

REMEDIATIONS

Sono state risolte le 3 vulnerabilità qua sotto elencate:


- 51988 - Bind Shell Backdoor Detection
- 11356 - NFS Exported Share Information Disclosure
- 61708 - VNC Server 'password' Password

51988 - Bind Shell Backdoor Detection

Creo un file chiamato “close_port.sh” al cui interno scrivo il seguente comando:

“ iptables -A INPUT -p tcp --dport 1524 -j DROP “

Questo comando permette la chiusura della porta quindi non permette più accesso malevolo.



```
GNU nano 2.0.7 File: close_port.sh Modified
iptables -A INPUT -p tcp --dport 1524 -j DROP
File Name to Write: close_port.sh_
^G Get Help      ^T To Files      M-M Mac Format   M-P Prepend
^C Cancel        M-D DOS Format   M-A Append      M-B Backup File
```

A questo punto copiamo il file dentro alla cartella “init.d” in modo da rendere eseguibile il nostro comando ad ogni avvio del sistema.

```
root@metasploitable:/home/msfadmin# cp close_port.sh /etc/init.d/
root@metasploitable:/home/msfadmin# chmod +x /etc/init.d/close_port.sh
```

11356 - NFS Exported Share Information Disclosure

Per risolvere questa vulnerabilità è bastato entrare nel file `/etc/exports` e inserire questa riga:
“ `/nfs_share 192.168.32.120(rw,sync)` “

Ci permette di rendere leggibile le shares NFS solo dall'ip specificato (nel nostro caso solo metasploitable)



```
GNU nano 2.0.7 File: /etc/exports
# /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)
#
#/*(rw,sync,no_root_squash,no_subtree_check)
/nfs_share 192.168.32.120(rw,sync)

[ Wrote 13 lines ]
```

61708 - VNC Server 'password' Password

Per risolvere questa vulnerabilità è stato sufficiente modificarla tramite il seguente comando:
“ **vncpasswd** “

```
Metasploitable 2 - 192.168.32.120
TX packets:33956 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:5951289 (5.6 MB) TX bytes:0 (0.0 B)

lo    Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       UP LOOPBACK RUNNING  MTU:16436  Metric:1
       RX packets:424 errors:0 dropped:0 overruns:0 frame:0
       TX packets:424 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:175501 (171.3 KB) TX bytes:175501 (171.3 KB)

msfadmin@metasploitable:~$ sudo su
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#
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin#
```