# Remediation Meta

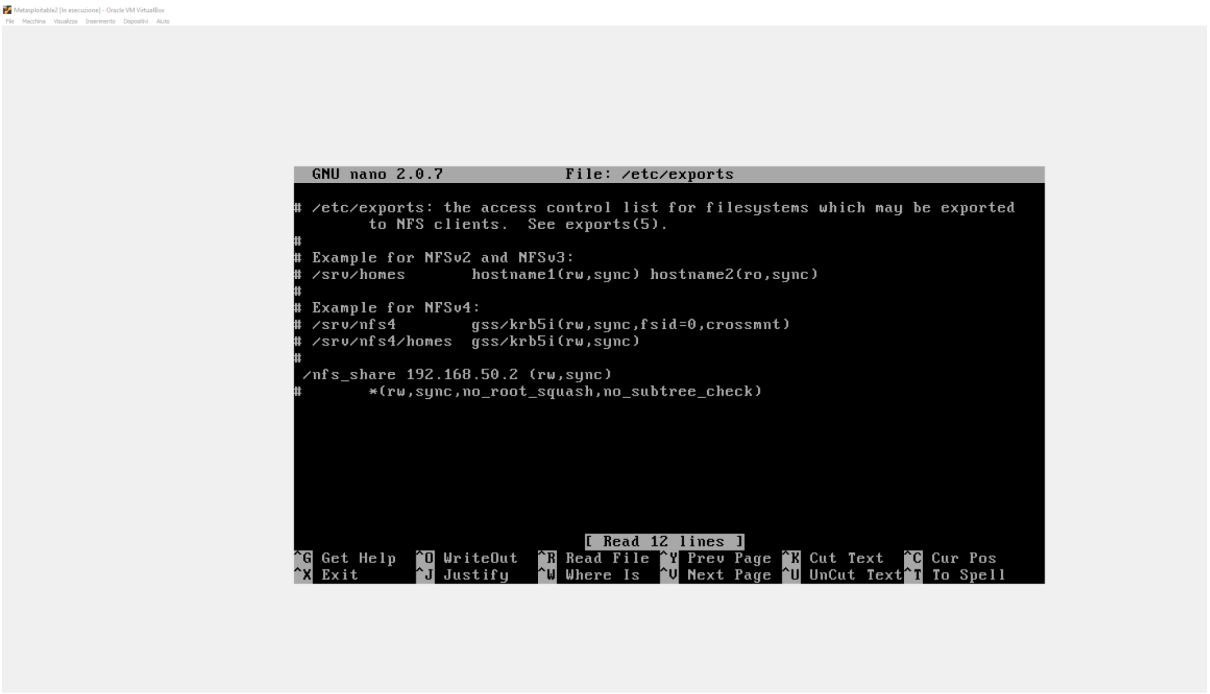
Dopo aver effettato una scansione con Nessus sulll'indirizzo IP 192.168.50.100 sono state rilevate molte vulnerabilità.
Ho iniziato a risolvere quelle di impatto CRITICO indicate nella traccia.

## 1. NFS Exported Share Information Disclosure

Come possiamo leggere dalla pagina di Nessus la seguente vulnerabilità permette a un host remoto di accedere a :

- Elenco delle directory o dei file condivisi tramite NFS.
- Parametri di configurazione delle condivisioni, inclusi i permessi di accesso.
- Alcune informazioni sul sistema host.

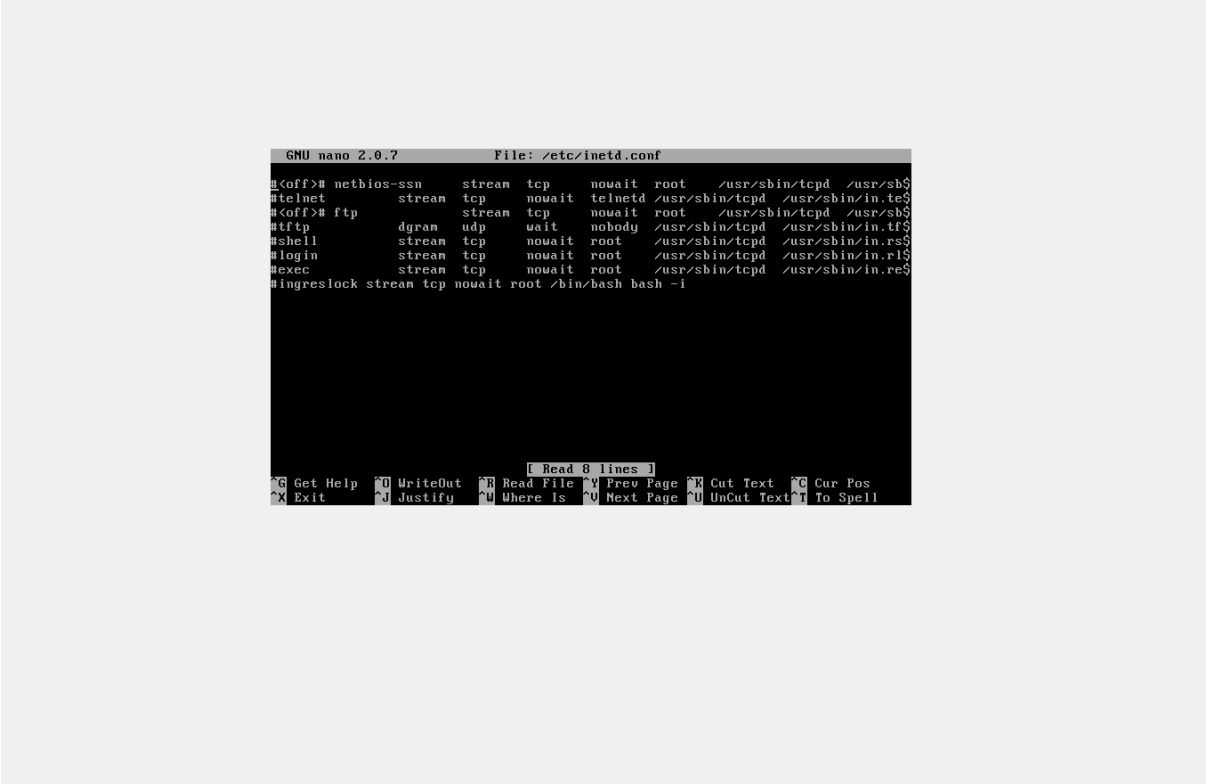
Come indicato sempre da Nessus per risolvere la vulnerabilità ho commentato quindi l'ultima riga che risultava essere la riga che causava la vulnerabilità nel file exports presente nella directory /etc.
In più ho dato i permessi alla mia macchina di Kali per leggere e sincronizzare file, directory e informazioni



# 2. Rexecd Service Detection

Nessus ci indica che questa vulnerabilità permette agli utenti della rete di eseguire comandi da remoto, i per se questa non è una vulnerabilità, il problema è che rexecd non fornisce nessun serivizio di autenticazione, quindi può essere usato per attaccare il sistema.

Per risolvere questa vulnerabilità Nessus ci indica quale riga modificare all'interno del file inetd.conf  presente nella cartella /etc.
Possiamo notare che la vulnerabilità viene risolta commentando la penultima riga del file.
( #exec stream tcp nowait root /usr/sbin/tcpd…)




NB : possiamo notare che tutte le righe nel file sono commentate, questo perchè in questo file sono presenti altre righe che corrispondono a vulnerabilità.
Per esempio questo  file conteneva anche la vulnerabilità : **rlogin Service Detection** risolta commentando la linea che inizia con **login**.
Le altre righe sono state commentate in maniera preventiva.

# 3. VNC Server Password

Per risolvere questa Vulnerabilità molto semplicemente basta impostare una password sicura al Servizio VNC, visto che la password di base era "password".

```
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Passwords do not match. Please try again.

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

# 4. Bind Shell Backdoor Detection

Nessus ci indica che c'è una backdoor exploitabile sulla porta 1524 con il protocollo TCP, in questo caso creerò una regola su iptables chiudendo in ingresso la porta, impedendo così di connettersi sulla porta 1524.

Regola -> sudo iptables -A INPUT -p tcp --dport 1524 -j DROP

```
root@metasploitable:~# 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
```