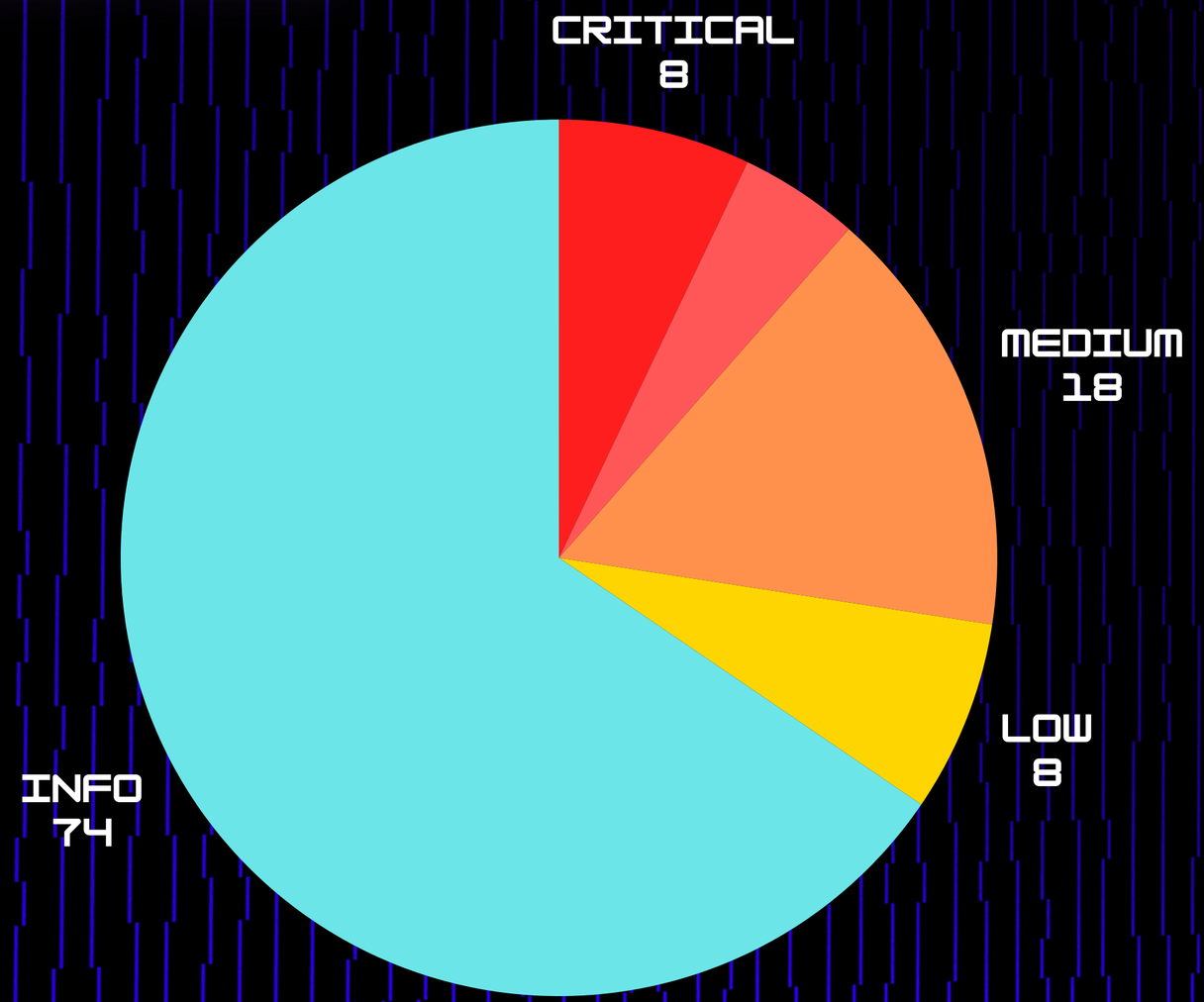
RICCARDO LEPORE

FASE REMEDIATION

SITUAZIONE INIZIALE

QUESTA E' LA SITUAZIONE INIZIALE FACENDO UNO SCAN UTILIZZANDO IL TOOL NESSUS SU TUTTE LE PORTE DELLA MACCHINA TARGET METASPLOITABLE 2



192.168.50.101

8	5	18	8	74
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 113

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

VULNERABILITA' DA FIXARE

- Apache Tomcat AJP Connector Request Injection (Ghostcat)
- Bind Shell Backdoor Detection
- NFS Exported share information disclosure
- VCN server "password" password

ANALISI INFO VULNERABILITÀ

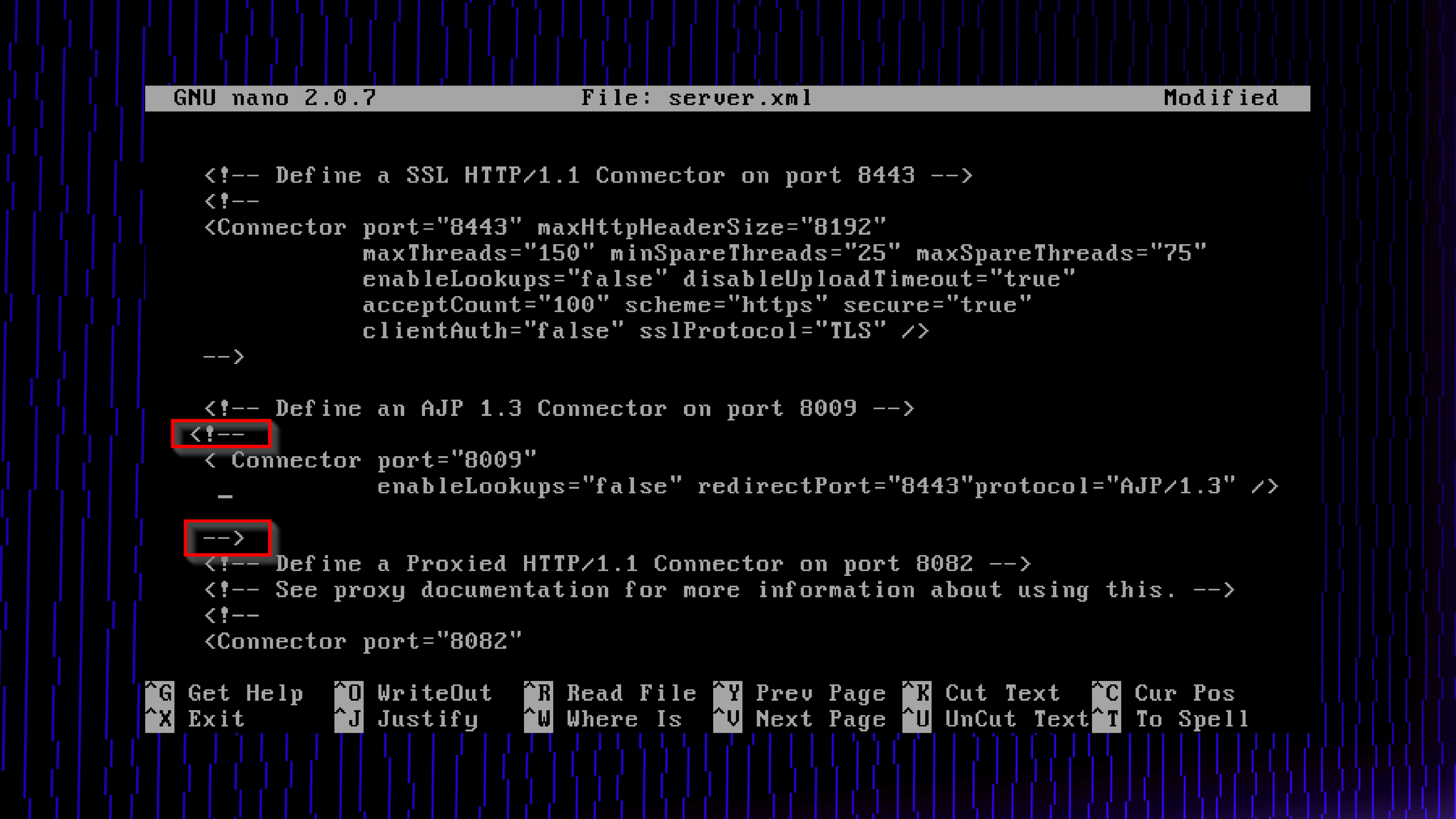
CRITICAL Apache Tomcat AJP Connector Request Injection (Ghostcat)

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.


GNU nano 2.0.7 File: server.xml Modified
<!-- 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. -->
<!--
<Connector port="8082"
^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

Sulla macchina metasploitable seguendo il percorso /etc/tomcat5.5 troviamo il file di configurazione “server.xml” se utilizziamo “ctrl+W+AJP” andiamo alle righe di configurazione del connettore in analisi.
Per evitare che un utente malintenzionato possa sfruttare questa vulnerabilità su questo connettore ho deciso di disattivarlo in modo semplice e rapido COMMENTANDO le righe della sua configurazione così da non farle eseguire

ANALISI INFO VULNERABILITÀ

CRITICAL Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Esaminando la vulnerabilità e ipotizzando che questa porta sia stata creata esclusivamente per poterla sfruttare come backdoor per potersi collegare in remoto ho ritenuto opportuno bloccare le connessioni in entrata per evitare che una persona possa sfruttare questa vulnerabilità.

Ecco quali sono stati i passaggi della remediation che ho svolto.

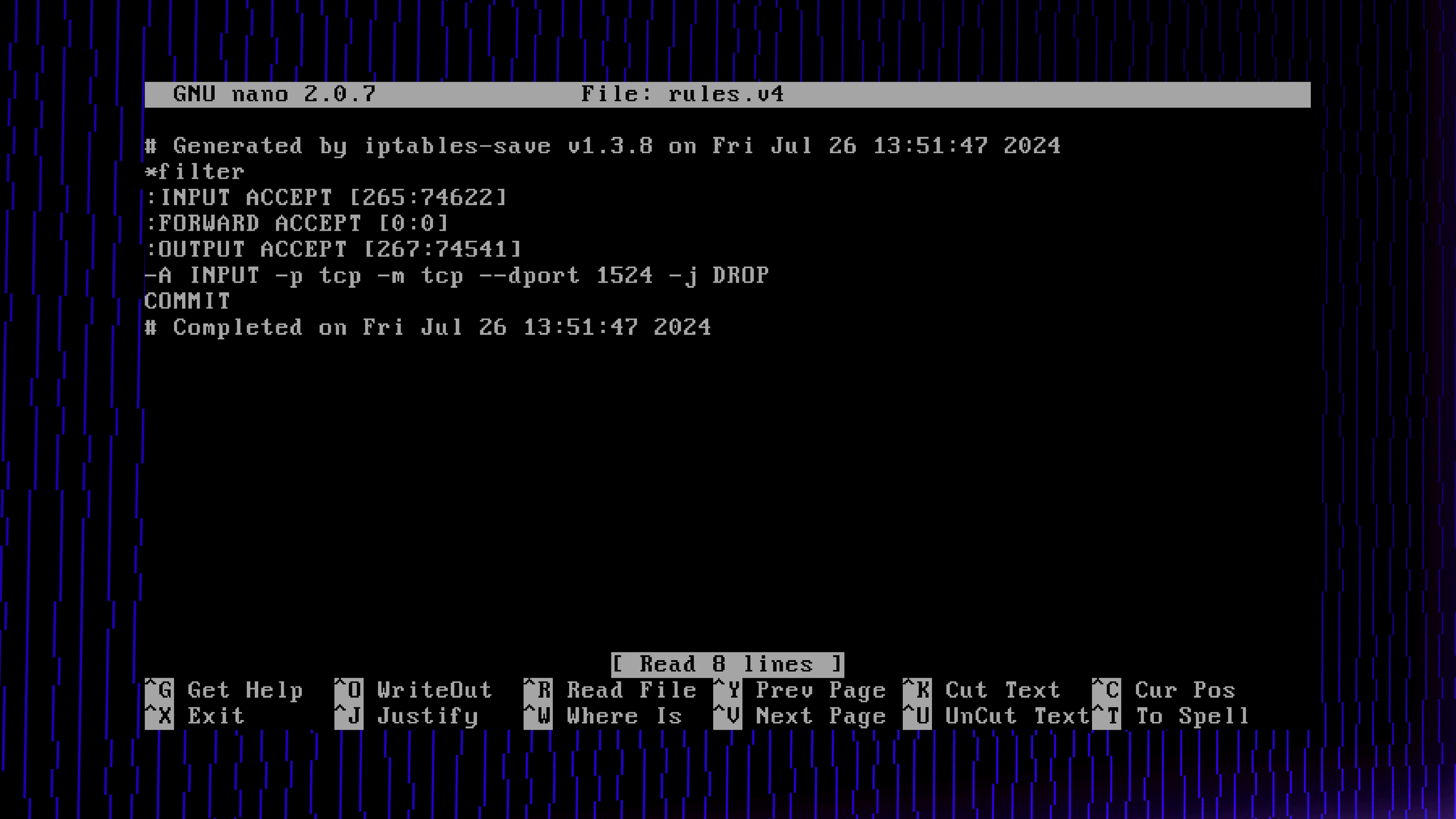
Come prima cosa ho creato una regola su "iptables" che potesse droppare i tentativi di connessione alla porta 1524 (la porta su cui è stata rilevata la vulnerabilità).

Nello specifico la regola che ho creato:

iptables -A INPUT -p tcp -m tcp --dport 1524 -j DROP

successivamente ho salvato questa regola in un file "rule.v4"

iptables-save > /etc/iptables/rules.v4


GNU nano 2.0.7 File: rules.v4
Generated by iptables-save v1.3.8 on Fri Jul 26 13:51:47 2024
*filter
:INPUT ACCEPT [265:74622]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [267:74541]
-A INPUT -p tcp -m tcp --dport 1524 -j DROP
COMMIT
Completed on Fri Jul 26 13:51:47 2024
[Read 8 lines]
^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

Dopo aver creato la regola e averla salvata ho creato uno script per far si che la mia regola si avvii all'accensione della macchina così da non dare possibilià ad un potenziale attaccante di aver tempo per poter sfruttare la vulnerabilità.

Nel percorso /etc/network/if-pre-up.d/iptables vado ad inserire lo script che permetterà di eseguire la regola di iptables all'accensione della macchina metasploitable2.

Lo script: #!/bin/sh iptables-restore < /etc/iptables/rules.v4

Successivamente faccio in modo che sia eseguibile aggiungendogli i permessi di esecuzione:

chmod +x /etc/network/if-pre-up.d/iptables

```
  GNU nano 2.0.7                File: iptables

#!/bin/sh
iptables-restore < /etc/iptables/rules.v4
```

[Read 2 lines]

^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

```
msfadmin@metasploitable:~$ sudo iptables -L -v -n
Chain INPUT (policy ACCEPT 767K packets, 83M bytes)
 pkts bytes target     prot opt in     out     source               destination

   10   464 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
       tcp dpt:1524

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 619K packets, 242M bytes)
 pkts bytes target     prot opt in     out     source               destination

msfadmin@metasploitable:~$ _
```

ANALISI INFO VULNERABILITÀ

CRITICAL NFS Exported Share Information Disclosure

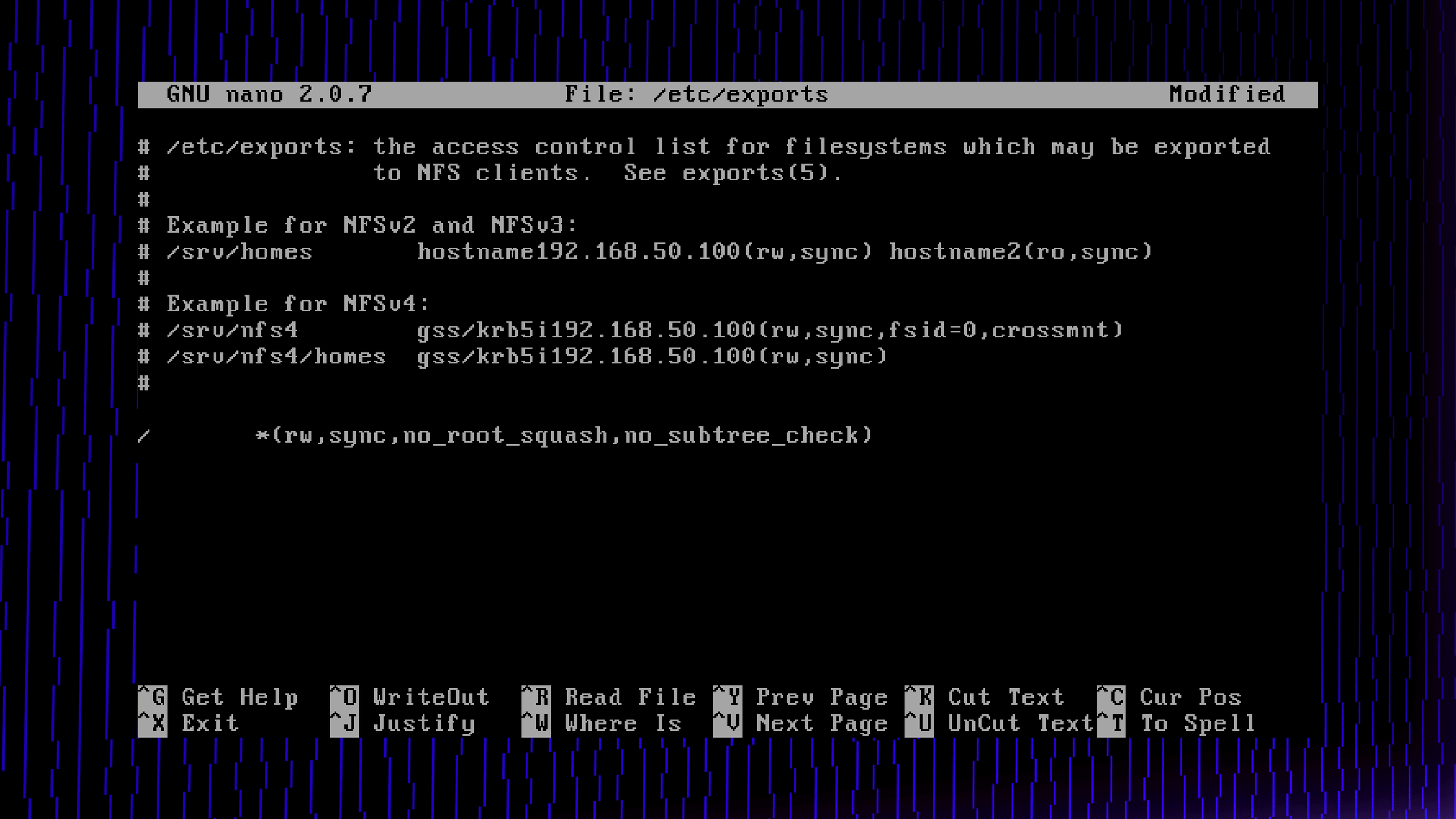
Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

LA VULNERABILITA' IN QUESTIONE PUO' ESSERE SFRUTTATA PER ACCEDERE AI FILE DI CONDIVISIONE DI METASPLOITABLE2.
PER MITIGARE QUESTA VULNERABILITA' HO SCELTO DI RENDERE DISPONIBILE LA CONDIVISIONE FILE SOLO AD UN INDIRIZZO IP (QUELLO DI KALI)


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 hostname192.168.50.100(rw,sync) hostname2(ro,sync)
#
Example for NFSv4:
/srv/nfs4 gss/krb5i192.168.50.100(rw,sync,fsid=0,crossmnt)
/srv/nfs4/homes gss/krb5i192.168.50.100(rw,sync)
#
/ *(rw,sync,no_root_squash,no_subtree_check)
^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

ANALISI INFO VULNERABILITÀ

CRITICAL VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

NESSUS HA RILEVATO QUESTA VULNERABILITA' IN QUANTO LA PASSWORD E' TROPPO DEBOLE (PASSWORD=PASSWORD) COSI' COME REMEDIATION HO DECISO DI IMPOSTARE UNA PASSWORD PIU' FORTE PER RENDERE L ACCESSO AL VNC SERVER PIU' SICURO.
PER FARLO SONO ANDATO SULLA MACCHINA METASPLOITABLE2 E CON IL COMANDO "VNCPASSWD" IMPOSTIAMO UNA NUOVA PASSWORD PIU' SICURA.
SUCCESSIVAMENTE ANDIAMO DA TERMINALE KALI LINUX E DIGITIAMO "VNCVIEWER+INDIRIZZO IP METASPLOITABLE + PORTA TARGET" E VERIFICHIAMO CHE LA PASSWORD SIA STATA CAMBIATA

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
```

```
┌──H4ckNi0-[~]
└──→vncviewer 192.168.50.101:5901
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
```

File Azioni Modifica Visualizza Aiuto

```
8009/tcp closed ajp13
MAC Address: 08:00:27:93:E5:A8 (Oracle

Nmap done: 1 IP address (1 host up) sc

┌──H4ckNi0-[~]
└──→nmap -sS  -T5 -p2049  192.168.50.
You requested a scan type which requir
QUITTING!

┌──H4ckNi0-[~]
└──→sudo nmap -sS  -T5 -p2049  192.16
[sudo] password di kali:
Starting Nmap 7.94SVN ( https://nmap.o
Nmap scan report for 192.168.50.101
Host is up (0.0014s latency).

PORT     STATE  SERVICE
2049/tcp closed nfs
MAC Address: 08:00:27:93:E5:A8 (Oracle

Nmap done: 1 IP address (1 host up) sc

┌──H4ckNi0-[~]
└──→vncviewer 192.168.50.101:5901
Connected to RFB server, using protoco
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "msfadmin's X desktop (me
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each
  True colour: max red 255 green 255 b
Using default colormap which is TrueCo
  32 bits per pixel.
  Least significant byte first in each
  True colour: max red 255 green 255 b
```

X Desktop

```
msfadmin@metasploitable:~$
```

POST REMEDIATION

192.168.50.101

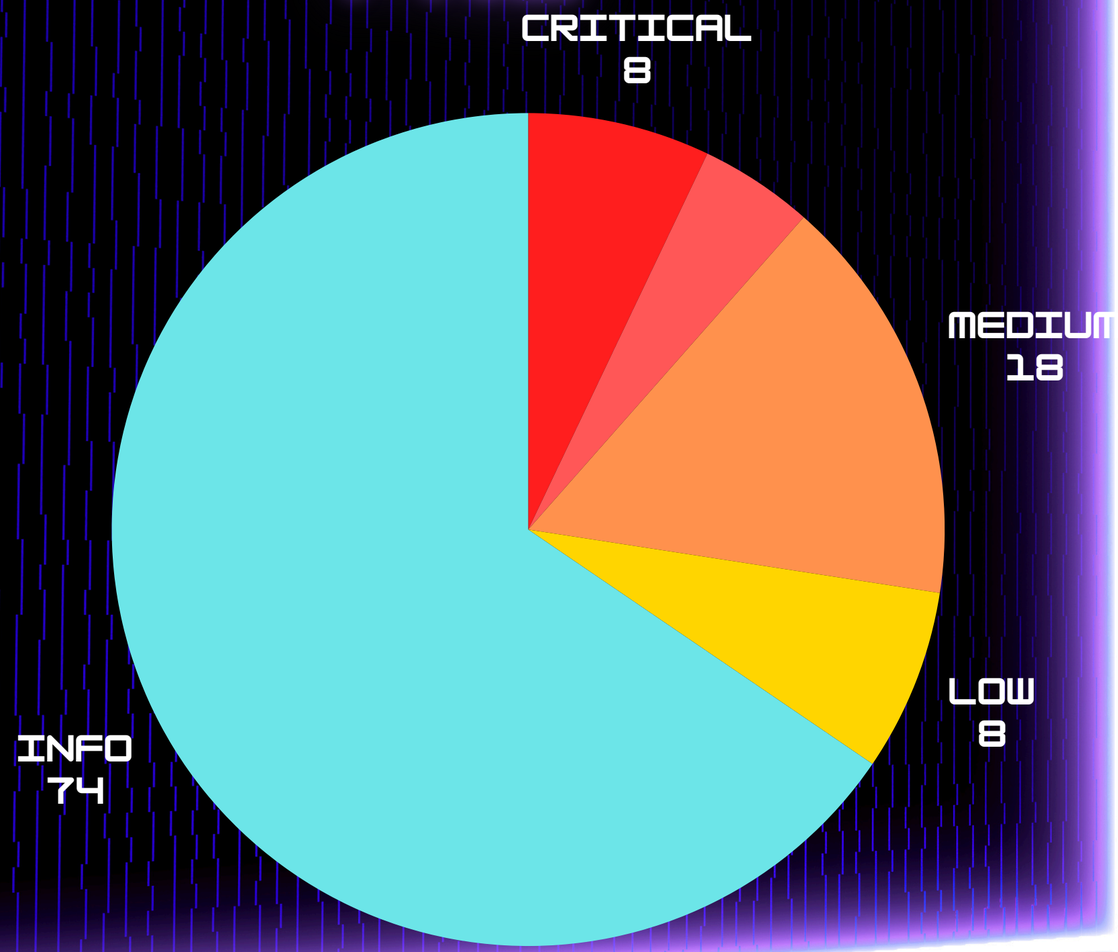
CRITICAL	HIGH	MEDIUM	LOW	INFO
4	7	30	10	89

Vulnerabilities — Total: 140

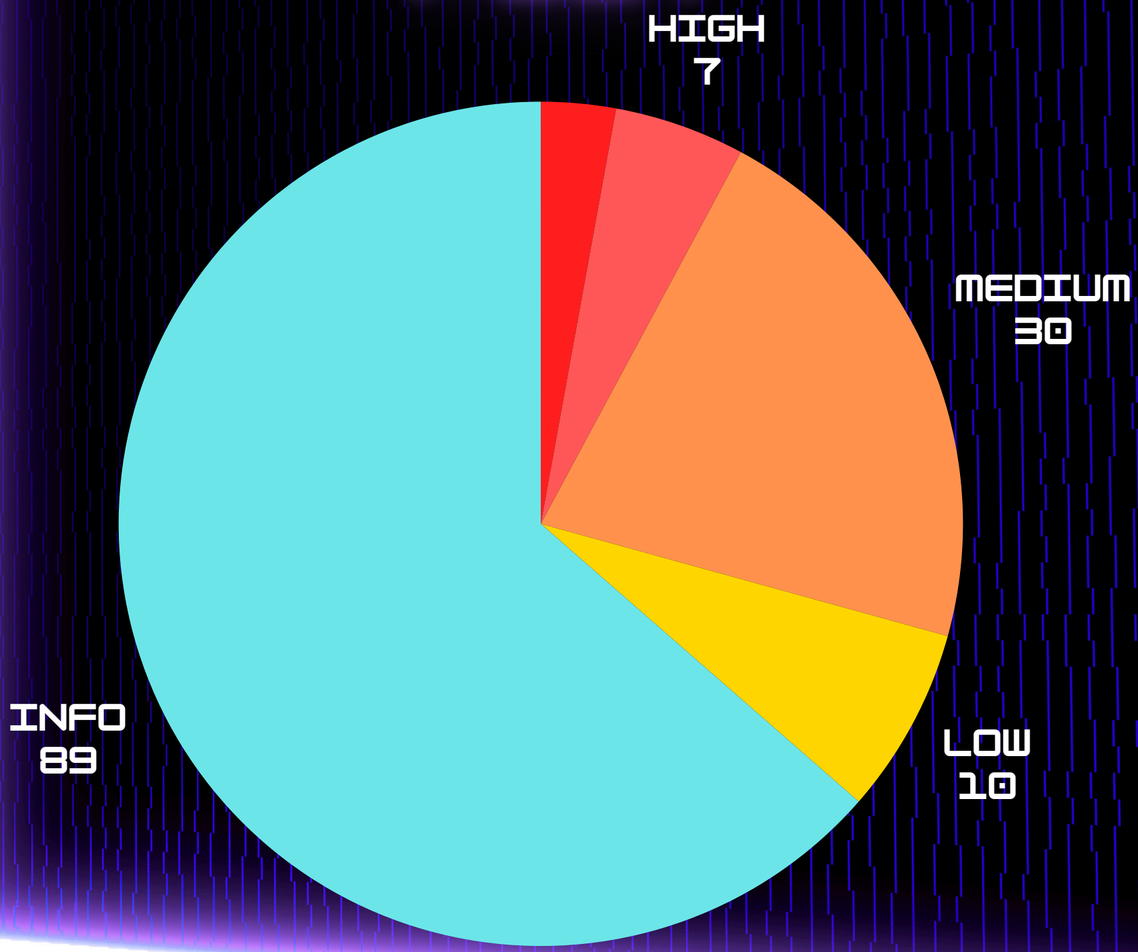
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
HIGH	8.8	7.4	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	5.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	90509	Samba Badlock Vulnerability
HIGH	7.5*	-	39469	CGI Generic Remote File Inclusion

PRE E POST REMEDIATION

PRE



POST




FINE DEL REPORT
RICCARDO LEPORE