

REMEDICATION META

Prima di iniziare la remediation meta, ho effettuato da kali una scansione con lo strumento “nmap” verso metasploitable. Ho usato il comando `nmap -O 192.168.50.100`

```
└─$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 17:45 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00031s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:1B:77:32 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

NFS Export Share Information Disclosure

Per risolvere il problema di questa vulnerabilità, ho aperto la shell di meta, con il comando “sudo su” sono entrato nel root di meta. Per cambiare la configurazione NFS, con il comando “nano /etc/exsprot”, sono entrato nel file e nell’ultima riga c’è un *, al suo posto ho inserito l’IP di meta per non permettere la cmunicazione con gli altri client .

```
GNU nano 2.0.7          File: /etc/exports          Modified
# /etc/exports: the access control list for filesystems which may be exported
#                  to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes        hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4         gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes   gss/krb5i(rw,sync)
#
/      192.168.50.101(rw,sync,no_root_squash,no_subtree_check)

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

VNC server 'password' Password

Per risolvere questa vulnerabilità, sempre dalla shell di meta e sempre con root, usando il comando “vncpasswd” si ha la possibilità di cambiare la password della VNC per inserirne una più complessa.

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

Bind Shell Backdoor Detection

Per risolvere questa minaccia aprendo la shell root di meta, usando il comando “iptables” (questo comando ci fa vedere i firewall dei sistemi linux).

Con il comando “iptables -I INPUT -p tcp --dport 1524 -j DROP” sono andato a bloccare il traffico sulla porta 1524.

Infine con il comando “iptables -L” ho controllato se la regola è stata aggiunta.

```
root@metasploitable:/home/msfadmin# iptables -I INPUT -p tcp --dport 1524 -j DROP
root@metasploitable:/home/msfadmin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination          tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@metasploitable:/home/msfadmin#
```