

Remediation

1- 61708 VNC Server 'password' Password

Seguendo la soluzione suggerita da Nessus sono andato a modificare la password del servizio VNC.
Per farlo sono andato a lanciare il comando [vncpasswd](#).

```
msfadmin@metasploitable:~$ sudo su
[sudol] password for msfadmin:
Sorry, try again.
[sudol] password for msfadmin:
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)? y
Password:
Verify:
root@metasploitable:/home/msfadmin#
```

2- 10203 rexecd Service Detection

Il report Nessus ci indica di andare a rendere Commento una linea presente in inetd.conf, nello specifico la linea "exec".

```
[ Wrote 8 lines ]
msfadmin@metasploitable:/etc$ sudo nano inetd.conf_
#<off># netbios-ssn      stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.td
telnet                  stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.tel
#<off># ftp              stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ft
tftp                   dgram  udp    wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.r
shell                  stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs
login                  stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl
#exec                  stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re
ingreslock stream tcp nowait root /bin/bash bash -i
```

3- 11356 NFS Exported Share Information Disclosure

In questo caso Nessus ci consigliava di configurare l'NFS in modo da consentire l'accesso solo agli autorizzati. Inizialmente ho provato a modificare dei permessi in /etc/hosts.deny e /etc/hosts.allow. Ma continuava a rilevarmi la vulnerabilità, quindi ricercando sono riuscito a risolverla andando a modificare /etc/exports inserendo nell'ultima riga l'indirizzo di meta in modo da concedere solo a se stesso l'accesso.

```
/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)

192.168.1.102(rw,sync,no_root_squash,no_subtree_check)
```

4- 51988 Bind Shell Backdoor Detection

Qui Nessus diceva di verificare se l'host fosse compromesso e se necessario reinstallare il sistema. In questo caso ho preferito creare una regola nel firewall di meta iptables andando a chiudere la porta per Kali (192.168.1.100) tramite il comando **iptables -I INPUT -p tcp -s 192.168.1.100 --dport 1524 -j DROP**. Avrei potuto chiudere la porta a tutti togliendo "-s 192.168.1.100".

```
4 -j DROP
iptables v1.3.8: can't initialize iptables table 'filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# msfadmin
bash: msfadmin: command not found
root@metasploitable:/home/msfadmin# iptables -I INPUT -p tcp -s 192.168.1.100 --dport 1524 -j DROP
root@metasploitable:/home/msfadmin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination          tcp dpt:ingreslock
DROP      tcp  --  192.168.1.100          anywhere             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# _
```