

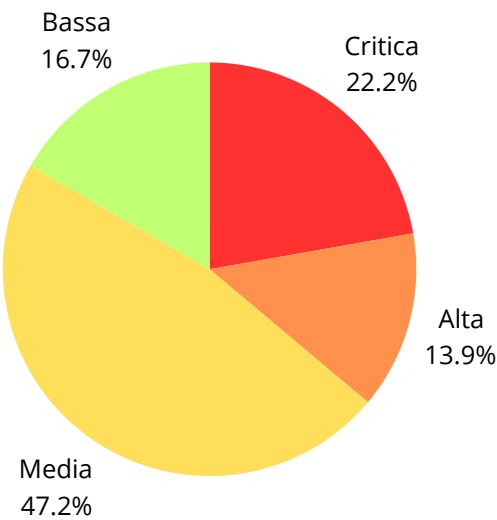
Vulnerability Assessment - Metasploitable

1) Descrizione

L'obiettivo di questa Vulnerability Scan è identificare quante e quali sono le vulnerabilità sulla macchina Metasploitable, tramite l'utilizzo del tool Nessus (versione 10.7.2).

Dalla scansione è emerso un totale di **53** vulnerabilità; come possiamo notare dalla tabella (ricavata dal report automatico di Nessus), le vulnerabilità hanno diversi livelli di gravità.

Gravità della vulnerabilità	Numero
Critica	12
Alta	7
Media	26
Bassa	8



2) Vulnerabilità riscontrate

Possiamo vedere dai risultati dell'analisi di Nessus quali sono le vulnerabilità riscontrate. In questo caso prenderemo in esame solo le vulnerabilità critiche, che hanno una valutazione CVSS compresa fra 9.0 e 10.0 (il voto è da 1 a 10, dove 10 è il grado massimo di gravità della vulnerabilità).

Meta Start / 192.168.178.100

< Back to Hosts

Configure Audit Trail Launch Report Export

Vulnerabilities 70

Filter Search Vulnerabilities 70 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclos...	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Ve...	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5 *	5.9	rlogin Service Detection	Service detection	1
HIGH	7.5 *	5.9	rsh Service Detection	Service detection	1

Host Details

IP: 192.168.178.100
MAC: 08:00:27:2A:34:2B
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 12:55 PM
End: Today at 1:15 PM
Elapsed: 19 minutes
KB: [Download](#)

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

- **Versione del sistema operativo Unix non supportata**

La versione di Unix installata è datata: il che indica che non riceverà più supporto dagli sviluppatori riguardo alle patch di sicurezza, che andrebbero ad agire su eventuali falle del sistema.

- **La password del server VLC è "password"**

Come scritto nella descrizione, la password è troppo debole e scontata, facilmente trovabile sia con che senza un BruteForce.

- **Una shell con permessi di root è in ascolto sulla porta TCP 1524**

Questa shell crea una backdoor che permette di eseguire comandi sulla macchina con permessi di amministratore.

- **Il Network File System condivide l'accesso a tutte le cartelle e file contenuti nell'host**

NFS è un protocollo che permette di condividere cartelle e file attraverso la rete su sistemi operativi differenti. Se è malconfigurato, potrebbe fornire a un attaccante la possibilità di leggere, eseguire o scrivere file nell'host vittima.

- **Il server UnrealIRCd contiene una backdoor con permessi di root sulla porta TCP 6667**

Questa backdoor permette di eseguire codice malevolo sulla macchina presa in esame.

- **Il server Apache cripta il traffico con protocolli di cifratura che hanno delle vulnerabilità note (SSL 2.0 e SSL 3.0)**

I protocolli SSL 2.0 e SSL 3.0 usano degli algoritmi di cifratura obsoleti comparati agli standard più moderni. Questo li rende suscettibili ad attacchi BruteForce e Decryption da attaccanti con sufficiente potenza computazionale.

- **Il connector AJP è in ascolto sulla porta TCP 8009**

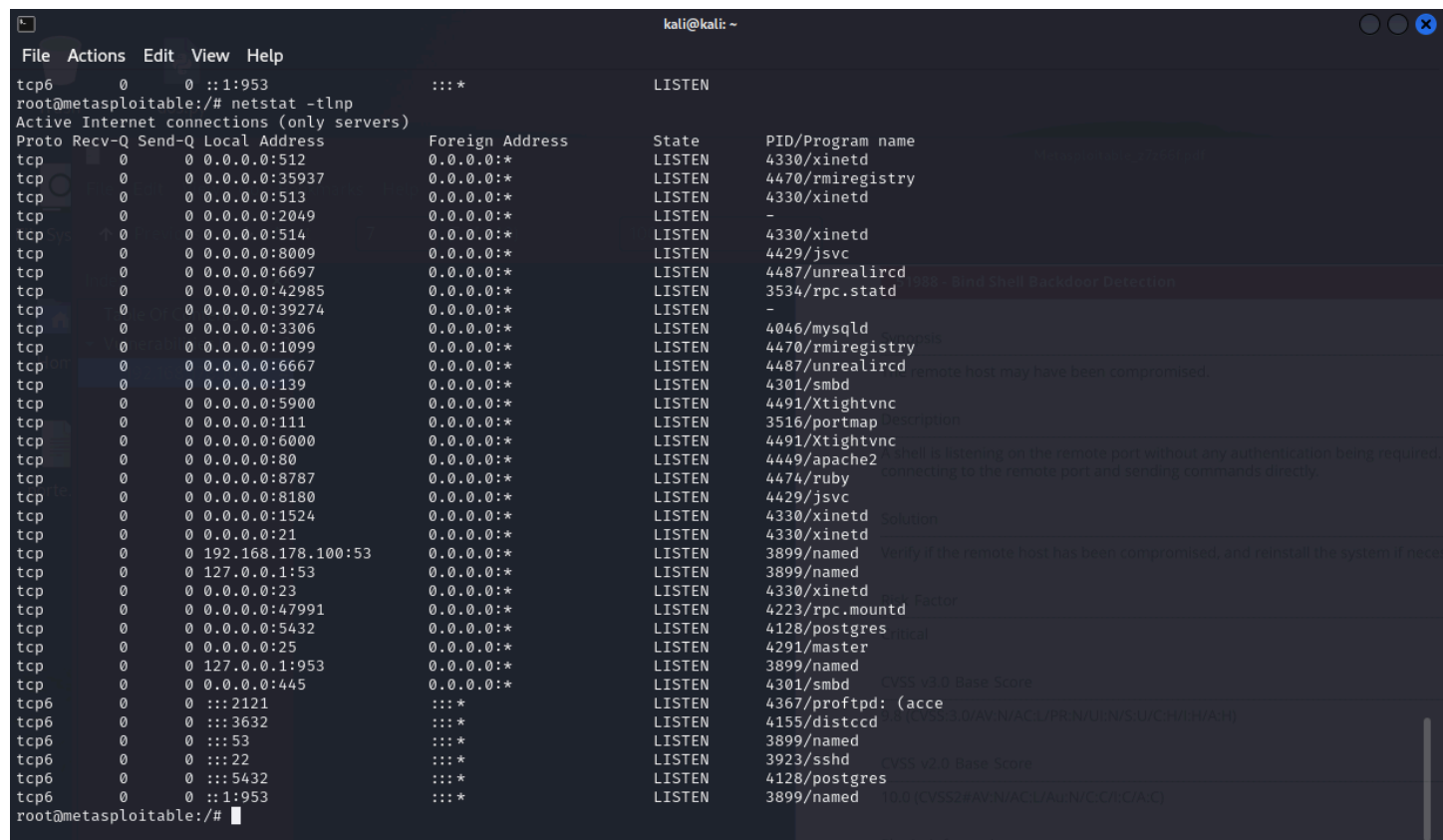
I file sul connector AJP del server Tomcat sono leggibili senza autenticazione.

3) Remediation

Di seguito le 4 vulnerabilità scelte a cui applicare una remediation e il relativo procedimento.

- **Shell in ascolto sulla porta TCP 1524**

Per eliminare la backdoor sulla porta TCP 1524, cominciamo a identificare il PID e il nome del servizio a cui è associata quella porta, tramite il comando **netstat -tlnp**. Come vediamo dall'immagine, il servizio in questione è nominato **xinetd** con PID 4330. Eseguiremo il comando da Kali Linux andando effettivamente a prendere il controllo di Metasploitable tramite la backdoor in questione per comodità di utilizzo, con il comando **nc <ip di Metasploitable> 1524**



```
kali@kali: ~  
File Actions Edit View Help  
tcp6 0 0 :::1953 :::* LISTEN  
root@metasploitable:/# netstat -tlnp  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name  
tcp 0 0 0.0.0.0:512 0.0.0.0:* LISTEN 4330/xinetd  
tcp 0 0 0.0.0.0:35937 0.0.0.0:* LISTEN 4470/rmiregistry  
tcp 0 0 0.0.0.0:513 0.0.0.0:* LISTEN 4330/xinetd  
tcp 0 0 0.0.0.0:2049 0.0.0.0:* LISTEN -  
tcp 0 0 0.0.0.0:514 0.0.0.0:* LISTEN 4330/xinetd  
tcp 0 0 0.0.0.0:8009 0.0.0.0:* LISTEN 4429/jsvc  
tcp 0 0 0.0.0.0:6697 0.0.0.0:* LISTEN 4487/unrealircd  
tcp 0 0 0.0.0.0:42985 0.0.0.0:* LISTEN 3534/rpc.statd  
tcp 0 0 0.0.0.0:39274 0.0.0.0:* LISTEN -  
tcp 0 0 0.0.0.0:3306 0.0.0.0:* LISTEN 4046/mysqld  
tcp 0 0 0.0.0.0:1099 0.0.0.0:* LISTEN 4470/rmiregistry  
tcp 0 0 0.0.0.0:6667 0.0.0.0:* LISTEN 4487/unrealircd  
tcp 0 0 0.0.0.0:139 0.0.0.0:* LISTEN 4301/smbd  
tcp 0 0 0.0.0.0:5900 0.0.0.0:* LISTEN 4491/Xtightvnc  
tcp 0 0 0.0.0.0:111 0.0.0.0:* LISTEN 3516/portmap  
tcp 0 0 0.0.0.0:6000 0.0.0.0:* LISTEN 4491/Xtightvnc  
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN 4449/apache2  
tcp 0 0 0.0.0.0:8787 0.0.0.0:* LISTEN 4474/ruby  
tcp 0 0 0.0.0.0:8180 0.0.0.0:* LISTEN 4429/jsvc  
tcp 0 0 0.0.0.0:1524 0.0.0.0:* LISTEN 4330/xinetd  
tcp 0 0 0.0.0.0:21 0.0.0.0:* LISTEN 4330/xinetd  
tcp 0 0 192.168.178.100:53 0.0.0.0:* LISTEN 3899/named  
tcp 0 0 127.0.0.1:53 0.0.0.0:* LISTEN 3899/named  
tcp 0 0 0.0.0.0:23 0.0.0.0:* LISTEN 4330/xinetd  
tcp 0 0 0.0.0.0:47991 0.0.0.0:* LISTEN 4223/rpc.mountd  
tcp 0 0 0.0.0.0:5432 0.0.0.0:* LISTEN 4128/postgres  
tcp 0 0 0.0.0.0:25 0.0.0.0:* LISTEN 4291/master  
tcp 0 0 127.0.0.1:953 0.0.0.0:* LISTEN 3899/named  
tcp 0 0 0.0.0.0:445 0.0.0.0:* LISTEN 4301/smbd  
tcp6 0 0 :::2121 :::* LISTEN  
tcp6 0 0 :::3632 :::* LISTEN  
tcp6 0 0 :::53 :::* LISTEN  
tcp6 0 0 :::22 :::* LISTEN  
tcp6 0 0 :::5432 :::* LISTEN  
tcp6 0 0 :::1953 :::* LISTEN  
root@metasploitable:/#
```

Per terminare il servizio permanentemente non basta effettuare un normale **kill**, ma dobbiamo usare il comando **sudo update-rc.d -f xinetd remove**, altrimenti al prossimo avvio della macchina il servizio sarebbe di nuovo attivo. Come vediamo, eseguendo di nuovo il comando per controllare Metasploitable, esce scritto "connessione rifiutata".

```

root@metasploitable:/# sudo systemctl disable xinetd
sudo: systemctl: command not found
root@metasploitable:/# sudo update-rc.d -f xinetd remove
Removing any system startup links for /etc/init.d/xinetd ...
/etc/rc0.d/K20xinetd
/etc/rc1.d/K20xinetd
/etc/rc2.d/S20xinetd
/etc/rc3.d/S20xinetd
/etc/rc4.d/S20xinetd
/etc/rc5.d/S20xinetd
/etc/rc6.d/K20xinetd
root@metasploitable:/# ^C

```

```

(kali㉿kali)-[~]
$ netcat 192.168.178.100 1524
root@metasploitable:/# ^C

```

```

(kali㉿kali)-[~]
$ netcat 192.168.178.100 1524
(UNKNOWN) [192.168.178.100] 1524 (ingreslock) : Connection refused

```

```

(kali㉿kali)-[~]
$

```

Anche rilanciando il comando per vedere la lista dei processi attivi vediamo che il servizio xinetd non è più in esecuzione sulla porta TCP 1524.

```

root@metasploitable:/# netstat -tlnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:35937          0.0.0.0:*               LISTEN      4470/rmiregistry
tcp        0      0 0.0.0.0:2049          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8009          0.0.0.0:*               LISTEN      4429/jsvc
tcp        0      0 0.0.0.0:6697          0.0.0.0:*               LISTEN      4487/unrealircd
tcp        0      0 0.0.0.0:42985         0.0.0.0:*               LISTEN      3534/rpc.statd
tcp        0      0 0.0.0.0:39274         0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:3306          0.0.0.0:*               LISTEN      4046/mysqld
tcp        0      0 0.0.0.0:1099          0.0.0.0:*               LISTEN      4470/rmiregistry
tcp        0      0 0.0.0.0:6667          0.0.0.0:*               LISTEN      4487/unrealircd
tcp        0      0 0.0.0.0:139           0.0.0.0:*               LISTEN      4301/smbd
tcp        0      0 0.0.0.0:5900          0.0.0.0:*               LISTEN      4491/Xtightvnc
tcp        0      0 0.0.0.0:111           0.0.0.0:*               LISTEN      3516/portmap
tcp        0      0 0.0.0.0:6000          0.0.0.0:*               LISTEN      4491/Xtightvnc
tcp        0      0 0.0.0.0:80            0.0.0.0:*               LISTEN      4449/apache2
tcp        0      0 0.0.0.0:8787          0.0.0.0:*               LISTEN      4474/ruby
tcp        0      0 0.0.0.0:8180          0.0.0.0:*               LISTEN      4429/jsvc
tcp        0      0 0.0.0.0:192.168.178.100:53 0.0.0.0:*               LISTEN      3899/named
tcp        0      0 0.0.0.0:127.0.0.1:53   0.0.0.0:*               LISTEN      3899/named
tcp        0      0 0.0.0.0:47991         0.0.0.0:*               LISTEN      4223/rpc.mountd
tcp        0      0 0.0.0.0:5432          0.0.0.0:*               LISTEN      4128/postgres
tcp        0      0 0.0.0.0:25            0.0.0.0:*               LISTEN      4291/master
tcp        0      0 0.0.0.0:127.0.0.1:953   0.0.0.0:*               LISTEN      3899/named
tcp        0      0 0.0.0.0:445          0.0.0.0:*               LISTEN      4301/smbd
tcp6       0      0 :::2121              :::*                   LISTEN      4367/proftpd: (acce
tcp6       0      0 :::3632              :::*                   LISTEN      4155/distccd
tcp6       0      0 :::53                :::*                   LISTEN      3899/named
tcp6       0      0 :::22                :::*                   LISTEN      3923/ssh
tcp6       0      0 :::5432              :::*                   LISTEN      4128/postgres
tcp6       0      0 :::1:953             :::*                   LISTEN      3899/named
root@metasploitable:/#

```

- La password del server VNC è "password"

Per risolvere questa vulnerabilità, eseguiamo su Metasploitable il comando **vncpasswd** per inserirne una nuova che non sia individuabile troppo facilmente da un BruteForce.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
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:~$ _
```

- Il Connector AJP è in ascolto sulla porta TCP 8009

Per risolvere questo problema, dobbiamo modificare la configurazione di ACP per far sì che richieda un'autenticazione per essere usato. Accediamo al file `/var/lib/tomcat5.5/conf/server.xml` e inseriamo sulla Connector Port 8009 le opzioni **secretRequired="true"** e **secret="Mnbv12#"**

```
msfadmin@metasploitable:~$ cd /var/lib/tomcat5.5
msfadmin@metasploitable:/var/lib/tomcat5.5$ ls
conf logs shared temp webapps work
msfadmin@metasploitable:/var/lib/tomcat5.5$ cd conf
msfadmin@metasploitable:/var/lib/tomcat5.5/conf$ ls
Catalina context.xml server-minimal.xml tomcat-users.xml
catalina.policy logging.properties server.xml web.xml
catalina.properties policy.d tomcat5.5
msfadmin@metasploitable:/var/lib/tomcat5.5/conf$ nano server.xml
```

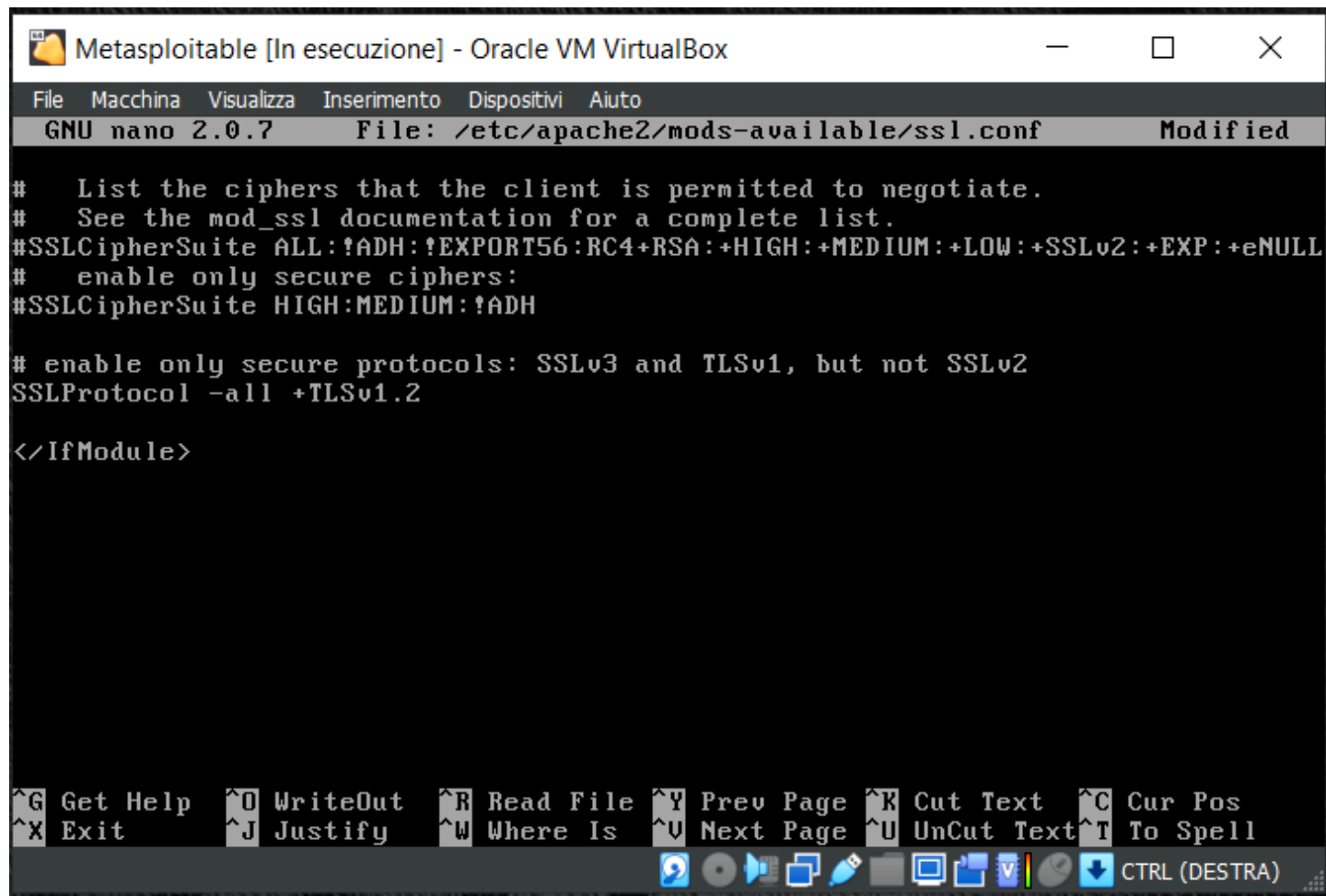
```
<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009"
           enableLookups="false" secretRequired="true" redirectPort="8443" $
```

```
<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009"
$8443" protocol="AJP/1.3" secret="string" />
```

- Il server Apache cripta il traffico con protocolli di cifratura che hanno delle vulnerabilità note (SSL 2.0 e SSL 3.0)

Per risolvere questo problema, dobbiamo disabilitare i protocolli di cifratura SSL 2.0 e SSL 3.0, ed abilitare il **Transport Layer Security v1.2**, andando nel file di configurazione `/etc/apache2/mods-available/ssl.conf` e inserendo nel parametro **SSL Protocol** la stringa:

-all +TLSv1.2 in modo da disabilitare tutti protocolli ad eccezione del TLSv1.2



```

Metasploitable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7  File: /etc/apache2/mods-available/ssl.conf  Modified

# List the ciphers that the client is permitted to negotiate.
# See the mod_ssl documentation for a complete list.
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
# enable only secure ciphers:
#SSLCipherSuite HIGH:MEDIUM:!ADH

# enable only secure protocols: SSLv3 and TLSv1, but not SSLv2
SSLProtocol -all +TLSv1.2

</IfModule>

^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

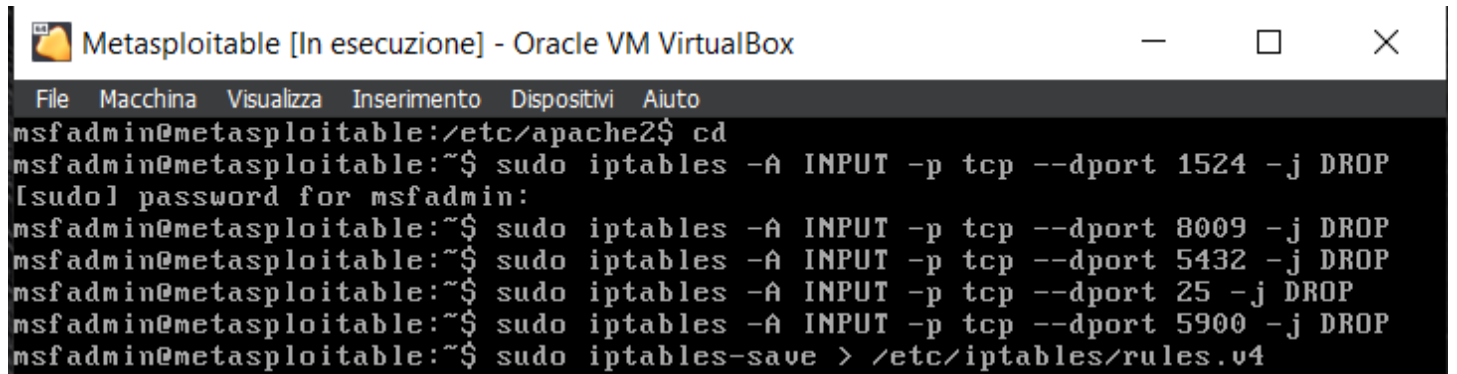
CTRL (DESTRA)
```

Dopo aver svolto queste azioni di rimedio, possiamo aggiungere una regola del firewall Iptables per rendere ancora più sicuro il sistema. Le porte da prendere in considerazione sono:

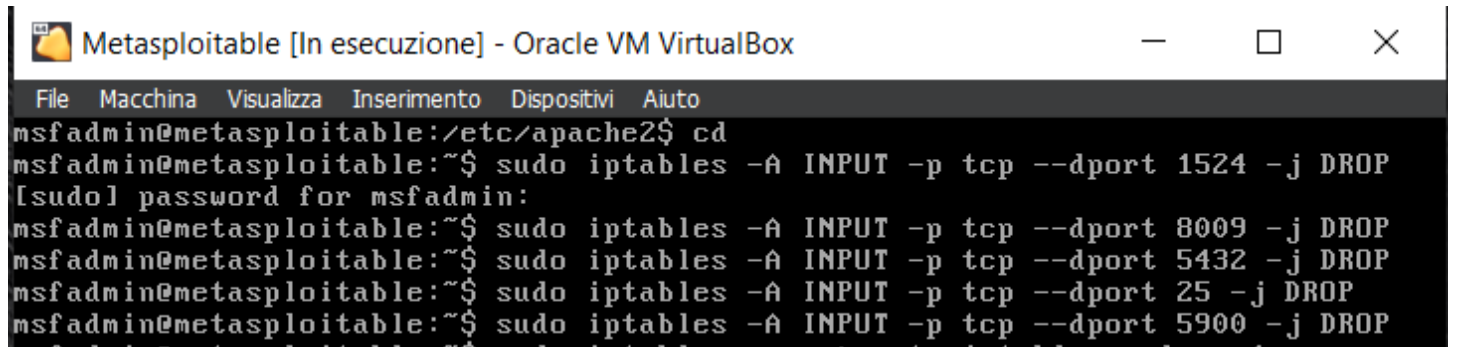
- TCP 1524 (Backdoor con permessi di root)
- TCP 8009 (Connector AJP)
- TCP 5432 e TCP 25 (usate da Apache per il traffico)
- TCP 5900

Eseguiamo il seguente comando per bloccare tutto il traffico in ingresso dalle porte specificate prima:

sudo iptables -A INPUT -s <indirizzo_IP> -p tcp --dport <porta> -j DROP



```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
msfadmin@metasploitable:/etc/apache2$ cd
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 8009 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 5432 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 25 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 5900 -j DROP
msfadmin@metasploitable:~$ sudo iptables-save > /etc/iptables/rules.v4
```



```
Metasploitable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
msfadmin@metasploitable:/etc/apache2$ cd
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 8009 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 5432 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 25 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 5900 -j DROP
```

Possiamo salvare le modifiche in un file tramite il comando

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

Così facendo si possono richiamare tramite il comando seguente, al successivo riavvio della macchina, dato che queste regole non vengono salvate in modo permanente.

iptables-restore < /etc/iptables/rules.v4

4) Scansione finale

Come vediamo dall'immagine della scansione di Nessus, le vulnerabilità critiche prese in esame sono state risolte dalle *remediation* viste in precedenza.

Meta Fixata / 192.168.178.100

Configure

Audit Trail

Launch

Report

Export

Vulnerabilities48

Filter

Search Vulnerabilities

48 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/>	CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detect...	Backdoors	1	
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Share Informa...	RPC	1	
<input type="checkbox"/>	CRITICAL	10.0 *	5.1	Debian OpenSSH/OpenSSL ...	Gain a shell remotely	1	
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Uns...	General	1	
<input type="checkbox"/>	HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1	
<input type="checkbox"/>	HIGH	7.5		NFS Shares World Readable	RPC	1	
<input type="checkbox"/>	MIXED	ISC Bind (Multiple Issues)	DNS	5	
<input type="checkbox"/>	MEDIUM	2.1 *	4.2	ICMP Timestamp Request R...	General	1	

Host Details

IP:

192.168.178.100

MAC:

08:00:27:C9:FC:84

OS:

Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Start:

Today at 12:57 AM

End:

Today at 1:10 AM

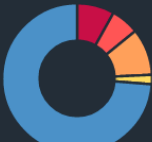
Elapsed:

12 minutes

KB:

[Download](#)

Vulnerabilities



Critical

High

Medium

Low

Info

CTRL (DESTRA)