Gabriele Di giampietro **Data 25/11/2022**

Obbiettivo: Effettuare una VA sulla macchina virtuale Metasploitable, analizzare e attuare delle remediation action su un minimo di 2 ad un massimo di 4 vulnerabilità trovate di livello Critical.

Rimediation Action

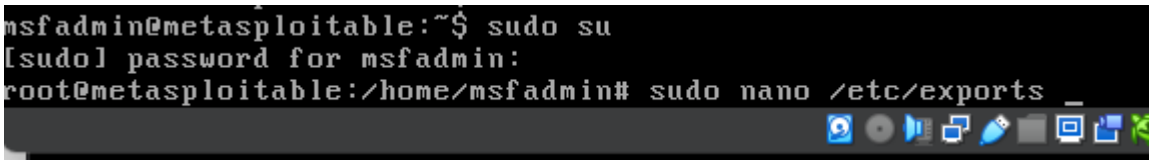
Prima Vulnerabilità:

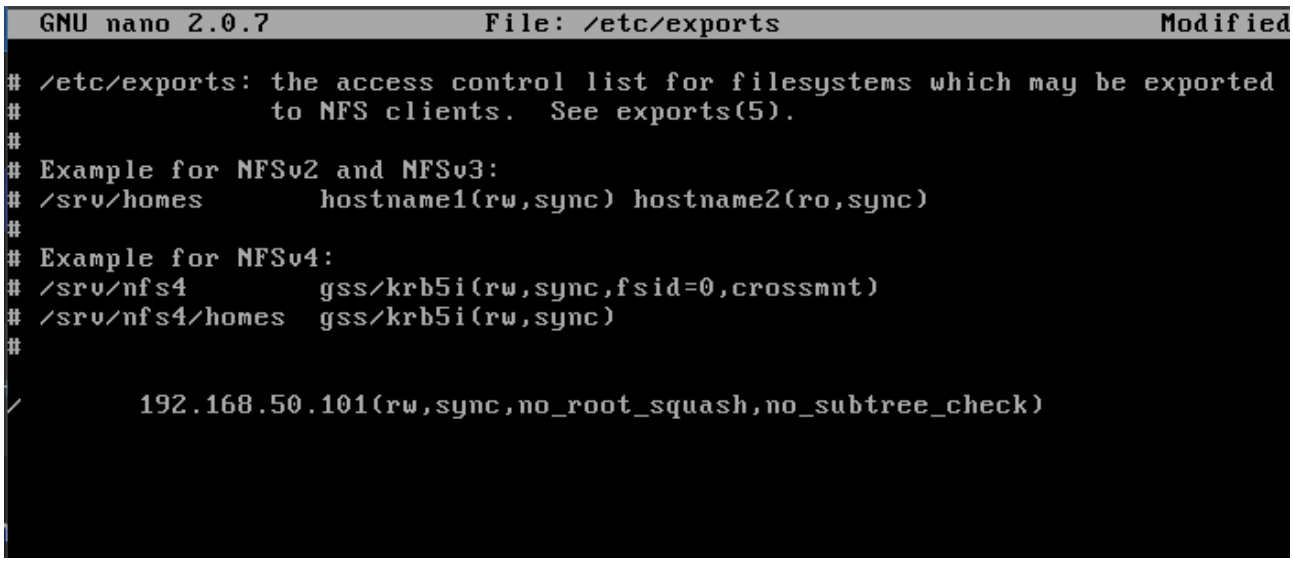
11356 - NFS Exported Share Information Disclosure

Nella prima vulnerabilità che abbiamo riscontrato dalla VA, abbiamo constatato dalla descrizione che almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (e possibilmente scrivere) file su host remoto.

Come ci indica la soluzione del report andiamo a configurare il nostro NFS server su Metsploitable per correggere la problematica. Entriamo prima sul root e poi andiamo a modificare il file /etc/exports che riguarda gli access da parte client sul NFS, quindi modifichiamo l'ultima stringa al posto del simbolo * inseriamo l'indirzzio ip della nostra macchina Metasploitable, così che da non permettere modifiche arbitrarie alle informazioni del nostro NFS da altri client da remoto.

Possiamo vedere le modifiche apportate nell'immagine seguente:





Seconda Vulnerabilità:

61708 - VNC Server 'password' Password

Nella seconda vulnerabilità che andiamo ad analizzare riscontriamo come da descrizione il problema sulla password troppo debole sul server VNC. Andiamo quindi a modificare la nostra password per renderla più difficile, attraverso sempre il root andiamo ad inserire una password più complessa ad 8 caratteri (Password: c43abt17).

Possiamo vedere le modifiche apportate e il relativo comando utilizzato nell'immagine seguente.

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

Terza Vulnerabilità:

51988 – Bind Shell Backdoor Detection

Nella terza vulnerabilità riscontriamo invece che una shell è in ascolto sulla porta remota (una Backdoor) senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando comandi direttamente. In questo caso andiamo ad utilizzare il Firewall, Iptables, modifichiamo le policy così da non permettere connessioni TCP sulla porta in questione (1524). Tenendo a mente che ogni volta che riavviamo la macchina dobbiamo reimpostare le policy, in quanto vengono resettate.

Possiamo vedere la configurazione delle policy nell'immagine seguente.

```
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p TCP --dport 1524 -j DROP
msfadmin@metasploitable:~$ sudo 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
msfadmin@metasploitable:~$ _
```