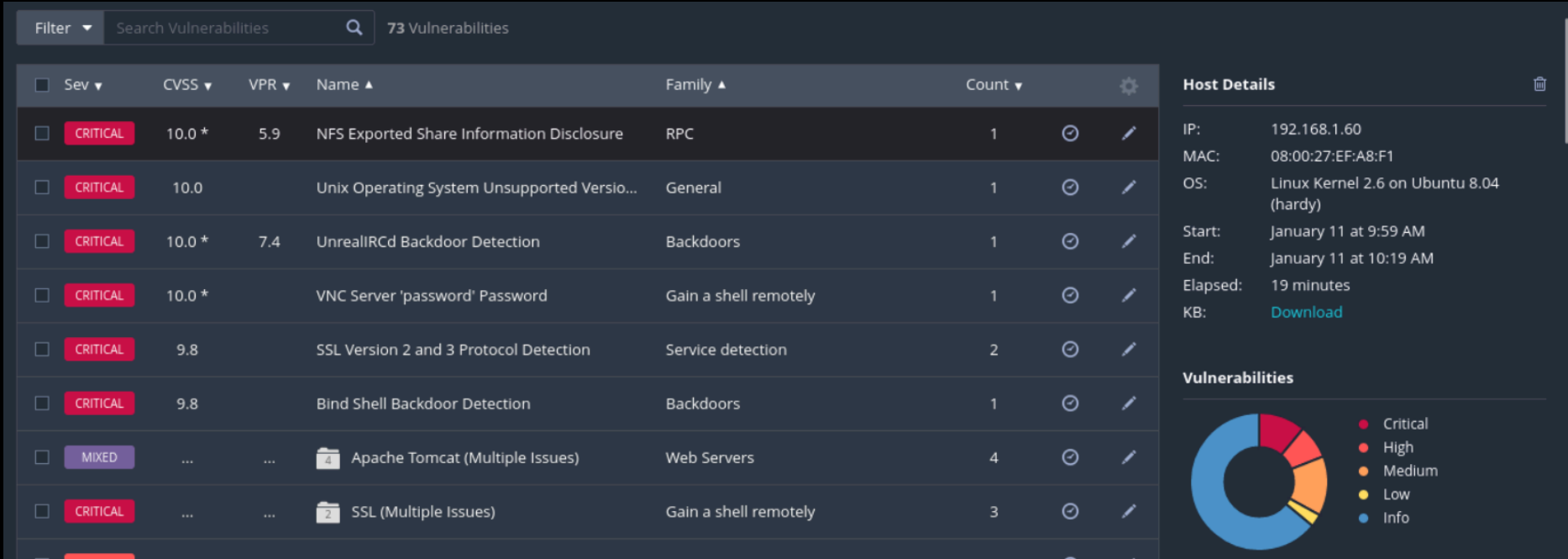


# Metasploitable vulnerability

Richiesta: Scanning vulnerabilità Metasploitable e implemento di azioni di rimedio.

Tool utilizzati: Nessus.

## Scanning:



Notiamo un’elevata criticità delle vulnerabilità rilevate.

Obiettivo: Ridurre il livello di criticità di almeno 2 vulnerabilità critiche.

Vulnerabilità 1:  
VNC Server “password” Password

## Risoluzione:

```
metasploitable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
curl: (35) error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure
root@metasploitable:/usr/bin# cd
Display all 1038 possibilities? (y or n)
root@metasploitable:/usr/bin# cd
Display all 1038 possibilities? (y or n)
root@metasploitable:/usr/bin# cd /etc/vncserver
bash: cd: /etc/vncserver: No such file or directory
root@metasploitable:/usr/bin# cd /etc/
root@metasploitable:/etc# cd /.vnc
bash: cd: /.vnc: No such file or directory
root@metasploitable:/etc# cd ~/.vnc
root@metasploitable:~/.vnc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

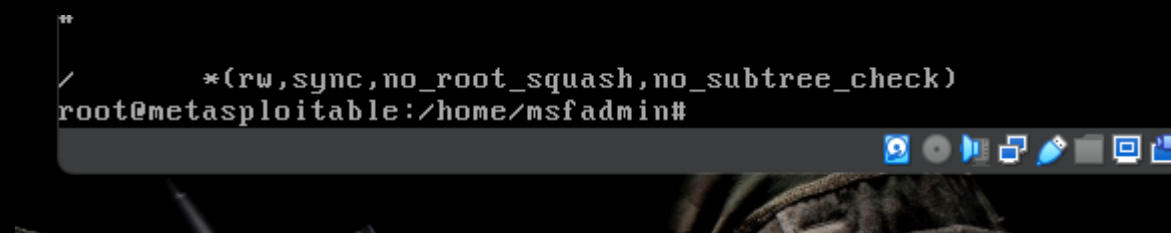
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:~/.vnc#
```

Cambio della password “password” con una password più sicura “GHIje25%”.

## Vulnerabilità 2:

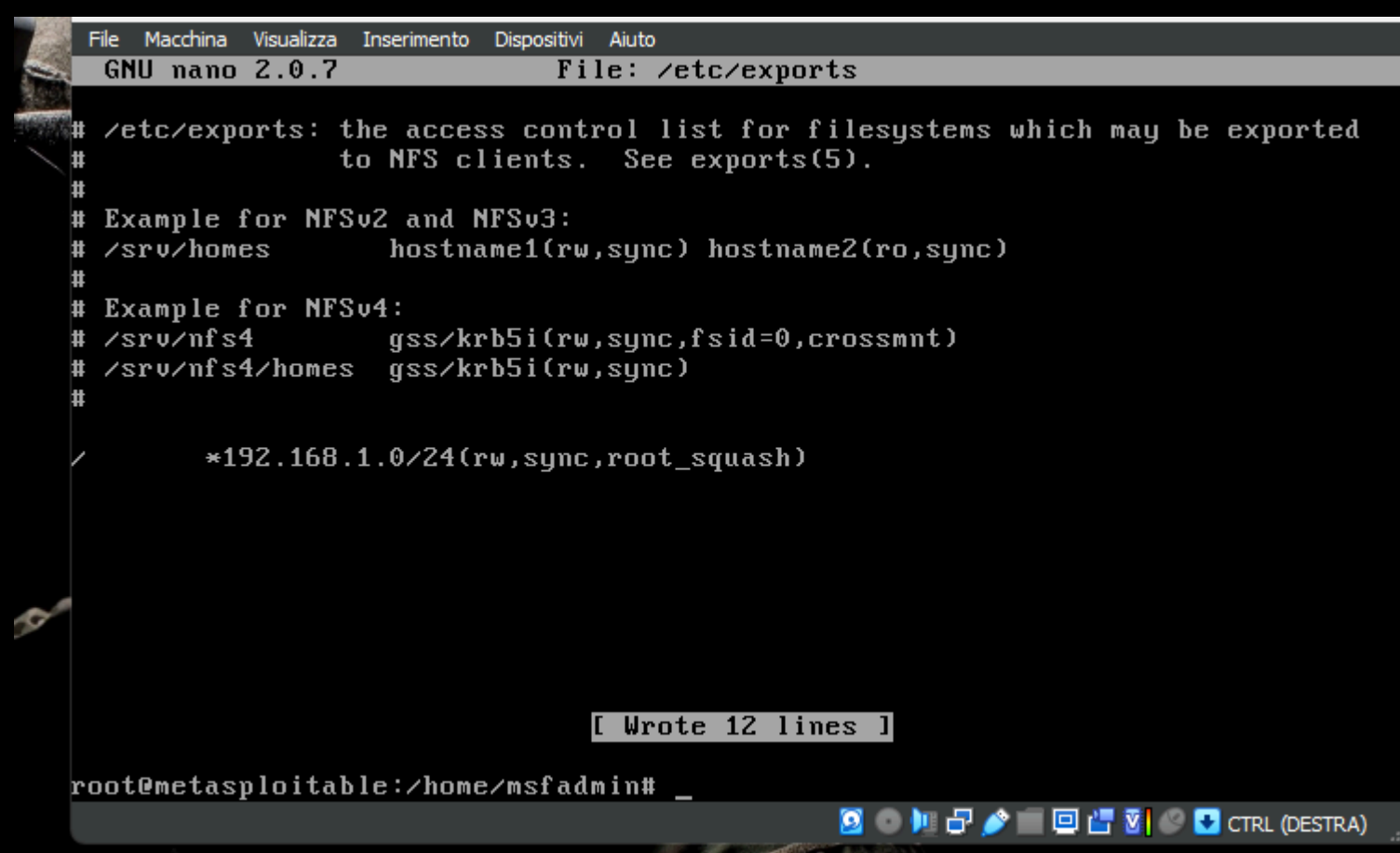
### NFS Exported Share Information Disclosure

#### Problema:



Riguarda le configurazioni non sicure del Network File System (NFS) che possono permettere la divulgazione non autorizzata di informazioni. NFS è utilizzato per condividere file tra sistemi in una rete. Se non configurato correttamente, può esporre file sensibili o permettere a un attaccante di montare il filesystem in modo non autorizzato.

#### Soluzione:



#### Spiegazione:

- 192.168.1.0/24: Questo indica che solo i dispositivi nella subnet 192.168.1.0 con una maschera di sottorete di 255.255.255.0 (che è cosa significa /24) possono montare questa condivisione NFS.
- rw: Permette sia lettura che scrittura sulla condivisione NFS.
- sync: Richiede che le modifiche al filesystem siano confermate sul disco prima che le operazioni di scrittura siano considerate complete.

- `root_squash`: Mappa le richieste da UID/GID 0 (root) a un UID/GID anonimo, di solito rendendo root equivalente all'utente "nobody", per una maggiore sicurezza.