آموزش Hack

جلسه سوم

Command Prompt چیست؟

در بسیاری از دروس آینده، از Command Prompt (خط فرمان) ویندوز استفاده خواهیم‌کرد. برای بازکردن آن، یکی‌از روش‌های زیر را به‌کار برید:

۱- مسیر زیر را در ویندوز طی کنید:

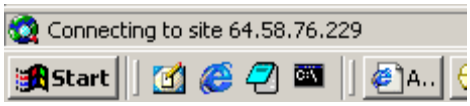
```
Start -> All Programs (or Programs) -> Accessories -> Command Prompt
```

۲- درقسمت Run از منوی Start بنویسید: Command یا CMD و کلید Enter را فشاردهید یا برروی OK کلیک کنید.

پیداکردن IP یک سایت با دانستن آدرس اینترنتی آن (پیداکردن IP کامپیوتر Server) :

برای این‌کار روش‌های مختلفی وجود دارد:

۱- در IE (Internet Explorer) آدرس موردنظر را تایپ‌کنید و کلید Enter را فشاردهید. درقسمت پایین مرورگر یعنی نوار وضعیت (Status Bar) پس‌از چندلحظه، برای مدت کوتاهی IP نمایش‌داده می‌شود و می‌توانید آنرا یادداشت‌کنید. اگر طول این‌مدت بسیار کوتاه است، می‌توانید از صفحه عکس‌بگیرید (با دکمه Print Screen یا PrtScrn صفحه‌کلید) و در یک نرم‌افزار گرافیکی (مثلاً MS-Paint یا Adobe Photoshop، بعد از بازکردن یک صفحه خالی، به‌کمک کلیدهای Ctrl + V آنرا مشاهده‌کنید (عجب راه ابلهانه‌ای!). اگر این‌کار را برای www.yahoo.com انجام‌دهیم:



که همان شماره IP برای www.yahoo.com است.

نکته بسیار مهم این‌است که به‌دلیل ضریب اشتباه بسیار بالای این روش، هیچ‌گاه از آن استفاده‌نکنید. نتایج ممکن‌است کاملاً اشتباه‌باشد که بعداً خواهم‌گفت چرا؟

۲- در داخل Command Prompt، دستور Ping را با ساختار زیر صادر کنید:

```
ping domain
```

و به‌جای *domain*، آدرس سایت موردنظر را بنویسید. در این‌حالت، می‌توانید IP آن سایت را مشاهده‌کنید (البته کار اصلی Ping چیز دیگری‌است و می‌توان‌گفت از آن سوءاستفاده می‌کنیم). مثلاً برای پیداکردن IP سایت www.yahoo.com می‌نویسیم:

```
ping www.yahoo.com
```

و جواب می‌گیریم:

```
Pinging www.yahoo-ht3.akadns.net [69.147.114.210] with 32 bytes of data:


Reply from 69.147.114.210: bytes=32 time=250ms TTL=41
Reply from 69.147.114.210: bytes=32 time=247ms TTL=41
```

```
Reply from 69.147.114.210: bytes=32 time=249ms TTL=41
Reply from 69.147.114.210: bytes=32 time=247ms TTL=41


Ping statistics for 69.147.114.210:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 247ms, Maximum = 250ms, Average = 248ms
```

به اعداد تولیدشده (69.147.114.210) دقت‌کنید. می‌بینید که با شکل روش اول، تفاوت‌دارد (من که گفتم ممکن‌است روش اول نتایج اشتباه تولیدکند!). دقت‌کنید که نتایج Ping برای سایت‌های بزرگ، با www. و بدون آن، ممکن‌است متفاوت‌باشد. مثلاً نتایج Ping برای yahoo.com را با نتایج Ping آدرس www.yahoo.com مقایسه‌کنید:

```
Pinging yahoo.com [216.109.112.135] with 32 bytes of data:


Reply from 216.109.112.135: bytes=32 time=255ms TTL=41
Reply from 216.109.112.135: bytes=32 time=256ms TTL=41
Reply from 216.109.112.135: bytes=32 time=257ms TTL=41
Reply from 216.109.112.135: bytes=32 time=258ms TTL=41


Ping statistics for 216.109.112.135:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 255ms, Maximum = 258ms, Average = 256ms
```

۳- کامل‌ترین روش، روش Whois کردن به بعضی سایت‌هیا خاص است. بعداً این‌روش را کامل‌تر توضیح می‌دهم؛ ولی فعلاً روش کـار را می‌گویم: آدرس زیر را در مرورگر خود تایپ‌کنید:

http://samspade.org/whois/*domain*

و به‌جای *domain*، آدرس سایت موردنظر را بنویسید. درمورد www.yahoo.com نتایج زیر به‌دست می‌آیند:

```
www.yahoo.com = [ 69.147.114.210 ]
(Asked whois.markmonitor.com:43 about yahoo.com)
MarkMonitor.com -
 Registrant:
        Yahoo! Inc.
        (DOM-272993)
        701 First Avenue Sunnyvale
        CA
        94089 US
     Domain Name: yahoo.com
        Registrar Name: Markmonitor.com
        Registrar Whois: whois.markmonitor.com
        Registrar Homepage: http://www.markmonitor.com
     Administrative Contact:
        Domain Administrator
        (NIC-1382062)
        Yahoo! Inc.
        701 First Avenue Sunnyvale
        CA
        94089 US
 domainadmin@yahoo-inc.com
 1.4083493300 Fax- 1.4083493301
     Technical Contact  Zone Contact:
        Domain Administrator
        (NIC-1372925)
        Yahoo! Inc.
        701 First Avenue Sunnyvale
        CA
        94089 US
```

```
domainadmin@yahoo-inc.com
1.4083493300 Fax- 1.4083493301
    Created on..............: 1995-Jan-18.
    Expires on..............: 2012-Jan-19.
    Record last updated on..: 2007-Sep-18 09: 45: 58.
    Domain servers in listed order:
    NS4.YAHOO.COM
    NS5.YAHOO.COM
    NS1.YAHOO.COM
    NS2.YAHOO.COM
    NS3.YAHOO.COM
MarkMonitor.com - The Leader in Corporate Domain Management
-------------------------------------------------------------
For Global Domain Consolidation  Research & Intelligence
and Enterprise DNS  go to: www.markmonitor.com
-------------------------------------------------------------
```

فعلاً به همین‌توضیح قناعت‌کنید که آدرس IP واقعی، در سطر اول نوشته‌شده‌است. این‌را هم به‌عنوان یک قانون قبول‌کنید که نتایج حاصل‌از Whois، نتایج دقیق‌تری هستند.

تقسیم‌بندی آدرس‌های IP :

آدرس‌های IP به ۵ کلاس تقسیم‌بندی می‌شوند که A تا E نام‌دارند ولی از این‌بین، سه کلاس اول (یعنی A، B و C) کاربرد عملی دارند که آنها را شرح می‌دهیم:

۱- کلاس A : اگر IP را به‌صورت xxx.yyy.yyy.yyy درنظر بگیرید، این‌کلاس تمام IPهایی را شامل می‌شود که xxx بین ۱ تا ۱۲۶ است. این کلاس ویژه Backboneهای بزرگ اینترنتی است و درهنگام ثبت Domain برای گرفتن IP از آنها برای گرفتن IP استفاده‌می‌شود. بنابراین اکثر سایت‌ها چنین IPهایی دارند. این کلاس را 8/ هم می‌گویند.

۲- کلاس B : این کلاس تمام IPهایی را شامل می‌شود که xxx بین ۱۲۸ و ۱۹۱ است. این کلاس هم ازجمله کلاس‌های پرکاربرد است. این کلاس را 16/ هم می‌نامند.

۳- کلاس C : این کلاس تمام IPهایی را شامل می‌شود که xxx بین ۱۹۲ و ۲۲۳ است. این‌کلاس معمولاً به ISPهایی که خدمات Dialup ارائه می‌دهند، تعلق می‌گیرد (البته این‌جمله به‌معنای بیان دقیق و همراه‌با یقین نیست و ممکن‌است موارد استثنا هم وجودداشته‌باشد. بنابراین اگر به‌صورت Dialup به اینترنت متصل‌شوید، معمولاً چنین IP دریافت‌خواهیدکرد. از این‌کلاس تحت‌عنوان 24/ هم نام‌برده می‌شود.

سؤالی که ممکن‌است مطرح‌شود این‌است که چرا xxx در هیچ کلاسی، شامل عدد ۱۲۷ نمی‌شود؟ جواب این‌است که ۱۲۷ برای کامپیوتر خودمان رزرو شده‌است. مثلاً 127.0.0.1 معمولاً برای localhost یعنی کامپیوتر خودمان درنظر گرفته می‌شود.

به‌دست‌آوردن IP خودتان بعد از اتصال به اینترنت :

برای این‌کار راه‌های متفاوتی وجوددارد:

۱- راحت‌ترین راه، استفاده از دستور IPConfig است. من با تایپ‌کردن آن در Command Prompt به نتایج زیر رسیدم:

```
Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.8.38
        Subnet Mask . . . . . . . . . . . : 255.255.248.0
        IP Address. . . . . . . . . . . . : fe80::21a:4dff:fe51:6519%4
        Default Gateway . . . . . . . . . : 192.168.9.1

PPP adapter CRESG:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 172.16.9.106
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 172.16.9.106

Tunnel adapter Teredo Tunneling Pseudo-Interface:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 3ffe:831f:4136:e38e:0:96c:af40:53f6
        IP Address. . . . . . . . . . . . : fe80::5445:5245:444f%5
        Default Gateway . . . . . . . . . : ::

Tunnel adapter Automatic Tunneling Pseudo-Interface:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : fe80::5efe:172.16.9.106%2
        Default Gateway . . . . . . . . . :

Tunnel adapter Automatic Tunneling Pseudo-Interface:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : fe80::5efe:192.168.8.38%2
        Default Gateway . . . . . . . . . :
```

که آدرس IP خودتان را در بخش ??? PPP adapter (به‌جای ??? نام اتصال اینترنت خود را خواهید دید)، و درمقابل IP Address مشاهده خواهید کرد (فعلاً مسئله Proxy را نادیده بگیرید).

۲- بعداز اتصال به اینترنت، حداقل یک وب‌سایت را بازکنید و بعد درحالی که صفحه موردنظر باز است، در Command Prompt از دستور Netstat -n استفاده‌کنید. من بااستفاده‌از این دستور، به نتایج زیر رسیدم:

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.16.9.106:2469      64.58.76.177:80        ESTABLISHED
  TCP    172.16.9.106:2471      66.163.175.130:80      ESTABLISHED
  TCP    172.16.9.106:2473      212.73.194.143:80      ESTABLISHED
  TCP    172.16.9.106:2474      212.73.194.143:80      ESTABLISHED
  TCP    172.16.9.106:2476      212.73.194.136:80      SYN_SENT
```

ستونی که زیر عبارت Local Address قراردارد، IP من در آن اتصال است. بنابراین، IP من در آن اتصال، 172.16.9.106 بوده‌است.

پیداکردن IP طرف‌مقابل هنگام Chat با Yahoo! Messenger:

نکته: این‌روش قدیمی‌شده و در بعضی‌مواقع کار نمی‌کند! من دراینجا فقط جهت آشنایی شما با روش‌های مختلف، آنرا ذکر می‌کنم.

می‌خواهیم درباره یک Client مثلاً کسی‌که مثل شما یک اتصال ازنوع Dialup به اینترنت دارد و فرضاً دارد با شما Chat می‌کند، اطلاعات کسب‌کنیم.

دراین‌مورد هم اولین‌نکته‌ای که باید کشف‌شود، IP وی است. در این جلسه، می‌گویم که چگونه زمانی‌که با یک‌نفر ازطریق برنامه Yahoo! Messenger به‌صورت PM (Private Message) Chat می‌کنید، IP وی را بیابید. البته باید توجه‌کنید که این‌روش گاهی کارنمی‌کند. همچنین فرض بر این‌است که فقط با یک‌نفر درحال Chatکردن هستید.

یکی‌از دستورات زیر را در Command Prompt تایپ‌کنید:

```
netstat -n
netstat
```

دستور اول برای پیداکردن IP طرف‌مقابل است و دستور دوم، گاهی ممکن‌است اسم کامپیوتر وی را به‌شما نشان‌دهد. من از دستور netstat -n استفاده‌کردم و به نتایج زیر رسیدم:

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.16.9.106:1296      66.163.175.130:5050   ESTABLISHED
  TCP    172.16.9.106:1341      66.218.75.149:80      LAST_ACK
  TCP    172.16.9.106:1325      212.234.112.74:5101   SYN_SENT
```

اولین‌کاری که می‌کنید، این‌است که سطری را پیدا می‌کنید که در Local Address یا Foreign Address آن، Port شماره ۵۱۰۱ داشته‌باشد. در این مثال، سطر آخر، سطر موردنظر ما است، زیرا در ستون Foreign Address از سطر آخر، پورت آن، ۵۱۰۱ است. البته اگر در ستون Local Address هم بود، فرقی نمی‌کرد. وقتی آن‌سطر را پیدا کردید، IP طرف مقابل را از ستون مربوطبه Foreign Address یادداشت‌کنید. در مورد اطلاعات بالا، IP طرف‌مقابل، 212.234.112.74 است.

حال به‌جای netstat -n از netstat استفاده کردم و به نتایج زیر رسیدم:

```
  Proto  Local Address          Foreign Address               State
  TCP    cresg:1296             cs55.msg.sc5.yahoo.com:5050   ESTABLISHED
  TCP    cresg:1298             dl3.yahoo.com:http            TIME_WAIT
  TCP    cresg:1325             majid:5101                    SYN_SENT
```

ملاحظه می‌فرمایید که همه IPها به معادل‌های اسمی تبدیل شده‌اند و درمورد همان سطر آخر، به‌جای IP طرف‌مقابل، اسم کامپیوتر فرد را می‌نویسد (البته درحالتی‌که اتصال طرف‌مقابل ازنوع Dialup نباشد، قضیه فرق می‌کند).

حالا فرض‌کنید که یک PM دیگر هم اضافه می‌شود. دوباره از دستور netstat -n استفاده می‌کنم و به نتایج زیر می‌رسم:

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.16.9.106:1296      66.163.175.130:5050   ESTABLISHED
  TCP    172.16.9.106:1341      66.218.75.149:80      ESTABLISHED
  TCP    172.16.9.106:5101      212.234.112.74:3735   ESTABLISHED
  TCP    172.16.9.106:5101      194.225.184.95:1460   ESTABLISHED
```

الآن دو سطر دارم که دارای Port شماره ۵۱۰۱ هستند، و چون می‌دانم که 212.234.112.74 مربوطبه نفر قبلی است، پس 194.225.184.95 مربوطبه PM دوم است.