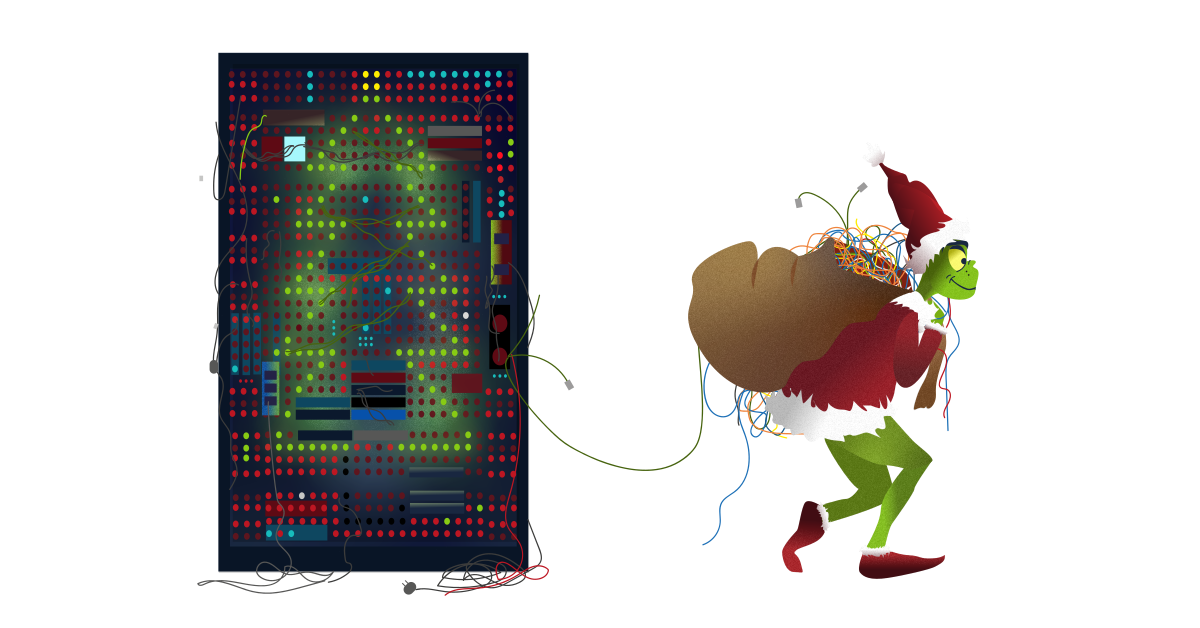
Grinch Enterprises has been leaving traces of how their hackers have been accessing data from the system - you’ve found a unique server they use. We need your help to find out what method they’ve been using to extract any data.

We have noticed that 10.10.44.163 is generating unusual traffic. We highly suspect that Grinch Enterprises are using it to access our data. We will use Nmap to discover the services are running on their server.



***Answer the questions below***

Scan the target server with the IP 10.10.44.163. Remember that MS Windows hosts block pings by default, so we need to add -Pn, for example, nmap -Pn 10.10.44.163 for the scan to work correctly. How many TCP ports are open?



Correct Answer

 Hint

Network File System (NFS) is a protocol that allows the ability to transfer files between different computers and is available on many systems, including MS Windows and Linux. Consequently, NFS makes it easy to share files between various operating systems.

In the scan results you received earlier, you should be able to spot NFS or mountd, depending on whether you used the -sV option with Nmap or not. Which port is detected by Nmap as NFS or using the mountd service?



Correct Answer

Now that we have discovered an NFS service is listening, let’s check what files are being shared. We can do this using the command showmount. In the terminal below, we run showmount -e 10.10.44.163. The -e or --exports show the NFS server’s export list.

Pentester Terminal

pentester@TryHackMe**$** showmount -e 10.10.44.163 Export list for 10.10.44.163: /share (everyone) /my-notes (noone)

As we can see in the terminal output above, we have two shares, /share and /my-notes. After you have started the attached machine, use the AttackBox terminal to discover the shares on 10.10.44.163.

How many shares did you find?



Correct Answer

How many shares show “everyone”?



Correct Answer

Let’s try to mount the shares we have discovered. We can create a directory on the AttackBox using mkdir tmp1, where tmp1 is the directory’s name. Then we can use this directory  we created to mount the public NFS share using: mount 10.10.44.163:/my-notes tmp1.

Pentester Terminal

pentester@TryHackMe**$** mount 10.10.44.163:/my-notes tmp1 mount.nfs: access denied by server while mounting 10.10.44.163:/my-notes

We can see that the mounting has failed. my-notes is not public and requires specific authentication mechanisms that we don’t have access to. Let’s try again with the other folder, share.

Pentester Terminal

pentester@TryHackMe**$** mount 10.10.44.163:/share tmp1

We didn’t get any error messages, so it was a success. Let’s go inside the share to see what’s inside it using cd tmp1, then ls.

Pentester Terminal

pentester@TryHackMe**$** ls 132-0.txt 2680-0.txt

There are two text files. We can open the file using any text editor such as nano FILENAME or something quicker such as less FILENAME.

What is the title of file 2680-0.txt?



Correct Answer

 Hint

It seems that Grinch Enterprises has forgotten their SSH keys on our system. One of the shares contains a private key used for SSH authentication (id\_rsa). What is the name of the share?



Correct Answer

We can calculate the MD5 sum of a file using md5sum FILENAME. What is the MD5 sum of id\_rsa?