

Netbios Over TCP/IP – nbtstat usage in detail – Information Security Newspaper

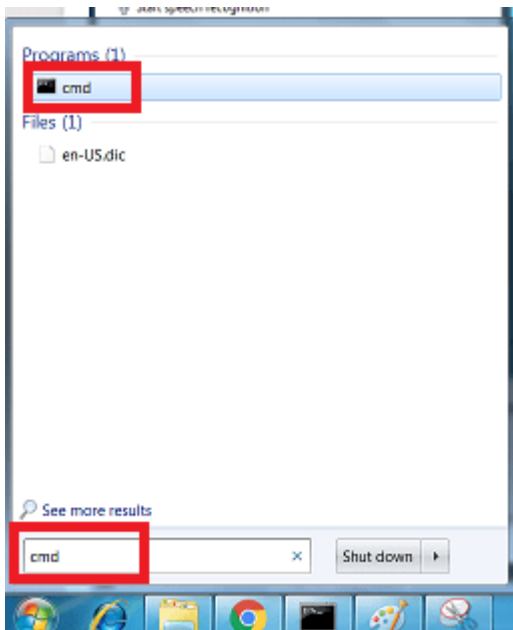
By Jim Gill

Published: 2018-11-28 · Archived: 2026-04-05 23:40:01 UTC

As per ethical hacking professionals, Nbtstat is a network tool that is used to check the running TCP/IP connections. Nbtstat list all the network connections that are used in Windows OS. This tool is pre-installed in Windows you no need use any external software to run nbtstat. It's an effective tool to determine all the TCP/IP connections of the Windows machines.

According the [ethical hacking](#) researcher of iicybersecurity, nbtstat can be used in public wifi networks to gather all the Ip addresses and use them in fingerprinting or attacking on any pubic ip addresses.

- For starting nbtstat.
 - Go to Windows start menu.
 - Type **cmd**.



In order see the TCP/IP connections you must have **IPv4** address to determine TCP/IP connections. You can get **IPv4** by following steps:-

- For getting an IPv4
 - Type **ipconfig** in cmd which will list all your IP configuration.

```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32 ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :

Wireless LAN adapter Wireless Network Connection:

    Connection-specific DNS Suffix . . . . . :
    Link-local IPv6 Address . . . . . : fe80::b99c:49c4:832e:5629%12
    IPv4 Address. . . . . : 192.168.1.100 IPv4 Address
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::ed2:b5ff:fe2c:555c%12
                                192.168.1.1

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :

Tunnel adapter isatap.{B3D926DA-3DC3-4C6C-826E-2180FA8BE22D}:
```

NBTSTAT :-

- For using nbtstat, type **NBTSTAT** in cmd of windows machine. Nbtstat options are case sensitive. please type each command very carefully.

```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>NBTSTAT

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
          [-r] [-R] [-RR] [-s] [-S] [interval] ]

-a (adapter status) Lists the remote machine's name table given its name
-A (Adapter status) Lists the remote machine's name table given its
                    IP address.
-c (cache)          Lists NBT's cache of remote [machine] names and their IP
addresses
-n (names)          Lists local NetBIOS names.
-r (resolved)       Lists names resolved by broadcast and via WINS
-R (Reload)         Purges and reloads the remote cache name table
-S (Sessions)       Lists sessions table with the destination IP addresses
-s (sessions)       Lists sessions table converting destination IP
                    addresses to computer NETBIOS names.
-RR (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refr
esh

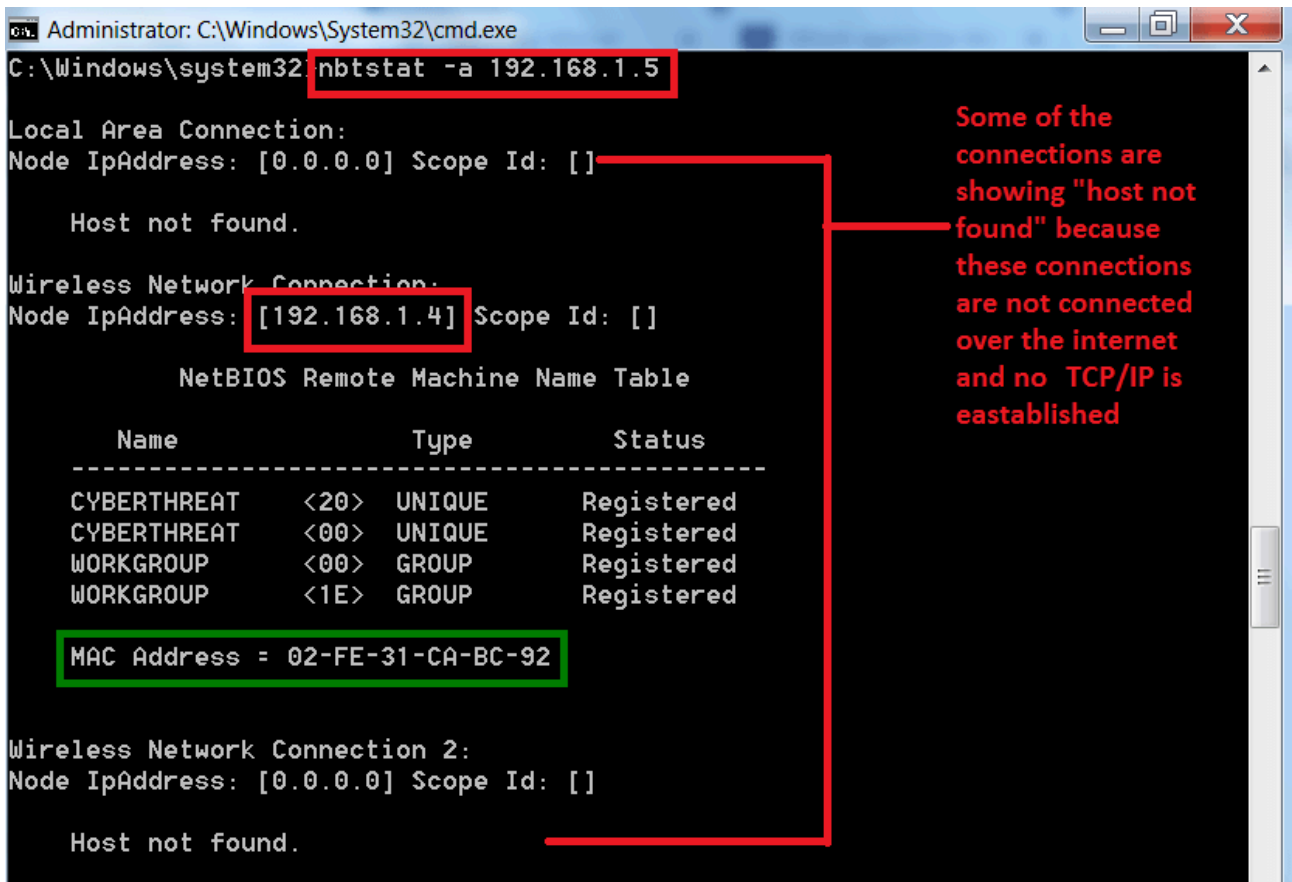
RemoteName      Remote host machine name.
IP address       Dotted decimal representation of the IP address.
interval        Redisplays selected statistics, pausing interval seconds
between each display. Press Ctrl+C to stop redisplaying
statistics.
```

- The above commands can be used to list all the TCP/IP connections in windows machine.

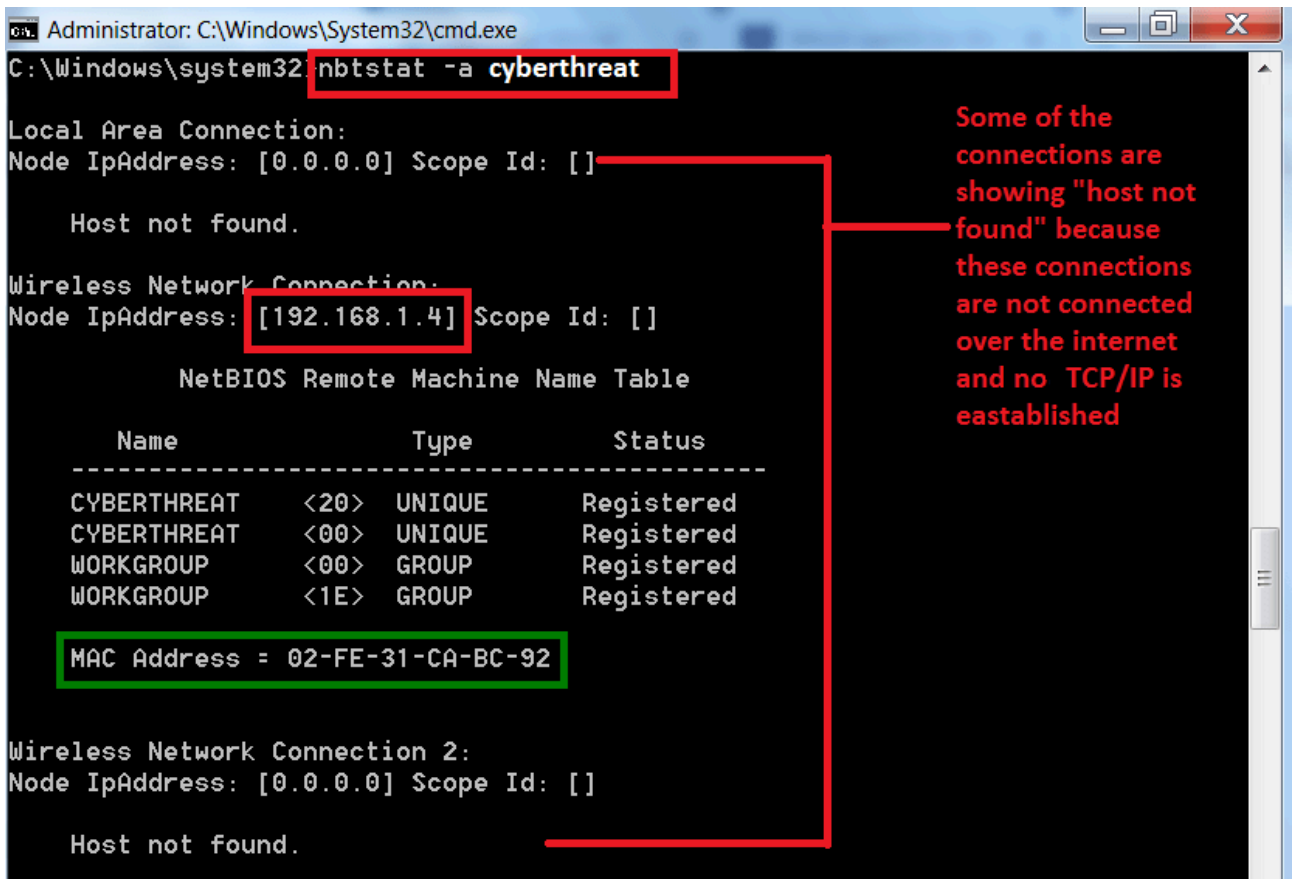
USING -A / -a option in nbtstat :-

- Command – **nbtstat -a / -A <remote name> <Ip address>**. If you use <remote name> <IP address> the output will be same as shown below.
- Type **nbtstat -a 192.168.1.5**

USING IP ADDRESS (192.168.1.5):-



USING AN REMOTE HOST NAME (cyberthreat):-



- After scanning the target IP address, the command also provides the mac address.
- The above information especially the mac address can be use in other hacking activities.

USING -c option in nbtstat :-

- Type `nbtstat -c`

```
C:\Windows\system32 nbtstat -c
Local Area Connection:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Wireless Network Connection:
Node IpAddress: [192.168.1.4] Scope Id: []

                NetBIOS Remote Cache Name Table

-----
Name                Type                Host Address        Life [sec]
-----
JAI-PC              <20>                UNIQUE              192.168.1.2        30
-----

Wireless Network Connection 2:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache
```

These are not captured by -c command. As these Ip address do not stay in cache for longer time.

- As you can see, <-c> has returned with the one ip address. The above IP address can be used in exploiting.
- -c option listnbtstat cache table.

REMOTE CACHE NAME TABLE :-

Name	Type	Host Address	Life [sec]
JAI-PC	<20> UNIQUE	192.168.1.2	220

1. remote user name

2. There are many type like- unique, group. unique define as - main network adapter group define as - groups as another network adapters.

3. IPv4 Address

4. expires in 220 seconds

- **Jai-Pc** (1) is the remote user name .
- Types (2) is used to show IP address it has returned is **unique** or **group**. If it is **unique** that mean its main PC if it is **group** that might be another network adapters which are installed.
- For example if you installed **vmware** or **virtualbox** both of them will install their own network adapters with different MAC/IP addresses.
- IPv4 (3) address – 192.168.1.2
- Life (sec) – (4) is showing 220 that means it will expire in 220 seconds.

USING -n option in netstat:-

- Type **nbtstat -n**
- **<-n>** will list the local netbios names.

```
C:\Windows\system32>nbtstat -n

Local Area Connection:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Wireless Network Connection:
Node IpAddress: [192.168.1.4] Scope Id: []

                NetBIOS Local Name Table

                Name                Type                Status
-----
A-PC             <20>               UNIQUE             Registered
A-PC             <00>               UNIQUE             Registered
WORKGROUP       <00>               GROUP              Registered
WORKGROUP       <1E>               GROUP              Registered

Wireless Network Connection 2:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache
```

- After executing the above command, -n has returned with local netbios names.
- This is helpful to check your computer netbios names. To know how many network adapters are present.

USING -r option in netstat :-

- Type nbtstat -r
- <-r> to list names resolved by broadcast and via WINS.

```
C:\Windows\system32>nbtstat -r

NetBIOS Names Resolution and Registration Statistics
-----

Resolved By Broadcast      = 9
Resolved By Name Server    = 0

Registered By Broadcast    = 7
Registered By Name Server  = 0

NetBIOS Names Resolved By Broadcast
-----

JAI-PC
JAI-PC
JAI-PC
JAI-PC
JAI-PC
CYBERTHREAT <00>
JAI-PC
JAI-PC
```

- After executing the above command, -r has listed the broadcasts names.
- This command returns with no. of users which has been configured to use the WINS and registered using the broadcast.
- **WINS** is used to maintain the mapping of computer names to addresses.



Cyber Security Researcher. Information security specialist, currently working as risk infrastructure specialist & investigator. He is a cyber-security researcher with over 25 years of experience. He has served with the Intelligence Agency as a Senior Intelligence Officer. He has also worked with Google and Citrix in development of cyber security solutions. He has aided the government and many federal agencies in thwarting many cyber crimes. He has been writing for us in his free time since last 5 years.

2018-11-28