

## REMEDIATION OF VULNERABILITIES

### Elenco vulnerabilità risolte

Sev ▼	Score ▼	Name ▲
CRITICAL	10.0 *	NFS Exported Share Information Disclosure
CRITICAL	10.0 *	rexecd Service Detection
CRITICAL	10.0 *	VNC Server 'password' Password
CRITICAL	9.8	Bind Shell Backdoor Detection

### Elenco passaggi effettuati per risolvere le vulnerabilità

#### 1) NFS Exported Share Information Disclosure

Nell'immagine sottostante possiamo vedere, all'ultima riga del file, la configurazione errata del file system NFS nel quale viene data la possibilità a qualsiasi indirizzo IP (rappresentato dall'asterisco) di accedere ai dati dalla cartella root (indicata dalla barra).

```
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)
```

Al fine di risolvere tale vulnerabilità è stato deciso di restringere l'accesso alla sola directory *media*, quindi non più quella *root*, ai soli host presenti sulla stessa rete della macchina scansionata ipotizzando il caso nel quale tale macchina operi come scambio di media tra i vari client della rete. È stata anche eliminata l'opzione *no\_root\_squash* in quanto è un'opzione estremamente pericolosa che consente agli utenti root remoti lo stesso privilegio dell'utente root della macchina host.

```
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)
#
/media 192.168.2.0/24(rw,sync,no_subtree_check)
```

Con il comando `sudo exportfs -arv` sono state applicate le modifiche apportate al file di configurazione.

```
msfadmin@metasploitable:~$ sudo exportfs -arv
exporting 192.168.2.0/24:/media
```

Infine, come si può notare dall'immagine seguente, le modifiche apportate impediscono il `mount` della cartella `media` in quanto la macchina kali si trova su un'altra rete rispetto alla macchina Metasploitable.

```
(kali@kali)-[~]
$ sudo mount -t nfs 192.168.2.100:/ /media
[sudo] password for kali:
Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service → /lib/systemd/system/rpc-statd.service.
mount.nfs: access denied by server while mounting 192.168.2.100:/
```

## 2) rexecd Service Detection

Questa vulnerabilità è stata risolta disabilitando dai file di configurazione del demone `inetd`, il servizio `exec` ovvero il servizio che è causa la vulnerabilità.

GNU nano 2.0.7	File: inetd.conf	Modified
#<off># netbios-ssn	stream tcp nowait root /usr/sbin/tcpd /usr/sbin	
telnet	stream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd	
#<off># ftp	stream tcp nowait root /usr/sbin/tcpd /usr/sbin	
tftp	dgram udp wait nobody /usr/sbin/tcpd /usr/sbin/in.tftpd	
shell	stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rsh	
login	stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rlogin	
#<off>#exec	stream tcp nowait root /usr/sbin/tcpd /usr/sbin	
#<off>#ingreslock	stream tcp nowait root /bin/bash bash -i	

Come controprova è stata verificata la presenza del servizio `exec` sulla porta 512 in quanto quest'ultima è quella utilizzata da tale servizio.

```
msfadmin@metasploitable:~$ sudo lsof -i :512
msfadmin@metasploitable:~$ _
```

## 3) VNC Server 'password' Password

La terza vulnerabilità è stata risolta cambiando la password di accesso precedente ovvero "password" con una più complessa tramite il comando `vncpasswd` da utente root.

```
root@metasploitable:/home/msfadmin# 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# _
```

#### 4) Bind Shell Backdoor Detection

L'ultima vulnerabilità risolta permetteva l'utilizzo della shell della macchina target tramite una macchina remota come si può evincere dall'immagine successiva.

```
(kali@kali)~[~]
$ nc -nv 192.168.2.100 1524
(UNKNOWN) [192.168.2.100] 1524 (ingreslock) open
root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
root@metasploitable:/#
```

Per correggere tale vulnerabilità è stato necessario disabilitare il servizio *ingreslock* operante sulla porta 1524 tramite la quale avviene la connessione tra macchine.

```
msfadmin@metasploitable:~$ netstat -n | grep 1524
tcp        0      0 192.168.2.100:1524    192.168.1.100:40756  ESTABLISHED
tcp        0      0 192.168.2.100:1524    192.168.1.100:45822  CLOSE_WAIT
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ sudo lsof -i :1524
COMMAND  PID USER  FD  TYPE DEVICE SIZE NODE NAME
xinetd   4453 root  12u  IPv4  12080      TCP *:ingreslock (LISTEN)
bash     4766 root   0u  IPv4  12648      TCP 192.168.2.100:ingreslock->192.168
.1.100:45822 (CLOSE_WAIT)
bash     4766 root   1u  IPv4  12648      TCP 192.168.2.100:ingreslock->192.168
.1.100:45822 (CLOSE_WAIT)
bash     4766 root   2u  IPv4  12648      TCP 192.168.2.100:ingreslock->192.168
.1.100:45822 (CLOSE_WAIT)
bash     4766 root  255u  IPv4  12648      TCP 192.168.2.100:ingreslock->192.168
.1.100:45822 (CLOSE_WAIT)
nano     4779 root   0u  IPv4  12648      TCP 192.168.2.100:ingreslock->192.168
.1.100:45822 (CLOSE_WAIT)
nano     4779 root   1u  IPv4  12648      TCP 192.168.2.100:ingreslock->192.168
.1.100:45822 (CLOSE_WAIT)
nano     4779 root   2u  IPv4  12648      TCP 192.168.2.100:ingreslock->192.168
.1.100:45822 (CLOSE_WAIT)
msfadmin@metasploitable:~$ _
```

```
COMMAND  PID USER  FD  TYPE DEVICE SIZE NODE NAME
xinetd   4453 root  12u  IPv4  12080      TCP *:ingreslock (LISTEN)
bash     4766 root   0u  IPv4  12648      TCP 192.168.2.100:ingreslock->192.16$
bash     4766 root   1u  IPv4  12648      TCP 192.168.2.100:ingreslock->192.16$
bash     4766 root   2u  IPv4  12648      TCP 192.168.2.100:ingreslock->192.16$
bash     4766 root  255u  IPv4  12648      TCP 192.168.2.100:ingreslock->192.16$
nano     4779 root   0u  IPv4  12648      TCP 192.168.2.100:ingreslock->192.16$
nano     4779 root   1u  IPv4  12648      TCP 192.168.2.100:ingreslock->192.16$
nano     4779 root   2u  IPv4  12648      TCP 192.168.2.100:ingreslock->192.16$
```

Per disabilitare il servizio *ingreslock* sono stati modificati i file di configurazione dei demoni *inetd* e *xinetd*.

```
GNU nano 2.0.7      File: inetd.conf      Modified
#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet               stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp            stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp                 dgram  udp    wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
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$
#<off>#ingreslock stream tcp nowait root /bin/bash bash -i
```

```
msfadmin@metasploitable:/etc$ cat xinetd.conf
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/

defaults
{
    # Please note that you need a log_type line to be able to use log_on_success
    # and log_on_failure. The default is the following :
    # log_type = SYSLOG daemon info
}

includedir /etc/xinetd.d
msfadmin@metasploitable:/etc$ _
```

```
GNU nano 2.0.7      File: ingreslock
service ingreslock
{
    disable = yes
}
```

Come controprova è stata verificata la presenza del servizio sulla porta 1524 in quanto quest'ultima è quella utilizzata da tale servizio.

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

Infine, come si può notare dall'immagine seguente, le modifiche apportate impediscono l'accesso alla shell sulla macchina target.

```
(kali@kali)-[~]
$ nc -nv 192.168.2.100 1524
(UNKNOWN) [192.168.2.100] 1524 (ingreslock) : Connection refused
```