

In questo secondo documento descriverò i passaggi di remediation per le vulnerabilità critiche identificate nel sistema Metasploitable. Inizierò con le prime tre vulnerabilità obbligatorie, seguite da altre due scelte tra le vulnerabilità critiche identificate. Per ciascuna vulnerabilità, includerò screenshot e una spiegazione dettagliata dei passaggi intrapresi per mitigare il rischio.

Remediation per la Vulnerabilità NFS Exported Share Information Disclosure

Metodo 1: ha come obiettivo quello di limitare l'accesso alle condivisioni NFS solo agli host autorizzati, riducendo il rischio di accesso non autorizzato ai dati.

In questo contesto lavorerò sull'indirizzo IP del server su cui sto eseguendo il servizio NFS, e che corrisponde all'IP della Metasploitable. (IP: 192.168.50.101).

Eseguo il comando `showmount -e 192.168.50.101` e come risultato mostra che attualmente c'è una condivisione NFS esportata a tutti gli host, e possiamo vederlo dal *. Ciò significa che ogni host può montare la condivisione NFS.

```
msfadmin@metasploitable:~$ showmount -e 192.168.50.101
Export list for 192.168.50.101:
/ *
msfadmin@metasploitable:~$
```

Ora vado a modificare il file di configurazione NFS, chiamato 'exports'. Questo file definisce quali directory sono esportate e quali host sono autorizzati ad accedervi. Il comando è `sudo nano /etc/exports`.

File prima della modifica:

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

[Read 12 lines]

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

File dopo la modifica:

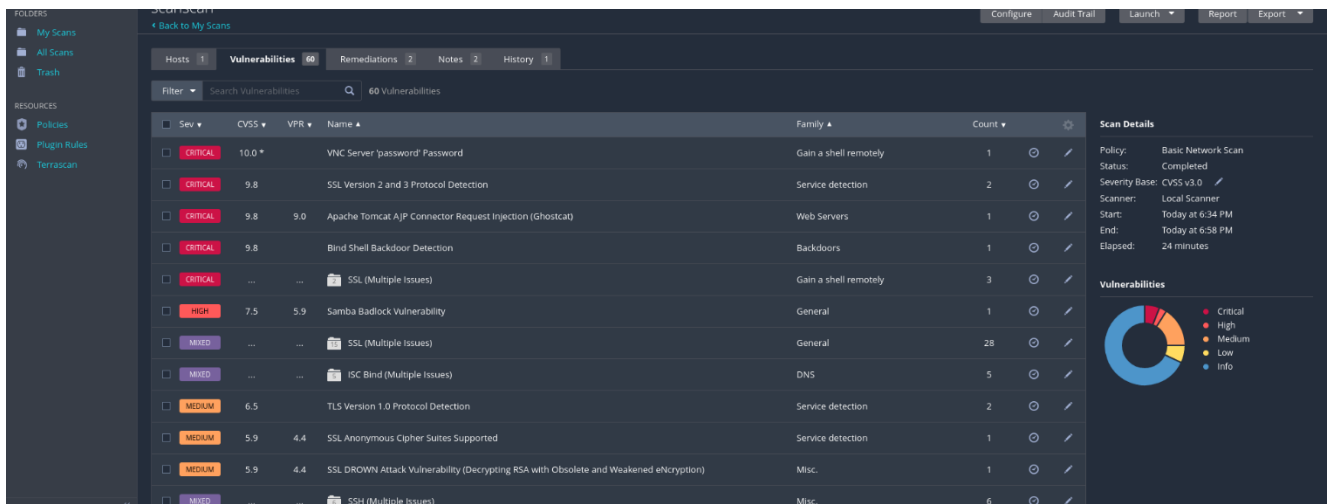
```
GNU nano 2.0.7      File: /etc/exports      Modified
# /etc/exports: the access control list for filesystems which may be exported
#                 to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
/      192.168.50.101(rw,sync,no_root_squash,no_subtree_check)

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

Riavvio il servizio NFS

```
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server restart
* Stopping NFS kernel daemon [ OK ]
* Unexporting directories for NFS kernel daemon... [ OK ]
* Exporting directories for NFS kernel daemon... [ OK ]
* Starting NFS kernel daemon [ OK ]
msfadmin@metasploitable:~$ showmount -e 192.168.50.101
Export list for 192.168.50.101:
/ 192.168.50.101
msfadmin@metasploitable:~$
```

E poi faccio una prova facendo una nuova scansione con Nessun. Come si può vedere dallo screenshot, la remediation ha funzionato, in quanto lo scan non rileva più la criticità.



Un secondo metodo che si può adottare è quello di disabilitare il servizio completamente. Non è preferibile in quanto a volte il servizio potrebbe essere necessario per il corretto funzionamento di altre applicazioni o altri servizi.

Comunque, da terminale si procede con il comando sudo /etc/init.d/nfs-kernel-server stop e il servizio verrà arrestato correttamente e senza errori. Per essere sicuri di verifica che esso non sia più in esecuzione con sudo /etc/init.d/nfs-kernel-server status e ci apparirà che * nfs-kernel-server is not running.

Remediation per la Vulnerabilità VNC Server 'password' Password

Metodo 1: cambiare la password del server VNC con una più sicura

```
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:~$
```

Siccome il file che contiene la password è crittografato, uso il comando ls -l ~/.vnc/passwd e l'output mostrerà la data e l'ora in cui il file 'passwd' è stato modificato l'ultima volta. In questo caso corrisponderà proprio al cambio della password.

```
GNU nano 2.0.7      File: /home/msfadmin/.vnc/passwd
^KSJ♦♦♦♦r^KSJ♦♦♦♦r

[ Read 1 line ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell

msfadmin@metasploitable:~$ ls -l ~/.vnc/passwd
-rw----- 1 msfadmin msfadmin 16 2024-07-27 13:40 /home/msfadmin/.vnc/passwd
msfadmin@metasploitable:~$ _
```

È importante ricordarsi di ‘killare’ tutti i processi già attivi che utilizzavano la vecchia password e quindi, ad uno scan di Nessus, potevano far risultare la vulnerabilità, anche se, nell’effettivo, la password è stata cambiata, e, infine, fare reboot.

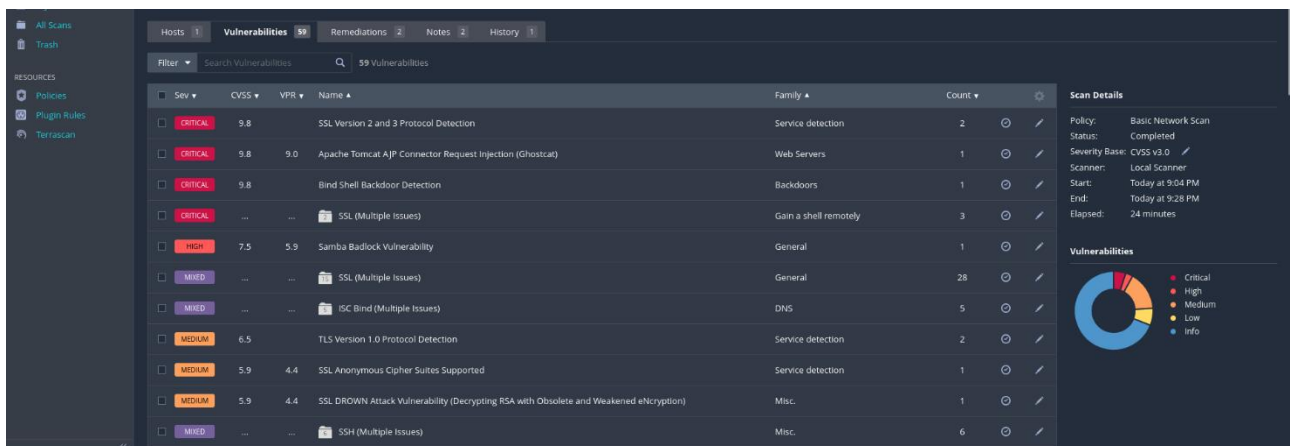
```
fbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fonts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/share/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co /etc/X11/rgb
root      4677  0.0  0.0   2724  1188 ?        S    13:58   0:00 /bin/sh /root/.vnc/xstartup
msfadmin  8782  0.0  0.0   3004   752 tty1    R+   15:01   0:00 grep vnc
msfadmin@metasploitable:~$ kill -9 4673
-bash: kill: (4673) - Operation not permitted
msfadmin@metasploitable:~$ sudo kill -9 4673
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo kill -9 4677
msfadmin@metasploitable:~$ ps aux | grep vnc
msfadmin  8853  0.0  0.0   3004   748 tty1    R+   15:03   0:00 grep vnc
msfadmin@metasploitable:~$ vncserver :1

New 'X' desktop is metasploitable:1

Starting applications specified in /home/msfadmin/.vnc/xstartup
Log file is /home/msfadmin/.vnc/metasploitable:1.log

msfadmin@metasploitable:~$ ls -l ~/.vnc/passwd
-rw----- 1 msfadmin msfadmin 16 2024-07-27 14:46 /home/msfadmin/.vnc/passwd
msfadmin@metasploitable:~$
```

Eseguo una scansione e la vulnerabilità non viene più rilevata.



Remediation per la Vulnerabilità Bind Shell Backdoor Detection

La presenza di una bind shell backdoor indica che il sistema potrebbe essere compromesso e che un attaccante ha installato un meccanismo per ottenere l'accesso remoto al sistema. È essenziale rimuovere la bind shell, rafforzare le configurazioni di sicurezza e monitorare il sistema.

Metodo 1: identificare e rimuovere la Bind Shell

Utilizzo il comando nmap su terminale Kali per eseguire una scansione completa delle porte aperte sulla macchina Metasploitable. L'output mi mostrerà tutte le porte e i relativi servizi associati, così potrò identificare le porte 'sospette' che non corrispondono a servizi legittimi.

```

(root@kali)~[~]
# nmap -p 1-65535 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 21:43 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00020s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
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
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
35943/tcp open  unknown
38051/tcp open  unknown
42796/tcp open  unknown
49604/tcp open  unknown
MAC Address: 08:00:27:14:97:79 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 26.47 seconds
```

A saltare all'occhio è sicuramente la porta 1524 a cui è associato un servizio con un nome sospetto 'ingreslock' (anche nel report delle criticità è riportata la porta 1524).

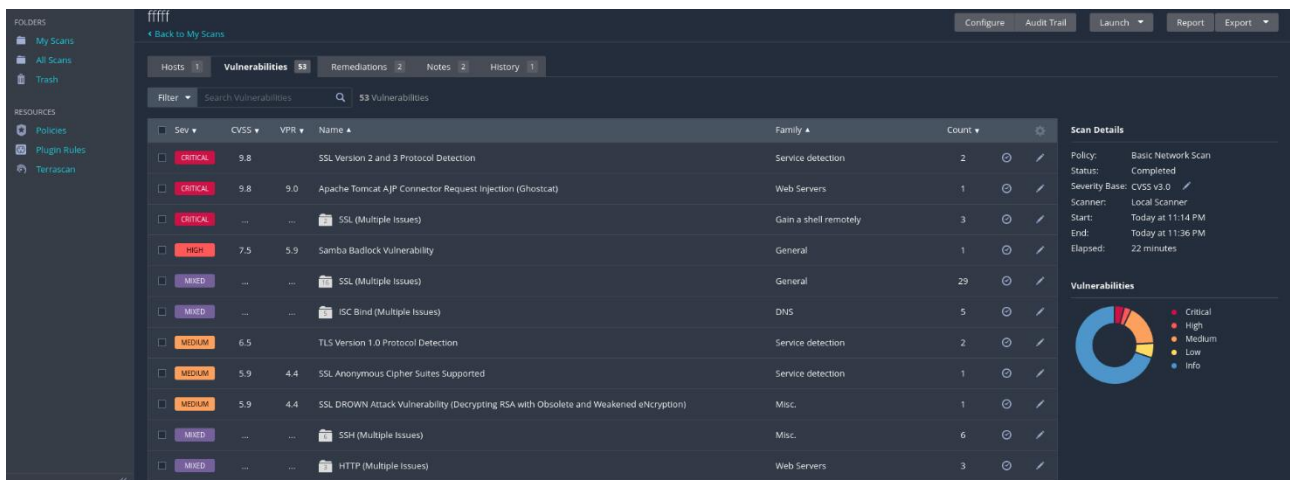
Vado sulla Metasploitable e utilizzo 'netstat' per confermare se la porta è effettivamente in ascolto.

```
msfadmin@metasploitable:~$ netstat -tulnp | grep :1524
(No info could be read for "-p": geteuid()=1000 but you should be root.)
tcp        0      0 0.0.0.0:1524        0.0.0.0:*           LISTEN
-
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep :1524
[sudo] password for msfadmin:
tcp        0      0 0.0.0.0:1524        0.0.0.0:*           LISTEN
4496/xinetd
msfadmin@metasploitable:~$
```

Questo comando, inoltre, mi darà il PID del processo e così posso procedere al kill per terminarlo

```
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep :1524
[sudo] password for msfadmin:
tcp        0      0 0.0.0.0:1524        0.0.0.0:*           LISTEN
4496/xinetd
msfadmin@metasploitable:~$ kill -9 4496
-bash: kill: (4496) - Operation not permitted
msfadmin@metasploitable:~$ sudo kill -9 4496
msfadmin@metasploitable:~$
```

Faccio una veloce scansione con Nessun per vedere se le mie considerazioni erano esatte ed effettivamente la vulnerabilità non viene più individuata e, per ulteriore conferma, rifaccio nmap da Kali



```

Nmap done: 1 IP address (1 host up) scanned in 26.47 seconds

(root@kali)-[~]
# nmap -p 1-65535 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 23:04 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0012s latency).
Not shown: 65511 closed tcp ports (reset)
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  rmiregistry
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
35943/tcp open  unknown
38051/tcp open  unknown
42796/tcp open  unknown
49604/tcp open  unknown
MAC Address: 08:00:27:14:97:79 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 30.46 seconds

(root@kali)-[~]
#

```

Adesso si deve identificare il percorso che porta all'esecuzione del processo

Uso il PID per trovare il percorso dell'eseguibile del processo sospetto e poi lo rimuovo.

```

msfadmin@metasploitable:~$ sudo netstat -tulnp | grep :1524
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN
4511/xinetd
msfadmin@metasploitable:~$ sudo ls -l /proc/4511/exe
lrwxrwxrwx 1 root root 0 2024-07-27 18:11 /proc/4511/exe -> /usr/sbin/xinetd
msfadmin@metasploitable:~$ sudo rm -f /usr/sbin/xinetd
msfadmin@metasploitable:~$

```

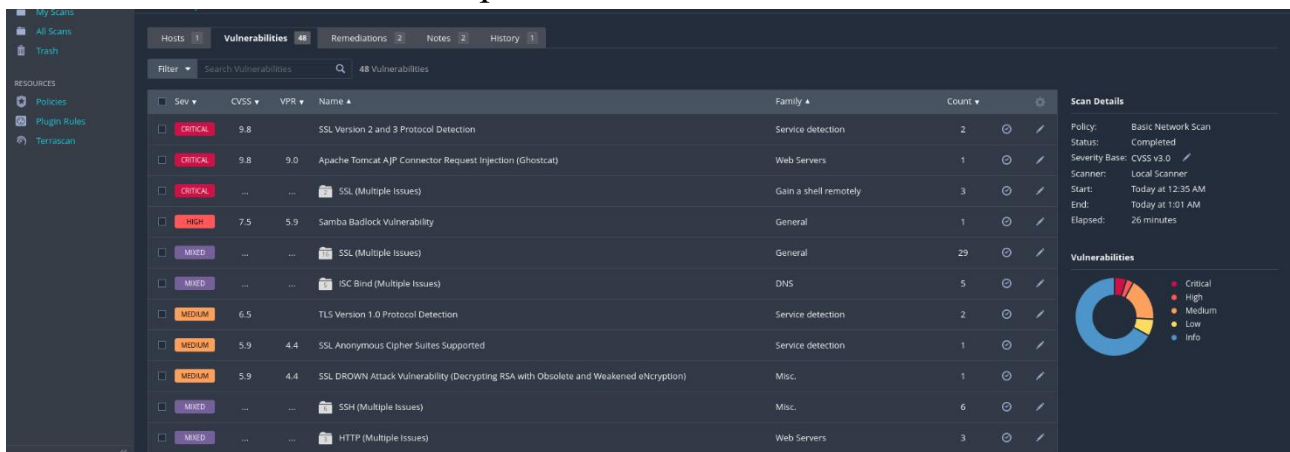
Vado nel file di avvio e commento le linee 'sospette'

```

GNU nano 2.0.7      File: /etc/rc.local
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
#
#nohup /usr/bin/rmiregistry >/dev/null 2>&1 &
#nohup /usr/bin/unrealircd &
#rm -f /root/.vnc/*.pid
#HOME=/root LOGNAME=root USER=root nohup /usr/bin/vncserver :0 >/root/.vnc.log 2&
#nohup /usr/sbin/druby_tineserver.rb &

```

Faccio un reboot per salvare le modifiche, avvio una nuova scansione su Nessus e vedo che lo scan non rileva più la vulnerabilità relativa alla backdoor.



The screenshot shows the Nessus interface with the 'Vulnerabilities' tab selected. A table lists various vulnerabilities with columns for Severity, CVSS, VPR, Name, Family, and Count. On the right, 'Scan Details' and a 'Vulnerabilities' pie chart are visible.

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1
MIXED	SSL (Multiple Issues)	General	29
MIXED	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	5.9	4.4	SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eEncryption)	Misc.	1
MIXED	SSH (Multiple Issues)	Misc.	6
MIXED	HTTP (Multiple Issues)	Web Servers	3

Altri metodi per mitigare questa vulnerabilità sono sicuramente quello di tenere sempre aggiornato il sistema e le patch di sicurezza o installare strumenti con 'lynis' o 'openvas' che eseguono scansioni delle vulnerabilità sul sistema. Inoltre, si possono anche installare dei firewall per bloccare la porta sospetta utilizzando 'iptables' e specificando, in questo caso, la porta 1524 (`sudo iptables -A INPUT -p tcp --dport 1524 -j DROP || sudo iptables -A INPUT -p udp --dport 1524 -j DROP`).

Remediation per la vulnerabilità rexecd Service Detection

Il servizio rexecd (Remote Execution Daemon) è un servizio che permette di eseguire comandi su un sistema remoto. Questo servizio, noto per le sue vulnerabilità di sicurezza, è obsoleto e non dovrebbe essere utilizzato nei sistemi moderni. Le principali vulnerabilità associate a rexecd includono la possibilità di eseguire comandi non autorizzati, mancanza di cifratura delle comunicazioni e potenziali escalation di privilegi.

Sebbene la vulnerabilità rexecd non sia stata rilevata nella scansione con Nessus della mia Metasploitable, mi sono documentata riguardo le opportune remediation che è possibile attuare, in quanto ritengo importante essere preparati per gestire questa vulnerabilità nel caso si presenti in futuro.

Sulla mia macchina ho eseguito il comando `ps aux | grep rexecd` per vedere se il servizio fosse in esecuzione ma ho verificato che non lo era.

```
msfadmin@metasploitable:~$ ps aux | grep rexecd
msfadmin  4716  0.0  0.0   3004   756 tty1    R+   10:01   0:00 grep rexecd
msfadmin@metasploitable:~$
```


Nel caso lo fosse stato, potevo procedere con ‘killare’ il processo con kill -9 PID e poi procedere con la visualizzazione e la modifica del file di configurazione, per assicurarmi che il servizio non venisse avviato ad ogni boot, con sudo nano /etc/inetd.conf e commentando le linee che potevano risultare ‘sospette’. Infine, si potevano proprio rimuovere tutti i pacchetti relativi a ‘rexecd’ se fossero presenti sul sistema con sudo apt-get remove –purge rsh-server e poi riavviare il servizio inetd dopo avere effettuato queste modifiche con sudo /etc/init.d/inetd restart.

In alternativa si può anche bloccare l’eventuale porta in cui rexecd si collega, solitamente la 512, usando iptables, ovvero usando un firewall e dando delle regole che non permettano il traffico.

Remediation Apache Tomcat AJP Connector Request Injection (Ghostcat)

Il metodo più veloce per risolvere questa criticità è quello di disabilitare il connettore APJ, ovvero la porta a cui il server si collega per funzionare, nello specifico la numero 8009. Ho adottato questo metodo in quanto voglio mantenere la mia macchina non collegata a internet e quindi non aggiornata.

Apro il file di configurazione del server con sudo nano /etc/tomcat5.5/server.xml e vado a commentare le righe che riguardano il connettore AJP

```
GNU nano 2.0.7      File: /etc/tomcat5.5/server.xml      Modified

                                noCompressionUserAgents="gozilla, 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. -->
<!--

Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
Y Yes
N No      ^C Cancel
```

Poi riavvio il server Tomcat con `sudo /etc/init.d/tomcat5.5 restart`

```
[ Wrote 384 lines ]  
msfadmin@metasploitable:~$ sudo /etc/init.d/tomcat5.5 restart  
* Stopping Tomcat servlet engine tomcat5.5 [ OK ]  
* Starting Tomcat servlet engine tomcat5.5 [ OK ]  
msfadmin@metasploitable:~$
```

Facendo nmap possiamo notare che la porta, che prima era aperta, adesso risulta chiusa

```
File Actions Edit Simple Text Editor  
(kali@kali)-[~]  
$ nmap -p 0-65535 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 16:57 CEST  
Nmap scan report for 192.168.50.101  
Host is up (0.0016s latency).  
Not shown: 65519 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  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
3632/tcp  open  distccd  
5432/tcp  open  postgresql  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
33635/tcp open  unknown  
53412/tcp open  unknown  
57535/tcp open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 23.97 seconds  
  
(kali@kali)-[~]  
$ nmap -p 0-65535 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 17:00 CEST  
Nmap scan report for 192.168.50.101  
Host is up (0.0012s latency).  
Not shown: 65521 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  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
3632/tcp  open  distccd  
5432/tcp  open  postgresql  
33635/tcp open  unknown  
53412/tcp open  unknown  
57535/tcp open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 20.53 seconds
```

Avvio la scansione con Nessun per vedere se la vulnerabilità risulta e vediamo che effettivamente è stata risolta

