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.

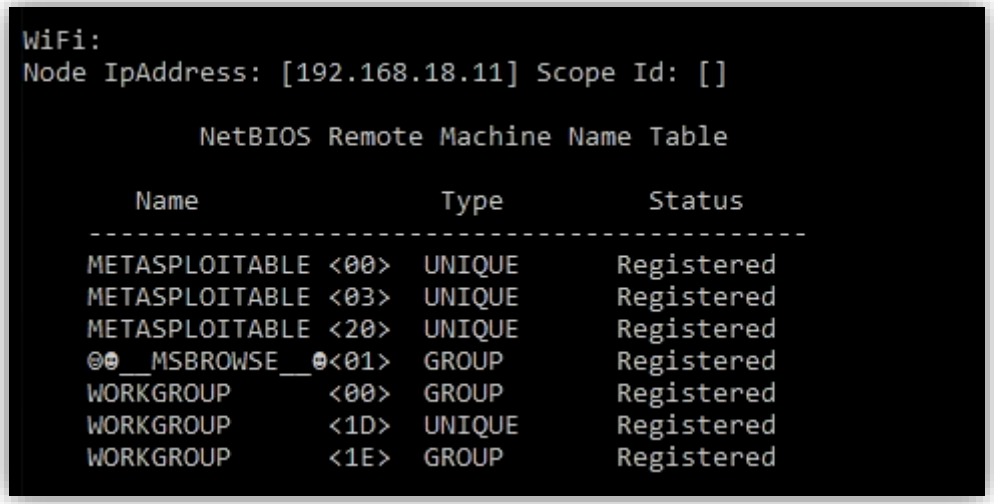
Nbtstat

(Windows Command line utility)

nbtstat

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

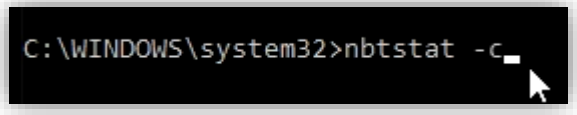
```
>nbtstat -a 192.168.18.110
```

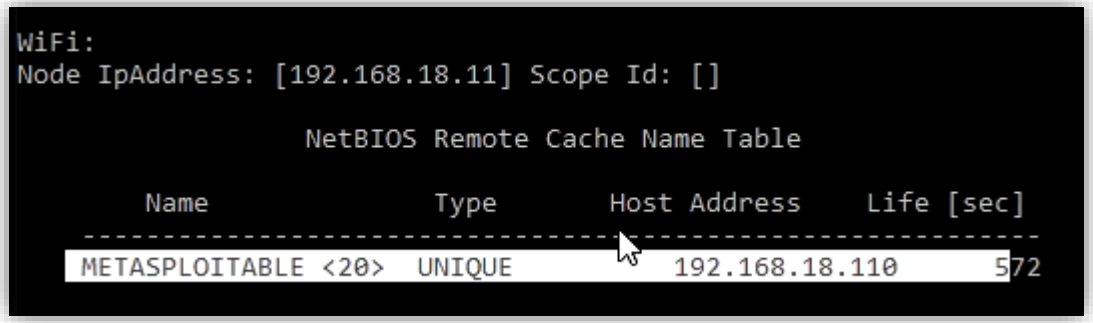


nbtstat

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

```
>nbtstat -c
```





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