Ethical Hacking and Countermeasures
Nbtstat Cheat Sheet

Nbtstat
Source: https://docs.microsoft.com

Nbtstat displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache. Nbtstat allows a refresh of the NetBIOS name cache and the names registered with Windows Internet Name Service (WINS). Used without parameters, nbtstat displays help.

Syntax

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

Nbtstat Parameters

Parameter	Description
`/a`	Displays the NetBIOS name table of a remote computer, where remoteName is the NetBIOS computer name of the remote computer
`/A`	Displays the NetBIOS name table of a remote computer, specified by the IP address (in dotted decimal notation) of the remote computer
`/c`	Displays the contents of the NetBIOS name cache, the table of NetBIOS names and their resolved IP addresses
`/n`	Displays the NetBIOS name table of the local computer. The status of registered indicates that the name is registered either by broadcast or with a WINS server
`/r`	Displays NetBIOS name resolution statistics
`/R`	Purges the contents of the NetBIOS name cache and then reloads the #PRE-tagged entries from the Lmhosts file
`/RR`	Releases and then refreshes NetBIOS names for the local computer that is registered with WINS servers
`/s`	Displays NetBIOS client and server sessions, attempting to convert the destination IP address to a name
`/S`	Displays NetBIOS client and server sessions, listing the remote computers by destination IP address only
`/?`	Displays help at the command prompt
`Interval`	Redisplays selected statistics, pausing the number of seconds specified in Interval between each display. Press CTRL+C to stop redisplaying statistics. If this parameter is omitted, nbtstat prints the current configuration information only once

Nbtstat Commands

Command	Description
`nbtstat /c`	Shows the contents of the NetBIOS name cache, which contains NetBIOS name-to-IP address mappings
`nbtstat /n`	Displays the names that have been registered locally on the system by NetBIOS applications such as the server and redirector
`nbtstat /A 10.0.0.99`	Displays the NetBIOS name table of the remote computer assigned the IP address of 10.0.0.99
`nbtstat /r`	Displays the count of all NetBIOS names resolved by broadcast and by querying a WINS server
`nbtstat /S`	Lists the current NetBIOS sessions and their statuses.
`nbtstat /R`	Used to purge the NetBIOS name cache and reload the #PRE-tagged entries in the local Lmhosts file
`nbtstat /RR`	Release NetBIOS names registered with the WINS server and re-register them
`nbtstat /a CORP07`	Displays the NetBIOS name table of the remote computer with the NetBIOS computer name of CORP07
`nbtstat /S 10`	Display NetBIOS session statistics by IP address every 10 seconds