بسمه تعالی

دستـــورات Netstat

سلام دوستان ، در این مقاله میخوام راجع به برنامه Netstat و دستورات آن کمی توضیح بدم تا شما یک آشنایی با این برنامه داشته باشین.

دستور Netstat فرمان اصلی این برنامه هست که با تایپ این دستور شما IP سیستمها و پورتهایی که با آنها در ارتباط هستین بدست میارین و همچنین مشاهده میکنین که چه پورتهایی Listening و یا Established هستن و چه چیزی روی پورتهای مختلف در حال شنیده شدن هست که خب این باعث میشه اگر پورتی مخصوص یک تروجن مثل ۲۷۳۷٤ که پورت اصلی Sub7 هست در سیستم شما باز بود شما متوجه این پورت باز بروی سیستمتان بشین.
(زمانی که یه session برگزار میشه،حالت یا stateمون established است پس در نتیجه اون پورتهایی که شماره هاش روبروی IP آدرسها نوشته شده باز شدند که session و ارتباطمون برقرار شدند.
شماره پورتی که روبروی آدرس local نوشته شده پورت باز شده در کامپیوتر مبدا و شماره پورتی که در foreign نوشته شده پورت باز شده در سیستم مقصد رو نشون میده.)
اگر در قسمتForeign Address هم یک آیپی بوسیله آن پورت به سیستم شما وصل بود شما میفهمین که یک نفر با آن آیپی در سیستم شماست ، پس این یک راهی هست که متوجه بشین سیستمتان آسیب پذیر هست یا نه ، برای مثال من با تایپ دستور Netstat در Ms-Dos این نتایج را گرفتم :

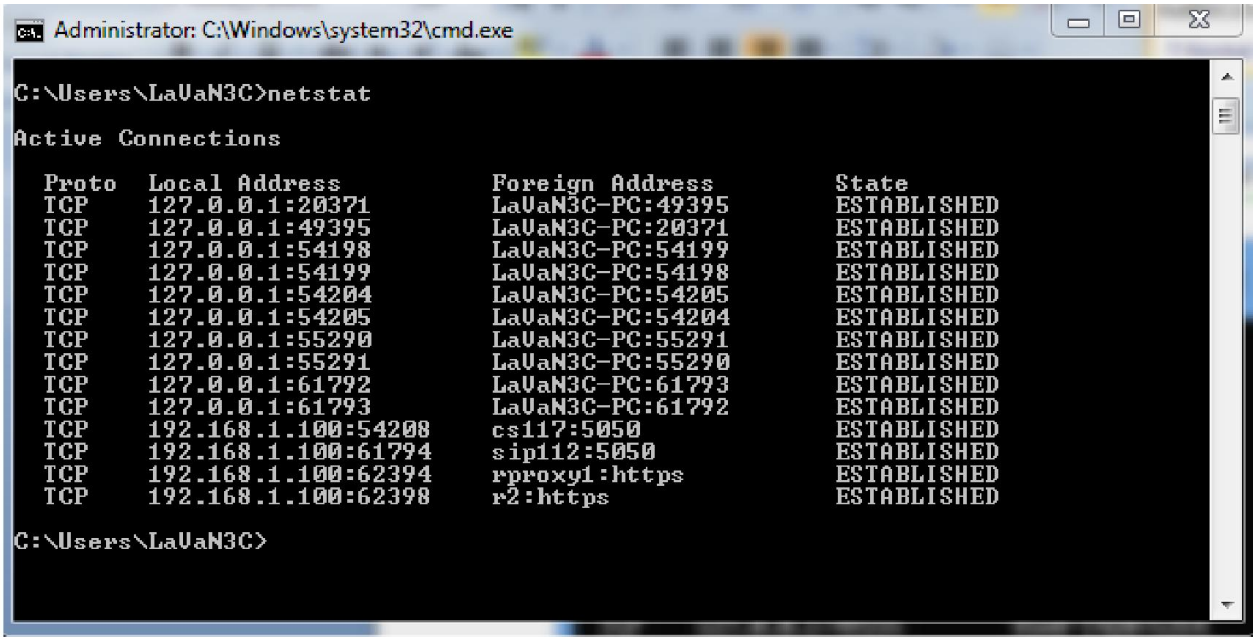
```
C:\Users\LaVaN3C>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1: 1454 cs33.msg.sc5.yahoo.com:5050 ESTABLISHED
  TCP    127.0.0.1: 1488 63.123.44.222:80            ESTABLISHED
  TCP    127.0.0.1: 1491 opi1.vip.sc5.yahoo.com:80   TIME_WAIT
  TCP    127.0.0.1: 1497 64.187.54.23:80             ESTABLISHED
  TCP    127.0.0.1: 1498 64.187.54.23:80             ESTABLISHED
```

این دستور گاهی اوقات اسم صاحب سیستم کلاینتی که شما با آن در ارتباط هستین را نیز میده و چون اینجا من با کسی در PM نبودم اسم کسی را نمیبینید ولی اگر کسی با من چت کنه و دستور Netstat را بزنه اسم LaVaN3C را میبینه و متوجه میشه که این صاحب آن سیستم کلاینتی هست که داره با آن چت میکنه و همچنین مشخصه که من با پورت ۵۰۵۰ با یاهو مسنجر ارتباط برقرار کردم و همچنین نتایجی که در زیر Local Address مشخص اطلاعاتی درباره خود من هست :

```
IP/Hostname:Port open ===> LaVaN3C:1488
```

و نتایجی که در Foreign Address بدست میاد مشخص میکنه که ما با چه سرور یا کلاینتی در ارتباطیم که در سطر دوم مثال بالا یعنی ٦٣.١٢٣.٤٤.٢٢٢:٨٠ که آیپی سایت یاهو هست من در سایت یاهو بودم و به وسیله پورت ٨٠ که پورت Http هست من با این وب سرور ارتباط برقرار کردم و در قسمت Status هم مشخص میشه که شما با چه پورتهایی Established هستین یعنی ارتباط برقرار کردین و وصل هستین و چه پورتهایی Listening یا منتظر Request و در حال شنیدن هستن .
بنابراین میشه با دستور Netstat یک عمل مانیتورینگ از تمام آیپی ها – پورتها و ماشینهایی که شما با آنها در ارتباطین گرفت .

Netstat دستورات زیادی داره که بعضی از آنها به یک هکر کمکهای زیادی میکنه که من دستورها را براتون توضیح میدم ولی قبلش باید بفهمیم که اصلاً Netstat چیه و چکار میکنه ؟
این دستور وضعیت پروتکل‌ها و پورت‌های ارتباطی TCP/IP را نمایش می دهد.
در صورتی که این دستور بدون هیچ سوئیچی استفاده شود ، این دستور کلیه پورت‌ها و ارتباطات خروجی فعال را نمایش می دهد.
چندین نوع سوئیچ با این دستور می توانید بکار ببرید که نوع خروجی را مشخص می کنند. در ادامه با برخی از این سوئیچ‌ها آشنا خواهید شد.



دستور netstat برای نمایش وضعیت پورت‌ها در هردوپروتکل TCP و UDPبکار می رود و ارتباطات به خارج و به درون را نمایش می دهد. وقتی که از این دستور بدون سوئیچ استفاده می کنید، چهار گونه اطلاعات به شما نمایش داده می شود:

١- لیست پروتکل‌های استفاده شده و TCPو UDP
٢- آدرسهای کامپیوتر لوکال و پورت‌های استفاده شده
٣- آدرس‌های خارجی و پروتکل‌های استفاده شده در آنها
٤- وضعیت ارتباط و اینکه آیا پورتی استفاده شده یا خیر

ESTABLISHED :یعنی پس از انجام SYN ،ارتباط در حال حاضر به طور کامل برقرار است.
TIME-WAIT:بعد از بستن یک فعالیت ،کلاینت در این وضعیت قرار می گیرد.
LISTENING :سرور در انتظار یک ارتباط است.

لازمه ی درک مفهوم دستور NBTSTAT ،آشنایی با NETBIOS می باشد .از اینرو در ابتدا به بررسی ساختار NETBIOS می پردازیم.
(netbios یک پروتکل تقریبا قدیمی است که اگر در ویندوز فعال باشد از پورتهای ۱۳۷و۱۳۸و۱۳۹ استفاده می کند که در واقع پورت مهم و اصلی پورت TCP یا ۱۳۹ است.
پورت ۱۳۷ برای name service
و پورت ۱۳۸ برای datagram service می باشد.
این پروتکل در واقع هیچ کار تحت شبکه ای انجام نمی دهد و فقط خیلی راحت یک اسم برای سیستم شما در نظر می گیرد که ۱٦ کاراکتر است. این سرویس را IBM طراحی و سپس Microsoft آن را برای استفاده در سیستم عامل های مبنی بر شبکه پذیرفت .البته لازم به ذکر است که این پروتکل مبتنی بر پروتکل TCP/IP کار میکند و از آن پیروی میکند.)

Netstat هم مثل Netbios یک برنامه خدماتی هست که در خود سیستم عاملها گذاشته شده ، مثلاً در ویندوز xp و Me در پوشه **Windows** با اسم Netstat.exe قرار گرفته و در ویندوزهای بر پایه NT مثل ۲۰۰۰ نیز در پوشه **D:\WinNT\System32** قرار گرفته و کلاً برای نمایش تمام ارتباطات ما در شبکه و فهمیدن پورتها و IP های سیستمها و ماشین هایی که ما با آنها در ارتباط هستیم بکار میره.

برای استفاده از Netstat احتیاج به هیچ برنامه کمکی و اضافی ندارین فقط کافیه به MS-DOS Prompt برین و دستوراتی که در ادامه این مقاله میگم را تایپ کنید.

دستور : Netstat/?
این دستور راهنما یا Help برنامه Netstat هست که با تایپ کردن آن شما یک صفحه کامل راجب فرمان Netstat میبینین و توضیح مختصری هم در جلوی 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.

a- ارتباطات جاری و پورت‌هایی که در حال listen هستند را نمایش می دهد.

e- وضعیت اترنت را نمایش می دهد

n- لیستی عددی از آدرس‌ها و پورت‌ها را نشان می دهد

p- وضعیت ارتباط را تنها درخصوص پروتکلی خاص نمایش می دهد

r-جدول روتینگ را نمایش می دهد

s-وضعیت pre-protocolها را لیست می کند

Interval مشخص کننده مدت زمانی است که باید صبر شود تا وضعیت جدید نمایش داده شود.

البته این تمام دستورات Netstat نیست و کلاً Help کاملی نیست ولی برای کسانی که میخواهن دانش سطحی از Netstat بدست بیارن مفید و میتونن از این دستور و help آن کمک بگیرن ولی من توضیح بیشتری راجب هر دستور میدم .

دستور Netstat -n :

همانطور که در بالا توضیح دادم میشه با استفاده از Netstat آیپی و پورت سیستمی که شما با آن در ارتباطین را بدست آورد حتی میشه آیپی کسی داره با شما از طریقه PM در مسنجر چت میکنه را هم بدست آورد چون وقتی شما مسنجرها را باز میکنید با یک پورت خاصی شما با مسنجر ارتباط برقرار میکنین که مثلاً شما با پورت ۵۰۵۰ با یاهو مسنجر ارتباط برقرار میکنین .

شما با استفاده از دستور Netstat -n که در MS-DOS تایپ میکنین میتونین آیپی طرف را بدست بیارین اگرچه برنامه ProPort اینکار را با قابلیتهای بیشتری انجام میده ولی 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 آیپی سیستمی بوسیله پورت ۵۱۰۱ ارتباط برقرار کرده بودین مطمئن باشین آن آیپی برای کسی هست که داره با شما چت میکنه مثلاً من با تایپ دستور Netstat -n 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 آیپی ۲۱۳.۱۰۲.۲۹.۱۳۷ در حال چت کردن بودم که آیپی خود من هم در قسمت Local Address مشخص میشه ، در قسمت Proto نیز پروتکلی که ما بوسیله آن با یک سیستم ارتباط برقرار کردیم مشخص میشه که اینجا از طریقه پروتکل TCP هستش .

دستور Netstat -na :

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

```
C:\Users\LaVaN3C>netstat -na

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    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49164          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:895          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:896          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1001         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:20371        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:20371        127.0.0.1:49395        ESTABLISHED
  TCP    127.0.0.1:49156        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49160        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49161        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49162        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49395        127.0.0.1:20371        ESTABLISHED
  TCP    127.0.0.1:54198        127.0.0.1:54199        ESTABLISHED
  TCP    127.0.0.1:54199        127.0.0.1:54198        ESTABLISHED
  TCP    127.0.0.1:54204        127.0.0.1:54205        ESTABLISHED
  TCP    127.0.0.1:54205        127.0.0.1:54204        ESTABLISHED
  TCP    127.0.0.1:55290        127.0.0.1:55291        ESTABLISHED
  TCP    127.0.0.1:55291        127.0.0.1:55290        ESTABLISHED
  TCP    127.0.0.1:61792        127.0.0.1:61793        ESTABLISHED
```

```
  TCP    127.0.0.1:61793        127.0.0.1:61792        ESTABLISHED
  TCP    192.168.1.100:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.100:54208    66.196.114.227:5050    ESTABLISHED
  TCP    192.168.1.100:61794    98.138.26.52:5050      ESTABLISHED
  TCP    192.168.1.100:61837    66.196.113.5:443       ESTABLISHED
  TCP    192.168.1.100:62359    66.196.66.213:443      TIME_WAIT
  TCP    192.168.1.100:62360    66.196.66.213:443      ESTABLISHED
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:49152             [::]:0                 LISTENING
  TCP    [::]:49153             [::]:0                 LISTENING
  TCP    [::]:49154             [::]:0                 LISTENING
  TCP    [::]:49155             [::]:0                 LISTENING
  TCP    [::]:49164             [::]:0                 LISTENING
  UDP    0.0.0.0:500*:*
  UDP    0.0.0.0:1900*:*
  UDP    0.0.0.0:4500*:*
  UDP    0.0.0.0:5355*:*
  UDP    127.0.0.1:1900*:*
  UDP    127.0.0.1:55669*:*
  UDP    127.0.0.1:60014*:*
  UDP    127.0.0.1:63820*:*
  UDP    192.168.1.100:137*:*
  UDP    192.168.1.100:138*:*
  UDP    192.168.1.100:1900*:*
  UDP    [::]:500*:*
  UDP    [::]:4500*:*
  UDP    [::]:5355*:*
  UDP    [::1]:1900*:*
  UDP    [::1]:60013*:*
  UDP    [fe80::812f:b115:9122:a7d2%11]:1900*:*
```

خب میبینید که پورتهای باز روی سیستم من لیست شده مثل ٦١٨٣٧-٦١٧٩٤ -٥٤٢٠٨... این دستور همان دستور Netstat -an **هست که هر ۲ تا یک عمل را انجام میدن و کارشون اینه که پورتها را با معادل عددیشان نشان میدن مثلاً پورت** Netbios **را با معادل عددیش یعنی ۱۳۹ نشان میدن ، درست مثل دستور** Netstat -n **که آیپی ها را با معادل عددیشان نشان میداد ، این دستور پورتها را با معادل عددی نشان میده.**

دستور Netstat -a :

این دستور نیز مثل دستور Netstat -an **یا** na- **عمل میکنه فقط فرقش در اینه که این دستور پورتها را با معادل اسمیشان نشان میده ، برای مثال پورت ۱۳۹ را با معادل اسمیش یعنی** Netbios **نشان میده و**

همچنین مانند دستور Netstat **اسم صاحب سیستم را هم نشان میده ، مثلاً من با تایپ این دستور در** MS-DOS **به این نتایج سیدم :**

```
C:\Users\LaVaN3C>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49395        LaVaN3C-PC:20371       ESTABLISHED
  TCP    127.0.0.1:54198        LaVaN3C-PC:54199       ESTABLISHED
  TCP    127.0.0.1:54199        LaVaN3C-PC:54198       ESTABLISHED
  TCP    127.0.0.1:54204        LaVaN3C-PC:54205       ESTABLISHED
  TCP    127.0.0.1:54205        LaVaN3C-PC:54204       ESTABLISHED
  TCP    127.0.0.1:55290        LaVaN3C-PC:55291       ESTABLISHED
  TCP    127.0.0.1:55291        LaVaN3C-PC:55290       ESTABLISHED
  TCP    127.0.0.1:61792        LaVaN3C-PC:61793       ESTABLISHED
  TCP    127.0.0.1:61793        LaVaN3C-PC:61792       ESTABLISHED
  TCP    192.168.1.100:139      LaVaN3C-PC:0           LISTENING
  TCP    192.168.1.100:54208    cs117:5050             ESTABLISHED
  TCP    192.168.1.100:61794    sip112:5050            ESTABLISHED
  TCP    192.168.1.100:62365    rproxy1:https          ESTABLISHED
  TCP    192.168.1.100:62367    93.184.220.29:http     TIME_WAIT
  TCP    192.168.1.100:62368    93.184.220.29:http     TIME_WAIT
  TCP    192.168.1.100:62369    r1:https               ESTABLISHED
  TCP    [::]:135               LaVaN3C-PC:0           LISTENING
  TCP    [::]:445               LaVaN3C-PC:0           LISTENING
  TCP    [::]:49152             LaVaN3C-PC:0           LISTENING
  TCP    [::]:49153             LaVaN3C-PC:0           LISTENING
  TCP    [::]:49154             LaVaN3C-PC:0           LISTENING
  TCP    [::]:49155             LaVaN3C-PC:0           LISTENING
  TCP    [::]:49164             LaVaN3C-PC:0           LISTENING
  UDP    127.0.0.1:2053         *:*
  UDP    192.168.1.100:discard  *:*
  UDP    192.168.1.100:nbname   *:*
  UDP    192.168.1.100:nbdatagram *:*
  UDP    192.168.1.100:nfs      *:*
  UDP    127.0.0.1:1037         *:*
```

همانطور که مشاهده می کنید، خروجی شامل چهار ستون است که پروتکل ، آدرس لوکال ، آدرس خارجی و وضعیت پورت را مشخص می کند. ارتباطات TCP **آدرس های لوکال (محلی) و خارجی و وضعیت ارتباط را مشخص می کند.** UDP **هرچند کمی متفاوت است و آن بدین ترتیب است که تنها پورت استفاده شده نمایش داده شده است و آدرس و وضعیت ارتباط مشخص نمی شود و این به این دلیل است که همانطور که می دانید** UDP **از نوع پروتکل** Connectionless **می باشد. در لیست زیر اطلاعاتی که در اینجا نمایش داده شده است را توضیح می دهم :**

۱- Proto نوع پروتکل استفاده شده را نمایش می دهد
۲- آدرس لوکال نشانگر آدرس شبکه و پورتی است که کامپیوتر ما استفاده کرده است. در صورت دیدن ستاره در این قسمت در می یابیم که ارتباط هنوز ایجاد نشده است.
۳- آدرس خارجی آدرس کامپیوتر مقصد (دور) و پورت آن است. علامت ستاره هم نشانگر این است که ارتباط هنوز برقرار نشده است.
٤- State یا وضعیت : نشانگر وضعیت ارتباطی است که آیا ارتباط ایجاد شده است یا اینکه در حالت های listening یا closed یا waiting**(انتظار) قرار دارد.**

بعضی از پورتهای اصلی با معادل اسمی نشان داده شدن مثل پورت nbsession **ولی این دستور برای تست کردن نقطه ضعفها و پورتهای باز در سیستم خودمان خیلی مفیده و اگر سیستم آلوده به تروجن بود میشه از این دستورها و کلاً برنامه** Netstat **این موضوع را فهمید ، پس آنهایی که سوال میکنن ما چطوری بفهمیم سیستم خودمان آلوده به تروجن هست یا نه ، استفاده از این دستور و کلاً دستورات** Netstat **میتونه خیلی بهشون کمک کنه .**

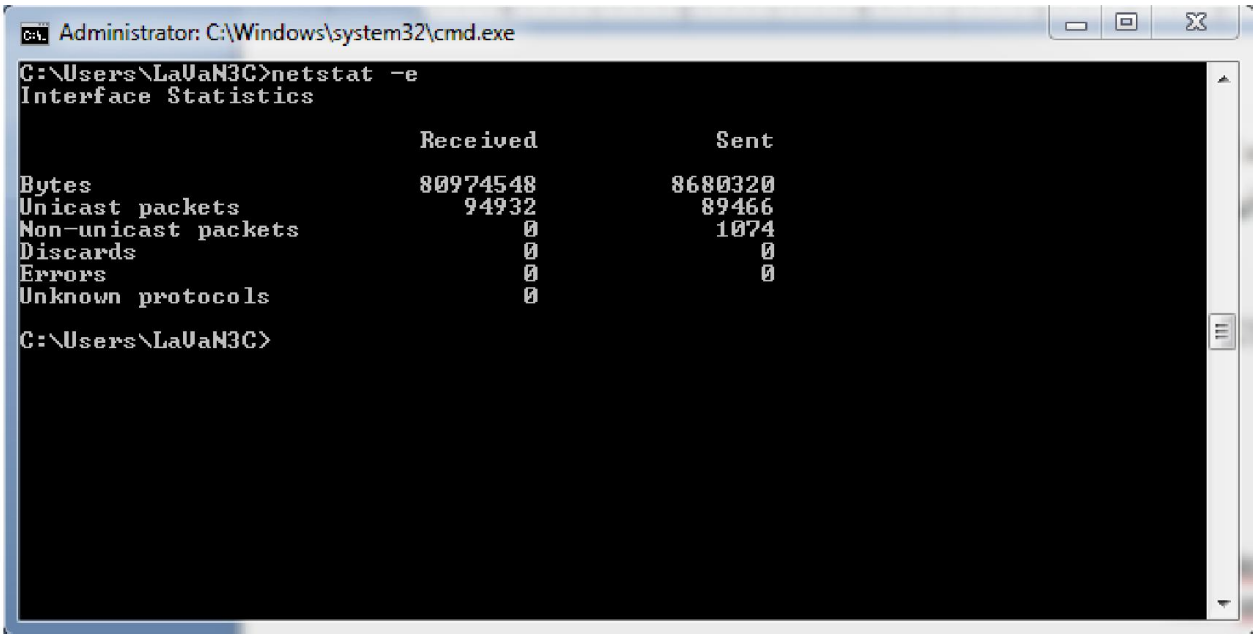
دستور Netstat -p xxx :
منظور از xxx **یعنی آن پروتکلی که شما در نظر دارین که میتونه** TCP **و** UDP **باشه ، من با تایپ این دستور در** MS-DOS **به این نتیجه رسیدم :**

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

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    s4ra:1030              baym-cs12.msgr.hotmail.com:1863  ESTABLISHED
  TCP    s4ra:1036              cs46.msg.sc5.yahoo.com:5050  TIME_WAIT
  TCP    s4ra:1059              svcs.microsoft.com:80   TIME_WAIT
  TCP    s4ra:1060              msntoday.msn.com:80     TIME_WAIT
  TCP    s4ra:1063              207.46.134.30:80        TIME_WAIT
  TCP    s4ra:1067              207.46.134.30:80        TIME_WAIT
  TCP    s4ra:1073              digital-island-bos-37.focaldata.net:80  CLOSE_WAIT
IT
  TCP    s4ra:1074              digital-island-bos-37.focaldata.net:80  CLOSE_WAIT
IT
  TCP    s4ra:1077              cs46.msg.sc5.yahoo.com:5050  ESTABLISHED
  TCP    s4ra:1087              64.124.82.13.akamai.com:80  ESTABLISHED
  TCP    s4ra:1111              64.124.82.21.akamai.com:80  ESTABLISHED
```

که همانطور که مشاهده میکنید من ارتباطم را در پروتکل TCP **امتحان کردم برای مثال با** MSN Messanger **با پورت ۱۸٦۳ و با آدرس** baym-cs12.msgr.hotmail.com **ارتباط برقرار کردم و شما اگر میخواین آیپی این سرور را بفهمین میتونین از دستور** Netstat -n **استفاده کنید و آیپی که قبل از پورت ۱۸٦۳ در آن دستور مشاهده میکنید آیپی این سرور هست .**

دستور Netstat -e :

این دستور نیز یکی از دستورات Netstat هستش که آماری از ارتباطها و بسته ها و شماره های ارسال و ذخیره بسته ها و داده ها را نشان میده ، من با تایپ دستور Netstat -e در MS-DOS Prompt این نتایج را گرفتم :



همانطور که مشاهده می کنید اطلاعات مختلفی در این قسمت مشاهده می شود:

۱ -میزان بایتی از اطلاعات ردوبدل شده از زمانی که کامپیوتر روشن شده است.

۲ -پاکت‌های یونیکستی که به این کامپیوتر ارسال یا دریافت شده است.

۳ -پاکت‌های غیر یونیکس که توسط کارت شبکه دریافت شده است

٤ -پاکت‌های قبول نشده به دلیل خرابی اطلاعاتی

٥ -خطاهای صورت گرفته . این قسمت باید نمایانگر عدد پایینی باشد درصورتیکه عدد بالا باشد نشانگر خرابی در کارت شبکه می تواند باشد.

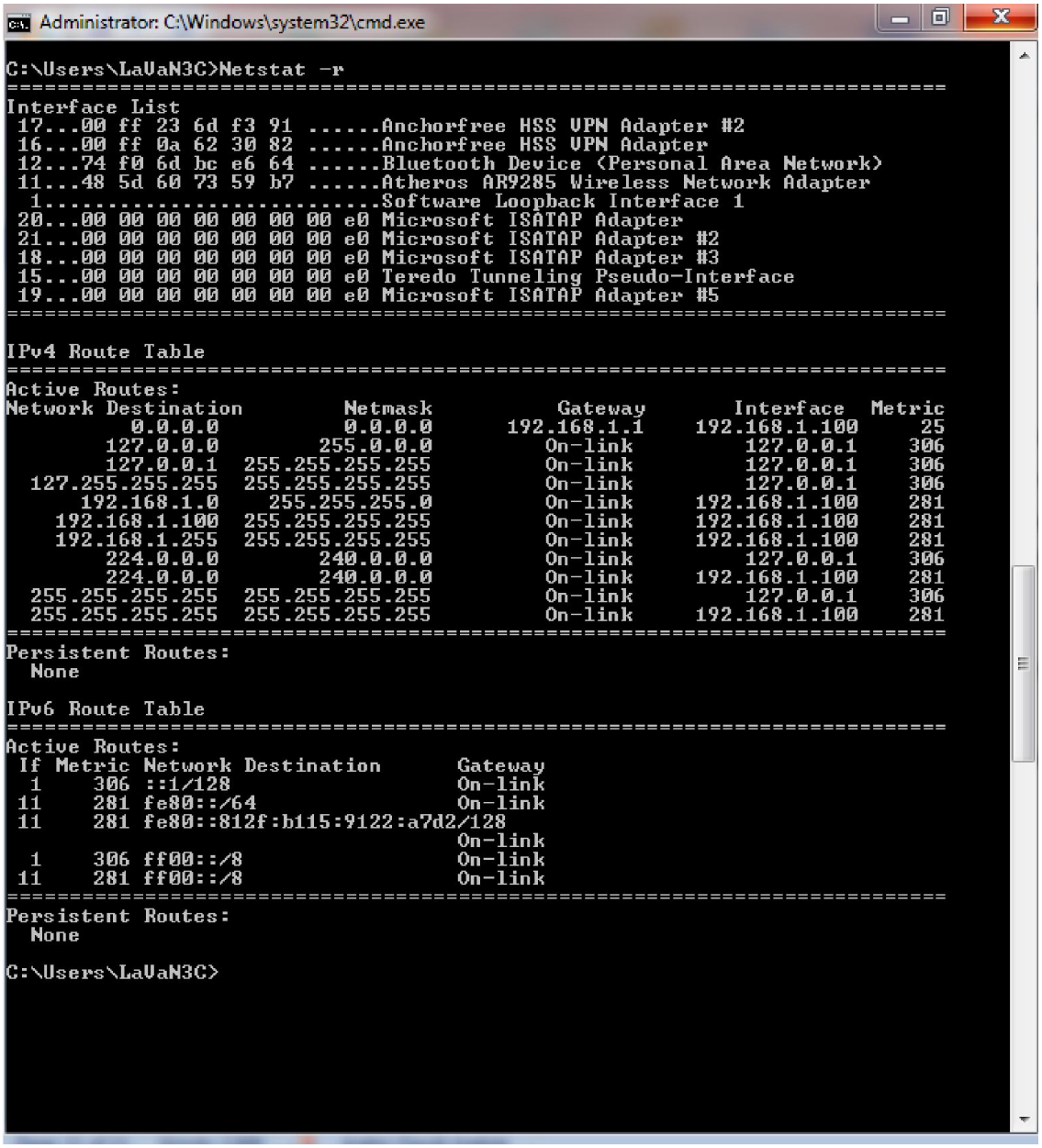
٦ -پروتکل‌های ناشناخته که توسط کامپیوتر شناسایی نشده اند.

این دستور بیشتر برای ویندوزهای XP-ME و همینطور مودمهایی که آمار بسته ها را نمیدن خوبه چون در ویندوز ۲۰۰۰ – XP قسمتی از این آمار براحتی در اختیار User قرار میگیره ، شما میتونین با استفاده از این دستور ترافیک ISP و شبکه را ببینید و همینطور برنامه هایی که دارین دانلود میکنید را چک کنید و یا اگر بسته ای در ارسالش مشکلی پیش بیاد میتونین در قسمت Errors مشاهده کنید ، ...

دستور Netstat -r :

این دستور توسط کاربران معمولی اینترنت زیاد بکار گرفته نمیشه چون درک بعضی از گزینه هاش برای کاربران عادی دشوار ، به هرحال این دستور جزییات دقیقی مثل:

آدرس Netmask -Interface Metric - Gateway , ... درباره آدرس آیپیتون در شبکه میده ، همچنین در ویندوزهای xp - ME کار دستور Netstat -a روهم انجام میده ، برای هکینگ نیز این دستور و کلاً اطلاعات Routing Tables مهم و مفیده ، من با تایپ این دستور این نتایج را گرفتم :



گاهی از این دستور برای نمایش جدول روتینگ کامپیوتر استفاده می شود. سیستم از این جدول برای تشخیص مسیر ترافیک مربوط به TCP استفاده می نماید.

برنامه های زیادی برای استفاده آسان تر از NETSTAT آمده که احتیاجی به رفتن در Ms-Dos ندارد و کار کاربران اینترنت و شبکه را راحت تر کرده که یکی از بهترین برنامه ها برای این کار X-NETSTAT است که اطلاعات زیادی از ارتباط های شما وقتی که به شبکه وصل هستید میدهد،درست مثل برنامه Netstat.exe ولی به صورت گرافیکی و تحت ویندوز.

این برنامه همچنین سیستم هایی که از خارج سعی می کنند به سیستم شما وصل شوند را هم نشان می دهد، IPآنها را مشخص می کند درست مثل یک فایروال.
همچنین پورت های Localو Remote و پروتکل هایی که شما با آنها ارتبط دارید را مشخص می کند.

X-Netstat_C7 **برای کاربران معمولی نسخه** Standard **را عرضه کرده که جدیدترین نسخه آن** X-Netstat Standard **ورژن ۵.۰** Beta **است**
و برای کاربران حرفه ای نیز X-Netstat Professional **را ارائه داده که جدیدترین نسخه آن ٤.۰ است که برای مدیران شرکت ها نیز مفید است.**
شما می توانید این لینک رو دانلود کنید http://www.freshsw.com/files/xnsp400.exe
این یکی از برنامه های مفیدی هست که مربوط به Netstat**میباشد.**

پایان

باتشکر

محبوبه محمودآبادی