خلاصه جلسات اول تا سوم دوره جامع شبکه

گردآورنده:آرمین امینیان

مدرس:محمدحسن ارمی

TYPE OF FIREWALL
SECURITY OF NETWORK DEVICES
5 PHASE OF PENTRATION
TYPE OF PENTRATION TESTING
TYPE OF NETWORK ATTACK

آشنایی با Firewall

Firewall اصولا یک سیستم سخت افزاری و یا نرم افزاری می باشد و یا ترکیبی از سخت افزار و نرم افزار که از دسترسی غیر مجاز به سمت شبکه ما و یا از سمت شبکه ما جلوگیری می کند به عنوان مثال افرادی که در بیرون از شبکه ی ما قرار دارند اجازه دسترسی به فایل سرور درون شبکه ما را ندارند (به سمت شبکه ما) و یا اینکه بعضی از کاربران شبکه ی ما اجازه دسترسی به اینترنت را ندارند (از سمت شبکه ما)

عموما Firewall را برای جلوگیری از دسترسی غیر مجاز از سمت جهان خارج تنظیم می کنند که منظور از جهان خارج هر شبکه ای به غیر از شبکه ی ما می باشد .

Firewall را براساس تعریفی از سازمان NSA می توان به انواع مختلف زیر تقسیم بندی کرد که بر اساس افزایش توانایی و پیچیدگی عملکرد مرتب شده اند :

- Packet Filtering
- Stateful Packet Filtering
- Application Proxies

Packet Filtering

یک Packet Filter ترافیک را فقط براساس Packet Header بررسی می کند که این Header شامل آدرس IP مبدا و مقصد ، آدرس Port مبدا و مقصد و پروتکل استفاده شده می باشد .

Packet Filtering معمولا به صورت Access Control List (ACL) بر روی روترها پیاده سازی می شود که عملکرد ACL بر روی روتر بسیار سریع و موثر می باشد . در ACL نیز می توان Rules را بر حسب Protocol ، رنج آدرس های مبدا و مقصد و حتی نیز ترافیک ورودی و خروجی نوشت .(Extended ACL)

Router ACL

	In-Flow	Out-Flow
Source IP	Client	**Server**
Destination IP	Server	**Client**
Source Port	ANY	**TCP/80**
Destination Port	23/TCP	**Any**
Decision	Deny	**Allow**

به عنوان مثال در دیاگرام بالا یک Client قصد ارتباط با یک سرور از طریق ارتباط Telnet را دارد و با توجه به سیاست سازمان این Client اجازه دسترسی از طریق Telnet به سرور مورد نظرش را ندارد و با توجه به فاکتور های موجود برای دسترسی و یا عدم دسترسی می توان از قابلیت Packet Filtering استفاده کرد که برای پیاده سازی آن می توان از روتر به همراه ACL استفاده نمود .

Stateful Packet Filtering

مانند Packet Filtering ، Stateful Packet Filtering نیز در لایه Transport و Network مدل OSI ، Packet Header را بررسی می کند با این تفاوت که اگرجریانی از ترافیک اجازه عبور را داشته باشد اطلاعاتی در مورد وضعیت Connection این ترافیک ذخیره شده و در جدولی به نام State Table ذخیره می شود . که این اطلاعات شامل آدرس IP مبدا و مقصد ، Interface ورودی ترافیک ، شماره Port مبدا و مقصد ، پروتکل و همچنین ACK & SEQ Number و مواردی از این قبیل می باشد .

در این روش Rules ها می توانند به صورت خیلی سریعتر از سیستم Packet Filtering و به صورت اتوماتیک تولید شوند و دیگر نیاز به وارد کردن آنها به صورت دستی نمی باشد .

مکانیزم این سیستم بدین صورت می باشد که ترافیک ورودی به سمت Firewall ابتدا توسط State Table چک می شود نه توسط ACL ! حال اگر این ترافیک ورودی جزو یک Established Connection باشد این ترافیک اجازه عبور از Firewall را دارد در غیر این صورت این ترافیک ورودی با ACL ها چک می شود و اگر مورد قبول واقع شود وارد State Table می شود .

Example State Table

Rule Description	Flow
Source IP	**Server**
Destination IP	**Client**
Source Port	**TCP/80**
Destination Port	**ANY**
ACK	**1000**
SEQ	**200**
Firewall Interface	**Etho**

بعضی از Stateful Packet Filter توانایی این را دارند که با توجه به اطلاعات و پروتکل های لایه Application نیز کار کنند به عنوان مثال اجازه استفاده از HTTP GET Message مجاز باشد ولی HTTP POST Message غیر مجاز باشد .

ضعف این Firewall 1 – محدودیت در پروتکل ها قابل استفاده برای تصمیم گیری 2 – و عدم توانایی Filtering بر روی ترافیک های رمز شده می باشد.

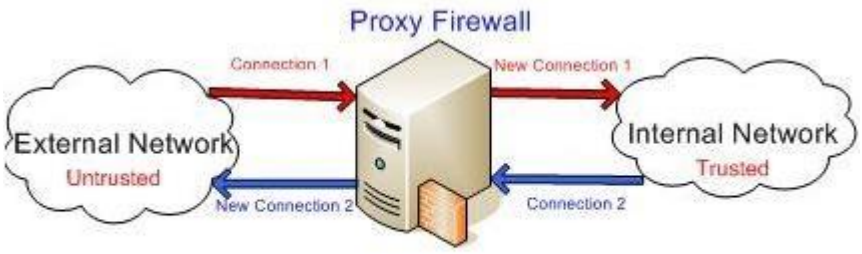
مثالی از این Firewall ها :PiX , NetScreen

Application Proxies

این مدل از Firewall ها یکی از پیچیده ترین انواع Firewall می باشد . در این مدل از Firewall ها علاوه بر

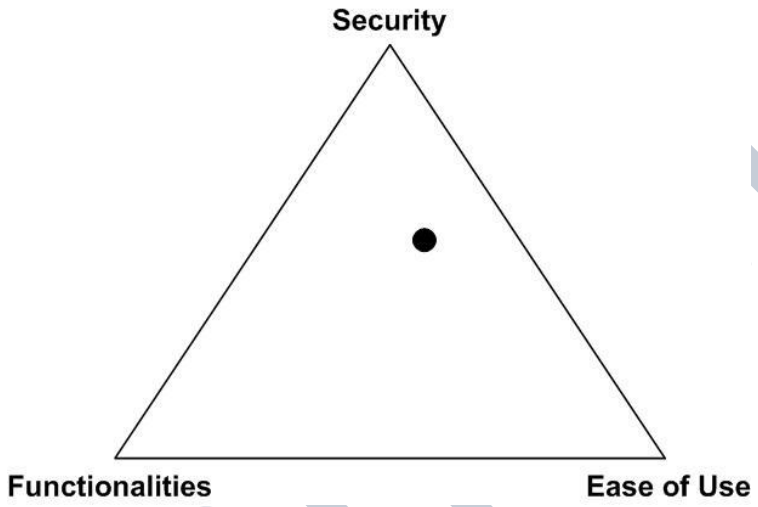
قابلیت هایی که در مدل های Stateful Packet Filters , Packet Filter وجود دارد که وجود یک پروسه هم برای سمت Client و هم برای Server به ازای هر پروتکل است . در این مدل Session از سمت Client به سمت Server به دو Session جداگانه تقسیم می شود یک Session از Client به Firewall و Session دیگری از سمت Firewall به سمت Server . در این حالت Firewall در حالت Proxy عمل می کند و ترافیک را چک کرده و در صورت مجاز بودن آنها را دوباره بر روی Session دیگری ارسال می کند که در این حالت از ارتباط مستقیم بین Client و Server جلوگیری می شود یکی از قابلیت های مهم این نوع از Firewall ها توانایی خواندن ترافیک رمز شده می باشد . Firewall همچنین با طرز کار پروتکل ها آشنایی دارد و می تواند پروتکل ها را مجبور به رعایت سیاست جاری کند (برای کسب مجوز)

این مدل از Firewall ها در مقابل دیگر انواع Firewall از سرعت کمتری برخوردار است که بدلیل پیچیدگی مکانیزم کنترل ترافیک می باشد ، به عنوان مثال این نوع Firewall می تواند در جلوگیری از حمله Overflow موفقیت بیشتری نسبت به دیگر Firewall ها کسب کند .



کدام نوع !؟

برای پاسخ به این سوال باید نوعی از Firewall را انتخاب کرد که بتواند به خوبی از پیاده کردن سیاست امنیتی ما بر آید و همچنین بر دو فاکتور دیگر از مثلث امنیتی ما تاثیر منفی نداشته باشد !



همچنین باید به این نکته توجه کرد که یک Firewall به تنهایی نمی تواند امنیت صد در صد را برای ما فراهم سازد و ما نیاز به استراتژی های امنیتی دیگری برای برقراری امنیت مورد نیازمان خواهیم داشت .

امنیت تجهیزات شبکه

برای تامین امنیت بر روی یک شبکه، یکی از بحرانی ترین و خطیرترین مراحل، تامین امنیت دسترسی و کنترل تجهیزات شبکه است. تجهیزاتی همچون مسیریاب، سوئیچ یا دیوارهای آتش.

اهمیت امنیت تجهیزات به دو علت اهمیت ویژه‌ای می‌یابد :

الف – عدم وجود امنیت تجهیزات در شبکه به نفوذگران به شبکه اجازه می‌دهد که با دسترسی به تجهیزات امکان پیکربندی آنها را به گونه‌ای که تمایل دارند تغییر بدهند بنابراین فرد نفوذگر می تواند هرگونه نفوذ و سرقت اطلاعات و یا هر نوع صدمه دیگر به شبکه را به راحتی عملی کند .

ب – برای جلوگیری از خطرهای DoS (Denial of Service) تأمین امنیت تجهزات بر روی شبکه الزامی است. توسط این حمله‌ها فرد نفوذگر می تواند سرویس‌هایی را در شبکه از کار بیاندازد و یا مختل کند که از این طریق در برخی موارد امکان دسترسی به اطلاعات با دور زدن هر یک از فرایندهای AAA فراهم می‌شود.

حال اصول اولیه امنیت تجهیزات مورد بررسی اجمالی قرار می دهیم . عناوین برخی از این موضوعات به شرح زیر هستند :

- امنیت فیزیکی و تأثیر آن بر امنیت کلی شبکه
- امنیت تجهیزات شبکه در سطوح منطقی
- بالابردن امنیت تجهیزات توسط افزونگی در سرویس‌ها و سخت‌افزارها

موضوعات فوق در قالب دو جنبه اصلی امنیت تجهیزات مورد بررسی قرار می‌گیرند :

- امنیت فیزیکی
- امنیت منطقی

۱ – امنیت فیزیکی

امنیت فیزیکی بازه وسیعی از تدابیر را در بر می‌گیرد که استقرار تجهیزات در مکان‌های امن و به دور از خطر حملات نفوذگران و استفاده از افزونگی در سیستم از آن جمله‌اند(Fault Tolerance).

با استفاده از افزونگی، اطمینان از صحت عملکرد سیستم در صورت ایجاد و رخداد نقص در یکی از تجهیزات و یا سرویس های شبکه (با جایگزین کردن آن) بدست می آید .

در بررسی امنیت فیزیکی و اعمال آن، ابتدا باید به خطرهایی که از این طریق تجهزات شبکه را تهدید می‌کنند نگاهی داشته باشیم. پس از شناخت نسبتاً کامل این خطرها و حمله‌ها می‌توان به راه‌حل‌ها و ترفندهای دفاعی در برار این‌گونه حملات پرداخت.

در امنیت فیزیکی ابتدا باید خطرهای و حملاتی که در این زمینه تجهیزات شبکه را تهدید می کند شناسایی کرد و پس از شناخت این خطرها و حمله ها می توان راه حلی برای دفاع در مقابل این حملات و یا خطرها پرداخت.

به عنوان مثال برای جلوگیری از دسترسی فیزکی غیر مجاز به تجهیزات شبکه می توان تجهیزات را در محلی نگهداری کرد که فقط افراد مجاز به این محل دسترسی دارند و همچنین در این محل از دوربین های مداربسته استفاده کرد .

۱-۱ – افزونگی در محل استقرار شبکه

یکی از راه‌کارها در قالب ایجاد افزونگی در شبکه‌های کامپیوتری ایجاد سیستمی کامل مشابه شبکه‌ی اولیه‌ی در حال کار است. در این راستا، شبکه‌ی ثانویه‌ی، کاملاً مشابه شبکه‌ی اولیه، چه از بعد تجهیزات و چه از بعد کارکرد، در محلی که می‌تواند از نظر جغرافیایی با شبکه‌ی اول فاصله‌ای نه چندان کوتاه نیز داشته باشد برقرار می‌شود. با استفاده از این دو سیستم مشابه، علاوه بر آنکه در صورت رخداد وقایعی که کارکرد هریک از این دو شبکه را به طور کامل مختل می‌کند (مانند زلزله) می‌توان از شبکه‌ی دیگر به طور کاملاً جایگزین استفاده کرد، در استفاده‌های روزمره نیز در صورت ایجاد ترافیک سنگین بر روی شبکه، حجم ترافیک و پردازش بر روی دو شبکه‌ی مشابه پخش می‌شود تا زمان پاسخ به حداقل ممکن برسد.

با وجود آنکه استفاده از این روش در شبکه‌های معمول که حجم چندانی ندارند، به دلیل هزینه‌های تحمیلی بالا، امکان‌پذیر و اقتصادی به نظر نمی‌رسد، ولی در شبکه‌های با حجم بالا که قابلیت اطمینان و امنیت در آنها از اصول اولیه به حساب می‌آیند از الزامات است.

برای مثال می توان در سطح روترهای شبکه از پروتکل های VRRP,HSRP استفاده کرد و یا در سطح سرورهای AD از چند سرور به عنوان BDC(Backup Domain Controller) استفاده کرد که در صورت از کار افتادن روترها و یا سرورها ، روترس و یا سروری برای جایگزینی وجود داشته باشد .

۱ – ۲ – توپولوژی شبکه

طراحی توپولوژیکی شبکه، یکی از عوامل اصلی است که در زمان رخداد حملات فیزیکی می‌تواند از خطای کلی شبکه جلوگیری کند.

در این مقوله، سه طراحی که معمول هستند مورد بررسی قرار می‌گیرند :

الف – طراحی سری : در این طراحی با قطع خط تماس میان دو نقطه در شبکه، کلیه سیستم به دو تکه منفصل تبدیل شده و امکان سرویس دهی از هریک از این دو ناحیه به ناحیه دیگر امکان پذیر نخواهد بود.

ب – طراحی Star : در این طراحی، در صورت رخداد حمله فیزیکی و قطع اتصال یک نقطه از شبکه اصلی، سرویس‌دهی به دیگر نقاط دچار اختلال نمی‌گردد. با این وجود از آنجاییکه شبکه اصلی در این میان نقش محوری دارد، در صورت اختلال در کارایی این نقطه مرکزی، که می‌تواند بر اثر حمله فیزیکی به آن رخ دهد، ارتباط کل شبکه دچار اختلال می‌شود، هرچند که با درنظر گرفتن افزونگی برای شبکه اصلی از احتمال چنین حالتی کاسته می‌شود.

ج – طراحی Mesh : در این طراحی که تمامی نقاط ارتباطی با دیگر نقاط در ارتباط هستند، هرگونه اختلال فیزیکی در سطوح دسترسی منجر به اختلال عملکرد شبکه نخواهد شد، با وجود آنکه زمان‌بندی سرویس‌دهی را دچار اختلال خواهد کرد. پیاده‌سازی چنین روش با وجود امنیت بالا، به دلیل محدودیت‌های اقتصادی، تنها در موارد خاص و بحرانی انجام می‌گیرد.

به عنوان مثال در سطح اینترنت روترها بصورت Mesh (و یا Partial Mesh) به یکدیگر متصل می باشند که در صورت بروز مشکل و یا افزایش ترافیک بر روی یک لینک بتوان از لینک دیگری برای ترافیک ها استفاده کرد .

۱-۳ – محل‌های امن برای تجهیزات

در تعیین یک محل امن برای تجهیزات دو نکته مورد توجه قرار می‌گیرد :

- یافتن مکانی که به اندازه کافی از دیگر نقاط مجموعه متمایز باشد، به گونه‌ای که هرگونه نفوذ در محل آشکار باشد.

- در نظر داشتن محلی که در داخل ساختمان یا مجموعه‌ای بزرگتر قرار گرفته است تا تدابیر امنیتی بکارگرفته شده برای امن سازی مجموعه‌ی بزرگتر را بتوان برای امن سازی محل اختیار شده نیز به کار گرفت.

با این وجود، در انتخاب محل، میان محلی که کاملاً جدا باشد (که نسبتاً پرهزینه خواهد بود) و مکانی که درون محلی نسبتاً عمومی قرار دارد و از مکان‌های بلااستفاده سود برده است (که باعث ایجاد خطرهای امنیتی می‌گردد)، می‌توان اعتدالی منطقی را در نظر داشت.

در مجموع می‌توان اصول زیر را برای تضمین نسبی امنیت فیزیکی تجهیزات در نظر داشت :

- محدود سازی دسترسی به تجهیزات شبکه با استفاده از قفل‌ها و مکانیزم‌های دسترسی دیجیتالی به همراه ثبت زمان‌ها، مکان‌ها و کدهای کاربری دسترسی‌های انجام شده.
- استفاده از دوربین‌های مداربسته در ورودی محل‌های استقرار تجهیزات شبکه و اتاق‌های اتصالات و مراکز پایگاه‌های داده.
- اعمال ترفندهایی برای اطمینان از رعایت اصول امنیتی.

۱–۴ – انتخاب لایه کانال ارتباطی امن

با وجود آنکه زمان حمله‌ی فیزیکی به شبکه‌های کامپیوتری، آنگونه که در قدیم شایع بوده، گذشته است و در حال حاضر تلاش اغلب نفوذگران بر روی به دست گرفتن کنترل یکی از سرویس‌دهنده‌های مورد اطمینان شبکه معطوف شده است، ولی گونه‌ای از حمله‌ی فیزیکی کماکان دارای خطری بحرانی است.

عمل شنود بر روی سیم‌های مسی، چه در انواع Coaxial و چه در Twisted Pair، هم‌اکنون نیز از راه‌های نفوذ به شمار می‌آیند. با استفاده از شنود می‌توان اطلاعات بدست آمده از تلاش‌های دیگر برای نفوذ در سیستم‌های کامپیوتری را گسترش داد و به جمع‌بندی مناسبی برای حمله رسید. هرچند که می‌توان سیم‌ها را نیز به گونه‌ای مورد محافظت قرار داد تا کمترین احتمال برای شنود و یا حتی تخریب فیزیکی وجود داشته باشد، ولی در حال حاضر، امن ترین روش ارتباطی در لایه‌ی فیزیکی، استفاده از فیبرهای نوری است. در این روش به دلیل نبود سیگنال‌های الکتریکی، هیچگونه تشعشعی از نوع الکترومغناطیسی وجود ندارد، لذا امکان استفاده از روش‌های معمول شنود به پایین‌ترین حد خود نسبت به استفاده از سیم در ارتباطات می‌شود.

۱–۵ – منابع تغذیه

از آنجاکه داده‌های شناور در شبکه به منزله‌ی خون در رگهای ارتباطی شبکه هستند و جریان آنها بدون وجود منابع تغذیه، که با فعال نگاه‌داشتن نقاط شبکه موجب برقراری این جریان هستند، غیر ممکن است، لذا چگونگی چینش و نوع منابع تغذیه و قدرت آنها نقش به سزایی در این میان بازی می‌کنند. در این مقوله توجه به دو نکته زیر از بالاترین اهمیت برخوردار است :

- طراحی صحیح منابع تغذیه در شبکه بر اساس محل استقرار تجهیزات شبکه. این طراحی باید به گونه‌ای باشد که تمامی تجهیزات فعال شبکه، برق مورد نیاز خود را بدون آنکه به شبکه‌ی تامین فشار بیش‌اندازه‌ای (که باعث ایجاد اختلال در عملکرد منابع تغذیه شود) وارد شود، بدست آورند.
- وجود منبع یا منابع تغذیه پشتیبان به گونه‌ای که تعداد و یا نیروی پشتیبانی آنها به نحوی باشد که نه تنها برای تغذیه کل شبکه در مواقع نیاز به منابع تغذیه پشتیبان کفایت کند، بلکه امکان تامین افزونگی مورد نیاز برای تعدادی از تجهیزات بحرانی درون شبکه را به صورت منفرد فراهم کند.

۱ – ۶ – عوامل محیطی

یکی از نکات بسیار مهم در امن سازی فیزیکی تجهیزات و منابع شبکه، امنیت در برار عوامل محیطی است. نفوذگران در برخی از موارد با تاثیرگذاری بر روی این عوامل، باعث ایجاد اختلال در عملکرد شبکه می‌شوند. از مهمترین عواملی در هنگام بررسی امنیتی یک شبکه رایانه‌ای باید در نظر گرفت می‌توان به دو عامل زیر اشاره کرد :

- احتمال حریق (که عموماً غیر طبیعی است و منشآ انسانی دارد)
- زلزله، طوفان و دیگر بلایای طبیعی

با وجود آنکه احتمال رخداد برخی از این عوامل، مانند حریق، را می‌توان تا حدود زیادی محدود نمود، ولی تنها راه حل عملی و قطعی برای مقابله با چنین وقایعی، با هدف جلوگیری در اختلال کلی در عملکرد شبکه، وجود یک سیستم کامل پشتیبان برای کل شبکه است. تنها با استفاده از چنین سیستم پشتیبانی است که می‌توان از عدم اختلال در شبکه در صورت بروز چنین وقعایعی اطمینان حاصل کرد.

۲ – امنیت منطقی

امنیت منطقی به معنای استفاده از روش‌هایی برای پایین آوردن خطرات حملات منطقی و نرم‌افزاری بر ضد تجهیزات شبکه است. برای مثال حمله به روترها و سوئیچ‌های شبکه بخش مهمی از این گونه حملات را تشکیل می‌دهند. در این بخش به عوامل و مواردی که در اینگونه حملات و ضد حملات مورد نظر قرار می‌گیرند می‌پردازیم.

۲ – ۱ – امنیت روترها

حملات ضد امنیتی منطقی برای روترها و دیگر تجهیزات فعال شبکه، مانند سوئیچ‌ها، را می‌توان به سه دسته‌ی اصلی تقسیم نمود :

- حمله برای غیرفعال سازی کامل
- حمله به قصد دستیابی به سطح کنترل
- حمله برای ایجاد نقص در سرویس‌دهی

طبیعی است که راه‌ها و نکاتی که در این زمینه ذکر می‌شوند مستقیماً به امنیت این عناصر به تنهایی مربوط بوده و از امنیت دیگر مسیرهای ولو مرتبط با این تجهیزات منفک هستند. لذا تأمین امنیت تجهیزات فعال شبکه به معنای تأمین قطعی امنیت کلی شبکه نیست، هرچند که عملاً مهمترین جنبه‌ی آنرا تشکیل می‌دهد.

۲-۲ – مدیریت پیکربندی

یکی از مهمترین نکات در امینت تجهیزات، نگاهداری نسخه پشتیبان فایل های پیکربندی است. از این فایل ها که در حافظه‌های گوناگون این تجهیزات نگاهداری می‌شوند، می‌توان در فواصل زمانی مرتب یا تصادفی، و یا زمانی که پیکربندی تجهیزات تغییر می‌یابند، نسخه پشتیبان تهیه کرد.

با وجود فایلا پشتیبان، منطبق با آخرین تغییرات اعمال شده در تجهیزات، در هنگام رخداد اختلال در کارایی تجهزات، که می‌تواند منجر به ایجاد اختلال در کل شبکه شود، در کوتاه‌ترین زمان ممکن می‌توان با جایگزینی آخرین پیکربندی، وضعیت فعال شبکه را به آخرین حالت بی‌نقص پیش از اختلال بازگرداند. طبیعی است که در صورت بروز حملات علیه بیش از یک سخت‌افزار، باید پیکربندی تمامی تجهیزات تغییریافته را بازیابی نمود.

نرم‌افزارهای خاصی برای هر دسته از تجهیزات مورد استفاده وجود دارند که قابلیت تهیه فایل پشتیبان را فاصله‌های زمانی متغیر دارا می‌باشند. با استفاده از این نرم‌افزارها احتمال حملاتی که به سبب تآخیر در ایجاد پشتیبان بر اثر تعلل عوامل انسانی پدید می‌آید به کمترین حد ممکن می‌رسد.

۲-۳ – کنترل دسترسی به تجهیزات

دو راه اصلی برای کنترل تجهزات فعال وجود دارد :

- کنترل از راه دور
- کنترل از طریق درگاه کنسول

در روش اول می‌توان با اعمال محدودیت در امکان پیکربندی و دسترسی به تجهیزات از آدرس‌هایی خاص یا استانداردها و پروتکل‌های خاص، احتمال حملات را پایین آورد.

در مورد روش دوم، با وجود آنکه به نظر می‌رسد استفاده از چنین درگاهی نیاز به دسترسی فیزکی مستقیم به تجهیزات دارد، ولی دو روش معمول برای دسترسی به تجهیزات فعال بدون داشتن دسترسی مستقیم وجود دارد. لذا در صورت عدم کنترل این نوع دسترسی، ایجاد محدودیت‌ها در روش اول عملاً امنیت تجهیزات را تآمین نمی‌کند.

برای ایجاد امنیت در روش دوم باید از عدم اتصال مجازی درگاه کنسول به هریک از تجهیزات داخلی مسیریاب، که امکان دسترسی از راه‌دور دارند، اطمینان حاصل نمود.

۲-۴ – امن سازی دسترسی

علاوه بر پیکربندی تجهیزات برای استفاده از Authentication، یکی دیگر از روش‌های معمول امن‌سازی دسترسی، استفاده از کانال رمز شده در حین ارتباط است. یکی از ابزار معمول در این روش SSH(Secure Shell) است. SSH ارتباطات فعال را رمز کرده و احتمال شنود و تغییر در ارتباط که از معمول‌ترین روش‌های حمله هستند را به حداقل می‌رساند.

از دیگر روش‌های معمول می‌توان به استفاده از کانال‌های VPN مبتنی بر IPsec اشاره نمود. این روش نسبت به روش استفاده از SSH روشی با قابلیت اطمینان بالاتر است، به گونه‌ای که اغلب تولیدکنندگان تجهیزات فعال شبکه، خصوصاً تولید کنندگان روترها ، این روش را مرجح می‌دانند.

۲–۵ – مدیریت رمزهای عبور

مناسب‌ترین محل برای ذخیره رمزهای عبور بر روی سرور Authentication است. هرچند که در بسیاری از موارد لازم است که بسیاری از این رموز بر روی خود سخت‌افزار نگاه‌داری شوند. در این صورت مهم‌ترین نکته به یاد داشتن فعال کردن سیستم رمزنگاری رموز بر روی مسیریاب یا دیگر سخت‌افزارهای مشابه است.

۳ – ملزومات و مشکلات امنیتی ارائه دهندگان خدمات

زمانی که سخن از ارائه دهندگان خدمات و ملزومات امنیتی آنها به میان می‌آید، مقصود شبکه‌های بزرگی است که خود به شبکه‌های رایانه‌ای کوچکتر خدماتی ارائه می‌دهند. به عبارت دیگر این شبکه‌های بزرگ هستند که با پیوستن به یکدیگر، عملاً شبکه‌ی جهانی اینترنت کنونی را شکل می‌دهند. با وجود آنکه غالب اصول امنیتی در شبکه‌های کوچکتر رعایت می‌شود، ولی با توجه به حساسیت انتقال داده در این اندازه، ملزومات امنیتی خاصی برای این قبیل شبکه‌ها مطرح هستند.

۳–۱ – قابلیت‌های امنیتی

ملزومات مذکور را می‌توان، تنها با ذکر عناوین، به شرح زیر فهرست نمود :

۱ – قابلیت بازداری از حمله و اعمال تدابیر صحیح برای دفع حملات

۲ – وجود امکان بررسی ترافیک شبکه، با هدف تشخیص بسته‌هایی که به قصد حمله بر روی شبکه ارسال می‌شوند. از آنجاییکه شبکه‌های بزرگتر نقطه تلاقی مسیرهای متعدد ترافیک بر روی شبکه هستند، با استفاده از سیستم‌های IDS بر روی آنها، می‌توان به بالاترین بخت برای تشخیص حملات دست یافت.

۳ – قابلیت تشخیص منبع حملات. با وجود آنکه راه‌هایی از قبیل سرقت آدرس و استفاده از سیستم‌های دیگر از راه دور، برای حمله کننده و نفوذگر، وجود دارند که تشخیص منبع اصلی حمله را دشوار می‌نمایند، ولی استفاده از سیستم‌های ردیابی، کمک شایانی برای دست یافتن و یا محدود ساختن بازه‌ی مشکوک به وجود منبع اصلی می‌نماید. بیشترین تأثیر این مکانیزم زمانی است که حملاتی از نوع DoS از سوی نفوذگران انجام می‌گردد.

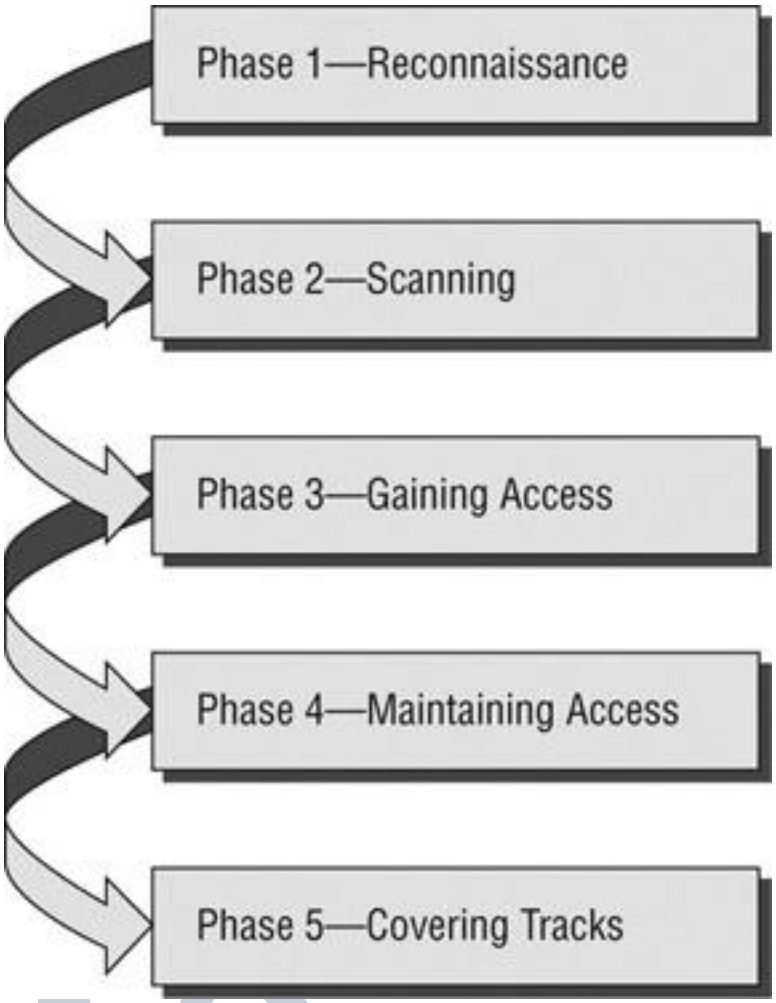
۳–۲ – مشکلات اعمال ملزومات امنیتی

با وجود لزوم وجود قابلیت‌هایی که بطور اجمالی مورد اشاره قرار گرفتند، پیاده‌سازی و اعمال آنها همواره آسان نیست.

یکی از معمول‌ترین مشکلات، پیاده‌سازی IDS است. خطر یا ترافیکی که برای یک دسته از کاربران به عنوان حمله تعبیر می‌شود، برای دسته‌ای دیگر به عنوان جریان عادی داده است. لذا تشخیص این دو جریان از یکدیگر بر پیچیدگی IDS افزوده و در اولین گام از کارایی و سرعت پردازش ترافیک و بسته‌های اطلاعاتی خواهد کاست. برای جبران این کاهش سرعت تنها می‌توان متوسل به تجهیزات گران‌تر و اعمال سیاست‌های امنیتی پیچیده‌تر شد.

با این وجود، با هرچه بیشتر حساس شدن ترافیک و جریان‌های داده و افزایش کاربران، و مهاجرت کاربردهای متداول بر روی شبکه‌های کوچکی که خود به شبکه‌های بزرگتر ارائه دهنده خدمات متصل هستند، تضمین امنیت، از اولین انتظاراتی است که از اینگونه شبکه‌ها می‌توان داشت.

5 فاز برای یک نفوذ موفق به یک شبکه


Phase 1—Reconnaissance
Phase 2—Scanning
Phase 3—Gaining Access
Phase 4—Maintaining Access
Phase 5—Covering Tracks

فاز 1 : Reconnaissance

فاز شناسایی معمولا یکی از طولانی ترین فازهای نفوذ به یک شبکه می باشد ، که معمولا **می تواند** چند هفته و حتی ماه طول بکشد. معمولا هکرها از منابع متنوعی برای کسب اطلاعات در مورد هدفشان و طریقه عملکرد آن استفاده می کنند که در زیر به مواردی اشاره شده است :

- جست و جو در سطح اینترنت
- مهندس اجتماعی
- Dumpster Diving
- کسب اطلاعات کلی در مورد شبکه : مانند فرد ثبت کننده دامنه سازمان

این فاز به گونه ای می باشد که عمل دفاع در مقابل آن کمی برای سازمان مشکل می باشد زیرا اطلاعات در مورد یک سازمان را می توان از طریق اینترنت و یا راه های گوناگونی بدست آورد ، به عنوان مثال کارمندان سازمان معمولا به راحتی گول خورده و اطلاعاتی از سازمان را در اختیار فرد نفوذگر قرار می دهند .

با این حال می توان سیاست هایی را در نظر گرفت که این فاز را برای فرد نفوذگر کمی دشوار تر کرد که شامل موارد زیر می شود :

- اطمینان حاصل کردن از پخش اطلاعات حساس در مورد سازمان در سطح اینترنت مانند :
  - نرم افزارهایی و ورژن آنها که در سازمان مورد استفاده قرار می گیرد
  - ایمیل آدرس های سازمان و کارمندان
  - اسامی و سمت افراد مهم در سازمان
- اطمینان از نابود کردن اطلاعت پرینت شده در سازمان

- استفاده از اطلاعات عمومی برای ثبت دامنه
- در دید نبودن تجهیزات LAN/Wan در سطح سازمان

فاز 2: Scanning

هنگامی که فرد نفوذگر اطلاعات کافی در مورد سازمان و نحوه کار آن بدست آورد اقدام به اسکن کردن تجهیزات درونی شبکه وکامپیوترها برای یافتن نقطه ضعفی می کند که شامل موارد زیر می باشد :

- Open Ports
- Open Services
- نرم افزار های نا امن مانند سیستم عامل
- محافظت ضعیف از ترافیک سازمان
- رسم یک نقشه برای شبکه سازمان

اسکن کردن تجهیزات سازمان معمولا بوسیله IDS شناسایی و یا بوسیله IPS جلوی آنها گرفته می شود ، اگر فرد نفوذگر از دانش خوبی برخوردار باشد این شناسایی و جلوگیری همیشه موفق نمی باشد !

در زیر بعضی از راه کارهای که برای بی نتیجه گذاشتن عمل اسکن کردن می توان انجام داد ذکر شده است :

- غیرفعال کردن تمام پورت ها و سرویس های غیرقابل استفاده
- تجهیزات حیاتی(مانند روتر مرکزی) فقط به درخواست های تجهیزات تایید شده پاسخ بدهند

- ادمین ها فقط بتوانند تجهیزات را بصورت لوکالی تنظیم کنند
- دسترسی ریموت با سیاست بسیار سخت تر از دسترسی از طریق لوکال تدوین گردد
- بروزرسانی تمامی تجهیزات بصورت مداوم

فاز 3 Gaining Access

کسب دسترسی به منابع مهترین **هدف** در نفوذ می باشد ، که فرد نفوذگر از طریق این منابع می تواند به اطلاعات مهمی دست پیدا کند و یا با استفاده از این منابع اقدام به نفوذ در قسمت های دیگر سازمان کند . در این فاز فرد نفوذگر تلاش می کند که دسترسی در هر سطحی کسب کند و سپس **درصورت امکان** این سطح دسترسی را افزایش دهد.

در این مورد مدیر امنیت باید اطمینان حاصل کند که سیستم ها و سرور های درون شبکه به راحتی توسط افراد تصدیق نشده غیر قابل دسترس اند که به عنوان مثال می توان به غیرفعال کردن دسترسی سطح ادمین بصورت لوکال برای کامپیوتر های درون **دامین** اشاره کرد .

یکی دیگر از مواردی که برای جلوگیری از به نتیجه رسیدن این فاز می توان انجام داد رمز کردن اطلاعات مهم و محافظت از کلید برای رمز گشایی است ، زیرا در بیشتر نفوذ ها هدف فرد نفوذگر بدست آوردن اطلاعات مهم می باشد که حتی اگر شبکه ما ضعیف باشد و نتوانیم جلو فرد نفوذگر را در موارد دیگری بگیریم با این کار می توانیم فرد نفوذ گر را از **رسیدن به هدفش مایوس کنیم .**

البته تنها نباید به مکانیزم رمز نگاری تکیه کرد ممکن است فرد نفوذگر قصد اختلال سیستم ها را داشته باشد و یا از شبکه ما برای رسیدن به مقاصد مجرمانه ی دیگری استفاده کند (مانند استفاده از سازمان به عنوان زامبی)

فاز 4 Maintaining Access

کسب دسترسی به یک شبکه از اهمیت قابل توجه ای برخوردار است ولی فرد نفوذگر در این فاز باید دسترسی اش را تا رسیدن به هدفش حفظ کند . با این حال که با رسیدن فرد نفوذ گر با رسیدن به این فاز توانسته سیسیتم امنیتی سازمان را پشت سر بگذارد اما در این فاز احتمال پیدا کردن فرد نفوذگر افزایش می یابد (منظور **از طریق** دسترسی). برای این کار می توان از IPS ویا IDS استفاده کرد که بررسی موارد زیر احتمال یافتن فرد نفوذ گر افزایش می یابد :

- شناسایی و جلوگیری ازانتقال فایل به بیرون سازمان
- شناسایی و جلوگیری از ارتباط مستقیم بین سرورها در درون دیتاسنتر و شبکه ها و یا سیسیتم هایی که تحت کنترل سازمان نمی باشند
- جلوگیری از ارتباط بر اساس پروتکل های غیر استاندارد
- شناسایی ارتباطات طولانی و با حجم زیاد تبادل ترافیک
- شناسایی رفتار غیر عادی شبکه و یا سرور های سازمان

فاز 5 Covering Tracks

در این فاز فرد نفوذگر پس از رسیدن به خواسته اش اقدام به پاک کردن نشانه های نفوذش می کند و همچنین راه نفوذش برای دفعات بعدی را تسهیل می کند (به عنوان مثال از Backdoor **استفاده می کند**).

انواع تست نفوذ

- Daniel Of Services (DoS)

این نوع از تست شامل تلاش برای حمله به یک نقطه ضعیف یک سیستم یا سرور به طور مداوم است که نتیجه آن می تواند عدم پاسخگویی این سرور یا سیستم یه درخواست های روتین باشد. در این نوع از تست می توان از ابزارهای آماده که بصورت اتوماتیک عمل می کنند و یا بصورت دستی استفاده کرد.این نوع از تست شامل دو نوع Software Exploit و Flood Attack می باشد.حد و یا میزان این نوع تست می تواند وابسته به اهمیت در دسترس بودن یک سرویس برای یک سازمان باشد. به عنوان مثال یک سایت فروش اینترنتی که نیاز دارد سرویس هایش همیشه در دسترس باشد این نوع تست برایش از اهمیت خاصی برخوردار می شود و نیاز است این نوع تست بصورت گسترده و طولانی تر بر روی سرویس هایش انجام شود .

این نوع از تست می تواند بصورت مدل های زیر صورت گیرد :

Resource Overload

در این نوع از حمله یا تست در تلاش هستیم که منابع هدفمان را اشغال کنیم که نتیجه آن می تواند عدم پاسخگویی هدف به درخواست ها به سمتش باشد .

Flood Attack

این نوع حمله یا تست شامل ارسال مقدار زیادی درخواست تحت شبکه به قصد Overload کردن هدف می باشد که می تواند به صورت های زیر انجام شود :

- ICMP (Smurf Attack)
- UDP (Fraggle Attack)
- Half Open SYN Attack

Out-Of-Band Attacks

در این نوع تست یا حمله قصد Crash شدن هدف مورد حمله می باشد که می توان با شکستن استاندارد های IP Header به این مقصود رسید .

- Oversized Packet(Ping of Death)
- Fragmentation (Teardrop Attack)
- IP Source Address Spoofing (Land Attack)
- Malformed UDP Packet Header (UDP Bomb)

Application Security Testing

با ظهور تجارت الکترونیکی عملیات تجاری بیشتر شرکت ها و یا سازمان ها بصورت اینترنتی ویا تحت وب در آمده است که در این حالت این سیستم ها می تواند بیشتر تحت حملات باشد . به عنوان مثال برای کاهش احتمال حملات به قصد دزدیدن اطلاعات مهم این سیستم ها باید داده های خود را بصورت رمز شده انتقال بدهند . در این نوع از تست تمرکزاصلی بر روی نرم افزار ها برای کشف نقاط ضعف و بهبود آنها می باشد. این نوع از تست شامل اجزای زیر می باشد :

Code Review

در این مورد کد برنامه برای اطمینان از نبود اطلاعات حساس در آن که باعث آسیب پذیری آن می شود مورد بازنگری قرار می گیرد . به عنوان مثال در کد می تواند کامنت ها و یا اسم ها و همچنین Clear Text Password هایی باشد که اطلاعت خوبی به فرد نفوذگر بدهد .

Authorization Testing

در این نوع از تست قسمتی از برنامه که با کاربر در تعامل است مورد تست قرار می گیرد که شامل موارد زیر می باشد :

- Input Validation of Login Field

ورود کاراکترهای نا مربوط و یا طولانی که می تواند نتیجه غیرقابل پیش بینی داشته باشد .

- Cookie Security

ممکن است کوکی ها دزدیده شود و کانکشین ارتباطی توسط فردی ناشناس مورد استفاده قرار گیرد.

- Lookout Testing

در این تست مدت زمان مجاز برای انجام یک عملیات توسط کاربر ، برای جلوگیری از دزدین کانکشین ارتباطی توسط فردی دیگر تست می شود .

Functionality Testing

در این نوع از تست عملکرد سیسیتم در مقابل کاربر تست می شود که شامل موارد زیر می باشد :

- Input Validation

ورود کاراکترهای نامربوط و یا طولانی و بررسی عملکرد سیستم در مقابل این ورودی ها

- Transaction Testing

اطمینان از انجام درخواست کاربر و نه عملی اضافه تر توسط سیسیتم که امکان سو استفاده را توسط کاربر داشته باشد

War dialing

در این نوع از تست هدف این باشد که کنترل تجهیزات شبکه ای را در دست بگیریم و از این طریق به دیگر نقاط شبکه و سازمان نفوذ کنیم .

به عنوان مثال فرد نفوذگر با نفوذ به Access Point درون شرکت و Sniff کردن ترافیک می تواند به اطلاعات مهمی دست پیدا کند و از این اطلاعات برای نفوذ به دیگر نقاط حساس شبکه استفاده کند.

Penetration testing for wireless networks

ارتباط های وایرلس یکی از نا امن ترین بسترهای ارتباطی می باشد به این دلیل که ترافیک ما در هوا بصورت سیگنال پخش می شود و هر کسی چه در درون و یا بیرون سازمان می تواند به آن دسترسی پیدا کند به همین دلیل باید تمرکز خاصی برای امنیت این نوع بستر ارتباطی انجام دهد.

در این نوع تست هدف ارتباط های وایرلس شرکت و یا سازمان می باشد که می تواند شامل بررسی پروتکل های امنیتی تجهیزات وایرلس ، الگوریتم های رمزنگاری استفاده شده در این نوع از ارتباط و ... باشد .

Social engineering

در این نوع از تست تمرکز بر روی افراد سازمان می باشد که فرد نفوذگر قصد دارد که با جلب اعتماد این افراد و یا دیگر روش ها به اطلاعات مهمی دست پیدا کند. که این نوع تست می تواند شامل تست

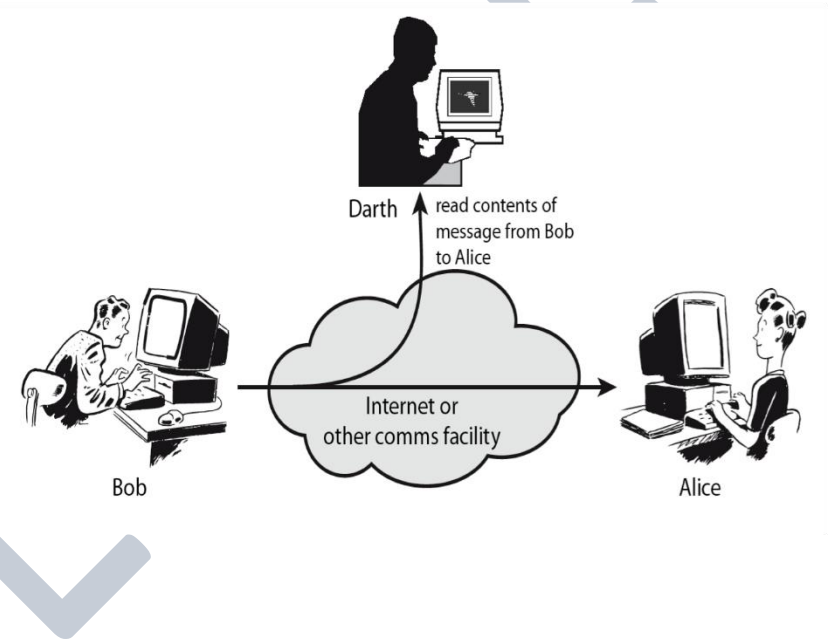
رو در رو و یا دور ا دور باشد .

برای مثالی از روش دور را دور کارمندی را تصور کنید که علاقه خاصی به آهنگ ها خواننده خاصی دارد حال فرد نفوذ گر با دانستن این نکته اقدام به ارسال یک ایمیل حاوی آهنگی از این خواننده برای این کارمند می کند که این آهنگ آلوده به یک Keylogger می باشد حال اگر این کارمند این فایل را دانلود کند این Keylogger نیز برروی سیستمش نصب می شود و بدین صورت فرد نفوذگر می تواند به یکه دسترسی به درون سازمان ما پیدا کند .

انواع حملات

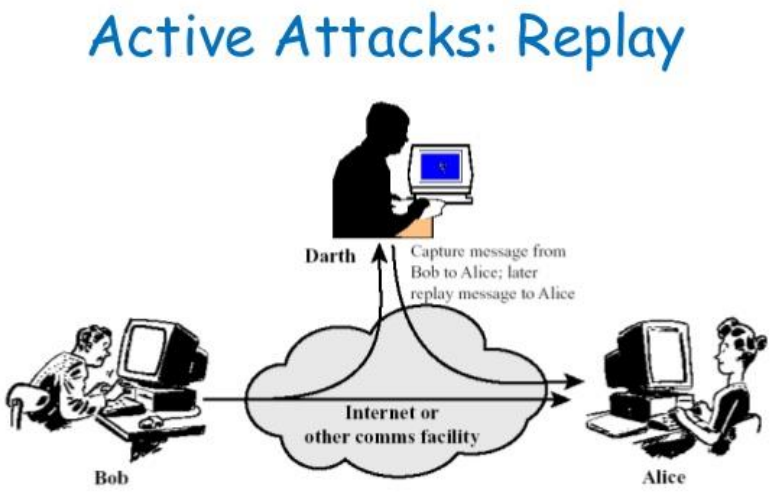
Passive Attack

این نوع از حملات شامل مشاهده ترافیک رمز نشده و جستجو به دنبال Clear-Text Password و یا اطلاعات حساسی که بتوان از آنها در انواع حملات دیگر استفاده کرد . این نوع حملات شامل آنالیز ترافیک (Traffic Analysis)، مشاهده کردن ارتباطات نا امن،Decrypt ترافیکی که از الگوریتم های ضعیف Encryption استفاده کرده اند و یا Capture کردن اطلاعات احراز هویت مانند رمز عبور کاربران . نتیجه این نوع حملات مجموعه ای جمع آوری مجموعه ای فایل و یا اطلاعات بدون اطلاع کاربر است .



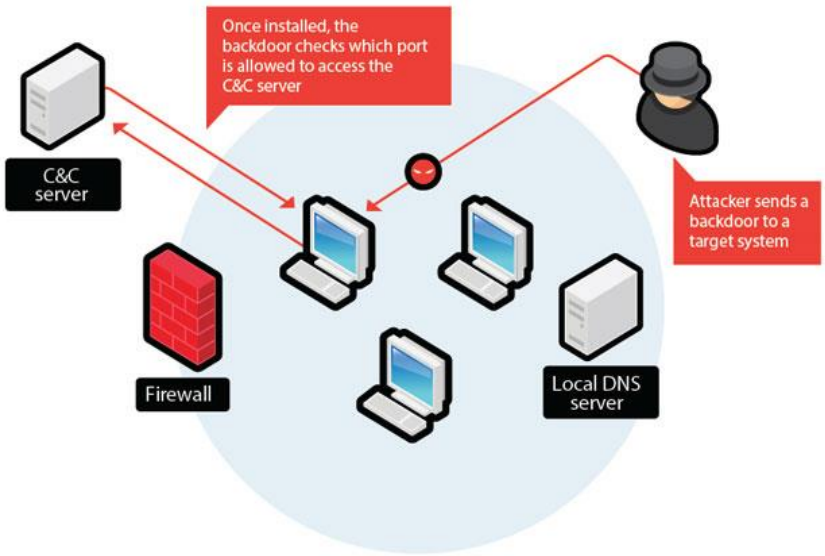
Active Attack

در این نوع از حملات هدف مهاجم ورود به یک سیستم امن می باشد که این عمل می تواند با استفاده از Virus , Horse Trojan , Worm صورت بگیرد که هدف از این نوع حمله می تواند اجرای کد مخرب ، دزدین اطلاعات و یا تغییر آن ها و همچنین اختلال باشد . نتیجه این حملات می تواند مجموعه ای از فایل ها و یا اطلاعات ، اختلال در سرویس ها و اطلاعات دستکاری شده باشد .



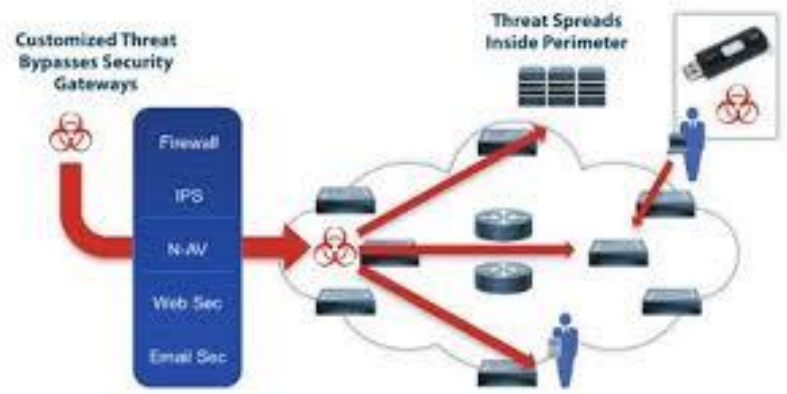
Distributed Attack

این نوع حملات نیازمند یک سری برنامه مثل Trojan و یا Back-Door می باشد که به عنوان برنامه های قابل اعتماد در شبکه نقش ایفا کنند و بتوانند در سطح شبکه پخش شوند .هدف این نوع حملات مختل کردن برنامه ها و یا سخت افزار های کامپیوترهای درون شبکه می باشد و یا وجود آوردن راهی برای ورود به شبکه بدون مواجه شدن با مکانیزم های احراز هویت برای دسترسی به اطلاعات و یا تغییر آنها .



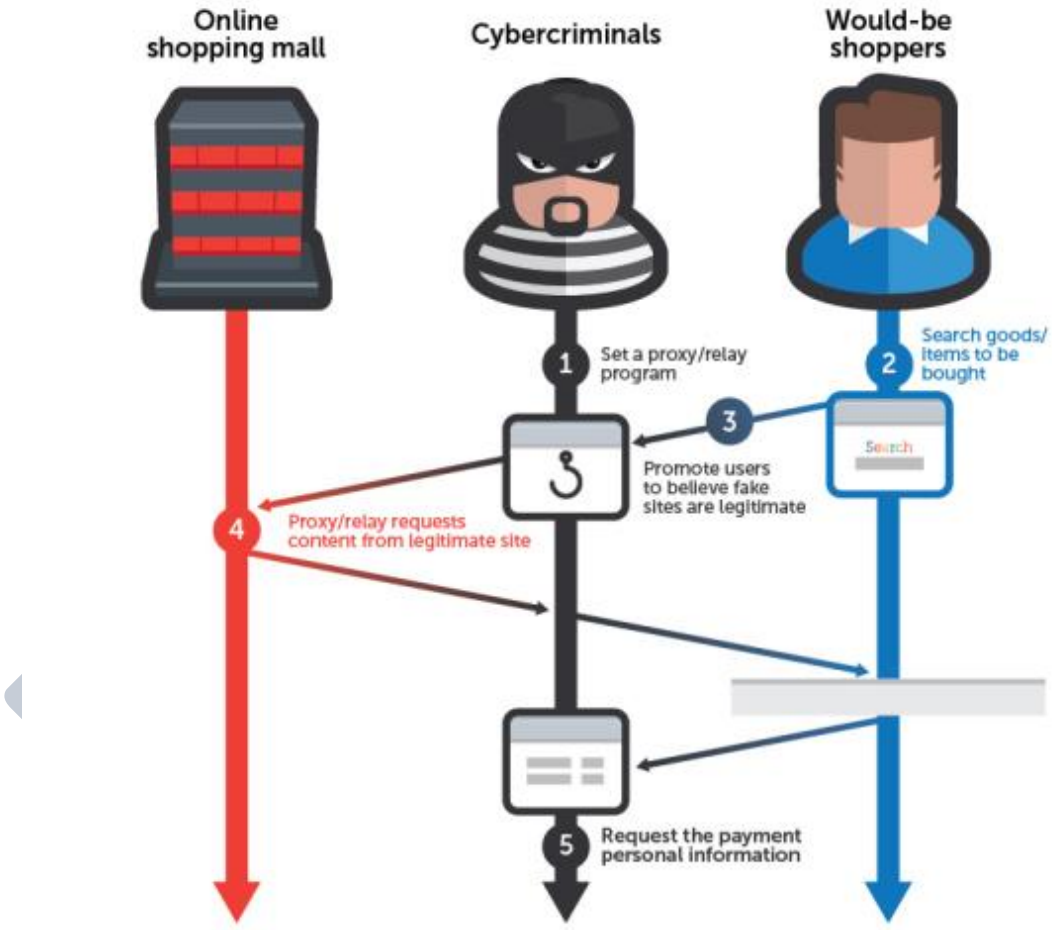
Insider Attack

این نوع از حملات از درون سازمان صورت می گیرد (برای مثال می توان کارمندی ناراضی را که به حمله دست می زند نام برد) این نوع حمله می تواند از روی عمد و یا غیر عمد باشد که حملات عمدی می تواند شامل دزدین اطلاعات ، اختلال در سیسیتم ها و ... باشد و حملات غیر عمدی می تواند شامل کم دقتی کارمندان ، کمبود دانش کارمندان و ... باشد .



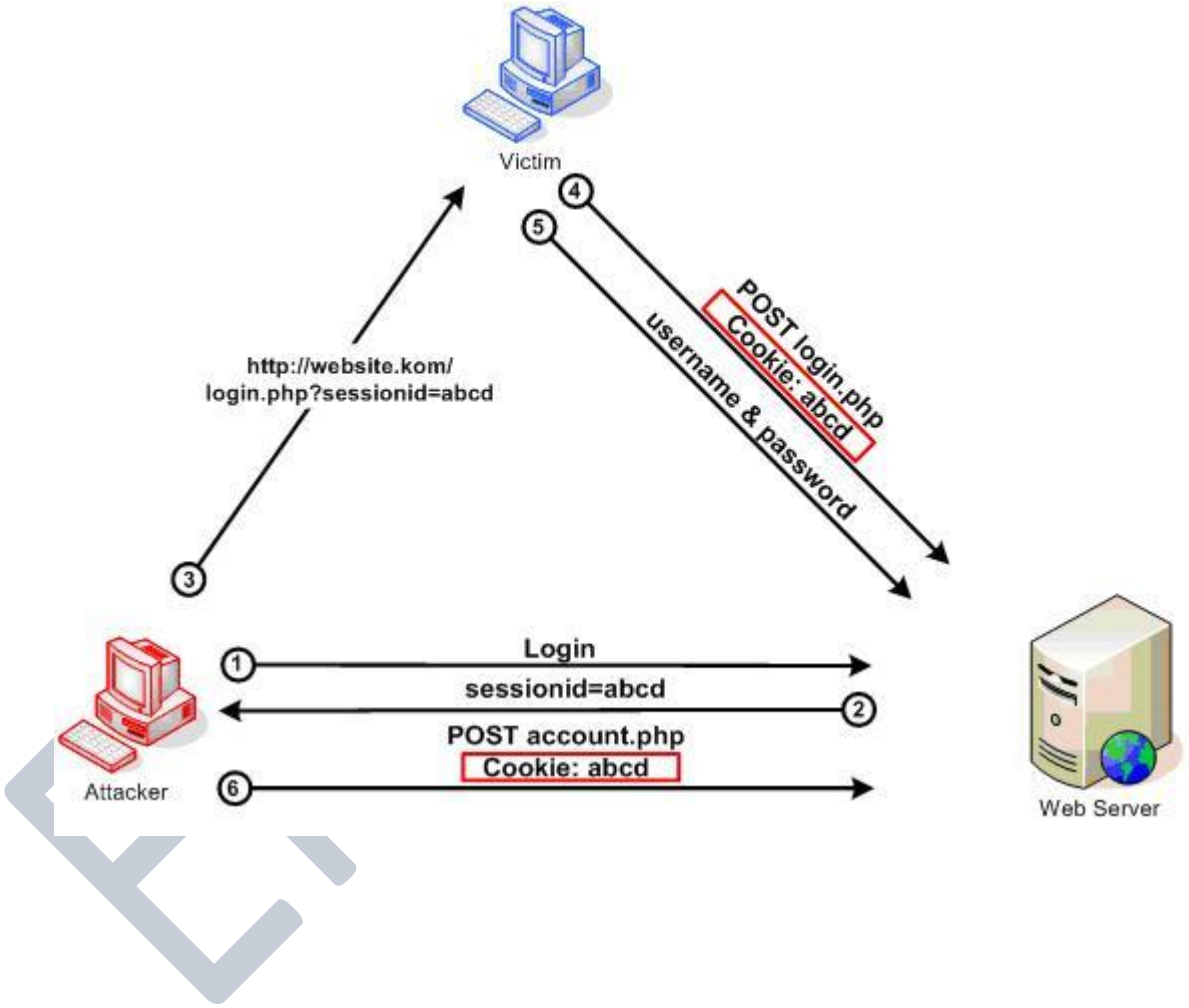
Phishing Attack

در این نوع از حملات قصد هکر فریب دادن کاربران و دزدین اطلاعات آن ها می باشد که عمده این نوع حملات شامل ساخت یک صفحه قلابی از سایت های معروف مانند بانک ها و موسسات مالی است که قصد هکر از این کار فریب کاربران و معرفی این صفحه به جای صفحه اصلی سایت مورد نظر و دزدین اطلاعات کاربران است .



Hijack Attack

در این نوع از حمله قصد هکر دزدیدن کانال ارتباطی بین دو سیستم و بیرون انداختن یکی از آن دو و معرفی خود به جای یکی از آنها به منظور دستیابی به اطلات حساس و مهم است .

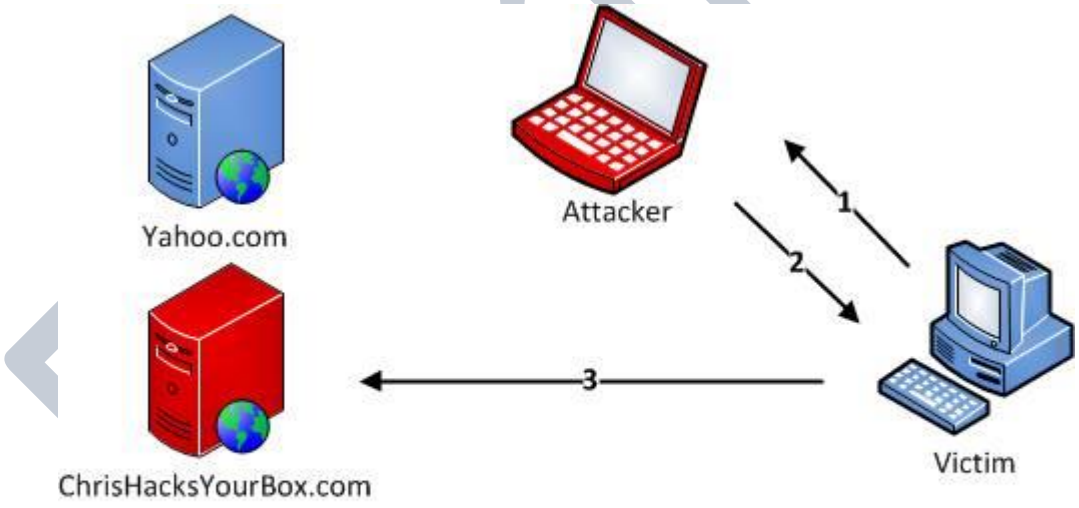


Close-in Attack

این نوع از حملات شامل شخصی می باشد که قصد دارد به صورت فیزیکی به سازمان (چه تجهیزات ، چه کارمندان) نزدیک شود که از این طریق بتواند به اطلاعات مهمی از سازمان ما و یا شبکه ما دست پیدا کند . مهمترین حمله از این نوع حملات از نوع مهندسی اجتماعی می باشد .

Spoof Attack

در این نوع از حمله هکر آدرس یکی از Node های درون شبکه را دزدیده و خود را به جای آن Node جا می زند .



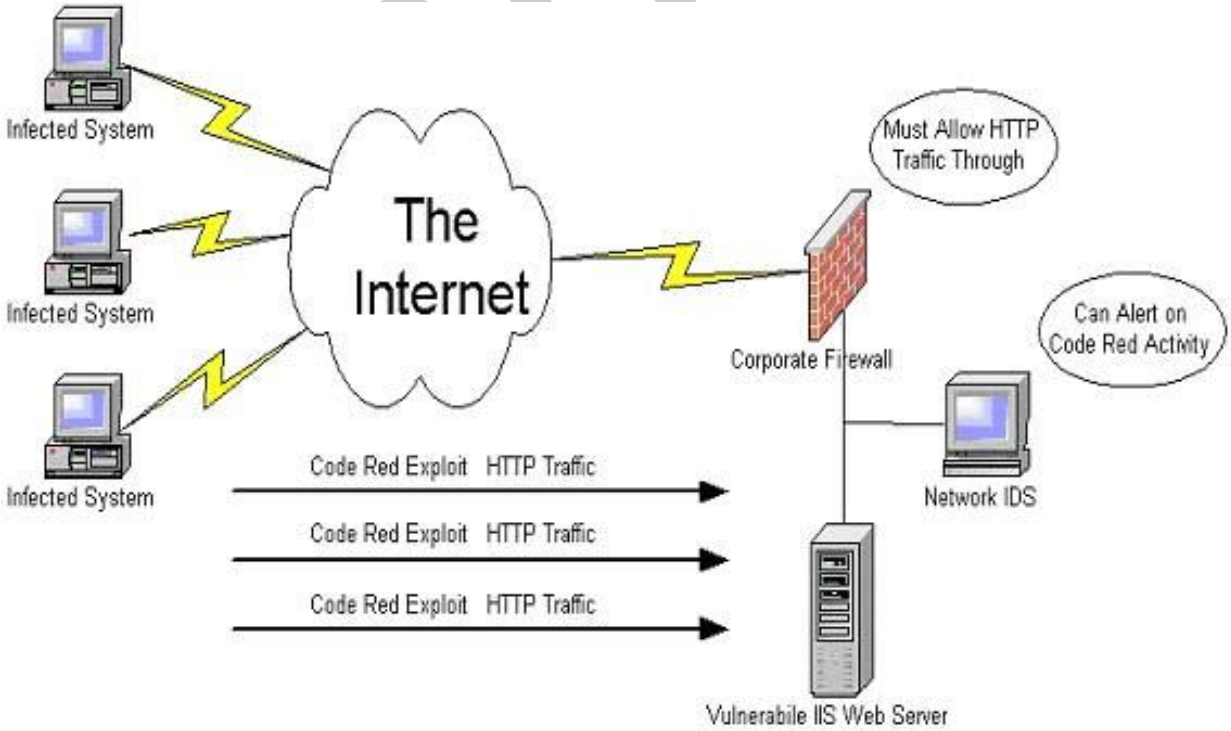
1. Legitimate DNS Request Destined for DNS Server
2. Fake DNS Reply from Listening Attacker
3. Victim begins communicating with malicious site as a result

Exploit Attack

یکی از انواع حملات می باشد که در آن مهاجم از مشکلات امنیتی درون سیسیتم عامل و یا برنامه های درون شبکه آگاه می باشد و از این دانش برای اجرا یک کد مخرب و دسترسی به شبکه و یا اختلال در آن استفاده می کند .

Buffer overflow

این نوع حمله شامل ارسال بیش از حد داده به سمت یک نرم افزار که انتظار آن را ندارد می باشد که نتیجه آن اختلال در کار آن نرم افزار می باشد . در نوعی از این حمله مهاجم می تواند به سطح ادمین در Command Prompt و یا Shell برسد .



Password Attack

در این نوع حمله مهاجم در تلاش است که کلمه های عبوری که در درون Network Account Database و یا Password-Protected File را کرک کند . که خود شامل Dictionary Attack , Brute-Force Attack , Hybrid Attack می باشد. Dictionary Attack از یک لیست شامل رشته هایی که احتمال اینکه کلمه عبور باشند استفاده می کند. Brute-Force Attack حالتی است که مهاجم در تلاش است که هر ترکیب ممکن از کاراکتر ها را برای کرک کلمه عبور چک کند . همچنین استفاده از Keylogger برای ذخیره رشته هایی که کاربر وارد کرده و فرستادن آن برای هکر نیز می تواند جزو این نوع از حملات باشد .