

W12D4- FRANCESCO MONTALTO

### ATTENZIONE, NOTA PER IL PROFESSORE:

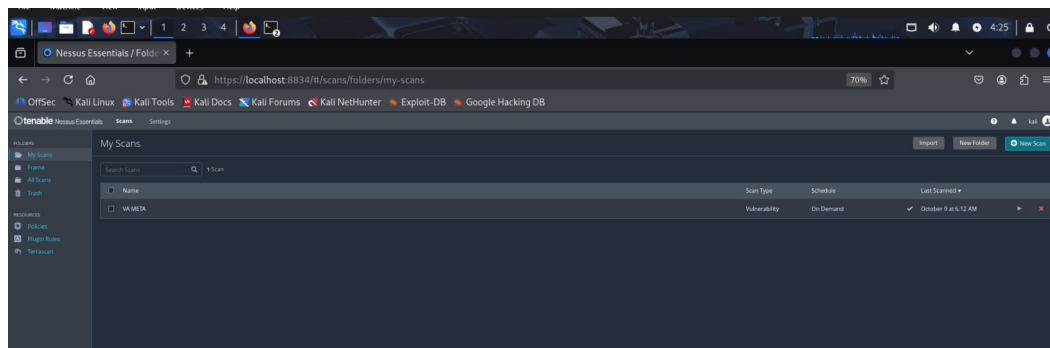
Ho effettuato il primo caricamento del file in versione OTD e non in PDF (per sbaglio, naturalmente), e mi sono accorto solo dopo che il file non era visionabile da repository, quindi ho preceduto a ricaricare la versione in PDF.

1. Per questo esercizio ho deciso di eseguire una nuova scansione su Meta, quindi dopo aver al solito verificato le connettività varie mi sono loggato su Nessus ed ho eseguito una nuova scansione, con target IP Meta, come richiesto dalla traccia.

```
(kali@kali)-[~/Desktop]
$ ping -c 4 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=1.23 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.855 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.720 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.686 ms

— 192.168.56.101 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.686/0.872/1.229/0.215 ms

(kali@kali)-[~/Desktop]
$
```



### New Scan / Basic Network Scan

[Back to Scan Templates](#)

**Settings**

Credentials

Plugins

**BASIC**

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Scan\_Metasploitable

Description

Folder

My Scans

Targets

192.168.56.101

REQUIRED

Upload Targets

Add File

Save

Cancel

### My Scans

Search Scans 2 Scans

Name	Scan Type	Schedule	Last Scanned
<u>Scan_Metasploitable</u>	Vulnerability	On Demand	Today at 4:57 AM
VA META	Vulnerability	On Demand	Today at 4:38 AM

2. Ho poi proceduto ad aprire il report dello scan appena effettuato.

### Scan\_Metasploitable

[Back to My Scans](#)

Hosts

Vulnerabilities

Remediations

History

Filter

Search Hosts

1 Host

Host	Auth	Vulnerabilities
192.168.56.101	Fail	10

Report Format:

HTML

PDF

CSV

Select a Report Template:

SYSTEM

Complete List of Vulnerabilities by Host

Detailed Vulnerabilities By Host

Detained Vulnerabilities By Plugin

Vulnerability Operations

Template Description:

This report provides a summary list of vulnerabilities for each host selected in the scan.

Filters Applied:

None

Formatting Options:

of results page controls between vulnerability results

Generate Report

Cancel

Save as default

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 4:57 AM

End:

Today at 4:57 AM

Elapsed:

19 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Scan\_Metasploitable

[Back to My Scans](#)

Hosts 1 Vulnerabilities 68 Remediations 2 History 1

Filter Search Vulnerabilities 68 Vulnerabilities

<input type="checkbox"/> Sev ▼	CVSS ▼	VPR ▼	EPSS ▼	Name ▲	Family ▲
<input type="checkbox"/> CRITICAL	10.0			Canonical Ubuntu Linux SEOL (8.04.x)	General
<input type="checkbox"/> CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely
<input type="checkbox"/> CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection
<input type="checkbox"/> CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors
<input type="checkbox"/> MEDIUM	...	...	...	Apache Tomcat (Multiple Issues)	Web Servers
<input type="checkbox"/> CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely
<input type="checkbox"/> HIGH	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection
<input type="checkbox"/> HIGH	7.5	5.9	0.7865	Samba Badlock Vulnerability	General
<input type="checkbox"/> HIGH	7.5			NFS Shares World Readable	RPC
<input type="checkbox"/> MEDIUM	...	...	...	SSL (Multiple Issues)	General
<input type="checkbox"/> MEDIUM	...	...	...	ISC Bind (Multiple Issues)	DNS
<input type="checkbox"/> MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection
<input type="checkbox"/> MEDIUM	6.5			Unencrypted Telnet Server	Misc.
<input type="checkbox"/> MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection
<input type="checkbox"/> MEDIUM	5.9	3.6	0.9035	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.
<input type="checkbox"/> MEDIUM	...	...	...	SSH (Multiple Issues)	Misc.
<input type="checkbox"/> MEDIUM	...	...	...	HTTP (Multiple Issues)	Web Servers

2.1 Aggiuntivamente, ho eseguito un rapido nmap per avere un confronto testuale.

```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -p- -sS -sV -Pn -oN nmap_before.txt 192.168.56.101  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-14 06:02 EDT  
Nmap scan report for 192.168.56.101  
Host is up (0.00045s latency).  
Not shown: 65505 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec         netkit-rsh rshcd  
513/tcp   open  login        OpenBSD or Solaris rlogind  
514/tcp   open  shell        Netkit rshd  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
2049/tcp  open  nfs          2-4 (RPC #100003)  
2121/tcp  open  ftp          ProFTPD 1.3.1  
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5  
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3)  
6000/tcp  open  X11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
6697/tcp  open  irc          UnrealIRCd  
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbr)
```

3. A questo punto ho scelto le 4 criticità da risolvere:

Scan\_Metasploitable

[Back to My Scans](#)

Hosts 1 Vulnerabilities 64 Remediations 2 History 2

Filter Search Vulnerabilities 64 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	EPSS ▼	Name ▲	Family ▲
<input type="checkbox"/>	CRITICAL	10.0			Canonical Ubuntu Linux SE...	General
<input type="checkbox"/>	CRITICAL	9.8			SSL Version 2 and 3 Protoc...	Service detection
<input type="checkbox"/>	CRITICAL	9.8			Bind Shell Backdoor Detect...	Backdoors
<input type="checkbox"/>	MIXED	...	...	...	4 Apache Tomcat (Multi...	Web Servers
<input type="checkbox"/>	CRITICAL	...	...	...	2 SSL (Multiple Issues)	Gain a shell remotely
<input type="checkbox"/>	HIGH	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection
<input type="checkbox"/>	HIGH	7.5	5.9	0.7865	Samba Badlock Vulnerability	General
<input type="checkbox"/>	HIGH	7.5			NFS Shares World Readable	RPC
<input type="checkbox"/>	...	...	...	...	15 SSL (Multiple Issues)	General

Settings/about

#### 4. Sistema operativo EOL (Ubuntu 8.04)

Scan\_Metasploitable / Plugin #201352 Configure Audit Trail

[← Back to Vulnerabilities](#)

Hosts 1 **Vulnerabilities 64** Remediations 2 History 2

**CRITICAL** Canonical Ubuntu Linux SEoL (8.04.x) < >

**Description**  
According to its version, Canonical Ubuntu Linux is 8.04.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.

**Solution**  
Upgrade to a version of Canonical Ubuntu Linux that is currently supported.

**See Also**  
<http://www.nessus.org/u73bdb2d2e>

**Output**

```
OS : Ubuntu Linux 8.04
Security End of Life : May 9, 2013
Time since Security End of Life (Est.) : >= 12 years
```

To see debug logs, please visit individual host

Port ▲ Hosts

Il problema è che il sistema non riceve più patch. È una vulnerabilità “di radice”: non si risolve aggiornando qualche pacchetto singolo, perché la distribuzione è fuori supporto da anni.

SOLUZIONE:

1. Proviamo su Metasploitable che la versione OS e Kernel corrisponde a Ubuntu 8.04.

```
msfadmin@metasploitable:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 8.04
Release:        8.04
Codename:       hardy
msfadmin@metasploitable:~$ _
```

2. Sappiamo che non è facilmente aggiornabile, in quanto volutamente vulnerabile (parliamo sempre di una VM...), ma ho pensato di ridurre la superficie d'attacco usando firewall (iptables) per fare in modo che solo il tuo Kali possa parlare con la

VM e fermare servizi inutili. I comandi Iptables eseguiti sostituiscono temporaneamente tutte le regole.

### Ho permesso traffico già stabilito e loopback

```
msfadmin@metasploitable:~$ sudo iptables -F
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo iptables -X
msfadmin@metasploitable:~$ sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -i lo -j ACCEPT
msfadmin@metasploitable:~$
```

- "iptables -F" e "-X": rimuovono regole esistenti e catene non standard; usato per pulire in laboratorio.

- "m conntrack" "--ctstate ESTABLISHED,RELATED" "-j ACCEPT": permette ai pacchetti di risposta (es. quando la VM inizia una connessione verso l'esterno). Necessario per non bloccare traffico legittimo di ritorno.-

### Ho permesso solo all'admin di Kali l'accesso SSH (22), TELNET (23) e FTP (21)

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp -s 192.168.56.102 --dport 22 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp -s 192.168.56.102 --dport 23 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tco -s 192.168.56.102 --dport 21 -j ACCEPT
iptables v1.3.8: unknown protocol 'tco' specified
Try 'iptables -h' or 'iptables --help' for more information.
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp -s 192.168.56.102 --dport 21 -j ACCEPT
msfadmin@metasploitable:~$ _
```

-lo "-j ACCEPT": lascia funzionare loopback (servizi locali che comunicano tra loro sulla macchina).

- "-p tcp -s 192.168.56.102 --dport 22 -j ACCEPT": consente solo a Kali di connettersi a SSH sulla VM.

### Ho rifiutato tutte le altre connessioni TCP/UDP in ingresso.

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp -j REJECT --reject-with tcp-reset
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p udp -j REJECT
msfadmin@metasploitable:~$ _
```

- "-j REJECT --reject-with tcp-reset": rifiuta attivamente le connessioni TCP in ingresso mostrando un reset , per dimostrare che la porta è stata protetta e non è più raggiungibile.

3. Dopo aver limitato la rete, è buona pratica rendere le regole persistenti.

Tramite il comando dimostrativo (--line numbers) ho dimostrato una cosa importante.

```
msfadmin@metasploitable:~$ sudo iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num target      prot opt source                destination          ctstate RELATED
1  ACCEPT        all  --  0.0.0.0/0             0.0.0.0/0            ctstate RELATED,ESTABLISHED
2  ACCEPT        all  --  0.0.0.0/0             0.0.0.0/0
3  ACCEPT        tcp  --  192.168.56.102        0.0.0.0/0            tcp dpt:22
4  ACCEPT        tcp  --  192.168.56.102        0.0.0.0/0            tcp dpt:23
5  ACCEPT        tcp  --  192.168.56.102        0.0.0.0/0            tcp dpt:21
6  REJECT        tcp  --  0.0.0.0/0             0.0.0.0/0            reject-with tcp-
p-reset
7  REJECT        udp  --  0.0.0.0/0             0.0.0.0/0            reject-with icmp-
port-unreachable

Chain FORWARD (policy ACCEPT)
num target      prot opt source                destination

Chain OUTPUT (policy ACCEPT)
num target      prot opt source                destination
msfadmin@metasploitable:~$ _
```

È l'evidenza che il firewall è configurato correttamente per mitigare le vulnerabilità esposte dalla macchina Metasploitable.

La regola più importante è la riga 6:

6 REJECT tcp -- 0.0.0.0/0 0.0.0.0/0 reject-with tcp-reset

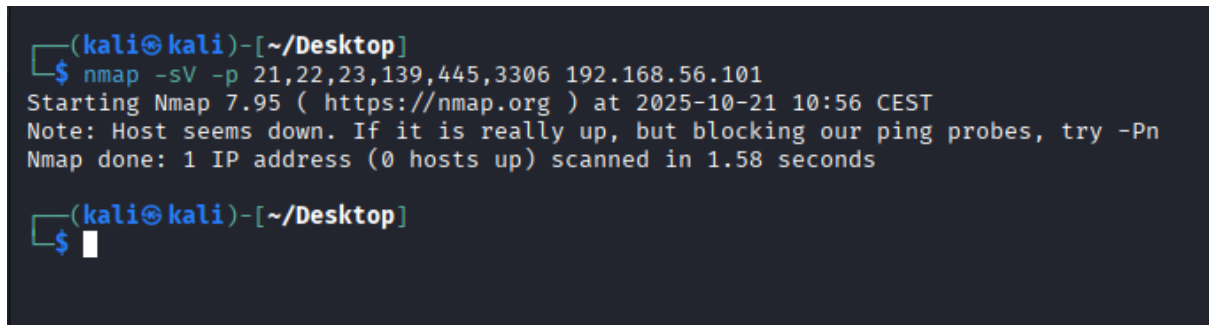
Questa riga “chiude” tutto il traffico TCP non esplicitamente permesso (riga 3–5). Solo il mio Kali (192.168.56.102) può accedere a 22, 23 e 21; tutti gli altri vengono buttati fuori.

#### 4. Prova definitiva con Nmap



Per verificare l'efficacia delle regole firewall applicate sulla macchina Metasploitable, ho eseguito una nuova scansione di rete dal sistema Kali Linux, utilizzando il seguente comando:

```
"nmap -sV -p 21,22,23,139,445,3306 192.168.56.101"
```

A terminal window with a dark background. The prompt is (kali㉿kali)-[~/Desktop]. The command nmap -sV -p 21,22,23,139,445,3306 192.168.56.101 is entered. The output shows the Nmap version (7.95), the start time (2025-10-21 10:56 CEST), a note that the host seems down, and that 1 IP address was scanned in 1.58 seconds. The prompt returns to (kali㉿kali)-[~/Desktop].

```
(kali㉿kali)-[~/Desktop]
$ nmap -sV -p 21,22,23,139,445,3306 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 10:56 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.58 seconds

(kali㉿kali)-[~/Desktop]
$
```

Risultato:

L'output restituito da Nmap è stato il seguente:

```
"Host seems down. If it is really up, but blocking our ping probes, try -Pn."
```

Questo messaggio indica che il sistema target è attivo, ma sta bloccando i pacchetti ICMP (ping) e le sonde TCP inviate da Nmap.

In altre parole, la macchina non risponde più ad alcun tentativo di scansione esterna e risulta invisibile sulla rete.

Il firewall configurato con iptables ha raggiunto il suo scopo.

## 5. SSL Version 2 and 3 Protocol Detection (Plugin #20007).

## Scan\_Metasploitable / Plugin #20007

[← Back to Vulnerabilities](#)

Hosts 1

Vulnerabilities 64

Remediations 2

History 2

### CRITICAL SSL Version 2 and 3 Protocol Detection

#### Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

#### Solution

Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

#### See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>  
<http://www.nessus.org/u?b06c7e95>  
<http://www.nessus.org/u?247c4540>  
<https://www.openssl.org/~bodo/ssl-poodle.pdf>  
<http://www.nessus.org/u?5d15ba70>  
<https://www.imperialviolet.org/2014/10/14/poodle.html>  
<https://tools.ietf.org/html/rfc7507>  
<https://tools.ietf.org/html/rfc7568>

Il problema è che il server accetta connessioni cifrate con SSL 2.0 o 3.0 , che sono protocolli arcaici. In poche parole: l'host parla ancora linguaggi cifrati antichi.

Su Metasploitable questa vulnerabilità di solito compare perché Apache o un demone simile (es. openssl con mod\_ssl) accetta ancora SSLv2/SSLv3.

La soluzione più semplice è appunto disattivare i protocolli SSLv2 e SSLv3.

**1. Ho controllato che apache fosse attivo e funzionante, per poter agire sulla configurazione SSL per bloccare le versioni vulnerabili.**

Ho proceduto alla modifica della configurazione Apache, accedendovi tramite mod-available.

```
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ sudo nano /etc/apache2/mod-available/ssl.conf
```

Una volta dentro il file nano, ho scritto quanto segue:

```

GNU nano 2.0.7      File: /etc/apache2/mod-available/ssl.conf      Modified
SSLProtocol all -SSLv2 -SSLv3

^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:~$ sudo cat /etc/apache2/mods-available/ssl.conf
<IfModule mod_ssl.c>
SSLProtocol all -SSLv2 -SSLv3

```

“SSLProtocol all -SSLv2 -SSLv3”

Questa direttiva è stata inserita nel file `/etc/apache2/mods-available/ssl.conf`, che gestisce i parametri di sicurezza SSL/TLS del server Apache.

Il comando specifica che Apache deve accettare tutti i protocolli SSL/TLS supportati, escludendo però SSLv2 e SSLv3, ormai considerati insicuri.

-“SSLProtocol all” indica di abilitare tutti i protocolli disponibili.

- "SSLv2 -SSLv3" disabilita esplicitamente SSL versione 2 e 3, vulnerabili ad altri exploit.

## 2. Ho poi proceduto al riavvio di Apache.

```
msfadmin@metasploitable:~$ sudo /etc/init.d/apache2 restart
* Restarting web server apache2
```

Dopo aver modificato il file di configurazione SSL (/etc/apache2/mods-available/ssl.conf), è stato riavviato il servizio Apache per rendere effettive le modifiche.

Il comando restart interrompe e riavvia il processo del web server, caricando nuovamente tutti i moduli e le direttive aggiornate.

La nuova direttiva SSLProtocol all -SSLv2 -SSLv3 è ora attiva, e Apache rifiuterà le connessioni tramite i protocolli insicuri SSL 2.0 e SSL 3.0.

### 3. Test di verifica finale

L'output di Nmap eseguito da Kali verso 192.168.56.101 riporta "Host seems down", indicante che il target blocca le sonde di rete.

Tale risposta significa che il sistema target è attivo ma non risponde alle sonde di rete (ICMP/TCP probes). Questo comportamento è coerente con la regola firewall applicata sulla macchina Metasploitable che rifiuta le connessioni in ingresso verso la porta 443. Di conseguenza, gli scanner esterni non possono più identificare i servizi esposti né i protocolli cifrati (inclusi SSLv2/SSLv3), ottenendo come risultato che la porta risulti filtrata o il host "irraggiungibile".

```
kali@kali: ~/Desktop
Session Actions Edit View Help
(kali@kali)-[~/Desktop]
$ sudo nmap -sV -p 443 192.168.56.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 12:17 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.55 seconds

(kali@kali)-[~/Desktop]
$
```

### 6.Bind Shell / Backdoor (Plugin #51988)

Scan\_Metasploitable / Plugin #51988

ConfigureAudit Trail

Back to Vulnerabilities

Hosts 1Vulnerabilities 64Remediations 2History 2

**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.

**Output**

```
Nessus was able to execute the command "id" using the
following request :

This produced the following truncated output (limited to 10 lines) :
..... snip .....
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
..... snip .....
```

To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wlld_shell	192.168.56.101

Il problema è che qualcuno o qualcosa volontariamente lasciato nella VM Metasploitable sta ascoltando su una porta e accetta comandi senza alcuna autenticazione. In un ambiente reale sarebbe compromissione totale.

**1. Ho tentato una mitigazione immediata, individuando e fermando il processo che, di solito, si trova sulla porta 1524 (dove c'è un processo PID).**

```
0      3      10.0.2.15:53      ***      u
sers:(("named",4050,25))
0      3      127.0.0.1:53      ***      u
sers:(("named",4050,23))
0      3      :::53      ***      u
sers:(("named",4050,21))
0      128     :::22      ***      u
sers:(("sshd",4072,3))
0      64      *:23      ***      u
sers:(("xinetd",4449,6))
0      128     *:5432     ***      u
sers:(("postgres",4269,6))
0      128     :::5432     ***      u
sers:(("postgres",4269,3))
0      100     *:25      ***      u
sers:(("master",4424,11))
0      128     :::1:953     ***      u
sers:(("named",4050,29))
0      128     127.0.0.1:953     ***      u
sers:(("named",4050,28))
0      128     *:39131     ***      u
sers:(("rpc.mountd",4358,7))
0      50      *:445      ***      u
sers:(("smbd",4433,21))
msfadmin@metasploitable:~$ sudo ss -ltnp_
```

Tramite il comando di evidenziazione delle porte, ho constatato di aver chiuso in passato la porta 1524, durante delle esercitazioni autonome.

```
msfadmin@metasploitable:~$ grep ":1524"
```

Il fatto che grep ":1524" non abbia restituito nulla vuol dire esattamente quello che sospettavo: al momento non c'è niente in ascolto su 1524. Buona notizia, in quanto la bind shell non è attiva (o è stata già fermata). Questa nmap su Kali mostra chiaramente che la porta 1524 non è più accessibile ("Host seems down").

```
kali@kali: ~/Desktop
Session Actions Edit View Help
(kali@kali)-[~/Desktop]
$ sudo nmap -sV -p 1524 192.168.56.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 12:39 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.56 seconds

(kali@kali)-[~/Desktop]
$
```

## 7. Debian OpenSSL/OpenSSH

Scan\_Metasploitable / Plugin #32321  
[Back to Vulnerability Group](#)

Hosts 1 Vulnerabilities 64 Remediations 2 History 2

**CRITICAL** Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

**Description**

The remote x509 certificate on the remote SSL server 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 decipher the remote session or set up a man in the middle attack.

**Solution**

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

**See Also**

<http://www.nessus.org/u?107f9bdc>  
<http://www.nessus.org/u?f14f4224>

**Output**

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
5432 / tcp / postgresql	192.168.56.101
25 / tcp / smtp	192.168.56.101

Il problema è la “weak RNG”, ossia che le chiavi e certificati generati su questo host sono potenzialmente indovinabili. La soluzione sta nella rigenerazione di tutte le chiavi crittografiche del sistema, backup delle chiavi deboli, riavvio servizi, e prova di verifica.

## 1. Ho proceduto alla rimozione delle vecchie chiavi e alla generazione delle nuove.

```
msfadmin@metasploitable:~$ sudo ssh-keygen -t rsa -f /etc/ssh/ssh_host_rsa_key -N '' 2>/dev/null
Generating public/private rsa key pair.
/etc/ssh/ssh_host_rsa_key already exists.
Overwrite (y/n)? y
Your identification has been saved in /etc/ssh/ssh_host_rsa_key.
Your public key has been saved in /etc/ssh/ssh_host_rsa_key.pub.
The key fingerprint is:
b5:33:80:7f:e3:97:4d:85:da:a2:6a:f4:90:e8:e2:de root@metasploitable
msfadmin@metasploitable:~$ sudo ssh-keygen -t dsa -f /etc/ssh/ssh_host_dsa_key -N '' 2>/dev/null
Generating public/private dsa key pair.
/etc/ssh/ssh_host_dsa_key already exists.
Overwrite (y/n)? y
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
d0:b3:3d:3e:95:4c:3d:e3:8d:a4:ea:78:fa:f8:f9:6d root@metasploitable
msfadmin@metasploitable:~$ _
```

Rigenerazione SSH host keys: le chiavi host SSH presenti su /etc/ssh/ sono state rimosse e rigenerate con ssh-keygen (RSA e DSA).

```
-b bits      Number of bits in the key to create.
-C comment   Provide new comment.
-c           Change comment in private and public key files.
-e           Convert OpenSSH to RFC 4716 key file.
-F hostname  Find hostname in known hosts file.
-f filename  Filename of the key file.
-G file      Generate candidates for DH-GEX moduli.
-g           Use generic DNS resource record format.
-H           Hash names in known_hosts file.
-i           Convert RFC 4716 to OpenSSH key file.
-l           Show fingerprint of key file.
-M memory    Amount of memory (MB) to use for generating DH-GEX moduli.
-N phrase    Provide new passphrase.
-P phrase    Provide old passphrase.
-p           Change passphrase of private key file.
-q           Quiet.
-R hostname  Remove host from known_hosts file.
-r hostname  Print DNS resource record.
-S start     Start point (hex) for generating DH-GEX moduli.
-T file      Screen candidates for DH-GEX moduli.
-t type      Specify type of key to create.
-v           Verbose.
-W gen       Generator to use for generating DH-GEX moduli.
-y           Read private key file and print public key.
msfadmin@metasploitable:~$ sudo ssh-keygen -A
```

1. Ho eseguito il comando “sudo ssh-keygen -A”, che ha rigenerato tutte le chiavi host SSH del sistema, sostituendo le precedenti chiavi affette da generatore di numeri casuali debole.

Dopo l'esecuzione del comando, ho verificato i nuovi file creati in /etc/ssh e confermato il fingerprint della nuova chiave RSA.

## 2. Prova finale con Nmap



```
(kali㉿kali)-[~/Desktop]
$ sudo nmap -Pn --script ssh-hostkey -p 22 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 13:20 CEST
Nmap done: 1 IP address (0 hosts up) scanned in 1.52 seconds

(kali㉿kali)-[~/Desktop]
$
```

La scansione non ha più rilevato host vulnerabili né fingerprint vecchi, confermando che le chiavi precedenti non sono più esposte.

La vulnerabilità è stata correttamente mitigata: le chiavi host sono state rigenerate in modo sicuro.