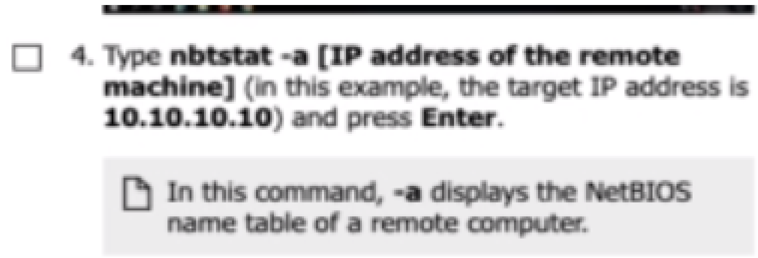
Enumeration



□ 4. Type **nbtstat -a [IP address of the remote machine]** (in this example, the target IP address is **10.10.10.10**) and press **Enter**.

In this command, **-a** displays the NetBIOS name table of a remote computer.

To display all the NETBIOS name tables of the Remote Windows Computer

```
nbtstat -a [IP] (Windows)
```

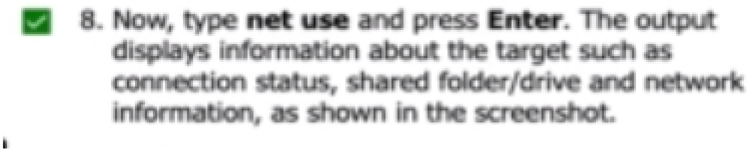
Display NETBIOS name cache of Windows Computer

```
nbtstat -c [IP]
```

List local NetBios names

```
nbtstat -n [IP]
```

use the NETBIOS share on Windows Computer



☑ 8. Now, type **net use** and press **Enter**. The output displays information about the target such as connection status, shared folder/drive and network information, as shown in the screenshot.

```
net use
```

snmp-check

> **Simple Network Management Protocol (SNMP)** lives on Port number: **161**

snmp-check

- snmp-check is a tool used to check whether the respective server is vulnerable to SNMP Attacks.
- If the server is vulnerable then the snmp-check enumerate the information of that machine.

```
snmp-check 10.10.10.x
```

NFS

NFS

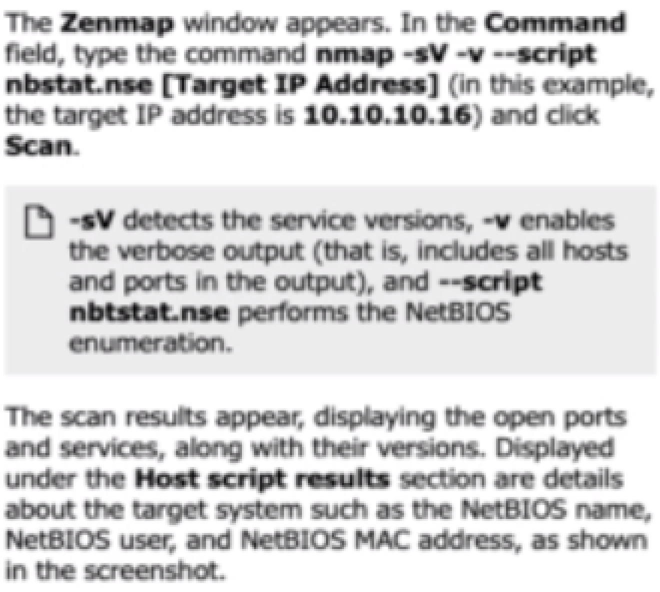
The Network File System (NFS) is a **mechanism for storing files on a network**. It is a distributed file system that allows users to access files and directories located on remote computers and treat those files and directories as if they were local.

> **Network File System (NFS)** runs on port number: **2049**

Nmap Script

```
nmap -p 2049 10.10.10.x
```

Netbios Enumeration using nmap or zenmap



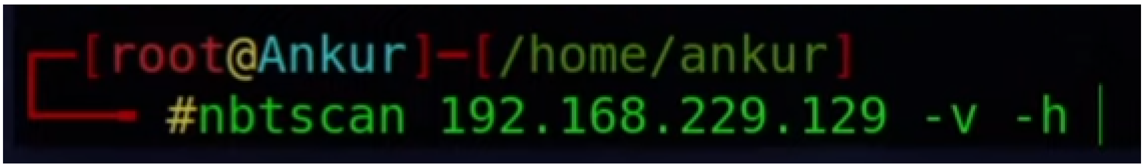
The **Zenmap** window appears. In the **Command** field, type the command **nmap -sV -v --script nbstat.nse [Target IP Address]** (in this example, the target IP address is **10.10.10.16**) and click **Scan**.

> **-sV** detects the service versions, **-v** enables the verbose output (that is, includes all hosts and ports in the output), and **--script nbtstat.nse** performs the NetBIOS enumeration.

The scan results appear, displaying the open ports and services, along with their versions. Displayed under the **Host script results** section are details about the target system such as the NetBIOS name, NetBIOS user, and NetBIOS MAC address, as shown in the screenshot.

`nmap -sV -v --script nbtstat.nse [IP]`

Netbios Enumeration using 'nbtscan'



```
┌─[root@Ankur]─[/home/ankur]
└──╼ #nbtscan 192.168.229.129 -v -h
```

'-h' -> for human readable

DNS ENumeration

```
dnsrecon -d "Domain Name"
```