Come esempio vengono proposte le soluzioni per le seguenti vulnerabilitá:
- NFS Exported Share Information Disclosure
- Bind Shell Backdoor Detection
- VNC Server 'password' Password

1. NFS Exported Share Information Disclosure

Il server NFS è configurato nel file /etc/exports, che presenta la seguente riga che causa il problema di sicurezza:

/ *(rw,sync,no_root_squash,no_subtree_check)

Ovvero qualunque client può montare la directory root. La remediation consiste di due passaggi:

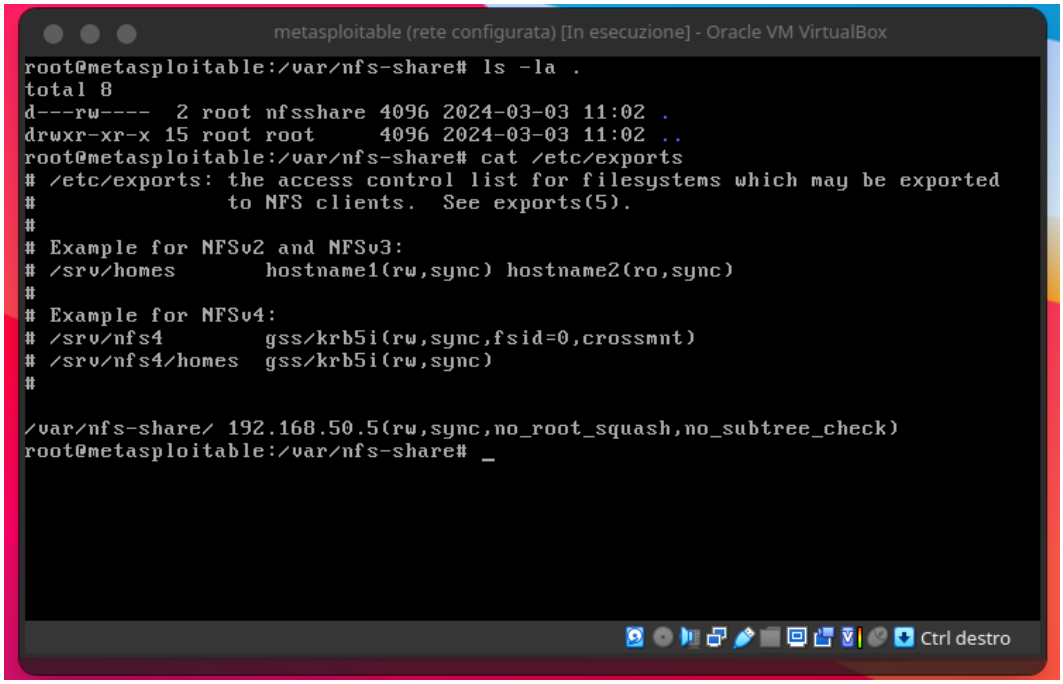
1) creare una cartella specifica per la condivisione, associandovi un nuovo gruppo “nfsshare” con permessi di lettura/scrittura

sudo mkdir /var/nfs-share
sudo groupadd nfsshare
sudo chgrp nfsshare /var/nfs-share
cd /var/nfs-share
sudo chmod a-rwx .
sudo chmod g+rw .

2) limitare gli IP da cui viene accettata la connessione. Supponendo che un solo computer nella rete avente IP 192.168.50.5 abbia bisogno di montare la cartella NFS, viene cambiato il file /etc/exports nel seguente modo:

/var/nfs-share 192.168.50.5 (rw,sync,no_root_squash,no_subtree_check)

Da evidenziare che essendo NFS un protocollo vecchio non cripta il traffico.
In casi più complessi, in cui per esempio sia necessario garantire l’accesso al server NFS anche da Internet, si potrebbe configurare un server VPN come WireGuard, e accettare connessioni solo dall’IP del server dove viene installato quest’ultimo. Ciò avrebbe anche il vantaggio di criptare il traffico (quanto meno verso l’esterno della rete locale).



2 . Bind Shell Backdoor Detection

Questa vulnerabilitá indica che il server é stato compromesso in quanto è presente un programma che rimane in ascolto sulla porta 1524 e accetta connessioni dall'esterno, permettendo di eseguire qualunque comando.

Non è possibile sapere cosa è stato compromesso, quindi l'unica soluzione è creare un'immagine del disco per analisi successiva e procedere con una completa formattazione e reinstallazione del sistema operativo e di tutti i servizi necessari.

Per lo scopo didattico del corso, viene identificato quale processo ascolta sulla porta 1524 con il comando lsof:

lsof -i :1524

Risulta essere il comando xinetd, che da una ricerca su internet risulta configurato tramite il file /etc/inetd.conf, il quale presenta nell'ultima riga la sorgente del problema

Quindi viene cancellata la riga incriminata.

3. VNC Server 'password' Password

Questa vulnerabilità indica che il server VNC presenta una password debole. La soluzione consiste banalmente nel cambiare la password con una robusta (lunga e con caratteri alfanumerici + simboli; o in alternativa una passphrase).

Per cambiare la password del server VNC, basta dare il comando “vncpasswd”.

Si nota peró, tramite il comando “ps aux | grep vnc”, che il server Xtightvnc viene lanciato tramite utente root. Per migliorare la sicurezza, si propone di configurare il server per un utente regolare e non root.