۱- IDS مبتنی بر خلاف قاعده آماری

۲- IDS مبتنی بر امضا یا تطبیق الگو

روش اول مبتنی بر تعیین آستانه انواع فعالیتها بر روی شبکه است، مثلا چند بار یک دستور مشخص توسط یک کاربر در یک تماس با یک میزبان (host) اجرا می شود.لذا در صورت بروز یک نفوذ امکان تشخیص آن به علت خلاف معمول بودن آن وجود دارد. اما بسیاری از حملات به گونه ای هستند که نمی توان براحتی و با کمک این روش آنها را تشخیص داد.

در واقع روشی که در بیشتر سیستمهای موفق تشخیص نفوذ به کار گرفته می شود، IDS مبتنی بر امضا یا تطبیق الگو است.منظور از امضا مجموعه قواعدی است که یک حمله در حال انجام را تشخیص می دهد. دستگاهی که قرار است نفوذ را تشخیص دهد با مجموعه ای از قواعد بارگذاری می شود.هر امضا دارای اطلاعاتی است که نشان می دهد در داده های در حال عبور باید به دنبال چه فعالیتهایی گشت. هرگاه ترافیک در حال عبور با الگوی موجود در امضا تطبیق کند، پیغام اخطار تولید می شود و مدیر شبکه را از وقوع یک نفوذ آگاه می کند. در بسیاری از موارد IDS علاوه بر آگاه کردن مدیر شبکه، اتصال با هکر را بازآغازی می کند و یا با کمک یک فایروال و انجام عملیات کنترل دسترسی با نفوذ بیشتر مقابله می کند.

اما بهترین روش برای تشخیص نفوذ، استفاده از ترکیبی از دو روش فوق است.

مقایسه تشخیص نفوذ و پیش گیری از نفوذ

Intrusion Prevention

ایده پیش گیری از نفوذ (Intrusion Prevention) این است که تمام حملات علیه هر بخش از محیط محافظت شده توسط روش های به کار گرفته شده ناکام بماند. این روش ها می توانند تمام بسته های شبکه را بگیرند و نیت آنها را مشخص کنند ـ آیا هرکدام یک حمله هستند یا یک استفاده قانونی ـ سپس عمل مناسب را انجام دهند.

تفاوت شکلی تشخیص با پیش گیری

در ظاهر، روش های تشخیص نفوذ و پیش گیری از نفوذ رقیب هستند. به هرحال، آنها لیست بلند بالایی از عملکردهای مشابه، مانند بررسی بسته داده، تحلیل با توجه به حفظ وضعیت، گردآوری بخش های TCP، ارزیابی پروتکل و تطبیق امضاء دارند. اما این قابلیت ها به عنوان ابزاری برای رسیدن به اهداف متفاوت در این دو روش به کار گرفته می شوند. یک IPS (Intrusion Prevention System) یا سیستم پیش گیری مانند یک محافظ امنیتی در مدخل یک اجتماع اختصاصی عمل می کند که بر پایه بعضی گواهی ها و قوانین یا سیاست های از پیش تعیین شده اجازه عبور می دهد. یک IDS (Intrusion Detection System) یا سیستم تشخیص مانند یک اتومبیل گشت زنی در میان اجتماع عمل می کند که فعالیت ها را به نمایش می گذارد و دنبال موقعیت

های غیرعادی می گردد. بدون توجه به قدرت امنیت در مدخل، گشت زن ها به کار خود در سیستم ادامه می دهند و بررسی های خود را انجام می دهند.

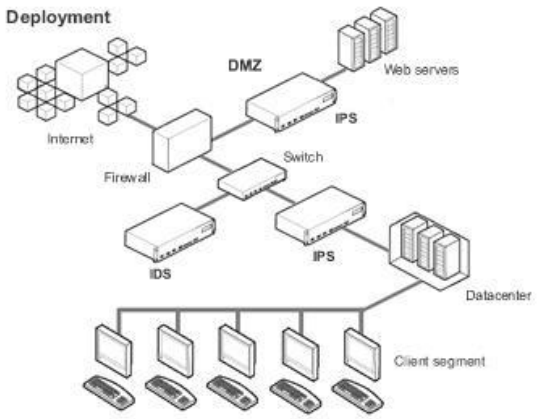
تشخیص نفوذ

هدف از تشخیص نفوذ نمایش، بررسی و ارائه گزارش از فعالیت شبکه است. این سیستم روی بسته های داده که از ابزار کنترل دسترسی عبور کرده اند، عمل می کند. به دلیل وجود محدودیت های اطمینان پذیری، تهدیدهای داخلی و وجود شک و تردید مورد نیاز، پیش گیری از نفوذ باید به بعضی از موارد مشکوک به حمله اجازه عبور دهد تا احتمال تشخیص های غلط (positive false) کاهش یابد. از طرف دیگر، روش های IDS با هوشمندی همراه هستند و از تکنیک های مختلفی برای تشخیص حملات بالقوه، نفوذها و سوء استفاده ها بهره می گیرند. یک IDS معمولاً به گونه ای از پهنای باند استفاده می کند که می تواند بدون تأثیر گذاشتن روی معماری های محاسباتی و شبکه ای به کار خود ادامه دهد. طبیعت منفعل IDS آن چیزی است که قدرت هدایت تحلیل هوشمند جریان بسته ها را ایجاد می کند. همین امر IDS را در جایگاه خوبی برای تشخیص موارد زیر قرارمی دهد:

- حملات شناخته شده از طریق امضاءها 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 غیرعادی با استفاده از تحلیل انحراف معیار

- تشخیص فعالیت مشکوک با استفاده از تکنیک های آماری، تحلیل جریان و تشخیص خلاف قاعده

بعضی حملات تا درجه ای از یقین بسختی قابل تشخیص هستند، و بیشتر آنها فقط می توانند توسط روش هایی که دارای طبیعت غیرقطعی هستند تشخیص داده شوند. یعنی این روش ها برای تصمیم گیری مسدودسازی براساس سیاست مناسب نیستند.



پیش گیری از نفوذ

چنانچه قبلاً هم ذکر شد، روش های پیش گیری از نفوذ به منظور محافظت از دارایی ها، منابع، داده و شبکه ها استفاده می شوند. انتظار اصلی از آنها این است که خطر حمله را با حذف ترافیک مضر شبکه کاهش دهند در حالیکه به فعالیت صحیح اجازه ادامه کار می دهند. هدف نهایی یک سیستم کامل است- یعنی نه تشخیص غلط حمله (false positive) که از بازدهی شبکه می کاهد

و نه عدم تشخیص حمله (false negative) که باعث ریسک بی مورد در محیط شبکه شود. شاید یک نقش اساسی تر نیاز به مطمئن بودن است؛ یعنی فعالیت به روش مورد انتظار تحت هر شرایطی. بمنظور حصول این منظور، روش های IPS باید طبیعت قطعی (deterministic) داشته باشند.

قابلیت های قطعی، اطمینان مورد نیاز برای تصمیم گیری های سخت را ایجاد می کند. به این معنی که روش های پیش گیری از نفوذ برای سروکار داشتن با موارد زیر ایده آل هستند:

- برنامه های ناخواسته و حملات اسب تروای فعال علیه شبکه ها و برنامه های اختصاصی، با استفاده از قوانین قطعی و لیست های کنترل دسترسی
- بسته های دیتای متعلق به حمله با استفاده از فیلترهای بسته داده ای سرعت بالا
- سوءاستفاده از پروتکل و دستکاری پروتکل شبکه با استفاده از بازسازی هوشمند
- حملات DoS/DDoS مانند طغیان SYN وICMP با استفاده از الگوریتم های فیلترینگ برپایه حد آستانه
- سوءاستفاده از برنامه ها و دستکاری های پروتکل ـ حملات شناخته شده و شناخته نشده علیه HTTP، FTP، DNS، SMTP و غیره با استفاده از قوانین پروتکل برنامه ها و امضاءها
- باراضافی برنامه ها با استفاده از ایجاد محدودیت های مصرف منابع

تمام این حملات و وضعیت آسیب پذیری که به آنها اجازه وقوع می دهد به خوبی مستندسازی شده اند. بعلاوه، انحرافات از پروتکل های ارتباطی از لایه شبکه تا لایه برنامه جایگاهی در هیچ گونه ترافیک صحیح ندارند.

نتیجه نهایی

تفاوت بین IDS و IPS به فلسفه جبرگرایی می انجامد. یعنی IDS می تواند (و باید) از روش های غیرقطعی برای استنباط هرنوع تهدید یا تهدید بالقوه از ترافیک موجود استفاده کند. این شامل انجام تحلیل آماری از حجم ترافیک، الگوهای ترافیک و فعالیت های غیرعادی می شود. IDS به درد افرادی می خورد که واقعاً می خواهند بدانند چه چیزی در شبکه شان در حال رخ دادن است.

از طرف دیگر، IPS باید در تمام تصمیماتش برای انجام وظیفه اش در پالایش ترافیک قطعیت داشته باشد. از یک ابزار IPS انتظار می رود که در تمام مدت کار کند و در مورد کنترل دسترسی تصمیم گیری کند. فایروال ها اولین رویکرد قطعی را برای کنترل دسترسی در شبکه ها با ایجاد قابلیت اولیه IPS فراهم کردند. ابزارهای IPS قابلیت نسل بعد را به این فایروال ها اضافه کردند و هنوز در این فعالیت های قطعی در تصمیم گیری برای کنترل دسترسی ها مشارکت دارند.

حملات DoS

شاید تاکنون شنیده باشید که یک وب سایت مورد تهاجمی از نوع DoS قرار گرفته است. این نوع از حملات صرفا" متوجه وب سایت ها نبوده و ممکن است شما قربانی بعدی باشید. تشخیص حملات DoS از طریق عملیات متداول شبکه امری مشکل است ولی با مشاهده برخی علائم در یک شبکه و یا کامپیوتر می توان از میزان پیشرفت این نوع از حملات آگاهی یافت.

حملات از نوع DoS (denial-of-service)

در یک تهاجم از نوع DoS ، یک مهاجم باعث ممانعت دستیابی کاربران تائید شده به اطلاعات و یا سرویس های خاصی می نماید. یک مهاجم با هدف قرار دادن کامپیوتر شما و اتصال شبکه ای آن و یا کامپیوترها و شبکه ای از سایت هائی که شما قصد استفاده از آنان را دارید، باعث سلب دستیابی شما به سایت های Email ، وب سایت ها، account های online و سایر سرویس های ارائه شده بر روی کامپیوترهای سرویس دهنده می گردد.

متداولترین و مشهودترین نوع حملات DoS ، زمانی محقق می گردد که یک مهاجم اقدام به ایجاد یک سیلاب اطلاعاتی در یک شبکه نماید. زمانی که شما آدرس URL یک وب سایت خاص را از طریق مرورگر خود تایپ می نمائید، درخواست شما برای سرویس دهنده ارسال می گردد. سرویس دهنده در هر لحظه قادر به پاسخگوئی به حجم محدودی از درخواست ها می باشد، بنابراین اگر یک مهاجم با ارسال درخواست های متعدد و سیلاب گونه باعث افزایش حجم عملیات سرویس دهند گردد، قطعا" امکان پردازش درخواست شما برای سرویس دهنده وجود نخواهد داشت. حملات فوق از نوع DoS می باشند، چراکه امکان دستیابی شما به سایت مورد نظر سلب شده است.

یک مهاجم می تواند با ارسال پیام های الکترونیکی ناخواسته که از آنان با نام Spam یاد می شود، حملات مشابهی را متوجه سرویس دهنده پست الکترونیکی نماید. هر account پست الکترونیکی (صرفنظر از منبعی که آن را در اختیار شما قرار می دهد، نظیر سازمان مربوطه و یا سرویس های رایگانی نظیر یاهو و hotmail) دارای ظرفیت محدودی می باشند. پس از تکمیل ظرفیت فوق، عملا" امکان ارسال Email دیگری به account فوق وجود نخواهد داشت. مهاجمان با ارسال نامه های الکترونیکی ناخواسته سعی می نمایند که ظرفیت account مورد نظر را تکمیل و عملا" امکان دریافت email های معتبر را از account فوق سلب نمایند.

حملات از نوع DDoS (distributed denial-of-service)

در یک تهاجم از نوع DDoS ، یک مهاجم ممکن است از کامپیوتر شما برای تهاجم بر علیه کامپیوتر دیگری استفاده نماید. مهاجمان با استفاده از نقاط آسیب پذیر و یا ضعف امنیتی موجود بر روی سیستم شما می توانند کنترل کامپیوتر شما را بدست گرفته و در ادامه از آن به منظور انجام عملیات مخرب خود استفاده نمایند. ارسال حجم بسیار بالائی داده از طریق کامپیوتر شما برای یک وب سایت و یا ارسال نامه های الکترونیکی ناخواسته برای آدرس های Email خاصی، نمونه هائی از همکاری کامپیوتر شما در بروز یک تهاجم DDOS می باشد. حملات فوق، "توزیع شده " می باشند، چراکه مهاجم از چندین کامپیوتر به منظور اجرای یک تهاجم DoS استفاده می نماید.

نحوه پیشگیری از حملات

متاسفانه روش موثری به منظور پیشگیری در مقابل یک تهاجم DoS و یا DDoS وجود ندارد. علیرغم موضوع فوق، می توان با رعایت برخی نکات و انجام عملیات

پیشگیری، احتمال بروز چنین حملاتی (استفاده از کامپیوتر شما برای تهاجم بر علیه سایر کامپیوتر ها) را کاهش داد.

- نصب و نگهداری نرم افزار آنتی ویروس
- نصب و پیکربندی یک فایروال
- تبعیت از مجموعه سیاست های خاصی در خصوص توزیع و ارائه آدرس Email خود به دیگران

چگونه از وقوع حملات DoS و یا DDoS آگاه شویم ؟

خرابی و یا بروز اشکال در یک سرویس شبکه، همواره بدلیل بروز یک تهاجم DoS نمی باشد. در این رابطه ممکن است دلایل متعددی فنی وجود داشته و یا مدیر شبکه به منظور انجام عملیات نگهداری موقتا" برخی سرویس ها را غیر فعال کرده باشد. وجود و یا مشاهده علائم زیر می تواند نشاندهنده بروز یک تهاجم از نوع DoS و یا DDoS باشد:

- کاهش سرعت و یا کارآئی شبکه بطرز غیر معمول (در زمان باز نمودن فایل ها و یا دستیابی به وب سایت ها).
- عدم در دسترس بودن یک سایت خاص(بدون وجود دلایل فنی)
- عدم امکان دستیابی به هر سایتی(بدون وجود دلایل فنی)
- افزایش محسوس حجم نامه های الکترونیکی ناخواسته دریافتی

در صورت بروز یک تهاجم ، چه عملیاتی را می بایست انجام داد؟

حتی در صورتی که شما قادر به شناسائی حملات از نوع DoS و یا DDoS باشید، امکان شناسائی مقصد و یا منبع واقعی تهاجم، وجود نخواهد داشت. در این رابطه لازم

است با کارشناسان فنی ماهر، تماس گرفته تا آنان موضوع را بررسی و برای آن راهکار مناسب را ارائه نمایند.

- در صورتی که برای شما مسلم شده است که نمی توانید به برخی از فایل های خود و یا هر وب سایتی خارج از شبکه خود دستیابی داشته باشید، بلافاصله با مدیران شبکه تماس گرفته و موضوع را به اطلاع آنان برسانید. وضعیت فوق می تواند نشاندهنده بروز یک تهاجم بر علیه کامپیوتر و یا سازمان شما باشد.
- در صورتی که وضعیت مشابه آنچه اشاره گردید را در خصوص کامپیوترهای موجود در منازل مشاهده می نمائید با مرکز ارائه دهنده خدمات اینترنت (ISP) تماس گرفته و موضوع را به اطلاع آنان برسانید. ISP مورد نظر می تواند توصیه های لازم به منظور انجام عملیات مناسب را در اختیار شما قرار دهد.

عدم پذیرش سرویس (۱)

قصد داریم تا طی چند قسمت با نوعی از حمله به نام DoS آشنا شویم که مخفف عبارت Denial-of-Service یا عدم پذیرش سرویس است. همانطور که در روش های معمول حمله به کامپیوترها اشاره مختصری شد، این نوع حمله باعث از کارافتادن یا مشغول شدن بیش از اندازه کامپیوتر می شود تا حدی که غیرقابل استفاده می شود. در بیشتر موارد، حفره های امنیتی محل انجام این حملات است و لذا نصب آخرین وصله های امنیتی از حمله جلوگیری خواهند کرد. شایان گفتن است که علاوه بر اینکه کامپیوتر شما هدف یک حمله DoS قرار می گیرد، ممکن است که در حمله DoS علیه یک سیستم دیگر نیز شرکت داده شود. نفوذگران با ایجاد ترافیک بی مورد و بی استفاده باعث می شوند که حجم زیادی از منابع سرویس دهنده و پهنای باند شبکه مصرف یا به نوعی درگیر رسیدگی به این تقاضاهای بی مورد شود و این تقاضا تا جایی که دستگاه سرویس دهنده را به زانو در آورد ادامه پیدا می کند. نیت اولیه و تأثیر حملات DoS جلوگیری از استفاده صحیح از منابع کامپیوتری و شبکه ای و از بین بردن این منابع است.

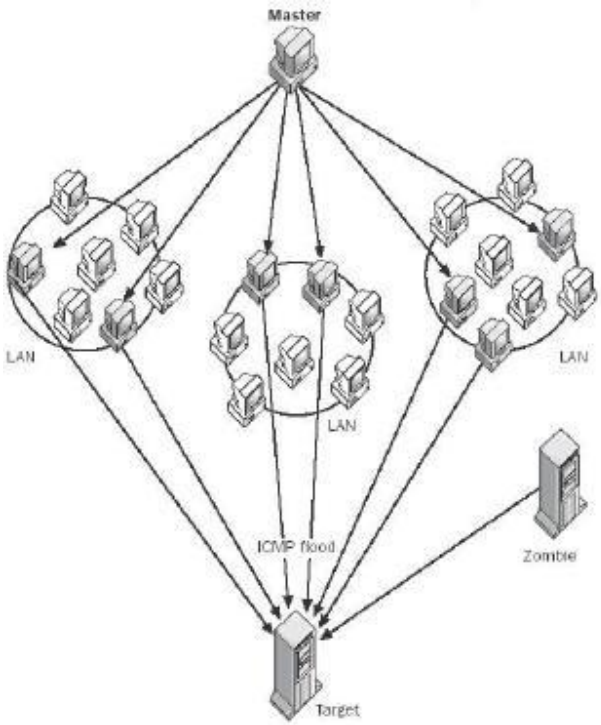
علیرغم تلاش و منابعی که برای ایمن سازی علیه نفوذ و خرابکاری مصـــروف گشته است، سیستم های متصل به اینترنت با تهـــدیدی واقعی و مداوم به نام حملات DoS مواجه هستند. این امر بدلیل دو مشخصه اساسی اینترنت است:

- **منابع تشکیل دهنده اینترنت به نوعی محدود و مصرف شدنی هستند.**

زیرساختار سیستم ها و شبکه های بهم متصل که اینترنت را می سازند، کاملاً از منابع محدود تشکیل شده است. پهنای باند، قدرت پردازش و ظرفیت های ذخیره سازی، همگی محدود و هدف های معمول حملات DoS هستند. مهاجمان با انجام این حملات سعی می کنند با مصرف کردن مقدار قابل توجهی از منابع در دسترس، باعث قطع میزانی از سرویس ها شوند. وفور منابعی که بدرستی طراحی و استفاده شده اند ممکن است عاملی برای کاهش میزان تاثیر یک حمله DoS باشد، اما شیوه ها و ابزار امروزی حمله حتی در کارکرد فراوان ترین منابع نیز اختلال ایجاد می کند.

- **امنیت اینترنت تا حد زیادی وابسته به تمام عوامل است.**

حملات DoS معمولاً از یک یا چند نقطه که از دید سیستم یا شبکه قربانی عامل بیرونی هستند، صورت می گیرند. در بسیاری موارد، نقطه آغاز حمله شامل یک یا چند سیستم است که از طریق سوءاستفاده های امنیتی در اختیار یک نفوذگر قرار گرفته اند و لذا حملات از سیستم یا سیستم های خود نفوذگر صورت نمی گیرد. بنابراین، دفاع برعلیه نفوذ نه تنها به حفاظت از اموال مرتبط با اینترنت کمک می کند، بلکه به جلوگیری از استفاده از این اموال برای حمله به سایر شبکه ها و سیستم ها نیز کمک می کند. پس بدون توجه به اینکه سیستم هایتان به چه میزان محافظت می شوند، قرار گرفتن در معرض بسیاری از انواع حمله و مشخصاً DoS ، به وضعیت امنیتی در سایر قسمت های اینترنت بستگی زیادی دارد.

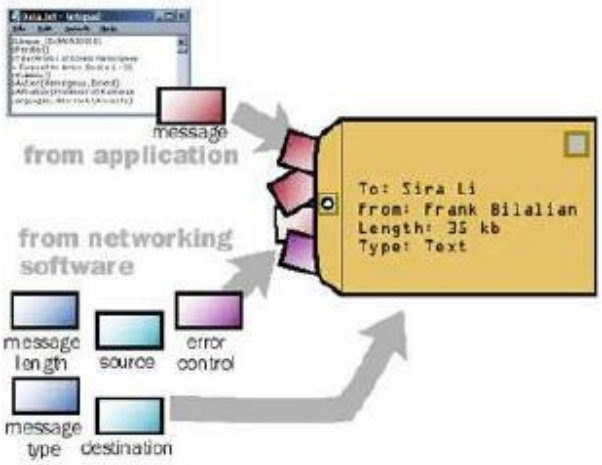


مقابله با حملات DoS تنها یک بحث عملی نیست. محدودکردن میزان تقاضا، فیلترکردن بسته ها و دستکاری پارامترهای نرم افزاری در بعضی موارد می تواند به محدودکردن اثر حملات DoS کمک کند، اما بشرطی که حمله DoS در حال مصرف کردن تمام منابع موجود نباشد. در بسیاری موارد، تنها می توان یک دفاع واکنشی داشت و این در صورتی است که منبع یا منابع حمله مشخص شوند. استفاده از جعل آدرس IP در طول حمله و ظهور روش های حمله توزیع شده و ابزارهای موجود یک چالش همیشگی را در مقابل کسانی که باید به حملات DoS پاسخ دهند، قرار داده است.

تکنولوژی حملات DoS اولیه شامل ابزار ساده ای بود که بسته ها را تولید و از «یک منبع به یک مقصد» ارسال می کرد. با گذشت زمان، ابزارها تا حد اجرای حملات از «یک

منبع به چندین هدف»، «از چندین منبع به هدف های تنها» و «چندین منبع به چندین هدف»، پیشرفت کرده اند.

امروزه بیشترین حملات گزارش شده به CERT/CC مبنی بر ارسال تعداد بسیار زیادی بسته به یک مقصد است که باعث ایجاد نقاط انتهایی بسیار زیاد و مصرف پهنای باند شبکه می شود. از چنین حملاتی معمولاً به عنوان حملات طغیان بسته (Packet flooding) یاد می شود. اما در مورد «حمله به چندین هدف» گزارش کمتری دریافت شده است.



انواع بسته ها (Packets) مورد استفاده برای حملات طغیان بسته، در طول زمان تغییر کرده است، اما چندین نوع بسته معمول وجود دارند که هنوز توسط ابزار حمله DoS استفاده می شوند.

- **طغیان های TCP**: رشته ای از بسته های TCP با پرچم های (flag) متفاوت به آدرس IP قربانی فرستاده می شوند. پرچم های SYN، ACK و RST بیشتر استفاده می شوند.
- **طغیان های تقاضا\پاسخ ICMP** (مانند طغیان های ping): رشته ای از بسته های ICMP به آدرس IP قربانی فرستاده می شود.
- **طغیان های UDP**: رشته ای از بسته های UDP به آدرس IP قربانی ارسال می شوند.

درقسمت بعدی به بررسی بیشتر حملات DoS خوهیم پرداخت.

عدم پذیرش سرویس (۲) : انواع حملات

در قسمت پیش با حمله DoS آشنا شدیم. از آنجا که حملات طغیان بسته های دیتا معمولاً تلاش می کنند منابع پهنای باند و پردازش را خلع سلاح کنند، میزان بســته ها و حجم دیتای متناظر با رشته بسته ها عوامل مهمی در تعیین درجه موفقیت حمله هستند. بعضی از ابزارهای حمله خواص بسته ها را در رشته بسته ها بدلایلی تغییر می دهند:

- **آدرس IP منبع** – در بعضی موارد، یک آدرس IP منبع ناصحیح، (روشی که جعل IP نامیده می شود) برای پنهان کردن منبع واقعی یک رشته بسته استفاده می شود. در موارد دیگر، جعل IP هنگامی استفاده می شود که رشته های بسته به یک یا تعداد بیشتری از سایت های واسطه فرستاده می شوند تا باعث شود که پاسخ ها به سمت قربانی ارسال شود. مثال بعدی در مورد حملات افزایش بسته است (مانند smurf و fraggle)
- **پورتهای منبع\مقصد**- ابزار حمله طغیان بسته بر اساس TCP و UDP ، گاهی اوقات پورت منبع و یا مقصد را تغییر می دهند تا واکنش توسط فیلتر کردن بسته را مشکل تر کنند.
- **مقادیر IP Header دیگر** - در نهایت در ابزار حمله DoS مشاهده کرده ایم که برای مقداردهی تصادفی، مقادیر Header هر بسته در رشته بسته ها طراحی شده اند که تنها آدرس IP مقصد است که بین بسته ها ثابت می ماند.

بسته ها با خواص ساختگی بسادگی در طول شبکه تولید و ارسال می شوند. پروتکل TCP/IP به آسانی مکانیزم هایی برای تضمین پیوستگی خواص بسته ها در هنگام تولید و یا ارسال نقطه به نقطه بسته ها ارائه نمی کند. معمولاً، یک نفوذگر فقط به داشتن اختیار کافی روی یک سیستم برای بکارگیری ابزار و حملاتی که قادر به تولید و ارسال بسته های با خواص تغییریافته باشند، نیاز دارد.

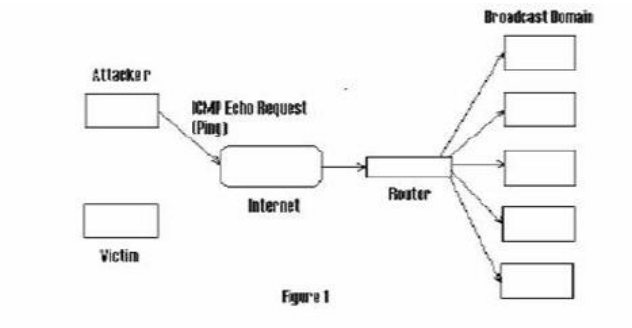
ژوئن ۱۹۹۹، آغاز بکارگیری ابزار DoS با چندین منبع یا DDos (Distributed DoS) بود.

روش های حمله DoS

در این قسمت به یک تقسیم بندی کلی درباره انواع حملات DoS می پردازیم:

Smurf یا Fraggle

حملات smurf یک از مخرب ترین حملات DoS هستند. (شکل زیر)



در حمله Smurf (حمله براساس ازدیاد بسته های ICMP)، نفوذگر یک تقاضای اکوی ICMP (ping) به یک آدرس ناحیه می فرستد.

آدرس منبع تقاضای اکو، آدرس IP قربانی است. (از آدرس IP قربانی بعنوان آدرس برگشت استفاده می شود). بعد از دریافت تقاضای اکو، تمام ماشین های ناحیه پاسخ های اکو را به آدرس IP قربانی می فرستند. در این حالت قربانی هنگام دریافت طغیان بسته های با اندازه بزرگ از تعداد زیادی ماشین، از کار خواهد افتاد.

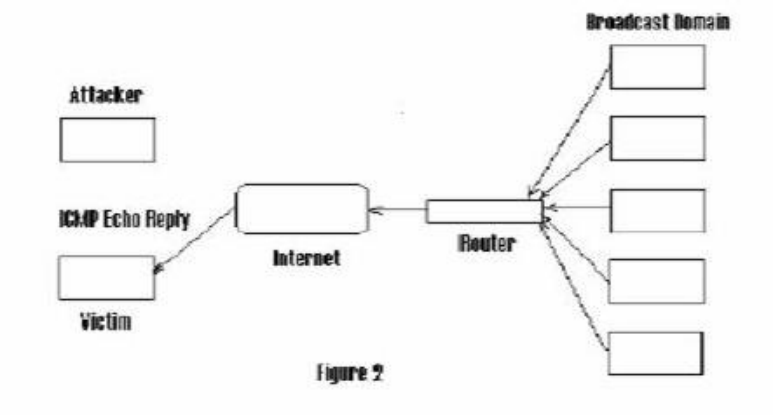


Figure 2

حمله Smurf برای ازکار انداختن منابع شبکه سیستم قربانی از روش مصرف پهنای باند استفاده می کند. این حمله این عمل را با استفاده از تقویت پهنای باند نفوذگران انجام می دهد. اگر شبکه تقویت کننده ۱۰۰ ماشین دارد، سیگنال می تواند ۱۰۰ برابر شود، و بنابراین حمله کننده با پهنای باند پایین (مانند مودم ۵۶ کیلوبیتی) می تواند سیستم قربانی را با پهنای باند بیشتری (مانند اتصال T1) از کار بیندازد.

حمله Fraggle (تقویت بسته UDP) در حقیقت شباهت هایی به حمله Smurf دارد. حمله Fraggle از بسته های اکوی UDP بر طبق همان روش بسته های اکوی ICMP در حمله Smurf استفاده می کند.

Fraggle معمولاً به ضریب تقویت کمتری نسبت به Smurf می رسد، و در بیشتر شبکه ها اکوی UDP سرویسی با اهمیت کمتر نسبت به اکوی ICMP است، بنابراین Fraggle عمومیت Smurf را ندارد.

SYN Flood

حمله طغیان SYN قبل از کشف حمله Smurf بعنوان مخرب ترین شیوه حمله DoS بشمار می رفت. این روش برای ایجاد حمله DoS بر اساس قحطی منابع عمل می کند.

در طول برقراری یک ارتباط معمولی TCP، سرویس گیرنده یک تقاضای SYN به سرویس دهنده می فرستد، سپس سرور با یک ACK/SYN به کلاینت پاسخ می دهد، در نهایت کلاینت یک ACK نهایی را به سرور ارسال می کند و به این ترتیب ارتباط برقرار می شود.

اما در حمله طغیان SYN، حمله کننده چند تقاضای SYN به سرور قربانی با آدرس های منبع جعلی بعنوان آدرس برگشت، می فرستد. آدرس های جعلی روی شبکه وجود ندارند. سرور قربانی سپس با ACK/SYN به آدرس های ناموجود پاسخ می دهد. از آنجا که هیچ آدرسی این ACK/SYN را دریافت نمی کند، سرور قربانی منتظر ACK از طرف کلاینت می ماند. ACK هرگز نمی رسد، و زمان انتظار سرور قربانی پس از مدتی به پایان می رسد. اگر حمله کننده به اندازه کافی و مرتب تقاضاهای SYN بفرستد، منابع موجود سرور قربانی برای برقراری یک اتصال و انتظار برای این ACKهای در حقیقت تقلبی

مصرف خواهد شد. این منابع معمولاً از نظر تعداد زیاد نیستند، بنابراین تقاضاهای SYN جعلی حتی با تعداد نسبتاً کم می توانند باعث وقوع یک حمله DoS شوند.

حملات DNS

در نسخه های اولیه BIND (Berkely Internet Name Domain)، حمله کنندگان می توانستند بطور مؤثری حافظه نهان یک سرور DNS را که در حال استفاده از عملیات بازگشت برای جستجوی یک ناحیه بود که توسط این سرور سرویس داده نمی شد، مسموم کنند. زمانی که حافظه نهان مسموم می شد، یک کاربر قانونی به سمت شبکه مورد نظر حمله کننده یا یک شبکه ناموجود هدایت می شد. این مشکل با نسخه های جدیدتر BIND برطرف شده است. در این روش حمله کننده اطلاعات DNS غلط که می تواند باعث تغییر مسیر درخواست ها شود، ارسال می کند.

حملات DDoS

حملات DDoS (Distributed Denial of Service) حمله گسترده ای از DoS است. در اصل DDos حمله هماهنگ شده ای برعلیه سرویس های موجود در اینترنت است. در این روش حملات DoS بطور غیرمستقیم از طریق تعداد زیادی از کامپیوترهای هک شده بر روی کامپیوتر قربانی انجام می گیرد. سرویس ها و منابع مورد حمله ، «قربانی های اولیه» و کامپیوترهای مورد استفاده در این حمله «قربانی های ثانویه» نامیده می شوند. حملات DDoS عموماً در از کار انداختن سایت های کمپانی های عظیم از حملات DoS مؤثرتر هستند.

انواع حملات DDoS

عموماً حملات DDoS به سه گروه Trinoo، TFN/TFN2K و Stecheldraht تقسیم می شوند.

Trinoo

Trinoo در اصل از برنامه های Master/Slave است که با یکدیگر برای یک حمله طغیان UDP بر علیه کامپیوتر قربانی هماهنگ می شوند. در یک روند عادی، مراحل زیر برای برقراری یک شبکه Trinoo DDoS واقع می شوند:

مرحله۱: حمله کننده، با استفاده از یک میزبان هک شده، لیستی از سیستم هایی را که می توانند هک شوند، گردآوری می کند. بیشتر این پروسه بصورت خودکار از طریق میزبان هک شده انجام می گیرد. این میزبان اطلاعاتی شامل نحوه یافتن سایر میزبان ها برای هک در خود نگهداری می کند.

مرحله۲: به محض اینکه این لیست آماده شد، اسکریپت ها برای هک کردن و تبدیل آنها به اربابان(Masters) یا شیاطین (Daemons) اجراء می شوند. یک ارباب می تواند چند شیطان را کنترل کند. شیاطین میزبانان هک شده ای هستند که طغیان UDP اصلی را روی ماشین قربانی انجام می دهند.

مرحله۳: حمله DDoS هنگامی که حمله کننده فرمانی به میزبانان Master ارسال می کند، انجام می گیرد. این اربابان به هر شیطانی دستور می دهند که حمله DoS را علیه آدرس IP مشخص شده در فرمان آغاز کنند و با انجام تعداد زیادی حمله DoS یک حمله DDoS شکل می گیرد.

TFN / TFN2K

TFN (Tribal Flood Network) یا شبکه طغیان قبیله ای، مانند Trinoo، در اصل یک حمله Master/Slave است که در آن برای طغیان SYN علیه سیستم قربانی هماهنگی صورت می گیرد. شیاطین TFN قادر به انجام حملات بسیار متنوع تری شامل طغیان ICMP، طغیان SYN و حملات Smurf هستند، بنابراین TFN از حمله Trinoo پیچیده تر است.

TFN2K نسبت به ابزار TFN اصلی چندین برتری و پیشرفت دارد. حملات TFN2K با استفاده از جعل آدرس های IP اجرا می شوند که باعث کشف مشکل تر منبع حمله می شود. حملات TFN2K فقط طغیان ساده مانند TFN نیستند. آنها همچنین شامل حملاتی می شوند که از شکاف های امنیتی سیستم عامل ها برای بسته های نامعتبر و ناقص سوءاستفاده می کنند تا به این ترتیب باعث از کار افتادن سیستم های قربانی شوند. حمله کنندگان TFN2K دیگر نیازی به اجرای فرمان ها با وارد شدن به ماشین های مخدوم (Client) (به جای Master در TFN) ندارند و می توانند این فرمان ها را از راه دور اجراء کنند. ارتباط بین Clientها و Daemonها دیگر به پاسخ های اکوی ICMP محدود نمی شود و می تواند روی واسط های مختلفی مانند TCP و UDP صورت گیرد. بنابراین TFN2K خطرناک تر و همچنین برای کشف کردن مشکل تر است.

Stacheldraht

کد Stacheldraht بسیار شبیه به Trinoo و TFN است، اما Stacheldraht اجازه می دهد که ارتباط بین حمله کننده و Masterها (که در این حمله Handler نامیده می شوند) رمزنگاری شود؛ عامل ها می توانند کد خود را بصورت خودکار ارتقاء دهند، می توانند اقدام به انواع مختلفی از حملات مانند طغیان های ICMP، طغیان های UDP و طغیان های SYN کنند.

در قسمت بعدی به روشهای مقابله با این نوع حملات خواهیم پرداخت.

عدم پذیرش سرویس (۳) : روش های مقابله

در قسمت پیش با انواع حملات DoS و DDoS آشنا شدیم. در این شماره با چند روش مقابله با حملات DoS و DDoS آشنا می شویم.

دفاع علیه حملات Smurf یا Fraggle

اگر در معرض حمله Smurf قرار گرفته باشید، کار چندانی از شما ساخته نیست. هرچند که این امکان وجود دارد که بسته های مهاجم را در روتر خارجی مسدود کنید، اما پهنای باند منشاء آن روتر مسدود خواهد شد. برای اینکه فراهم کننده شبکه بالاسری شما، حملات را در مبداء حمله مسدود کند، به هماهنگی نیاز است.

بمنظور جلوگیری از آغاز حمله از سایت خودتان، روتر خارجی را طوری پیکربندی کنید که تمام بسته های خارج شونده را که آدرس مبداء متناقض با زیرشبکه شما دارند، مسدود کند. اگر بسته جعل شده نتواند خارج شود، نمی تواند آسیب چندانی برساند.

برای جلوگیری از قرار گرفتن بعنوان یک واسطه و شرکت در حمله DoS شخص دیگر، روتر خود را طوری پیکربندی کنید که بسته هایی را که مقصدشان تمام آدرس های شبکه شماست، مسدود کند. یعنی، به بسته های ICMP منتشر شده به شبکه خود، اجازه عبور از روتر ندهید. این عمل به شما اجازه می دهد که توانایی انجام ping به تمام سیستم های موجود در شبکه خود را حفظ کنید، در حالیکه اجازه این عمل را از یک

سیستم بیرونی بگیرید. اگر واقعاً نگران هستید، می توانید سیستم های میزبان خود را طوری پیکربندی کنید که از انتشارهای ICMP کاملاً جلوگیری کنند.

دفاع علیه حملات طغیان SYN

بلاک های کوچک

بجای تخصیص یک شیء از نوع ارتباط کامل (که باعث اشغال فضای زیاد و نهایتاً اشکال در حافظه می شود)، یک رکورد کوچک (micro-record) تخصیص دهید. پیاده سازی های جدیدتر برای SYN های ورودی ، تنها ۱۶ بایت تخصیص می دهد.

کوکی های SYN

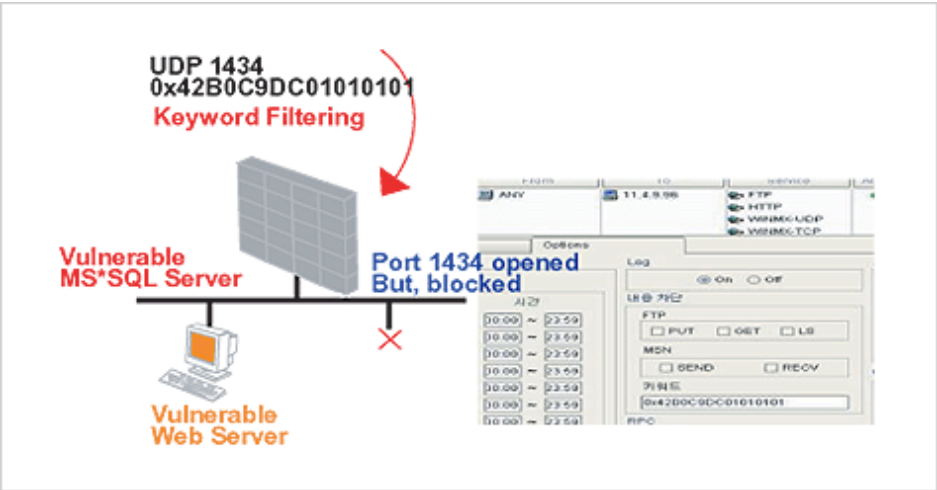
یک دفاع جدید علیه طغیان SYN «کوکی های SYN» است. در کوکی های SYN، هر طرف ارتباط، شماره توالی (Sequence Number) خودش را دارد. در پاسخ به یک SYN، سیستم مورد حمله واقع شده، یک شماره توالی مخصوص از ارتباط ایجاد می کند که یک «کوکی» است و سپس همه چیز را فراموش می کند یا بعبارتی از حافظه خارج می کند (کوکی بعنوان مشخص کننده یکتای یک تبادل یا مذاکره استفاده می شود). کوکی در مورد ارتباط اطلاعات لازم را در بردارد، بنابراین بعداً می تواند هنگامی که بسته ها از یک ارتباط سالم می آیند، مجدداً اطلاعات فراموش شده در مورد ارتباط را ایجاد کند.

کوکی های RST

جایگزینی برای کوکی های SYN است، اما ممکن است با سیستم عامل های ویندوز ۹۵ که پشت فایروال قرار دارند، مشکل ایجاد کند. روش مذکور به این ترتیب است که سرور یک ACK/SYN اشتباه به کلاینت ارسال می کند.

کلاینت باید یک بسته RST تولید کند تا به سرور بگوید که چیزی اشتباه است. در این هنگام، سرور می فهمد که کلاینت معتبر است و ارتباط ورودی از آن کلاینت را بطور طبیعی خواهد پذیرفت.

پشته های (stack) های TCP بمنظور کاستن از تأثیر طغیان های SYN می توانند دستکاری شوند. معمول ترین مثال کاستن زمان انقضاء (timeout) قبل از این است که پشته، فضای تخصیص داده شده به یک ارتباط را آزاد کند. تکنیک دیگر قطع بعضی از ارتباطات بصورت انتخابی است.



دفاع علیه حملات DNS

دفاع از سرور اصلی (root server)

پایگاه داده سرور اصلی کوچک است و بندرت تغییر می کند. یک کپی کامل از پایگاه داده اصلی تهیه کنید، روزی یک بار آپدیت ها را چک کنید و گاه و بیگاه بارگذاری های مجدد انجام دهید. از سرورهای اصلی با استفاده از آدرس های anycast استفاده کنید

(این عمل باعث می شود که سیستم ها در شبکه های با موقعیت های مختلف بعنوان یک سرور بنظر برسند.)

دفاع از سازمان تان

اگر سازمان شما یک اینترانت دارد، باید دسترسی های جداگانه ای از DNS برای کاربران داخلی و مشتریان خارجی خود فراهم کنید. این عمل DNS داخلی را از حملات خارجی در امان نگاه می دارد. ناحیه اصلی را کپی کنید تا سازمان خود را از حملات DDoS آتی روی قسمت های اصلی محفوظ نگه دارید. همچنین به کپی کردن نواحی DNS از شرکای تجاری خود که در خارج از شبکه شما قرار دارند، توجه کنید. هنگامی که بروز رسان های DNS به روی اینترنت می روند، می توانند در هنگام انتقال مورد ربایش و دستکاری قرار گیرند. از TSIGها (transaction signature) یا امضاهای معاملاتی برای امضای آن ها یا ارسال بروز رسان ها روی VPN (شبکه های خصوصی مجازی) یا سایر کانال ها استفاده کنید.

مقابله با حملات DDoS

چگونه می توانید از سرورهای خود در مقابل یورش دیتاهای ارسالی از طرف کامپیوترهای آلوده موجود در اینترنت مراقبت کنید تا شبکه شرکت شما مختل نشود؟ در اینجا به چند روش بطور مختصر اشاره می شود:

سیاه چاله

این روش تمام ترافیک را مسدود می کند و به سمت سیاه چاله! یعنی جایی که بسته ها دور ریخته می شود هدایت می کند. اشکال در این است که تمام ترافیک – چه خوب و چه بد– دور ریخته می شود و در حقیقت شبکه مورد نظر بصورت یک سیستم off-line قابل استفاده خواهد بود. در روش های اینچنین حتی اجازه دسترسی به کاربران قانونی نیز داده نمی شود.

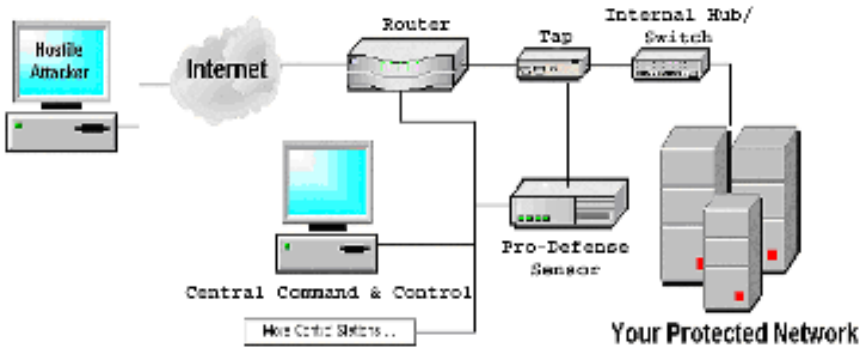
مسیریاب ها و فایروال ها

روتر ها می توانند طوری پیکربندی شوند که از حملات ساده ping با فیلترکردن پروتکل های غیرضروری جلوگیری کنند و می توانند آدرس های IP نامعتبر را نیز متوقف کنند. بهرحال، روترها معمولاً در مقابل حمله جعل شده پیچیده تر و حملات در سطح Application با استفاده از آدرس های IP معتبر، بی تأثیر هستند.

سیستم های کشف نفوذ

روش های سیستم های کشف نفوذ (intrusion detection systems) توانایی هایی ایجاد می کند که باعث تشخیص استفاده از پروتکل های معتبر بعنوان ابزار حمله می شود. این سیستمها می توانند بهمراه فایروال ها بکار روند تا بتوانند بصـورت خودکار

در مواقع لزوم ترافیک را مسدود کنند. در بعضی مواقع سیستم تشخیص نفوذ نیاز به تنظیم توسط افراد خبره امنیتی دارد و البته گاهی در تشخیص نفوذ دچار اشتباه می شود.



سرورها

پیکربندی مناسب applicationهای سرویس دهنده در به حداقل رساندن تأثیر حمله DDoS تأثیر بسیار مهمی دارند. یک سرپرست شبکه می تواند بوضوح مشخص کند که یک application از چه منابعی می تواند استفاده کند و چگونه به تقاضاهای کلاینت ها پاسخ دهد. سرورهای بهینه سازی شده، در ترکیب با ابزار تخفیف دهنده، می توانند هنوز شانس ادامه ارائه سرویس را در هنگامی که مورد حمله DDoS قرار می گیرند، داشته باشند.

ابزار تخفیف DDoS

چندین شرکت ابزارهایی تولید می کنند که برای ضدعفونی ! کردن ترافیک یا تخفیف حملات DDoS استفاده می شوند که این ابزار قبلاً بیشتر برای متعادل کردن بار شبکه یا فایروالینگ استفاده می شد. این ابزارها سطوح مختلفی از میزان تأثیر دارند. هیچکدام کامل

نیستند. بعضی ترافیک قانونی را نیز متوقف می کنند و بعضی ترافیک غیرقانونی نیز اجازه ورود به سرور پیدا می کنند. زیرساخت سرور هنوز باید مقاوم تر شود تا در تشخیص ترافیک درست از نادرست بهتر عمل کند.

پهنای باند زیاد

خرید یا تهیه پهنای باند زیاد یا شبکه های افزونه برای سروکار داشتن با مواقعی که ترافیک شدت می یابد، می تواند برای مقابله با DDoS مؤثر باشد.

عموماً، شرکت ها از قبل نمی دانند که یک حمله DDoS بوقوع خواهد پیوست. طبیعت یک حمله گاهی در میان کار تغییر می کند و به این نیاز دارد که شرکت بسرعت و بطور پیوسته در طی چند ساعت یا روز، واکنش نشان دهد. از آنجا که تأثیر اولیه بیشتر حملات، مصرف کردن پهنای باند شبکه شماست، یک ارائه کننده سرویس های میزبان روی اینترنت که بدرستی مدیریت و تجهیز شده باشد، هم پهنای باند مناسب و هم ابزار لازم را در اختیار دارد تا بتواند تأثیرات یک حمله را تخفیف دهد.

روش‌های معمول حمله به کامپیوترها (۱)

روش‌هایی که مورد استفاده خرابکاران برای ورود به کامپیوتر یا از کارانداختن آن قرارمی‌گیرد، بشرح ذیل میباشد.

۱- برنامه‌های اسب تروا

۲- درهای پشتی و برنامه‌های مدیریت از راه دور

۳-عدم پذیرش سرویس

۴- وساطت برای یک حمله دیگر

۵- اشتراکهای ویندوزی حفاظت‌نشده

۶- کدهای قابل انتقال (Java ، JavaScript و ActiveX)

۷- اسکریپتهای Cross-Site

۸- ایمیلهای جعلی

۹- ویروسهای داخل ایمیل

۱۰- پسوندهای مخفی فایل

۱۱- سرویس‌گیرندگان چت

۱۲- شنود بسته‌های اطلاعات

۱- برنامه‌های اسب تروا

برنامه‌های اسب تروا روشی معمول برای گول زدن شما هستند (گاهی مهندسی اجتماعی نیز گفته می‌شود) تا برنامه‌های "درپشتی" را روی کامپیوتر شما نصب کنند. و به این ترتیب اجازه دسترسی آسان کامپیوترتان را بدون اطلاعتان به مزاحمین می‌دهند، پیکربندی سیستم شما را تغییر می‌دهند، یا کامپیوترتان را با یک ویروس آلوده می‌کنند.

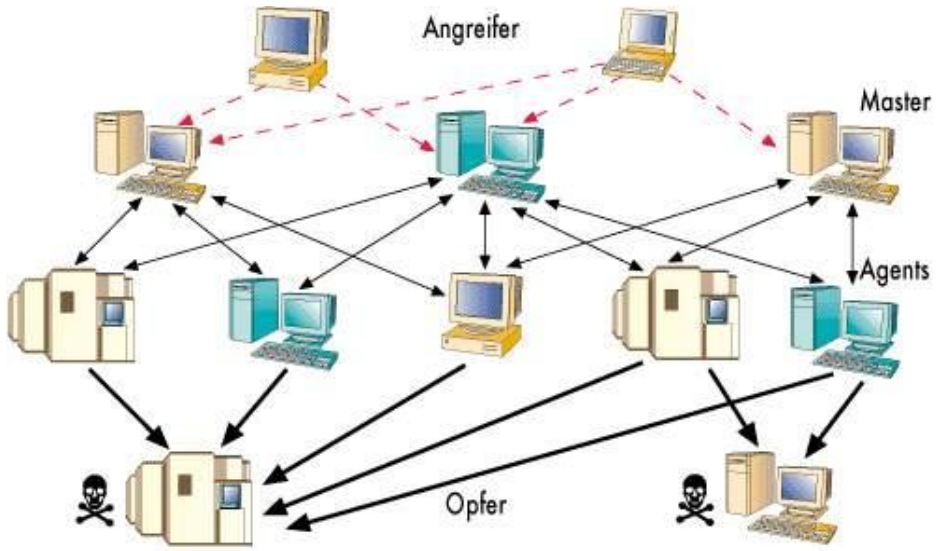
۲- درهای پشتی و برنامه‌های مدیریت از راه دور

روی کامپیوترهای ویندوزی، معمولا سه ابزار توسط مزاحمین برای دسترسی از راه دور به کامپیوترتان استفاده می‌شود. BackOrifice ، Netbus و SubSeven. این برنامه‌های درپشتی یا مدیریت از راه‌دور وقتی نصب می‌شوند، به افراد دیگر اجازه دسترسی و کنترل کامپیوترتان را می‌دهند. به شما توصیه می‌کنیم که شکاف‌های امنیتی را بخصوص در مورد BackOrifice از CERT مطالعه کنید.

۳- عدم پذیرش سرویس

نوعی دیگر از حمله، Denial-of-Service یا عدم‌پذیرش‌سرویس نام دارد. این نوع حمله باعث از کارافتادن یا مشغول شدن بیش از حد کامپیوتر تا حد غیرقابل‌استفاده

شدن می‌شود. در بیشتر موارد، آخرین وصله‌های امنیتی از حمله جلوگیری خواهند کرد. شایان گفتن است که علاوه بر اینکه کامپیوتر شما هدف یک حمله DoS قرار می‌گیرد، ممکن است که در حمله DoS علیه یک سیستم دیگر نیز شرکت داده شود.



۴- وساطت برای یک حمله دیگر

مزاحمین به‌کرات از کامپیوترهای مورد حمله قرارگرفته برای پایگاهی برای حمله به سیستم‌های دیگر استفاده می‌کنند. یک مثال آن چگونگی استفاده از آنها بعنوان ابزار حملات DoS توزیع‌شده است. مزاحمین یک "عامل" را (معمولا از طریق یک اسب تروا) نصب می‌کنند که روی کامپیوتر مورد حمله قرارگرفته اجرا می‌شود و منتظر دستورهای بعدی می‌ماند. سپس، هنگامی که تعدادی از عامل‌ها روی کامپیوترهای مختلف در حال اجرا هستند، به تمام آنها دستور داده می‌شود که یک حمله denial-of-service را روی یک سیستم پیاده کنند. بنابراین، هدف نهایی حمله، کامپیوتر شما

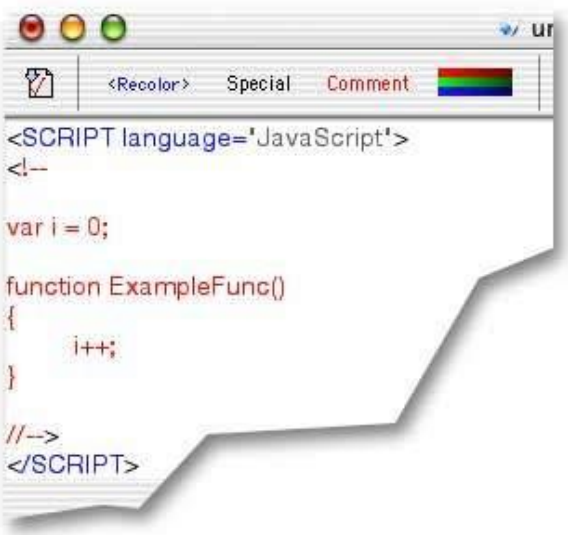
نیست، بلکه سیستم شخص دیگری است – کامپیوتر شما فقط یک ابزار مناسب برای یک حمله بزرگتر است.

۵- اشتراکهای ویندوزی حفاظت‌نشده

اشتراکهای شبکه ویندوزی محافظت‌نشده می‌توانند توسط مزاحمین تحت یک روش خودکار برای قراردادن ابزارها روی تعداد زیادی از کامپیوترهای ویندوزی متصل به اینترنت مورد سوءاستفاده قرار گیرند. از آنجا که برای امنیت سایت روی اینترنت وابستگی بین سیستمها وجود دارد، یک کامپیوتر مورد حمله قرارگرفته نه تنها مشکلاتی برای صاحبش فراهم می‌کند، بلکه تهدیدی برای سایتهای دیگر روی اینترنت محسوب می‌شود. عامل بالقوه بزرگی در گستره وسیع برای ظهور ناگهانی سایر ابزارهای مزاحمت وجود دارد که از اشتراکهای شبکه ویندوزی محافظت‌نشده استفاده می‌کند.

۶- کدهای قابل انتقال (Java ، JavaScript و ActiveX)

گزارشهایی در مورد مشکلات با "کدهای سیار" (مانند JavaScript Java و ActiveX) وجود داشته است. اینها زبانهای برنامه‌سازی هستند که به توسعه‌دهندگان وب اجازه نوشتن کدهای قابل اجرا در مرورگر شما را می‌دهند. اگرچه کد عموما مفید است، اما می‌ؤواند توسط مزاحمان برای جمع‌آوری اطلاعات (مثلا وب‌سایتهایی که سر می‌زنید) یا اجرای کدهای آسیب‌رسان روی کامپیوتر شما مورد استفاده قرار گیرد. امکان از کار انداختن JavaScript Java و ActiveX در مرورگر شما وجود دارد. توصیه می‌شود که اگر در حال مرور وب‌سایتهایی هستید که با آنها آشنا نیستید یا اطمینان ندارید، این کار را انجام دهید، اگرچه از خطرات احتمالی در استفاده از کدهای سیار در برنامه‌های ایمیل آگاه باشید. بسیاری از برنامه‌های ایمیل از همان کد بعنوان مرورگرهای وب برای نمایش HTML استفاده می‌کنند. بنابراین، شکافهای امنیتی که بر JavaScript Java و ActiveX اثرگذارند، اغلب علاوه بر صفحات وب در ایمیلها هم قابل اجرا هستند.



در قسمت بعد به ادامه روشها پرداخته خواهد شد...

روش های معمول حمله به کامپیوترها (۲)

در قسمت قبل به ۶ روش حمله بطور مختصر پرداختیم ...

۷- اسکریپتهای Cross-Site

یک برنامه نویس وب با افکار بدخواهانه ممکن است اسکریپتی به آنچه که به یک وب سایت فرستاده می شود، مانند یک URL ، یک عنصر در شکلی خاص، یا درخواست از یک پایگاه داده، بچسباند. بعدا، وقتی وب سایت به شما پاسخ می دهد، اسکریپت زیان رسان به مرورگر شما منتقل می شود.

شما می توانید مرورگر وب تان را توسط روشهای زیر در اختیار اسکریپتهای زیان رسان قرار دهید:

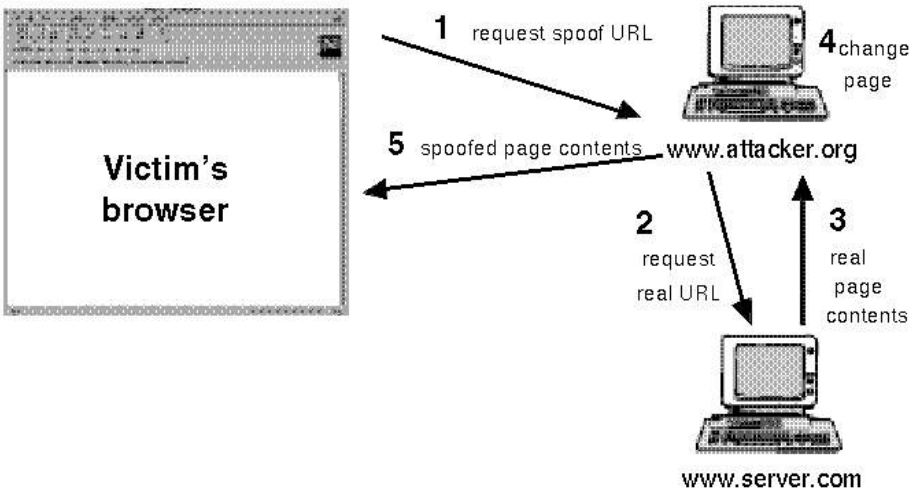
× تعقیب لینک ها در صفحات وب، ایمیلها یا پیام های گروه های خبری بدون دانستن به آنچه لینک داده شده است.

× استفاده از فرم های محاوره ای روی یک سایت غیرقابل اطمینان

× دیدن گروه های بحث آنلاین، مجمع ها یا دیگر صفحاتی که بصورت پویا تولید می شوند در جایی که کاربران می توانند متنهای شامل تگ های HTML ارسال کنند.

۸- ایمیلهای جعلی

این حالت زمانی اتفاق می افتد که یک ایمیل به ظاهر متعلق به منبعی می باشد درحالیکه در حقیقت از منبعی دیگر ارسال شده است. Email Spoofing اغلب برای گول زدن کاربر بمنظوراین که اطلاعات حساس (مانند کلمات عبور) را افشاء کند بکار می رود.



ایمیل جعل شده می تواند گستره ای از شوخی های بی ضرر تا اقدامات مربوط به مهندسی اجتماعی داشته باشد. مثالهایی از مورد دوم اینها هستند:

× ایمیل ادعا می کند که از مدیر یک سیستم است و از کاربران تقاضای تغییر کلمات عبورشان را به یک رشته مشخص دارد و آنها را در صورت عدم تابعیت به تعلیق اکانتهایشان تهدید می کند.

× ایمیل ادعا می کند از یک شخص با اختیارات لازم است و از کاربران تقاضا می کند که یک کپی از فایل کلمات عبور یا سایر اطلاعات حساس را برایش ارسال کنند.

توجه کنید وقتی سرویس دهندگان گهگاهی تقاضا می کنند که کلمه عبورتان را تغییر دهید، معمولا مشخص نمی کنند که به چه کلمه ای تغییر کند. همچنین، بیشتر سرویس دهندگان قانونی از شما هرگز تقاضای ارسال کلمات عبورتان را از طریق ایمیل نمی کنند. اگر شک دارید که یک ایمیل جعلی از شخصی با تمایلات بدخواهانه دریافت کرده اید، باید با پرسنل پشتیبانی سرویس دهنده خود سریعا تماس بگیرید.

۹- ویروسهای داخل ایمیل

ویروس ها و سایر کدهای آسیب رسان اغلب بعنوان پیوست ایمیلها گسترش می یابند. قبل از بازکردن هر پیوستی، از شناخته شده بودن منبع آن اطمینان حاصل کنید. اینکه ایمیل از آدرسی باشد که شما می شناسید، کافی نیست. ویروس ملیسا دقیقا به این علت گسترش یافت که آدرس فرستنده آن آشنا بود. همچنین، کدهای آسیب رسان ممکن است در برنامه های سرگرم کننده یا فریبنده گسترش پیدا کنند.

هرگز برنامه ای را اجرا نکنید، مگر اینکه توسط شخص یا شرکتی نوشته شده باشد که به آن اعتماد دارید. بعلاوه، برنامه هایی را که از منابع ناشناخته دریافت می کنید، صرفا بخاطر اینکه سرگرم کننده هستند، برای دوستان یا همکاران خود ارسال نکنید.

۱۰- پسوندهای مخفی فایل

سیستم عاملهای ویندوز انتخابی را در اختیار شما قرار می دهند که " پسوند فایلهایی که نوع آنها شناخته شده است را پنهان می کند". این انتخاب بصورت پیش فرض فعال است، اما ممکن است یک کاربر این قابلیت را بمنظور به نمایش درآمدن پسوند تمام فایلها توسط ویندوزغیرفعال کند. ویروسهای داخل ایمیل از پنهان ماندن پسوند فایلهای شناخته شده بهره برداری می کنند. اولین حمله عمده که از این قابلیت بهره گرفت کرم VBS/LoveLetter بود که حاوی یک پیوست به نام "LOVE-LETTER-FOR-YOU.TXT.vbx" بود. سایر برنامه های آسیب رسان چنین طرحهای نامگذاری مشابهی دارند. چندین مثال اینها هستند:

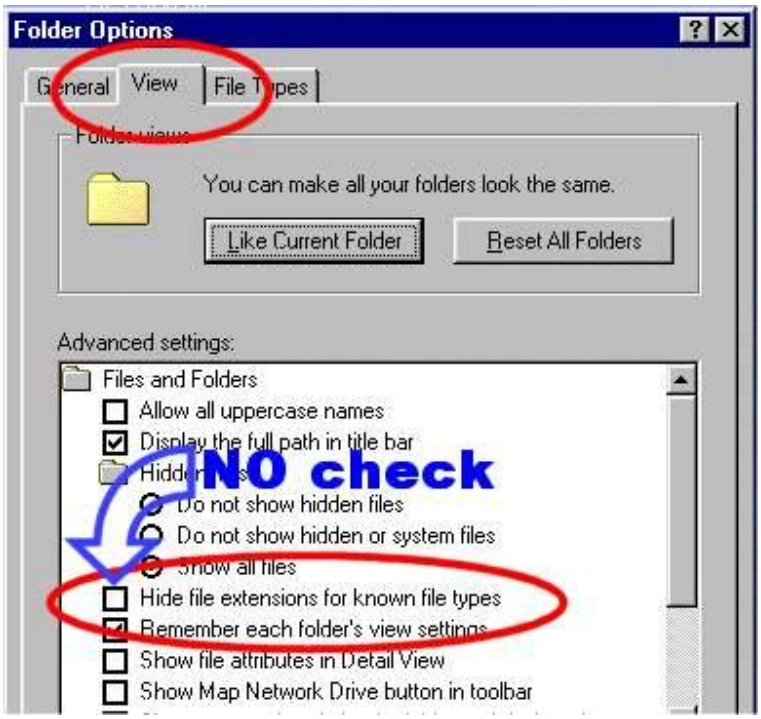
Downloader (MySis.avi.exe or QuickFlicking.mpg.exe)×

VBS/Timofonica (TIMOFONICA.TXT.vbs)×

VBS/CoolNote (COOL_NOTEPAD_DEMO.TXT.vbs)×

VBS/OnTheFly (AnnaKournikova.jpg.vbs)×

فایلهای پیوسته به ایمیلها که توسط این ویروسها فرستاده می شوند، ممکن است بی ضرر بنظر برسند، فایلهای متنی (.txt)، فایلهای تصویری (.mpg یا .avi) یا دیگر انواع فایل در حالیکه در حقیقت این فایل یک اسکریپت یا فایل اجرایی آسیب رسان است (برای مثال .vbs یا .exe)



۱۱- سرویس گیرندگان چت

برنامه های چت اینترنتی، مانند برنامه های پیام رسانی سریع و شبکه های IRC، مکانیسمی را فراهم می کنند تا اطلاعات بصورت دوطرفه بین کامپیوترهای متصل به اینترنت منتقل شود. برنامه های چت برای گروههایی از افراد، امکان مکالمه، تبادل URL و در بسیاری موارد انتقال انواع فایلها را فراهم می کنند.

چون بسیاری از برنامه های چت اجازه تبادل کدهای قابل اجرا را می دهند، خطراتی مشابه برنامه های انتقال ایمیل را ایجاد می کنند. مانند برنامه های ایمیل، باید دقت کافی برای محدودکردن توانایی برنامه های چت برای اجرای فایلهای دانلود شده، بکار گرفته شود. مثل همیشه، باید مواظب تبادل فایل با طرفهای ناشناس باشید.