Esercizio S5-L5

Vulnerabilities Total: 109

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	-	33850	Unix Operating System Unsupported Version Detection
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
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	5.9	10205	rlogin Service Detection
HIGH	7.5*	5.9	10245	rsh Service Detection
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted

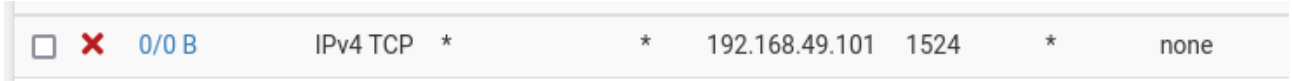
Come si può notare dall'immagine in sovrimpressione, notiamo che ci sono tante vulnerabilità critiche verso l'host target (Metasploitable) e per rimediare applicheremo delle solution messe a disposizione del tool Nessus. Cliccando su ogni criticità, Nessus ci indicherà alcune delle possibili soluzioni da utilizzare per andare a risolvere le varie vulnerabilità. Iniziamo dalla bind shell:

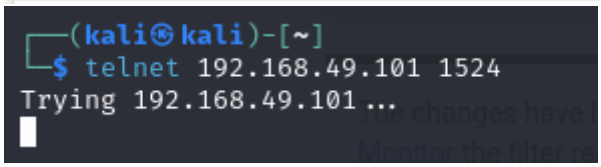
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.49.101 1524
Trying 192.168.49.101 ...
Connected to 192.168.49.101.
Escape character is '^]'.
root@metasploitable:/# whoami
root
root@metasploitable:/# root@metasploitable:/# exit
exit
Connection closed by foreign host.
```

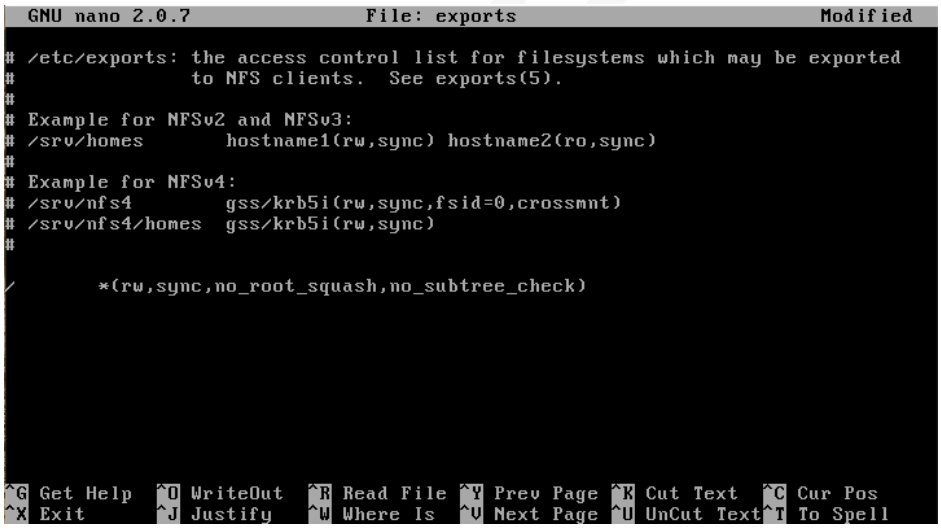
Esercizio S5-L5

Come prima cosa siamo andati a testare se la vulnerabilità fosse vera e sfruttabile a tutti gli effetti per evitare un falso positivo. Una volta verificato ciò siamo andati ad applicare la fix attraverso un firewall (pfsense) e abbiamo poi verificato che effettivamente funzionasse.



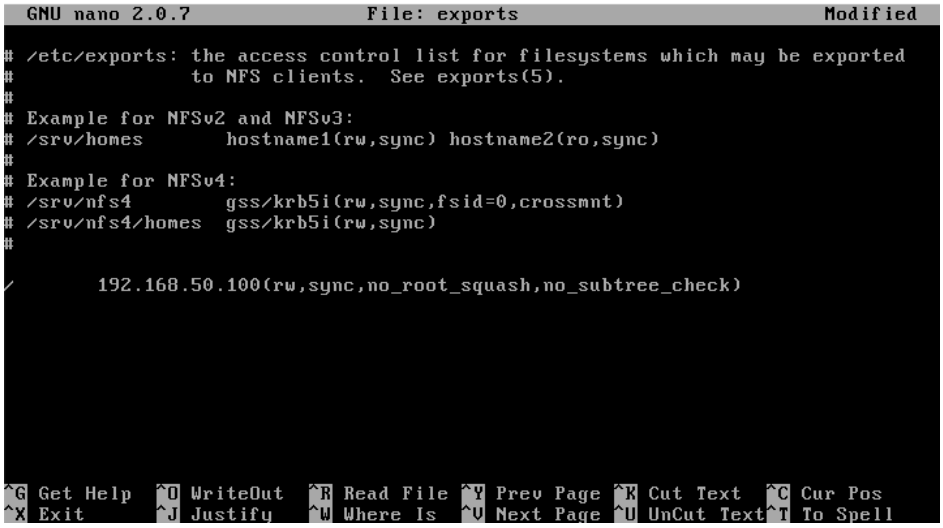


Poi abbiamo ripetuto questo passaggio anche per altre vulnerabilità. Di seguito sono elencati gli screen:



Solution

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



Esercizio S5-L5

CRITICAL	10.0*	-	61708	VNC Server 'password' Password

Solution

Secure the VNC service with a strong password.

```
msfadmin@metasploitable:/$ sudo su
root@metasploitable:/# vncserver

New 'X' desktop is metasploitable:2

Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/metasploitable:2.log

root@metasploitable:/# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? _
```

HIGH	7.5*	5.9	10205	rlogin Service Detection
HIGH	7.5*	5.9	10245	rsh Service Detection

Solution

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Solution

Comment out the 'rsh' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

```
  GNU nano 2.0.7                File: inetd.conf

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
#shell          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
#login          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
exec            stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i
```

Esercizio S5-L5

Una volta applicate le varie soluzioni, abbiamo rieffettuato uno scan verso l'host, e abbiamo notato che le vulnerabilità a cui sono state applicate le soluzioni proposte, non risultano più presenti nel report finale.

Vulnerabilities Total: 95

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
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	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

Fonti utilizzate per le varie soluzioni non esplicite:
NFS FIX: https://www.html.it/pag/66986/configurare-nfs/

VNC FIX: https://linuxconfig.org/how-to-change-vnc-password-on-linux

Backdoor fix: Firewall (pfsense)