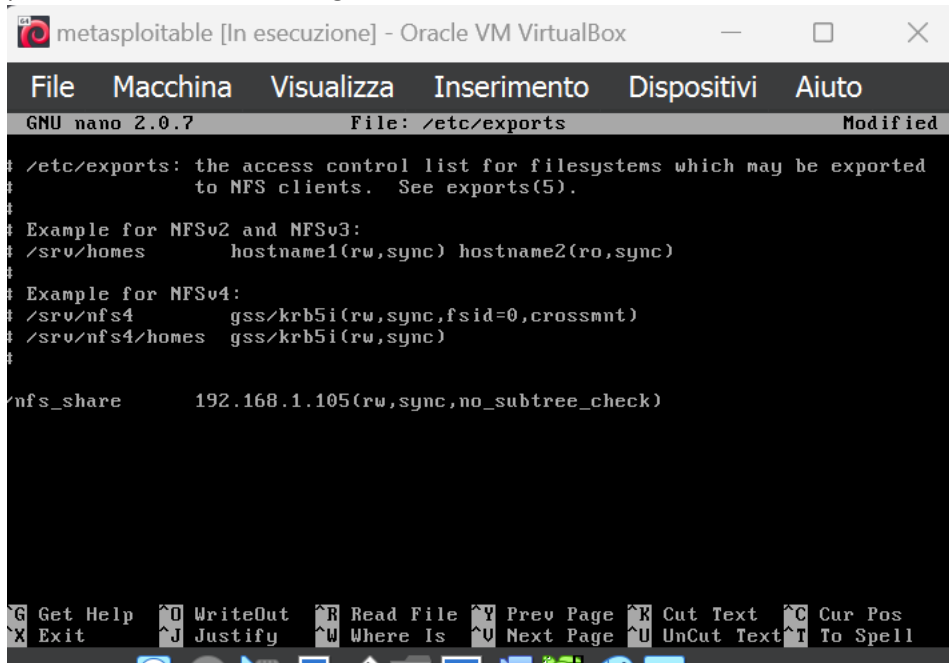


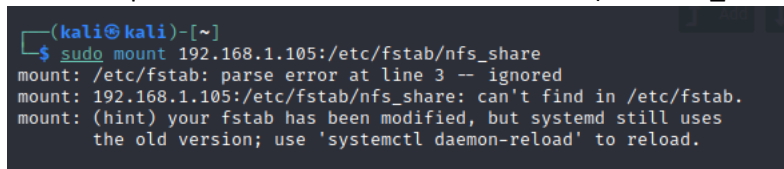
La vulnerabilità di accesso alle condivisioni NSF dall'host remoto è stata risolta configurando NFS in modo da permettere l'accesso solo agli autorizzati, nel nostro caso abbiamo consentito l'accesso e la scrittura solo all'host



```
metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/exports Modified
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw, sync) hostname2(ro, sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw, sync, fsid=0, crossmnt)
# /srv/nfs4/homes gss/krb5i(rw, sync)
#
nfs_share 192.168.1.105(rw, sync, no_subtree_check)
G Get Help ^O WriteOut ^R Read File ^V Prev Page ^K Cut Text ^C Cur Pos
X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell
```

192.168.1.105 (kali).

Abbiamo quindi creato la cartella di condivisione (mkdir nfs_share) sul server ed in seguito è stata montata



```
(kali@kali)-[~]
$ sudo mount 192.168.1.105:/etc/fstab/nfs_share
mount: /etc/fstab: parse error at line 3 -- ignored
mount: 192.168.1.105:/etc/fstab/nfs_share: can't find in /etc/fstab.
mount: (hint) your fstab has been modified, but systemd still uses
the old version; use 'systemctl daemon-reload' to reload.
```

sul client.

La vulnerabilità della Blackdoor sulla Bind Shell è stata risolta mettendo una regola del firewall che blocchi la porta 1524 che causa la vulnerabilità. Per farlo abbiamo usato ufw, lo abilitiamo tramite comando “sudo ufw enable” e poi inseriamo la regola “sudo ufw deny 1524/tcp”. Infine controlliamo se la regola è stata inserita tramite comando “nc 192.168.1.103 1524” che dovrebbe aprire una connessione ma adesso viene bloccata

```
(kali@kali)~$ nc 192.168.1.103 1524
(UNKNOWN) [192.168.1.103] 1524 (ingreslock) : Connection timed out
```

```
(kali@kali)~$ nmap 192.168.1.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-27 04:20 EDT
Nmap scan report for 192.168.1.103
Host is up (0.0039s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds
```

La vulnerabilità del server VNC con password “password” è stato risolto cambiando la password di accesso con una più sicura tramite il comando “sudo su” per avere i diritti di amministratore e successivamente “vncpasswd” che ci chiederà poi di reimpostare la password e confermarla. Nel nostro caso abbiamo inserito come password msfadmin che è anch’essa semplice ma ci permette di aggirare temporaneamente la vulnerabilità di meta.

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