نفوذ به شبکه های کامپیوتری

مؤلف : دکتر حشمدار

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 ضعف‌هاي شبكه و برطرف كردن آنهاست به همين دليل در اواخر دهه 80 هكرها را بر اساس فعاليتهايشان دسته‌بندي كردند.

I.) گروه نفوذگران کلاه سفید (White Hacker Group)

II.) گروه نفوذگران کلاه سیاه (Black Hacker Grpoup)

III.) گروه نفوذگران کلاه خاکستري (Gray Hat Haker Group)

IV.) گروه نفوذگران کلاه صورتي (Pink Hat Haker Group)

I. این گروه در واقع دانشجويان و اساتيدي هستند که هدفشان نشان دادن ضعف سيستمهاي امنيتي شبکه‌هاي کامپيوتري مي‌باشد. اين گروه به هکرهاي خوب معروفند که در تحکيم ديواره حفاظتي شبکه‌هاي نقش اساسي دارند. اين گروه خلاقيت عجيبي دارند و معمولاً هر بار با روشهاي نو و جديدي از ديواره‌هاي امنيتي عبور مي‌کنند.

II. اين گروه خراب‌کارانه‌ترين نوع هکرها هستند و به Crackerها معروف هستند. کلاه سياه‌ها اغلب ويروس نويسند و با ارسال ويروس نوشته شده خود بر روي سيستم قرباني به آن نفوذ مي‌کنند. 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 هکرها

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 اوردن 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" شـايد بهتـرين روش نباشد ولي با كمي دقت مي‌توان به نتيجه درسـت رسـيد.

```
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

برای اینکه عملکرد یک پورت برای شما روشن شود، باید به آن پورت Telnet کنید. (البته معمولا تعدادی از پورت‌هایی را که ممکن است اطلاعاتی مهم را در اختیار هکرها قرار دهند مثل پورت ۷۹ معمولا بسته است و ارتباط با آنها شاید برقرار نشود.) برای telnet کردن در command prompt دستور زیر را تایپ کنید:

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

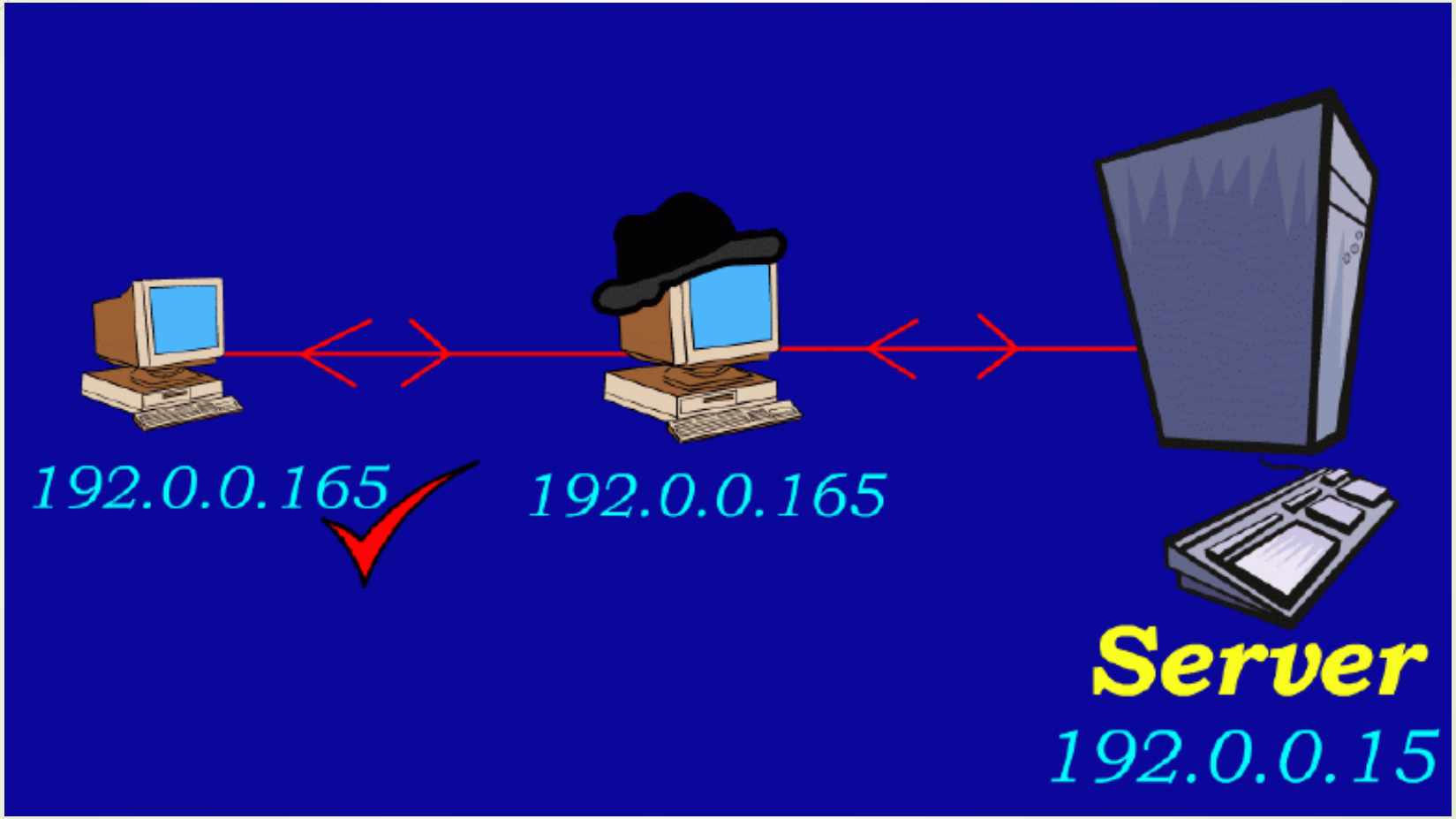
البته در آن دستورات به جای عدد ۱۳ می‌توان معادلش را نوشت که daytime است.
پورت 13 کارش اینه که زمان و تاریخ رو در اون کامپیوتر به ما می‌ده. فقط کافیه که بهش وصل بشویم تا اطلاعات بیرون بریزه. البته این پورت رو خیلی از کامپیوترها بسته است.
(یادتون باشه که وقتی می‌توان با یه پورت کار کرد که باز باشد).!!!

نكاتي لازم در مورد پروتكل TCP))) ...

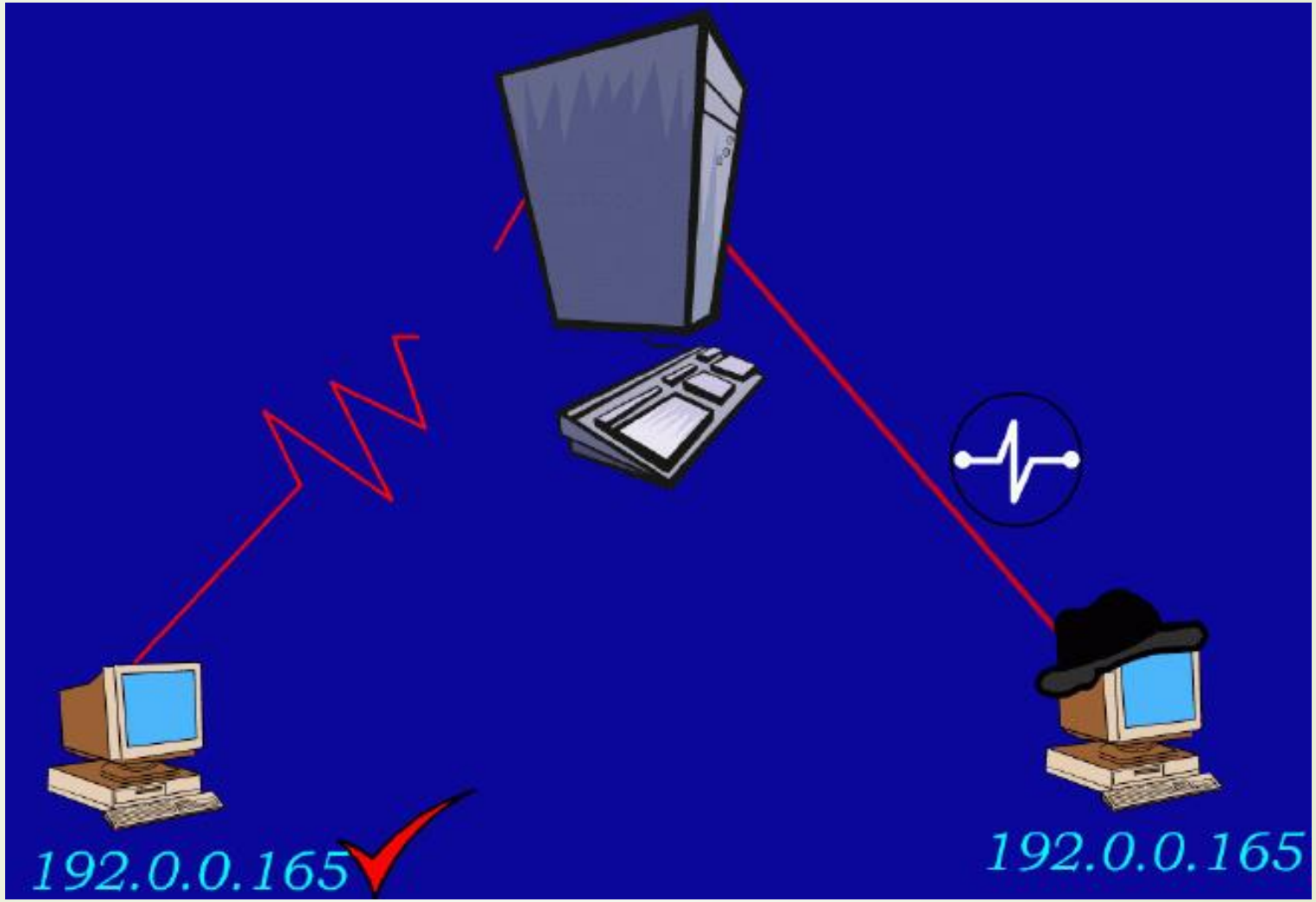
در پروتكل TCP قبل از آنكه داده‌ها به مقصد ارسال شوند يك ارتباط بايد بين منبع و مقصد برقرار شود. TCP به هر بسته يك شماره سريال اختصاص مي‌دهد. در مقصد اين شماره سريال براي كليه بسته‌ها مورد بررسي قرار مي‌گيرد تا از دريافت صحيح كليه آنها اطمينان حاصل شود. هنگامي كه در طرف گيرنده يك بسته دريافت مي‌شود با 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.

- ***حمله از طريق IP***: در اين روش ابتدا هكر به روشهاي مختلف IP سرويس دهنده (ايگاه وب، ISP و ..) را بدست مي‌آورد. اين كار با پيدا كردن نقشه شبكه راحت‌تر است سپس هكر خود را در بين سرويس‌دهنده و كاربر قرار مي‌دهد و با ارسال بسته‌هاي تقلبي اطلاعات را به سرقت مي‌برد. در اين روش در واقع هكر خود را براي سرويس دهنده، گيرنده و براي كاربر سرويس دهنده معرفي مي‌كند و به عنوان واسط بين كاربر و Server قادر است بسته‌هاي خود را با شماره‌هاي صحيح انتقال دهد.


192.0.0.165
192.0.0.165
Server
192.0.0.15

- ***حمله به TCP:*** اين حمله از متداولترين نوع حمله به سرويس دهنده‌ها در اينترنت مي‌باشد. هكر در اين روش ارتباط كاربر را از سرويس دهنده قطع مي‌كند و IP خود را به جاي كاربر به سرويس دهنده معرفي مي‌كند و از اين پس هر گونه تبادل اطلاعات بين سرويس دهنده و هكر صورت مي‌گيرد. مزيت اين روش به روش حمله به IP اين است كه در اين روش هكر تنها يك بار حمله مي‌كند و از مقابله با سيستمهاي امنيتي رمز عبور در مراحل بعد فرار مي‌كند. "برخلاف حمله به IP"


192.0.0.165
192.0.0.165

- ***حملات جاسوسي***: در نمونه‌اي از اين روش هكر در ارتباط TCP ناهماهنگي ايجاد مي‌كند. شماره سريال بسته‌هايي كه براي سرويس دهنده ارسال مي‌شوند. در بين راه توسط هكر با سريال بسته‌هاي بعدي تعويض مي‌شود و در اين حالت كه شماره سريال با سريال بسته كاربر متفاوت است، سرويس دهنده آن بسته را به كاربر مرجوع كرده و هكر كه منتظر چنين عملي است بسته را براي خود نسخه‌برداري مي‌كند.

پس از اين كار هكر براي بار ديگر بسته مورد نظر خود را مي‌فرستد. ولي اين بار با شماره سريال صحيح و چون شماره سريال تصحيح شده سرويس دهنده آنها را قبول مي‌كند و بدين صورت بدون اينكه كاربر و سرويس دهنده بفهمند اطلاعات توسط هكر كم و زياد مي‌گردد.

استفاده از برنامه Telnet ويندوز يكي از راه‌هاي حملات جاسوسي مي‌باشد. با اجراي اين برنامه از منوي Run ويندوز و پس از گفتن نام ميزبان راه دور يا IP آن و برقراري اتصال با ميزبان سيستم به عنوان بخشي از سرويس شروع به نمايش اطلاعات مي‌كند!

- **جعل اطلاعات :**

- جعل IP
- جعل Email
- جعل يك وب

جعل IP : در سرويسهاي UDP و TCP به آدرس ميزبان اطمينان داريد، هكر مي‌تواند با مسيريابي خود را به عنوان ميزبان و يا كاربر معتبر معرفي كند. هكر آدرس سرويس دهنده را مطابق با آدرس كاربر جعل و سپس براي كاربر يك آدرس جديد مي‌سازد و به اين صورت هكر ارتباط كاربر را با سرويس دهنده قطع و ارتباط خود را با همان آدرس جعل شده كاربر با سرويس دهنده برقرار مي‌كند. در بسياري از موارد نيز ممكن است هكر منتظر بماند تا كاربر كامپيوتر خود را خاموش كند سپس يك ارتباط با ميزبان برقرار مي‌كند و خود را به عنوان كاربر معرفي مي‌كند.

جعل Email : جعل Email در اينترنت بسيار اسان مي‌باشد و غالباً نمي‌توان به Email هاي فاقد سيستمهاي امنيتي اطمينان 100 % پيدا كرد. با استفاده از TelNet مي‌توان به پورت SMTP متصل شد. همچنين فرستادن Email جعلي از طرف يك كاربر با IP مشخص توسط هكر به راحتي امكان پذير است. كافيست هكر اطلاعاتي در زمينه برنامه‌نويسي و فرستادن Email داشته باشد و با پروتكل‌هاي SMTP آشنايي داشته باشد.

جعل وب : يكي ديگر از شيوه‌هاي حمله هكرها جعل يك صفحه وب مي‌باشد. در اين روش يك نسخه از وب سايت نسخه‌برداري مي‌گردد و هكر نسخه ذخيره شده را تغيير مي‌دهد ولي تمامي ظواهر وب بدون تغيير باقي مي‌ماند. هكر صفحه جعل شده را Upload مي‌كند و به طريقي توجه كاربر را براي ورود به آن صفحه جلب مي‌كند. كاربر با كليك روي لينك فرستاده شده هكر به صفحه جعل شده هدايت مي‌شود و چون شكل ظاهري صفحه درست مي‌باشد احتمال استفاده كاربر از آن صفحه وجود دارد. كه در اين صورت هكر به هدف خود مي‌رسد. اين شيوه بيشتر در امور تجاري نقش دارد. مثلاً در بسياري از خريدهاي اينترنتي از خريدار خواسته مي‌شود تا كد كارت اعتباري خود را وارد كند. حال اگر اين سايت جعلي باشد كد كارت اعتباري شما به هكر فرستاده مي‌شود.

هك كردن از طريق جعل وب از روشهاي هك از طريق مهندسي اجتماعي محسوب مي‌شود.

- ***Applet*ها** : علاوه بر خدماتي كه Applet هاي جاوا در طراحي صفحاتن وب انجام مي‌دهند. اين كدها مي‌توانند خطرناك باشند. زيرا Applet ها مستقيماً توسط مرورگر به حافظه بارگذاري مي‌گردند يعني با ورود به يك صفحه وب مرورگر به طور اتوماتيك كدهاي جاوا را اجرا مي‌كند. هكر مي‌تواند كدهاي مخربي بنويسد و برنامه جاسوس خود را بر روي كامپيوتر كاربر نصب كند و يا اطلاعات مورد نياز را بدست بياورد ... . اين نوع حمله از متداولترين و مخرب‌ترين نوع حملات هكرها محسوب مي‌شود.
- ***Cookie*ها** : كوكي‌ها فايلهاي كوچكي هستند كه صفحات پوياي وب مي‌تواند روي كامپيوتر كاربر ايجاد كند. حداكثر طول اين فايلها 4 كيلوبايت مي‌باشد. بسياري از صفحات وب اطلاعات پر شده فرمهاي سايت توسط كاربر و يا اطلاعات مورد نياز خود را براي ورودهاي بعدي به صفحه توسط كاربر در فايلهايي به نام Cookie در كامپيوتر كاربر ذخيره مي‌كنند. اين كار با اجازه خود كاربر و يا در مواردي بدون نظرخواهي كاربر روي كامپيوتر او ذخيره مي‌گردد. هكر مي‌تواند از اطلاعات داخل اين كوكيها نهايت استفاده را ببرد و با دزديدن اين اطلاعات زمينه نفوذ را فراهم كند.

- ***حمله به کلمات عبور*** : در اين روش هكر با پيدا كردن كلمات عبور شامل رمز عبور اطلاعات محرمانه، تجاري، امنيتي و حتي كلمه عبور Email افراد كنترل تمامي قسمتهاي مورد نياز را به دست مي‌گيرد.

شكستن كلمات عبور به دو صورت انجام مي‌شود:

1- توليد كليه رمزهاي محتمل و امتحان كردن آنها در اين روش از نرم‌افزارهايي استفاده مي‌شود كه قادرند در هر ثانيه چندين كلمه عبور را جستجو كنند و با پيدا كردن تمامي تركيبات حروف و تست كردن اتوماتيك آنها رمز عبور شكسته مي‌شود.

بهترين حالت براي هكر اين است كه رمز عبور از كلمات با معني باشد كه در اين صورت نرم‌افزار هكر به جاي توليد تمامي تركيبات حروف از DataBase ديكشنري‌ها يا DB اسامي و ... براي پيدا كردن رمز عبور استفاده مي‌كند. اتفاقاً افراد در بسياري از موارد كلمات عبور خود را ساده و طوري انتخاب مي‌كنند تا فراموش نشود.

2- در روش ديگري از پيدا كردن رمز عبور هكر از ديكد كردن رمز كد شده استفاده مي‌كند. در هر سيستم معمولاً كلمات عبور به صورت رمز شده در فايلي روي كامپيوتر كاربر يا شبكه ذخيره مي‌شوند هكر با دزديدن اين فايل و يافتن الگوريتم رمز گشايي آن كلمه عبور را پيدا مي‌كند. در اين موارد اگر رمز گذاري فايل از روشهاي معمول و شناخته شده نباشد ديكد كردن رمز براي هكر بسيار مشكل است. مثلاً تمامي پسوردها و كليه Account number ها در ويندوز NT درون فايلي با نام SAM در ويندوز نگهداري مي‌شود كه علاوه بر اينكه از رمز گذاري قوي و پيچيده نظير (MD4) استفاده شده ولي باز هم شكست پذير است.

در روش Hash كه براي رمزهاي ويندوز NT صورت مي‌گيرد كلمه عبور به صورت 14 كاراكتر تنظيم مي‌شود و سپس روي آن روش MD4 سه بار اعمال مي‌شود تا كلمه عبور به رمز در آيد. اين روش با تمام قدرتي كه دارد باز هم با تركيبي از روش (1) و استفاده از MD4 قابل شكستن است.

در مورد فايل SAM ويندوز NT ... هكر نمي‌تواند به راحتي آن را در حال اجراي سيستم عامل بدست آورد زيرا اين فايل كاملاً توسط هسته ويندوز محافظت مي‌شود و حتي خود كاربر نمي‌تواند مستقيماً اين فايل را دستكاري كند و يا آن را پاك كند يا از آن نسخه‌برداي كند!

- ***حمله به برنامه‌هاي كاربردي:*** در اين روش هكر مستقيماً به برنامه‌هاي كاربردي تحت وب حمله مي‌كند. هكر در اين روش معمولاً User ID و Password عبور را بدست مي‌آورد.

به اين ترتيب كه وقتي يك برنامه كاربردي مانند Internet explorer درخواست يك كلمه عبور مي‌شود. اگر كاربر نام عبور را اشتباه وارد كند. در خط آدرس دستور نوع نادرستي نام عبور گزارش داده مي‌شود و در واقع در اين روش يك بيت صحت و يا نادرستي كلمه عبور مشخص مي‌شود. هكر به اين وسيله مرحله به مرحله نام عبور را پيدا مي‌كند و سپس با يك جستجوگر رمز عبور آن نام را پيدا مي‌كند.

كلاً هكرها در بسياري از موارد از ضعف‌هاي برنامه‌هاي تحت وب آگاهي پيدا مي‌كنند و از اين ضعفها براي نفوذ استفاده مي‌كنند. اين ضعف‌ها گاهي در نسخه‌هاي بعدي اين نرم‌افزارهاي كاربردي رفع مي‌شوند و گاهي امكان رفع آن براي شركت سازنده نيست و اين موضوع به نفع هكر تمام مي‌شود.

- ***Sniffing*** : در این روشها هکر قادر است اقدام به استراق سمع داده‌ها در شبکه کند 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* :

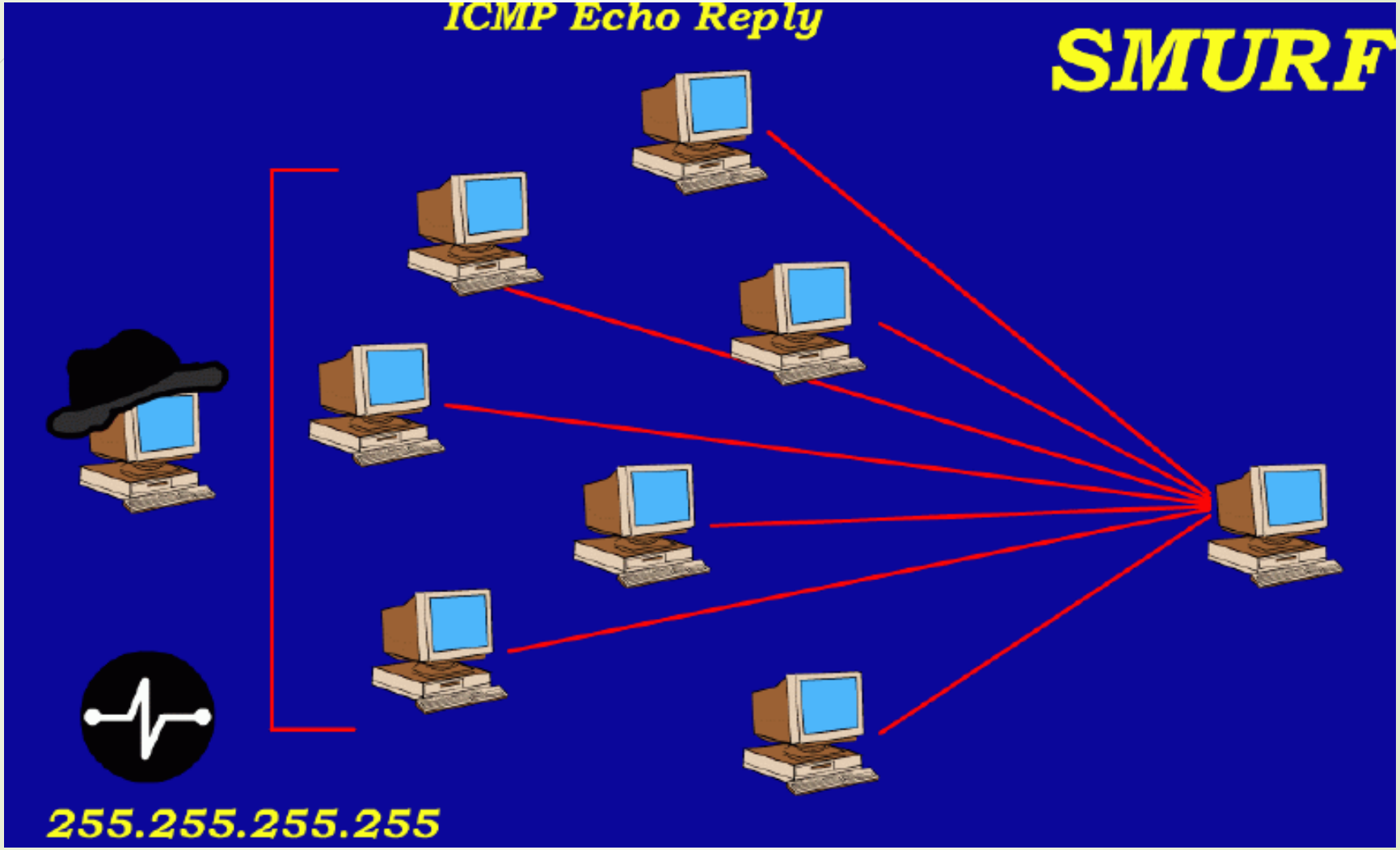
در ايـن نـوع حملـه يـك بـسته ping بـا انـدازه بـيش از 64 k بـراي پروسـه ICMP ارسـال مي‌گردد با دريافت چنين بسته‌اي به دليل اينكه TCP براي چنين حالتي طراحي نگرديـده مختل مي‌گردد.

حمله نوع *Jolt 2* :

در اين نوع حمله يك جريان طولاني و وسيع از بسته‌هـاي قطعـه قطعـه شـده بـه سـمت ماشـين هدف در شبكه هدايت مي‌شوند. از اين رو پروسـه TCP بايـد ايـن قطعـه‌هـا را در خود نگهداري كند و چون تحت بمباران قرار گرفته در هم مي‌شكند و ارتباط آن ماشين بـا شبكه قطع مي‌گردد. طبق گزارشها تمامي سيستمهاي عامل ويندوز از اين مشكل رنـج 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.


ICMP Echo Reply
SMURF
255.255.255.255

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 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.

If you have any question, don't heisted to contact me
Email: Dr.Hashamdar @ Gmail.com WWW.Hashamdar.com
Programmer analyst (Cyber Security & Digital)