

راه‌های نفوذ به شبکه‌های کامپیوتری

یکی از مهمترین مشغله‌های کارشناسان شبکه امنیت شبکه و مقابله با نفوذگران می‌باشد. بنابراین کشف راه‌های نفوذ به شبکه باید همواره مورد توجه مسئولان شبکه‌های کامپیوتری قرار بگیرد.

یک مسئول شبکه و حتی یک کاربر ساده باید با راه‌های نفوذ به شبکه آشنا باشد تا با بستن و کنترل این راه‌ها شبکه یا سیستم موردنظر را از حملات هکرها محفوظ بدارد. در ذهنیت عمومی هکر یک انسان شرور و خرابکار است ولی در واقع اینگونه نیست و هکرها در بسیاری از موارد هدفشان پیدا کردن ضعف‌های شبکه و برطرف کردن آنهاست به همین دلیل در اواخر دهه 80 هکرها را بر اساس فعالیت‌هایشان دسته‌بندی کردند.

- I. (White Hacker Group) گروه نفوذگران کلاه سفید
- II. (Black Hacker Group) گروه نفوذگران کلاه سیاه
- III. (Gray Hat Hacker Group) گروه نفوذگران کلاه خاکستری
- IV. (Pink Hat Hacker Group) گروه نفوذگران کلاه صورتی

I. این گروه در واقع دانشجویان و اساتیدی هستند که هدفشان نشان دادن ضعف سیستم‌های امنیتی شبکه‌های کامپیوتری می‌باشد. این گروه به هکرها خوب معروفند که در تحکیم دیواره حفاظتی شبکه‌های نقش اساسی دارند. این گروه خلاقیت عجیبی دارند و معمولاً هر بار با روش‌های نو و جدیدی از دیواره‌های امنیتی عبور می‌کنند.

II. این گروه خراب‌کارانه‌ترین نوع هکرها هستند و به Crackerها معروف هستند. کلاه سیاه‌ها اغلب ویروس نویسنده و با ارسال ویروس نوشته شده خود بر روی سیستم قربانی به آن نفوذ می‌کنند. این گروه همیشه سعی در پنهان نمودن هویت خود را دارند.

III. نام دیگر این گروه واکرها است "whacker". هدف اصلی واکرها استفاده از اطلاعات سایر کامپیوترها به مقاصد مختلف می‌باشد. در صورتی که با نفوذ به شبکه صدمه‌ای به کامپیوترها وارد نمی‌کنند. مثلاً در سال 1994 یک هکر "کلاه خاکستری" ژاپنی به سایت ناسا Nasa آمریکا نفوذ پیدا کرد و تمامی اسناد محرمانه متعلق به این سازمان را ربود و به طور رایگان بر روی اینترنت در اختیار عموم قرار داد.

IV. این گروه افراد بی‌سوادی هستند که فقط قادرند به وسیله نرم‌افزارهای دیگران در سیستم‌ها اختلال به وجود بیاورند و مزاحمت ایجاد کنند. به این افراد Booter گفته

می‌شود. بوترها خود سواد برنامه‌نویسی ندارند ولی در بعضی از موارد همین نوع هکرها می‌توانند خطرهای جدی برای شبکه به وجود آورند.

انواع حملات هکرها ...

حمله از نوع دستکاری اطلاعات "Modification"

به این معنی که هکر در حین انتقال اطلاعات به مقصد آنها را مطابق خواسته خود تغییر داده و به کاربر می‌فرستد و کاربر بدون اطلاع از تغییر آنها را مورد استفاده قرار می‌دهد.

حمله از نوع افزودن اطلاعات "Farication"

در این نوع از حمله هکر به جای تغییر دادن اطلاعات، اطلاعات جدیدی را به آن می‌افزاید مانند یک ویروس جهت اقدامات بعدی.

حمله از نوع استراق سمع "Interception"

در این نوع حمله هکر فقط به اطلاعات در حین تبادل گوش می‌دهد و در صورت لزوم از آن نسخه‌برداری می‌کند.

حمله از نوع وقفه "Interruption"

در این نوع حمله هکر با ایجاد اختلال در شبکه و وقفه در انتقال اطلاعات برای خود فرصت لازم جهت اقدامات بعدی را فراهم می‌آورد.

موارد مورد نیاز هکرها ...

اطلاعاتی هر چند بی‌اهمیت از دید شما می‌تواند برای هکر بسیار مهم باشد اما برای نفوذ به هر گونه شبکه کامپیوتری تحت TCP/IP داشتن IP قربانی مورد نیاز است. شما هر گاه به اینترنت متصل می‌شوید دارای یک IP منحصر به فرد جدید می‌باشید که این IP در حقیقت آدرس کامپیوتر شما در شبکه می‌باشد.

دومین مورد که برای نفوذ به کامپیوتر قربانی لازم می‌باشد داشتن حداقل یک پورت باز می‌باشد. اگر کامپیوتر قربانی را در شبکه به یک خانه در شهر تشبیه کنیم IP آدرس این خانه و پورت‌ها راههای ورودی این خانه از قبیل در، پنجره، دیوار و ... می‌باشند. بدیهی است که بدون در اختیار داشتن آدرس منزل و پیدا کردن یکی از ورودی‌های خانه که مسدود نمی‌باشد ورود به آن خانه تقریباً غیرممکن است.

نشانی IP از چهار عدد از صفر تا 255 تشکیل شده که با نقطه از هم جدا می‌شوند. برای پیدا کردن محل یک کامپیوتر در شبکه از روی IP به صورت زیر عمل می‌شود.

آدرس ماشین. آدرس زیر شبکه. آدرس شبکه

هکر با استفاده از روشها و ابزارهایی که در ادامه به آن اشاره خواهد شد قادر است نقشه شبکه را بدست آورد و این برای هکر یک موفقیت بزرگ محسوب می‌شود. شماره پورت همراه اطلاعات در بسته‌های ICP فرستاده می‌شود و مشخص می‌کند که بسته از چه برنامه کاربردی در لایه بالاتر تولید و به چه برنامه‌ای ارسال گردد و در

ماشین مقصد به آن تحویل داده شود. برخی از برنامه‌های کاربردی استاندارد و جهانی دارای شماره پورت استاندارد و مشخص می‌باشند. به عنوان مثال سرویس‌دهنده پست الکترونیک SMTP از شماره پورت 25 استفاده می‌کند و یا پورت استاندارد برنامه TelNet 23 می‌باشد. با دانستن پورت استاندارد نرم‌افزارها و بستن آن پورت در کامپیوتر می‌توان از تبادل اطلاعات آن برنامه با کامپیوترها جلوگیری کرد.

با استفاده از برنامه Netstat موجود در ویندوز می‌توانید کامپیوترها و پورت‌هایی را که کامپیوتر شما با آنها در حال تبادل اطلاعات می‌باشد، شناسایی کنید.

برای اجرای این نرم‌افزار در Ms – Dos Prompt ویندوز عبارت Netstat را تایپ کنید و کلید Enter را فشار دهید. در این هنگام لیستی از اتصال‌های اینترنتی که در حال حاضر مشغول کار هستند قابل مشاهده می‌باشد.

اگر روی خط فرمان عبارت Netstat – na را تایپ کنید. تمام پورت‌هایی که در حال تبادل اطلاعات هستند گزارش داده می‌شود.

از Netstat می‌توان برای شناسایی شبکه و نیز کشف حملات هکرها نیز استفاده کرد. نمونه خروجی دستور Netstat را مشاهده کنید :

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 برای کامپیوترهایی که نقش سرور را دارند. "مانند سایت‌ها و یا کامپیوترهایی که غیر از Dial up به اینترنت متصل می‌شوند عددی ثابت تعریف می‌شود ولی برای افراد "Client" های معمولی در هر بار اتصال به اینترنت IP تغییر می‌کند.

برای بدست آوردن IP خود در شبکه می‌توانید از دستور Ipconfig در خط فرمان ویندوز استفاده کنید. در این صورت IP شما در شبکه به عنوان خروجی دستور نمایش داده می‌شود.

```
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
```

برای بدست آوردن IP يك سايت روشهاي زيادي وجود دارد. يكي از اين روشها استفاده از دستور ping مي باشد. Ping دستوري است كه مشخص مي كند آيا كامپيوتري كه ما IP يا domain آن را مي دانيم 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 بسته ها از اين ارتباط به برخي مي برد. اگر چه دستور ping براي بدست آوردن IP سايت نيست ولي مي توان از اين روش به صورت زير IP سايت را پيدا كرد.

Ping www.com. نام سايت

- اين روش در بعضي از موارد "مثلاً سايتهاي بزرگي مانند yahoo" شايد بهترين روش نباشد ولي با كمی دقت مي توان 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 مي توانيد تمامي كامپيوترهاي را كه بسته هاي 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 گره هاي كه بسته شما براي رسيدن به مقصد بايد از آنها عبور كند مي توانيد بياييد.

Tracert www.Yahoo. Com

برای اينكه عملکرد يك پورت براي شما روشن شود، بايد به آن پورت Telnet كنيد. (البته معمولاً تعدادی از پورتهای را كه ممكن است اطلاعاتی مهم را در اختيار هكرها قرار دهند مثل پورت ۷۹ معمولاً بسته است و ارتباط با آنها شايد برقرار نشود.) برای telnet كردن در command prompt دستور زير را تايپ كنيد:

`portnum hostname telnet`

در این دستور به جای hostname شماره ip و یا نام سایت را وارد می‌کنید و به جای portnum شماره پورت و یا معادل آن از جدول. مثلاً برای تلنت کردن به پورت ۱۳ که ساعت و تاریخ را به دست 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)!!!

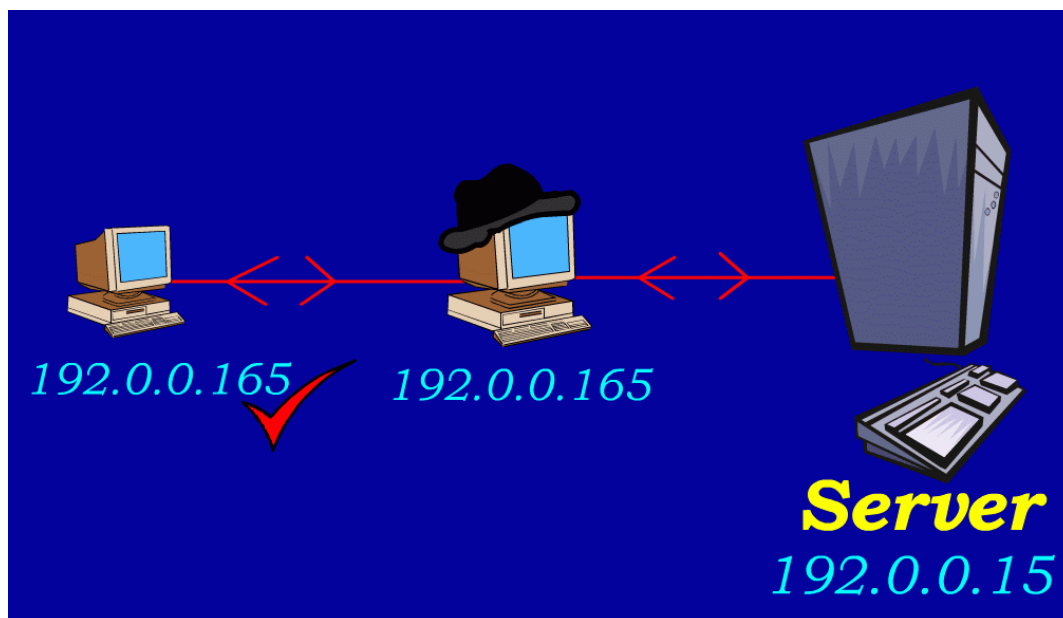
نکاتی لازم در مورد پروتکل TCP (((...

در پروتکل TCP قبل از آنکه داده‌ها به مقصد ارسال شوند یک ارتباط باید بین منبع و مقصد برقرار شود. TCP به هر بسته یک شماره سریال اختصاص می‌دهد. در مقصد این شماره سریال برای کلیه بسته‌ها مورد بررسی قرار می‌گیرد تا از دریافت صحیح کلیه آنها اطمینان حاصل شود. هنگامی که در طرف گیرنده یک بسته دریافت می‌شود با اعلام شماره سریال بسته بعدی به منبع دریافت صحیح بسته اعلام می‌شود. اگر منبع پاسخ را در مدت زمان معینی دریافت نکند بسته قبلی را مجدداً ارسال خواهد کرد.

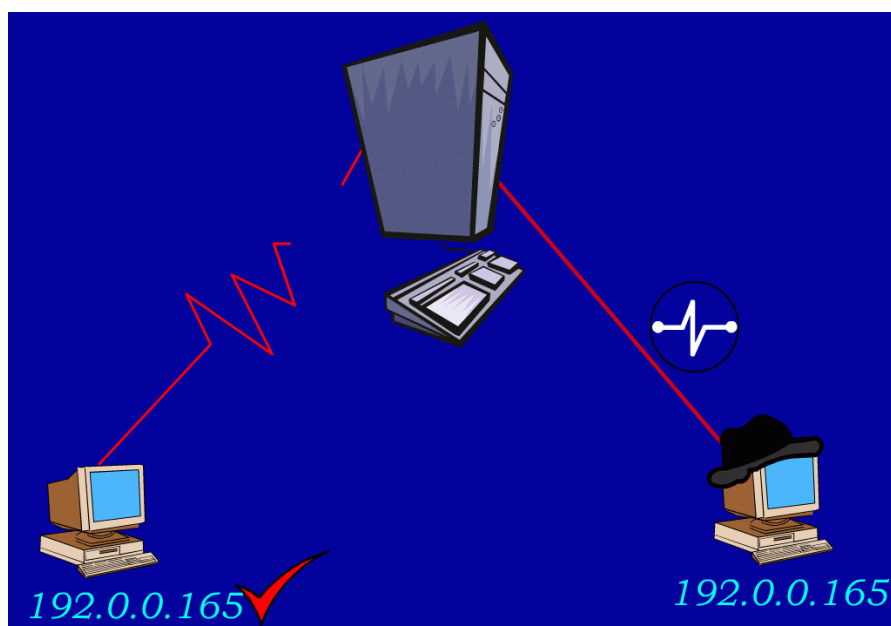
تذکر: هکر باید با پروتکل TCP آشنایی کامل داشته باشد و از فیلدهای هر بسته از قبیل Psh, Rst, Ack, Syn, Fin و Urg وظیفه هر یک از آنها اطلاعات لازم را داشته باشد. در اینجا به دلیل اینکه بحث ما در مورد راه‌های نفوذ به شبکه می‌باشد. فرض بر این است که شما با پروتکل TCP آشنایی کافی دارید.

راه‌های نفوذ

- **حمله از طریق IP:** در این روش ابتدا هکر به روش‌های مختلف IP سرویس دهنده (ایگاه وب، ISP و ..) را بدست می‌آورد. این کار با پیدا کردن نقشه شبکه راحت‌تر است سپس هکر خود را در بین سرویس‌دهنده و کاربر قرار می‌دهد و با ارسال بسته‌های تقلبی اطلاعات را به سرقت می‌برد. در این روش در واقع هکر خود را برای سرویس دهنده، گیرنده و برای کاربر سرویس دهنده معرفی می‌کند و به عنوان واسطه بین کاربر و Server قادر است بسته‌های خود را با شماره‌های صحیح انتقال دهد.



- **حمله به TCP:** این حمله از متداولترین نوع حمله به سرویس دهنده‌ها در اینترنت می‌باشد. هکر در این روش ارتباط کاربر را از سرویس دهنده قطع می‌کند و IP خود را به جای کاربر به سرویس دهنده معرفی می‌کند و از این پس هر گونه تبادل اطلاعات بین سرویس دهنده و هکر صورت می‌گیرد. مزیت این روش به روش حمله به IP این است که در این روش هکر تنها یک بار حمله می‌کند و از مقابله با سیستم‌های امنیتی رمز عبور در مراحل بعد فرار می‌کند. "برخلاف حمله به IP"



• **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 کاربر متفاوت است، سرويس دهنده آن بسته را به کاربر 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 صحيح شده سرويس دهنده آنها را قبول مي‌كند و بدین صورت بدون اينكه کاربر 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 اطمینان داريد، هكر مي‌تواند با مسيريابي خود را به عنوان ميزبان و يا کاربر معتبر معرفي كند. هكر آدرس سرويس دهنده را مطابق با آدرس کاربر جعل و سپس براي کاربر يك آدرس جديد مي‌سازد و به اين صورت هكر ارتباط کاربر را با سرويس دهنده قطع و ارتباط خود را با همان آدرس جعل شده کاربر با سرويس دهنده برقرار مي‌كند. در بسياري از موارد نيز ممكن است هكر منتظر بماند تا کاربر كامپيوتر خود را خاموش كند سپس يك ارتباط با ميزبان برقرار مي‌كند و خود را به عنوان کاربر معرفي مي‌كند.

جعل Email : جعل Email در اينترنت بسيار آسان مي‌باشد و غالباً نمي‌توان به Email هاي فاقد سيستمهاي امنيتي اطمینان 100 % پيدا كرد. با استفاده از TelNet مي‌توان به پورت SMTP متصل شد. همچنين فرستادن Email جعلي از طرف يك کاربر با IP مشخص توسط هكر به راحتی امكان پذير است. كافيست هكر اطلاعاتي در زمينه برنامه‌نويسي و فرستادن Email داشته باشد و با پروتكل‌هاي SMTP آشنائي 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 کاربر را براي ورود به آن صفحه جلب مي‌كند. کاربر با كليك روي لينك فرستاده شده هكر به صفحه جعل شده هدايت مي‌شود و چون شكل ظاهري صفحه درست مي‌باشد احتمال استفاده کاربر از آن صفحه وجود دارد. كه در اين

صورت هکر به هدف خود می‌رسد. این شیوه بیشتر در امور تجاری نقش دارد. مثلاً در بسیاری از خریدهای اینترنتی از خریدار خواسته می‌شود تا کد کارت اعتباری خود را وارد کند. حال اگر این سایت جعلی باشد کد کارت اعتباری شما به هکر فرستاده می‌شود. هک کردن از طریق جعل وب از روشهای هک از طریق مهندسی اجتماعی محسوب می‌شود.

- **Applet ها :** علاوه بر خدماتی که Applet های جاوا در طراحی صفحات وب انجام می‌دهند. این کدها می‌توانند خطرناک باشند. زیرا Applet ها مستقیماً توسط مرورگر به حافظه بارگذاری می‌گردند یعنی با ورود به یک صفحه وب مرورگر به طور اتوماتیک کدهای جاوا را اجرا می‌کند. هکر می‌تواند کدهای مخربی بنویسد و برنامه جاسوس خود را بر روی کامپیوتر کاربر نصب کند و یا اطلاعات مورد نیاز را بدست بیاورد ... این نوع حمله از متداولترین و مخربترین نوع حملات هکرها محسوب می‌شود.

- **Cookie ها :** کوکی‌ها فایل‌های کوچکی هستند که صفحات پویای وب می‌تواند روی کامپیوتر کاربر ایجاد کند. حداکثر طول این فایلها 4 کیلوبایت می‌باشد. بسیاری از صفحات وب اطلاعات پر شده فرمهای سایت توسط کاربر و یا اطلاعات مورد نیاز خود را برای ورودهای بعدی به صفحه توسط کاربر در فایل‌هایی به نام Cookie در کامپیوتر کاربر ذخیره می‌کنند. این کار با اجازه خود کاربر و یا در مواردی بدون نظرخواهی کاربر روی کامپیوتر او ذخیره می‌گردد. هکر می‌تواند از اطلاعات داخل این کوکیها نهایت استفاده را ببرد و با دزدیدن این اطلاعات زمینه نفوذ را فراهم کند.

- **حمله به کلمات عبور :** در این روش هکر با پیدا کردن کلمات عبور شامل رمز عبور اطلاعات محرمانه، تجاری، امنیتی و حتی کلمه عبور Email افراد کنترل تمامی قسمتهای مورد نیاز را به دست می‌گیرد.

شکستن کلمات عبور به دو صورت انجام می‌شود:

1- تولید کلیه رمزهای محتمل و امتحان کردن آنها در این روش از نرم‌افزارهایی استفاده می‌شود که قادرند در هر ثانیه چندین کلمه عبور را جستجو کنند و با پیدا کردن تمامی ترکیبات حروف و تست کردن اتوماتیک آنها رمز عبور شکسته می‌شود.

بهترین حالت برای هکر این است که رمز عبور از کلمات با معنی باشد که در این صورت نرم‌افزار هکر به جای تولید تمامی ترکیبات حروف از DataBase دیکشنری‌ها یا DB اسامی و ... برای پیدا کردن رمز عبور استفاده می‌کند. اتفاقاً افراد در بسیاری از موارد کلمات عبور خود را ساده و طوری انتخاب می‌کنند تا فراموش نشود.

2- در روش دیگری از پیدا کردن رمز عبور هکر از دیکد کردن رمز کد شده استفاده می‌کند. در هر سیستم معمولاً کلمات عبور به صورت رمز شده در فایل‌های کامپیوتر کاربر یا شبکه ذخیره می‌شوند هکر با دزدیدن این فایل و یافتن الگوریتم رمز گشایی آن کلمه عبور را پیدا می‌کند. در این موارد اگر رمز گذاری فایل از روشهای معمول و شناخته شده نباشد دیکد کردن رمز برای هکر بسیار مشکل است. مثلاً تمامی پسوردها و کلیه Account number ها در ویندوز NT درون فایل‌های با نام SAM در ویندوز نگهداری می‌شود که علاوه بر اینکه از رمز گذاری قوی و پیچیده نظیر (MD4) استفاده شده ولی باز هم شکست پذیر است.

در روش Hash که برای رمزهای ویندوز NT صورت می‌گیرد کلمه عبور به صورت 14 کاراکتر تنظیم می‌شود و سپس روی آن روش MD4 سه بار اعمال می‌شود تا کلمه عبور به رمز در آید. این روش با تمام قدرتی که دارد باز هم با ترکیبی از روش (1) و استفاده از MD4 قابل شکستن است.

در مورد فایل SAM ویندوز NT ... هکر نمی‌تواند به راحتی آن را در حال اجرای سیستم عامل بدست آورد زیرا این فایل کاملاً توسط هسته ویندوز محافظت می‌شود و حتی خود کاربر نمی‌تواند مستقیماً این فایل را دستکاری کند و یا آن را پاک کند یا از آن نسخه‌برداری کند!

● **حمله به برنامه‌های کاربردی:** در این روش هکر مستقیماً به برنامه‌های کاربردی تحت وب حمله می‌کند. هکر در این روش معمولاً User ID و Password عبور را بدست می‌آورد.

به این ترتیب که وقتی یک برنامه کاربردی مانند Internet explorer درخواست یک کلمه عبور می‌شود. اگر کاربر نام عبور را اشتباه وارد کند. در خط آدرس دستور نوع نادرستی نام عبور گزارش داده می‌شود و در واقع در این روش یک بیت صحت و یا نادرستی کلمه عبور مشخص می‌شود. هکر به این وسیله مرحله به مرحله نام عبور را پیدا می‌کند و سپس با یک جستجوگر رمز عبور آن نام را پیدا می‌کند.

کلاً هکرها در بسیاری از موارد از ضعف‌های برنامه‌های تحت وب آگاهی پیدا می‌کنند و از این ضعفها برای نفوذ استفاده می‌کنند. این ضعفها گاهی در نسخه‌های بعدی این نرم‌افزارهای کاربردی رفع می‌شوند و گاهی امکان رفع آن برای شرکت سازنده نیست و این موضوع به نفع هکر تمام می‌شود.

استراق سمع داده‌ها

● **Sniffing:** در این روشها هکر قادر است اقدام به استراق سمع داده‌ها در شبکه کند ولی در تغییر داده‌ها نقشی ندارد. این کار با نصب برنامه Sniffer هکر روی یکی از کامپیوترهای شبکه صورت می‌گیرد و بسته‌های روی کانال فیزیکی شبکه را به هکر می‌فرستد.

یک Sniffer در سه مرحله کار می‌کند:

- اول از همه سخت افزار شبکه را در حالت بی‌قید تنظیم می‌کند تا اطلاعات تمام آدرس‌ها و پورت‌ها برای این برنامه ارسال شود.
- سپس Sniffer از بین بسته‌های ارسال شده بسته‌های مورد نیاز هکر را جدا می‌کند.
- و در نهایت اطلاعات مورد نیاز هکر را برای او ارسال می‌کند.

● **حملات Dos:** این حمله با نام Denial of service به معنی اخلاف در سرویس دهی می‌باشد و تشابه اسمی آن با سیستم عامل Dos فقط یک تشابه اسمی است و هیچ ارتباطی با آن ندارد.

در این روش هکر در عمل سعی جلوگیری از سرویس دهی شبکه می‌کند و هدف اصلی از حملات Dos در هم شکستن سرویس دهنده و قطع ارتباط قربانی برای مدتی یا به طور دائم با شبکه می‌باشد. این حمله انواع مختلفی دارد و هکر از هر روشی برای

ایجاد اختلال در TCP استفاده می‌کند. حمله Dos ممکن است از درون شبکه و یا از خارج شبکه صورت گیرد. در حمله از درون شبکه هکر به عنوان مدیر یا در سطوح پایین‌تر قادر است هر پروسه سرویس دهنده‌ای را متوقف کند حمله از بیرون معمولاً حمله‌ای است که منجر به ترافیک شبکه و از بین رفتن منابع می‌گردد. برخی از انواع این حمله به اختصار شرح داده می‌شود:

حمله از نوع land : در این نوع حمله انبوهی از بسته‌های TCP با شرایط زیر به کامپیوتر سرویس دهنده فرستاده می‌شود.

1. فیلدهای Source port و Destination port دقیقاً مانند هم و به مقدار یکی از پورت‌های باز هر دو ماشین در شبکه.

2. فیلدهای Source IP Address و Destination IP Address و با هم مانند هم و به مقدار آدرس IP ماشینی مقصد.

با این کار پس از ارسال بسته به ماشین هدف چون آدرس مبدأ و مقصد یکی است. توسط TCP مورد قبول نمی‌باشد و به ماشین اصلی بر می‌گردد و در ماشین اصلی نیز چون همین مشکل وجود دارد به IP تنظیم شده بسته "ماشین هدف" برگشت داده می‌شود و این کار همینطور ادامه پیدا می‌کند تا زمانی که TCP شکست بخورد و مختل گردد.

حمله Ping Of Death :

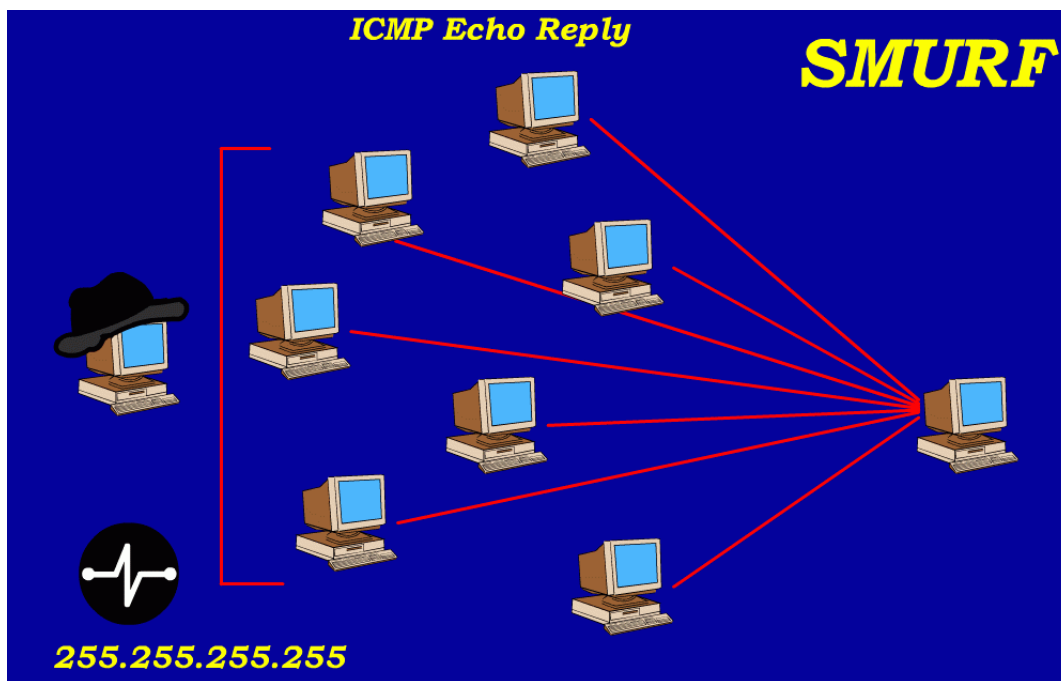
در این نوع حمله یک بسته ping با اندازه بیش از 64 k برای پروسه ICMP ارسال می‌گردد با دریافت چنین بسته‌ای به دلیل اینکه TCP برای چنین حالتی طراحی نگردیده مختل می‌گردد.

حمله نوع Jolt 2 :

در این نوع حمله یک جریان طولانی و وسیع از بسته‌های قطعه قطعه شده به سمت ماشین هدف در شبکه هدایت می‌شوند. از این رو پروسه TCP باید این قطعه‌ها را در خود نگهداری کند و چون تحت بمباران قرار گرفته در هم می‌شکند و ارتباط آن ماشین با شبکه قطع می‌گردد. طبق گزارشها تمامی سیستم‌های عامل ویندوز از این مشکل رنج می‌برند.

حمله نوع Smurf :

از آدرس IP 255. 255. 255. 255 برای ارسال پیام‌های فراگیر به ماشین‌های شبکه محلی استفاده می‌گردد به وسیله این آدرس می‌توان یک پیام را برای تمام ماشین‌هایی که فقط سمت راست IP آنها متفاوت هست ارسال کرد. در حمله Smurf هکر بسته‌ای را با مشخصات فراگیر به شبکه محلی می‌فرستد. با این تذکر که آدرس قربانی را به جای آدرس خود قرار می‌دهد. در نتیجه کلیه ماشین‌هایی که این بسته را دریافت کرده‌اند سعی در ارسال بسته ICMP Echo Reply می‌کنند. چون به یکباره تمامی این بسته‌ها به سوی سیستم قربانی ارسال می‌گردد و سیستم قربانی قادر به جواب دادن به آنها نیست هنگ می‌کند و ارتباط مختل می‌گردد.



در حمله Smurf به ماشینهای مورد استفاده هکر زامبی می‌گویند. زامبی اصطلاحی است که به کامپیوترهایی که بدون داشتن اطلاع صاحبشان توسط هکر به عنوان ابزار حمله Dos قرار می‌گیرند، اطلاق می‌گردد.

حمله Treadrop : در این روش بسته‌های قطعه شده با تنظیم غلط فیلدهای بسته پشت سر هم ارسال می‌شوند و در نهایت به طرز صحیحی بازسازی نخواهند شد و می‌تواند موجب اختلال TCP گردد.

• ویروسها:

کاربران کامپیوترهای شخصی و شبکه‌های کامپیوتری از ویروسها خسارات زیادی دیده‌اند. ویروس فقط یک برنامه کامپیوتری است که ممکن است با هر زبان برنامه‌نویسی نوشته شده باشد با این تفاوت که ویروسها برنامه‌های مخفی، مخرب و خطرناکی هستند که برخلاف برنامه‌های کاربردی مفید به نرم‌افزارها و حتی در مواردی به سخت‌افزارهای سیستم صدمه می‌زنند.

هکر با استفاده از ویروسی می‌تواند کامپیوتر قربانی را تا حد بسیار زیادی در مقابل حمله و نفوذ هکر شکست‌پذیر و ضعیف کند و راه را برای نفوذ هکر باز کند. هکر باید به طریقی ویروس را در کامپیوتر قربانی اجرا کند.

• اسبهای تراوا :

اسبهای تراوا یکی از پرکاربردترین برنامه‌ها در جهت نفوذ به سیستمها می‌باشد. استفاده از این ابزار برای تمامی گروههای هکرها و در هر سطحی امکان‌پذیر است. اسبهای تراوا ساختاری ساده و کاربردی راحت دارند. نامگذاری این برنامه‌ها به اسب تراوا به واقعه تاریخی در سالها قبل مربوط می‌شود. اسب تراوا، اسب چوبی و توخالی بود که یونانیان در جنگ تراوا وقتی که دیدند نمی‌توانند راه بازی را به درون قلعه پیدا

کنند. این اسب را به آنها هدیه دادند. در حالی که تعدادی از سربازان یونانی درون آن مخفی شده بودند. با وارد کردن اسب تراوا به درون قلعه سربازان یونانی مخفیانه درهای قلعه را برای نفوذ یونانیان باز کردند و از درون قلعه کنترل را بدست گرفتند. اسب‌های تراوا کامپیوتری نیز به همین گونه با ظاهری ساده و فریبنده بر سیستم قربانی وارد می‌شوند. - (با اجرای برنامه توسط خود قربانی) - و پس از ورود پنهان و مسکوت می‌مانند و در موقعیت لازم کنترل کامپیوتر قربانی را به هکر می‌سپارند. اسب‌های تراوا برخلاف ویروس‌های کامپیوتری خودشان هیچ‌گونه عملیات تخریبی انجام نمی‌دهند و فقط منتظر دستورهای هکر می‌مانند.

هر گاه کاربر فریب بخورد و این برنامه را در کامپیوتر خود اجرا کند. اسب تراوا معمولاً پیکربندی سیستم عامل را به گونه‌ای تغییر می‌دهد تا هرگاه کاربر به شبکه متصل شود برنامه نیز اجرا گردد. اسب‌های تراوا هیچ‌گونه علامت ظاهری و پنجره خاصی ندارند و کاملاً مخفی هستند.

از نمونه‌های معروف و پرکاربردترین اسب‌های تراوا برای هکرها می‌توان Bo2k Sub 7 و ... را نام برد.

• **درب‌های پشتی:**

این ابزارها بسیار مورد علاقه هکرها می‌باشند. چون نفوذ با این ابزارها بسیار راحت‌تر می‌باشد. درب پشتی به روشهایی می‌گویند که هکر به وسیله آنها بتواند بدون آنکه به تشریفات (کلمه رمز عبور و ...) احتیاج داشته باشد به کامپیوتر قربانی وارد شود. یکی از ساده‌ترین و کارآمدترین روشهای درب پشتی که هنوز هم برقرار است، استفاده از Netcat برای ارتباط روی یک پورت می‌باشد.

به وسیله دستور زیر می‌توان از Netcat به عنوان یک درب پشتی استفاده کرد.

```
Nc - I - P[port] - e cmd, exe
```

ویندوز

```
$ Nc - I - P[port] - w/ bin/ sh
```

Unix

بعد از این کار سریعاً برنامه پوسته فرمان اجرا می‌شود و هر چه هکر از طریق ماشین خود تایپ کند. به عنوان دستور تحویل سیستم مقابل داده و اجرا می‌شود. و هکر می‌تواند خروجی این دستورات را نیز در کامپیوتر خود مشاهده کند.

هکر برای نفوذ به در پشتی نیاز به هیچ عملی به جز برقراری یک ارتباط با پورت 12345 نداشته و احراز هویت و رمزنگاری معنایی ندارد و به این وسیله هکر می‌تواند اختیار آن سیستم را بدست بگیرد.

• **Rootkit :**

Rootkit ها بسیار بسیار قدرتمندتر از Virus ها و اسب‌های تراوا عمل می‌کنند. به این دلیل که Rootkit ها مستقیماً اجزای سیستم عامل را هدف قرار می‌دهند و با دستکاری سیستم عامل عملاً بیشترین نفوذ و بالاترین سطح دسترسی را برای خود نزدیکتر می‌کند. بدترین حالت Rootkit برای قربانی این است که هکر مستقیماً به هسته سیستم عامل نفوذ کند و آن را مطابق میل خود تغییر دهد. در این حالت هکر خود را غیرقابل شناسایی برای کاربر و حتی برنامه‌های بررسی شبکه و آنتی‌ها می‌سازد زیرا به قلب سیستم عامل نفوذ کرده و تمامی برنامه‌ها و موارد دیگر در اختیار اوست.

Rootkit ها بیشتر برای سیستم عامل Unix و خانواده آن نوشته می‌شوند. زیرا این ویندوزها Open source هستند و برنامه‌نویسی برای اجزای ویندوز بسیار راحت‌تر می‌باشد و از طرفی نیز در سطح هسته از قابلیت LKM سیستم‌های Unix و سیستم‌های سازگار با آن نهایت استفاده را می‌برند.

LKM مخفف Loadable Kernel Module قابلیت است که برای توسعه سیستم عامل Unix و پشتیبانی از آن قرار داده شده و اجازه بارگذاری ماژول‌های نوشته شده برنامه‌نویس به هسته سیستم عامل را می‌دهد. در این سیستم عامل‌ها (اغلب Unix و Solaris) برخلاف ویندوز نیاز به راه‌اندازی مجدد سیستم عامل نیست و Rootkit ها می‌توانند توسط LKM بسیار راحت نصب شوند و زمان را برای هکر تلف نمی‌کنند.

نفوذ از طریق Rootkit ها در سیستم‌های تحت ویندوز بسیار بسیار پیچیده‌تر از Unix و سیستم‌های پشتیبانی کننده از LKM ها است و به نسبت خیلی کم اتفاق می‌افتد که هکر موفق به نوشتن Rootkit بخصوص در سطح هسته Kernel ویندوز شود ولی از آنجایی که هیچ کاری برای هکرها غیرممکن نیست Rootkit هایی نیز برای ویندوز نوشته شده است که بعضاً با تغییر در فایل‌های سیستمی ویندوز مانند DLL ها تا حدود زیادی کنترل سیستم عامل را بدست می‌گیرد و با جایگزین کردن این DLL ها کامپیوتر قربانی را در برابر نفوذ شکست‌پذیر می‌کند.

در سیستم‌های ویندوز چون از LKM استفاده نمی‌شود Rootkit ها قابل بارگذاری نیستند ولی در این موارد از Path استفاده می‌گردد. پس از اجرای Path سیستم زمانی آلوده می‌گردد که سیستم عامل مجدداً راه‌اندازی شود. سپس برنامه هکر قسمتهای مختلف موردنظر را دست‌کاری می‌کند. برای جلوگیری از نفوذ هکرها به وسیله Rootkit پیشگیری همیشه بهتر از درمان می‌باشد و برای درمان نیز بهترین و مطمئن‌ترین راه حل نصب مجدد ویندوز یا هر سیستم عامل دیگر می‌باشد. زیرا زحمت و دردسری که درمان سیستم آلوده به Rootkit دارد بسیار بیشتر از نصب و راه‌اندازی مجدد سیستم عامل می‌باشد.

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 هکرها 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 ...