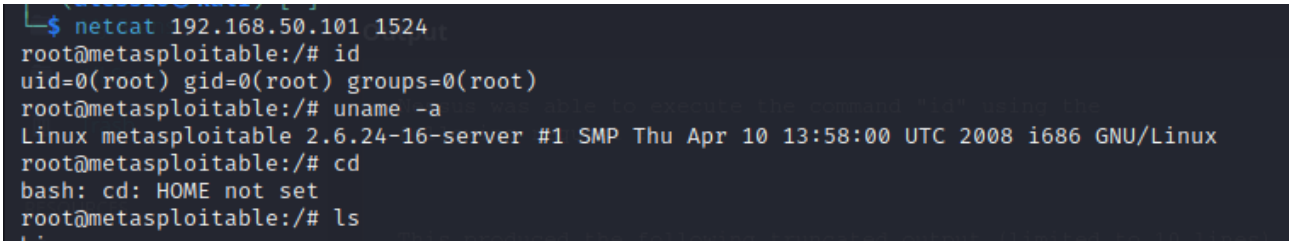
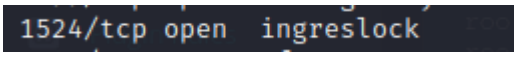
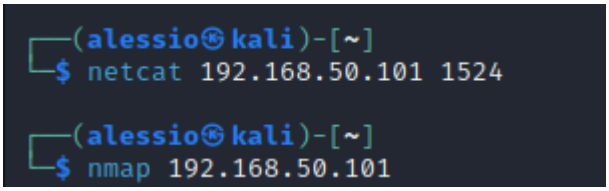
La prima vulnerabilità che ho affrontato e stata la presenza della backdoor sulla porta 1524 di meta.

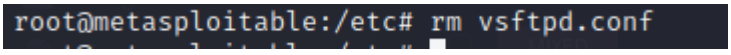




Innazitutto ho visto quali porte erano aperte con il comando nmap, poi ho visto che la 1524 era aperta (quella con la backdoor come mi aveva detto nessus), ed allora mi sono connesso con il comando netta alla porta in questione.



Questa e la parte finale dell ‘esercizio. Non ho riportato tutte le immagini per ogni passaggio perche avrei riempito troppe pagine. Comunque una volta connesso, con il comando ls ho visto che cartelle e file ci fossero all’interno della porta, poi aprendo tutte le cartelle e vedendo il contenuto con ls ho cercato file e elementi che mi facessero nascere qualche sospetto. Nella porta etc, ho trovato il file “vsftpd.conf” che mi ha fatto accendere subito la lampadina, dato che mi ha ricordato del comando letto su internet: /exploit/unix/ftp/vsftpd _234 backdoor. Il file mi sembrava sospetto, quindi dalla macchina metasploitable ho cancellato li filein questione.



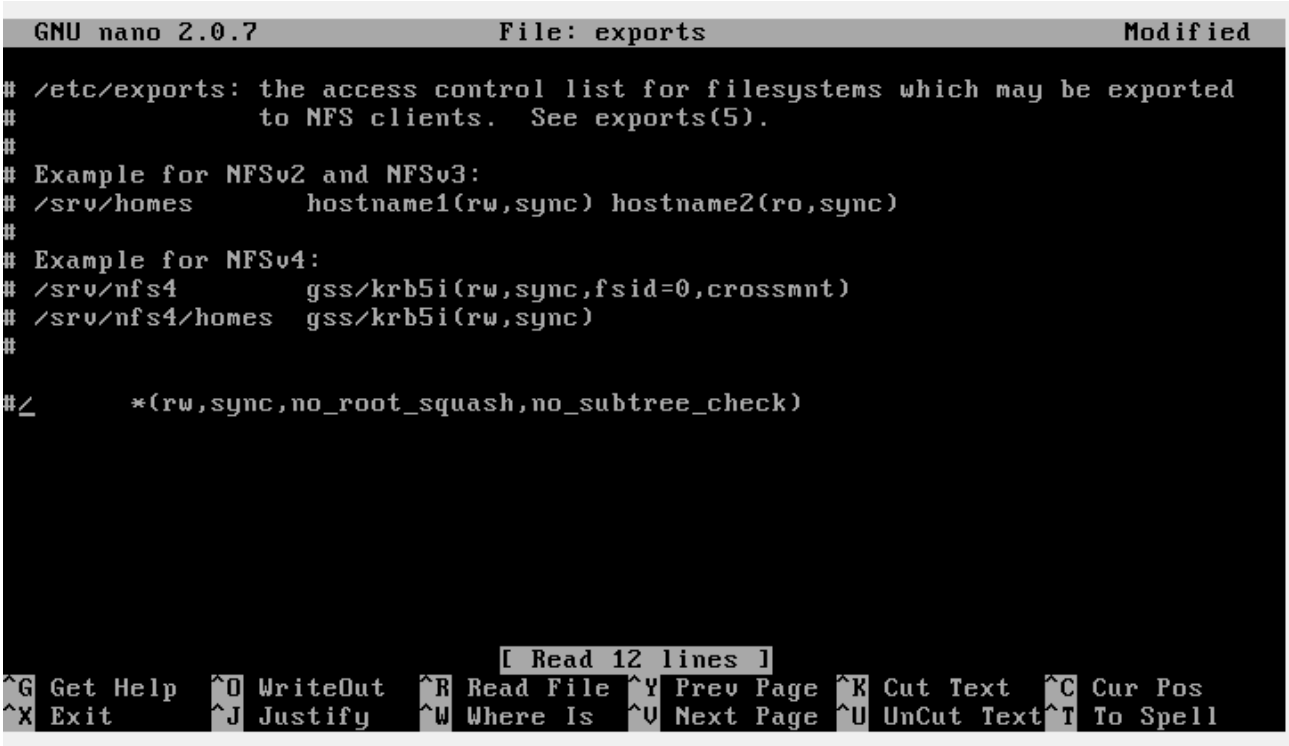
```
┌──(alessio㉿kali)-[~]
└─$ vncviewer 192.168.50.101
onnected to RFB server, using protocol version 3.3
erforming standard VNC authentication
assword:
uthentication successful
esktop name "root's X desktop (metasploitable:0)"
NC server default format:
 32 bits per pixel.
 Least significant byte first in each pixel.
 True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
sing default colormap which is TrueColor.  Pixel format:
 32 bits per pixel.
 Least significant byte first in each pixel.
 True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

L altra vulnerabilità risolta e quella della pssword weak sulla porta 5900. Mi sono connnesso alla porta usando il comando vncviewer e sono loggato con la password. POoi con il comando psswd, ho provveduto a cambiare la password con una piu sicura.

```
root@metasploitable:/# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@metasploitable:/#
```

☐	CRITICAL	10.0 *	NFS Exported Share Inform...	RPC	1

Questa e l ultima vulnerabilità che ho risolto. Fonfamentalmente su nfs (server per la condiviione file da remoto) permetteva a tutti i client che avevano la possiiblita di accedere i privilegi di root. Allora mi sono andato ad infomrmare ed ho scoperto che nel file exports, dentro la cartella etc (dove prima abbiamo eliminato la backdoor), c era la regola secondo la quale, seguendo qualunque path, ogni cliente avvea questi privilegi, quindi con il cancelletto la sono andato a neutralizzare :



La regola in questione era l'ultima.