استراق سمع داده‌ها

- ***Sniffing*** : در اين روشها هكر قادر است اقدام به استراق سمع داده‌ها در شبكه كند ولي در تغيير داده‌ها نقشي ندارد. اين كار با نصب برنامه Sniffer هكر روي يكي از كامپيوترهاي شبكه صورت مي‌گيرد و بسته‌هاي روي كانال فيزيكي شبكه را به هكر مي‌فرستد.

يك Sniffer در سه مرحله كار مي‌كند:

- اول از همه سخت افزار شبكه را در حالت بي‌قيد تنظيم مي‌كند تا اطلاعات تمام آدرس‌ها و پورت‌ها براي اين برنامه ارسال شود.
- سپس Sniffer از بين بسته‌هاي ارسال شده بسته‌هاي مورد نياز هكر را جدا مي‌كند.
- و در نهايت اطلاعات مورد نياز هكر را براي او ارسال مي‌كند.

- ***حملات Dos*** : اين حمله با نام Denial of service به معني اخلال در سرويس دهي مي‌باشد و تشابه اسمي آن با سيستم عامل Dos فقط يك تشابه اسمي است و هيچ ارتباطي با آن ندارد.

در اين روش هكر در عمل سعي جلوگيري از سرويس دهي شبكه مي‌كند و هدف اصلي از حملات Dos در هم شكستن سرويس دهنده و قطع ارتباط قرباني براي مدتي يا به طور دائم با شبكه مي‌باشد. اين حمله انواع مختلفي دارد و هكر از هر روشي براي ايجاد اخلال در TCP استفاده مي‌كند. حمله Dos ممكن است از درون شبكه و يا از خارج شبكه صورت گيرد. در حمله از درون شبكه هكر به عنوان مدير يا در سطوح پايين‌تر قادر است هر پروسه سرويس دهنده‌اي را متوقف كند حمله از بيرون معمولاً حمله‌اي است كه منجر به ترافيك شبكه و از بين رفتن منابع مي‌گردد.

برخي از انواع اين حمله به اختصار شرح داده مي‌شود:

حمله از نوع land : در اين نوع حمله انبوهي از بسته‌هاي TCP با شرايط زير به كامپيوتر سرويس دهنده فرستاده مي‌شود.

1. فيلدهاي Source port و Destination port دقيقاً مانند هم و به مقدار يكي از پورت‌هاي باز هر دو ماشين در شبكه.
2. فيلدهاي Source IP Address و Destination IP Address و با هم مانند هم و به مقدار آدرس IP ماشيني مقصد.

با اين كار پس از ارسال بسته به ماشين هدف چون آدرس مبدأ و مقصد يكي است. توسط TCP مورد قبول نمي‌باشد و به ماشين اصلي بر مي‌گردد و در ماشين اصلي نيز چون همين مشكل وجود دارد به IP تنظيم شده بسته "ماشين هدف" برگشت داده مي‌شود و اين كار همينطور ادامه پيدا مي‌كند تا زماني كه TCP شكست بخورد و مختل گردد.

حمله Ping Of Death :

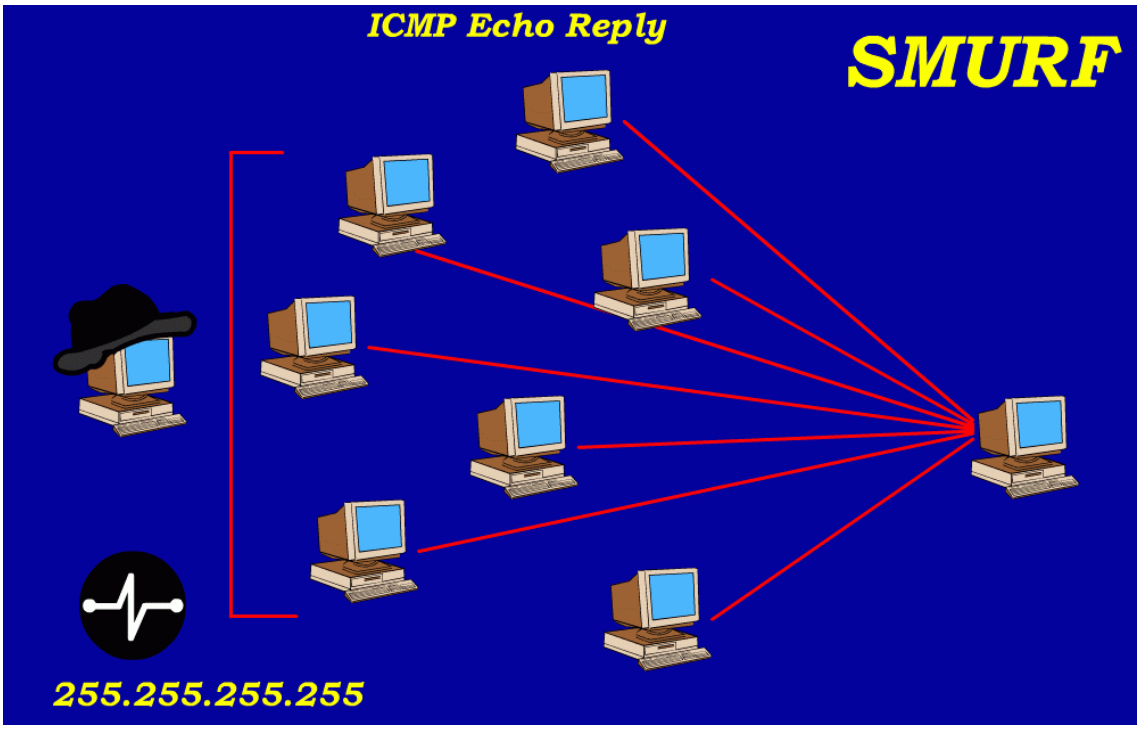
در اين نوع حمله يك بسته ping با اندازه بيش از 64 k براي پروسه ICMP ارسال مي‌گردد با دريافت چنين بسته‌اي به دليل اينكه TCP براي چنين حالتي طراحي نگرديده مختل مي‌گردد.

حمله نوع *Jolt 2* :

در اين نوع حمله يك جريان طولاني و وسيع از بسته‌هاي قطعه قطعه شده به سمت ماشين هدف در شبكه هدايت مي‌شوند. از اين رو پروسه TCP بايد اين قطعه‌ها را در خود نگهداري كند و چون تحت بمباران قرار گرفته در هم مي‌شكند و ارتباط آن ماشين با شبكه قطع مي‌گردد. طبق گزارشها تمامي سيستمهاي عامل ويندوز از اين مشكل رنج مي‌برند.

حمله نوع *Smurf* :

از آدرس IP 255. 255. 255. 255 براي ارسال پيامهاي فراگير به ماشين‌هاي شبكه محلي استفاده مي‌گردد به وسيله اين آدرس مي‌توان يك پيام را براي تمام ماشين‌هايي كه فقط سمت راست IP آنها متفاوت هست ارسال كرد. در حمله Smurf هكر بسته‌اي را با مشخصات فراگير به شبكه محلي مي‌فرستد. با اين تذكر كه آدرس قرباني را به جاي آدرس خود قرار مي‌دهد. در نتيجه كليه ماشينهايي كه اين بسته را دريافت كرده‌اند سعي در ارسال بسته ICMP Echo Reply مي‌كنند. چون به يكباره تمامي اين بسته‌ها به سوي سيستم قرباني ارسال مي‌گردد و سيستم قرباني قادر به جواب دادن به آنها نيست هنگ مي‌كند و ارتباط مختل مي‌گردد.



در حمله Smurf به ماشينهاي مورد استفاده هكر زامبي مي‌گويند. زامبي اصطلاحي است كه به كامپيوترهايي كه بدون داشتن اطلاع صاحبشان توسط هكر به عنوان ابزار حمله Dos قرار مي‌گيرند، اطلاق مي‌گردد.

حمله Treadrop : در اين روش بسته‌هاي قطعه قطعه شده با تنظيم غلط فيلدهاي بسته پشت سر هم ارسال مي‌شوند و در نهايت به طرز صحيحي بازسازي نخواهند شد و مي‌تواند موجب اختلال TCP گردد.

- ***ويروسها***:

كاربران كامپيوترهاي شخصي و شبكه‌هاي كامپيوتري از ويروسها خسارات زيادي ديده‌اند. ويروس فقط يك برنامه كامپيوتري است كه ممكن است با هر زبان برنامه‌نويسي نوشته شده باشد با اين تفاوت كه ويروس‌ها برنامه‌هاي مخفي، مخرب و خطرناكي هستند كه برخلاف برنامه‌هاي كاربردي مفيد به نرم‌افزارها و حتي در مواردي به سخت‌افزارهاي سيستم صدمه مي‌زنند.

هكر با استفاده از ويروسي مي‌تواند كامپيوتر قرباني را تا حد بسيار زيادي در مقابل حمله و نفوذ هكر شكست‌پذير و ضعيف كند و راه را براي نفوذ هكر باز كند. هكر بايد به طريقي ويروس را در كامپيوتر قرباني اجرا كند.

- ***اسبهاي تراوا*** :

اسبهاي تراوا يكي از پركاربردترين برنامه‌ها در جهت نفوذ به سيستم‌ها مي‌باشد. استفاده از اين ابزار براي تمامي گروههاي هكرها و در هر سطحي امكان‌پذير است. اسبهاي تراوا ساختاري ساده و كاربردي راحت دارند. نامگذاري اين برنامه‌ها به اسب تراوا به واقعه تاريخي در سالها قبل مربوط مي‌شود. اسب تراوا، اسب چوبي و توخالي بود كه يونانيان در جنگ تراوا وقتي كه ديدند نمي‌توانند راه بازي را به درون قلعه پيدا كنند. اين اسب را به آنها هديه دادند. در حالي كه تعدادي از سربازان يوناني درون آن مخفي شده بودند. با وارد كردن اسب تراوا به درون قلعه سربازان يوناني مخفيانه درهاي قلعه را براي نفوذ يونانيان باز كردند و از درون قلعه كنترل را بدست گرفتند.

اسب‌هاي تراواي كامپيوتري نيز به همين گونه با ظاهري ساده و فريبنده بر سيستم قرباني وارد مي‌شوند. - (با اجراي برنامه توسط خود قرباني) – و پس از ورود پنهان و مسكوت مي‌مانند و در موقعيت لازم كنترل كامپيوتر قرباني را به هكر مي‌سپارند. اسب‌هاي تراوا برخلاف ويروسهاي كامپيوتري خودشان هيچ‌گونه عمليات تخريبي انجام نمي‌دهند و فقط منتظر دستورهاي هكر مي‌مانند.

هر گاه كاربر فريب بخورد و اين برنامه را در كامپيوتر خود اجرا كند. اسب تراوا معمولاً پيكربندي سيستم عامل را به گونه‌اي تغيير مي‌دهد تا هرگاه كاربر به شبكه متصل شود برنامه نيز اجرا گردد. اسب‌هاي تراوا هيچگونه علامت ظاهري و پنجره خاصي ندارند و كاملاً مخفي هستند.

از نمونه‌هاي معروف و پركاربردترين اسب‌هاي تراوا براي هكرها مي‌توان Bo2k Sub 7 و ... را نام برد.

- ***درب‌هاي پشتي***:

اين ابزارها بسيار مورد علاقه هكرها مي‌باشند. چون نفوذ با اين ابزارها بسيار راحت‌تر مي‌باشد. درب پشتي به روشهايي مي‌گويند كه هكر به وسيله آنها بتواند بدون آنكه به تشريفات (كلمه رمز عبور و ...) احتياج داشته باشد به كامپيوتر قرباني وارد شود.

يكي از ساده‌ترين و كارآمدترين روشهاي درب پشتي كه هنوز هم برقرار است، استفاده از Netcat براي ارتباط روي يك پورت مي‌باشد.

به وسيله دستور زير مي‌توان از Netcat به عنوان يك درب پشتي استفاده كرد.

ويندوز Nc – I – P[port] – e cmd, exe

Unix $ Nc – I – P[port] – w/ bin/ sh

بعد از اين كار سريعاً برنامه پوسته فرمان اجرا مي‌شود و هر چه هكر از طريق ماشين خود تايپ كند. به عنوان دستور تحويل سيستم مقابل داده و اجرا مي‌شود. و هكر مي‌تواند خروجي اين دستورات را نيز در كامپيوتر خود مشاهده كند.

هكر براي نفوذ به در پشتي نياز به هيچ عملي به جز برقراري يك ارتباط با پورت 12345 نداشته و احراز هويت و رمزنگاري معنايي ندارد و به اين وسيله هكر مي‌تواند اختيار آن سيستم را بدست بگيرد.

- ***Rootkit*** :

Rootkitها بسيار بسيار قدرتمندتر از Virus ها و اسب‌هاي تراوا عمل مي‌كنند. به اين دليل كه Rootkit ها مستقيماً اجزاي سيستم عامل را هدف قرار مي‌دهند و با دستكاري سيستم عامل عملاً بيشترين نفوذ و بالاترين سطح دسترسي را براي خود نزديكتر مي‌كند. بدترين حالت Rootkit براي قرباني اين است كه هكر مستقيماً به هسته سيستم عامل نفوذ كند و آن را مطابق ميل خود تغيير دهد. در اين حالت هكر خود را غيرقابل شناسايي براي كاربر و حتي برنامه‌هاي بررسي شبكه و آنتي‌ها مي‌سازد زيرا به قلب سيستم عامل نفوذ كرده و تمامي برنامه‌ها و موارد ديگر در اختيار اوست.

Rootkit ها بيشتر براي سيستم عامل Unix و خانواده آن نوشته مي‌شوند. زيرا اين ويندوزها Open source هستند و برنامه‌نويسي براي اجزاي ويندوز بسيار راحت‌تر مي‌باشد و از طرفي نيز در سطح هسته از قابليت LKM سيستمهاي Unix و سيستمهاي سازگار با آن نهايت استفاده را مي‌برند.

LKM مخفف Loadable Kernel Module قابليتي است كه براي توسعه سيستم عامل Unix و پشتيباني از آن قرار داده شده و اجازه بارگذاري ماژولهاي نوشته شده برنامه‌نويس به هسته سيستم عامل را مي‌دهد. در اين سيستم عاملها (اغلب Unix و Solaris) برخلاف ويندوز نياز به راه‌اندازي مجدد سيستم عامل نيست و Rootkit ها مي‌توانند توسط LKM بسيار راحت نصب شوند و زمان را براي هكر تلف نمي‌كنند.

نفوذ از طريق Rootkit ها در سيستمهاي تحت ويندوز بسيار بسيار پيچيده‌تر از Unix و سيستمهاي پشتيباني كننده از LKM ها است و به نسبت خيلي كم اتفاق مي‌افتد كه هكر موفق به نوشتن Rootkit بخصوص در سطح هسته Kernell ويندوز شود ولي از آنجايي كه هيچ كاري براي هكرها غيرممكن نيست Rootkit هايي نيز براي ويندوز نوشته شده است كه بعضاً با تغيير در فايلهاي سيستمي ويندوز مانند Dll ها تا حدود زيادي كنترل سيستم عامل را بدست مي‌گيرد و با جايگزين كردن اين Dll ها كامپيوتر قرباني را در برابر نفوذ شكست‌پذير مي‌كند.

در سيستمهاي ويندوز چون از LKM استفاده نمي‌شود Rootkit ها قابل بارگذاري نيستند ولي در اين موارد از Path استفاده مي‌گردد. پس از اجراي Path سيستم زماني آلوده مي‌گردد كه سيستم عامل مجدداً راه‌اندازي شود. سپس برنامه هكر قسمتهاي مختلف موردنظر را دست‌كاري مي‌كند. براي جلوگيري از نفوذ هكرها به وسيله Rootkit

پيشگيري هميشه بهتر از درمان مي‌باشد و براي درمان نيز بهترين و مطمئن‌ترين راه حل نصب مجدد ويندوز يا هر سيستم عامل ديگر مي‌باشد. زيرا زحمت و دردسري كه درمان سيستم آلوده به Rootkit دارد بسيار بيشتر از نصب و راه‌اندازي مجدد سيستم عامل مي‌باشد.

در آخر متذکر میشوم که حتی با دانستن تمامی راههای نفوذ به شبکه که در این مقاله گفته شد و یا راههای مطرح نشده (که از حیطه این مقاله خارج بوده) نمیتوان به طور 100% از نفوذ ناپذیری شبکه اطمینان حاصل کرد زیرا هکر ها همواره در تلاش برای کشف راههای نفوذ جدید و ناشناخته میباشند . ولی با رعایت بسیاری از این موارد میتوان ضریب نفوذپذیری شبکه را به صفر نزدیک کرد ...

تهیه و تنظیم : افشین عباسپور

www.iranvig.com