Network Penetration Testing Methodology-Internal

6 Hr 40 Min Remaining

Instructions Resources Help  100%

Exercise 11: Pentesting Misconfigured RPC Service and NFS Shares

Scenario

Network File System (NFS) is a client/server application which allows you to view or share files and folders between Linux/Unix systems. It is a way of mounting Linux discs/directories over a network. RPC server is a program which accepts connections from an RPC client and provides services to the client.

Poor configuration of NFS and RPC services might allow attackers to:

* First, find the NFS and mountd services running on a computer, using rpc
* Second, mount the NFS shares and view the contents in the mounted directories

As a pentester, you need to know how to enumerate RPC services and mount poorly configured servers.

**Lab Duration**: **20** Minutes

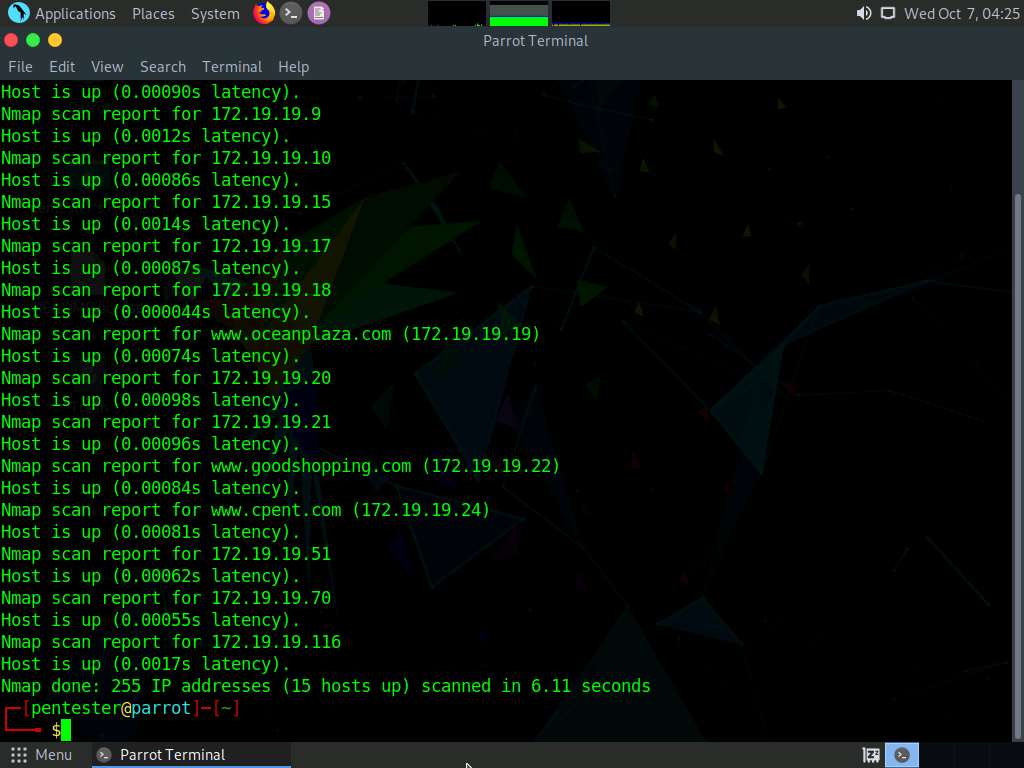
1. Click [Parrot](https://labclient.labondemand.com/Instructions/52f4d542-434e-4a10-8f51-0c2b8ca1d32b?rc=10). Parrot lock screen appears.



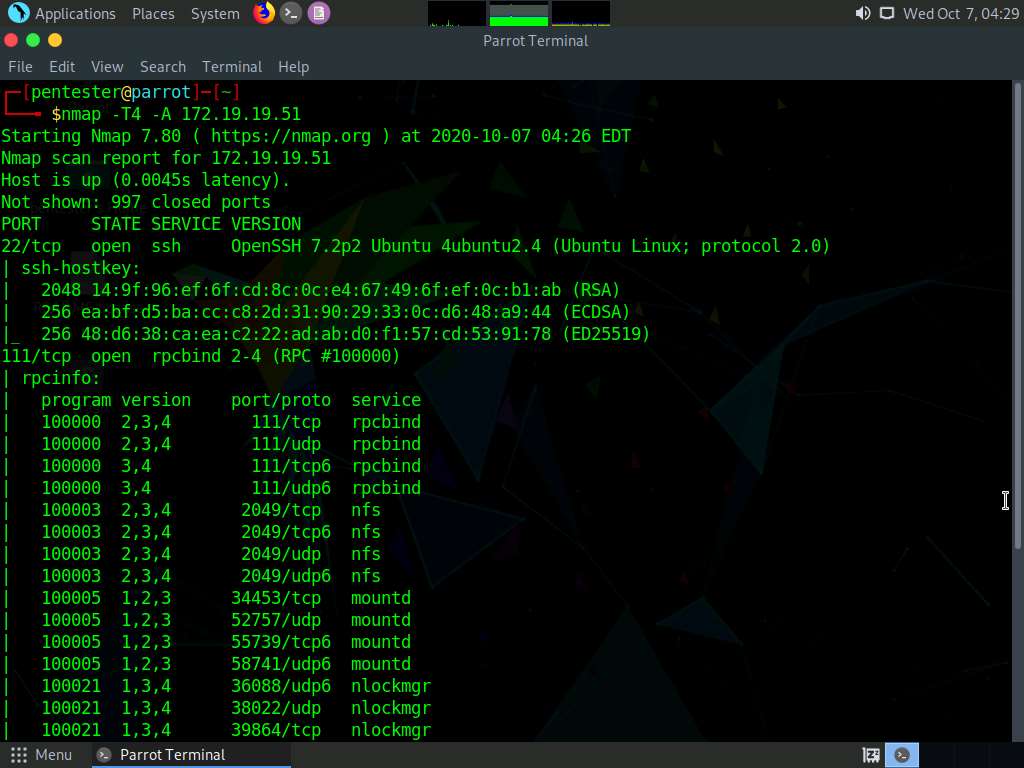
1. By default **pentester** is selected as the **user**. Type **toor** in the Password field and press **Enter**.

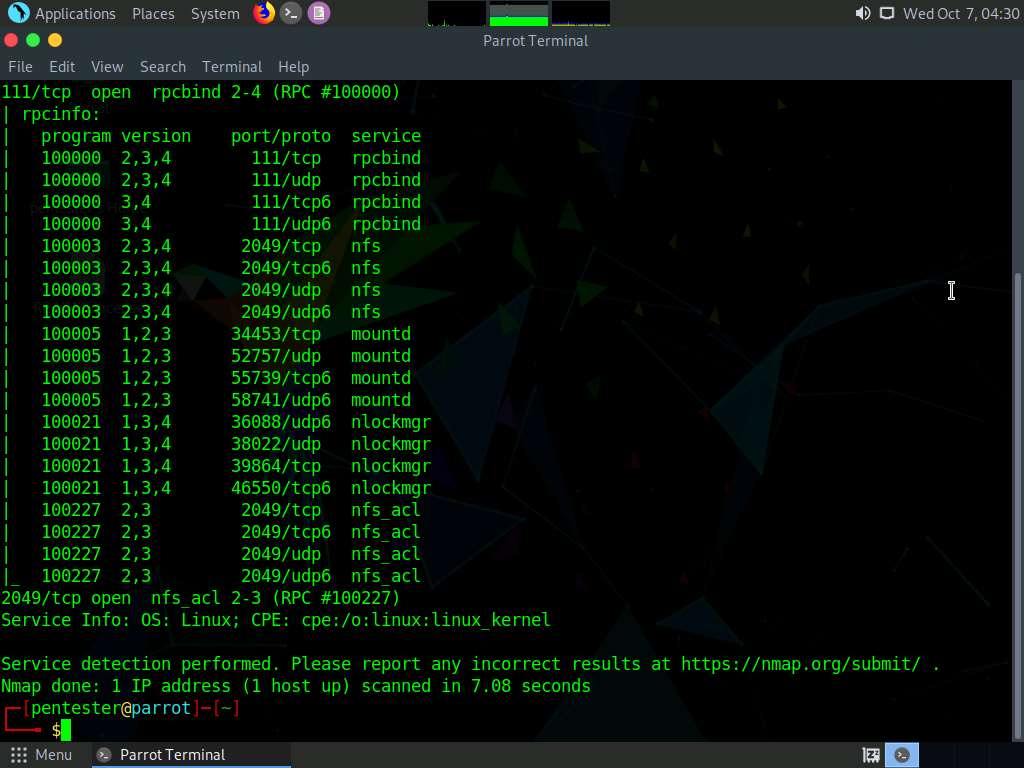


1. In this lab, we will be scanning a subnet for live machines. Select one machine and pentest the machine to gain access to it. For doing a quick scan, we will do a ping sweep using Nmap. In this lab, we are choosing an internal network for pentesting. Launch a command line terminal, type **nmap -sP 172.19.19.1-255** and press **Enter**. This displays all the hosts that are up in the network within a minute. In this lab, we are choosing **172.19.19.51** (**RPC Server Ubuntu**) as our target.

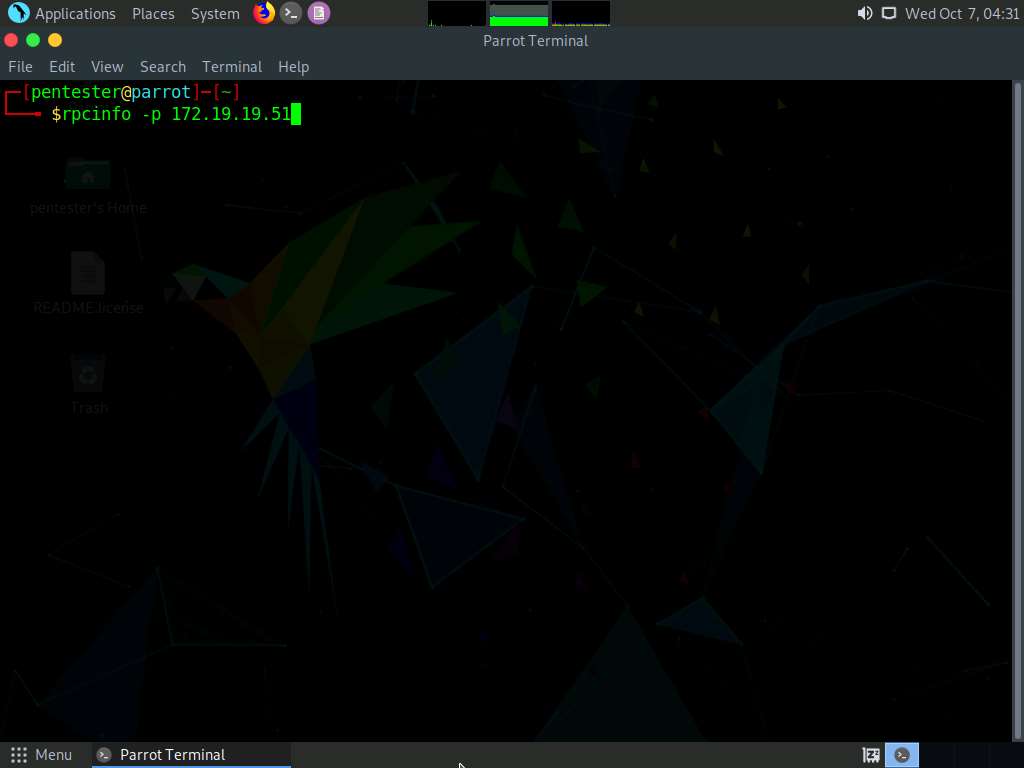


1. Type **nmap -T4 -A 172.19.19.51** in the terminal and press **Enter**. This will launch an Nmap scan on **RPC Server Ubuntu** machine.
2. Nmap takes around 30 seconds to complete the scan. On completing the scan, you will observe that the services rpc, ftp, nfs and mountd are running on the victim machine. From the scan, it is observed that an NFS File system is mounted on the remote machine. In this lab, we shall focus on the **RPC**, **NFS** and **mountd** services.

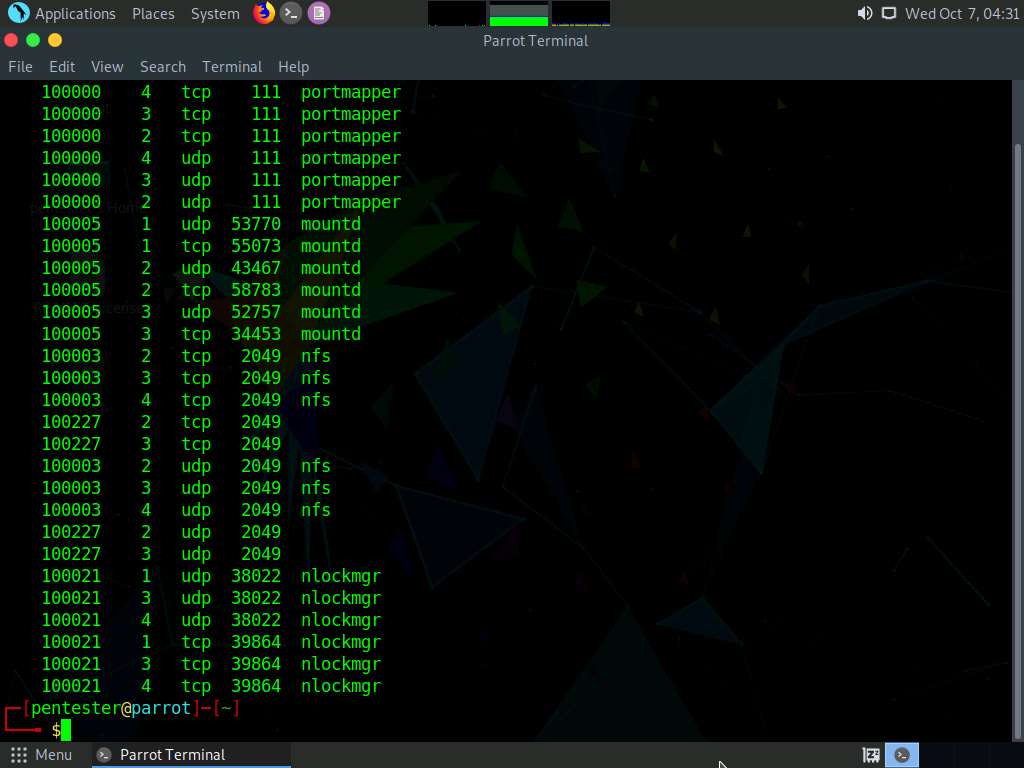




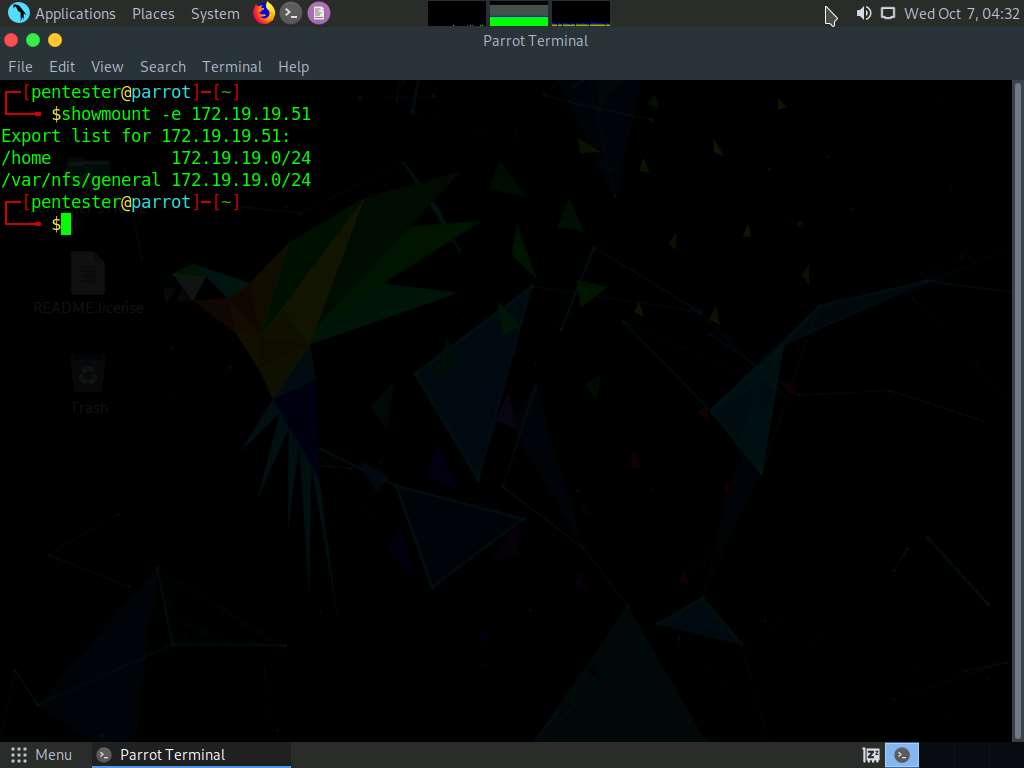
1. Now, we shall perform RPC enumeration to enumerate all the RPC services. Type **rpcinfo -p 172.19.19.51** in the command line terminal and press **Enter**.



1. We observe that **nfs** and **mountd** services are active on the remote machine.

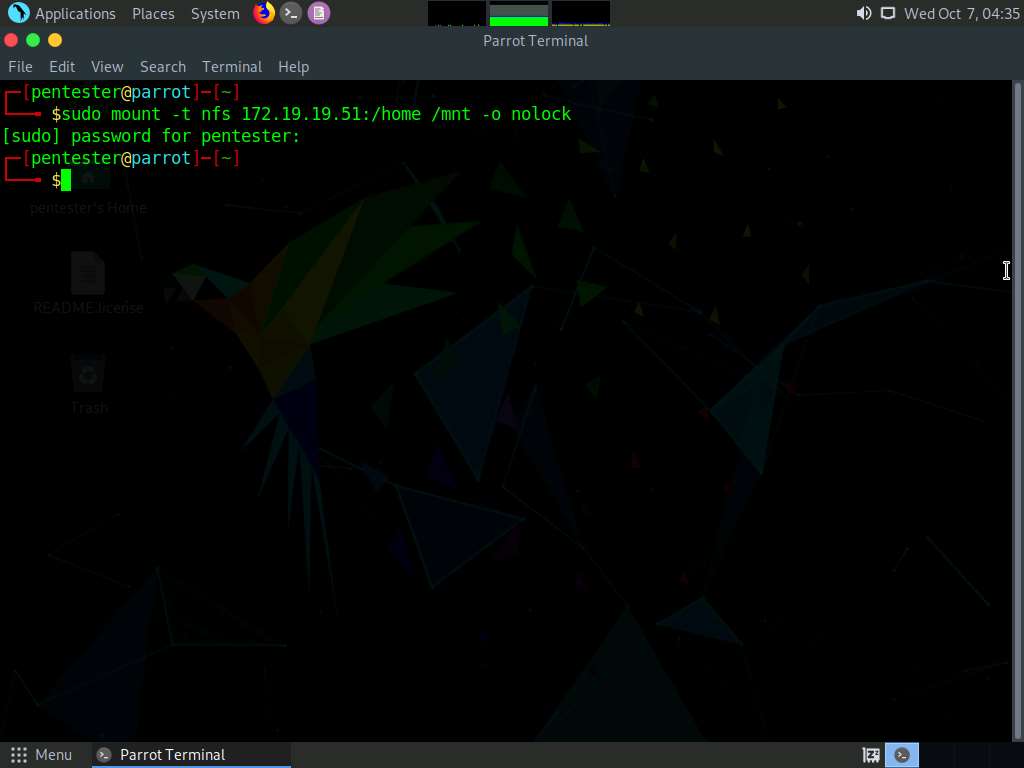


1. Now, we shall issue the **showmount** command to discover NFS shares listed in **/etc/exports** file of the remote machine. Type **showmount -e 172.19.19.51** and press **Enter**. This will display all the NFS shares on the remote machine as shown in the screenshot below:

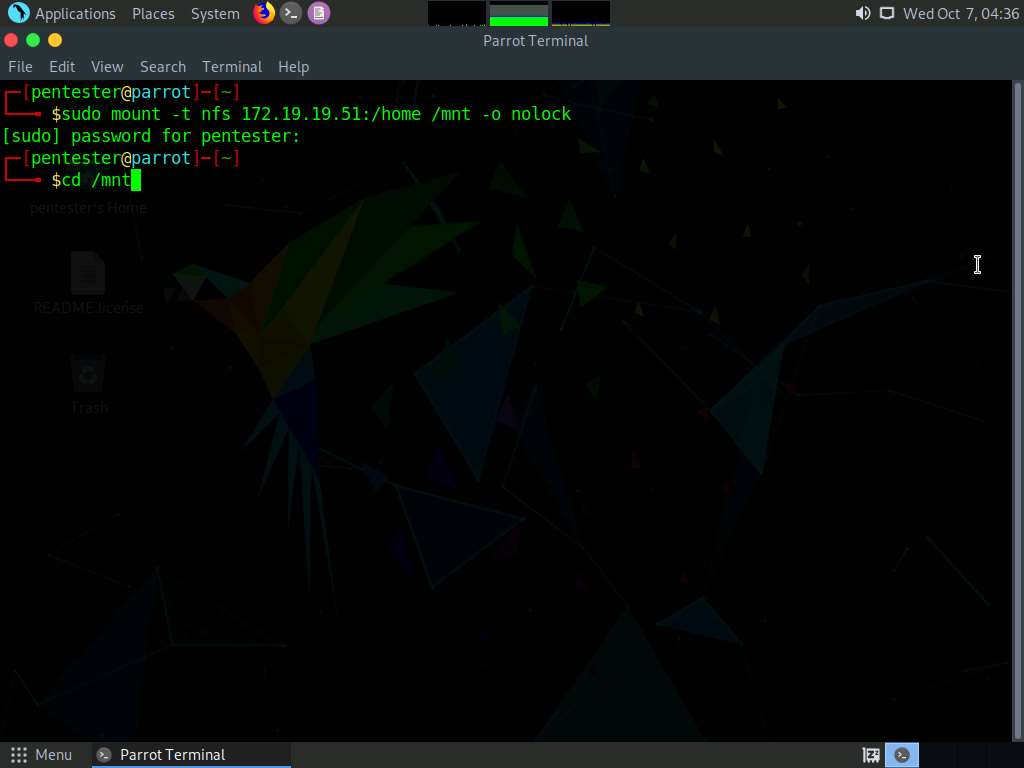


1. As we saw in the previous task, the /home file system was shared on the remote machine. We will be mounting this file system on the Parrot machine to the **mnt** directory. To mount, type **sudo mount -t nfs 172.19.19.51:/home /mnt -o nolock** and press **Enter**. Type **toor** and press **Enter** when prompted.

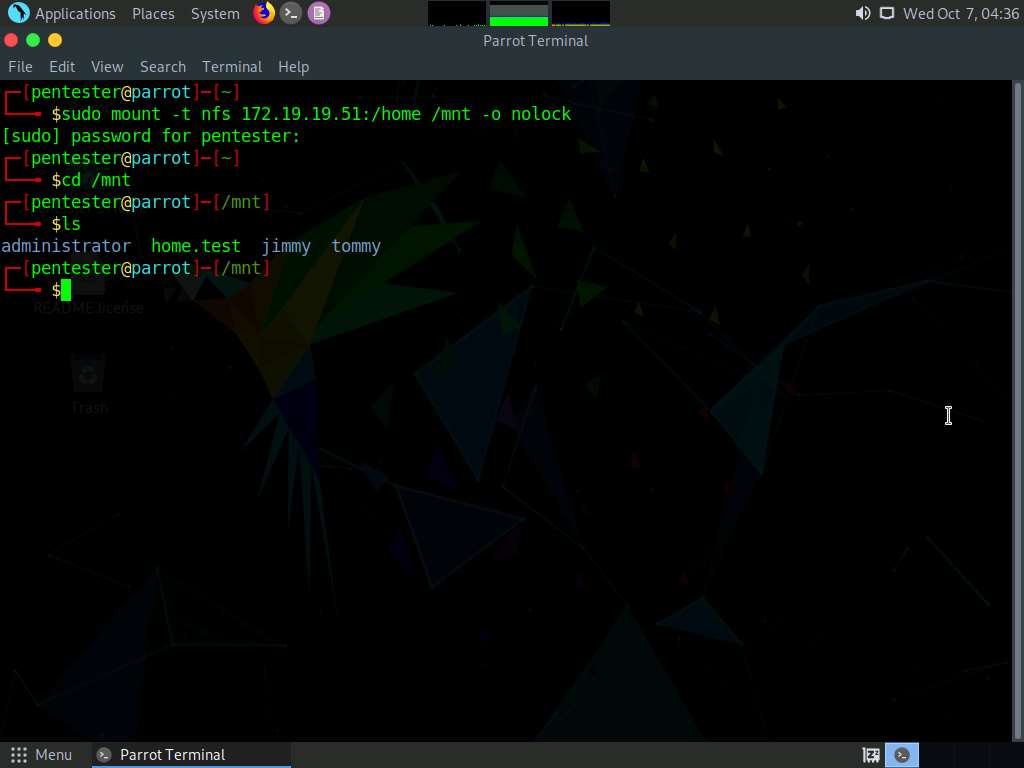
**-t** specifies the type of the file system (**nfs**). Specifying **nolock** disables the file locking.



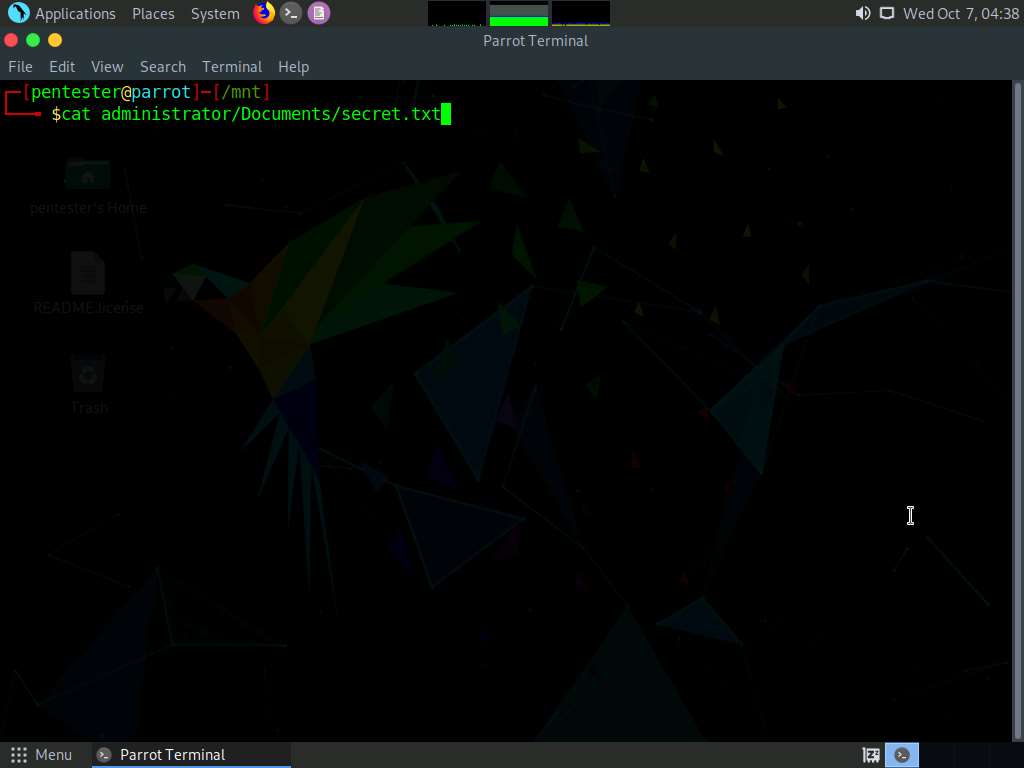
1. Now, we have successfully mounted the file system to the **/mnt** directory. To view the contents of the file system, we need to change the present directory to **/mnt**. Type **cd /mnt** and press **Enter**.



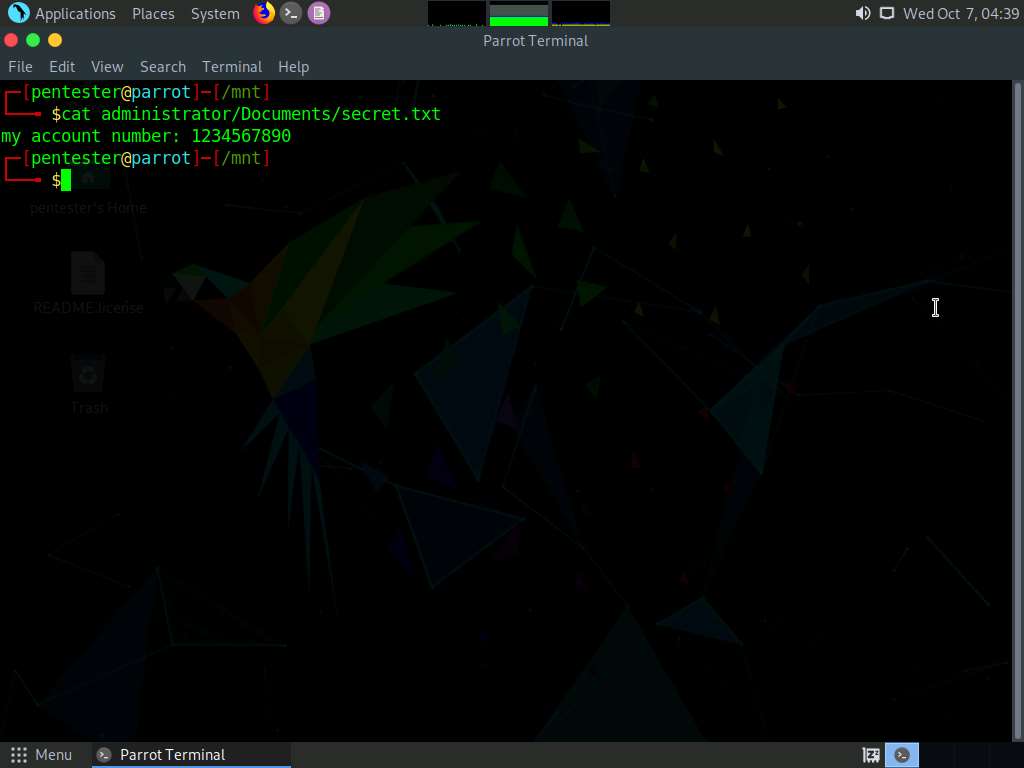
1. Type **ls** and press **Enter** to view the files and directories contained in the **/home** folder i.e., /mnt.



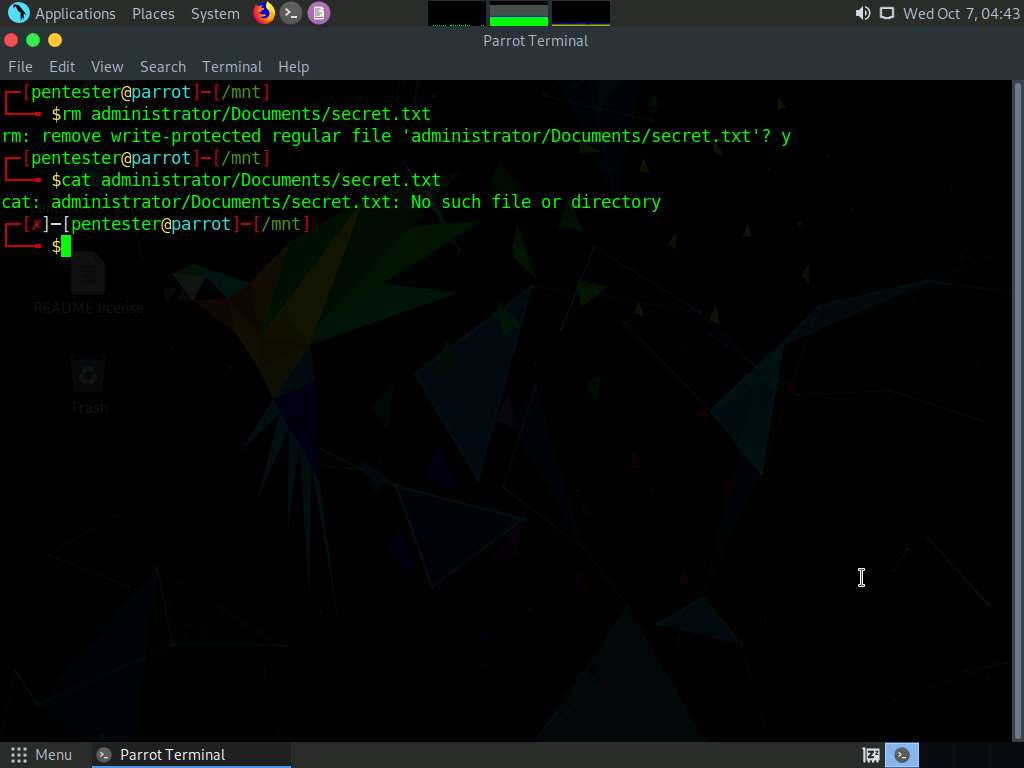
1. As a proof of concept, we shall now view the contents of a **secret.txt** file located in the **administrator/Documents** directory. Type **cat administrator/Documents/secret.txt** and press **Enter**.



1. On entering the command in the previous task, the cat command displays the file contents in the secret.txt file successfully, meaning we have successfully mounted the remote file system and accessed the contents in it.



1. Now, we shall see if we are able to tamper/delete the files in the remote file system. Type **rm administrator/Documents/secret.txt** and press **Enter**. Type **y** and press **Enter** to confirm the deletion. To confirm that the file has been successfully deleted, type **cat administrator/Documents/secret.txt** and press **Enter**. The terminal displays an error stating no such file or directory has been found. This proves that we have unrestricted access to the file system.

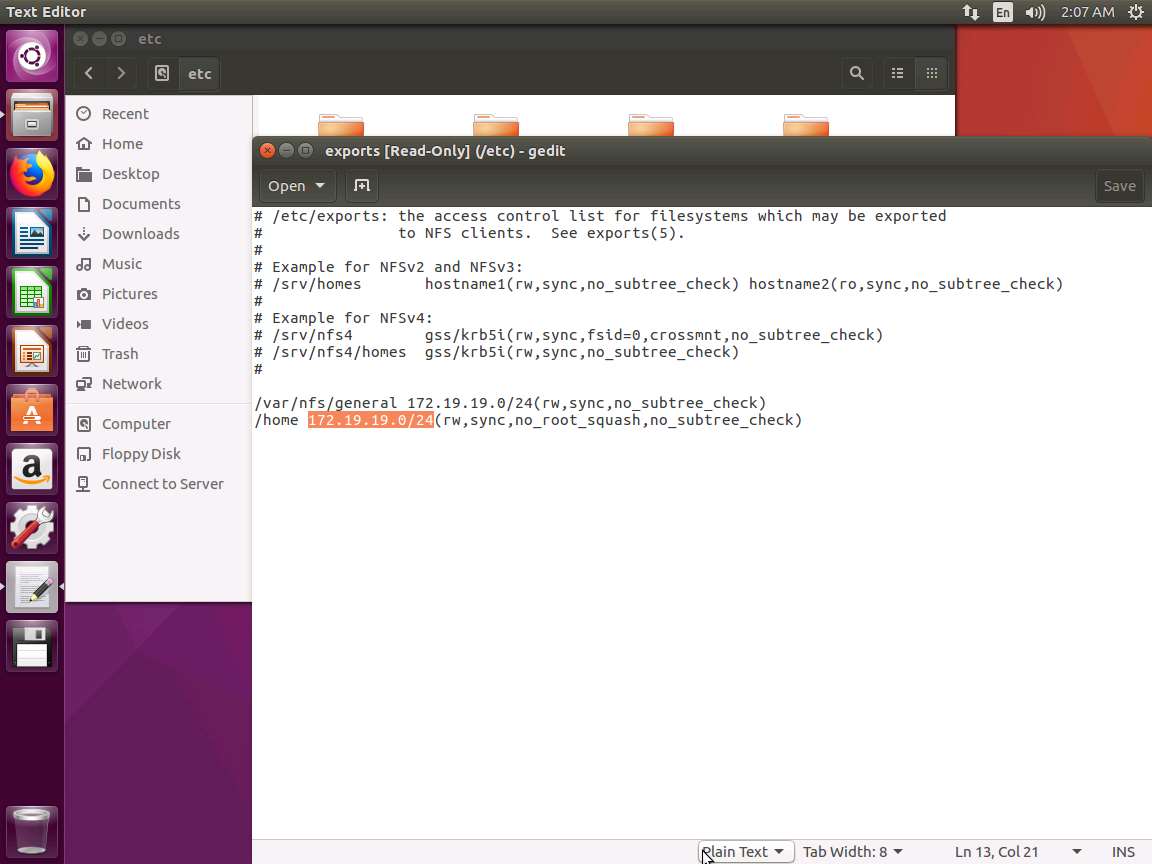


1. The reason we were able to access the remote shares is:
   1. The entire subnet has been specified in the exports file, allowing everyone in that particular network to access the file.

We were able to manipulate the files in the file system since:

* 1. no\_root\_squash option was enabled, allowing any user to perform read, write and execute actions on the mounted file system.

This is just a proof of concept to show the reason for the vulnerability and you are not required to log in to the machine to view the above-mentioned file.



In this lab, you have learned how to enumerate RPC services and mount NFS shared directories.