

Netbios Enumeration

@mmar



What is NetBios

NetBIOS is a legacy networking protocol used for communication between computers on a local area network (LAN). It provides services for naming, browsing, and sharing resources within a network. NetBIOS enables computers to identify each other using **unique names**, establishes sessions between applications, and facilitates file and printer sharing. By enumerating NetBIOS, we can identify **shared resources**, **detect potential vulnerabilities**, and assess the **overall network configuration**.



NetBIOS Ports

- ✓ **UDP port 137:** This port is used for the NetBIOS Name Service (NBNS) or the NetBIOS Name Resolution service. It handles the registration and resolution of NetBIOS names.
- ✓ **UDP port 138:** This port is used for the NetBIOS Datagram service. It supports the transmission of datagram messages between NetBIOS-enabled devices.

NetBIOS over TCP/IP (NBT) can also use TCP **port 139** for session establishment and data transfer.

Nbtstat

(Windows Command line utility)

nbtstat

- ❖ Use the following command on windows to enumerate NetBIOS names for a target

```
>nbtstat -a 192.168.18.110
```

```
WiFi:
Node IpAddress: [192.168.18.11] Scope Id: []

      NetBIOS Remote Machine Name Table

      Name                Type             Status
      -----
METASPLOITABLE <00>    UNIQUE          Registered
METASPLOITABLE <03>    UNIQUE          Registered
METASPLOITABLE <20>    UNIQUE          Registered
@@_MSBROWSE__@<01>    GROUP           Registered
WORKGROUP        <00>           GROUP           Registered
WORKGROUP        <1D>           UNIQUE          Registered
WORKGROUP        <1E>           GROUP           Registered
```

nbtstat

- ❖ We can check the local cache for Netbios with the following command

```
>nbtstat -c
```

```
C:\WINDOWS\system32>nbtstat -c
```

```
WiFi:
Node IpAddress: [192.168.18.11] Scope Id: []

          NetBIOS Remote Cache Name Table

  Name                Type           Host Address      Life [sec]
-----
METASPLOITABLE <20>  UNIQUE        192.168.18.110   572
```

Nmap

Nmap

- ❖ Nmap has a script for Netbios enumeration

```
>nmap -sV -v --script nbstat.nse 192.168.18.110
```

```
>nmap -sU -p 137 --script nbstat.nse 192.168.18.110
```

sV	-	version enumeration
----	---	---------------------

sU	-	udp scan
----	---	----------

Demo



THANKS