

Scanning NetBIOS

During a penetration testing engagement we might come across with the NetBIOS service. In the past the NetBIOS protocol was enabled in almost every network that was running Windows. In nowadays system administrators are disabling this service due to the fact that plenty of information can be unveiled regarding shares, users and domain controllers. However NetBIOS can still be found on default configurations of Windows Server 2008 and Windows Vista so in a penetration testing this protocol can be abused if we discover it.

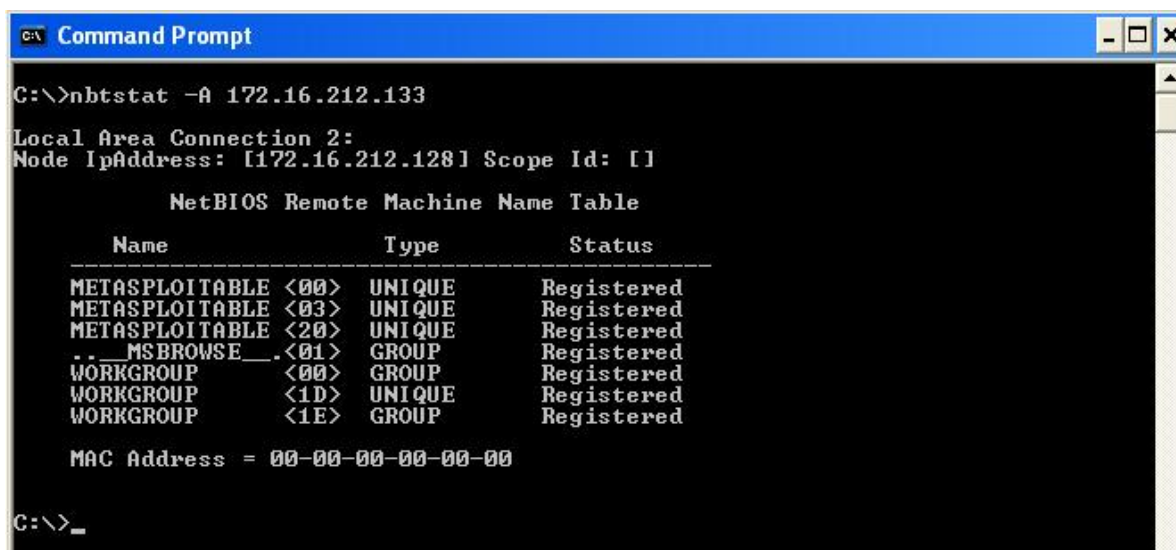
Generally the NetBIOS provides the following three services:

- Name Service: UDP/137
- Datagram Service: UDP/138
- Session Service: TCP/139

In systems that have this service enabled we can use some tools in order to discover information about the hostnames and domains especially in windows networks. In some cases this protocol can be found and in Linux systems.

The two basic tools are **nbtstat** and **nbtscan**. The **nbtstat** is a command line utility that is integrated in windows systems and it can unveil information about the netbios names and the remote machine name table or local but only for one host. From the other hand the **nbtscan** is a netbios nameserver scanner which has the same functions as **nbtstat** but it operates on a range of addresses instead of one.

The next image is showing the usage of the nbtstat:



```
C:\>nbtstat -A 172.16.212.133

Local Area Connection 2:
Node IpAddress: [172.16.212.128] 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

    MAC Address = 00-00-00-00-00-00

C:\>
```

nbtstat usage

The numeric values are called suffixes. For example the **<01>** and **<1D>** suffixes indicates the Master Browser, the **<20>** that the machine is running File Server service, the **<03>** that a messenger service is running and the **<00>** means that a workstation service is running as well. The **<1E>** is the Browser Service Elections.

The **nbtscan** is by default installed on backtrack but there is a version as well for windows platforms. We can use the **nbtscan** in order to scan the whole network. As we can see from the next image we have discovered the IP addresses, the NetBIOS names, the users that are logged in and the MAC addresses from the hosts that are running the NetBIOS service on the network.

```
root@encode:~# nbtscan 172.16.212.1-254
Doing NBT name scan for addresses from 172.16.212.1-254
```

IP address	NetBIOS Name	Server	User	MAC address
172.16.212.128	MAROON	<server>	<unknown>	00-50-56-bb-00-87
172.16.212.133	METASPLOITABLE	<server>	METASPLOITABLE	00-00-00-00-00-00

```
root@encode:~#
```

nbtscan

We can use also the **-v** option in order to produce a verbose output.

```
root@encode:~# nbtscan -v 172.16.212.1-254
Doing NBT name scan for addresses from 172.16.212.1-254
```

NetBIOS Name Table for Host 172.16.212.128:

Name	Service	Type
MAROON	<00>	UNIQUE
LONDON	<00>	GROUP
MAROON	<20>	UNIQUE
LONDON	<1e>	GROUP
LONDON	<1d>	UNIQUE
__MSBROWSE__	<01>	GROUP

```
Adapter address: 00-50-56-bb-00-87
```

nbtscan – verbose output

With the verbose option the output format is similar to the **nbtstat**. Again the **<01>** indicates the Master Browser service, the **<00>** the workstation, the **<20>** the File Server service and the **<1e>** and **<1d>** the Browser Service Elections and the Master Browser. Also we can see that the domain that this workstation belongs is London.

As an alternative option we can use the metasploit module **smb_version** which will unveil additional information like the operating system name and version, the service pack level, the language, the system and domain name.

```
msf > use scanner/smb/smb_version
msf auxiliary(smb_version) > set RHOSTS 172.16.212.128-133
RHOSTS => 172.16.212.128-133
msf auxiliary(smb_version) > run

[*] 172.16.212.128:445 is running Windows XP Service Pack 3 (language: English) (name:MAROON) (domain:LONDON)
[*] Scanned 1 of 6 hosts (016% complete)
[*] Scanned 2 of 6 hosts (033% complete)
[*] Scanned 3 of 6 hosts (050% complete)
[*] Scanned 4 of 6 hosts (066% complete)
[*] Scanned 5 of 6 hosts (083% complete)
[*] 172.16.212.133:445 is running Unix Samba 3.0.20-Debian (language: Unknown) (domain:WORKGROUP)
[*] Scanned 6 of 6 hosts (100% complete)
[*] Auxiliary module execution completed
```

Metasploit smb_version module

Conclusion

As we saw in this article from systems that had enabled the netbios service we have managed to discover plenty of information including the domain names, users, operating systems versions, MAC addresses and other. This service if found enabled can be used in the information gathering stage of a penetration test. So from the security point of view it is recommended this service to be disabled.