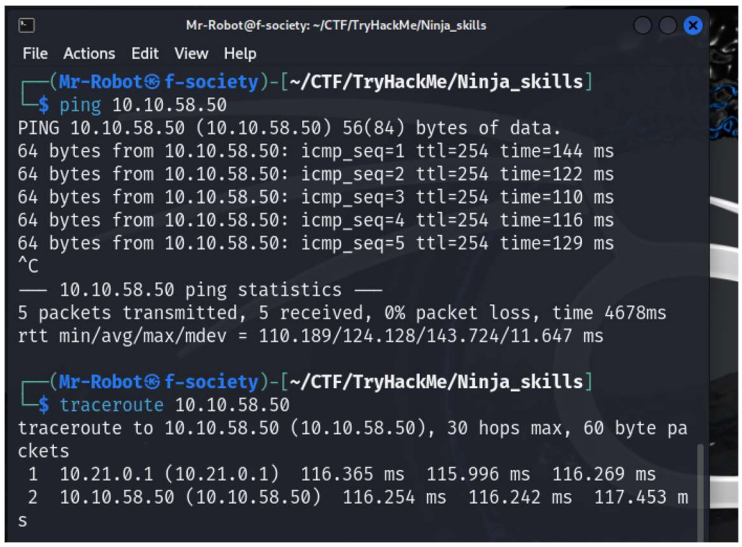
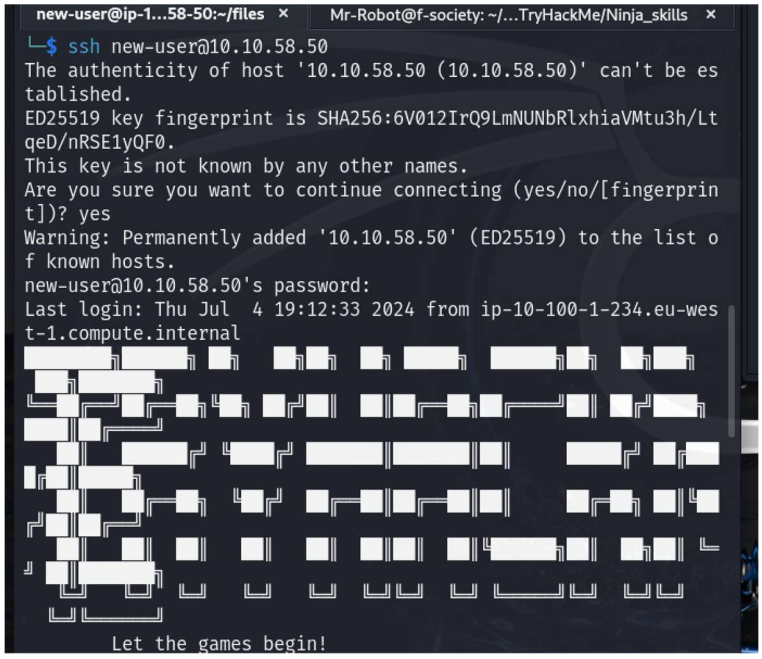
Ninja skills CTF from TryHackme

Follow the writeup to complete the CTF:

1. First as we always do we connect our VPN
    - sudo openvpn {name of vpn}
2. Now that we are connected let's check if the target machine is up by using ping and traceroute.



3. Since the target machine is up and running, we can now connect to it using ssh since we are given the username and password.



4. After login in, we can now start to search for the files using the “find” tool which is a powerful tool. First let’s find each file using find:

```
[new-user@ip-10-10-58-50 files]$ cd /tmp
[new-user@ip-10-10-58-50 tmp]$ find / -type f \( -name 8V2L -o -
o -name SRSq -o -name uqyw -o -name v2Vb -o -name X1Uy \) 2>/dev
/mnt/D8B3
/mnt/c4ZX
/var/FHl1
/var/log/uqyw
/opt/PFbD
/opt/oiMO
/media/rmfX
/etc/8V2L
/etc/ssh/SRSq
/home/v2Vb
/X1Uy
[new-user@ip-10-10-58-50 tmp]$
```

- / = search in the “root directory” which is top-level directory.
- -type = specify the type whether file or directory.
- 2>/dev/null = redirect error message to dev null

5. Since now know where each file is located we can navigate to where they are and find there group by using the comman “ls -la” or we can do the following:

```
[new-user@ip-10-10-58-50 etc]$ find / -type f \( -name 8V2L -o -
name bnyO -o -name c4ZX -o -name D8B3 -o -name FHl1 -o -name oiM
O -o -name PFbD -o -name rmfX -o -name SRSq -o -name uqyw -o -na
me v2Vb -o -name X1Uy \) -exec ls -la {} \;  2>/dev/null
-rw-rw-r-- 1 new-user best-group 13545 Oct 23  2019 /mnt/D8B3
-rw-rw-r-- 1 new-user new-user 13545 Oct 23  2019 /mnt/c4ZX
-rw-rw-r-- 1 new-user new-user 13545 Oct 23  2019 /var/FHl1
-rw-rw-r-- 1 new-user new-user 13545 Oct 23  2019 /var/log/uqyw
-rw-rw-r-- 1 new-user new-user 13545 Oct 23  2019 /opt/PFbD
-rw-rw-r-- 1 new-user new-user 13545 Oct 23  2019 /opt/oiMO
-rw-rw-r-- 1 new-user new-user 13545 Oct 23  2019 /media/rmfX
-rwxrwxr-x 1 new-user new-user 13545 Oct 23  2019 /etc/8V2L
-rw-rw-r-- 1 new-user new-user 13545 Oct 23  2019 /etc/ssh/SRSq
-rw-rw-r-- 1 new-user best-group 13545 Oct 23  2019 /home/v2Vb
-rw-rw-r-- 1 newer-user new-user 13545 Oct 23  2019 /X1Uy
[new-user@ip-10-10-58-50 etc]$
```

- Here we just added “exec” command and we are instructing “find” to run another command using each result from find.

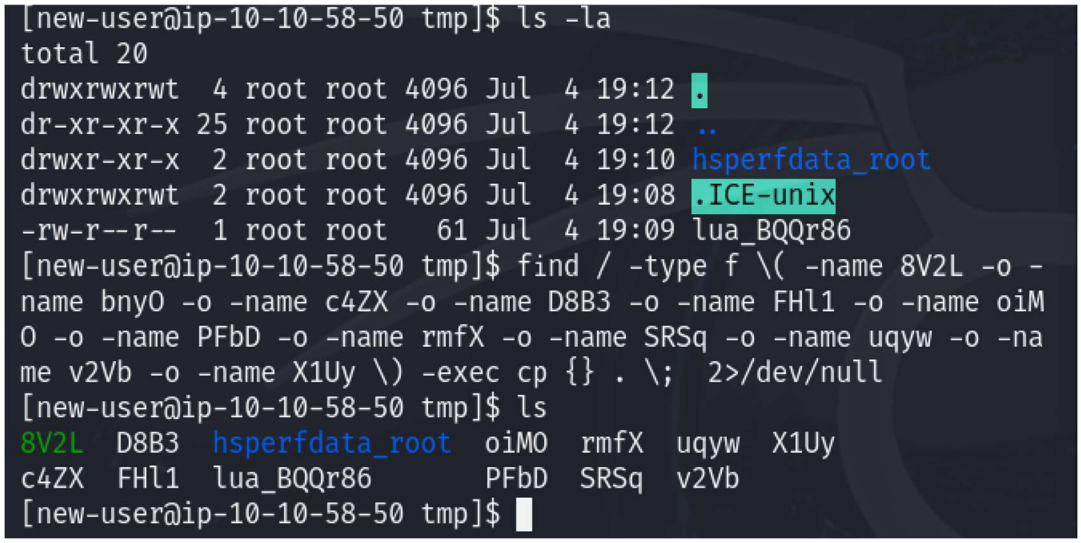
6. Since we found an easy way of finding and executing another command at the same time, we would do the same for finding the file with sha1sum, all we have to do is change the “ls -ls” with “sha1sum”.

```
[new-user@ip-10-10-58-50 etc]$ find / -type f \( -name 8V2L -o -
name bnyO -o -name c4ZX -o -name D8B3 -o -name FHl1 -o -name oiM
O -o -name PFbD -o -name rmfX -o -name SRSq -o -name uqyw -o -na
me v2Vb -o -name X1Uy \) -exec sha1sum {} \;  2>/dev/null
2c8de970ff0701c8fd6c55db8a5315e5615a9575  /mnt/D8B3
9d54da7584015647ba052173b84d45e8007eba94  /mnt/c4ZX
d5a35473a856ea30bfec5bf67b8b6e1fe96475b3  /var/FHl1
57226b5f4f1d5ca128f606581d7ca9bd6c45ca13  /var/log/uqyw
256933c34f1b42522298282ce5df3642be9a2dc9  /opt/PFbD
5b34294b3caa59c1006854fa0901352bf6476a8c  /opt/oiMO
4ef4c2df08bc60139c29e222f537b6bea7e4d6fa  /media/rmfX
0323e62f06b29ddbbe18f30a89cc123ae479a346  /etc/8V2L
acbbbce6c56feb7e351f866b806427403b7b103d  /etc/ssh/SRSq
7324353e3cd047b8150e0c95edf12e28be7c55d3  /home/v2Vb
59840c46fb64a4faeabb37da0744a46967d87e57  /X1Uy
```

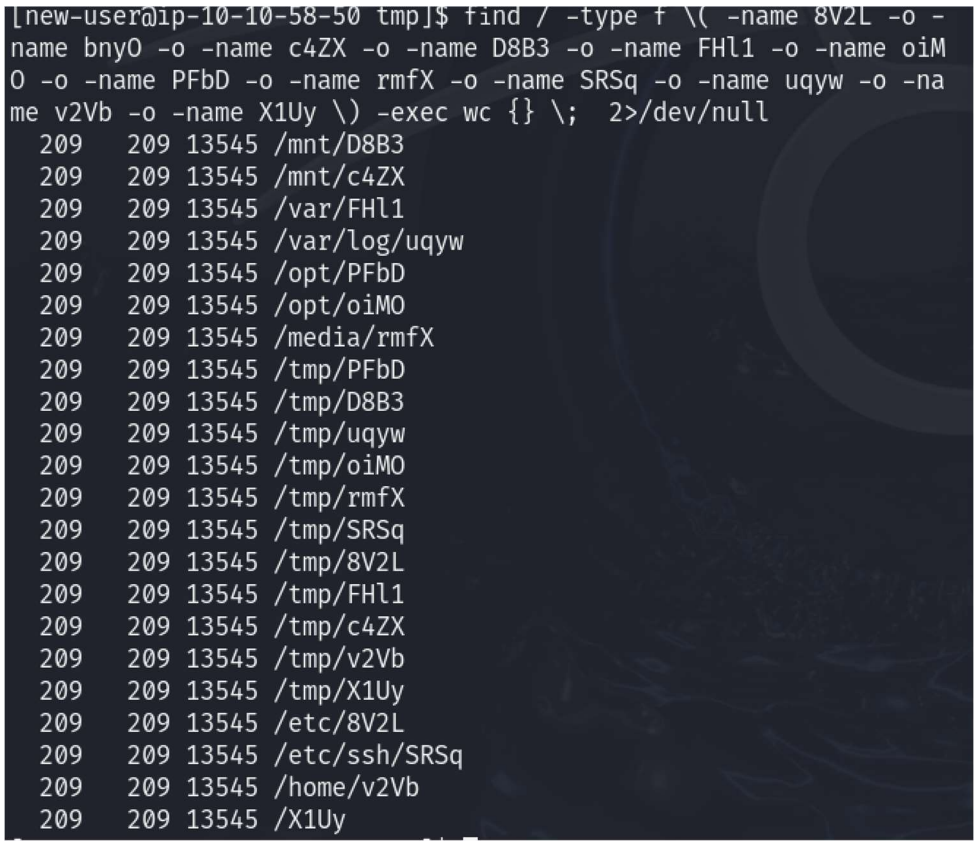
7. Next to find the file with and id of 502 we just change command after -exec to “ls -n”.

```
[new-user@ip-10-10-58-50 etc]$ find / -type f \( -name 8V2L -o -
name bnyO -o -name c4ZX -o -name D8B3 -o -name FHl1 -o -name oiM
O -o -name PFbD -o -name rmfX -o -name SRSq -o -name uqyw -o -na
me v2Vb -o -name X1Uy \) -exec ls -n {} \;  2>/dev/null
-rw-rw-r-- 1 501 502 13545 Oct 23  2019 /mnt/D8B3
-rw-rw-r-- 1 501 501 13545 Oct 23  2019 /mnt/c4ZX
-rw-rw-r-- 1 501 501 13545 Oct 23  2019 /var/FHl1
-rw-rw-r-- 1 501 501 13545 Oct 23  2019 /var/log/uqyw
-rw-rw-r-- 1 501 501 13545 Oct 23  2019 /opt/PFbD
-rw-rw-r-- 1 501 501 13545 Oct 23  2019 /opt/oiMO
-rw-rw-r-- 1 501 501 13545 Oct 23  2019 /media/rmfX
-rwxrwxr-x 1 501 501 13545 Oct 23  2019 /etc/8V2L
-rw-rw-r-- 1 501 501 13545 Oct 23  2019 /etc/ssh/SRSq
-rw-rw-r-- 1 501 502 13545 Oct 23  2019 /home/v2Vb
-rw-rw-r-- 1 502 501 13545 Oct 23  2019 /X1Uy
```

8. To find the executable file we will use the “cp” which copy command, to copy the executable file to our current directory.

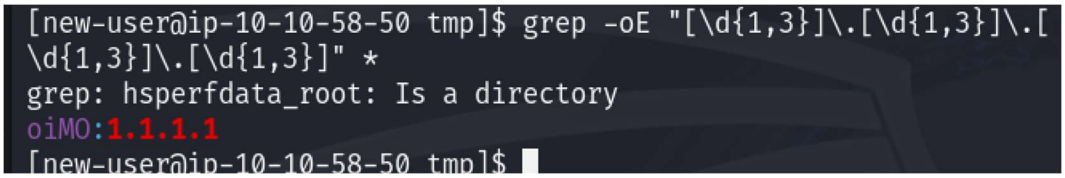


9. To find the file with 230 line we will use the “wc” command.



- Here since we see there is no file with 230 file so there is a file which does not appear on our search, so it should be that file.

10. To find the file with an ip we will use the grep command.



That’s all guys.

Happy learning and Happy Hacking.