Cyber Secuirty

**ESERCIZI GUIDATI**linea orizzontale

# 

# Introduzione

PS C:\Users\CyberOpsUser> Get-Alias dir

CommandTypeNameVersionSource

Aliasdir -> Get-ChildItem

PS C:\Users\CyberOpsUser> netstat -h

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]

-a Displays all connections and listening ports.

-b Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions.

<some output omitted>

PS C:\Users\CyberOpsUser> netstat -r

===========================================================================

Interface List

3...08 00 27 a0 c3 53 ......Intel(R) PRO/1000 MT Desktop Adapter

10...08 00 27 26 c1 78 ......Intel(R) PRO/1000 MT Desktop Adapter #2

1...........................Software Loopback Interface 1

===========================================================================

IPv4 Route Table

===========================================================================

Active Routes:

Network Destination Netmask Gateway Interface Metric

0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.5 25

127.0.0.0 255.0.0.0 On-link 127.0.0.1 331

127.0.0.1 255.255.255.255 On-link 127.0.0.1 331

127.255.255.255 255.255.255.255 On-link 127.0.0.1 331

169.254.0.0 255.255.0.0 On-link 169.254.181.151 281

169.254.181.151 255.255.255.255 On-link 169.254.181.151 281

169.254.255.255 255.255.255.255 On-link 169.254.181.151 281

192.168.1.0 255.255.255.0 On-link 192.168.1.5 281

192.168.1.5 255.255.255.255 On-link 192.168.1.5 281

192.168.1.255 255.255.255.255 On-link 192.168.1.5 281

224.0.0.0 240.0.0.0 On-link 127.0.0.1 331

224.0.0.0 240.0.0.0 On-link 192.168.1.5 281

224.0.0.0 240.0.0.0 On-link 169.254.181.151 281

255.255.255.255 255.255.255.255 On-link 127.0.0.1 331

255.255.255.255 255.255.255.255 On-link 192.168.1.5 281

255.255.255.255 255.255.255.255 On-link 169.254.181.151 281

===========================================================================

Persistent Routes:

None

IPv6 Route Table

===========================================================================

Active Routes:

If Metric Network Destination Gateway

1 331 ::1/128 On-link

3 281 fe80::/64 On-link

10 281 fe80::/64 On-link

10 281 fe80::408b:14a4:7b64:b597/128

On-link

3 281 fe80::dd67:9e98:9ce0:51e/128

On-link

1 331 ff00::/8 On-link

3 281 ff00::/8 On-link

10 281 ff00::/8 On-link

PS C:\Windows\system32> netstat -abno

Active Connections

Proto Local Address Foreign Address State PID

TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 756

RpcSs

[svchost.exe]

TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4

Can not obtain ownership information

TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 444

Can not obtain ownership information

TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 440

Schedule

[svchost.exe]

TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 304

EventLog

[svchost.exe]

TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING 1856

[spoolsv.exe]

TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING

PS C:\Users\CyberOpsUser> clear-recyclebin

Confirm

Are you sure you want to perform this action?

Performing the operation "Clear-RecycleBin" on target "All of the contents of the Recycle Bin".

[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y