آموزش کامل netstat و تمام دستورات آن

در این مقاله میخوام راجب برنامه Netstat و دستورات آن کمي توضیح بدم تا شما یک آشنایي با این برنامه داشته باشین ، خب بچه ها هر وقت صحبت از Netstat میشه همه به یاد فرمان n-Netstat مي افتن غافل از اینکه Netstat دستورات زیادي داره که بعضي از آنها به یک هکر کمکهاي زیادي میکنه که من تمام دستورها را براتون توضیح میدم ولي قبلش باید بفهمیم که اصلاً Netstat چیه و چکار میکنه ؟

Netstat هم مثل Netbios یک برنامه خدماتي هست که در خود سیستم عاملها گذاشته شده ، مثلاً در ویندوز x9 و eM در پوشه \Windows با اسم exe.Netstat قرار گرفته و در ویندوزهاي بر پایه NT مثل 2000 نیز در پوشه 32System\WinNT\:D قرار گرفته و کلاً براي نمایش تمام ارتباطات ما در شبکه و فهمیدن پورتها و آیپي هاي سیستمها و ماشین هایي که ما با آنها در ارتباط هستیم بکار میره ، براي استفاده از Netstat احتیاج به هیچ برنامه کمکي و اضافي ندارین

فقط کافیه به DOS Prompt-MS برین و دستوراتي که در ادامه این مقاله میگم را تایپ کنید ، ولي خب برنامه هاي زیادي براي استفاده آسان تر از Netstat آمده که احتیاجي به رفتن در Dos-Ms نداره و کار کاربران اینترنت و شبکه را راحت تر کرده که یکي از بهترین برنامه ها براي اینکار Netstat-X هست که اطلاعات زیادي از ارتباطهاي شما وقتي که به شبکه وصل هستین میده ، درست مثل برنامه exe.Netstat ولي به صورت گرافیکي و تحت ویندوز .

این برنامه همچنین سیستمهایي که از خارج سعي میکنن به سیستم شما وصل بشن را هم نشان میده و آیپي آنها را مشخص میکنه ، درست مثل یک فایروال و همچنین پورتهاي Local و Remote و پروتکل هایي که شما با آنها ارتباط دارین را مشخص میکنه .

Netstat-X بر_7cي کاربران معمولي نسخه Standard را عرضه کرده که جدیدترین نسخه Netstat Standard-X ورژین Beta 5.0 هست و براي کاربران حرفه اي مثل شما نیز Netstat Professional-X را ارائه داده که جدیدترین نسخه آن 4.0 هست که براي مدیران شرکتها نیز مفیده ، شما میتون http:\\www.freshsw.com\files\xnsp400 exe.

خب این یکي از برنامه هاي مفیدي هست که مربوط به Netstat بود ولي حالا توضیح درباره دستورات خود Netstat :

دستور Netstat : دستور Netstat فرمان اصلي این برنامه هست که با تایپ این دستور شما متوجه آیپي سیستمها و پورتهایي که با آنها در ارتباط هستین بدست میارین و همچنین مشاهده میکنین که پورتهایي Listening و یا Established هستن و چه چیزي روي پورتهاي مختلف در حال شنیده شدن هست که خب این باعث میشه اگر پورتي مخصوص یک تروجن مثل 27374 که پورت اصلي 7Sub هست در سیستم شما باز بود شما متوجه این پورت باز بروي سیستمتان بشین.

اگر در قسمتdressForeign Ad هم یک آیپي بوسیله آن پورت به سیستم شما وصل بود شما میفهمین که یک نفر با آن آیپي در سیستم شماست ، پس این یک راهي هست که متوجه بشین سیستمتان آسیب پذیر هست یا نه ، براي مثال من با تایپ دستور Netstat در Dos-Ms این نتایج 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 میکنید این دستور گاهي اوقات اسم صاحب سیستم کلاینتي که شما با آن در ارتباط هستین را نیز میده و چون اینجا من با کسي در PM نبودم اسم کسي را نمیبینید ولي اگر کسي با من چت کنه و دستور

Netstat را بزنه اسم بهروز را میبینه و متوجه میشه که این صاحب آن سیستم کلاینتي هست که داره با آن چت میکنه و همچنین مشخصه که من با پورت 5050 با یاهو مسنجر ارتباط برقرار کردم و همچنین نتایجي که در زیر Local Address مشخص اطلاعاتي درباره خود من هست :

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

و نتایجي که در ssForeign Addre بدست میاد مشخص میکنه که ما با چه سرور یا کلاینتي در ارتباطیم که در سطر دوم مثال بالا یعني 63.123.44.222:80 که آیپي سایت یاهو هست من در سایت یاهو بودم و به وسیله پورت 80 که پورت Http هست من با این وب سرور ارتباط برقرار کردم و در قسمت Status هم مشخص میشه که شما با چه پورتهایي Established هستین.

یعني ارتباط برقرار کردین و وصل هستین و چه پورتهایي Listening یا منتظر Request و در حال شنیدن هستن ، بنابراین میشه با دستور Netstat یک عمل مانیتورینگ از تمام آیپي ها - پورتها و ماشینهایي که شما با آنها در ارتباطین گرفت .

دستور n-Netstat :

همانطور که در بالا توضیح دادم میشه با استفاده از Netstat آیپي و پورت سیستمي که شما با آن در ارتباطین را بدست آورد حتا میشه آیپي کسي داره با شما از طریقه PM در مسنجر چت میکنه را هم بدست آورد چون وقتي شما مسنجرها را باز میکنید با یک پورت خاصي شما با مسنجر ارتباط برقرار میکنین که مثلاً شما با پورت 5050 با یاهو مسنجر ارتباط برقرار میکنین .

شما با استفاده از دستور n-Netstat که در DOS-MS تایپ میکنین میتونین آیپي طرف را بدست بیارین اگرچه من چند وقت پیش برنامه ProPort را معرفي کردم که اینکار را با قابلیتهاي بیشتري انجام میده ولي با این دستور هم میشه اینکار را کرد .

اگر شما بعد از تایپ این دستور و در نتیجه بدست آمده در قسمت Foreign Address با آیپي سیستمي بوسیله پورت 5101 ارتباط برقرار کرده بودین مطمئن باشین آن آیپي براي کسي هست که داره با شما چت میکنه مثلاً من با تایپ دستور n-Netstat این نتایج 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 213.102.29.137 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 2 دستور Netstat و n-Netstat معرفي میکردم چون این دستور راهنما یا Help برنامه Netstat هست که با تایپ کردن آن شما یک صفحه کامل راجب فرمان etstatN 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 اين تمام دستورات Netstat نيست و كلاً Help كاملي نيست ولي براي كساني كه ميخواهن دانش سطحي از Netstat بدست بيارن مفيد و ميتونن از اين دستور و help آن كمک بگيرن ولي من توضيح بيشتري راجب هر دستور ميدم .

دستور na-Netstat :

با تايپ كردن اين دستور در ptDOS Prom-MS تمام پورتهايي كه داده ها و بسته ها را ميفرستن مشخص ميشه ، نشان " na " در تمام دستورات به معني نمايش همه پورتها و ليست كردن آدرسهاي شبكه و شماره فرمها در يک قالب عددي هستش ، براي مثال من با تايپ اين فرمان در DOS-MS اين نتايج 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 1854-1971-2031 ... اين دستور همان دستور an-Netstat هست كه هر 2 تا يک عمل را انجام ميدن و كارشون اينه كه پورتها را با معادل عدديشان نشان ميدن مثلاً پورت Netbios را با معادل عدديش يعني 139 نشان ميدن ، درست مثل دستور n-Netstat كه آيپي ها را با معادل عدديشان نشان ميداد ، اين دستور پورتها را با معادل عددي نشان ميده .

دستور a-Netstat :

این دستور نیز مثل دستور an-Netstat یا -na عمل میکنه فقط فرقش در اینه که این دستور پورتها را با معادل اسمیشان نشان میده ، براي مثال پورت 139 را با معادل اسمیش یعني Netbios نشان میده و همچنین مانند دستور Netstat اسم صاحب سیستم را هم نشان میده ، مثلاً من با تایپ این دستور در DOS-MS به این نتایج سیدم :

```
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 که ملاحظه میکنید بعضي از پورتهاي اصلي با معادل اسمي نشان داده شدن مثل پورت nbsession ولي این دستور براي تست کردن نقطه ضعفها و پورتهاي باز در سیستم خودمان خیلي مفیده و اگر سیستم آلوده به تروجن بود میشه از این دستورها و کلاً برنامه Netstat این موضوع را فهمید ، پس آنهایي که سوال میکنن ما چطوري بفهمیم سیستم خودمان آلوده به تروجن هست یا نه ، استفاده از این دستور و کلاً دستورات Netstat میتونه خیلي بهشون کمک کنه .

خب تا اینجا شد 4 تا دستور ، این 4 تا دستور تمام ارتباطهاي شما در شبکه را در DOS-MS نشان میده ولي مخصوص پروتکل خاصي نبود ، یعني آیپي و پورتها را در TCP- UDP , ... نشان میداد ولي حالا میخوام یک دستور دیگه Netstat را بهتون معرفي کنم که باید خود شما پروتکل را انتخاب کنید تا ارتباطهاي شما را در آن پروتکل نشان بده .

دستور xxx-Netstat p :

منظور از xxx یعني آن پروتکلي که شما در نظر دارین که میتونه TCP و UDP باشه ، من با تایپ این دستور در MS-DOS به این نتیجه رسیدم :

```
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
```

که همانطور که مشاهده میکنید من ارتباطم را در پروتکل TCP امتحان کردم براي مثال با MSN Messanger با پورت 1863 و با آدرس com.hotmail.msgr.12cs-baym ارتباط برقرار کردم و شما اگر میخواین آیپي این سرور را بفهمین میتونین از دستور n-Netstat استفاده کنید و آیپي که قبل از پورت 1863 در آن دستور مشاهده میکنید آیپي این سرور هست .

دستور e-Netstat :

این دستور نیز یکي از دستورات Netstat هستش که آماري از ارتباطها و بسته ها و شماره هاي ارسال و ذخیره بسته ها و داده ها را نشان میده ، من با تایپ دستور e-Netstat در DOS Prompt-MS این نتایج 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
```

این دستور بیشتر براي ویندوزهاي ME -x 9 و همینطور مودمهایي که آمار بسته ها را نمیدن خوبه چون در ویندوز XP - 2000 قسمتي از این آمار براحتي در اختیار User قرار میگیره ، شما میتونین با استفاده از این دستور ترافیک ISP و شبکه را ببینید و همینطور برنامه هایي که دارین دانلود میکنید را چک کنید و یا اگر بسته اي در ارسالش مشکلي پیش بیاد میتونین در قسمت Errors مشاهده کنید ، ...

دستور r-Netstat :

این دستور توسط کاربران معمولي اینترنت زیاد بکار گرفته نمیشه چون درک بعضي از گزینه هاش براي کاربران عادي دشوار ، بحرحال این دستور جزییات دقیقي مثل آدرس Gateway- Netmask-Interface Metric , ... درباره آدرس آیپیتون در شبکه میده ، همچنین در ویندوزهاي ME -x 9 کار دستور a-Netstat روهم انجام میده ، براي هکینگ نیز این دستور و کلاً اطلاعات Routing Tables مهم و مفیده ، من با تایپ این دستور این نتایج 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

که البته اين دستور را من در ويندوز 2000 استفاده كردم و اگر شما در ويندوز ME يا x9 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 : s-Netstat و ببينيد كه چه اطلاعاتي ميتونيد با دادن اين دستور بدست بيارين .