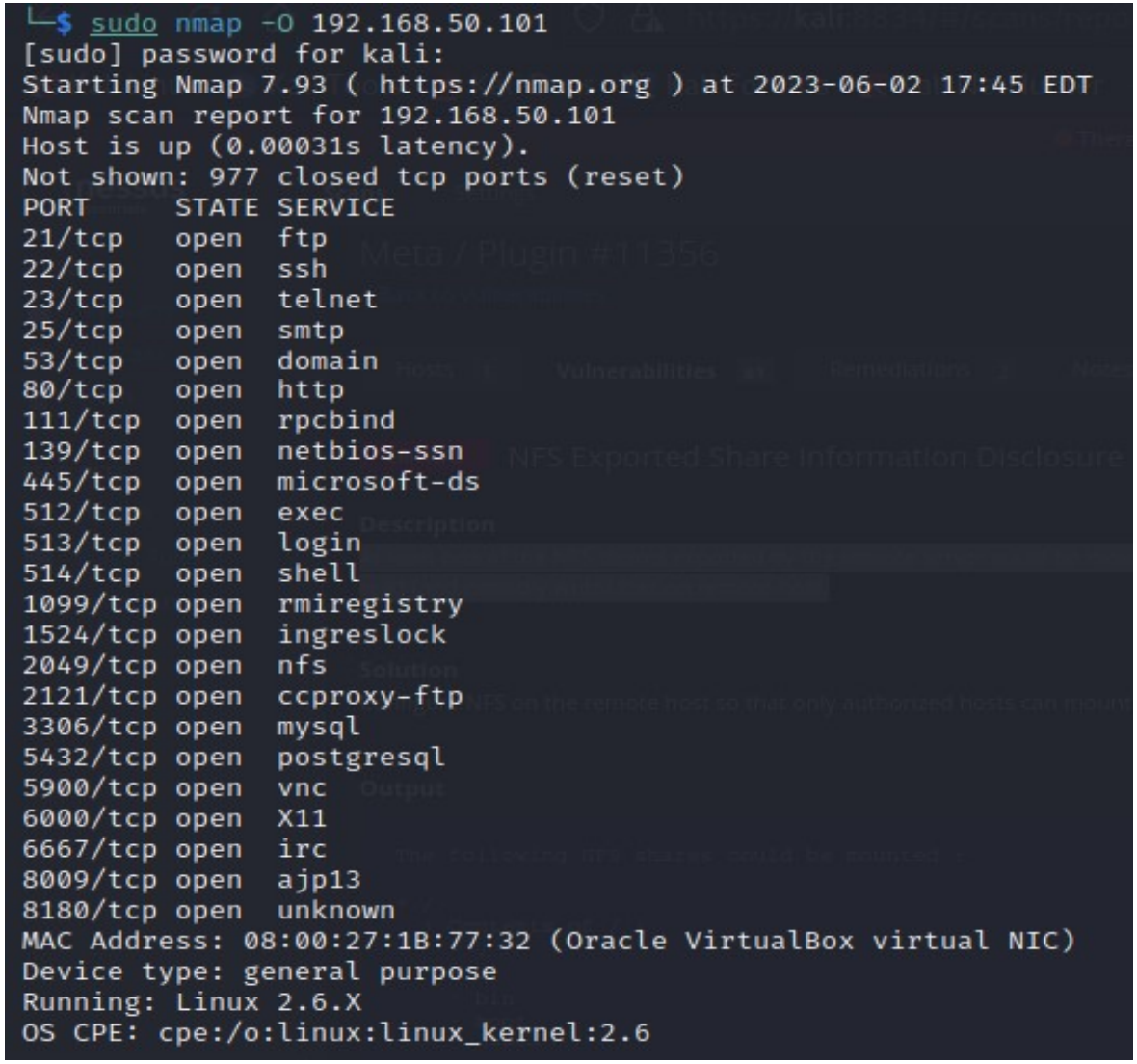
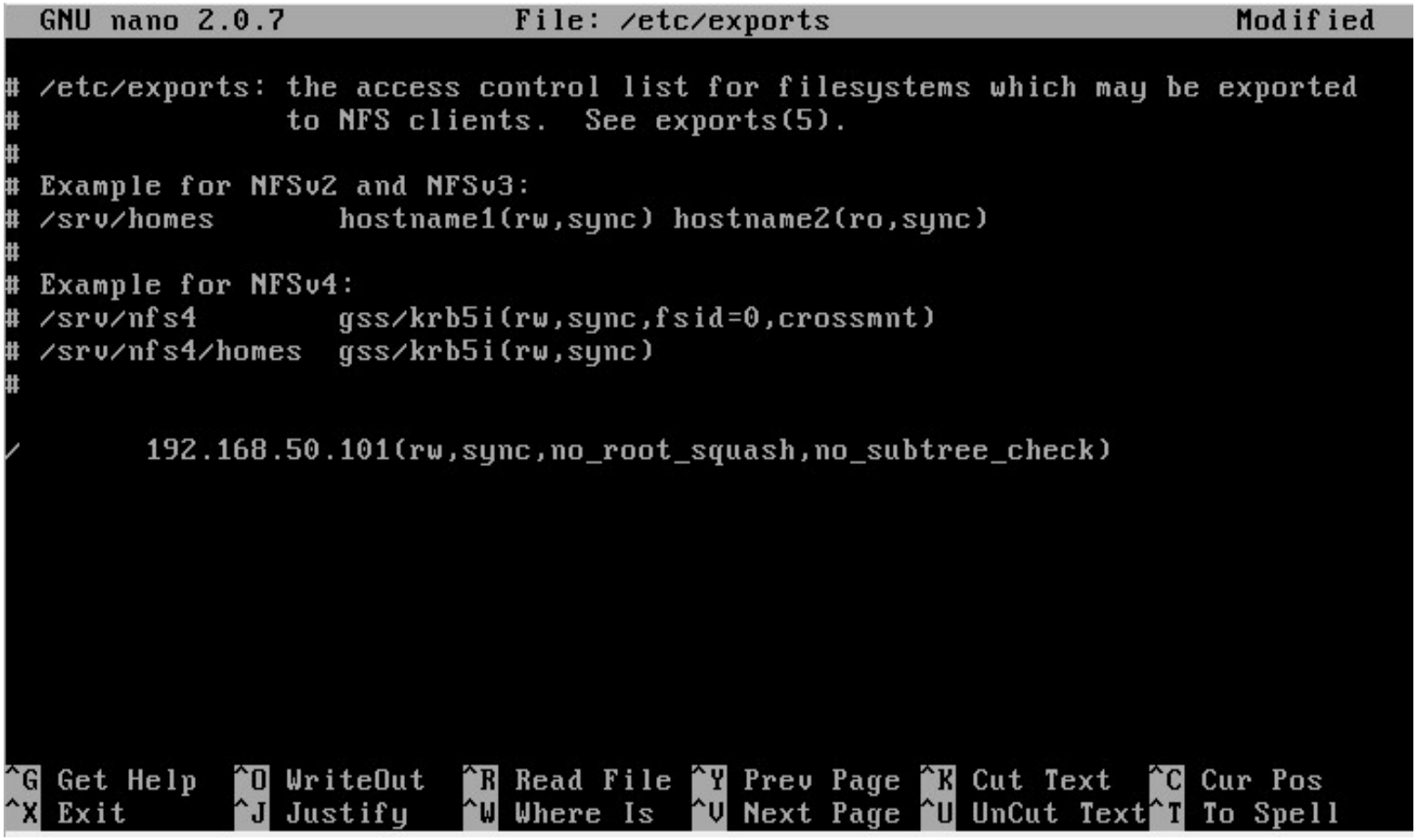
REMEDIATION META

Prima di iniziare la remediation meta, ho effetuato da kali una scansione con lo strumento “nmap” verso metasploitable. Ho usato il comando nmap –O 192.168.50.100



NFS Export Share Information Disclosure

Per risolvere il problema di questa vulnerabilità, ho aperto la shell di meta, con il comando “sudo su” sono entrato nel root di meta. Per cambiare la configurazione NFS, con il comando “nano /etc/exsport”, sono entrato nel file e nell’ultima riga c’è un *, al suo posto ho inserito l’IP di meta per non permettere la cmunicazione con gli altri client .



VNC server ‘password’ Password

Per risolvere questa vulnerabilità, sempre dalla shell di meta e sempre con root, usando il comando “vncpasswd” si ha la possibilita di cambiare la password della VNC per inserirne una più complessa.

```
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin#
```

Bind Shell Backdoor Detection

Per risolvere questa minaccia aprendo la shell root di meta, usando il comando "iptables" (questo comando ci fa vedere i firewall dei sistemi linux).

Con il comando "iptables –I INPUT –p tcp –dport 1524 –j DROP" sono andato a bloccare il traffico sulla porta 1524.

Infine con il comando "iptables -L" ho controllato se la regola è stata aggiunta.

```
root@metasploitable:/home/msfadmin# iptables -I INPUT -p tcp --dport 1524 -j DRO
P
root@metasploitable:/home/msfadmin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere            tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@metasploitable:/home/msfadmin#
```