RemediationMeta

NFS Exported Share Information Disclosure

1. Apro (edito) il file /etc/exports

```
msfadmin@metasploitable:~$ sudo nano /etc/exports
```

2. Modifico la riga `/ *(rw,sync,no_root_squash,no_subtree_check)` e la faccio diventare `/ 192.168.56.102(rw,sync,no_subtree_check,root_squash)` dove prendo l'ip su cui sto per abilitare solo quello.
3. Applico i cambiamenti e faccio ripartire il servizio NFS

```
msfadmin@metasploitable:~$ sudo exportfs -ra
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server restart
 * Stopping NFS kernel daemon                                    [ OK ]
 * Unexporting directories for NFS kernel daemon...              [ OK ]
 * Exporting directories for NFS kernel daemon...                [ OK ]
 * Starting NFS kernel daemon                                    [ OK ]
msfadmin@metasploitable:~$ _
```

4. Per migliorare la sicurezza, disabilito anche le vecchie versioni di NFS con "sudo nano /etc/default/nfs-kernel-server" modificando poi la seguente voce "RPCNFSDOPTS="-N 2 -N 3""

IL Problema è adesso risolto, facendo si che l'accesso sia restricted a chi appartiene alla rete della metasploitable (192.168.56.X)

rexecd Service Detection

Questa vulnerabilità non mi è stata rilevata da nessus in fase di scansione, ma effettuo i passaggi per "far finta" di risolverlo

1. Fermo il servizio rexecd come prima cosa

```
msfadmin@metasploitable:~$ sudo /etc/init.d/rexec stop
```

2. Lo disabilito all'avvio (così se per riavviassi la vulnerabilità rimarrebbe "sistemata")

```
msfadmin@metasploitable:~$ sudo update/rc.d rexec disable
```

VNC Server 'password' Password

1. Se attivo (cerco con "netstat -antp | grep LISTEN" se esiste) lo uccido (vncserver -kill :1)
2. Imposto una nuova password (che non sia "password" ovviamente)

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password: _
```

3. Faccio ripartire il servizio VNC vncserver :1

Bind Shell Backdoor Detection

1. Mi viene indicato che la porta è la 1524, quindi prima cosa identifico il pid con:" netstat -tulnp | grep 1524"
2. Vedo che "xinetd" è su quella porta, cerco altri dettagli con

```
msfadmin@metasploitable:~$ sudo lsof -i :1524_
```

3. E ne identifico l'eseguibile con il PID 4603 che trovo

```
msfadmin@metasploitable:~$ ls -l /proc/4603/exe_
```

4. Infine lo rimuovo con

```
msfadmin@metasploitable:~$ sudo rm /usr/sbin/xinetd
```

REGOLE FW PER "SISTEMARE" (NON ALLA RADICE COMUNQUE) ALTRE VULNERABILITÀ

SSL Version 2 and 3 Protocol Detection

1. Limito l'accesso ssl alla 443
2.

```
root@metasploitable:~# sudo iptables -A INPUT -p tcp --dport 443 -j DROP
```

Apache Tomcat AJP Connector Request Injection (Ghostcat)

1. Il Servizio è in ascolto su porta 8009 quindi blocco il traffico in entrata su quella porta
2.

```
root@metasploitable:~# sudo iptables -A INPUT -p tcp --dport 8009 -j DROP
```

TLS Version 1.0 Protocol Detection

1. Alcune porte usano questo, ormai datato, protocollo (5432, 25). Ne limito quindi l'accesso
2.

```
root@metasploitable:~# sudo iptables -A INPUT -p tcp --dport 5432 -j DROP
root@metasploitable:~# sudo iptables -A INPUT -p tcp --dport 25 -j DROP
```

Dopo che scrivo le regole, devo applicarle, usando:

```
root@metasploitable:~# sudo iptables-save
# Generated by iptables-save v1.3.8 on Sun Jul 28 10:36:50 2024
*filter
:INPUT ACCEPT [32332:3133981]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [26996:4433491]
-A INPUT -p tcp -m tcp --dport 443 -j DROP
-A INPUT -p tcp -m tcp --dport 8009 -j DROP
-A INPUT -p tcp -m tcp --dport 5432 -j DROP
-A INPUT -p tcp -m tcp --dport 25 -j DROP
COMMIT
# Completed on Sun Jul 28 10:36:50 2024
```