آموزش Hack

جلسه ششم

چگونه به یک پورت Telnet کنیم؟

برای اینکه عملکرد یک پورت برای شما روشن شود، باید به آن پورت Telnet کنید (البته معمولاً تعدادی از پورت‌هایی را که ممکن‌است اطلاعاتی مهم را دراختیار هکرها قراردهند - مثل پورت ۷۹ - می‌بندند و ممکن‌است ارتباط با آنها برقرار نشود). برای Telnetکردن در Command Prompt دستور زیر را تایپ کنید:

telnet *hostname portnum*

در این دستور به‌جای *hostname* شماره IP ویا نام سایت را وارد می‌کنید و به‌جای *portnum* شماره پورت ویا معادل آن را از جدول موجود در جلسه پنجم. مثلاً برای Telnetکردن به پورت ۱۳ که ساعت و تاریخ را به‌دست می‌آورد، در کامپیوتری به‌نام www.iums.ac.ir یکی از دو دستور زیر را می‌نویسید:

```
telnet iums.ac.ir 13
telnet iums.ac.ir daytime
```

هر دو این دستورات معادل هم هستند.

Telnetکردن معمولاً اولین کاری است که یک Hacker برای Hackکردن یک سایت انجام می‌دهد، زیرا بعضی‌از پورت‌ها درصورت بسته‌نبودن روی آن سرور، معمولاً حاوی اطلاعات بسیار مهمی هستند.

همین‌الآن شروع‌کنید و مثل یک Hacker واقعی به کامپیوترهای مختلف و پورت‌های گوناگون Telnet کنید و اطلاعات ارزشمندی درباره آنها جمع‌آوری‌نمایید.

انواع Scanning:

دو نوع رایج Scanning وجود دارد:

۱- Port Scanning:

در این حالت ما IP یا IPهای موردنظر را انتخاب کرده‌ایم و حالا می‌خواهیم بدانیم که کدام پورت‌ها روی آن کامپیوترها باز است.

۲- IP Scanning:

در این روش می‌خواهیم بدانیم که ازبین یک مجموعه IP، کدام‌موارد Up هستند؛ یعنی کدام IPها الآن قابل‌دسترسی هستند (یعنی به یک کامپیوتر در اینترنت نسبت‌داده شده‌است!). فرض‌کنید که شما یک‌سری IP مربوط‌به یک ISP خاص را دارید و می‌خواهید بدانید که در این‌لحظه کدام‌ها فعال (Up) هستند تا فقط آنها را بررسی‌کنید و نه همه را (این‌کار معمولاً وقتی پیش می‌آید که قراراست یک Client را Hackکنید و مهم‌نیست چه‌کسی باشد.

چگونه یک ارتباط TCP برقرار می‌شود تا بتوانیم بفهمیم Port خاصی باز است یا نه؟

برای اینکه تعیین‌کنیم که یک Port روی یک Server باز است یا نه، معمولاً باید یک TCP Connect Scan انجام‌دهیم. اول این‌را

بگویم که Port Scanning انواع مختلفی دارد و فعلاً ما نوع TCP Connect را مدنظر داریم. این نوع اسکن سه مرحله دارد که به آن TCP's 3-Way Handshake می‌گویند:

۱- اول کامپیوتر ما به‌سمت Server یک SYN Packet می‌فرستد که به‌معنی درخواست اتصال است.

۲- اگر Server این درخواست را قبول‌کند، در مرحله دوم Server به‌سمت ما یک SYN/ACK Packet ارسال می‌کند.

۳- در مرحله آخر کامپیوتر ما یک ACK Packet به‌سمت Server می‌فرستد.

نوع دیگری از Port Scan، TCP SYN Scan نام دارد. باتوجه‌به اینکه اگر Port Scan به روش بالا (TCP Connect Scan) انجام‌دهیم، معمولاً این اتصال در Server ذخیره خواهدشد و بعداً می‌توانند ما را ردیابی‌کنند. به‌جای آن می‌توان از TCP Syn Scan استفاده‌کرد. در این‌نوع اسکن، مراحل ۱ و ۲ فوق انجام می‌شود ولی مرحله ۳ نه! به‌جای آن، اگر در مرحله ۲ به ما یک SYN/ACK برسد، آن Port باز است و اگر یک RST/ACK برسد، یعنی بسته‌است.

انواع دیگری از Port Scanning هم وجود دارد؛ مثل TCP ACK، TCP Window Scan، UDP Scan، TCP FIN، TCP Xmas Tree، TCP Null، Scan Scan و...

چگونه می‌توان عمل Port Scanningرا انجام‌داد؟

در تمام مطالبی که تا این مرحله گفته‌ام، سعی کرده‌ام که فقط از ابزارهای موجود در ویندوز استفاده‌کنم و هیچ ابزار دیگری به‌کار نبرم، اما در مبحث Port Scanning چون هیچ ابزاری در ویندوز برای این‌کار نیست، به‌ناچار باید یک‌سری برنامه را از اینترنت Download کنید یا اینکه ازطریق CDهای موجود در بازار، آنها را تهیه‌کنید (توجه‌کنید که فعلاً حرفی از Linux نزده‌ام و سعی می‌کنم فعلاً هیچ بحثی را درمورد آن مطرح نکنم).

۱- nMAPWIN:

نسخه گرافیکی و مخصوص ویندوز برای nmap است (nmap در Linux مورداستفاده قرار می‌گیرد). nmap از کامل‌ترین ابزارهایی است که Hackerها به‌کار می‌برند و علاوه‌بر توانایی انجام انواع Port Scanning، می‌تواند کارهای بسیاری ازقبیل تشخیص سیستم‌عامل Server و... را انجام‌دهد (این ابزار را بعداً توضیح خواهم‌داد ولی فعلاً برای کار ما، بیش‌از حد پیشرفته است!).

۲- NetScanTools Pro 2000:

این‌هم از بهترین‌هاست ولی چون رایگان نیست، به‌جای Download باید در CDهای موجود در بازار آنرا بیابید!

۳- WinScan:

برای اسکن TCP (و نه UDP) می‌توانید از آن استفاده‌کنید (براساس تجربه شخصی، آنرا زیاد دلچسب ندیدم!).

۴- IPEye:

من در این درس از این نرم‌افزار استفاده خواهم‌کرد، برای دریافت آن از آدرس http://ntsecurity.nu/downloads/ipeye.exe استفاده‌کنید (حجم فایل: ۳۲کیلوبایت). لازم‌است بگویم که این نرم‌افزار فقط در ویندوزهای ۲۰۰۰ و XP کار می‌کند و نیز در هربار اجرا

فقط می‌تواند یک IP را تست‌کند. ضمناً فقط TCP را بررسی می‌کند.

چگونه از IPEye برای Port Scanning استفاده‌کنیم؟

Command Prompt را اجرا کرده و به مسیری که فایل IPEye.exe را در آنجا قرارداده‌اید بروید. مثلاً اگر فایل را در درایو C: و پوشه IPEye ذخیره کرده‌اید، با دستورات زیر درداخل Command Prompt می‌توانید به پوشه مربوطه بروید:

```
C:
CD\IPEye
```

حال با تایپ IPEYE در Command Prompt و فشردن کلید Enter نتایج زیر ظاهر می‌شود:

```
ipEye 1.2 - (c) 2000-2001, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
          - http://ntsecurity.nu/toolbox/ipeye/


Error: Too few parameters.


Usage:


  ipEye <target IP> <scantype> -p <port> [optional parameters]
  ipEye <target IP> <scantype> -p <from port> <to port> [optional parameters]


  <scantype> is one of the following:
     -syn  = SYN scan
     -fin  = FIN scan
     -null = Null scan
     -xmas = Xmas scan


     (note: FIN, Null and Xmas scans don't work against Windows systems.


  [optional parameters] are selected from the following:
     -sip <source IP>  = source IP for the scan
     -sp <source port> = source port for the scan
     -d <delay in ms>  = delay between scanned ports in milliseconds
                         (default set to 750 ms)
```

حال فرض‌کنید که می‌خواهیم سایت 404.ir را ازنظر Portها از ۱ تا ۲۰۰ بررسی‌کنیم. اول باید IP آن‌را به‌دست بیاوریم که به‌کمک مطالب جلسات قبل، IP به‌دست‌آمده از روش Whois این‌گونه است: 75.127.84.119 و حالا به‌کمک دستور زیر آن‌را بررسی می‌کنیم:

```
IPEYE 75.127.84.119 -syn -p 1 200
```

دقت‌کنید که عدد 75.127.84.119 عدد IP مربوط‌به سایت 404.ir، -syn یعنی SYN SCAN و -p 1 200 یعنی بررسی از Port شماره ۱ تا شماره ۲۰۰. البته پارامترهای دیگری را هم می‌توان تعیین‌کرد که فعلاً به‌درد ما نمی‌خورد. با اجرای این دستور به نتایج زیر می‌رسیم:

```
ipEye 1.2 - (c) 2000-2001, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
          - http://ntsecurity.nu/toolbox/ipeye/
```

```
1-20 [drop]
21 [open]
22 [closed or reject]
23-24 [drop]
25 [open]
26 [open]
27-52 [drop]
53 [open]
54-79 [drop]
80 [open]
81-109 [drop]
110 [open]
111-142 [drop]
143 [open]
144-200 [drop]
201-65535 [not scanned]
```

Closed یعنی کامپیوتر در آن‌طرف هست ولی به Port گوش نمی‌دهد؛ Reject یعنی اینکه یک Firewall وجود دارد که اجازه اتصال به آن Port را نمی‌دهد؛ Drop یعنی اینکه یک Firewall همه‌چیز را پس می‌زند و یا اصلاً کامپیوتری در آن‌طرف اتصال وجودندارد؛ Open نیز به‌معنی بازبودن Port و امکان برقراری ارتباط با آن است.

درمورد 404.ir می‌بینید که ازبین Portهای ۱ تا ۲۰۰، شماره‌های ۲۱، ۲۵، ۲۶، ۵۳، ۸۰، ۱۱۰ و ۱۴۳ باز است و می‌توان به آنها Telnet نمود. دقت‌کنید که تا تمام Portهایی که مشخص‌شده، بررسی نشده‌اند، چیزی نشان‌داده نمی‌شود و لذا کمی صبر لازم‌است.

تعیین Portهای باز کامپیوتر خودمان

می‌خواهیم درباره کامپیوتر خودمان این اطلاعات را پیدا کنیم. برای این‌کار یکی‌از دستورات زیر را به‌کار می‌بریم:

```
netstat -an
netstat -a
```

فرق این دو دستور در این است که اولی Portها را به‌صورت عددی و دومی به‌صورت معادل اسمی آن Port می‌نویسد. مثلاً معادل اسمی Port شماره ۷، echo است.

به‌عنوان مثال، اگر من روی کامپیوتر خودم netstat -an را تایپ کنم، به اطلاعات زیر می‌رسم:

```
Active Connections


  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1029         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:10110        0.0.0.0:0              LISTENING
  TCP    192.168.0.10:139       0.0.0.0:0              LISTENING
  TCP    192.168.0.10:1042      64.233.183.147:80      CLOSE_WAIT
  TCP    192.168.0.10:1044      66.29.87.160:80        CLOSE_WAIT
  TCP    192.168.0.10:1276      192.168.0.1:139        ESTABLISHED
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1025           *:*
```

```
  UDP    0.0.0.0:1162           *:*
  UDP    0.0.0.0:1178           *:*
  UDP    0.0.0.0:2336           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1035         *:*
  UDP    127.0.0.1:1900         *:*
  UDP    192.168.0.10:123       *:*
  UDP    192.168.0.10:137       *:*
  UDP    192.168.0.10:138       *:*
  UDP    192.168.0.10:1900      *:*
```

من دستور فوق را وقتی که ازطریق شبکه و توسط یک کامپیوتر دیگر به اینترنت متصل‌بودم، اجرا کردم. اگر همین‌کار را در زمان اتصال مستقیم اینترنت انجام می‌دادم، یک‌سری سطرها که مربوط‌به آن اتصال بودند، اضافه‌می‌شد. ضمناً دقت‌کنید که من از پارامتر an- استفاده کرده‌ام و Portها به‌صورت عددی نشان‌داده شده‌است.

اولین نکته‌ای که به‌نظر می‌رسد، نامی است که برای هر ستون نوشته شده‌است:

```
  Proto  Local Address          Foreign Address        State
```

Proto : یعنی Protocol که می‌تواند TCP یا UDP باشد.

Local Address : نشان‌دهنده IP کامپیوتر خودمان و شماره Portها است. مثلاً سطر اول می‌گوید که IP من 0.0.0.0 است (دقت‌کنید که من مستقیماً به اینترنت متصل نیستم) و اولین Port باز (ازنوع TCP) عدد ۷ است زیرا به‌صورت 0.0.0.0:7 نوشته‌شده‌است که قسمت قبل‌از : مشخص‌کننده IP و بعد از آن، Port است.

Foreign Address : چون در این مثال از پارامتر a- یا an- استفاده کرده‌ایم، کاربرد خاصی ندارد. ولی بعداً خواهیم‌دید که اگر از یک پارامتر دیگر استفاده‌کنیم، می‌تواند حاوی اطلاعات مهمی باشد.

State : وضعیت اتصال را نشان می‌دهد.

حال اگر Portها را یک‌به‌یک بررسی‌کنید، می‌بینید که در پروتکل TCP، Portyهای ۱۳۵، ۴۴۵، ۲۸۶۹ و...، و در پروتکل UDP، Portهای ۴۴۵، ۵۰۰، ۱۰۲۵ و... باز است.

ممکن‌است بپرسید که دانستن این اطلاعات درمورد کامپیوتر خودمان به‌چه‌دردی می‌خورد؟ جواب این‌است که دانستن این اطلاعات برای محافظت از خودتان دربرابر همکارانتان (Hackerها) است. مثلاً اگر یک Trojan روی کامپیوتر شما نصب شده‌باشد، با این دستور می‌توان آن‌را کشف‌کرد.