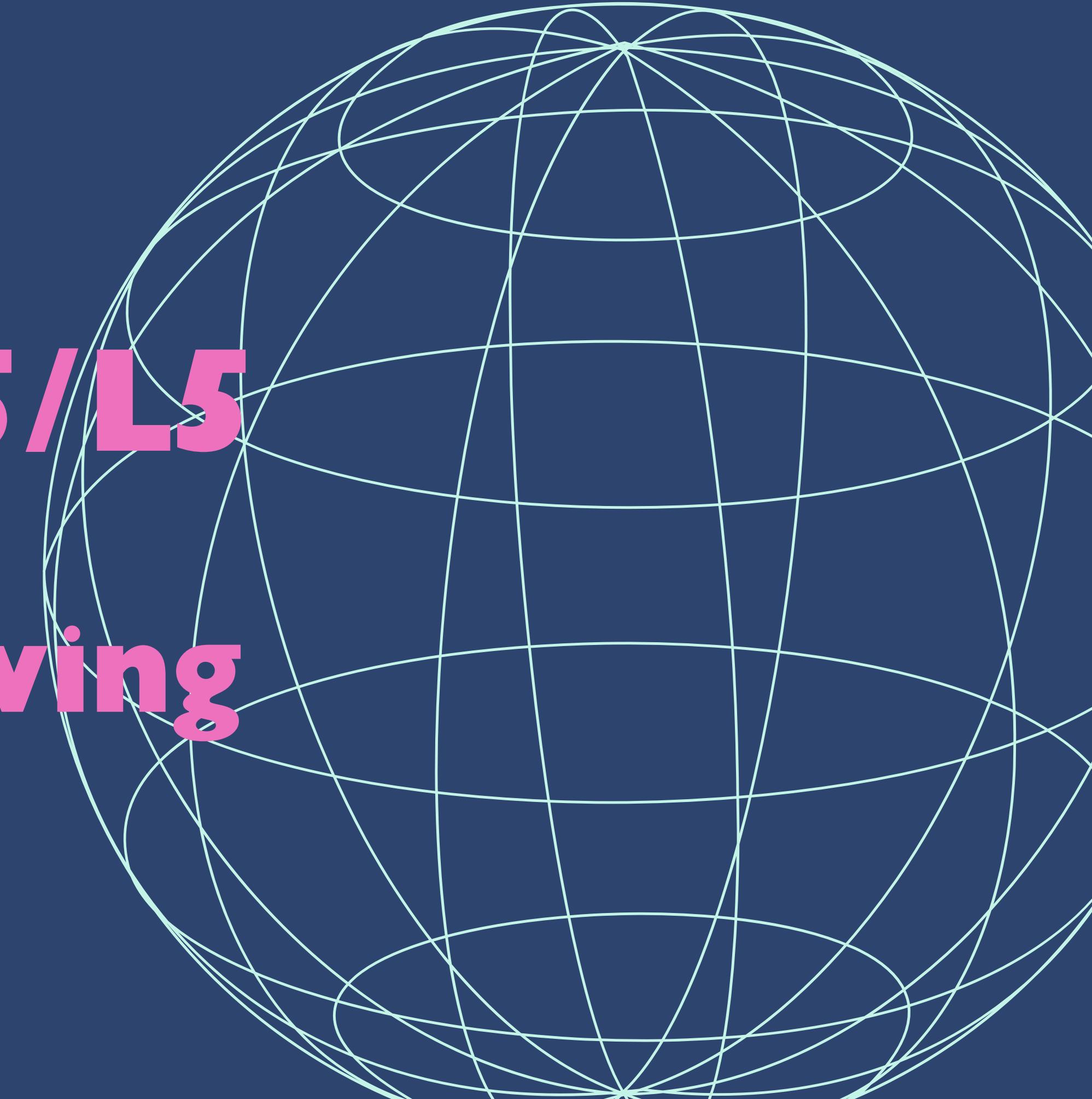


EPISODE

CS0424 - S5/L5

**Vulnerability
Scanner & Solving**

Victoria M. Braile



INDEX



- 1** Obiettivi esercitazione
- 2** Scansione vulnerabilità
- 3** Apache Tomcat AJP Connector Request Injection (Ghostcat)
- 4** Bind Shell Backdoor Detection
- 5** NFS Exported Share Information Disclosure
- 6** VNC Server 'password' Password
- 7** Scansione di verifica

OBIETTIVI ESERCITAZIONE

1
Effettuare **scansione** completa su target **Metasploitable** con **Nessus** per identificare vulnerabilità.

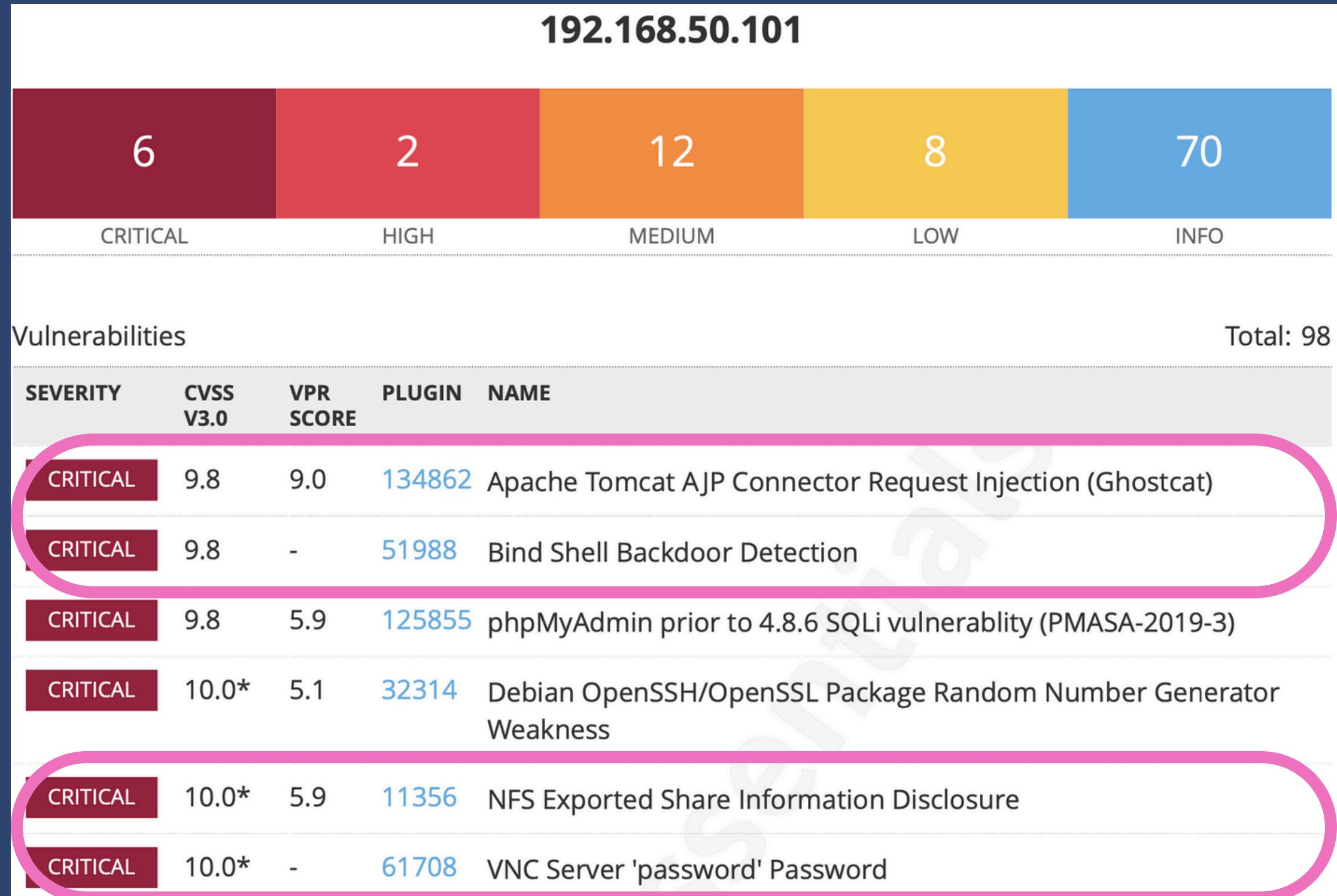
2
Implementare **azioni di rimedio** su 2-4 **vulnerabilità critiche** - high identificate.

3
Dimostrare **efficacia** azioni di rimedio con una **nuova scansione** sul target e confrontare i risultati ottenuti con quelli precedenti.

Scansione vulnerabilità

Ho effettuato una scansione base con **Nessus** allo scopo di individuare le **principali vulnerabilità** citate dalla traccia dell'esercitazione, inserendo come **target 192.168.50.101** (Metasploitable2).

Dopodiché, come evidenziato, ho individuato le **4 vulnerabilità critiche** da mitigare.



Apache Tomcat AJP Connector Request Injection (Ghostcat)



DESCRIZIONE

È stata riscontrata una vulnerabilità di lettura/inclusione di file nel **connettore AJP**. Un aggressore remoto non autenticato potrebbe sfruttare questa vulnerabilità per **leggere i file dell'applicazione Web** da un **server vulnerabile**. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe **caricare codice JavaServer Pages (SP) dannoso** all'interno di una serie di tipi di file e ottenere l'**esecuzione di codice in modalità remota (RCE)**.

SOLUZIONE

Aggiornare la **configurazione AJP** per richiedere l'autorizzazione e/o **aggiornare il server Tomcat** a 7.0.100, 8.5.51, 9.0.31 o successivo.

Port	Hosts
8009 / tcp / ajp13	192.168.50.101

RISOLUZIONE

- **Verificare la versione di Tomcat**

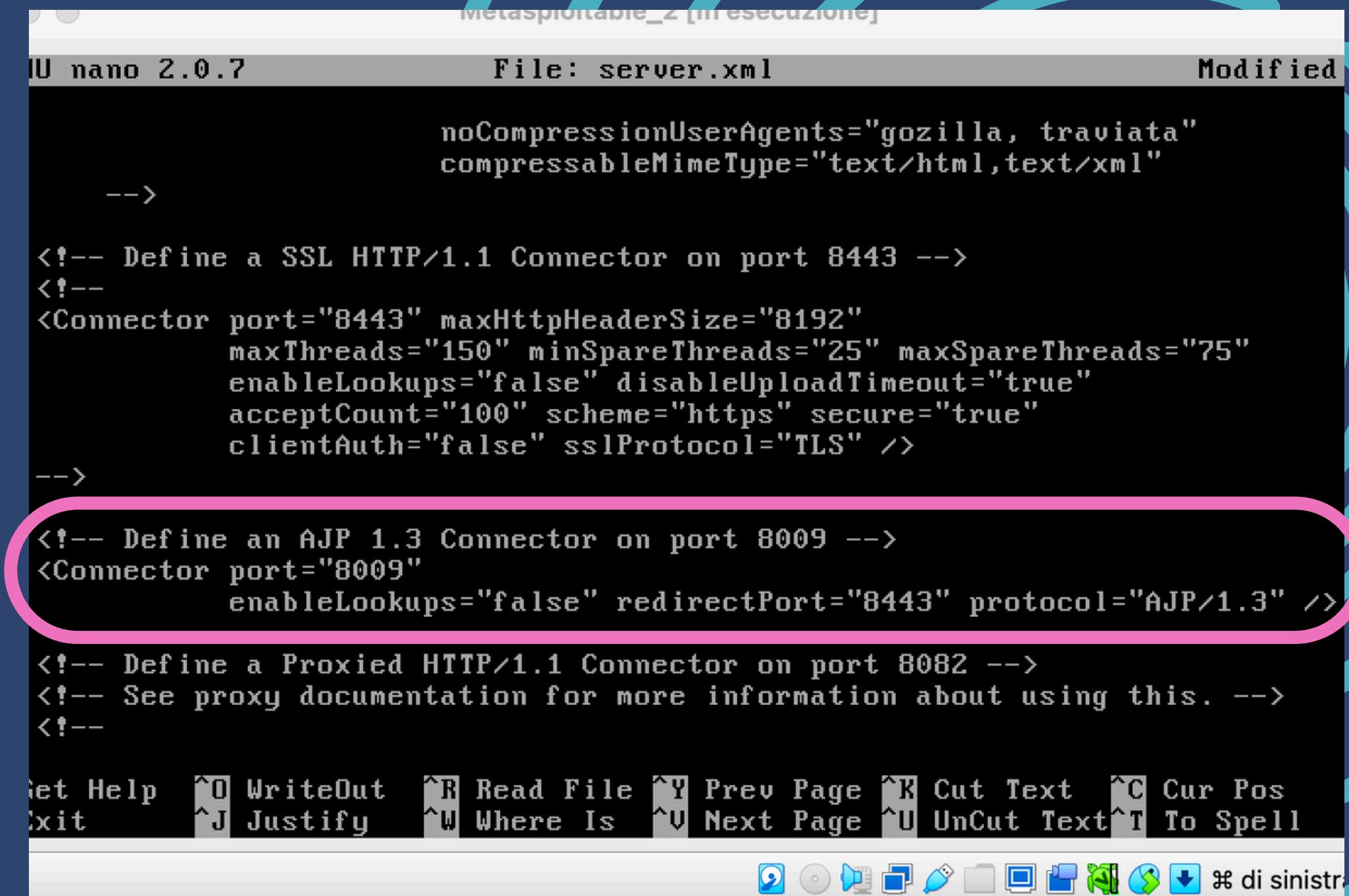
Per prima cosa ho cercato Apache Tomcat su Metasploitable2 in **/usr/share** verificando che vi è installata la versione **tomcat5.5**.

- **Modificare il file server.xml**

Entrando nella cartella **conf** all'interno di **tomcat5.5** trovo il file **server.xml** che andrò a modificare con il comando **sudo nano server.xml**.

- **Disabilitare il connettore AJP**

A questo punto vado a disabilitare il connettore **AJP** modificandolo all'interno del file **server.xml** di **Tomcat**.



```
Metasploitable_2 [in esecuzione]
File: server.xml
Modified: 2023-09-12 10:30:00

noCompressionUserAgents="ozilla, traviata"
compressableMimeType="text/html, text/xml"

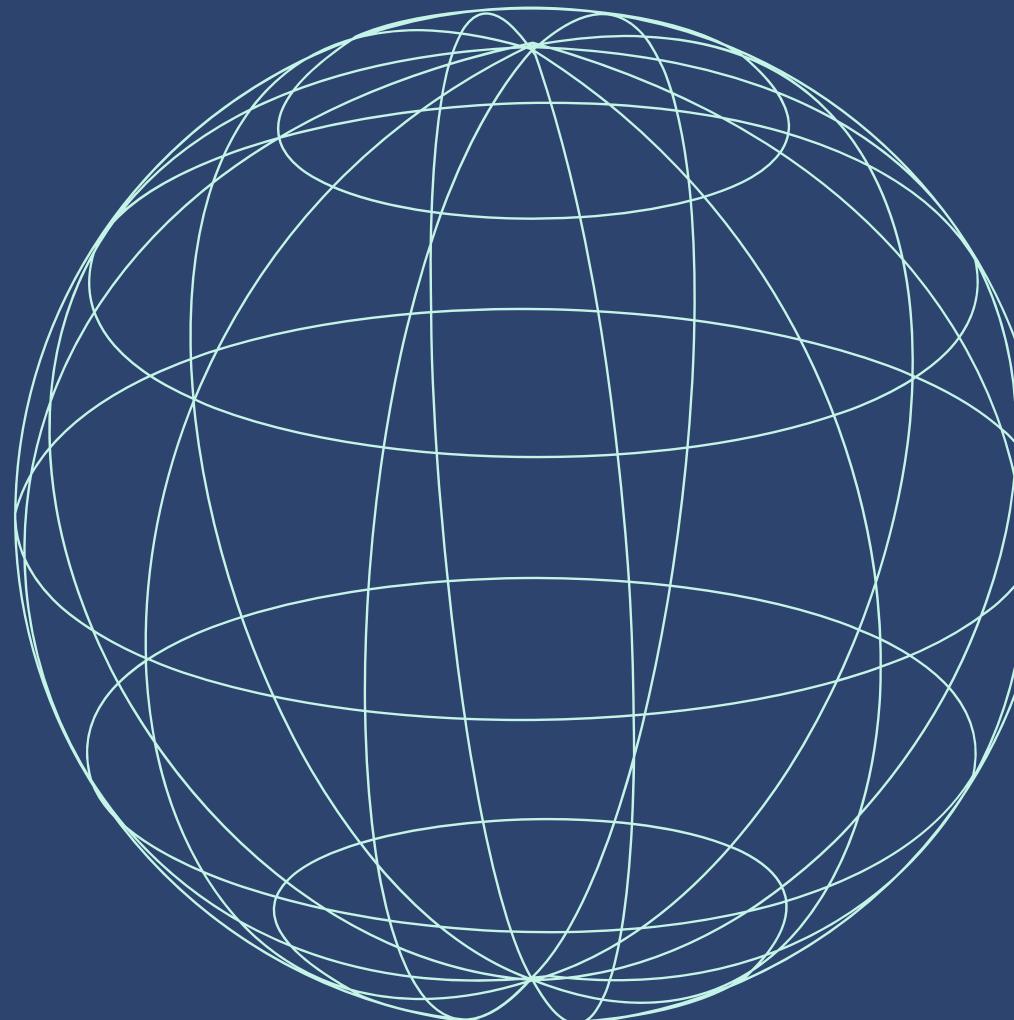
-->
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" />
-->

<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009"
enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />

<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this. -->
<!--

Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Bind Shell Backdoor Detection



DESCRIZIONE

Una **shell** è **in ascolto** sulla porta remota senza che sia richiesta **alcuna autenticazione**. Un utente malintenzionato può utilizzarla collegandosi alla porta remota e inviando direttamente i comandi.

SOLUZIONE

Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

Port	Hosts
1524 / tcp / wild_shell	192.168.50.101

RISOLUZIONE

- **Verificare la porta in ascolto**

Per prima cosa ho verificato con nmap che la porta in ascolto è la **1524/tcp**.

- **Verifica con netcut**

Ho verificato con **nc** che la shell fosse realmente in ascolto sulla porta **1524**.

- **Chiusura porta**

Ho dunque proceduto a chiudere la porta per tutti gli altri host con il comando **sudo iptables -A INPUT -o tcp --dport 1524 -j DROP**.

- **Verifica con nmap**

Ho verificato con **nmap** e questa volta la porta risulta filtrata.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV -ss 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 07:56 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00090s 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 smptd
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?      Netkit rshd
514/tcp   open  shell        Netkit rshd
1095/tcp  open  java-imi   Java Classpath grimiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2.4 (RPC #100002)

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: 08:00:27:00:43:18 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_ kernel_output (limited to 10 lines):
- snip -
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.60 seconds

(kali㉿kali)-[~]
└─$ nc 192.168.50.101 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# whoami
root
root@metasploitable:/# █
```

RISOLUZIONE

- **Verificare la porta in ascolto**

Per prima cosa ho verificato con **nmap** che la porta in ascolto è la **1524/tcp**.

- **Verifica con netcut**

Ho verificato con **nc** che la shell fosse realmente in ascolto sulla porta **1524**.

- **Chiusura porta**

Ho dunque proceduto a chiudere la porta per tutti gli altri host con il comando **sudo iptables -A INPUT -o tcp --dport 1524 -j DROP**.

- **Verifica con nmap**

Ho verificato con **nmap** e questa volta la porta risulta filtrata.

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
msfadmin@metasploitable:~$ iptables -L
iptables v1.3.8: can't initialize iptables table 'filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
DROP      tcp   --  anywhere       anywhere          tcp dpt:ingreslock

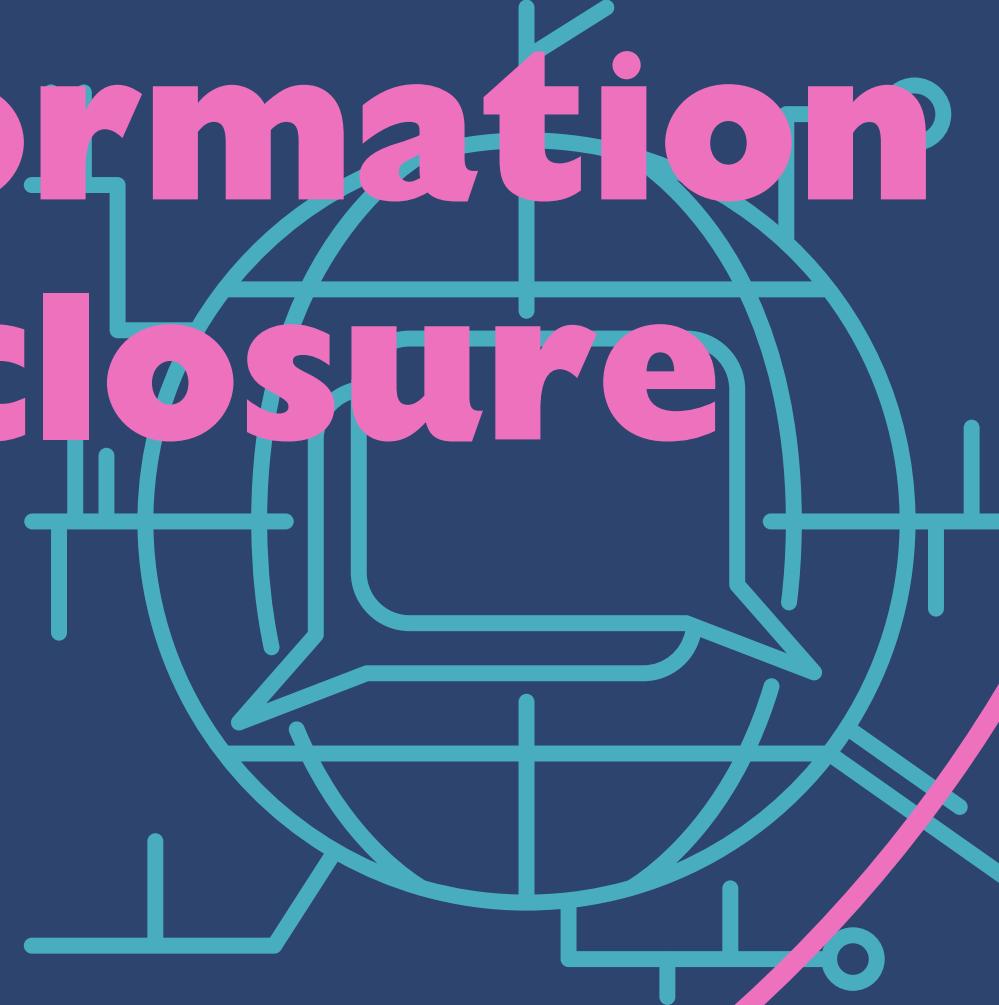
Chain FORWARD (policy ACCEPT)
target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
```

```
(kali㉿kali)-[~]
$ sudo nmap -sV -ss 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 09:57 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00055s latency).
Not shown: 982 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)
4999/tcp  open     java-rmi   Java RMI/Java Registry
5000/tcp  open     ingreslock  ingreslock
5001/tcp  open     ingreslock  ingreslock
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: 08:00:27:00:43:18 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: kernel

Service detection performed. Please report any incorrect results at https://
Nmap done: 1 IP address (1 host up) scanned in 23.40 seconds
```

NFS Exported Share Information Disclosure



DESCRIZIONE

Almeno una delle **condivisioni NFS** esportate dal server remoto potrebbe essere **montata dall'host di scansione**.

Un utente malintenzionato potrebbe essere in grado di sfruttare questa possibilità per **leggere (ed eventualmente scrivere)** i file **sull'host remoto**.

SOLUZIONE

Configurare NFS sull'host remoto in modo che **solo gli host autorizzati** possano montare le sue condivisioni remote.

Port	Hosts
2049 / udp / rpc-nfs	192.168.50.101

RISOLUZIONE

- **Identificare condivisione NFS**
Identifico la condivisione NFS
vulnerabile con **sudo nmap**
--script=nfs* 192.168.50.101 -sV -sS -p 111,2049.

- **Risolvere la vulnerabilità**
Per risolvere la vulnerabilità, ho
configurato NFS modificando il file
/etc(exports per restringere i
permessi di accesso solo agli host
autorizzati della rete
192.168.50.0/24.

```
(kali㉿kali)-[~]
$ sudo nmap --script=nfs* 192.168.50.101 -sV -sS -p 111,2049
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-29 07:40 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
111/tcp    open  rpcbind 2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp  nfs
|   100005  1,2,3     40083/tcp  mountd
|   100005  1,2,3     50491/udp mountd
|   100021  1,3,4     34805/udp nlockmgr
|   100021  1,3,4     39118/tcp  nlockmgr
|   100024  1          40599/tcp  status
|_  100024  1          40599/udp status

nfs-showmount:
|_ / *          2024-06-29T13:53:04

Filesystem  1K-blocks  Used   Available  Use%  Maxfilesize  Maxlink
|_ /          7282168.0 1500996.0 5414172.0 22%    2.0T        32000
nfs-ls: Volume /
|_ access: Read Lookup Modify Extend Delete NoExecute
|_ PERMISSION  UID  GID  SIZE  TIME      FILENAME
|_ drwxr-xr-x  0    0    4096  2012-05-14T03:35:33 bin
|_ drwxr-xr-x  0    0    4096  2010-04-16T06:16:02 home
|_ drwxr-xr-x  0    0    4096  2010-03-16T22:57:40 initrd
|_ lrwxrwxrwx  0    0    32   2010-04-28T20:26:18 initrd.img
|_ drwxr-xr-x  0    0    4096  2012-05-14T03:35:22 lib
|_ drwx-----  0    0   16384  2010-03-16T22:55:15 lost+found
|_ drwxr-xr-x  0    0    4096  2010-03-16T22:55:52 media
|_ drwxr-xr-x  0    0    4096  2010-04-28T20:16:56 mnt
|_ drwxr-xr-x  0    0    4096  2012-05-14T01:54:53 sbin
|_ drwxr-xr-x  0    0    4096  2010-04-28T04:06:37 usr

# /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)
#
# 192.168.50.0/24(rw,sync,no_root_squash,no_subtree_check)
```

VNC Server 'password' Password



DESCRIZIONE

Il **server VNC** in esecuzione sull'host remoto è protetto da una **password debole**. Nessus è stato in grado di effettuare il login utilizzando l'autenticazione VNC e una **password "password"**. Un aggressore remoto non autenticato potrebbe sfruttare questa situazione per **prendere il controllo del sistema**.

SOLUZIONE

Proteggere il servizio VNC con una **password forte**.

Port ▲	Hosts
5900 / tcp / vnc	192.168.50.101

RISOLUZIONE

• Modificare la password

Ho utilizzato il comando vncpasswd per impostare una nuova **password più forte**, ovvero: “**nm4`18VA**”.

Successivamente mi è stato chiesto se volessi impostare una password per la sola visualizzazione, e ho risposto no per garantire che la password permetta accesso e controllo completo.

Nessun messaggio di errore è stato mandato a schermo, dunque sappiamo che la **password è stata modificata con successo**.

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



Scansione di verifica

Al termine di tutte le remediation actions ho provato di nuovo lo **Scan con Nessus**, con le medesime impostazioni dello scan iniziale.

Come si vede nell'immagine, le **vulnerabilità** su cui abbiamo effettuato mitigazione **non sono più presenti nel report**, e dunque la loro **risoluzione** è risultata **efficace**.

