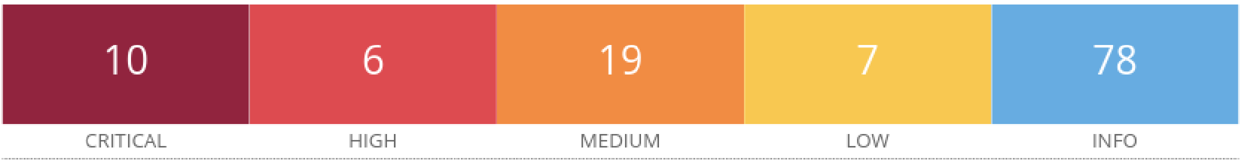
Benchmark Modulo 3 – Penetration Test e Vulnerability Assessment – Alessio Russo

Risultati Scansione, Valutazione Vulnerabilità e Remediation

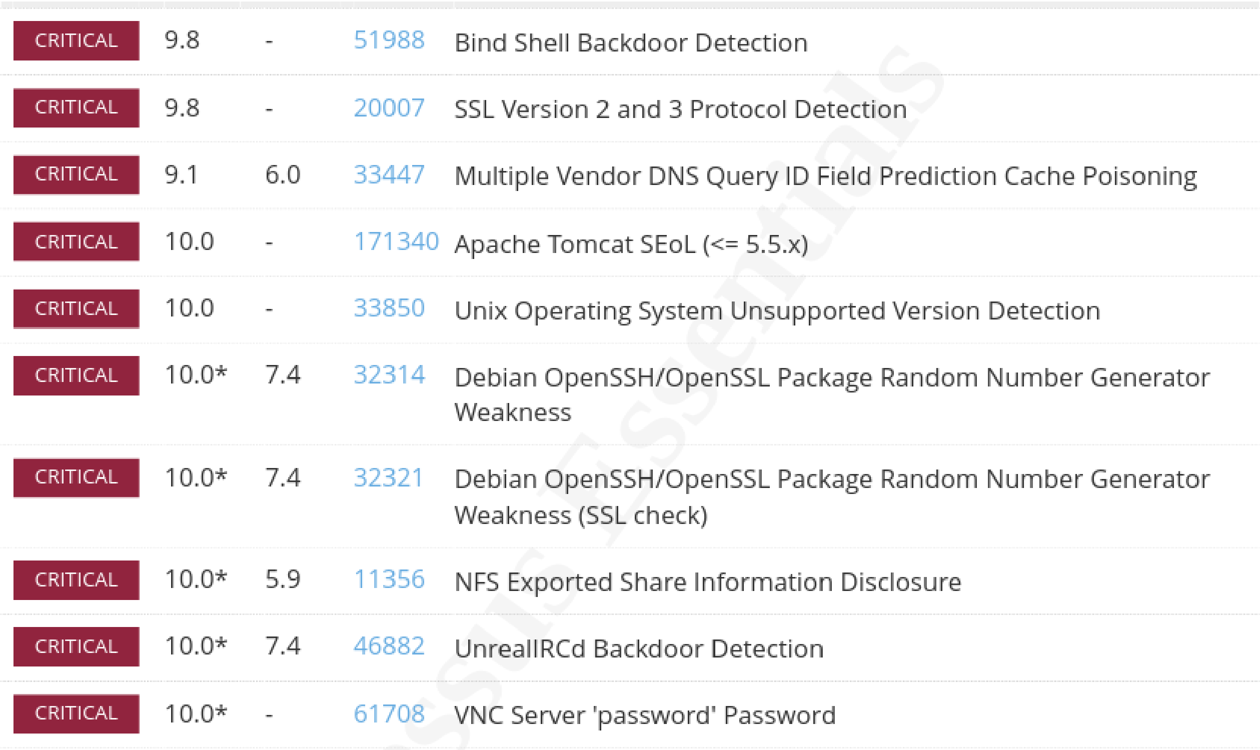
Scanning su macchina Metasploitable 2 e Valutazione Vulnerabilità critiche

- Scanning effettuato tramite Kali Linux attraverso il tool Nessus;
- Lo scanning ha reportato un totale di 10 vulnerabilità



10	6	19	7	78
CRITICAL	HIGH	MEDIUM	LOW	INFO

- Nel dettaglio tali vulnerabilità critiche sono:

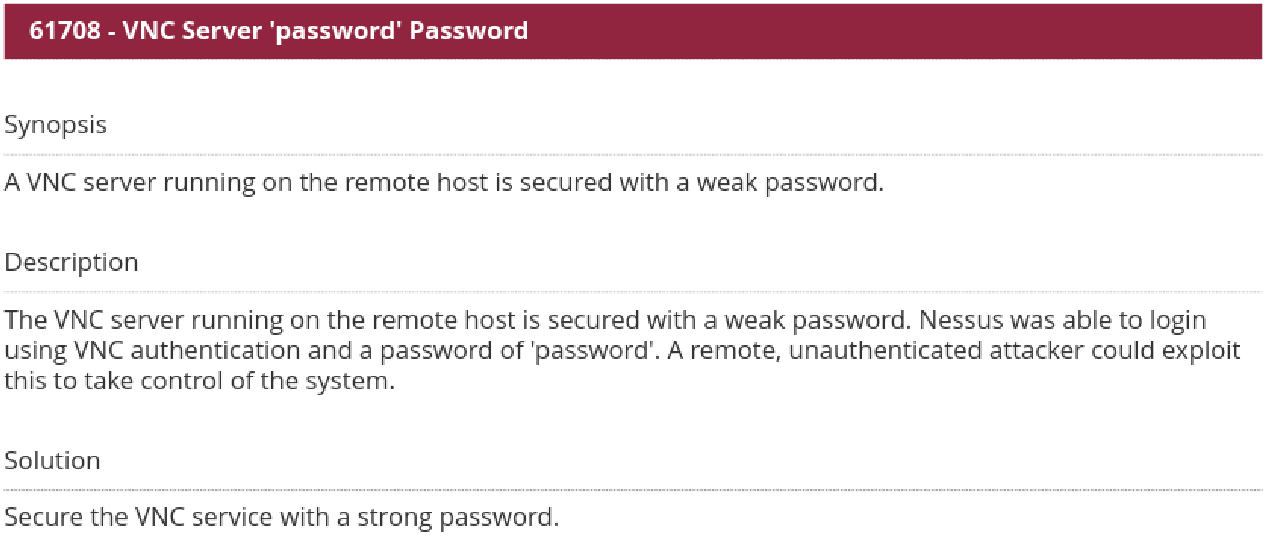


CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	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*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

- La traccia richiedeva di risolverne 4 utilizzando metodologie eterogenee (una sola con firewall), risolta la 4 si può procedere a risolverne una quinta (anche con firewall).
- L’attenzione nel dettaglio è ricaduta sulle vulnerabilità 61708, 51988, 171340, 11356

DESCRIPTION E RESOLUTION DELLE VULNERABILITÀ

1) 61708 – VNC Server password = Password



61708 - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak password.

Description

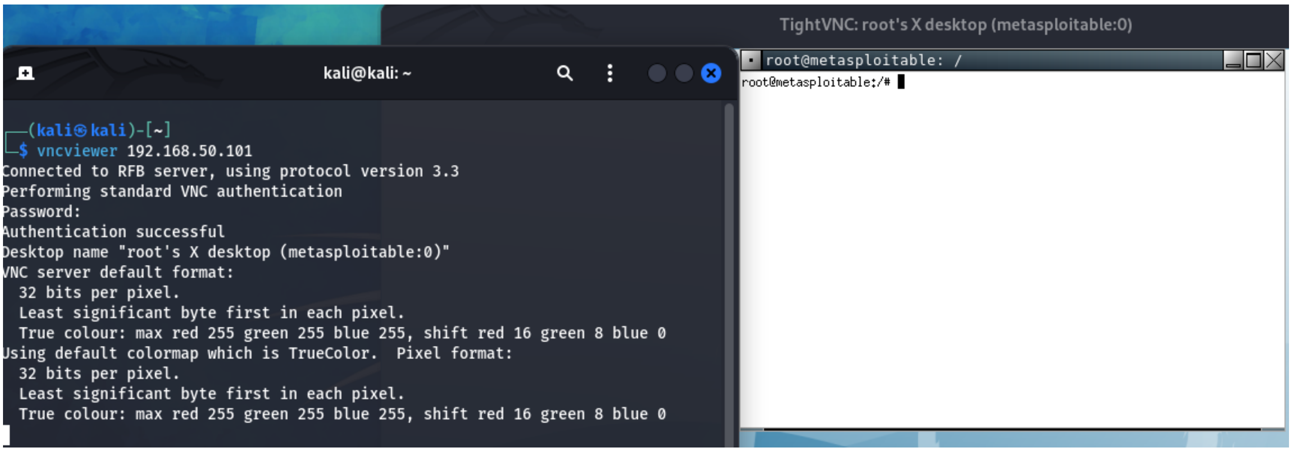
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

TEST EXPLOIT AND RESOLUTION:

- Lanciando *vncviewer 192.168.50.101* da macchina Kali Linux, inserendo IP Metasploitable e utilizzando “password” quando viene richiesta la stessa è possibile collegarsi al server VNC da remoto e agire da root su Metasploitable:

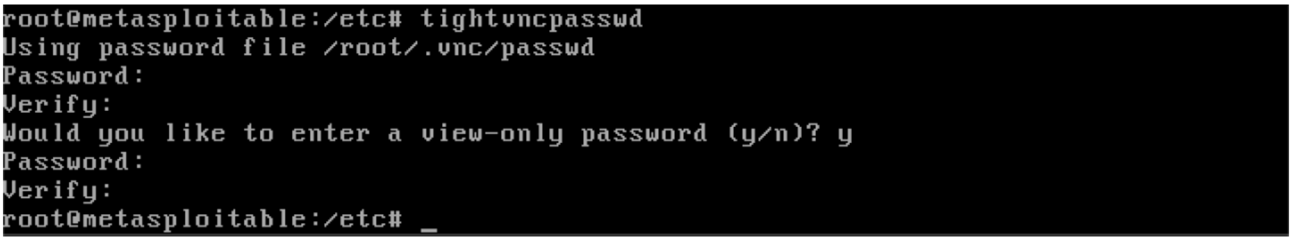


```
┌──(kali㉿kali)-[~]
└─$ vncviewer 192.168.50.101
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

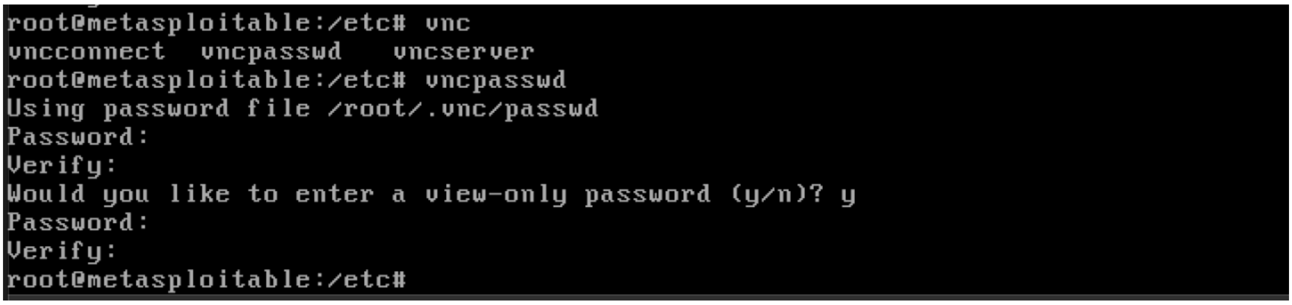
```
root@metasploitable:/# 
```

REMEDIATION:

- Mi autentico come root su Metasploitable 2 e cambio la password di vnc, visto che la vulnerabilità si potrebbe estendere anche a tightvnc cambio entrambe le password.

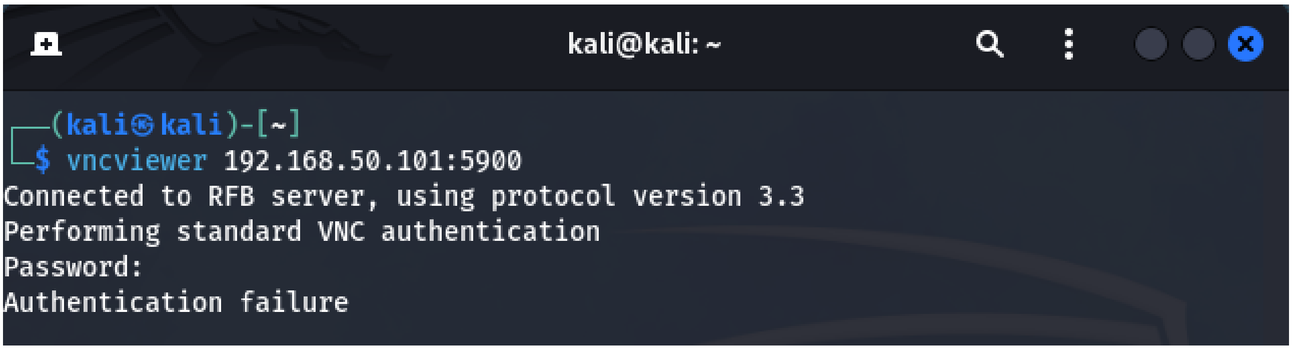


```
root@metasploitable:/etc# tightvncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/etc# _
```



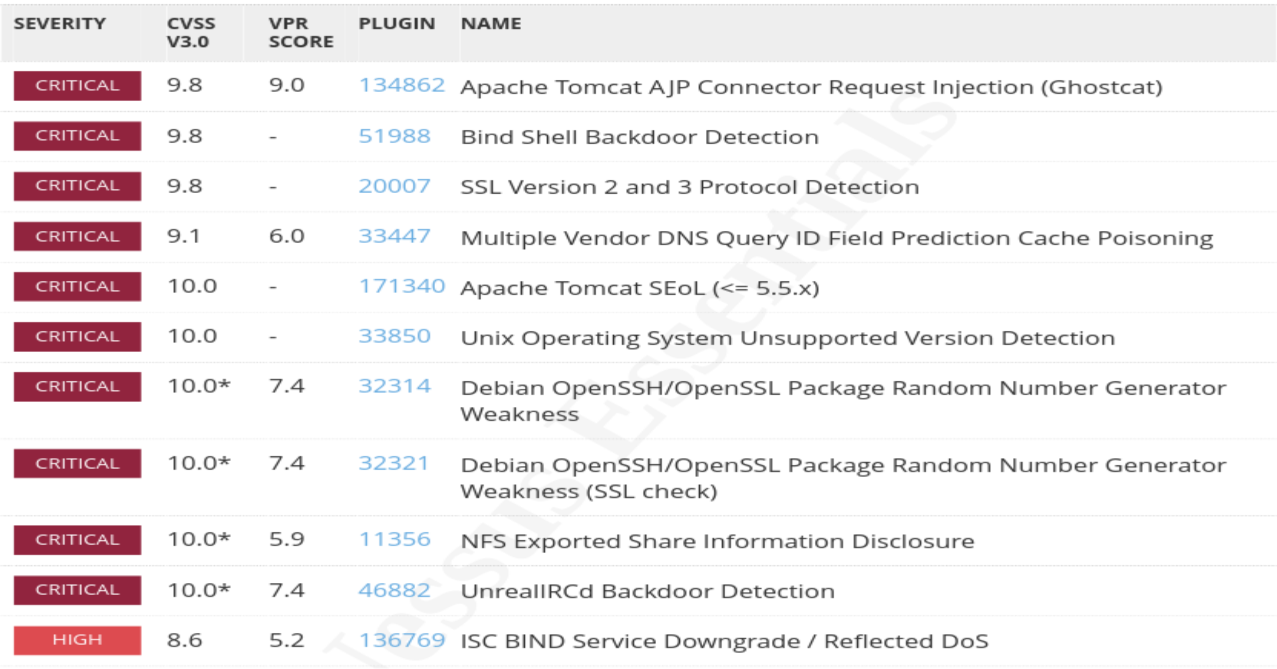
```
root@metasploitable:/etc# vnc
vncconnect  vncpasswd   vncserver
root@metasploitable:/etc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/etc#
```

- Test su vncviewer dove inserisco la password “password” e il risultato è questo sotto porta 5900 in quanto da report vulnerabilità la porta specificata era la stessa:



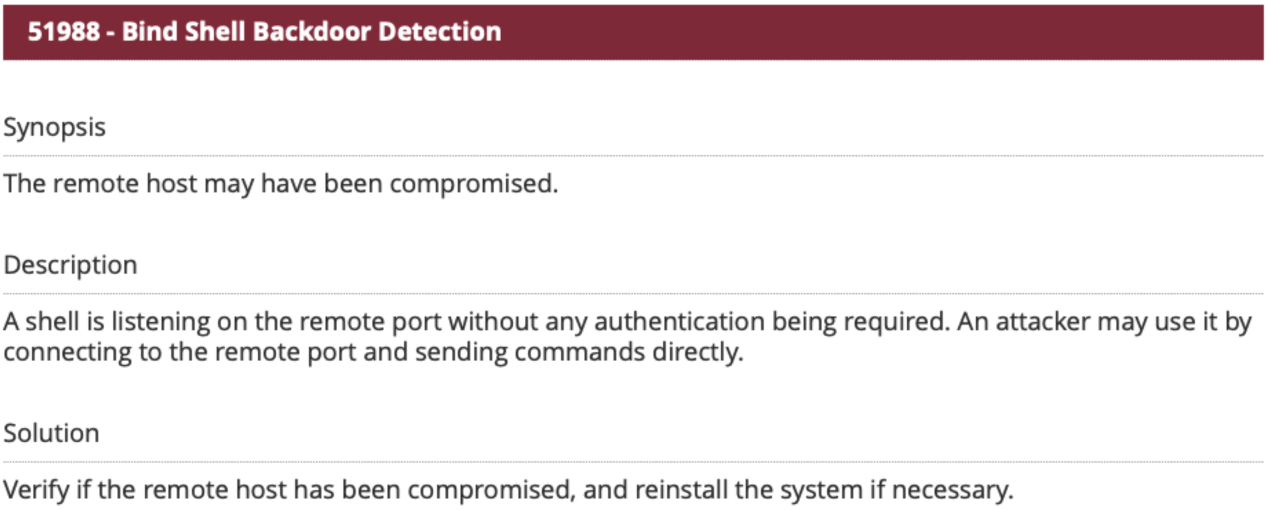
```
┌──(kali㉿kali)-[~]
└─$ vncviewer 192.168.50.101:5900
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication failure
```

- Risultato SCAN POST REMEDIATION (pagina successiva), si evince che la vulnerabilità 61708 non viene più rilevata.



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	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	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*	7.4	46882	UnrealIRCd Backdoor Detection
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS

2) ERRORE 51988 - A shell is listening on the remote port (1524) without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.



51988 - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

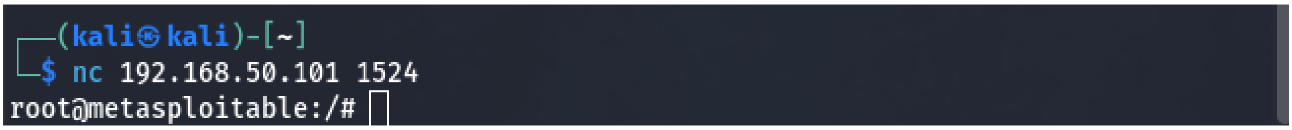
Description

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.

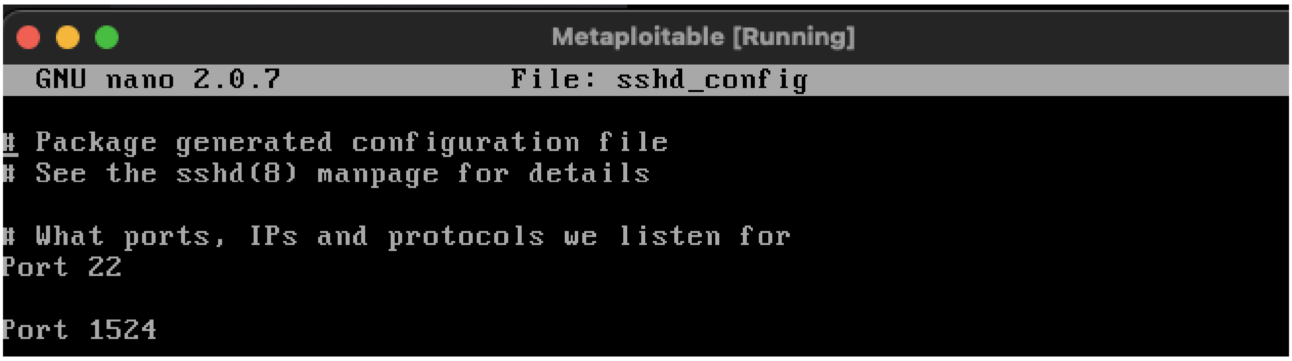
- Verifico da Kali l’effettiva potenzialità dannosa della porta con il comando:
  - nc 192.168.50.101 1524 dove possiamo vedere che diventiamo root metasploitable.



```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.101 1524
root@metasploitable:/# 
```

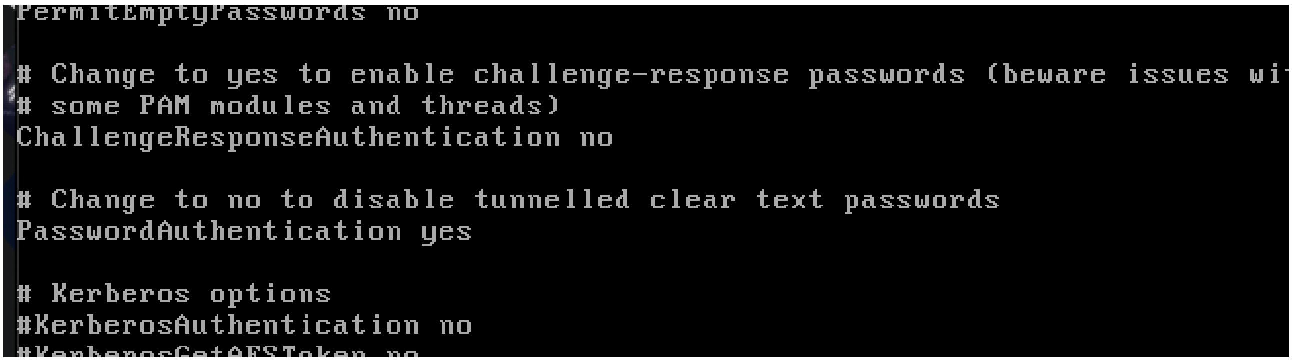
- Chiudo la porta 1524 applicando una servizio ssh in modo da autenticare con una password:

  - Inserisco la porta nelle porte a cui viene richiesta una password sudo nano *`/etc/ssh/sshd_conf`* aggiungendo “Port 1254”



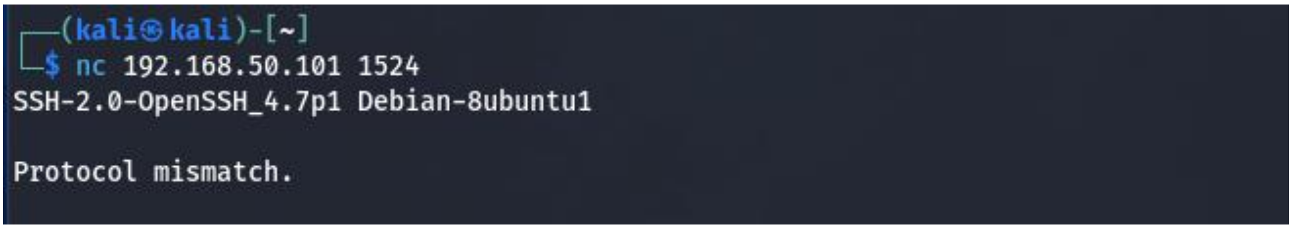
```
  GNU nano 2.0.7                 File: sshd_config

# Package generated configuration file
# See the sshd(8) manpage for details

# What ports, IPs and protocols we listen for
Port 22

Port 1524
```

  - Abilito l’autenticazione con password andando a de-commentare *`PasswordAuthentication yes`*

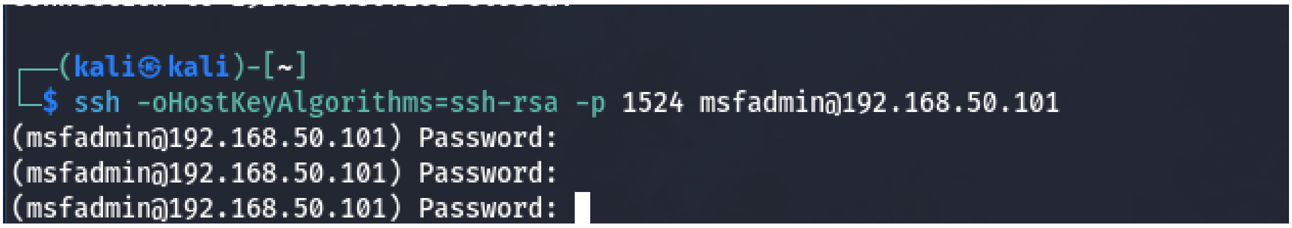


```
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues wi
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
PasswordAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
```

  - In questo caso se si digita *`nc 192.168.50.100 1524`* non ci collegheremo più come root metasploitable in Kali Linux, digitando il comando
`ssh -oHostKeyAlgorithms=ssh-rsa -p 1524 msfadmin@192.168.50.101`
ci verrà chiesta una password che sarebbe la password di metasploitable di admin

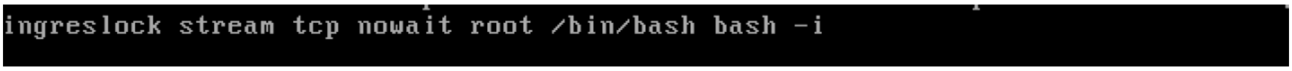


```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.50.101 1524
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

Protocol mismatch.
```



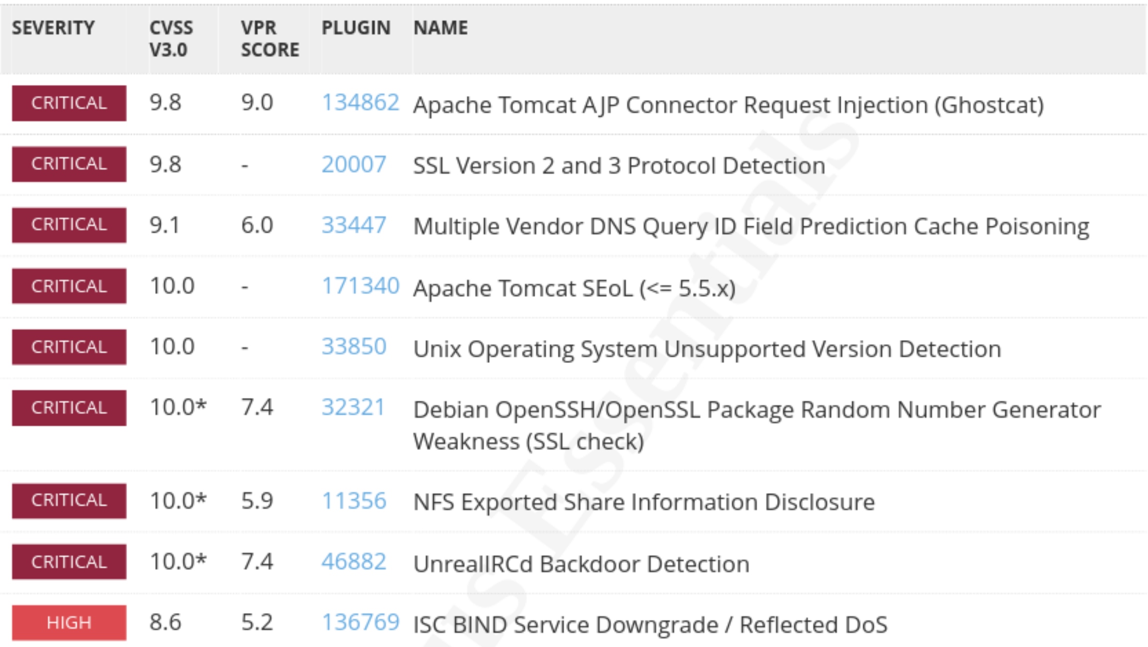
```
┌──(kali㉿kali)-[~]
└─$ ssh -oHostKeyAlgorithms=ssh-rsa -p 1524 msfadmin@192.168.50.101
(msfadmin@192.168.50.101) Password:
(msfadmin@192.168.50.101) Password:
(msfadmin@192.168.50.101) Password: 
```

- In alternativa avremmo potuto eliminare direttamente la porta, considerato che non fa parte delle well-know port chiudendo la vulnerabilità digitando: /etc/inetd.conf e cancellando la riga



```
ingreslock stream tcp nowait root /bin/bash bash -i
```

- Risultato SCAN POST REMEDIATION si evince che la vulnerabilità 51988 non viene più rilevata.



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	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	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*	7.4	46882	UnrealIRCd Backdoor Detection
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS

3) ERRORE 32314 - The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

See Also

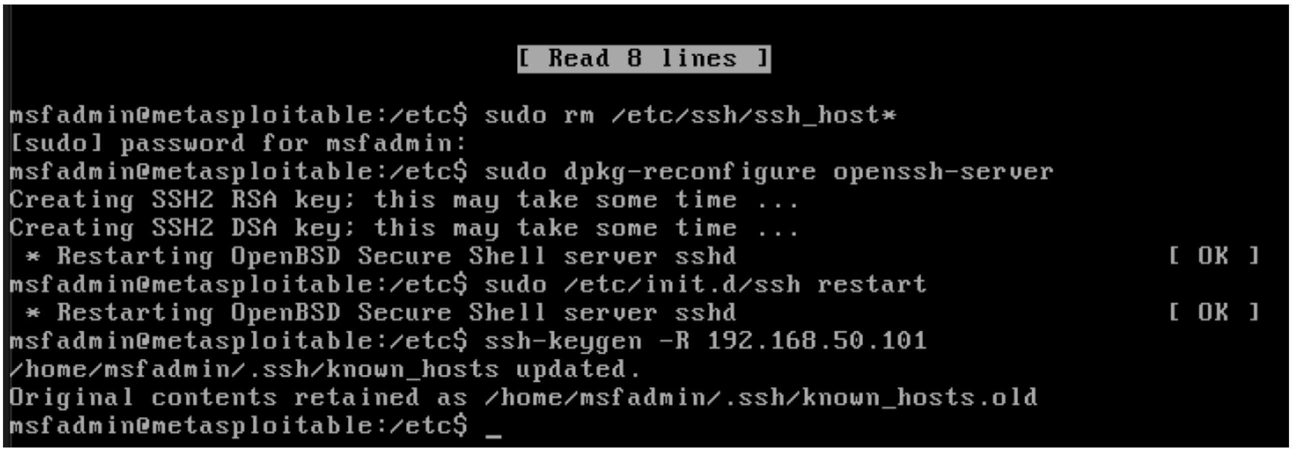
http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

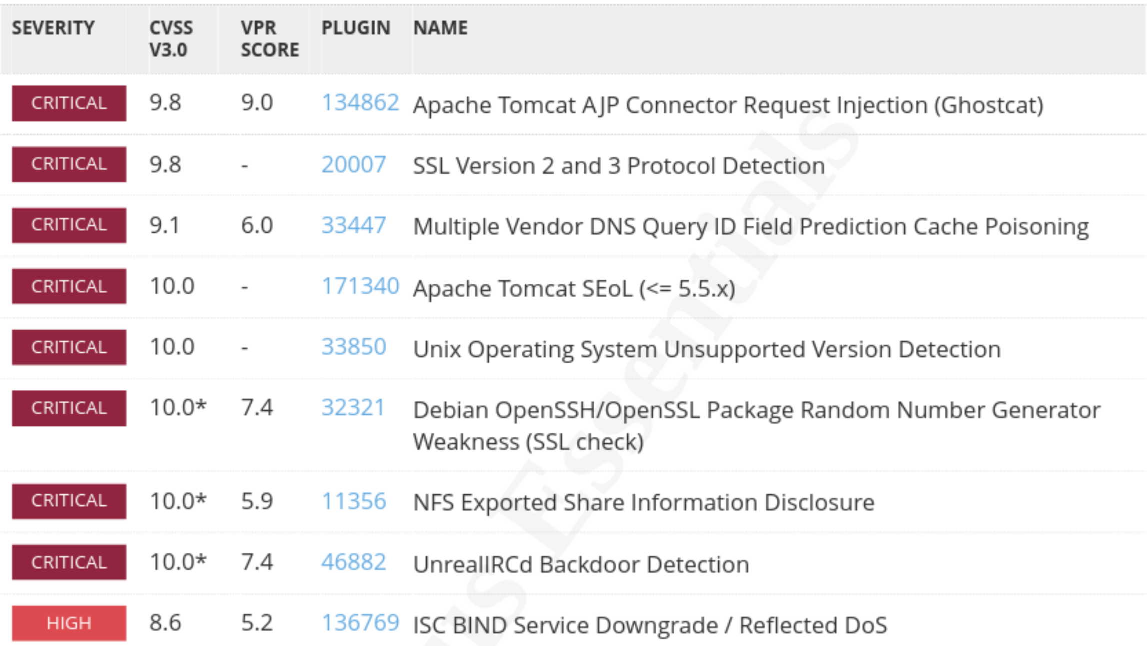
Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

- Nello step precedente risulta evidente come la vulnerabilità 32314 come da elenco all'inizio è stata risolta rigenerando le chiavi crittografiche SSH

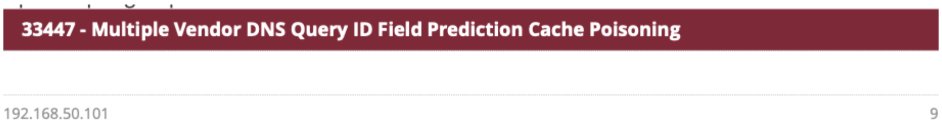


```
                                [ Read 8 lines ]

msfadmin@metasploitable:/etc$ sudo rm /etc/ssh/ssh_host*
[sudo] password for msfadmin:
msfadmin@metasploitable:/etc$ sudo dpkg-reconfigure openssh-server
Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
 * Restarting OpenBSD Secure Shell server sshd                           [ OK ]
msfadmin@metasploitable:/etc$ sudo /etc/init.d/ssh restart
 * Restarting OpenBSD Secure Shell server sshd                           [ OK ]
msfadmin@metasploitable:/etc$ ssh-keygen -R 192.168.50.101
/home/msfadmin/.ssh/known_hosts updated.
Original contents retained as /home/msfadmin/.ssh/known_hosts.old
msfadmin@metasploitable:/etc$ _
```



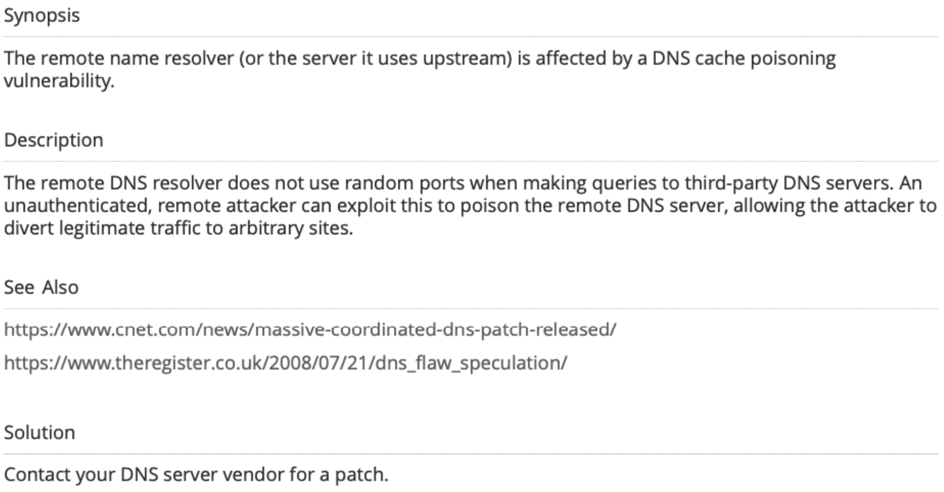
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	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*	7.4	46882	UnrealIRCd Backdoor Detection
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS

4) ERRORE 33447 - The remote DNS resolver does not use random ports when making queries to third-party DNS servers. An unauthenticated, remote attacker can exploit this to poison the remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites.



33447 - Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

192.168.50.101 9



Synopsis

The remote name resolver (or the server it uses upstream) is affected by a DNS cache poisoning vulnerability.

Description

The remote DNS resolver does not use random ports when making queries to third-party DNS servers. An unauthenticated, remote attacker can exploit this to poison the remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites.

See Also

https://www.cnet.com/news/massive-coordinated-dns-patch-released/

https://www.theregister.co.uk/2008/07/21/dns_flaw_speculation/

Solution

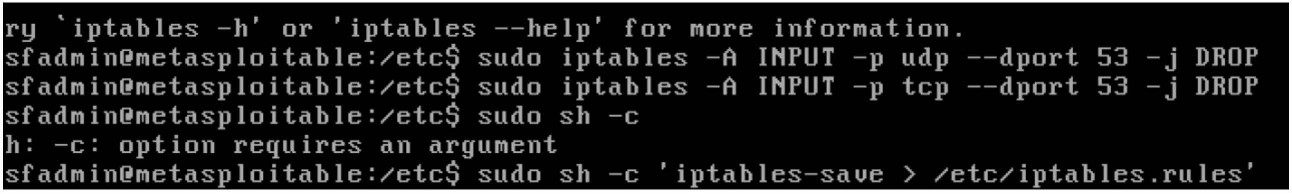
Contact your DNS server vendor for a patch.

(Utilizzo Iptables)

- Blocco la porta 53 digitando:

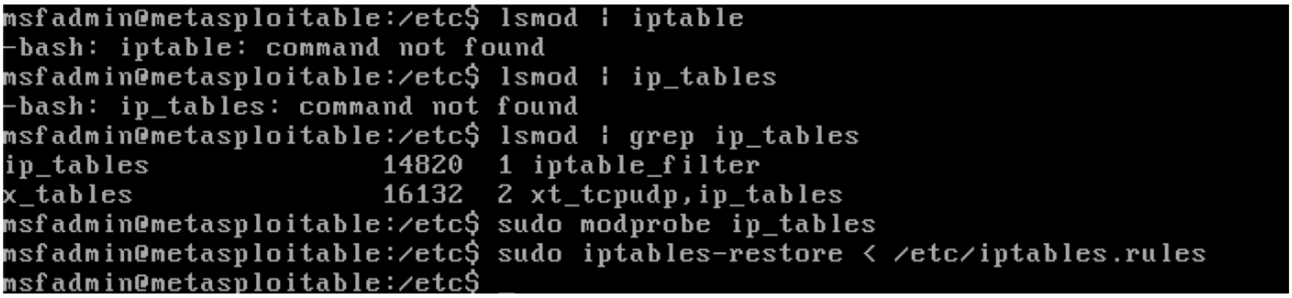
  sudo iptables -A INPUT -p udp --dport 53 -j DROP
  sudo iptables -A INPUT -p tcp --dport 53 -j DROP

  Salvo le regole iptables
  sudo sh -c 'iptables-save > /etc/iptables.rules'



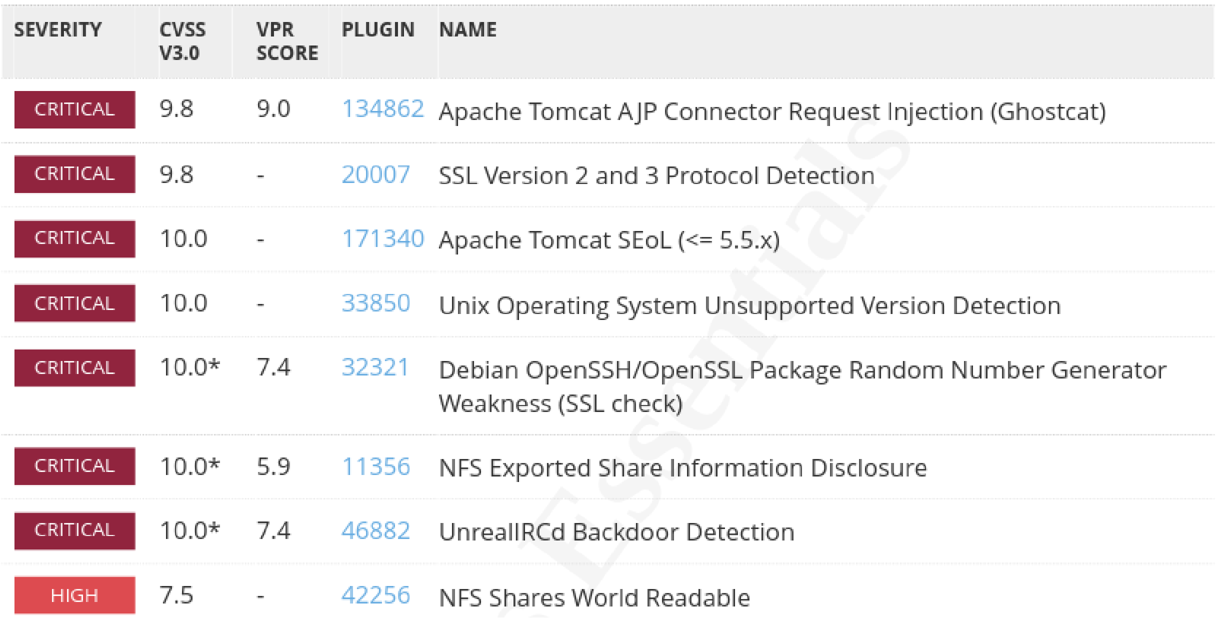
```
ry `iptables -h' or 'iptables --help' for more information.
sfadmin@metasploitable:/etc$ sudo iptables -A INPUT -p udp --dport 53 -j DROP
sfadmin@metasploitable:/etc$ sudo iptables -A INPUT -p tcp --dport 53 -j DROP
sfadmin@metasploitable:/etc$ sudo sh -c
h: -c: option requires an argument
sfadmin@metasploitable:/etc$ sudo sh -c 'iptables-save > /etc/iptables.rules'
```

- Per rendere permanenti le regole iptables salvo le regole in un file caricandole durante l'avvio del sistema.
  iptables-restore < /etc/iptables.rules



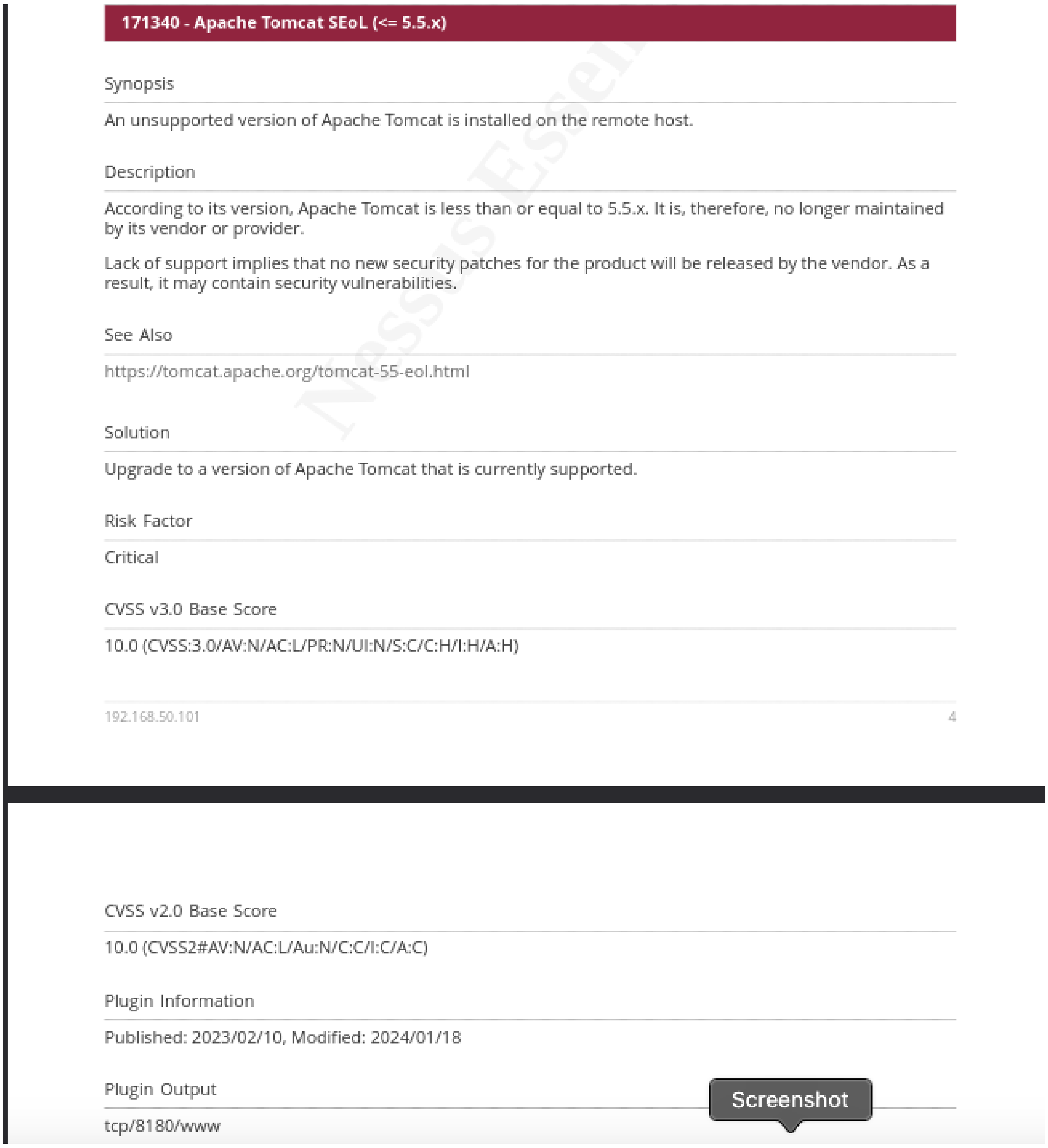
```
msfadmin@metasploitable:/etc$ lsmod ¦ iptable
-bash: iptable: command not found
msfadmin@metasploitable:/etc$ lsmod ¦ ip_tables
-bash: ip_tables: command not found
msfadmin@metasploitable:/etc$ lsmod ¦ grep ip_tables
ip_tables              14820  1 iptable_filter
x_tables               16132  2 xt_tcpudp,ip_tables
msfadmin@metasploitable:/etc$ sudo modprobe ip_tables
msfadmin@metasploitable:/etc$ sudo iptables-restore < /etc/iptables.rules
msfadmin@metasploitable:/etc$ _
```

- Risultato SCAN POST REMEDIATION si evince che la vulnerabilità 33447 non viene più rilevata.



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	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	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*	7.4	46882	UnrealIRCd Backdoor Detection
HIGH	7.5	-	42256	NFS Shares World Readable

5) ERRORE 171340 porta 8180 - BONUS – FIREWALL



171340 - Apache Tomcat SEoL (<= 5.5.x)

Synopsis

An unsupported version of Apache Tomcat is installed on the remote host.

Description

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

See Also

https://tomcat.apache.org/tomcat-55-eol.html

Solution

Upgrade to a version of Apache Tomcat that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

192.168.50.101 4

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

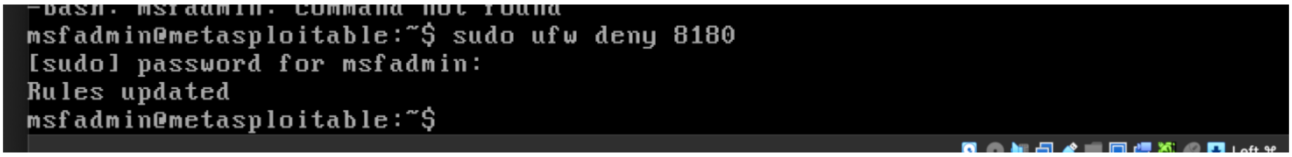
Published: 2023/02/10, Modified: 2024/01/18

Plugin Output

tcp/8180/www

- Blocco la porta 8180 digitando:

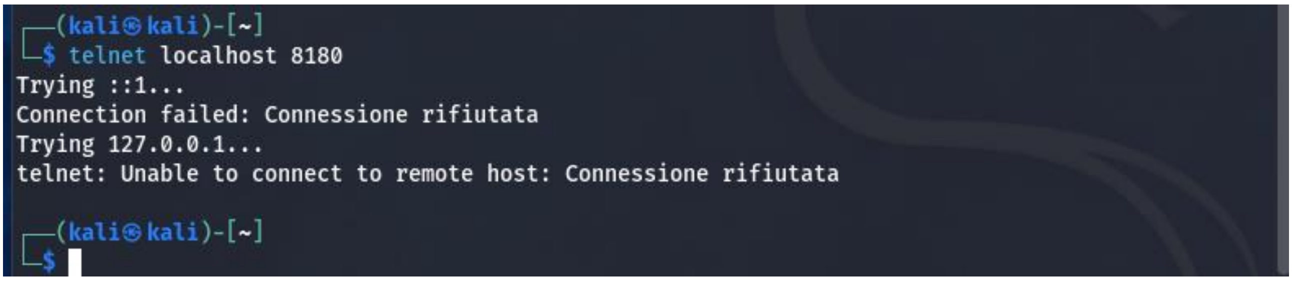
sudo ufw deny 8180



```
-bash: msfadmin: command not found
msfadmin@metasploitable:~$ sudo ufw deny 8180
[sudo] password for msfadmin:
Rules updated
msfadmin@metasploitable:~$
```

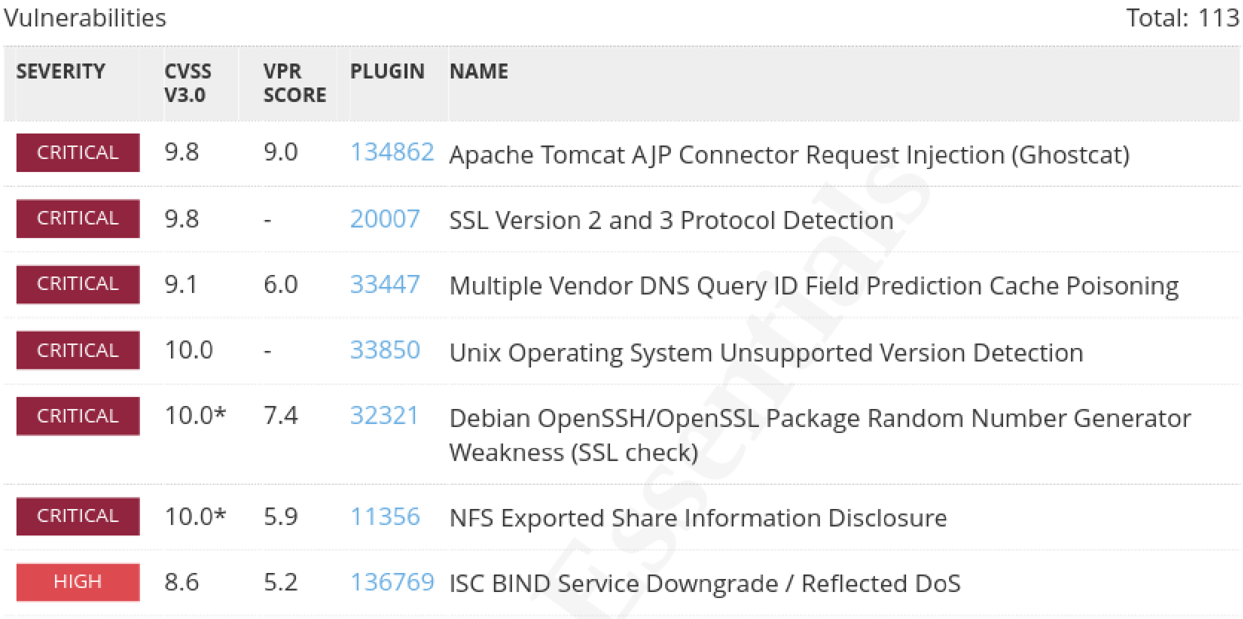
- Test con Kali Linux e telnet per vedere se effettivamente la porta 8180 è chiusa digitando

telnet localhost 8180



```
┌──(kali㉿kali)-[~]
└─$ telnet localhost 8180
Trying ::1...
Connection failed: Connessione rifiutata
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connessione rifiutata

┌──(kali㉿kali)-[~]
└─$ 
```

- Risultato SCAN POST REMEDIATION si evince che la vulnerabilità 171340 non viene più rilevata.



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	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS

NOTA:

Una volta terminato il procedimento di Remediation si rileva l'insorgere di una nuova vulnerabilità critica la 134862 non rilevata nel primo scanning