Rossella Amore

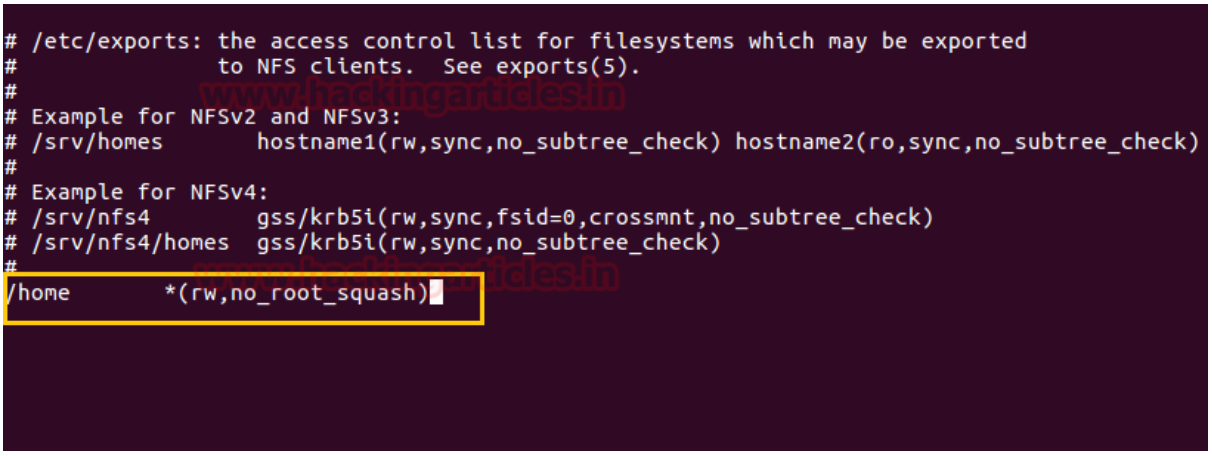
Remediation su Metasploitable

Report sul risk reduction delle vulnerabilità critiche di Metasploitable

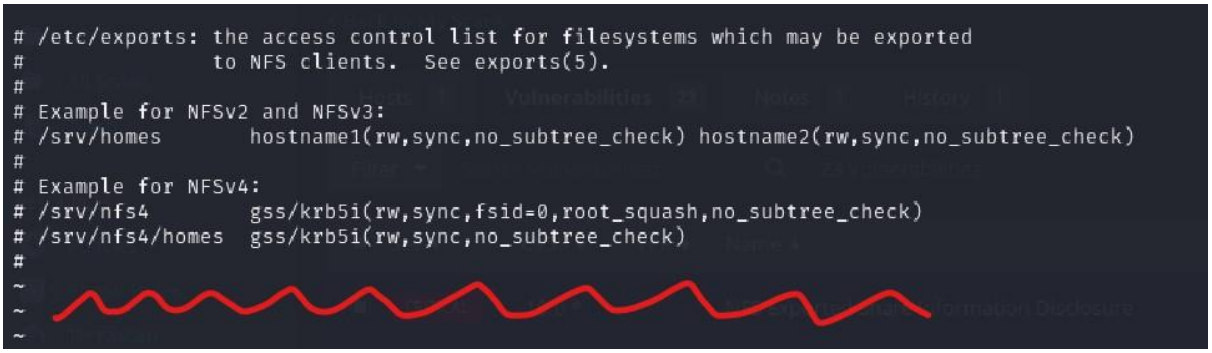
1. NFS Exported Share Information Disclosure

Una configurazione non ideale del file '/etc/exports' permette a chiunque di accedere e modificare dei file critici.
Per rimuovere i privilegi basta configurare il file e rimuovere la riga che assegna i privilegi a tutti gli utenti (*).
Per confermare la modifica basta riavviare il servizio NFS, oppure riavviare la VM.

Prima



Dopo



2. VNC Server 'password' Password

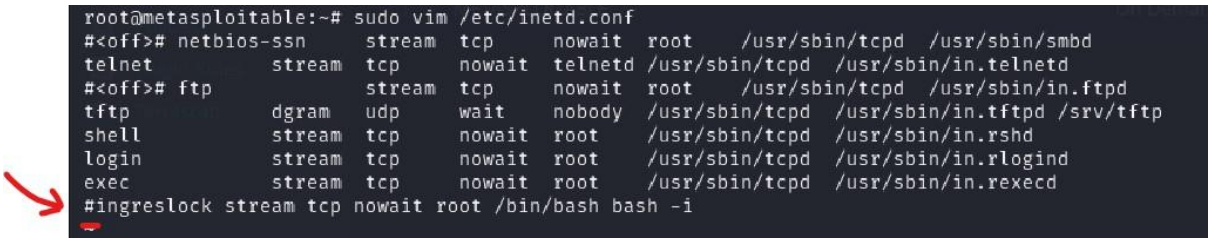
La password di default del server VNC è 'password'. Essendo troppo debole, è stata sostituita da una password più sicura con il comando 'vncpasswd'.

```
root@metasploitable:/# 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)? y
Password:
Warning: password truncated to the length of 8.
Verify:
root@metasploitable:/# vncpasswd
```

3. Bind Shell Backdoor Detection

Nel file '/etc/inetd.conf' è inserito un comando 'ingreslock' che collega un bash interattivo (shell) alla porta aperta 1524 per comunicare con un client remoto. Per rimuovere la backdoor, configurare il file '/etc/inetd.conf' e commentare o rimuovere il comando nell'ultima riga.



Non è più presente la 1524 nella lista delle porte aperte.

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet?
25/tcp    open  smtp?
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql?
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
6667/tcp  open  irc          UnrealIRCd (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13?
8180/tcp  open  unknown
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
45011/tcp open  nlockmgr     1-4 (RPC #100021)
51701/tcp open  mountd       1-3 (RPC #100005)
57683/tcp open  status       1 (RPC #100024)
60517/tcp open  java-rmi     GNU Classpath grmiregistry
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

4. rexecd Service Detection

Nonostante fosse una vulnerabilità segnalata nella slide, la scansione sulla VM Metasploitable non la mostra. Utilizzando il comando -sV su nmap per analizzare la versione e i servizi delle porte aperte, si può notare la mancanza di servizi attivi sulla porta 512, nonostante sia aperta. Sembra quindi che il servizio non sia abilitato o che non possa essere usato nemmeno dal client Kali.