAC (Message Authenticaty Check)** تضمیین میکند کوکی دچار تغییر نشده است.
- آدرس ip استفاده کننده از وب

***محتویات فعال* Active Contents:**

- اسکریپتهایی که باعث ایجاد منوهای Drop-down یا انجام افکتهای گرافیکی متفاوت در یک صفحه وب بعنوان مثال
- از جاوا اسکریپت نیز برای تولید اسکریپت استفاده میشود یکی از برنامه های مخرب هدایت کاربر به سایت مورد نظر میباشد.
- در صورت عدم شناخت از یک سایت بهتر است محتویات فعال ActiveX را غیر فعال نمود
- در صورت باز کردن ایمیلهای ناشناخته در محیط HTML بهتر است محتویات فعال ،غیر فعال شود و نامه ها بصورت متن معمولی مشاهده شود.

Session Kookie

- این نوع کوکیها صرفا تا زمانی که از مرورگر استفاده میشود اطلاعاتی را ذخیره میکندو پس از بستن مرورگر اطلاعات از بین میرود

Presistent Kookie

- بیشتر مرور گرها از این نوع کوکی برای مدت زمان مشخصی استفاده میکنند.

با بررسی history مرورگر و فایلهای موقت اینترنت Cache میتوان آگاهیهای لازم درخصوص وب سایتهای مشاهده شده توسط یک کاربر را بدست آورد

با بررسی فولدرهای Favorite,Bookmarks,Cookies میتوان اطلاعات مهمی را بدست آورد

با بررسی بخش آدرس یک مرورگر در رجیستری میتوان اطلاعات مهمی را بدست آورد

بررسی برنامه های واژه پرداز و سایر برنامه هایی که فایلهای موقت متنی ایجاد میکنند

بررسی Clipboard مربوط به ویندوز یا Office

برنامه های Instant messenger ممکن است طوری پیکره بندی شده باشند که ماحصل مکالمه یا محاوره را در فایلی ذخیره کرده باشند.

نرم افزار پست الکترونیکی یا برنامه نگهداری لیستهای تماس

فولدر MY Document

درایوهای مربوط به Tape سی دی،فلاپی و حافظه های فلش

Recycle bin

شاخه Temp

SPAM

Spam نسخه الکترونیکی از نامه های بدرد نخور است و به پیامهای الکترونیکی ناخواسته اطلاق میشود.این نوع نامه ها ی الکترونیکی ارتباط مستقیمی با ویروس نداشته و حتی ممکن است پیامهایی که از منابع معتبر ارسال شده اند را نیز در بر بگیرد.

چگونگی کاهش دادن میزان Spam :

- آدرس خود را بی دلیل در اختیار دیگران قرار ندهیم.
- بررسی سیاستها محرمانگی– قبل از ثبت ایمیل در یک سایت از سیاستهای اعلام شده در ارتبط با حفظ اطلاعات در آن سایت مطلع شویم
- دقت لازم در مورد گزینه هایی که بصورت پیش فرض فعال شده اند. مثلا در هنگامsign in برای ورود به سرویس ایمیل یا پذیرفتن ارسال ایمیلهای مختلف از آن سایت
- استفاده از فیلتر ها- مثلا فیلترینگ از طریق رنامه های پست الکترونیکی یاISP
- عدم کلیک برروی لینکهای موجود در یک Spam چون معتبر بودن آدرس ایمیل خود را اعلام میکنیم
- غیر فعال نمودن گزینه دریافت اتوماتیک گرافیک در نامه های الکترونیکی با فرمت HTML
- ایجاد و یا باز نمودن account های جدید اضافی برای محرمانگی بیشتر در دسترسی های online یا تجاری و....
- برای سایرین بعنوان کاربر متعهد Spam ارسال نگردد.

SPYWARE(adware)

نرم افزاری است که اقدام به جمع آوری اطلاعات شخصی بدون آگاهی و یا اجازه کاربران میکند.مانند لیست سایتهای مشاهده شده و-نام و رمز عبور ،این برنامه ها بر روی کامپیوتر مقصد بدون آگاهی کاربر نصب میگردد.

نحوه تشخیص spyware :

-نمایش مستمر پنجره های pop-up آگهی
- هدایت ناخواسته کاربران به وب سایتهایی که هرگز نام آنها در مرورگر تایپ نشده است.
- نصب toolbars جدید و ناخواسته در مرور گر وب
- تغییر ناگهانی و غیره منتظره صفحه اصلی مرورگر (home page)
- تغییر موتور جستجوی مرورگر پس از کلیک بر روی دکمه Search مرورگر
- عدم عملکرد صحیح برخی کلیدها در مرورگر
- نمایش تصادفی پیام های خطا
- کاهش ملموس سرعت کامپیوتر در زمان فعال نمودن برنامه ها و یا انجام عملیات خاص (مانند ذخیره فایل)
- فعال شدن اتوماتیک (بدون دخالت کاربر) مرورگر و بدنبال آن وب سایتهای آگهی
- عدم کارکرد صحیح لینکهای همراه یک برنامه
- عدم عملکرد صحیح برخی کلیدها در مرورگر
- توقف ناگهانی و غیره منتظره مرورگر وب
- عدم عملکرد صحیح برخی از عناصر سیستم عامل و یا سایر برنامه ها

نحوه پیشگیری از نصب Spyware:

- عدم کلیک بر روی لینکهای موجود در پنجره های pop-up و بستن آن از علامت×
- پاسخ منفی به سئولات ناخواسته و در موارد خاص استفاده از ایکون × موجود در titlebar
- دقت لازم در خصوص دریافت نرم افزارهای رایگان از اینترنت (download)

- عدم کلیک بر روی لینکهای موجود در Email که ادعای ارائه یک نرم افزار Anti-Spyware را دارند.

- اعمال محدودیت در رابطه با پنجره های Pop-up و کوکی از طریق تنظیمات برنامه مرورگر

نحوه حذف Spyware:

- اجرای یک برنامه ضد ویروس و پویش کامل کامپیوتر

- اجرای یک برنامه معتبر که مختص حذف Spyware طراحی شده است.

نرم افزارهای جاسوسی چیست:

هر نوع فناوری یا برنامه بر روی کامپیوتر است که اطلاعات را بصورت پنهانی جمع آوری میکند.

بعضی نرم افزارهای جاسوسی فقط اطلاعات سیستمی را ردیابی میکنند مانند نوع اتصال کاربر به اینترنت و سیستم عامل آن

الباقی نرم افزارهای جاسوسی اطلاعات فردی را جمع آوری میکنند مانند رد گیری عادات و علاقه کاربر در اینترنت یا فایلهای شخصی

انواع نرم افزارهای جاسوسی

نرم افزارهای جاسوسی خانگی (Domestic Spyware) :

نرم افزاری است که معمولا توسط صاحبان کامپیوترها به منظور آگاهی یافتن از تاثیرات اینترنت بر روی شبکه های کامپیوتری خودشان خریداری و نصب میگردد مانند آگاهی مدیران از فعالیتهای آنلاین کارمندان خود یا مشاهده اتاقهای گفتگو اینترنتی توسط والدین

نرم افزارهای جاسوسی تجاری (Commercial Spyware) :

این نرم افزار که بعنوان adware نیز شناخته میشود نرم افزاری است که شرکتها برای تعقیب فعالیتهای وبگردی کاربران اینترنت استفاده میکنند .این شرکتها اغلب اطلاعات حاصل را به بازاریابان می فروشند و آنها کاربران را با تبلیغات خاص مورد هدف قرار میدهند.

انواع و اهداف نرم افزار های جاسوسی مختلف

- ثبت کنندگان نشانی های وب و صفحات نمایش

- ثبت کنندگان چت و ایمیلها

- ثبت کنندگان کلید (کیبورد) و کلمات عبور

- حشرات وبی :جاسوسان تبلیغ کننده که به آن نرم افزارهای تبلیغ نیزگفته میشود

- مرورگر ربایان :به خدمت گرفتن مرورگر برای ارسال اسپم به کامپیوتر های دیگر

- مودم ربایان:نصب یک شماره گیر آنلاین برای برقراری یک اتصال جدید اینترنت بر روی کامپیوتر قربانی

- PC ربایان:میانبر های اینترنتی را در favorite مرورگر قرار میدهند که باعث میشود بطور اتفاقی از وب سایت مورد نظر دیدن شود.

- تروا‌ها و ویروسها: تراوا باعث میشود دیتا کپی،توزیع و یا تخریب شود و فرق آن با ویروس اینست که تکثیر نمیشود.

چگونگی قرار گرفتن نرم افزارهای جاسوسی روی کامپیوتر

- باز کردن ایمیل اسپمی

- کلیک کردن روی پنجره های باز شونده فریبنده

- دانلود کردن رایگان برنامه ها ،بازیها،ابزارها و غیره

- برنامه های اشتراک فایل مانند emule,kazza

- مشاهده وب سایتهای ناجور

- نرم افزارهای اجرای فایلهای صوتی و تصویری آنلاین

روشهای مقابله با نرم افزارهای جاسوسی

- تنظیم سطح امنیتی مرورگر به سطح پیش گزیده یا بالاتر

- نظارت دقیق برآنچه دانلود میشود

- به روز نگهداشتن سیستم عامل کامپیوتر

- نصب یک برنامه جاسوسی Anti Spyware

حمله مهندسی اجتماعی چیست؟

یک مهاجم با برقراری ارتباط با کاربران و استفاده از مهارتهای خاص (روابط عمومی مناسب،ظاهری آراسته،...) سعی مینماید به اطلاعات حساس یک سازمان و یا کامپیوتر شما دستیابی و یا به آنان آسیب رساند. بنابراین می بایست هرگز اطلاعات حساس خود و یا سازمان خود را در اختیار دیگران قرار ندهیم مگر اینکه مطمئن شویم آن فرد همان شخصی است که ادعا می نماید و میبایست به آن اطلاعات دسترسی داشته باشد.

یک حمله Phishing چیست؟

این نوع حملات شکل خاصی از حملات مهندسی اجتماعی بوده که با هدف کلاهبرداری و شیادی سازماندهی میشوند.در حملات فوق از آدرسهای Email و یا وب سایتهای مخرب به منظور جلب نظر کاربران و دریافت اطلاعات شخصی آنها نظیر اطلاعات مالی استفاده میشود. مانند ارسال یک email با ظاهری قابل قبول از طرف یک شرکت معتبر کارت اعتباری برای بدست آوردن اطلاعات مالی افراد و سوء استفاده از طریق اطلاعات بدست آمده.

نحوه پیشگیری از حملات مهندسی اجتماعی و کلاهبرداری

- به تلفنها ،نامه های الکترونیکی و ملاقاتهایی که عموما ناخواسته بوده و در آن درخواست اطلاعات خاص در مورد کارکنان و یا سایر اطلاعات شخصی میگردد مشکوک بوده و با سوء ظن به آن نگاه گردد.
- عدم ارائه اطلاعات شخصی و اطلاعات سازمان(مثلا ساختار و یا شبکه ها) به افرادی که صلاحیت آنها تایید شده است.
- عدم ارائه اطلاعات شخصی و یا مالی از طریق Email
- عدم ارسال اطلاعات شخصی یا سازمانی از طریق اینترنت قبل از اینکه Privacy آن وب سایت بدقت مطالعه شده باشد.
- دقت لازم در خصوص آدرس URL یک وب سایت (ممکن است سایتها همنام باشند ولی نام domain آنها متفاوت باشد.)
- در صورت عدم اطمینان از معتبر بودن یک email دریافتی با برقراری تماس مستقیم از هویت آن اطمینان حاصل کنیم.
- نصب و بروز رسانی نرم افزارهای Antivirus,Antispam,firewall

اقدامات لازم در صورت بروز تهاجم

- بلا فاصله موضوع را به افراد ذیربط اطلاع دهیم(مدیران شبکه)
- اگر اطلاعات مالی مورد تهدید باشد با موسسه مالی خود تماس گرفته و حسابها را مسدود گردد
- گزارشی از نوع تهاجم تهیه گردد و در اختیار سازمانهای ذیربط قانونی قرار گیرد.

پیشگیریهای لازم در خصوص بروز تهاجم

- سیستم عامل و نرم افزارهای موجود در یک محیط آزمایشی تست(توصیف) گردند واز نظرسرعت پاسخگویی،نحوه عمل و....
- استفاده از نرم افزارهای توصیف مانند Tripwire
- استفاده از ابزارهای تشخیص نفوذ (host-based) با توجه به نسخه سیستم عامل
- بررسی ترافیک شبکه: تعداد email ها یا زیادی اتصالات http
- کارایی: بررسی سرعت وب و یا تعداد تراکنش سرورها
- بررسی دستکاری شدن سیستم عامل

پیشگیریهای لازم در خصوص بروز تهاجم از طریق ضمائم پست الکترونیک

- بررسی ضمائم نامه های الکترونیکی بعلت تنوع آنها حتی برای آنان که هویتشان برای ما شناخته شده است.
- ذخیره وبررسی ضمائم با نرم افزار بروز شده آنتی ویروس
- غیر فعال نمودن ویژگی در یافت اتوماتیک فایلهای ضمیمه

تفاوت ابزارهای استفاده شده برای مبادلات Online

برنامه های IM(instant massage):

-این نوع برنامه ها بستر مناسبی برای ارتباطات یک به یک را ایجاد میکند و به منظور تفریح،سرگرمی،ارسال پیام،ارتباط صوتی یا تصویری و برای ارتباط بین کارکنان نیز استفاده میشود.

اطاقهای چت:

- تالارهایی برای گروههای خاص از مردم برای ارتباط با یکدیگر میباشند و بیشتر نرم افزارهای IM نیز قابلیت چت را دارند از چت بطور سنتی برای استفاده چند به چند نیز استفاده میشود و برای پیاده سازی نرم افزارهای چت از فناوریهای متعددی نظیر IM,IRC,Jabber استفاده میشود.

تهدیدات برنامه های IM,Chat

- وجود ابهام در مورد هویت مخاطب :استفاده از یک account توسط چندین نفر
- عدم وجود آگاهی لازم در خصوص سایر افراد درگیر و یا ناظر گفتگو : امکان ذخیره سازی ماحصل گفتگو بر روی سرویس دهنده Log
- امکان آسیب پذیری نرم افزار مورد استفاده
- تنظیمات امنیتی پیش فرض ممکن است به درستی مقدار دهی نشده باشد (امنیت پایین)

چگونه میتوان از ابزارهای IM,Chat به صورت ایمن استفاده نمود.

- بررسی و ارزیابی تنظیمات امنیتی:تغییر پیش فرض برنامه و غیر فعال کردن ویژگی در یافت اتوماتیک
- هوشیاری و دقت لازم در خصوص افشای اطلاعات
- شناسایی هویت افرادیکه در حال گفتگو با آنها هستید(حد المقدور)
- عدم اعتماد و باور هر چیز
- بهنگام نگه داشتن نرم افزارها: نرم افزار مرورگر وب، IM ،سیستم عامل ،پست الکترونیک،آنتی ویروس

انتخاب و محافظت از کلمات عبور

- تمام کلمات عبور در سطح سیستم باید حد اقل سه ماه یکبار عوض شوند.
- تمام کلمات عبور سطح کاربر(مانند ایمیل و کامپیوتر) باید هر شش ماه تغییر کند (بهینه چهار ماه)
- اکانتهای کاربری که مجوزهای سطح سیستم دارند باید کلمات عبوری داشته باشند که با کلمات عبور دیگر اکانتهای آن کاربر متفاوت باشند.
- کلمات عبور نباید در ایمیلها یا سایر شکلهای ارتباط الکترونیکی درج شوند

استفاده های معمول کلمات عبور

- اکانتهای سطح کاربر
- اکانتهای دسترسی به وب
- اکانتهای ایمیل
- حفاظت از مانیتور screen saver
- کلمه عبور صندوق پستی
- ورود به روتر محلی

مشخصات کلمات عبور ضعیف

- کلمه عبور کمتر از هشت کاراکتر
- کلمه عبوری که در فرهنگ لغت یافت شود. مانند نام خانوادگی ،حیوانات اهلی،دوستان ،.....
- نام شرکت یا کلمات مشتق شده از این نام
- تاریخ تولد و سایر اطلاعات شخصی
- الگوی کلمات یا شماره ها مانند 123321,zyxwvuts,qwerty,aaabbb
- هر کدام از عبارات فوق بطور برعکس
- هر کدام از عبارات فوق که تنها با یک رقم شروع یا به آن ختم شود

مشخصات کلمات عبور مناسب

- کلمه عبور شامل حروف بزرگ و کوچک (A-Z,a-z)
- علوه بر حروف از ارقام و نشانه ها استفاده شود مانند %Abghy789&
- حداقل 8 حرف دارند
- کلماتی که در هیچ زبان ،گویش و یا صنف خاصی نیستند
- برپایه اطلاعات شخصی نیستند
- کلمات عبور نباید هرگز جایی نوشته یا ذخیره شوند

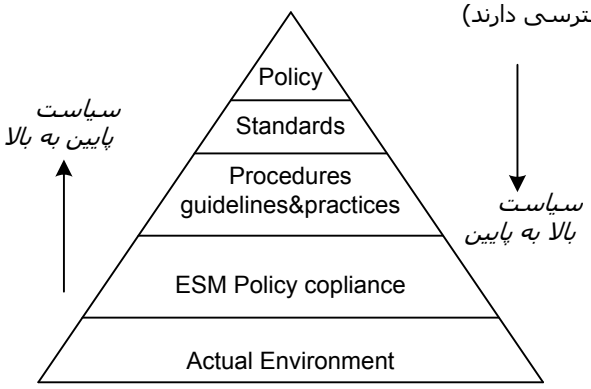
استاندارد های حفاظت از کلمه عبور

- کلمه عبور را از طریق تلفن به هیچ کس نگویید
- کلمه عبور را از طریق ایمیل فاش نکنید
- کلمه عبور را به رئیس نگویید
- در مورد کلمه عبور جلوی دیگران صحبت نکنید
- به قالب کلمه عبور اشاره نکنید(مثلا نام خانوادگی)
- کلمه عبور را روی فهرست سئولات یا فرمهای امنیتی درج نکنید
- کلمه عبور را با اعضای خانواده خود در میان نگذارید.
- کلمه عبور را در هنگامی که مرخصی هستید به همکاران نگوئید.
- اگر کسی از شما کلمه عبور راخواست از ایشان بخواهید که مطالب بالا را مطالعه کند و یا با کسی در قسمت امنیت اطلاعات تماس بگیرد
- از ویژگی Remember Password یا حفظ کلمه عبور در کامپیوتر استفاده نکنید.
- کلمات عبور را در هیچ جای محل کار خود یادداشت نکنید

سیاستهای امنیتی

سیاستهای امنیتی یک سازمان ،سندی است که برنامه های سازمان برای محافظت سرمایه های فیزیکی و مرتبط با فناوری اطلاعات و ارتباطات را بیان میکند و بعنوان یک سند زنده فرایند تکمیل و اصلاح آن متناسب با تغییر فناوری و نیازهای کاربران به روز میشود.

بهترین روش برای دستیابی به امنیت اطلاعات فرموله نمودن سیاست امنیتی است ،بطور کلی مشخص نمودن سرمایه های اصلی که باید امن شوند و تعیین سطح دسترسی افراد (چه افرادی به چه سرمایه هایی دسترسی دارند)



سیاست سازمان باید فعالیت خود را بر اساس اصول و استانداردهای صنعتی مانند ISO 17799 و یا HIPAA انجام دهد

محصولاتی مانند EMS سازگاری و انعطاف سیاست را با سیاستها و روالها ی امنیتی سیستم عاملها ،پایگاه داده ها و برنامه های کاربردی ارزیابی می نمایند.

سه محور اصلی در کنترل دسترسی در شبکه

AAA(Authentication,Authorization,Accounting)

Authentication

- پس از ارائه عناصر شناسایی از سوی متقاضی، سیستم کد کاربری و کلمه عبور را با بانک اطلاعاتی مختص کدهای شناسایی کاربری مقایسه کرده و پذیرش یا عدم پذیرش دسترسی به منابع را صادر میکند.
- عمل Authentication در طراحی شبکه هایی با حجم کم و متوسط عموما توسط تجهیزات مسیریابی و یا دیوارهای آتش انجام میپذیرد.
- عمل Authentication در طراحی شبکه هایی با حجم و پیچیدگی نسبتا بالا با استانداردهای +TACACS وRADIUS انجام میپذیرد.

فعال نمودن Authentication

1- فعال نمودن AAA بر روی سخت افزارهای مورد نظر

2- ایجاد پایگاه داده ای از کدهای کاربری کاربران یا تجهیزات شبکه به همراه کلمه های عبور

3- ایجاد فهرست(های) روش انجام عمل Authentication

4- اعمال فهرست(های) ساخته شده از مرحله قبل

Authorization

- فرایندی است که طی آن به کاربران و یا تجهیزات متقاضی دسترسی به منابع،امکان استفاده از منبع یا منابع مستقر در شبکه داده میشود.
-این عمل متقاضی را ملزم به استفاده از نوع خاصی از استانداردها یا پیکره بندیهای مورد نظر مدیر شبکه میکند.(مانند ملزم کردن به پرتکل PPP,Slip,....

فعال نمودن Authorization

1- فعال نمودن عمل Authentication بر روی سخت افزارهای مورد نظر بر اساس توضیحات 4 مرحله ای بالا

2- انجام فهرست(های) روش انجام عمل (مبین سرویس مورد نظر) Athorization

3- اعمال فهرست(های) ساخته شده از مرحله قبل

Accounting

- طی این فرایند گزارشی از عملکرد کاربران و یا سخت افزارهایی که هویت آنها طی اعمال Authentication وAuthorizatio تایید شده است به شکل رکورد میان تجهیزاتی که از طریق آنها دسترسی متقاضی درخواست شده و پایگاه داده ای از قبیل RADIUS یا +TACACS تبادل میگردد.

فعال نمودن Accounting

-همانند روشهای قبل

درگاه Port number

- هر بسته ای که در روی شبکه قرار میگیرد باید آدرس IP کامپیوتر گیرنده اطلاعات و همینطور شماره درگاه مربوطه را نیز در خود داشته باشد.
- شماره در گاه میتواند عددی بین 0 الی 65536 باشد
- درگاههای 0 الی 1023 رزرو هستند
- درگاههای 1024 الی 49151 برای خدمات ثبت شده اند
- درگاههای 49152 الی 65536 را اشخاص میتوانند استفاده کنند.
- در گاه توسط سیستم عامل باز نمیشود بلکه برنامه خاصی که در انتظار در یافت داده از این درگاه است آن را باز میکند.
- متوقف کردن سرویس یک برنامه از طریق ویندوز یا هر سیستم عامل دیگر باعث بستن درگاه میشود.

امضای دیجیتال

امضای دیجیتال از یک الگوریتم ریاضی به منظور ترکیب اطلاعات در یک کلید با اطلاعات پیام استفاده میشود و ماحصل آن تولید رشته ای مشتمل برمجموعه ای از حروف و پیام است.

تشخیص غیر جعلی بودن نامه های الکترونیکی

یک نامه الکترونیکی شامل یک امضای دیجیتال ،نشان دهنده این موضوع است که محتوی پیام از زمان ارسال تا زمانی که به دست گیرنده رسیده است تغییر نکرده است .در غیر اینصورت از درجه اعتبار ساقط میشود.

اصطلاحات امضای دیجیتال

کلیدها

کلیدخصوصی:
یک بخش ازکلید که شامل یک رمز عبور حفاظت شده بوده و نباید آنرا در اختیار دیگران قرار داد

کلیدعمومی:
بخشی از کلید است که برای یک حلقه کلید عمومی (key ring public) ویا شخص خاص ارسال میگردد ،آنان با استفاده از آن قادر به بررسی امضاء فرستنده خواهند بود.

حلقه کلید:
یک حلقه کلید از کلیدهای عمومی افرادی که برای ما کلید مربوط به خود را ارسال نموده و یا کلیدهایی که از طریق یک سرویس دهنده کلید عمومی دریافت نموده ایم

اثر انگشت:
هنگامی که یک کلید تایید میگردد در واقع منحصر بودن مجموعه ای از کلید و اعداد شامل اثر انگشت میشود.

گواهینامه های کلید:
در زمان انتخاب یک کلید از روی حلقه کلید به اطلاعات متفاوتی نظیر صاحب کلید،تاریخ ایجاد و اعتبار میشود دست یافت.

نحوه ایجاد و استفاده از کلیدها

-تولید یک کلید با استفاده از نرمافزارهایی نظیر PGP و GnuPG

- معرفی کلید تولید شده به سایر همکاران و افرادی که دارای کلید میباشند.

- ارسال کلید تولید شده به یک حلقه کلید عمومی تا سایر افراد قادر به بررسی و تایید امضای فرستنده شوند

- استفاده از امضای دیجیتال در زمان ارسال نامه های الکترونیکی

یک سیستم زیست سنجی شامل موارد زیر است(مثال ATM)

یک ابزار اندازه گیری: واسط کاربر را تشکیل میدهد.

نرم افزار عامل: شامل الگوریتمهای ریاضی است که پارامترهای سنجش شده را با الگوی مرجع مقایسه میکند.

سخت افزار و سیستمهای بیرونی: مانند تست اثر انگشت یا تشخیص صدا

تکنیکهای خصوصیات رفتاری برای تایید هویت
Behavioral

تایید امضاء:بررسی خودکار امضاء

الگو و دینامیک تایپ : تشخیص افراد ازروی الگوی تایپ کردن

تشخیص صدا:

تکنیکهای خصوصیات فیزیکی برای تایید هویت
Physiometric

اثر انگشت:

هندسه دست:

اسکن شبکیه: الگوی اسکن رگهای خونی بر رو ی شبکیه

اسکن عنبیه:

تحلیل DNA :

BCC چیست
Blind Carbon Copy

- امکان مخفی نگه داشتن آدرس دریافت کنندگان یک Email را فراهم میکند.

دلایل استفاده از BCC

- محرمانگی

- پیگیری: در صورتی که قصد پیگیری ،دستیابی و یا آرشیو نامه های الکترونیکی ارسالی بر روی یک accout دیگر را داشته باشیم.

- رعایت حقوق در یافت کنندگان: کمتر مشاهده شدن آدرس email دیگران

در برنامه outlook با فعال کردن headers all در منوی view میتوان BCC را فعال نمود.