آشنايي با Netstat و دستورات آن

سلام دوستان ، در اين مقاله ميخوام راجب برنامه Netstat و دستورات آن كمي توضيح بدم تا شما يک آشنايي با اين برنامه داشته باشين ، خب بچه ها هر وقت صحبت از Netstat ميشه همه به ياد فرمان Netstat -n مي افتن غافل از اينكه Netstat دستورات زيادي داره كه بعضي از آنها به يک هكر كمكهاي زيادي ميكنه كه من تمام دستورها را براتون توضيح ميدم ولي قبلش بايد بفهميم كه اصلاً Netstat چيه و چكار ميكنه ؟

Netstat هم مثل Netbios يک برنامه خدماتي هست كه در خود سيستم عاملها گذاشته شده ، مثلاً در ويندوز ۹x و Me در پوشه Windows\ با اسم Netstat.exe قرار گرفته و در ويندوزهاي بر پايه NT مثل ۲۰۰۰ نيز در پوشه D:\WinNT\System32 قرار گرفته و كلاً براي نمايش تمام ارتباطات ما در شبكه و فهميدن پورتها و آيپي هاي سيستمها و ماشين هايي كه ما با آنها در ارتباط هستيم بكار ميره ، براي استفاده از Netstat احتياج به هيچ برنامه كمكي و اضافي نداريم

فقط كافيه به MS-DOS Prompt برين و دستوراتي كه در ادامه اين مقاله ميگم را تايپ كنيد ، ولي خب برنامه هاي زيادي براي استفاده آسان تر از Netstat آمده كه احتياجي به رفتن در Ms-Dos نداره و كار كاربران اينترنت و شبكه را راحت تر كرده كه يكي از بهترين برنامه ها براي اينكار X-Netstat هست كه اطلاعات زيادي از ارتباطهاي شما وقتي كه به شبكه وصل هستين ميده ، درست مثل برنامه Netstat.exe ولي به صورت گرافيكي و تحت ويندوز .

اين برنامه همچنين سيستمهايي كه از خارج سعي ميكنن به سيستم شما وصل بشن را هم نشان ميده و آيپي آنها را مشخص ميكنه ، درست مثل يک فايروال و همچنين پورتهاي Local و Remote و پروتكل هايي كه شما با آنها ارتباط دارين را مشخص ميكنه .

X-Netstat بر_c7ي كاربران معمولي نسخه Standard را عرضه كرده كه جديدترين نسخه X-Netstat Standard ورژين ۵,۰ Beta هست و براي كاربران حرفه اي مثل شما نيز X-Netstat Professional را ارائه داده كه جديدترين نسخه آن ۴,۰ هست كه براي مديران شركتها نيز مفيده ، شما ميتون_http://www.freshsw.com/files/xnsp400.exe

خب اين يكي از برنامه هاي مفيدي هست كه مربوط به Netstat بود ولي حالا توضيح درباره دستورات خود Netstat :

دستور Netstat : دستور Netstat فرمان اصلي اين برنامه هست كه با تايپ اين دستور شما متوجه آيپي سيستمها و پورتهايي كه با آنها در ارتباط هستين بدست ميارين و همچنين مشاهده ميكنين كه پورتهايي Listening و يا Established هستن و چه چيزي روي پورتهاي مختلف در حال شنيده شدن هست كه خب اين باعث ميشه اگر پورتي مخصوص يک تروجن مثل ۲۷۳۷۴ كه پورت اصلي Sub7 هست در سيستم شما باز بود شما متوجه اين پورت باز بروي سيستمتان بشين.

اگر در قسمتForeign Address هم يک آيپي بوسيله آن پورت به سيستم شما وصل بود شما ميفهمين كه

يک نفر با آن آيپي در سيستم شماست ، پس اين يک راهي هست که متوجه بشين سيستمتان آسيب پذير هست يا نه ، براي مثال من با تايپ دستور Netstat در Ms-Dos اين نتايج را گرفتم :

C:\WINDOWS>netstat
Active Connections
Proto Local Address Foreign Address State
TCP behrooz:1454 cs33.msg.sc5.yahoo.com:5050 ESTABLISHED
TCP behrooz:1488 63.123.44.222:80 ESTABLISHED
TCP behrooz:1491 opi1.vip.sc5.yahoo.com:80 TIME_WAIT
TCP behrooz:1497 64.187.54.23:80 ESTABLISHED
TCP behrooz:1498 64.187.54.23:80 ESTABLISHED

همانطور که ملاحظه ميکنيد اين دستور گاهي اوقات اسم صاحب سيستم کلاينتي که شما با آن در ارتباط هستين را نيز ميده و چون اينجا من با کسي در PM نبودم اسم کسي را نميبينيد ولي اگر کسي با من چت کنه و دستور Netstat را بزنه اسم بهروز را ميبينه و متوجه ميشه که اين صاحب آن سيستم کلاينتي هست که داره با آن چت ميکنه و همچنين مشخصه که من با پورت ۵۰۵۰ با ياهو مسنجر ارتباط برقرار کردم و همچنين نتايجي که در زير Local Address مشخص اطلاعاتي درباره خود من هست :

IP/Hostname:Port open ===> behrooz:1488

و نتايجي که در Address Foreign بدست مياد مشخص ميکنه که ما با چه سرور يا کلاينتي در ارتباطيم که در سطر دوم مثال بالا يعني ۶۳,۱۲۳,۴۴,۲۲۲:۸۰ که آيپي سايت ياهو هست من در سايت ياهو بودم و به وسيله پورت ۸۰ که پورت Http هست من با اين وب سرور ارتباط برقرار کردم و در قسمت Status هم مشخص ميشه که شما با چه پورتهايي Established هستين.

يعني ارتباط برقرار کردين و وصل هستين و چه پورتهايي Listening يا منتظر Request و در حال شنيدن هستن ، بنابراين ميشه با دستور Netstat يک عمل مانيتورينگ از تمام آيپي ها - پورتها و ماشينهايي که شما با آنها در ارتباطين گرفت .

دستور Netstat -n :
همانطور که در بالا توضيح دادم ميشه با استفاده از Netstat آيپي و پورت سيستمي که شما با آن در ارتباطين را بدست آورد حتا ميشه آيپي کسي داره با شما از طريقه PM در مسنجر چت ميکنه را هم بدست آورد چون وقتي شما مسنجرها را باز ميکنيد با يک پورت خاصي شما با مسنجر ارتباط برقرار ميکنين که مثلاً شما با پورت ۵۰۵۰ با ياهو مسنجر ارتباط برقرار ميکنين .

شما با استفاده از دستور Netstat -n که در MS-DOS تايپ ميکنين ميتونين آيپي طرف را بدست بيارين اگرچه من چند وقت پيش برنامه ProPort را معرفي کردم که اينکار را با قابليتهاي بيشتري انجام ميده ولي با اين دستور هم ميشه اينکار را کرد .

اگر شما بعد از تايپ اين دستور و در نتيجه بدست آمده در قسمت Foreign Address با آيپي سيستمي بوسيله پورت ۵۱۰۱ ارتباط برقرار کرده بودين مطمئن باشين آن آيپي براي کسي هست که داره با شما چت ميکنه مثلاً من با تايپ دستور Netstat -n اين نتايج را گرفتم :

Active Connections

Proto	Local Address	Foreign Address	State
TCP	207.117.93.43:1425	216.136.175.226:5050	TIME_WAIT
TCP	207.117.93.43:1431	64.242.248.15:80	ESTABLISHED

TCP 207.117.93.43:1437 213.102.29.137:5101 ESTABLISHED

همانطور که ملاحظه میکنید من در این لحظه با آیپي ۲۱۳,۱۰۲,۲۹,۱۳۷ در حال چت کردن بودم که اشتراکش هم از البرز بوده و آیپي خود من هم در قسمت Local Address مشخص میشه ، در قسمت Proto نیز پروتکلي که ما بوسیله آن با یک سیستم ارتباط برقرار کردیم مشخص میشه که اینجا از طریقه پروتکل TCP هستش .

دستور ?/Netstat :

شاید بهتر بود من این دستور را قبل از ۲ دستور Netstat و Netstat -n معرفي میکردم چون این دستور راهنما یا Help برنامه Netstat هست که با تایپ کردن آن شما یک صفحه کامل راجب فرمان Netstat میبینین و توضیح مختصري هم در جلوي هر دستور مشاهده میکنید ، شما با تایپ این دستور به این نتایج میرسین :

C:\WINDOWS>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

-a Displays all connections and listening ports.
-e Displays Ethernet statistics. This may be combined with the -s option.
-n Displays addresses and port numbers in numerical form.
-p proto Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display per-protocol statistics, proto may be TCP, UDP, or IP.
-r Displays the routing table.
-s Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default.
interval Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

البته این تمام دستورات Netstat نیست و کلاً Help کاملي نیست ولي براي کساني که میخواهن دانش سطحي از Netstat بدست بیارن مفید و میتونن از این دستور و help آن کمک بگیرن ولي من توضیح بیشتري راجب هر دستور میدم .

دستور Netstat -na :

با تایپ کردن این دستور در MS-DOS Prompt تمام پورتهایي که داده ها و بسته ها را میفرستن مشخص میشه ، نشان " na " در تمام دستورات به معني نمایش همه پورتها و لیست کردن آدرسهاي شبکه و شماره فرمها در یک قالب عددي هستش ، براي مثال من با تایپ این فرمان در MS-DOS این نتایج را گرفتم :

C:\WINDOWS>netstat -na

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:1954	0.0.0.0:0	LISTENING

```
TCP    0.0.0.0:1971           0.0.0.0:0              LISTENING
TCP    0.0.0.0:5101           0.0.0.0:0              LISTENING
TCP    64.110.148.59:1954     207.46.106.21:1863     ESTABLISHED
TCP    64.110.148.59:1971     216.136.225.36:5050    ESTABLISHED
TCP    64.110.148.59:2031     63.121.106.74:80       TIME_WAIT
TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING
UDP    0.0.0.0:1958                                  *:*
UDP    64.110.148.59:9                               *:*
UDP    64.110.148.59:137                             *:*
UDP    64.110.148.59:138                             *:*
UDP    127.0.0.1:1037                                *:*
UDP 127.0.0.1:1074 *:*
```

خب ميبينيد كه پورتهاي باز روي سيستم من ليست شده مثل ۱۸۵۴-۱۹۷۱-۲۰۳۱ ... اين دستور همان دستور Netstat -an هست كه هر ۲ تا يک عمل را انجام ميدن و كارشون اينه كه پورتها را با معادل عددیشان نشان ميدن مثلاً پورت Netbios را با معادل عدديش يعني ۱۳۹ نشان ميدن ، درست مثل دستور Netstat -n كه آيپي ها را با معادل عدديشان نشان ميداد ، اين دستور پورتها را با معادل عددي نشان ميده .

دستور Netstat -a :

اين دستور نيز مثل دستور Netstat -an يا na- عمل ميكنه فقط فرقش در اينه كه اين دستور پورتها را با معادل اسميشان نشان ميده ، براي مثال پورت ۱۳۹ را با معادل اسميش يعني Netbios نشان ميده و همچنين مانند دستور Netstat اسم صاحب سيستم را هم نشان ميده ، مثلاً من با تايپ اين دستور در MS-DOS به اين نتايج سيدم :

```
C:\WINDOWS>netstat -a
Active Connections

Proto  Local Address          Foreign Address        State
TCP    behrooz:2055           BEHROOZ:0              LISTENING
TCP    behrooz:5101           BEHROOZ:0              LISTENING
TCP    behrooz:2047           BEHROOZ:0              LISTENING
TCP    behrooz:2055           cs43.msg.sc5.yahoo.com:5050 ESTABLISHED
TCP    behrooz:nbsession      BEHROOZ:0              LISTENING
TCP    behrooz:2047           baym-cs21.msgr.hotmail.com:1863 ESTABLISHED
TCP    behrooz:1025           BEHROOZ:0              LISTENING
UDP    behrooz:2053                                  *:*
UDP    behrooz:discard                               *:*
UDP    behrooz:nbname                                *:*
UDP    behrooz:nbdatagram                            *:*
UDP    behrooz:nfs                                   *:*
UDP behrooz:1037 *:*
```

خب همانطور كه ملاحظه ميكنيد بعضي از پورتهاي اصلي با معادل اسمي نشان داده شدن مثل پورت nbsession ولي اين دستور براي تست كردن نقطه ضعفها و پورتهاي باز در سيستم خودمان خيلي مفيده و اگر سيستم آلوده به تروجن بود ميشه از اين دستورها و كلاً برنامه Netstat اين موضوع را فهميد ، پس آنهايي كه سوال ميكنن ما چطوري بفهميم سيستم خودمان آلوده به تروجن هست يا نه ، استفاده از اين دستور و كلاً دستورات Netstat ميتونه خيلي بهشون كمک كنه .

خب تا اينجا شد ۴ تا دستور ، اين ۴ تا دستور تمام ارتباطهاي شما در شبكه را در MS-DOS نشان ميده ولي مخصوص پروتكل خاصي نبود ، يعني آيپي و پورتها را در TCP - UDP , ... نشان ميداد ولي حالا ميخوام يک دستور ديگه Netstat را بهتون معرفي كنم كه بايد خود شما پروتكل را انتخاب كنيد تا

ارتباطهاي شما را در آن پروتكل نشان بده .

دستور xxx -p Netstat :
منظور از xxx يعني آن پروتكلي كه شما در نظر داريد كه ميتونه TCP و UDP باشه ، من با تايپ اين دستور در MS-DOS به اين نتيجه رسيدم :

```
C:\WINDOWS>netstat -p TCP

Active Connections

Proto  Local Address          Foreign Address        State
TCP    behrooz:1030   baym-cs12.msgr.hotmail.com:1863  ESTABLISHED
TCP    behrooz:1036   cs46.msg.sc5.yahoo.com:5050      TIME_WAIT
TCP    behrooz:1059   svcs.microsoft.com:80            TIME_WAIT
TCP    behrooz:1060   msntoday.msn.com:80              TIME_WAIT
TCP    behrooz:1063   207.46.134.30:80                 TIME_WAIT
TCP    behrooz:1067   207.46.134.30:80                 TIME_WAIT
TCP    behrooz:1073   digital-island-bos-37.focaldata.net:80  CLOSE_WAIT
IT
TCP    behrooz:1074   digital-island-bos-37.focaldata.net:80  CLOSE_WAIT
IT
TCP    behrooz:1077   cs46.msg.sc5.yahoo.com:5050      ESTABLISHED
TCP    behrooz:1087   64.124.82.13.akamai.com:80       ESTABLISHED
TCP behrooz:1111 64.124.82.21.akamai.com:80 ESTABLISHED
```

كه همانطور كه مشاهده ميكنيد من ارتباطم را در پروتكل TCP امتحان كردم براي مثال با MSN Messanger با پورت ۱۸۶۳ و با آدرس baym-cs12.msgr.hotmail.com ارتباط برقرار كردم و شما اگر ميخواين آيپي اين سرور را بفهمين ميتونين از دستور Netstat -n استفاده كنيد و آيپي كه قبل از پورت ۱۸۶۳ در آن دستور مشاهده ميكنيد آيپي اين سرور هست .

دستور -e Netstat :
اين دستور نيز يكي از دستورات Netstat هستش كه آماري از ارتباطها و بسته ها و شماره هاي ارسال و ذخيره بسته ها و داده ها را نشان ميده ، من با تايپ دستور Netstat -e در MS-DOS Prompt اين نتايج را گرفتم :

```
C:\WINDOWS>netstat -e
Interface Statistics

                           Received            Sent

Bytes                      628308              224952
Unicast packets            2288                2218
Non-unicast packets        111                 111
Discards                   0                   0
Errors                     0                   0
Unknown protocols 74
```

اين دستور بيشتر براي ويندوزهاي ME۹ - x و همينطور مودمهايي كه آمار بسته ها را نميدن خوبه چون در ويندوز ۲۰۰۰ - XP قسمتي از اين آمار براحتي در اختيار User قرار ميگيره ، شما ميتونين با استفاده از اين دستور ترافيک ISP و شبكه را ببينيد و همينطور برنامه هايي كه داريد دانلود ميكنيد را چک كنيد و يا

اگر بسته اي در ارسالش مشكلي پيش بياد ميتونين در قسمت Errors مشاهده كنيد ، ...

دستور Netstat -r :

اين دستور توسط كاربران معمولي اينترنت زياد بكار گرفته نميشه چون درک بعضي از گزينه هاش براي كاربران عادي دشوار ، بحرحال اين دستور جزييات دقيقي مثل آدرس Gateway - Interface Metric - Netmask , ... درباره آدرس آيپيتون در شبكه ميده ، همچنين در ويندوزهاي ME۹ - x كار دستور Netstat -a روهم انجام ميده ، براي هكينگ نيز اين دستور و كلاً اطلاعات Tables Routing مهم و مفيده ، من با تايپ اين دستور اين نتايج را گرفتم :

```
D:\>netstat -r

Route Table
===========================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2000003 ...00 53 45 00 00 00 ..... WAN (PPP/SLIP) Interface
===========================================
===========================================
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 64.110.148.61 64.110.148.61 1
64.110.148.48 255.255.255.255 64.110.148.61 64.110.148.61 1
64.110.148.61 255.255.255.255 127.0.0.1 127.0.0.1 1
64.255.255.255 255.255.255.255 64.110.148.61 64.110.148.61 1
127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1
224.0.0.0 224.0.0.0 64.110.148.61 64.110.148.61 1
Default Gateway: 64.110.148.61
===========================================
Persistent Routes:
None
```

كه البته اين دستور را من در ويندوز ۲۰۰۰ استفاده كردم و اگر شما در ويندوز ME يا x۹ اين دستور را تايپ كنيد نتايج بيشتري از ارتباطهايتان خواهيذ گرفت .

خب دوستان اين دستورهايي كه راجبشون توضيح دادم معروفترين و پركاربردترين دستورهاي Netstat بود ولي بجز اينها دستورهاي ديگري هم وجود داره كه ديگه فكر نكنم توضيح راجب آنها ضروري بنظر برسه ولي براي اينكه خود شما هم تمريني كرده باشين اين دستور را تست كنيد : Netstat -s و ببينيد كه چه اطلاعاتي ميتونيد با دادن اين دستور بدست بيارين .

موفق باشين

برگرفته از سايت برنامه نويس

www.PishgamSoft.com