راههاي نفوذ به شبكه‌هاي كامپيوتري

يكي از مهمترين مشغله‌هاي كارشناسان شبكه امنيت شبكه و مقابله با نفوذگران مي‌باشد. بنابراين كشف راه‌هاي نفوذ به شبكه بايد همواره مورد توجه مسئولان شبكه‌هاي كامپيوتري قرار بگيرد.
يك مسئول شبكه و حتي يك كاربر ساده بايد با راه‌هاي نفوذ به شبكه آشنا باشد تا با بستن و كنترل اين راهها شبكه يا سيستم موردنظر را از حملات هكرها محفوظ بدارد.
در ذهنيت عمومي هكر يك انسان شرور و خرابكار است ولي در واقع اينگونه نيست و هكرها در بسياري از موارد هدفشان پيدا كردن صعف‌هاي شبكه و برطرف كردن آنهاست به همين دليل در اواخر دهه 80 هكرها را بر اساس فعاليتهايشان دسته‌بندي كردند.

I.) گروه نفوذگران كلاه سفيد (White Hacker Group)
II.) گروه نفوذگران كلاه سياه (Black Hacker Grpoup)
III.) گروه نفوذگران كلاه خاكستري (Gray Hat Haker Group)
IV.) گروه نفوذگران كلاه صورتي (Pink Hat Haker Group)

I. اين گروه در واقع دانشجويان و اساتيدي هستند كه هدفشان نشان دادن ضعف سيستم‌هاي امنيتي شبكه‌هاي كامپيوتري مي‌باشد. اين گروه به هكرهاي خوب معروفند كه در تحكيم ديواره حفاظتي شبكه‌هاي نقش اساسي دارند. اين گروه خلاقيت عجيبي دارند و معمولاً هر بار با روشهاي نو و جديدي از ديواره‌هاي امنيتي عبور مي‌كنند.
II. اين گروه خراب‌كارانه‌ترين نوع هكرها هستند و به Crackerها معروف هستند. كلاه سياه‌ها اغلب ويروس نويسند و با ارسال ويروس نوشته شده خود بر روي سيستم قرباني به آن نفوذ مي‌كنند. اين گروه هميشه سعي در پنهان نمودن هويت خود را دارند.
III. نام ديگر اين گروه واكرها است "whacker". هدف اصلي واكرها استفاده از اطلاعات ساير كامپيوترها به مقاصد مختلف مي‌باشد. در صورتي كه با نفوذ به شبكه صدمه‌اي به كامپيوترها وارد نمي‌كنند. مثلاً در سال 1994 يك هكر "كلاه خاكستري" ژاپني به سايت ناسا Nasa آمريكا نفوذ پيدا كرد و تمامي اسناد محرمانه متعلق به اين سازمان را ربود و به طور رايگان بر روي اينترنت در اختيار عموم قرار داد.
IV . اين گروه افراد بي‌سوادي هستند كه فقط قادرند به وسيله نرم‌افزارهاي ديگران در سيستمها اختلال به وجود بياورند و مزاحمت ايجاد كنند. به اين افراد Booter گفته

مي‌شود. بوترها خود سواد برنامه‌نويسي ندارند ولي در بعضي از موارد همين نوع هكرها مي‌توانند خطرهاي جدي براي شبكه به وجود آورند.

انواع حملات هكرها)))...

حمله از نوع دستكاري اطلاعات "Modification"

به اين معني كه هكر در حين انتقال اطلاعات به مقصد آنها را مطابق خواسته خود تغيير داده و به كاربر مي‌فرستد و كاربر بدون اطلاع از تغيير آنها را مورد استفاده قرار مي‌دهد.

حمله از نوع افزودن اطلاعات "Farication"

در اين نوع از حمله هكر به جاي تغيير دادن اطلاعات، اطلاعات جديدي را به آن مي‌افزايد مانند يك ويروس جهت اقدامات بعدي.

حمله از نوع استراق سمع "Interception"

در اين نوع حمله هكر فقط به اطلاعات در حين تبادل گوش مي‌دهد و در صورت لزوم از آن نسخه‌برداري مي‌كند.

حمله از نوع وقفه "Interruption"

در اين نوع حمله هكر با ايجاد اختلال در شبكه و وقفه در انتقال اطلاعات براي خود فرصت لازم جهت اقدامات بعدي را فراهم مي‌آورد.

موارد مورد نياز هكر)))...

اطلاعاتي هر چند بي‌اهميت از ديد شما مي‌تواند براي هكر بسيار مهم باشد اما براي نفوذ به هر گونه شبكه كامپيوتري تحت TCP/IP داشتن IP قرباني مورد نياز است. شما هر گاه به اينترنت متصل مي‌شويد داراي يك IP منحصر به فرد جديد مي‌باشيد كه اين IP در حقيقت آدرس كامپيوتر شما در شبكه مي‌باشد.

دومين مورد كه براي نفوذ به كامپيوتر قرباني لازم مي‌باشد داشتن حداقل يك پورت باز مي‌باشد. اگر كامپيوتر قرباني را در شبكه به يك خانه در شهر تشبيه كنيم IP آدرس اين خانه و پورت‌ها راههاي ورودي اين خانه از قبيل در، پنجره، ديوار و ... مي‌باشند.

بديهي است كه بدون در اختيار داشتن آدرس منزل و پيدا كردن يكي از ورودي‌هاي خانه كه مسدود نمي‌باشد ورود به آن خانه تقريباً غيرممكن است.

نشاني IP از چهار عدد از صفر تا 255 تشكيل شده كه با نقطه از هم جدا مي‌شوند. براي پيدا كردن محل يك كامپيوتر در شبكه از روي IP به صورت زير عمل مي‌شود.

آدرس ماشين. آدرس زير شبكه. آدرس شبكه

هكر با استفاده از روشها و ابزارهايي كه در ادامه به آن اشاره خواهد شد قادر است نقشه شبكه را بدست آورد و اين براي هكر يك موفقيت بزرگ محسوب مي‌شود.

شماره پورت همراه اطلاعات در بسته‌هاي ICP فرستاده مي‌شود و مشخص مي‌كند كه بسته از چه برنامه كاربردي در لايه بالاتر توليد و به چه برنامه‌اي ارسال گردد و در

ماشين مقصد به آن تحويل داده شود. برخي از برنامه‌هاي كاربردي استاندارد و جهاني داراي شماره پورت استاندارد و مشخص مي‌باشند. به عنوان مثال سرويس‌دهنده پست الكترونيك SMTP از شماره پورت 25 استفاده مي‌كند و يا پورت استاندارد برنامه TelNet 23 مي‌باشد. با دانستن پورت استاندارد نرم‌افزارها و بستن آن پورت در كامپيوتر مي‌توان از تبادل اطلاعات آن برنامه با كامپيوترها جلوگيري كرد.
با استفاده از برنامه Netstat موجود در ويندوز مي‌توانيد كامپيوترها و پورت‌هايي را كه كامپيوتر شما با آنها در حال تبادل اطلاعات مي‌باشد، شناسايي كنيد.
براي اجراي اين نرم‌افزار در Ms – Dos Prompt ويندوز عبارت Netstat را تايپ كنيد و كليد Enter را فشار دهيد. در اين هنگام ليستي از اتصال‌هاي اينترنتي كه در حال حاضر مشغول كار هستند قابل مشاهده مي‌باشد.
اگر روي خط فرمان عبارت Netstat – na را تايپ كنيد. تمام پورت‌هايي كه در حال تبادل اطلاعات هستند گزارش داده مي‌شود.
از Netstat مي‌توان براي شناسايي شبكه و نيز كشف حملات هكرها نيز استفاده كرد.
نمونه خروجی دستور Netstat را مشاهده كنيد :

```
D:\>netstat
Active Connections
Proto  Local Address          Foreign Address        State
TCP    afshin:1026            afshin:1208            TIME_WAIT
TCP    afshin:1026            afshin:1218            TIME_WAIT
TCP    afshin:1216            afshin:1026            TIME_WAIT
TCP    afshin:1220            afshin:1026            TIME_WAIT
TCP    afshin:1031            cs21.msg.dcn.yahoo.com:5050  ESTABLISHED
TCP    afshin:1212            18.67-18-50.reverse.theplanet.com:80  TIME_WAIT
TCP    afshin:1213            207.46.249.56:80       TIME_WAIT
TCP    afshin:1215            18.67-18-50.reverse.theplanet.com:80  TIME_WAIT
TCP    afshin:1217            18.67-18-50.reverse.theplanet.com:80  TIME_WAIT
TCP    afshin:1222            207.46.249.56:80       TIME_WAIT
TCP    afshin:1226            v4.windowsupdate.microsoft.com:80  TIME_WAIT
TCP    afshin:1227            v4.windowsupdate.microsoft.com:80  ESTABLISHED
TCP    afshin:1229            207.46.253.188:80      ESTABLISHED
TCP    afshin:5101            217.219.173.216:3407   ESTABLISHED
```

IP براي كامپيوترهايي كه نقش سرور را دارند. "مانند سايت‌ها و يا كامپيوترهايي كه غير از Dial up به اينترنت متصل مي‌شوند عددي ثابت تعريف مي‌شود ولي براي افراد "Client" هاي معمولي در هر بار اتصال به انيترنت IP تغيير مي‌كند.
براي بدست آوردن IP خود در شبكه مي‌توانيد از دستور IpconfiG در خط فرمان ويندوز استفاده كنيد. در اين صورت IP شما در شبكه به عنوان خروجي دستور نمايش داده مي‌شود.

D:\>ipconfig
Windows 2000 IP Configuration
PPP adapter 20 saate alborz roozane
Connection-specific DNS Suffix
IP Address. . . . . : 217.218.120.144
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 217.218.120.144

براي بدست آوردن IP يك سايت روشهاي زيادي وجود دارد. يكي از اين روشها استفاده از دستور ping مي‌باشد. Ping دستوري است كه مشخص مي‌كند آيا كامپيوتري كه ما IP يا domain آن را مي‌دانيم روشن و فعال است يا نه. اين دستور با ارسال چهار بسته به مقصد مورد نظر و گرفتن پاسخ آنها اطلاعاتي را در اين رفت و برگشت بسته‌ها از اين ارتباط به برخي مي‌برد. اگر چه دستور ping براي بدست آوردن IP سايت نيست ولي مي‌توان از اين روش به صورت زير IP سايت را پيدا كرد.

Ping www. نام سايت .com

- اين روش در بعضي از موارد "مثلاً سايتهاي بزرگي مانند yahoo" شايد بهترين روش نباشد ولي با كمي دقت مي‌توان به نتيجه درست رسيد.

D:\>ping www.yahoo.com
Pinging www.yahoo.akadns.net [68.142.197.79] with 32 bytes of data:
Reply from 68.142.197.79: bytes=32 time=1022ms TTL=47
Request timed out.
Request timed out.
Reply from 68.142.197.79: bytes=32 time=1382ms TTL=47
Ping statistics for 68.142.197.79:
Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
Minimum = 1022ms, Maximum = 1382ms, Average = 601ms

با استفاده از دستور Tracert شما مي‌توانيد تمامي كامپيوترهايي را كه بسته‌هاي اطلاعاتي رد و بدل شده بين كامپيوتر شما و "IP" ديگر را مشاهده كنيد. مثلاً اگر شما دستور زير را در خط فرمان بنويسيد. خروجي حاصل تمامي كامپيوترها و يا گره‌هايي كه بسته شما براي رسيدن به مقصد بايد از آنها عبور كند مي‌توانيد بيابيد.

Tracert www. Yahoo. Com

براى اينكه عملكرد يک پورت براى شما روشن شود، بايد به آن پورت Telnet كنيد. (البته معمولا تعدادى از پورت‌هايى را كه ممكن است اطلاعاتى مهم را در اختيار هكرها قرار دهند مثل پورت ۷۹ معمولا بسته است و ارتباط با آنها شايد برقرار نشود.) براى telnet كردن در command prompt دستور زير را تايپ كنيد:

portnum hostname **telnet**
در این دستور به‌جای hostname شماره ip و یا نام سایت را وارد می‌کنید و به‌جای portnum شماره پورت و یا معادل آن از جدول. مثلا برای تلنت کردن به پورت ۱۳ که ساعت و تاریخ را به‌دست می‌دهد

telnet 194.225.184.13 13

البته در آن دستورات به جای عدد ۱۳ می‌توان معادلش را نوشت که daytime است.
پورت 13 کارش اینه که زمان و تاریخ رو در اون کامپیوتر به ما می‌ده. فقط کافیه که بهش وصل بشویم تا اطلاعات بیرون بریزه. البته این پورت رو خیلی از کامپیوترها بسته است. (یادتون باشه که وقتی می‌توان با یه پورت کار کرد که باز باشد).!!!

نكاتي لازم در مورد پروتكل TCP))) ...
در پروتكل TCP قبل از آنكه داده‌ها به مقصد ارسال شوند يك ارتباط بايد بين منبع و مقصد برقرار شود. TCP به هر بسته يك شماره سريال اختصاص مي‌دهد. در مقصد اين شماره سريال براي كليه بسته‌ها مورد بررسي قرار مي‌گيرد تا از دريافت صحيح كليه آنها اطمينان حاصل شود. هنگامي كه در طرف گيرنده يك بسته دريافت مي‌شود با اعلام شماره سريال بسته بعدي به منبع دريافت صحيح بسته اعلام مي‌شود. اگر منبع پاسخ را در مدت زمان معيني دريافت نكند بسته قبلي را مجدداً ارسال خواهد كرد.
تذكر: هكر بايد با پروتكل TCP آشنايي كامل داشته باشد و از فيلدهاي هر بسته از قبيل Fin, Syn, Ack, Rst, Psh و Urg وظيفه هر يك از آنها اطلاعات لازم را داشته باشد. در اينجا به دليل اينكه بحث ما در مورد راه‌هاي نفوذ به شبكه مي‌باشد. فرض بر اين است كه شما با پروتكل TCP آشنايي كافي داريد.