

Lab 4: Perform NFS Enumeration

Lab Scenario

As a professional ethical hacker or penetration tester, the next step after LDAP enumeration is to perform NFS enumeration to identify exported directories and extract a list of clients connected to the server, along with their IP addresses and shared data associated with them.

After gathering this information, it is possible to spoof target IP addresses to gain full access to the shared files on the server.

Lab Objectives

- Perform NFS enumeration using RPCScan and SuperEnum

Overview of NFS Enumeration

NFS (Network File System) is a type of file system that enables computer users to access, view, store, and update files over a remote server. This remote data can be accessed by the client computer in the same way that it is accessed on the local system.

Task 1: Perform NFS Enumeration using RPCScan and SuperEnum

RPCScan communicates with RPC (remote procedure call) services and checks misconfigurations on NFS shares. It lists RPC services, mountpoints, and directories accessible via NFS. It can also recursively list NFS shares. SuperEnum includes a script that performs a basic enumeration of any open port, including the NFS port (2049).

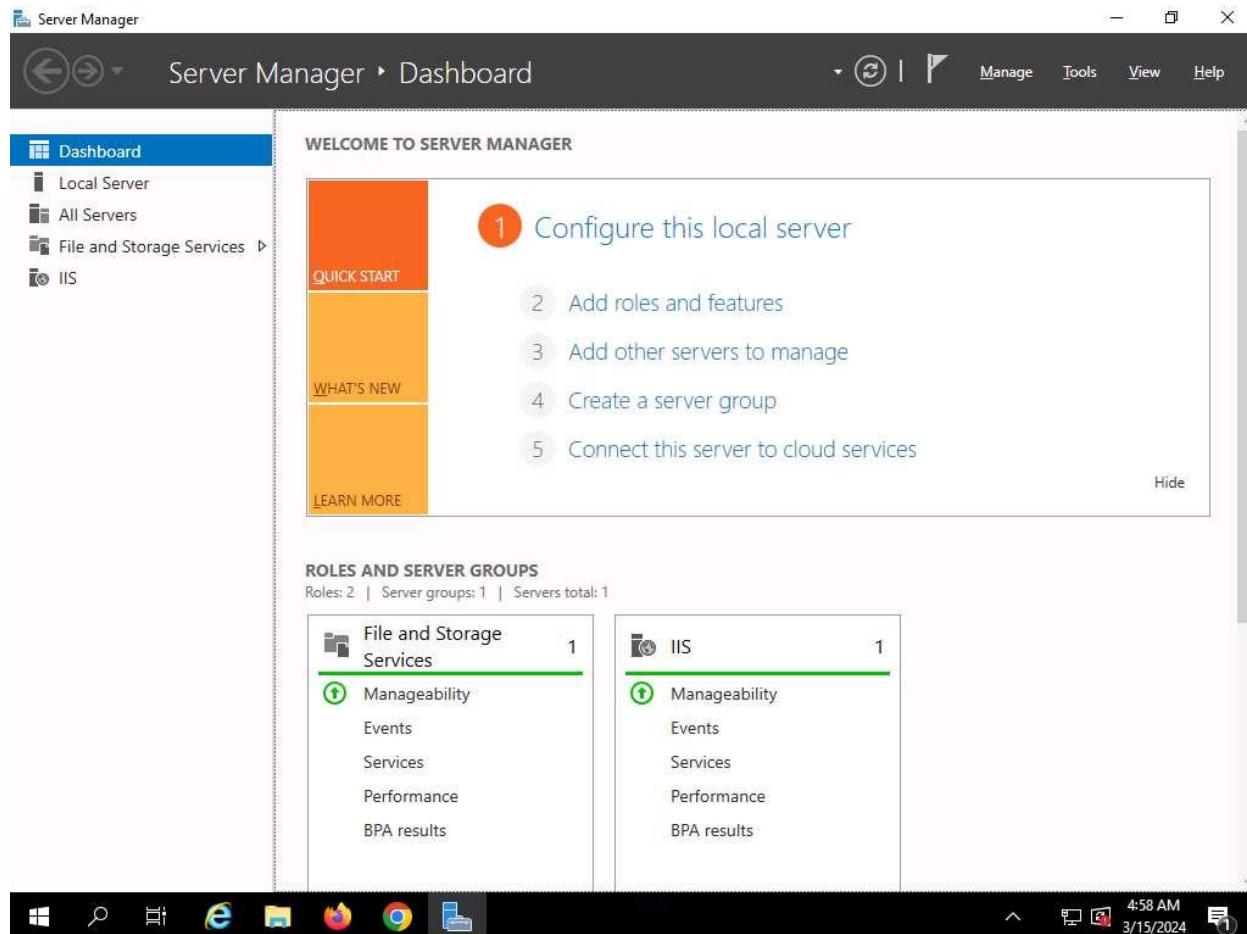
Here, we will use RPCScan and SuperEnum to enumerate NFS services running on the target machine.

Before starting this task, it is necessary to enable the NFS service on the target machine (**Windows Server 2019**). This will be done in **Step#1-6**.

1. Click [Windows Server 2019](#) to switch to the **Windows Server 2019** machine. In the **Windows Server 2019** machine, click the **Start** button at the bottom-left corner of **Desktop** and open **Server Manager**.

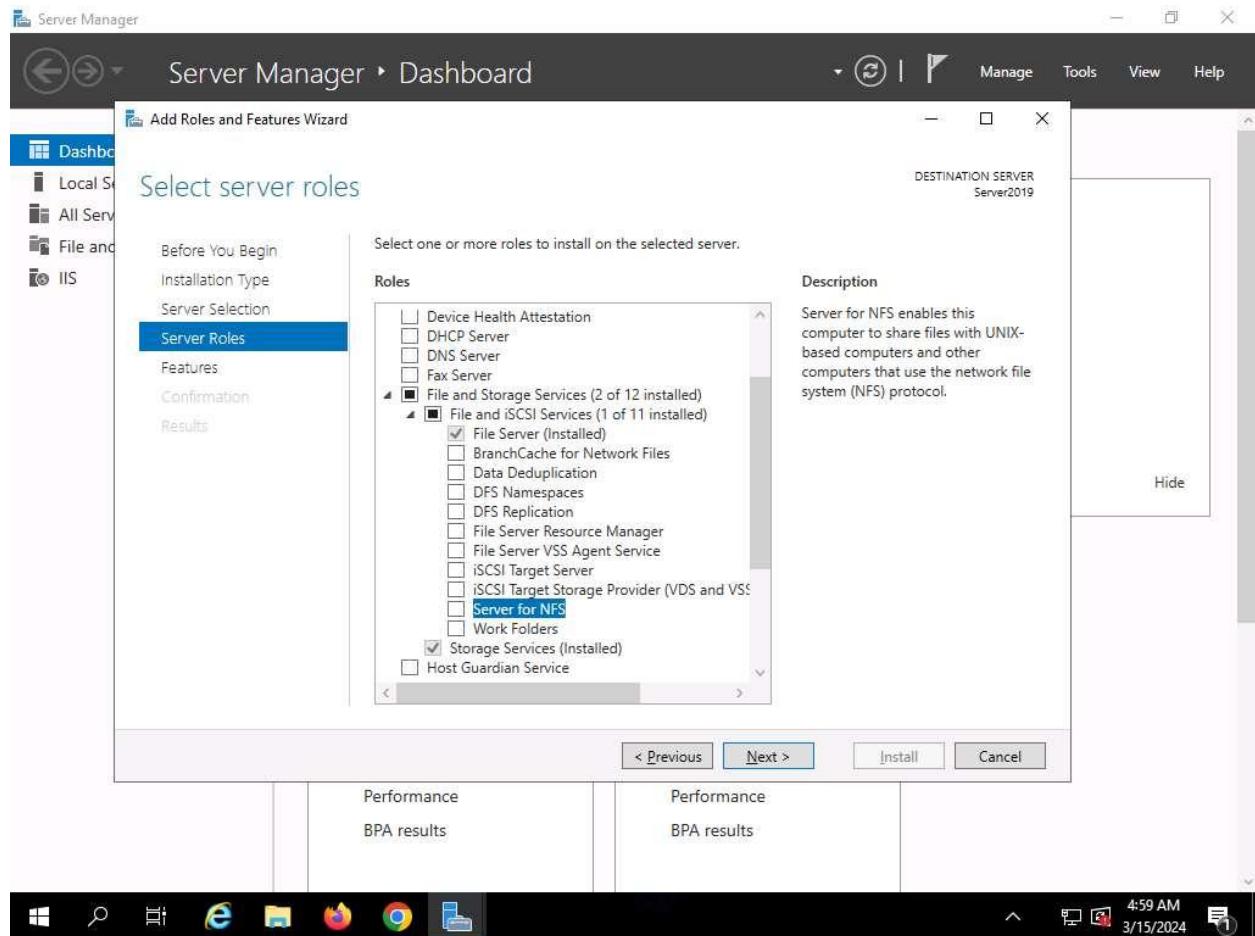
If you are logged out of the **Windows Server 2019** machine, click [Ctrl+Alt+Delete](#), then login with **Administrator/Pa\$\$w0rd**.

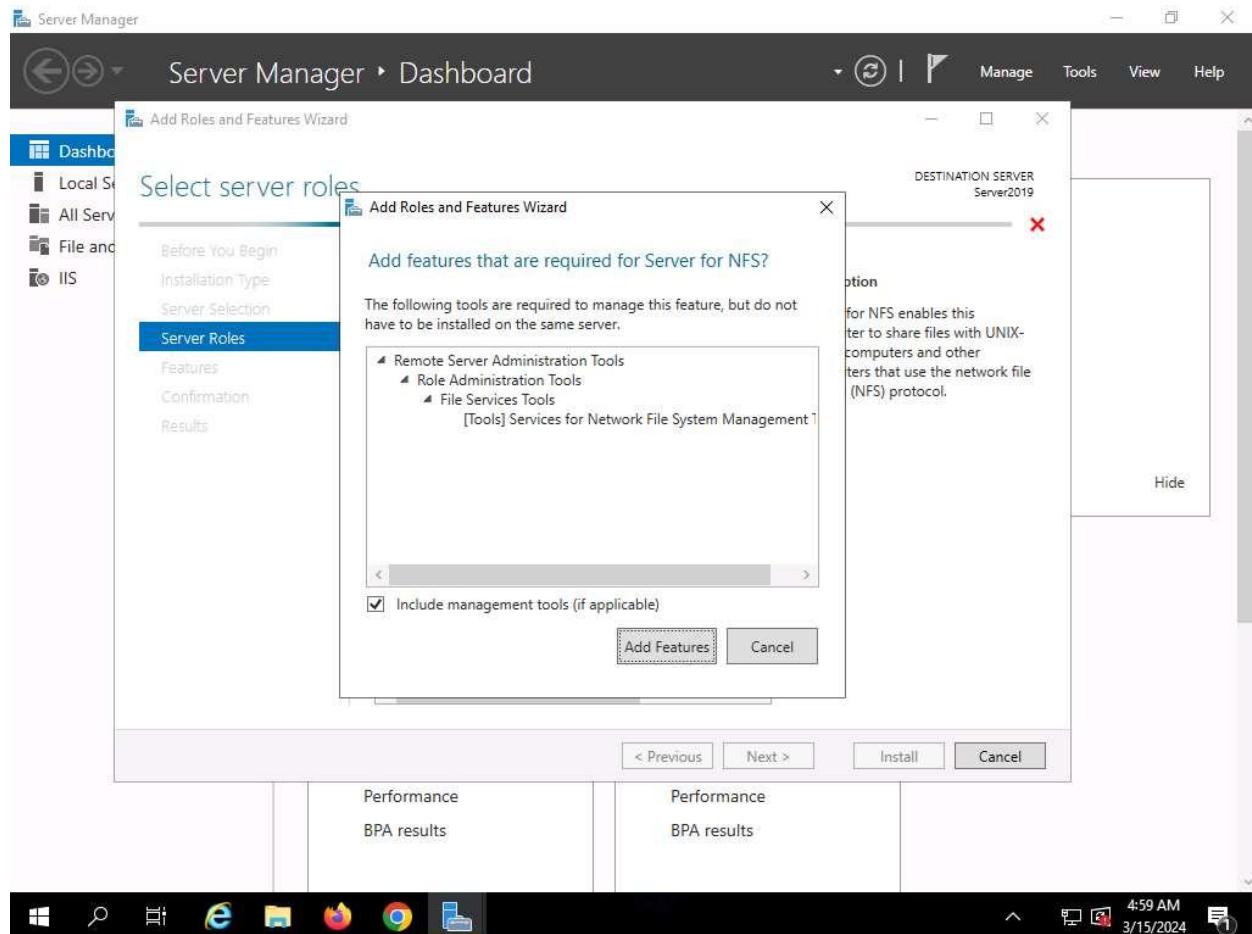
2. The **Server Manager** main window appears. By default, **Dashboard** will be selected; click **Add roles and features**.



3. The **Add Roles and Features Wizard** window appears. Click **Next** here and in the **Installation Type** and **Server Selection** wizards.
4. The **Server Roles** section appears. Expand **File and Storage Services** and select the checkbox for **Server for NFS** under the **File and iSCSI Services** option, as shown in the screenshot. Click **Next**.

In the **Add features that are required for Server for NFS?** pop-up window, click the **Add Features** button.





5. In the **Features** section, click **Next**. The **Confirmation** section appears; click **Install** to install the selected features.
6. The features begin installing, with progress shown by the **Feature installation** status bar. When installation completes, click **Close**.
7. Having enabled the NFS service, it is necessary to check if it is running on the target system (**Windows Server 2019**). In order to do this, we will use **Parrot Security** machine.
8. Click [**Parrot Security**](#) to switch to the **Parrot Security** machine. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

The password that you type will not be visible.

9. Execute **nmap -p 2049 [Target IP Address]** command (here the target IP address is , **10.10.1.19**).
-p: specifies port.
10. The scan result appears indicating that port 2049 is opened, and the NFS service is running on it, as shown in the screenshot.

```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# nmap -p 2049 10.10.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 08:02 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00069s latency).

PORT      STATE SERVICE
2049/tcp  open  nfs
MAC Address: 02:15:5D:64:A2:27 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
[root@parrot]~#
```

11. Run **cd SuperEnum** command to navigate to the **SuperEnum** folder.
12. Run **echo "10.10.1.19" >> Target.txt** command to create a file having a target machine's IP address (**10.10.1.19**).

You may enter multiple IP addresses in the **Target.txt** file. However, in this task we are targeting only one machine, the **Windows Server 2019 (10.10.1.19)**.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title is "echo "10.10.1.19" >> Target.txt - Parrot Terminal". The session starts with the user "attacker" at the root prompt, entering "sudo su" to become root. They then run an Nmap scan on port 2049 of the target IP 10.10.1.19, which finds an NFS service running. The user then navigates to the "/home/attacker/SuperEnum" directory, runs "SuperEnum", and outputs the results to "Target.txt". Finally, they echo the target IP back into the terminal.

```
Applications Places System echo "10.10.1.19" >> Target.txt - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# nmap -p 2049 10.10.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 08:02 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00069s latency).

PORT      STATE SERVICE
2049/tcp  open  nfs
MAC Address: 02:15:5D:64:A2:27 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
[root@parrot] ~
# cd SuperEnum/
[root@parrot] ~
# ./SuperEnum
# echo "10.10.1.19" >> Target.txt
[root@parrot] ~
#
```

13. Execute **./superenum** command. Under **Enter IP List filename with path**, type **Target.txt**, and press **Enter**.

If you get an error running the **./superenum** script, execute **chmod +x superenum** command, then repeat **Step#13**.

The screenshot shows a terminal window titled ".superenum - Parrot Terminal" running on a Parrot OS desktop environment. The terminal window has a dark blue header bar with icons for Applications, Places, System, and a volume control. The main terminal area displays the following command-line session:

```
[root@parrot]~[~/home/attacker/SuperEnum]
# ./superenum
Enter IP List filename with path
Target.txt

TCP Scan Started for IP: 10.10.1.19
```

The background of the desktop shows a network graph visualization.

14. The script starts scanning the target IP address for open NFS and other services.

The scan will take approximately 15-20 mins to complete.

15. After the scan is finished, scroll down to review the results. Observe that the port 2049 is open and the NFS service is running on it.

```
./superenum - Parrot Terminal
File Edit View Search Terminal Help
15-03-2024/10.10.1.19/open_ports/139/telnet: line 3: expect: command not found
15-03-2024/10.10.1.19/open_ports/139/null_session: line 3: expect: command not found

Testing for 10.10.1.19: 161
Testing for 10.10.1.19: 161, Tool: nmap_snmp-interfaces
Testing for 10.10.1.19: 161, Tool: nmap_snmp-netstat
Testing for 10.10.1.19: 161, Tool: nmap_snmp-processes
Testing for 10.10.1.19: 161, Tool: nmap_snmp-brute
15-03-2024/10.10.1.19/open_ports/161/telnet: line 3: expect: command not found
README license

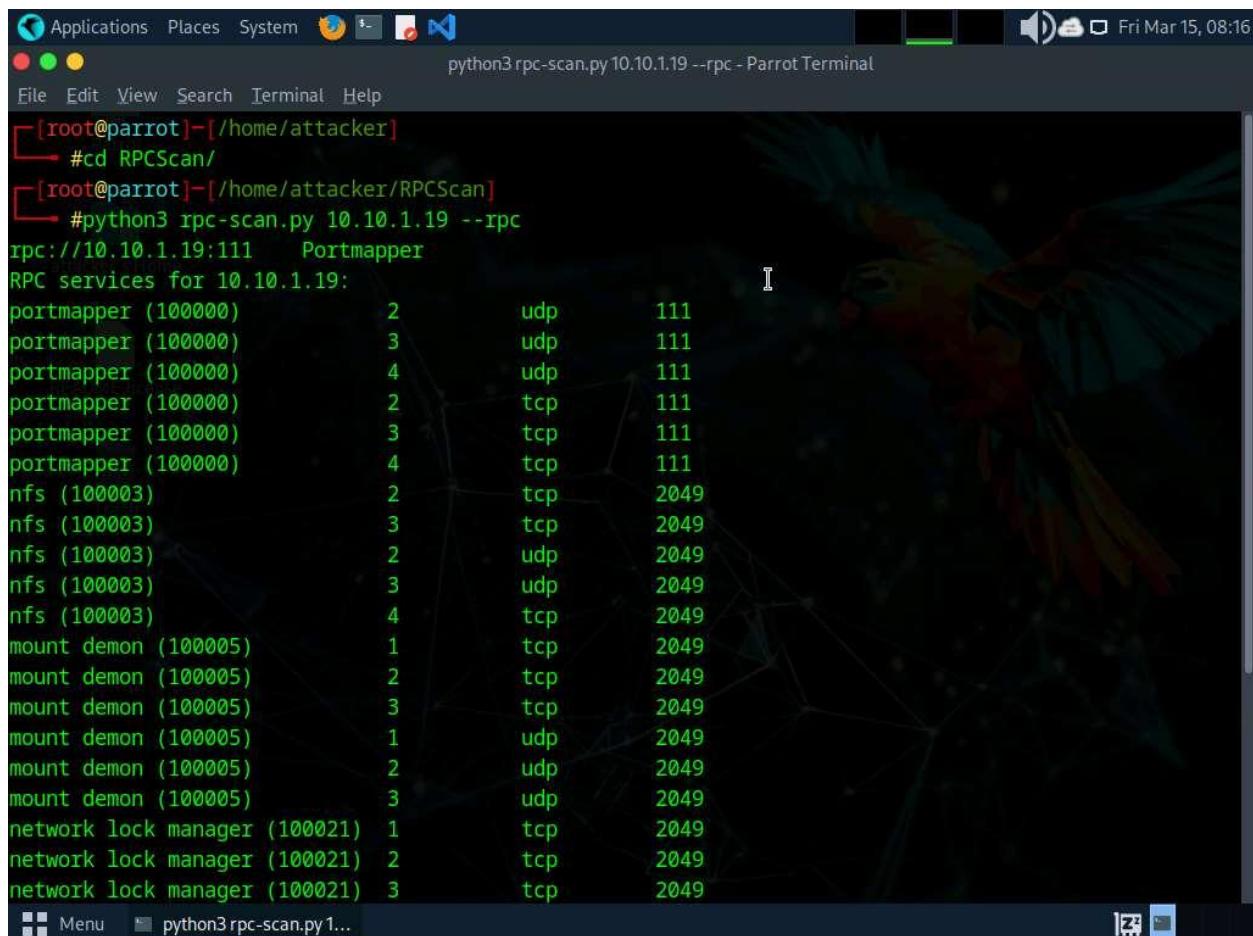
Testing for 10.10.1.19: 16452
15-03-2024/10.10.1.19/open_ports/16452/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 1801
15-03-2024/10.10.1.19/open_ports/1801/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 2049
Testing for 10.10.1.19: 2049, Tool: nmap_nfs-ls
Testing for 10.10.1.19: 2049, Tool: nmap_nfs-stats
Testing for 10.10.1.19: 2049, Tool: showmount
./superenum: line 116: showmount: command not found
15-03-2024/10.10.1.19/open_ports/2049/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 2103
15-03-2024/10.10.1.19/open_ports/2103/telnet: line 3: expect: command not found
```

16. You can also observe the other open ports and the services running on them.
 17. In the terminal window, run `cd ..` command to return to the root directory.
 18. Now, we will perform NFS enumeration using RPCScan. To do so, run `cd RPCScan` command.
 19. Execute `python3 rpc-scan.py [Target IP address] --rpc` command (here, the target IP address is **10.10.1.19**, the **Windows Server 2019** machine).
- rpc**: lists the RPC (portmapper).
20. The result appears, displaying that port 2049 is open, and the NFS service is running on it.



A terminal window titled "python3 rpc-scan.py 10.10.1.19 --rpc - Parrot Terminal". The window shows the output of the RPCScan tool. The command run was "#python3 rpc-scan.py 10.10.1.19 --rpc". The output lists various RPC services running on port 111. The table below summarizes the findings:

Service	Port	Protocol	Version
portmapper (100000)	2	udp	111
portmapper (100000)	3	udp	111
portmapper (100000)	4	udp	111
portmapper (100000)	2	tcp	111
portmapper (100000)	3	tcp	111
portmapper (100000)	4	tcp	111
nfs (100003)	2	tcp	2049
nfs (100003)	3	tcp	2049
nfs (100003)	2	udp	2049
nfs (100003)	3	udp	2049
nfs (100003)	4	tcp	2049
mount demon (100005)	1	tcp	2049
mount demon (100005)	2	tcp	2049
mount demon (100005)	3	tcp	2049
mount demon (100005)	1	udp	2049
mount demon (100005)	2	udp	2049
mount demon (100005)	3	udp	2049
network lock manager (100021)	1	tcp	2049
network lock manager (100021)	2	tcp	2049
network lock manager (100021)	3	tcp	2049

21. This concludes the demonstration of performing NFS enumeration using SuperEnum and RPCScan.

22. Close all open windows and document all the acquired information.

Question 4.4.1.1

Perform NFS Enumeration using RPCScan and SuperEnum and find the port used by the NFS service on 10.10.1.19.