

Vulnerability Report

Vulnerabilità: 11356 - NFS Exported Share Information Disclosure

Synopsis

È possibile accedere alle condivisioni NFS sull'host remoto.

Descrizione

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un attaccante potrebbe sfruttare questa vulnerabilità per leggere (e possibilmente scrivere) file sull'host remoto.

Dettagli di Rischio

Fattore di Rischio: Critico

Porte Aperte

Porta 2049/udp:

Servizio: NFS (Network File System)

Descrizione: Il report indica che il servizio NFS è in esecuzione sulla porta 2049/udp. Questo è evidenziato dalla sezione "Plugin Output"

```
(kali@kali)~$ nmap -p 2049 -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 04:35 EDT
Nmap scan report for 192.168.50.101
Host is up (0.010s latency).

PORT      STATE SERVICE VERSION
2049/tcp  open  nfs      2-4 (RPC #100003)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.39 seconds
```

Porta 111/tcp:

Servizio: RPCbind

Descrizione: Anche se non esplicitamente menzionato nel report, è noto che il servizio NFS utilizza RPCbind per gestire le richieste di montaggio. La porta 111/tcp è generalmente utilizzata da RPCbind

```
(kali@kali)~$ nmap -p 111 -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 04:36 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0023s latency).

PORT      STATE SERVICE VERSION
111/tcp   open  rpcbind 2 (RPC #100000)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.26 seconds
```

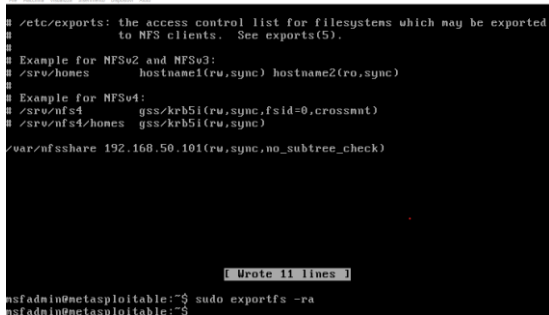
Impatto

Confidenzialità: Alta - L'attaccante potrebbe accedere a dati sensibili.

Integrità: Alta - L'attaccante potrebbe modificare i contenuti del server.

Disponibilità: Alta - L'attaccante potrebbe causare un crash del sistema.

Soluzione



```
/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)
/var/nfsshare 192.168.50.101(rw,sync,no_subtree_check)

[ Wrote 11 lines ]

msfadmin@metasploitable:~$ sudo exportfs -ra
msfadmin@metasploitable:~$
```

Password Debole del Server VNC

Synopsis

Un server VNC in esecuzione sull'host remoto è protetto con una password debole, rendendo possibile l'accesso non autorizzato.

Descrizione: Il server VNC sull'host remoto utilizza una password predefinita o debole ("password"). Questo consente a un attaccante remoto non autenticato di accedere al sistema utilizzando l'autenticazione VNC. Tale vulnerabilità può portare alla compromissione completa del sistema, permettendo all'attaccante di eseguire qualsiasi operazione.

Soluzione Raccomandata: Modificare immediatamente la password del server VNC, scegliendone una robusta e complessa. Una password forte deve contenere una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali.

Fattore di Rischio: Critico

Dettagli dell'Output del Plugin:

- Porta: tcp/5900/vnc

Nota: Nessus è riuscito ad accedere utilizzando la password "password".

Soluzione

Cambiare la password predefinita del server VNC con una più complessa e dare una regola al firewall per consentire solo l'accesso dalla macchina autorizzata.

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$
```

Rilevamento Backdoor Bind Shell

Synopsis

L'host remoto potrebbe essere stato compromesso.

Descrizione

Una shell sta ascoltando sulla porta remota senza richiedere alcuna autenticazione. Un attaccante potrebbe utilizzarla connettendosi alla porta remota e inviando comandi direttamente.

Fattore di Rischio

Critico

Output del Plugin

Porta: tcp/1524/wild_shell

Nessus è stato in grado di eseguire il comando id utilizzando la seguente richiesta:

Questo ha prodotto il seguente output non modificato (limitato a 10 righe):

```
root@metasploitable:/# id
```

```
uid=0(root) gid=0(root) gruppi=0(root)
```

Soluzione

```
(kali@kali)~$ nc 192.168.50.101 1524
root@metasploitable:/# fuser -k -n tcp 1524
1524/tcp: 4412 5209

(kali@kali)~$ nmap 192.168.50.101 1524
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 09:03 EDT
Nmap scan report for 192.168.50.101
Host is up (0.018s latency).
Not shown: 983 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1099/tcp  open  xrtregistry
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 2 IP addresses (1 host up) scanned in 13.30 seconds
```

Vulnerabilità: rexecd Service Detection

Synopsis

Il servizio `rexecd` è abilitato sulla macchina remota.

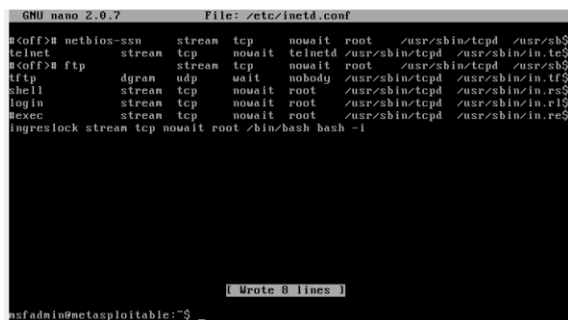
Descrizione

Il servizio `rexecd` permette agli utenti di una rete di eseguire comandi da remoto. Questo servizio, se abilitato, può essere sfruttato da un attaccante per eseguire comandi sulla macchina remota senza autenticazione adeguata, portando a una possibile compromissione del sistema.

Fattore di Rischio: Critico

Soluzione

Disabilitare il servizio `rexecd` sulla macchina remota per prevenire l'esecuzione non autorizzata di comandi. Questo può essere fatto commentando la riga `exec` nel file `/etc/inetd.conf` e riavviando il sistema.



```
GNU nano 2.0.7 File: /etc/inetd.conf
#off># netbios-ssn  stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/
telnet      stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.tel
#off># ftp          stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/
ftp         dgram   udp    wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.ft
shell       stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re
login       stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.r
rexecd      stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re
ingreslock  stream  tcp    nowait  root    /bin/bash bash -i

[ Wrote 0 lines ]
msfadmin@metasploitable:~$
```