

Remediation Meta

Dopo aver effettuato una scansione con Nessus sull'indirizzo IP 192.168.50.100 sono state rilevate molte vulnerabilità. Ho iniziato a risolvere quelle di impatto CRITICO indicate nella traccia.

1. NFS Exported Share Information Disclosure

Come possiamo leggere dalla pagina di Nessus la seguente vulnerabilità permette a un host remoto di accedere a :

- Elenco delle directory o dei file condivisi tramite NFS.
- Parametri di configurazione delle condivisioni, inclusi i permessi di accesso.
- Alcune informazioni sul sistema host.

Come indicato sempre da Nessus per risolvere la vulnerabilità ho commentato quindi l'ultima riga che risultava essere la riga che causava la vulnerabilità nel file exports presente nella directory /etc.

In più ho dato i permessi alla mia macchina di Kali per leggere e sincronizzare file, directory e informazioni

Metasploit2 [in esecuzione] - Oracle VM VirtualBox

```
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)
#
/nfs_share 192.168.50.2 (rw,sync)
# *(rw,sync,no_root_squash,no_subtree_check)

[ Read 12 lines ]
^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
```

2. Rexecd Service Detection

Nessus ci indica che questa vulnerabilità permette agli utenti della rete di eseguire comandi da remoto, i per se questa non è una vulnerabilità, il problema è che rexecd non fornisce nessun servizio di autenticazione, quindi può essere usato per attaccare il sistema.

Per risolvere questa vulnerabilità Nessus ci indica quale riga modificare all'interno del file `inetd.conf` presente nella cartella `/etc`.

Possiamo notare che la vulnerabilità viene risolta commentando la penultima riga del file. (`#exec stream tcp nowait root /usr/sbin/tcpd...`)



```
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$
#exec stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.re$
#ingreslock stream tcp nowait root /bin/bash bash -i

[ Read 8 lines ]
^G Get Help ^O WriteOut ^R Read File ^V Prev Page ^X Cut Text ^C Cur Pos
^X Exit ^J Justify ^U Where Is ^U Next Page ^U UnCut Text ^T To Spell
```

NB : possiamo notare che tutte le righe nel file sono commentate, questo perchè in questo file sono presenti altre righe che corrispondono a vulnerabilità.

Per esempio questo file conteneva anche la vulnerabilità : **rlogin Service Detection** risolta commentando la linea che inizia con **login**.

Le altre righe sono state commentate in maniera preventiva.

3. VNC Server Password

Per risolvere questa Vulnerabilità molto semplicemente basta impostare una password sicura al Servizio VNC, visto che la password di base era "password".

```

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)? n
root@metasploitable:/home/msfadmin# _

```

4. Bind Shell Backdoor Detection

Nessus ci indica che c'è una backdoor exploitabile sulla porta 1524 con il protocollo TCP, in questo caso creerò una regola su iptables chiudendo in ingresso la porta, impedendo così di connettersi sulla porta 1524.

Regola -> `sudo iptables -A INPUT -p tcp --dport 1524 -j DROP`

```

root@metasploitable:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:ingreslock
DROP       tcp  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

```