W12D4

EPICODE

Esercizio
Traccia e requisiti

Consegna:

1. Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (tecnico, già riassunto) - **ScansioneInizio.pdf**
2. **Screenshot e spiegazione dei passaggi della remediation - RemediationMeta.pdf**
3. Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità (il grafico che mostra tutte le vulnerabilità) - **ScansioneFine.pdf**

Oppure un report unico, a vostra scelta. Penso sia più comodo farne tre comunque.

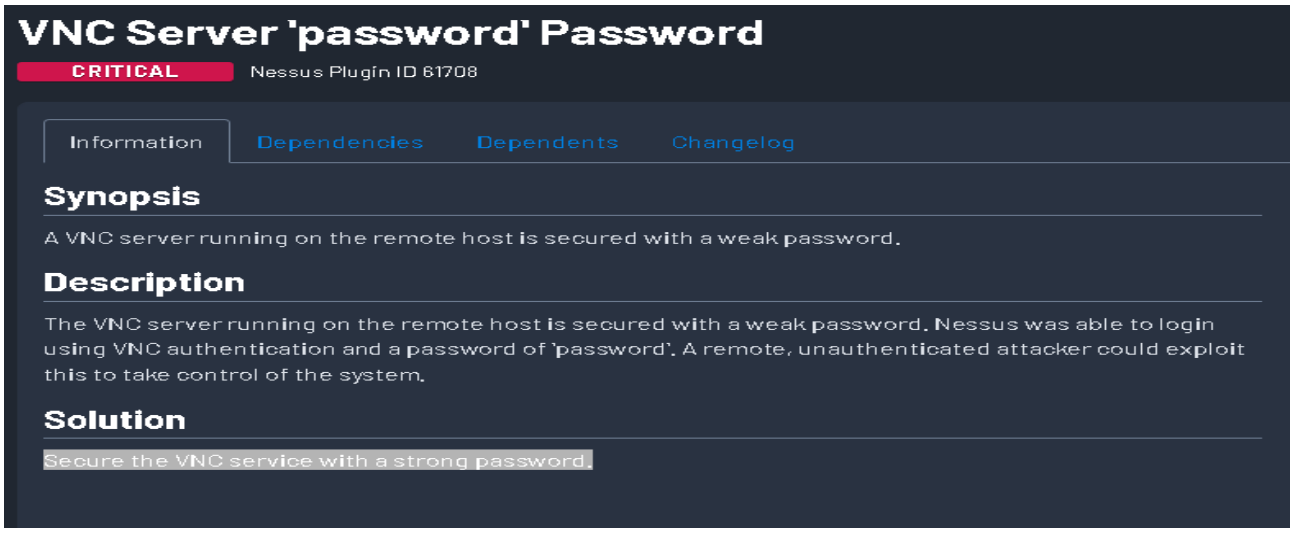
Nota: i report possono essere lasciati in inglese, senza problemi.

Se risolvete le 4 vulnerabilità, potete risolverne una quinta (a scelta), ad esempio con una regola di firewall

4

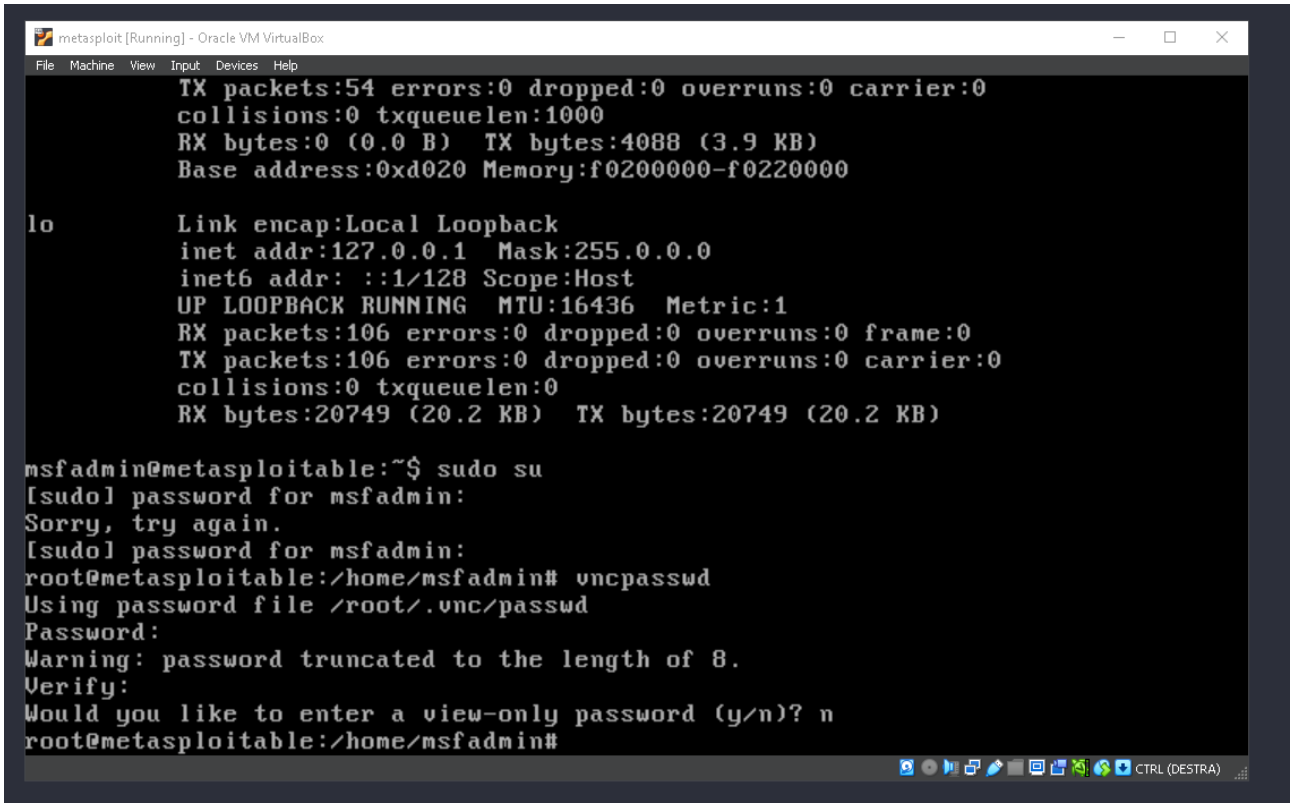
VULNERABILITA' 61708 :

CRITICAL 10.0* - 61708 VNC Server 'password' Password

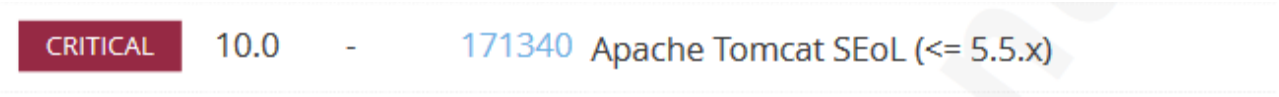


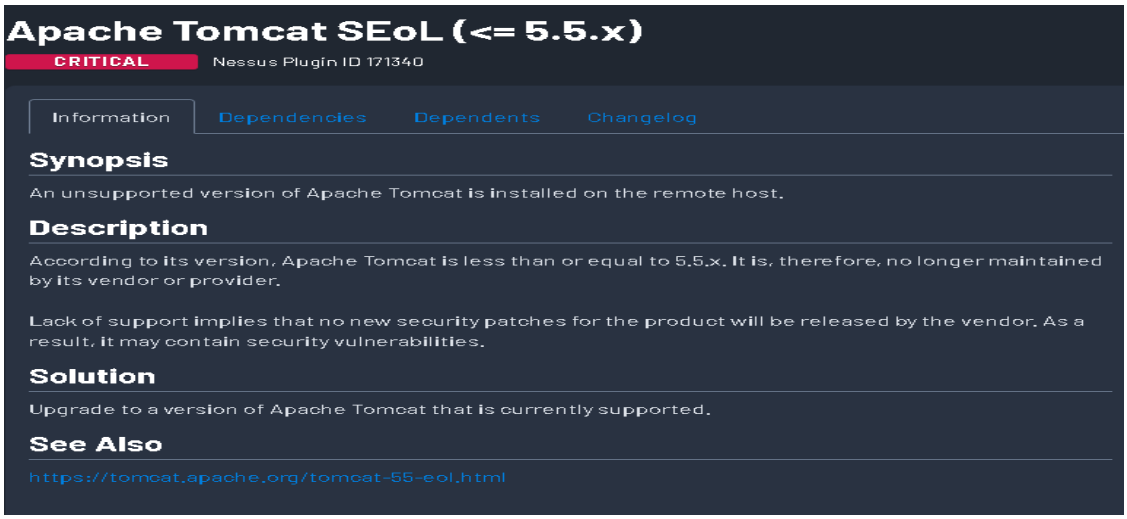
SOLUZIONE:

La soluzione consiste nel modificare la password “debole” con una password “forte”



Seconda Criticità





```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.101
```

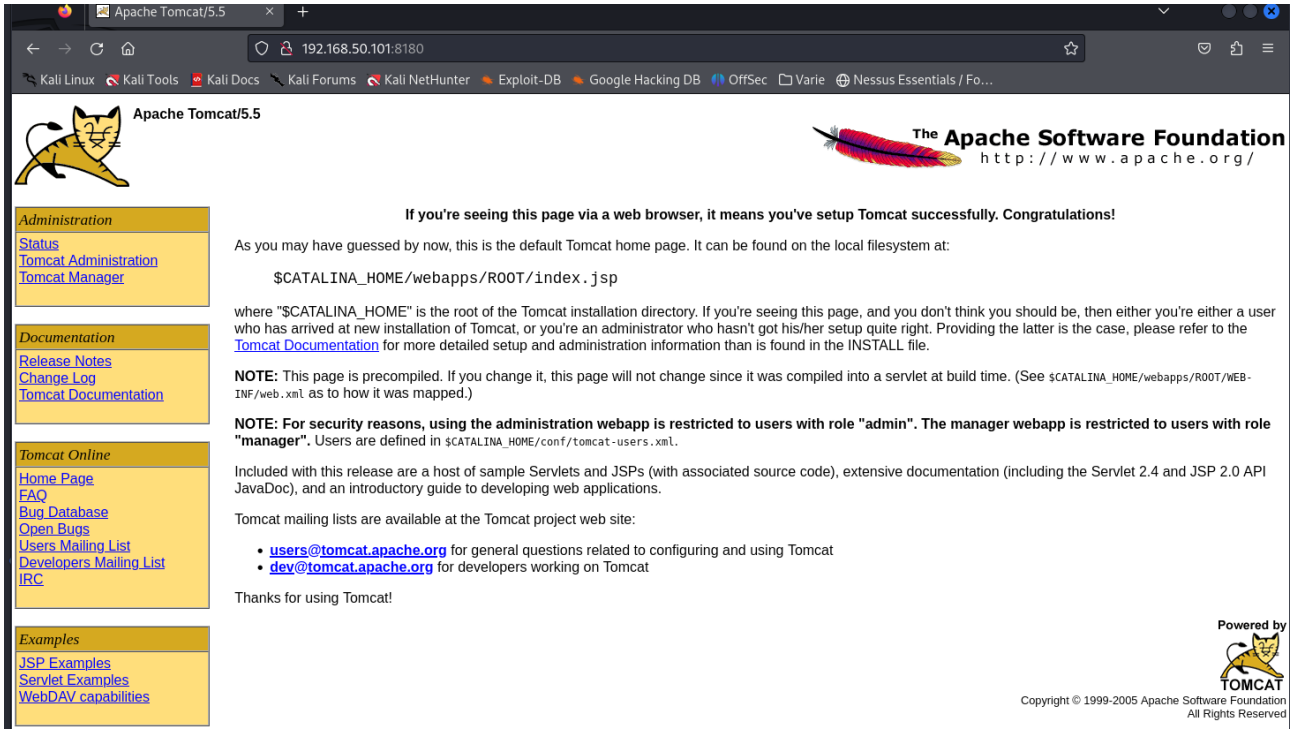
8180/tcp open http   Apache Tomcat/Coyote JSP engine 1.1

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script auth 192.168.50.101 -sS
```

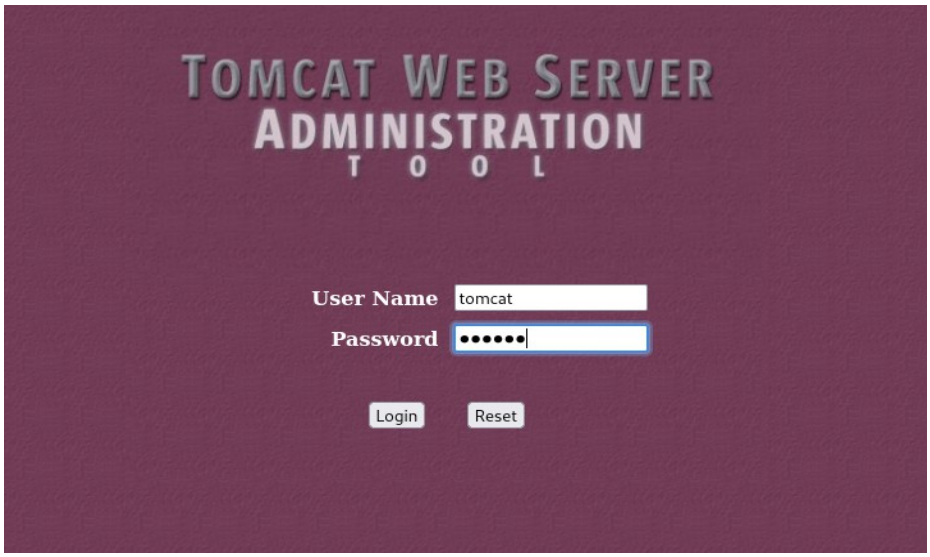
8180/tcp open unknown
| http-default-accounts:
| [Apache Tomcat] at /manager/html/
| tomcat:tomcat
| [Apache Tomcat Host Manager] at /host-manager/html/
|_   tomcat:tomcat
MAC Address: 08:00:27:5F:8F:56 (Oracle VirtualBox virtual NIC)

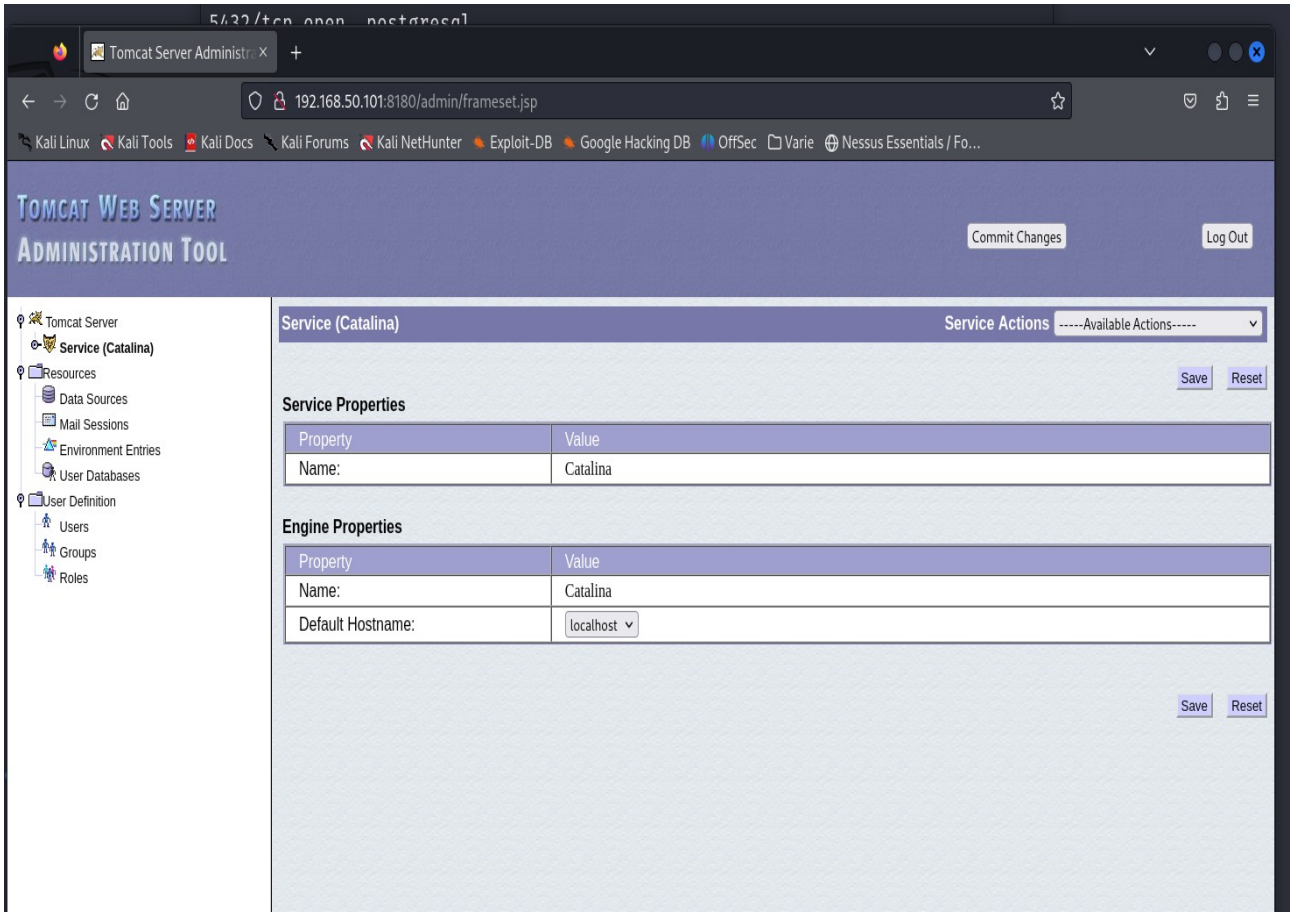
Post-scan script results:
| creds-summary:
| 192.168.50.101:
| 8180/nil:
| tomcat:tomcat - Valid credentials
|_   tomcat:tomcat - Valid credentials
Nmap done: 1 IP address (1 host up) scanned in 44.21 seconds

http://192.168.50.101:8180/

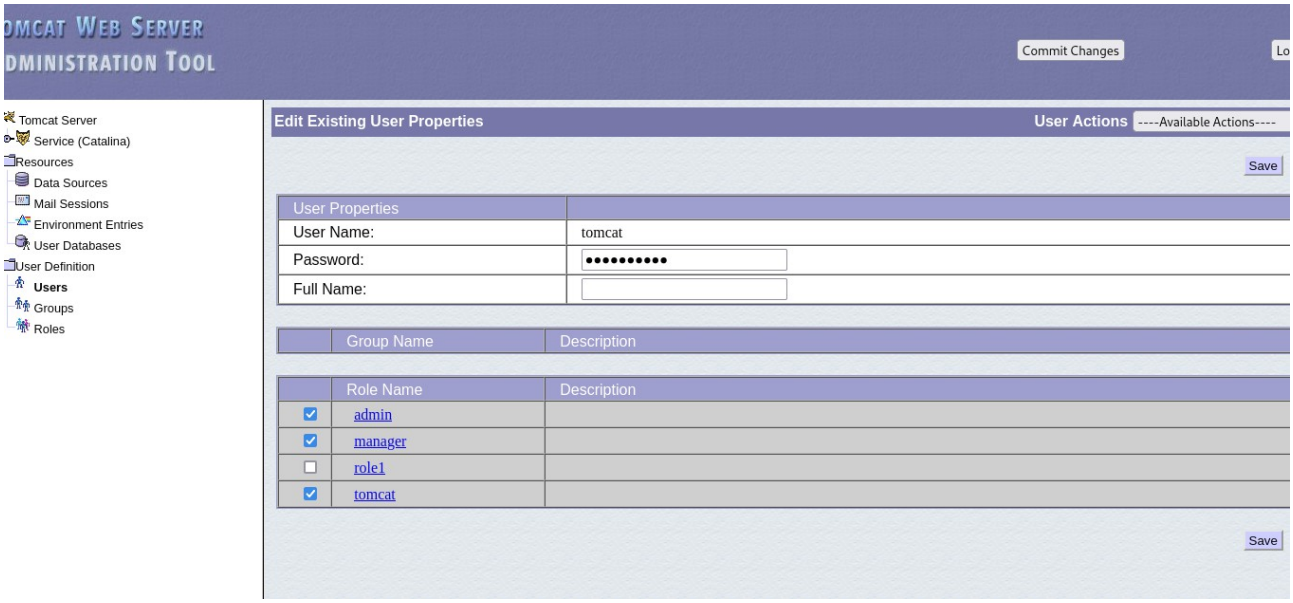


Accesso con credenziali tomcat : tomcat

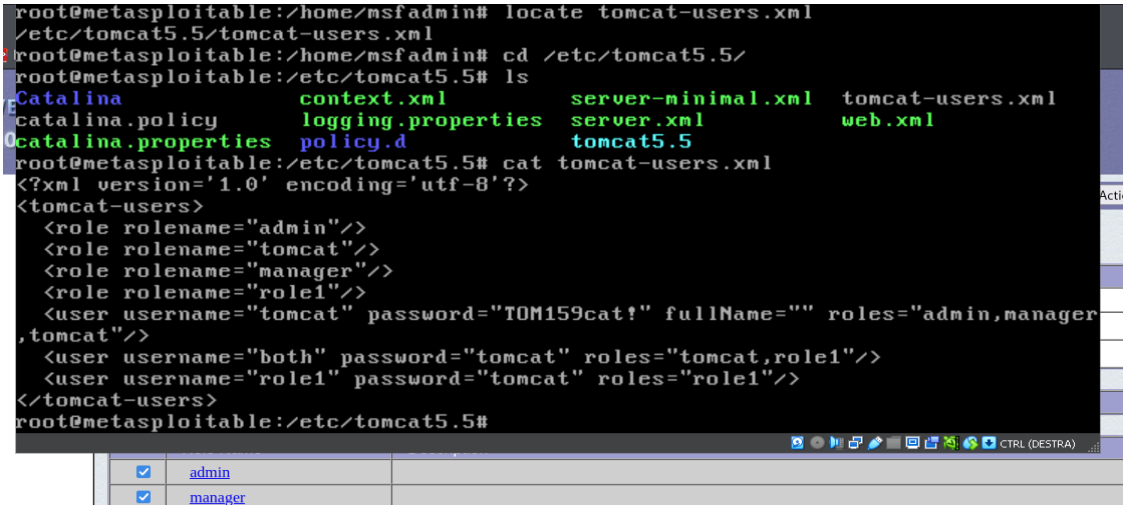




Cambio password amministartore con una piu forte.



Localizzazione file tomcat-users.xml su Metasploitable :



Modifica admin

```
root@metasploitable:/etc/tomcat5.5#
root@metasploitable:/etc/tomcat5.5# cat tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
  <role rolename="admin-gui"/>
  <role rolename="tomcat"/>
  <role rolename="manager"/>
  <role rolename="role1"/>
  <user username="tomcat" password="TOM159cat!" fullName="" roles="admin,manager
,tomcat"/>
  <user username="both" password="tomcat" roles="tomcat,role1"/>
  <user username="role1" password="tomcat" roles="role1"/>
</tomcat-users>
root@metasploitable:/etc/tomcat5.5#
```

Risultato finale delle modifiche per migliorare la sicurezza generale di Tomcat

Terza criticità:

CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection

```
File  Actions  Edit  View  Help
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 09:52 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00052s latency).
Not shown: 977 closed tcp ports (reset)
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      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
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        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:5F:8F:56 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs:
 Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Con “netcat” vediamo che la backdoor è funzionante (porta 1524)

```
┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.50.101 1524
root@metasploitable:/# msfadmin
bash: msfadmin: command not found
root@metasploitable:/# whoami
root
root@metasploitable:/# netstat -an | grep 192.168.50.101
tcp        0      0 192.168.50.101:53       0.0.0.0:*               LISTEN

tcp        0      0 192.168.50.101:1099     192.168.50.100:35304    CLOSE_WAIT

tcp        0      0 192.168.50.101:1524     192.168.50.100:55272    ESTABLISHE
D
udp        0      0 192.168.50.101:137      0.0.0.0:*

udp        0      0 192.168.50.101:138      0.0.0.0:*

udp        0      0 192.168.50.101:53       0.0.0.0:*

root@metasploitable:/#
```

Utilizzando il comando “fuser” tentermo di chiudere quella determinata porta per evitare un futuro utilizzo della backdoor.

```
root@metasploitable:/# fuser -k -n tcp 1524
1524/tcp:             4520  6270

┌──(root㉿kali)-[/home/kali]
└─#
```

Scansione con “nmap” per verificare che la porta sia effettivamente chiusa

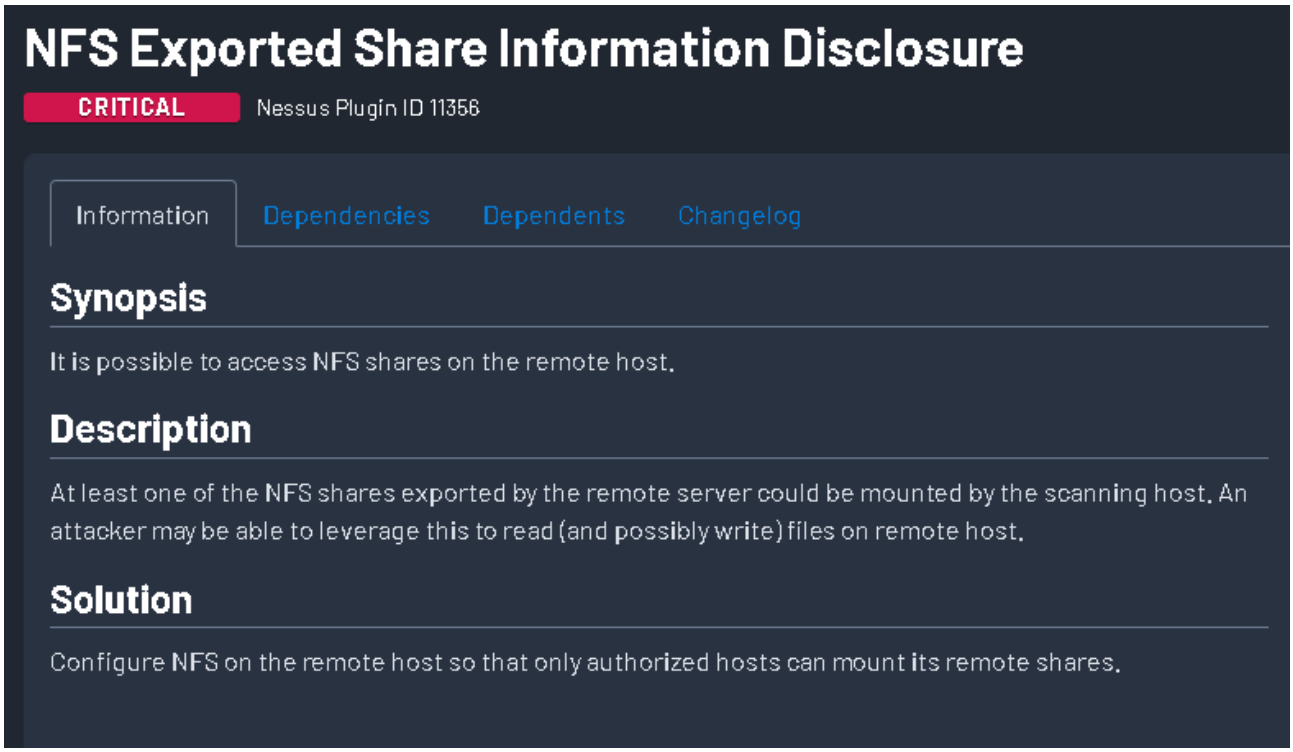
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 10:12 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00055s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp    open  smtp        Postfix smtpd
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)
1099/tcp open  java-rmi     GNU Classpath grmiregistry
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:5F:8F:56 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs:
 Linux, Unix; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.15 seconds
```

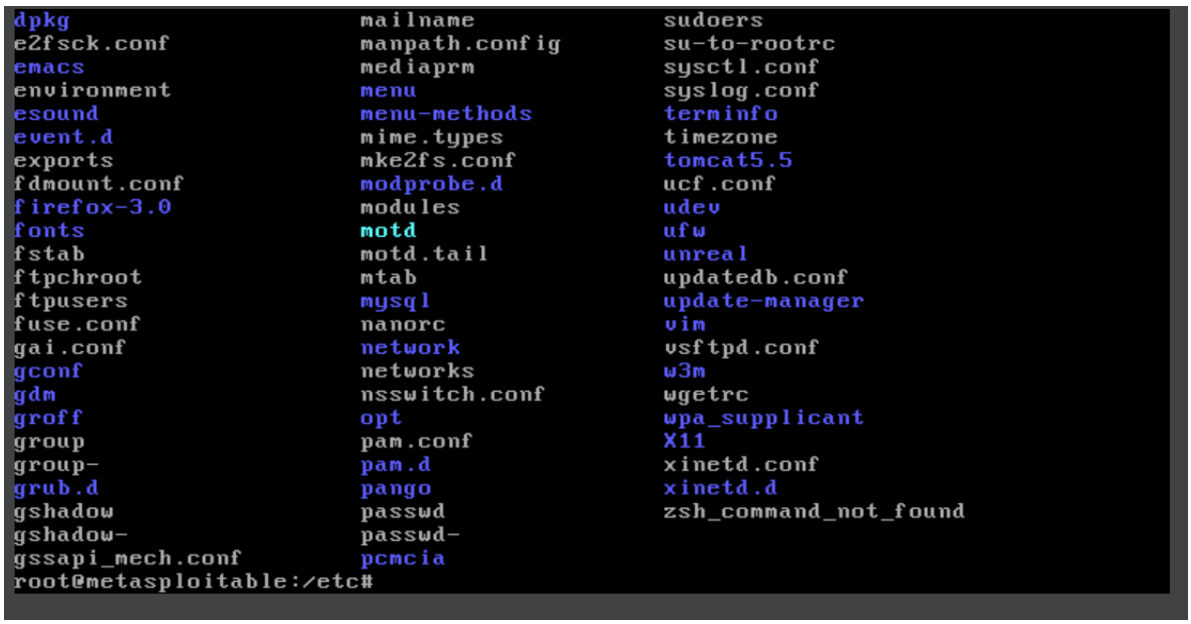
Purtoppo non è una soluzione definitiva,dato che al riavvio di Metasploitable la porta si riattiva e con essa la backdoor.

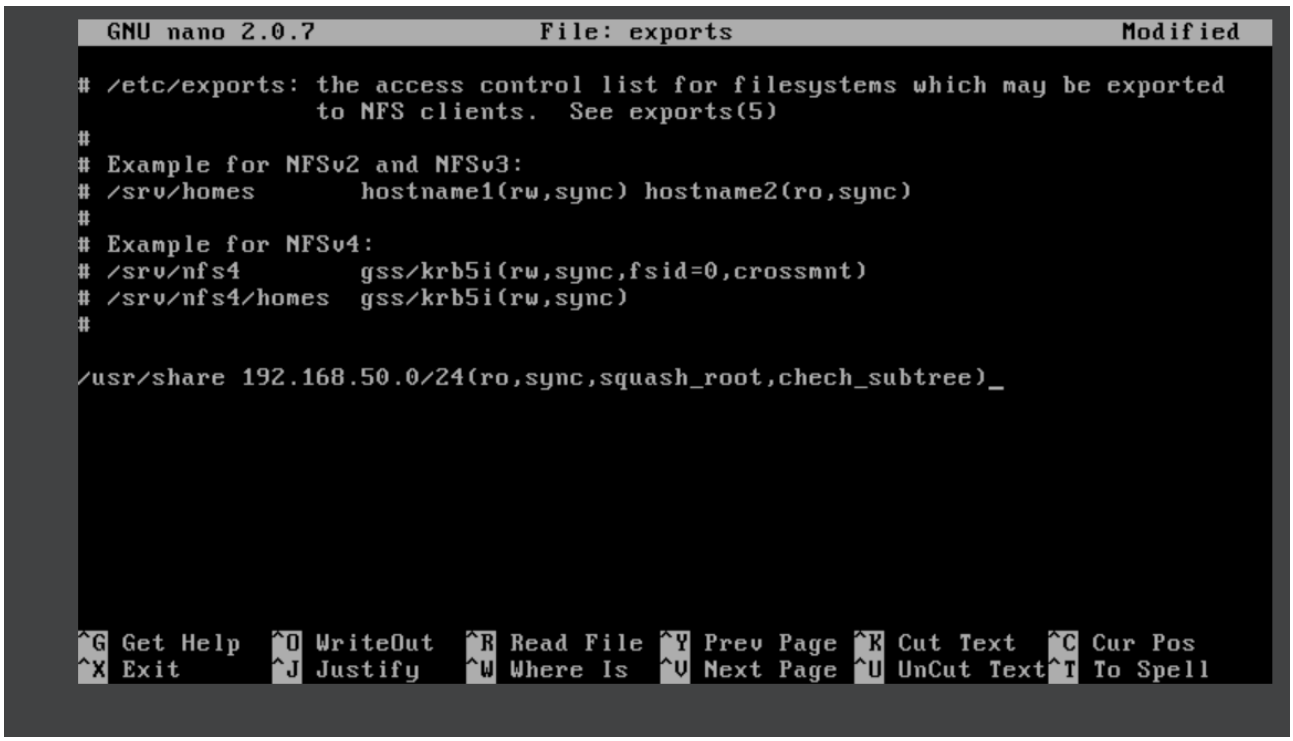
Quarta vulnerabilità:

CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure



Modifichiamo il file EXPORTS:
Questo fa si che SOLO i file nel percorso specificato siano condivisi e SOLO con tutta la rete interna di metasploitable.




GNU nano 2.0.7 File: exports Modified
/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)
#
/usr/share 192.168.50.0/24(ro,sync,squash_root,chech_subtree)_
^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