

# REMEDIATION META

(ATTACCHI ALLE WEB APP)

Nel seguente report, verranno riportate le modalità di risoluzione delle seguenti vulnerabilità:

- 1) VNC Server 'password' Password
- 2) Bind Shell Backdoor Detection
- 3) NFS Exported Share Information Disclosure

## 1. VNC Server 'password' Password

### DESCRIZIONE VULNERABILITA'

Il VNC server in esecuzione su host remoto, è protetto da una password debole. Nessus ha avuto la capacità di fare login utilizzando l'autenticazione VNC e una password di 'password'. Un utente non autorizzato potrebbe sfruttare tale vulnerabilità e prendere controllo del sistema da remoto

### SOLUZIONE

Proteggi il servizio VNC con una password più complessa.

#### 61708 - VNC Server 'password' Password

##### Synopsis

A VNC server running on the remote host is secured with a weak password.

##### Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

##### Solution

Secure the VNC service with a strong password.

##### Risk Factor

Critical

### REMEDIATION

Come suggerisce la soluzione della sopracitata vulnerabilità, dobbiamo proteggere il servizio VNC con una password più complessa. Per fare ciò dobbiamo passare all'utenza root e digitare 'vncpasswd'.

Cos'è il servizio VNC? VNC funziona su un modello client/server. Un componente server viene installato sul computer remoto (quello che si desidera controllare) e un visualizzatore VNC, o client, viene installato sul dispositivo da cui si desidera controllare. Questo può includere un altro computer, un tablet o un telefono cellulare. Quando il server e il visualizzatore sono connessi, il server trasmette una copia dello schermo del computer remoto al visualizzatore.

```
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin#
```

## 2. Bind Shell Backdoor Detection

### DESCRIZIONE VULNERABILITÀ

Una shell sta ascoltando da remoto una porta senza l'uso di alcuna autorizzazione. Un attaccante potrebbe usare questa vulnerabilità per connettersi da remoto e inviare comandi diretti.

### SOLUZIONE

Verifica se l'host remoto sia stato compromesso, e reinstalla il sistema se necessario

#### 51988 - Bind Shell Backdoor Detection

##### Synopsis

The remote host may have been compromised.

##### Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

##### Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

##### Risk Factor

Critical

### REMEDIATION

```
(kali㉿kali)-[~]
└─$ nc -nv 192.168.50.3 1524
(UNKNOWN) [192.168.50.3] 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:/#
```

Con il comando ``nc -nv 198.xx.xx.xxx 1524``

- nc netcat
- 198.xx.xx.xxx (Indirizzo IP di destinazione o nome host del server)
- 1524 (porta di binding 1524)

Cos'è Bind Shell

Bind shell è una shell normale proprio come la riga di comando del terminale Linux o il prompt dei comandi (cmd) in Windows, ma è necessario l'indirizzo IP del server e lo strumento net-cat. nc 198.xx.xx.xx 1524 (nc (nome utente) 198.xx.xx.xx (indirizzo IP) 1524 (nome porta). Utilizzando questo tipo di comando è possibile collegare facilmente il terminale al server di destinazione.

La porta ingreslock (1524/TCP) viene spesso utilizzata come backdoor dai programmi che sfruttano i servizi RPC (Remote Procedure Call) vulnerabili. La backdoor è solitamente accompagnata da un file chiamato /tmp/bob che è il file di configurazione che apre una shell sulla porta.

Configurare ad <off> le voci 'exec' e 'ingreslock'

```
GNU nano 2.0.7      File: /etc/inetd.conf
#<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$
#<off>#exec           stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
#<off>#ingreslock     stream  tcp    nowait  root    /bin/bash bash  -i
```

```
msfadmin@metasploitable:/etc$ cat inetd.conf
#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbi
n/smbd
telnet               stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.tel
netd
#<off># ftp           stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbi
n/in.ftpd
tftp                dgram  udp    wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tft
pd /srv/tftp
shell               stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rsh
d
login               stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlo
gind
#<off>#exec           stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbi
n/in.rexecd
#<off>#ingreslock     stream  tcp    nowait  root    /bin/bash bash  -i
msfadmin@metasploitable:/etc$ _
```

Possiamo verificare che le modifiche siano apportate correttamente quando digitando 'nc -nv <ipaddress> 1524' mi viene rifiutato l'accesso alla shell della macchina target

```
(kali@kali)-[~]
$ nc -nv 192.168.50.3 1524
(UNKNOWN) [192.168.50.3] 1524 (ingreslock) : Connection refused
```

---

### 3. NFS Exported Share Information Disclosure

#### DESCRIZIONE VULNERABILITÀ

Per risolvere questa vulnerabilità è necessario configurare l'NFS in un host remoto in modo tale che solamente gli host autorizzati

#### SOLUZIONE

Configura NFS in un host remoto in modo tale che solamente l'host autorizzato possa montare le sue condivisioni da remoto

#### 11356 - NFS Exported Share Information Disclosure

##### Synopsis

It is possible to access NFS shares on the remote host.

##### Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

##### Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

##### Risk Factor

Critical

#### REMEDIATION

```
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)
```

In questa configurazione:

- **/** = indica che viene condivisa la root del filesystem
- **\*** = qualsiasi indirizzo IP può accedere ai dati della directory root
- **rw** = consente agli host di apportare modifiche al file system, in lettura e scrittura;
- **ro** = ne permette solo la lettura
- **sync** = Il server NFS non risponderà alle richieste prima che le modifiche apportate dalle richieste precedenti vengano scritte su disco;
- **async** = Per abilitare invece le scritture asincrone
- **no\_root\_squash** = disabilita la configurazione di default di NFS, quindi un host che apporta modifiche su file di condivisione NFS verranno eseguite come utente anonimo.

- **no\_subtree\_check**= è una funzionalità di protezione che verifica che il file a cui si accede si trovi nella struttura esportata del server NFS)

Per evitare che un attaccante mi possa leggere e/o scrivere sui file della macchina, andiamo a commentare l'ultima stringa di codice

```
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)
```