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.

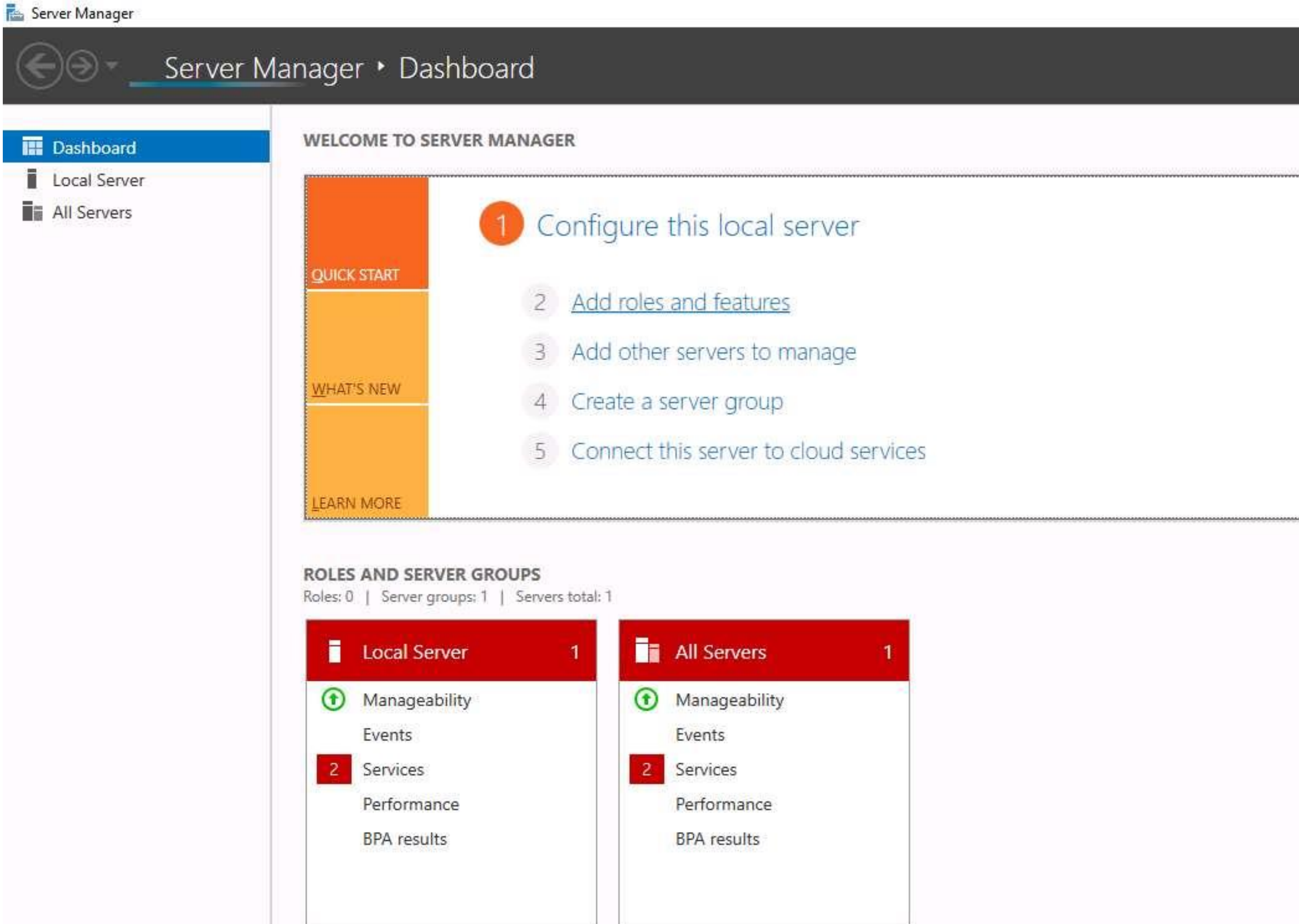
Task 1: Perform NFS Enumeration using RPCScan and SuperEnum

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 lab, it is necessary to enable the NFS service on the target machine (**Windows Server 2019**). This will be done in **steps 1-6**.

1. □ In the **Windows Server 2019** machine, click the **Start** button at the bottom-left corner of **Desktop** and open **Server Manager**.
2. □ The **Server Manager** main window appears. By default, **Dashboard** will be selected; click **Add roles and features**.



Server Manager

Server Manager ‣ Dashboard

WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

5 Connect this server to cloud services

ROLES AND SERVER GROUPS

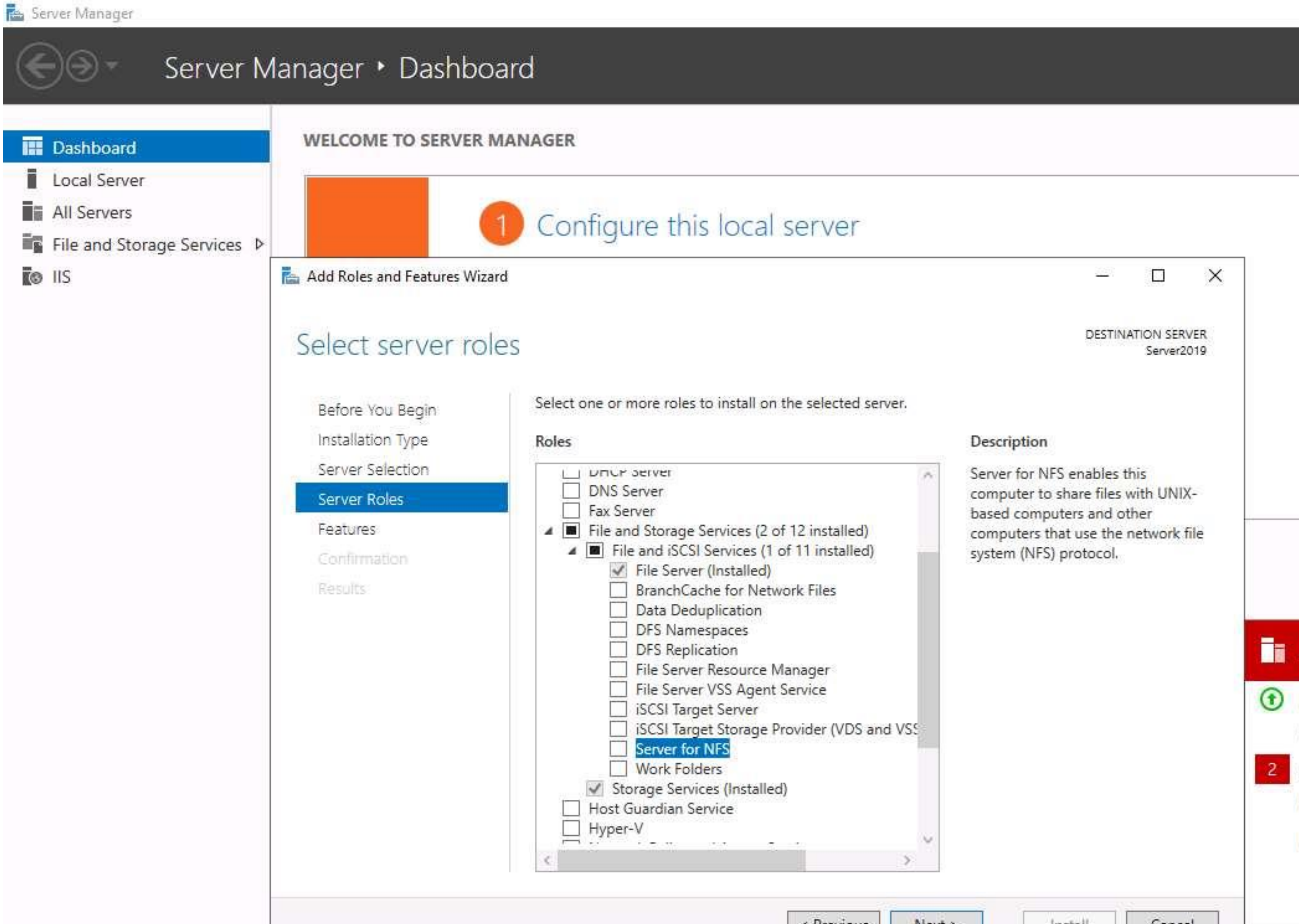
Roles: 0 | Server groups: 1 | Servers total: 1

Local Server	1
Manageability	
Events	
Services	2
Performance	
BPA results	

All Servers	1
Manageability	
Events	
Services	2
Performance	
BPA results	

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.



Server Manager

Server Manager ‣ Dashboard

- Dashboard
- Local Server
- All Servers
- File and Storage Services ▷
- IIS

WELCOME TO SERVER MANAGER

1 Configure this local server

Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
Server2019

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select one or more roles to install on the selected server.

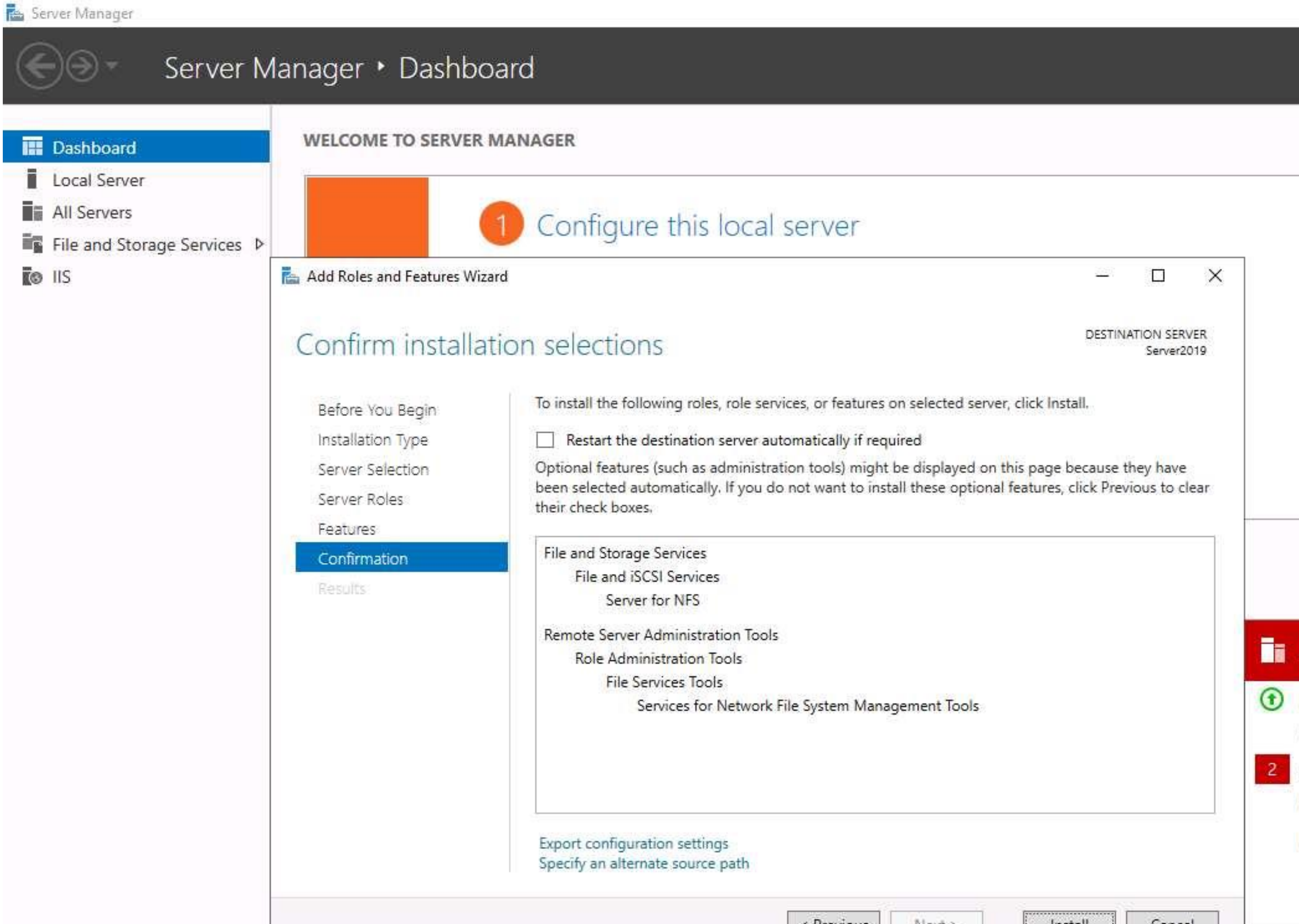
Roles

☐ DHCP Server
☐ DNS Server
☐ Fax Server
◢ ■ File and Storage Services (2 of 12 installed)
  ◢ ■ File and iSCSI Services (1 of 11 installed)
    ☑ File Server (Installed)
    ☐ BranchCache for Network Files
    ☐ Data Deduplication
    ☐ DFS Namespaces
    ☐ DFS Replication
    ☐ File Server Resource Manager
    ☐ File Server VSS Agent Service
    ☐ iSCSI Target Server
    ☐ iSCSI Target Storage Provider (VDS and VSS
    ☐ Server for NFS
    ☐ Work Folders
  ☑ Storage Services (Installed)
☐ Host Guardian Service
☐ Hyper-V

Description

Server for NFS enables this computer to share files with UNIX-based computers and other computers that use the network file system (NFS) protocol.

5. In the **Features** section, click **Next**. The **Confirmation** section appears; click **Install** to install the selected features.


Server Manager
Server Manager ‣ Dashboard
Dashboard
Local Server
All Servers
File and Storage Services ▷
IIS
WELCOME TO SERVER MANAGER
1 Configure this local server
Add Roles and Features Wizard
2

Confirm installation selections

DESTINATION SERVER
Server2019

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

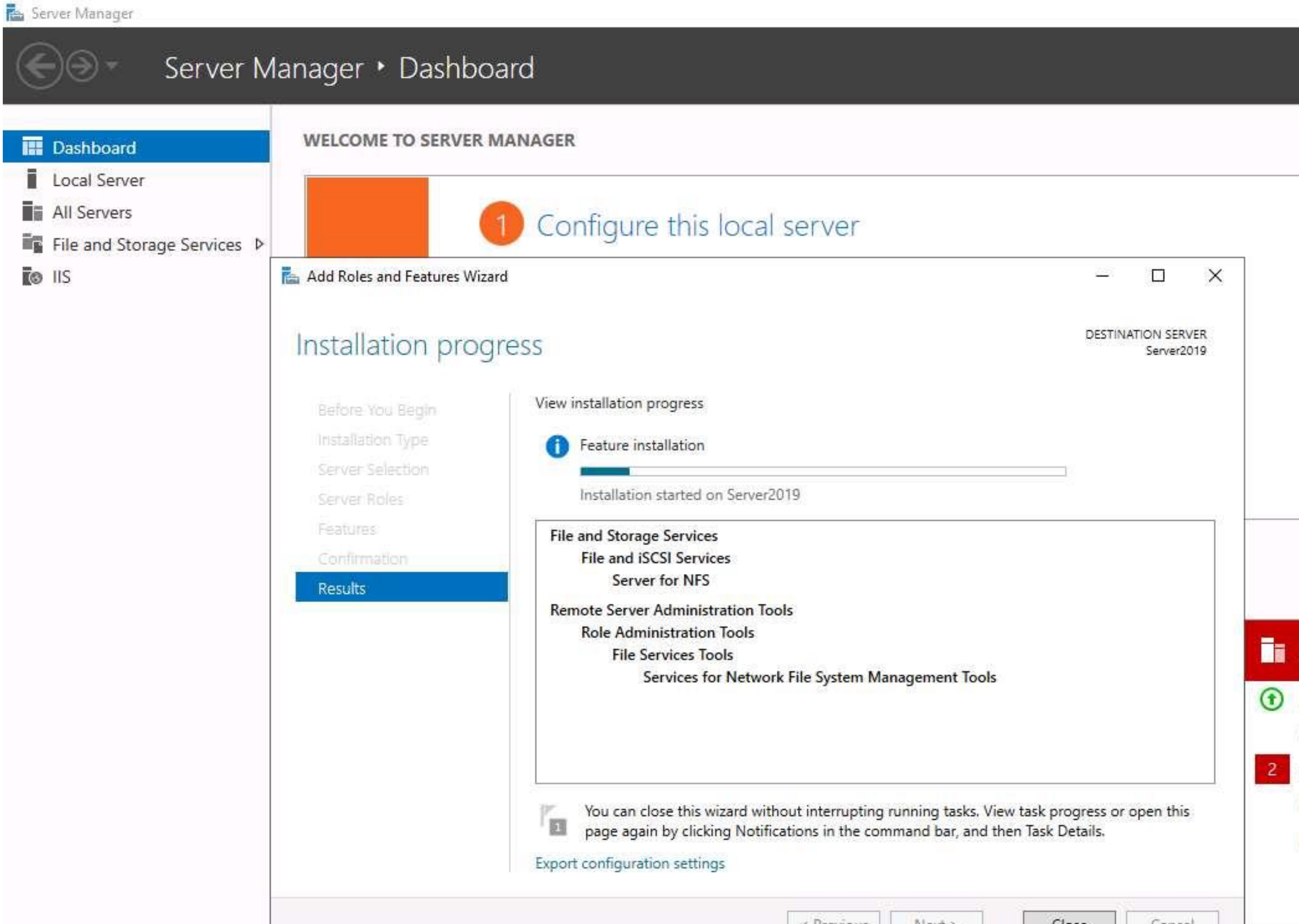
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

File and Storage Services
    File and iSCSI Services
        Server for NFS

Remote Server Administration Tools
    Role Administration Tools
        File Services Tools
            Services for Network File System Management Tools

Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

6. □ The features begin installing, with progress shown by the **Feature installation** status bar. When installation completes, click **Close**.



Installation progress

DESTINATION SERVER
Server2019

View installation progress

Feature installation

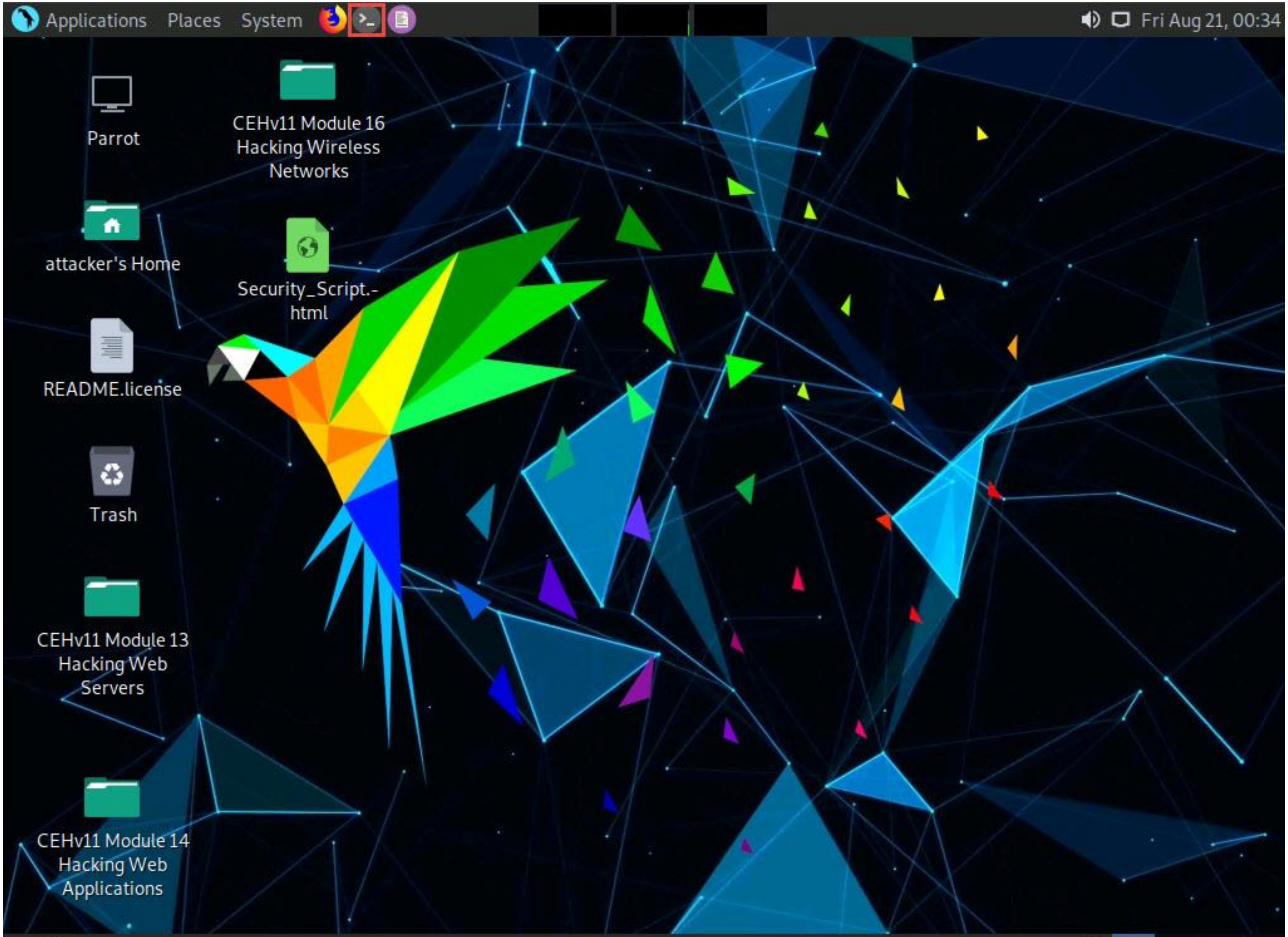
Installation started on Server2019

File and Storage Services
  File and iSCSI Services
    Server for NFS
Remote Server Administration Tools
  Role Administration Tools
    File Services Tools
      Services for Network File System Management Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

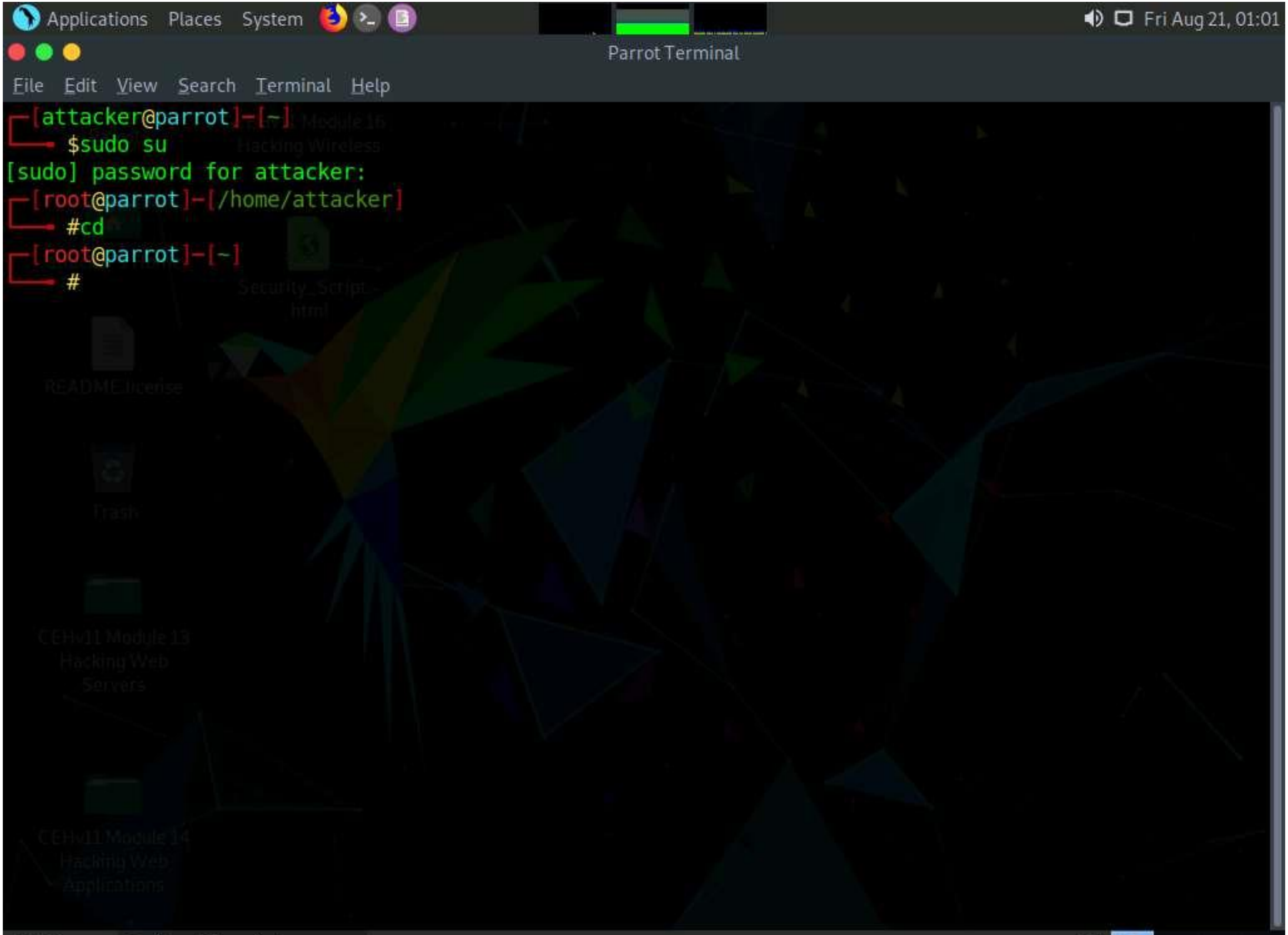
7. □ Having enabled the NFS service, it is necessary to check if it is running on the target system (**Windows Server 2019**). In order to do this, we will use **Parrot Security** machine.
8. □ Click Parrot Security to switch to the **Parrot Security** machine.
9. □ Click the **MATE Terminal** icon at the top-left corner of the **Desktop** window to open a **Terminal** window.


Applications
Places
System
Fri Aug 21, 00:34
Parrot
CEHv11 Module 16 Hacking Wireless Networks
attacker's Home
Security_Script.-html
README.license
Trash
CEHv11 Module 13 Hacking Web Servers
CEHv11 Module 14 Hacking Web Applications

10. □ A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
11. □ In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

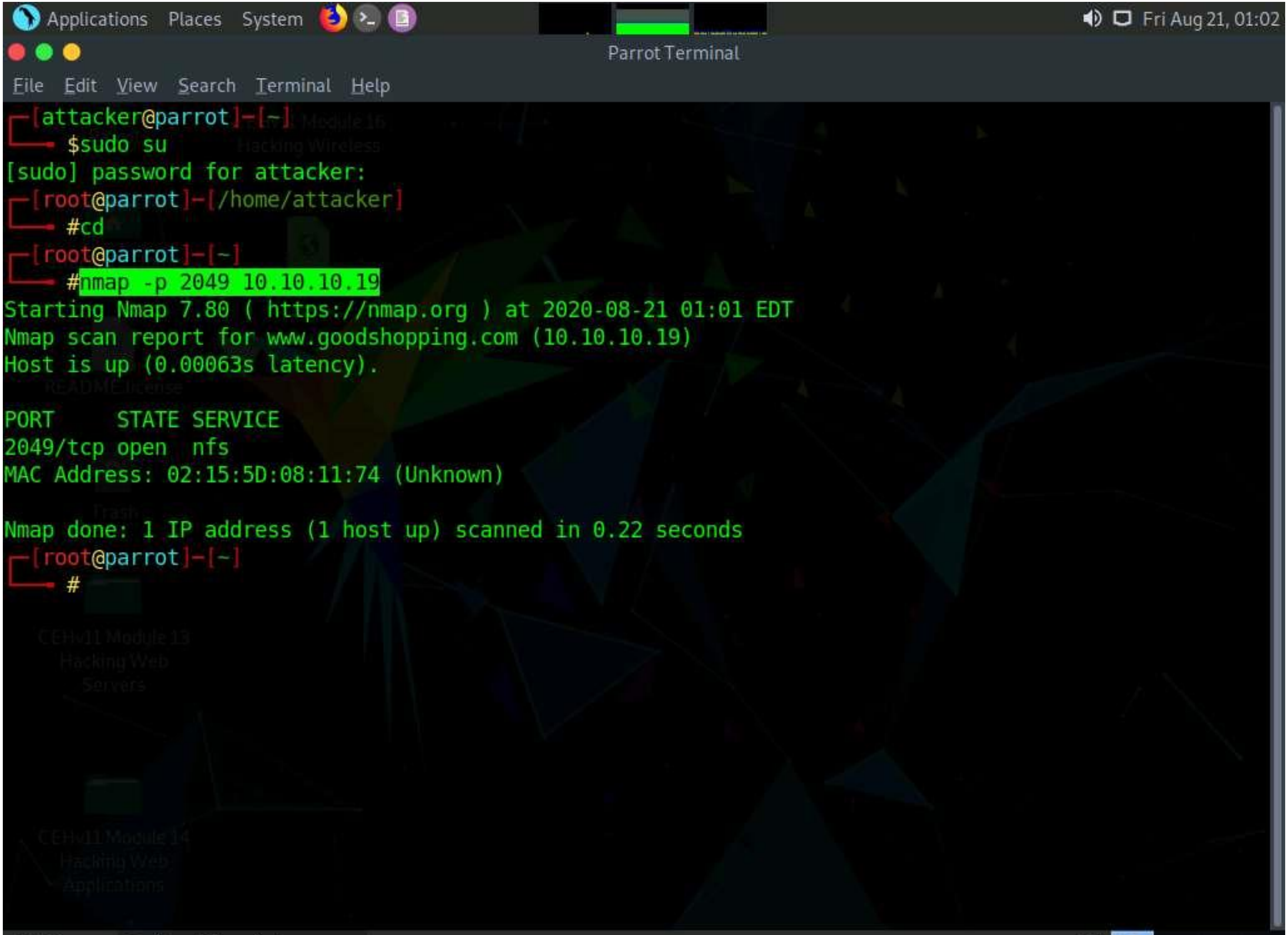
12. □ Now, type **cd** and press **Enter** to jump to the root directory.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

13. □ In the terminal window, type **nmap -p 2049 [Target IP Address]** (in this case, **10.10.10.19**) and press **Enter**.

14. □ The scan result appears indicating that port 2049 is opened, and the NFS service is running on it, as shown in the screenshot.

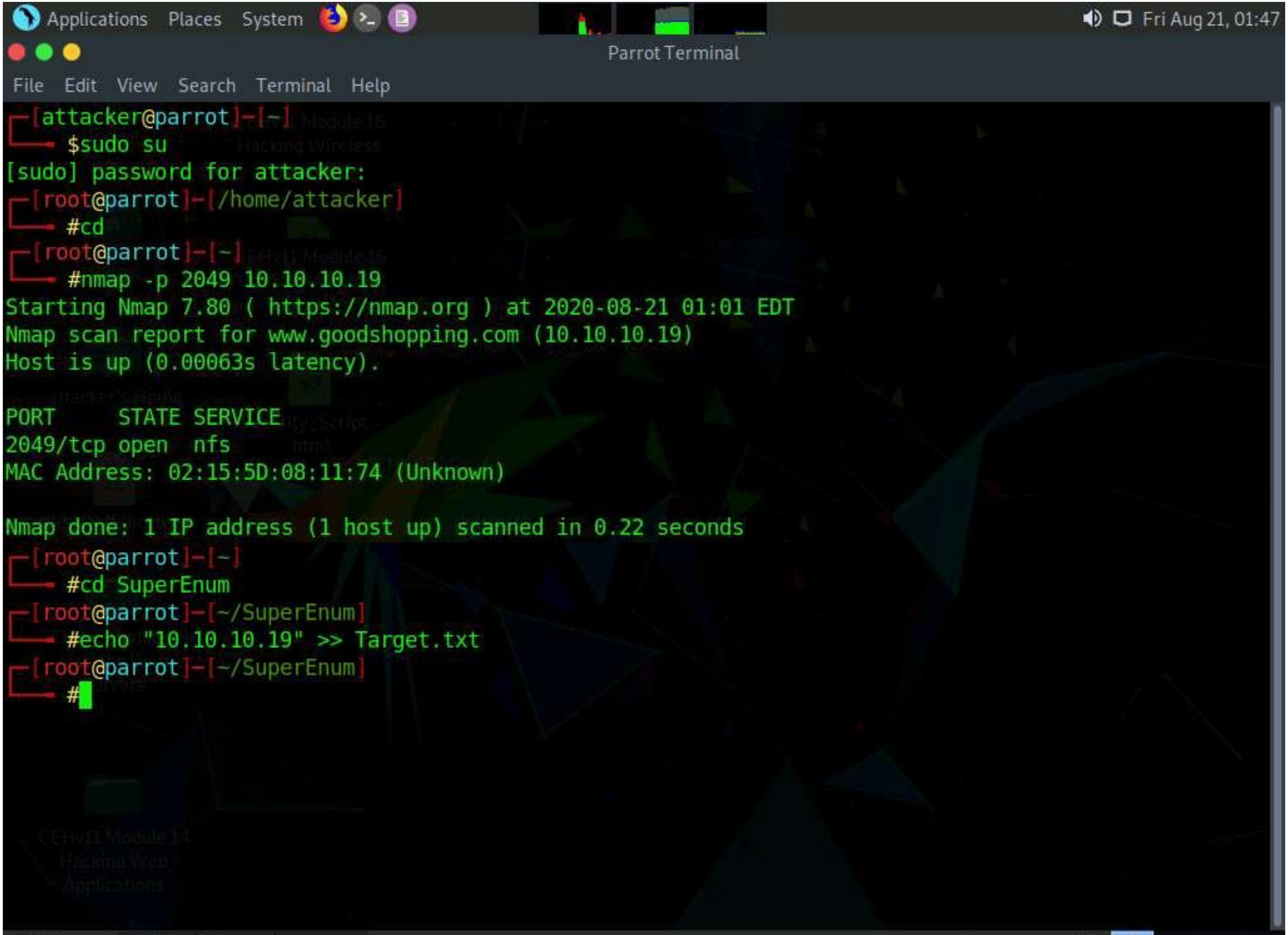


```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #nmap -p 2049 10.10.10.19
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-21 01:01 EDT
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.00063s latency).

PORT     STATE SERVICE
2049/tcp open  nfs
MAC Address: 02:15:5D:08:11:74 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
┌─[root@parrot]─[~]
└──╼ #
```

15. □ Type **cd SuperEnum** and press **Enter** to navigate to the **SuperEnum** folder.

16. □ Type **echo "10.10.10.19" >> Target.txt** and press **Enter** to create a file having a target machine's IP address (**10.10.10.19**).

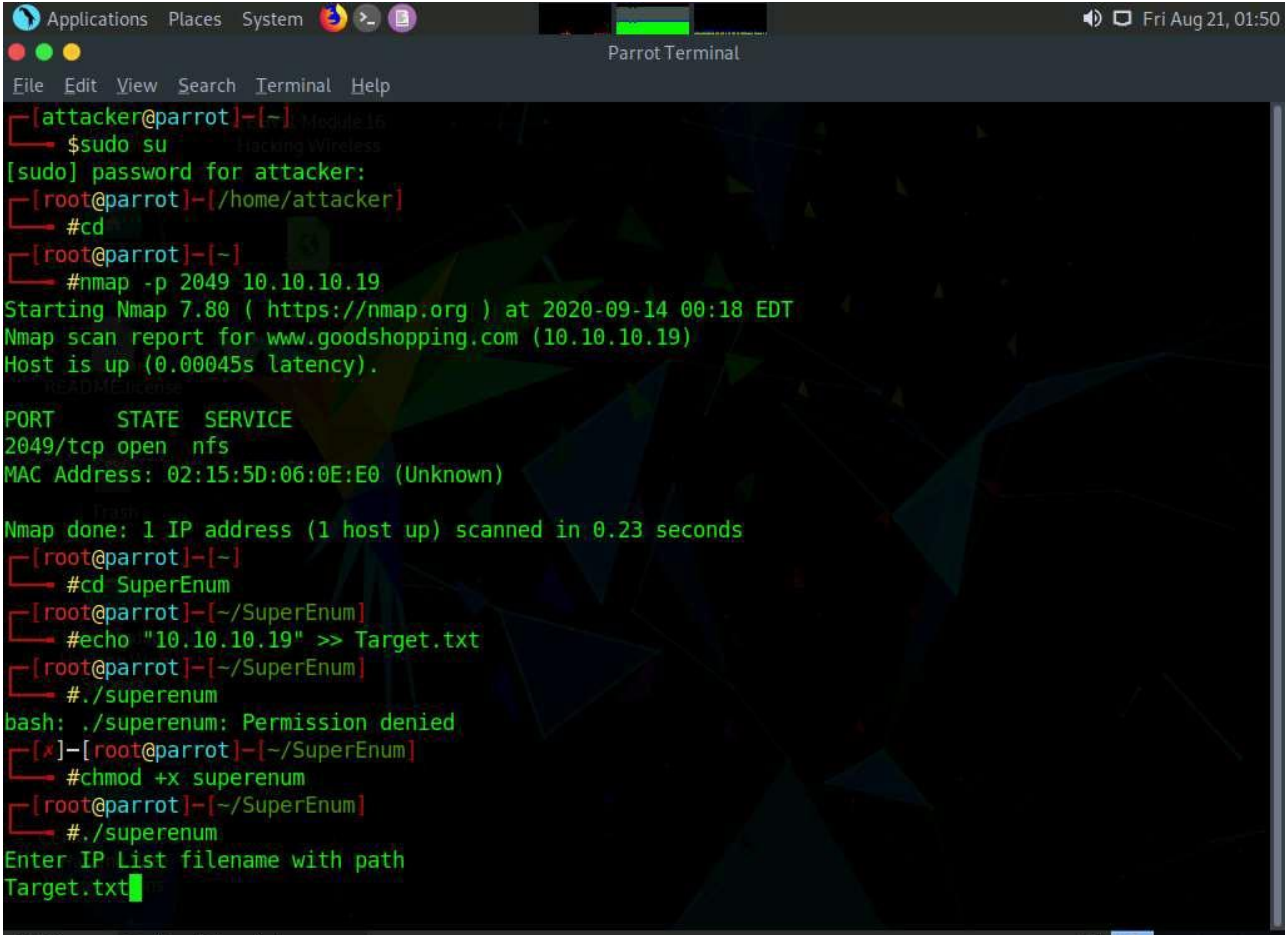
You may enter multiple IP addresses in the **Target.txt** file. However, in this task we are targeting only one machine, the **Windows Server 2019 (10.10.10.19)**. The IP address may vary in your lab environment.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #nmap -p 2049 10.10.10.19
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-21 01:01 EDT
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.00063s latency).

PORT     STATE SERVICE
2049/tcp open  nfs
MAC Address: 02:15:5D:08:11:74 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
┌─[root@parrot]─[~]
└──╼ #cd SuperEnum
┌─[root@parrot]─[~/SuperEnum]
└──╼ #echo "10.10.10.19" >> Target.txt
┌─[root@parrot]─[~/SuperEnum]
└──╼ #
```

17. □ Type **./superenum** and press **Enter**. Under **Enter IP List filename with path**, type **Target.txt**, and press **Enter**.

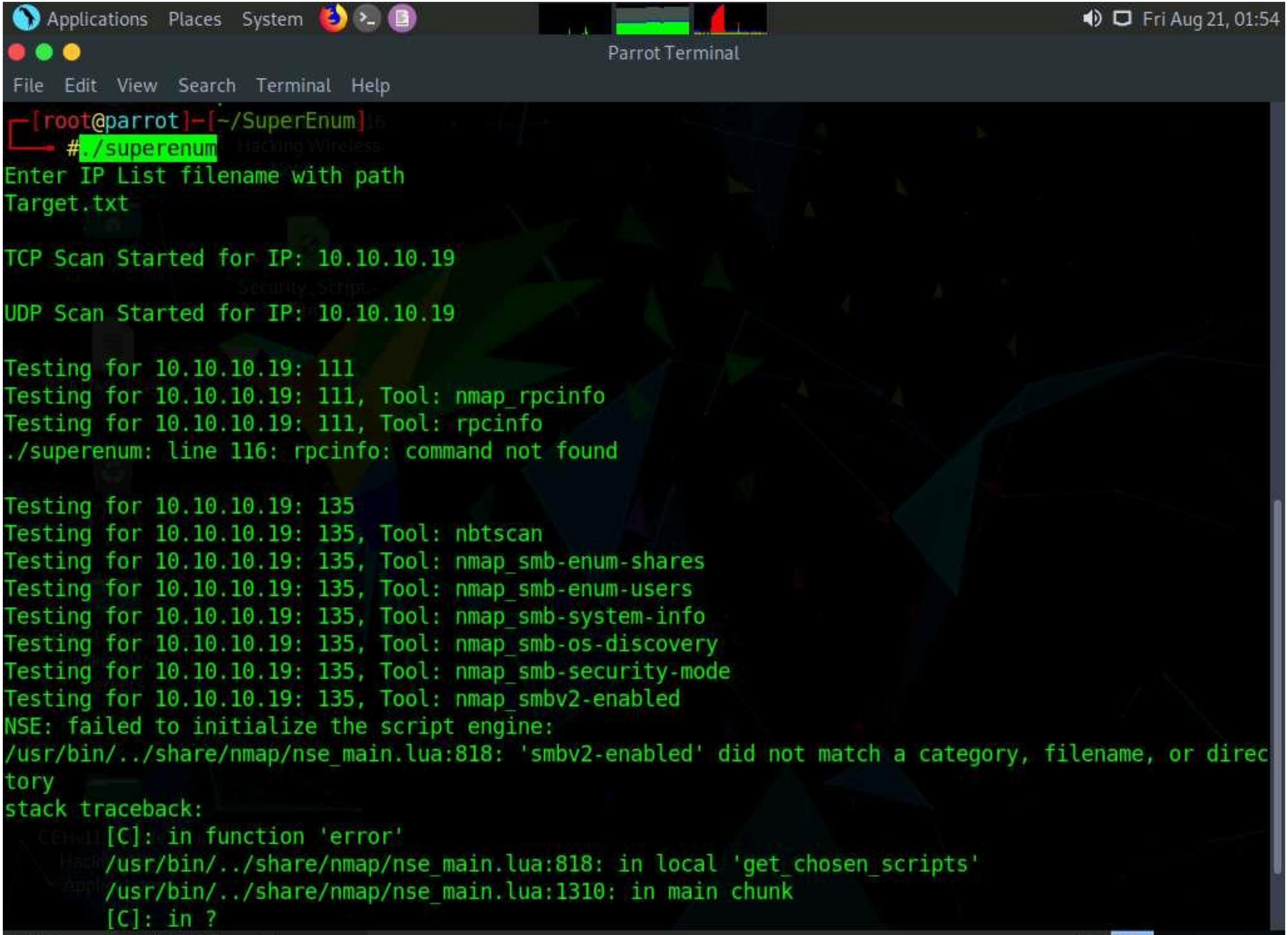
If you get an error running the ./superenum script, type **chmod +x superenum** and press **Enter**, then repeat **Step 17**.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #nmap -p 2049 10.10.10.19
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-14 00:18 EDT
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.00045s latency).

PORT     STATE  SERVICE
2049/tcp open   nfs
MAC Address: 02:15:5D:06:0E:E0 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
┌─[root@parrot]─[~]
└──╼ #cd SuperEnum
┌─[root@parrot]─[~/SuperEnum]
└──╼ #echo "10.10.10.19" >> Target.txt
┌─[root@parrot]─[~/SuperEnum]
└──╼ #./superenum
bash: ./superenum: Permission denied
┌─[✗]─[root@parrot]─[~/SuperEnum]
└──╼ #chmod +x superenum
┌─[root@parrot]─[~/SuperEnum]
└──╼ #./superenum
Enter IP List filename with path
Target.txt
```

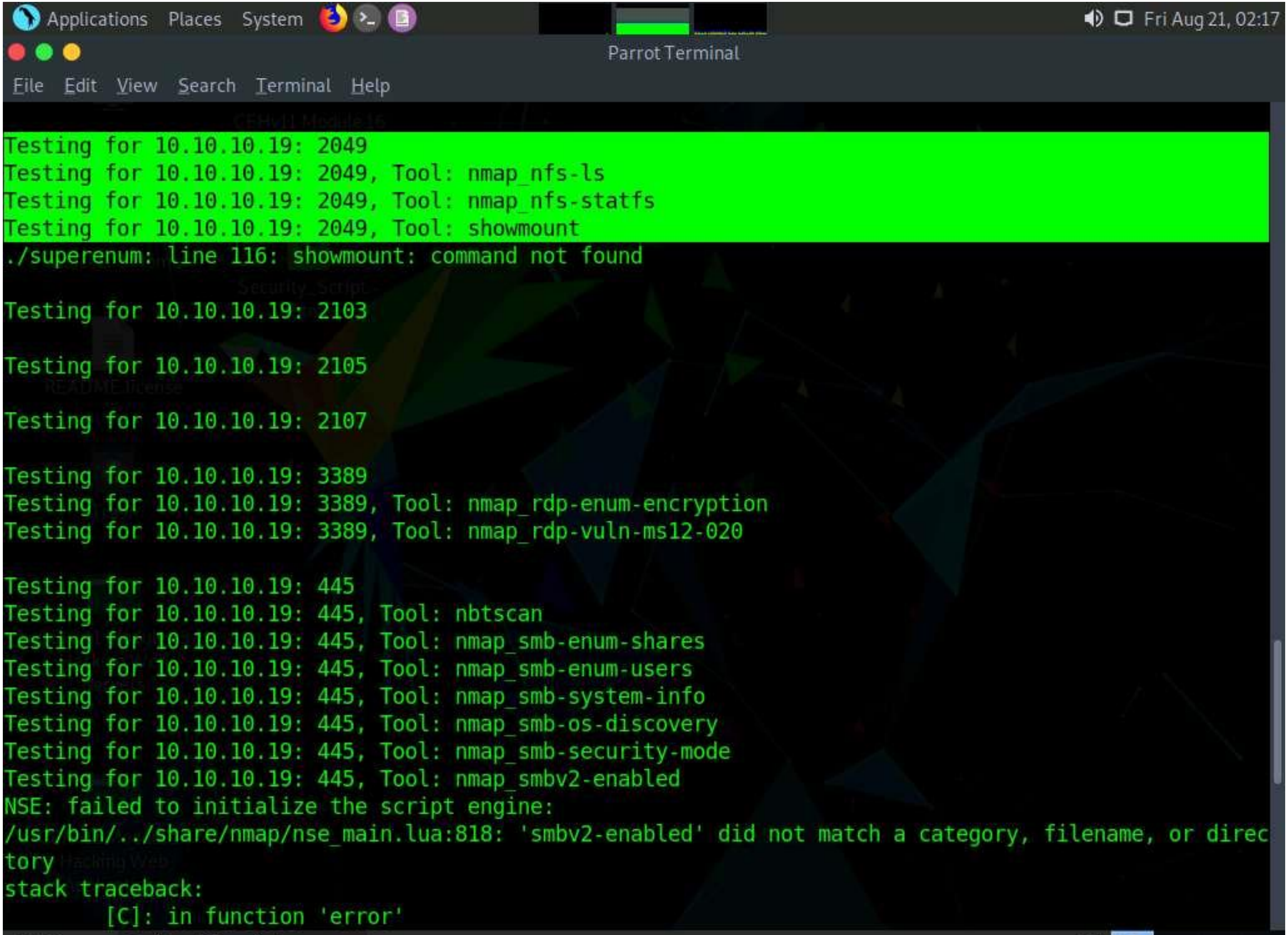
18. □ The script starts scanning the target IP address for open NFS and other.

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



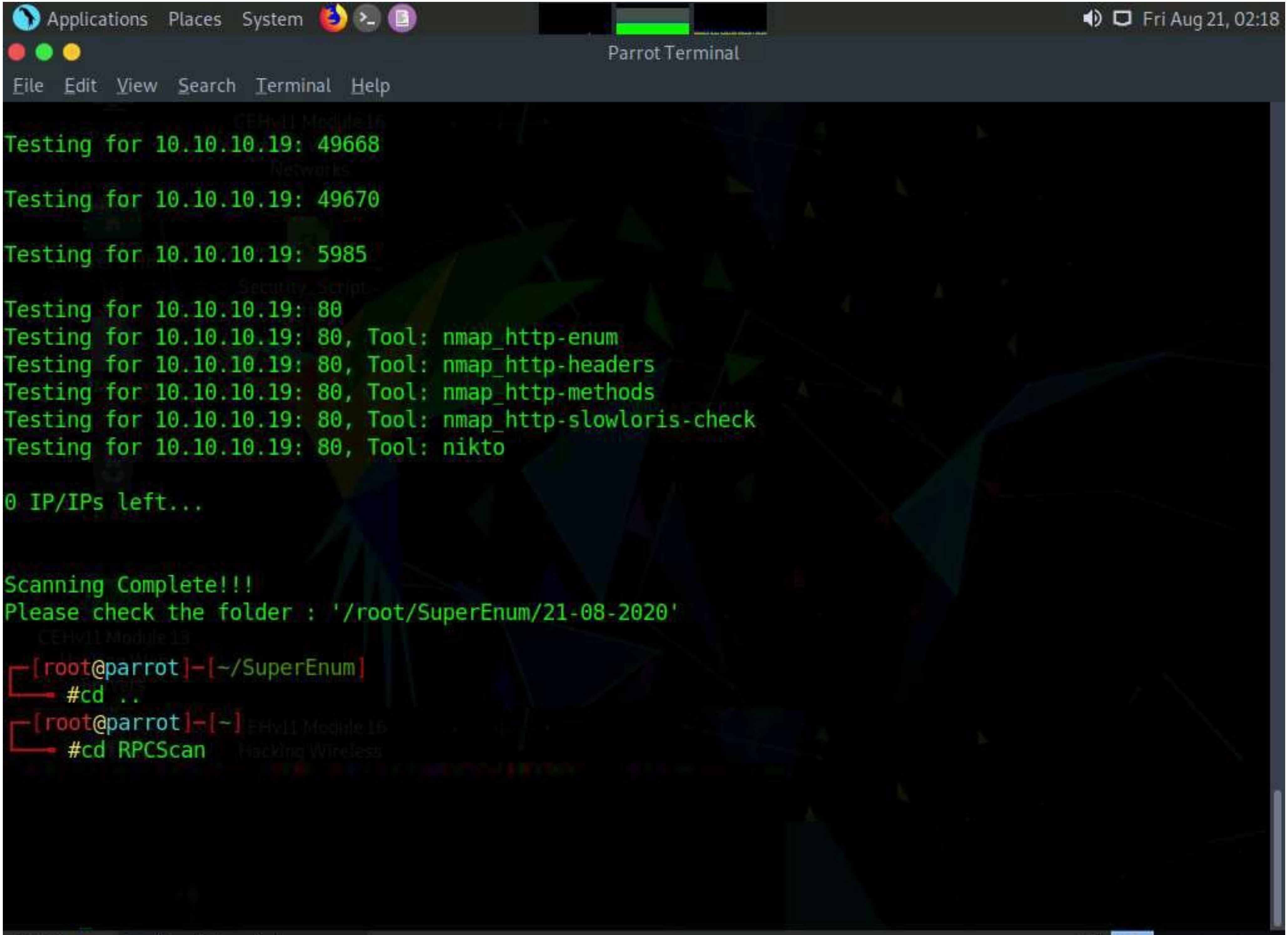
```
┌─[root@parrot]─[~/SuperEnum]
└──╼ #./superenum
Enter IP List filename with path
Target.txt

TCP Scan Started for IP: 10.10.10.19

UDP Scan Started for IP: 10.10.10.19

Testing for 10.10.10.19: 111
Testing for 10.10.10.19: 111, Tool: nmap_rpcinfo
Testing for 10.10.10.19: 111, Tool: rpcinfo
./superenum: line 116: rpcinfo: command not found

Testing for 10.10.10.19: 135
Testing for 10.10.10.19: 135, Tool: nbtscan
Testing for 10.10.10.19: 135, Tool: nmap_smb-enum-shares
Testing for 10.10.10.19: 135, Tool: nmap_smb-enum-users
Testing for 10.10.10.19: 135, Tool: nmap_smb-system-info
Testing for 10.10.10.19: 135, Tool: nmap_smb-os-discovery
Testing for 10.10.10.19: 135, Tool: nmap_smb-security-mode
Testing for 10.10.10.19: 135, Tool: nmap_smbv2-enabled
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:818: 'smbv2-enabled' did not match a category, filename, or direc
tory
stack traceback:
        [C]: in function 'error'
        /usr/bin/../share/nmap/nse_main.lua:818: in local 'get_chosen_scripts'
        /usr/bin/../share/nmap/nse_main.lua:1310: in main chunk
        [C]: in ?
```

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



```
Testing for 10.10.10.19: 2049
Testing for 10.10.10.19: 2049, Tool: nmap_nfs-ls
Testing for 10.10.10.19: 2049, Tool: nmap_nfs-statfs
Testing for 10.10.10.19: 2049, Tool: showmount
./superenum: line 116: showmount: command not found

Testing for 10.10.10.19: 2103

Testing for 10.10.10.19: 2105

Testing for 10.10.10.19: 2107

Testing for 10.10.10.19: 3389
Testing for 10.10.10.19: 3389, Tool: nmap_rdp-enum-encryption
Testing for 10.10.10.19: 3389, Tool: nmap_rdp-vuln-ms12-020

Testing for 10.10.10.19: 445
Testing for 10.10.10.19: 445, Tool: nbtscan
Testing for 10.10.10.19: 445, Tool: nmap_smb-enum-shares
Testing for 10.10.10.19: 445, Tool: nmap_smb-enum-users
Testing for 10.10.10.19: 445, Tool: nmap_smb-system-info
Testing for 10.10.10.19: 445, Tool: nmap_smb-os-discovery
Testing for 10.10.10.19: 445, Tool: nmap_smb-security-mode
Testing for 10.10.10.19: 445, Tool: nmap_smbv2-enabled
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:818: 'smbv2-enabled' did not match a category, filename, or direc
tory
stack traceback:
        [C]: in function 'error'
```

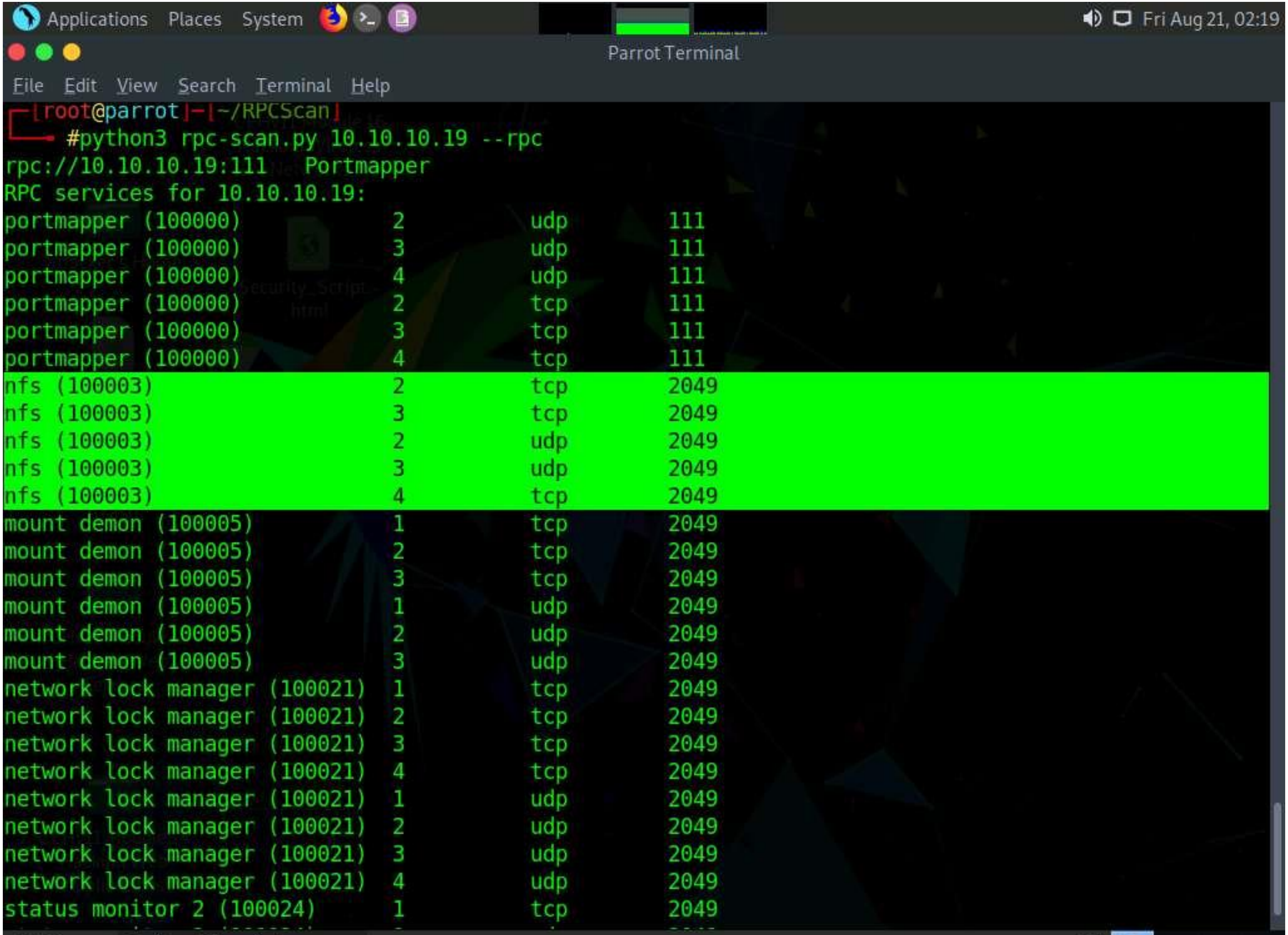
20. □ You can also observe the other open ports and the services running on them.
21. □ In the terminal window, type **cd ..** and press **Enter** to return to the root directory.
22. □ Now, we will perform NFS enumeration using RPCScan. To do so, type **cd RPCScan** and press **Enter**



```
Testing for 10.10.10.19: 49668

Testing for 10.10.10.19: 49670

Testing for 10.10.10.19: 5985

Testing for 10.10.10.19: 80
Testing for 10.10.10.19: 80, Tool: nmap_http-enum
Testing for 10.10.10.19: 80, Tool: nmap_http-headers
Testing for 10.10.10.19: 80, Tool: nmap_http-methods
Testing for 10.10.10.19: 80, Tool: nmap_http-slowloris-check
Testing for 10.10.10.19: 80, Tool: nikto

0 IP/IPs left...


Scanning Complete!!!
Please check the folder : '/root/SuperEnum/21-08-2020'

┌─[root@parrot]─[~/SuperEnum]
└──╼ #cd ..
┌─[root@parrot]─[~]
└──╼ #cd RPCScan
```

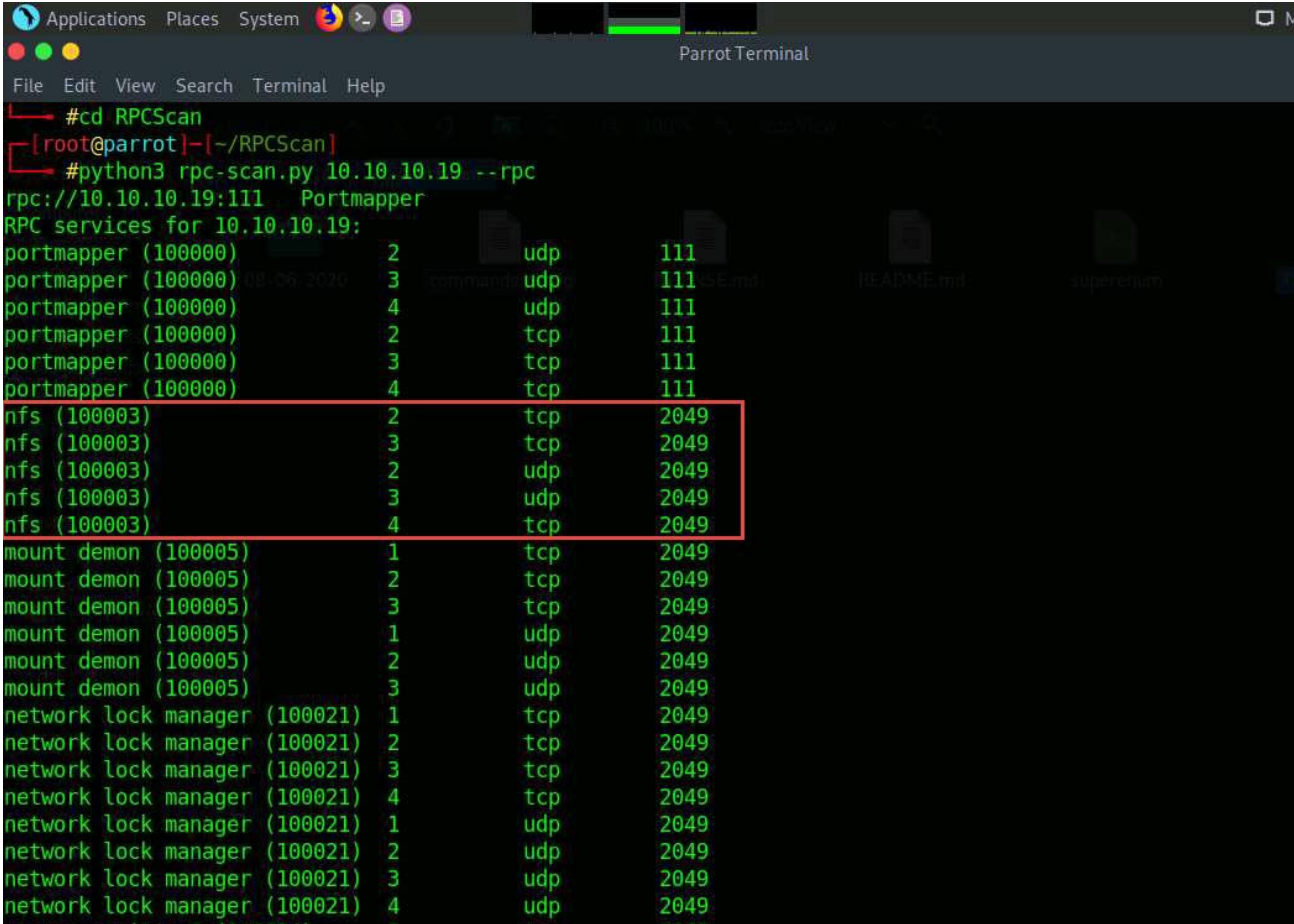
23. □ Type **python3 rpc-scan.py [Target IP address] --rpc** (in this case, the target IP address is **10.10.10.19**, the **Windows Server 2019** machine); press **Enter**.

--rpc: lists the RPC (portmapper); the target IP address may differ in your lab environment.



```
┌─[root@parrot]─[~/RPCScan]
└──╼ #python3 rpc-scan.py 10.10.10.19 --rpc
rpc://10.10.10.19:111   Portmapper
RPC services for 10.10.10.19:
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
network lock manager (100021)  4          tcp        2049
network lock manager (100021)  1          udp        2049
network lock manager (100021)  2          udp        2049
network lock manager (100021)  3          udp        2049
network lock manager (100021)  4          udp        2049
status monitor 2 (100024)      1          tcp        2049
```

24. The result appears, displaying that port 2049 is open, and the NFS service is running on it.



```
└──╼ #cd RPCScan
┌─[root@parrot]─[~/RPCScan]
└──╼ #python3 rpc-scan.py 10.10.10.19 --rpc
rpc://10.10.10.19:111   Portmapper
RPC services for 10.10.10.19:
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
network lock manager (100021)  4          tcp        2049
network lock manager (100021)  1          udp        2049
network lock manager (100021)  2          udp        2049
network lock manager (100021)  3          udp        2049
network lock manager (100021)  4          udp        2049
```

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

26. □ Close all open windows and document all the acquired information.