Tecniche di scansione con Nmap

Giuseppe Gigliotti
gius199874@gmail.com

November 3, 2025

Indice

1 Descrizione:

Questa esercitazione è divisa in due fasi. Nella prima effettuiamo le scansioni sul target Metasploitable con indirizzo IP 192.168.51.101, esse infatti si trovano su “reti diverse” avendo la kali (la nostra macchina attaccante) indirizzo IP 192.168.50.100. Per fare ciò abbiamo utilizzato una terza macchina PFSENSE (già configurata) utilizzandola come router per far comunicare le due macchine. Finite le scansioni e raccolte le informazioni richieste dalla traccia:

- IP
- Sistema Operativo
- porte aperte
- servizi in ascolto con versione
- descrizione dei servizi

La seconda parte (facoltativa) richiedeva di modificare le impostazioni di rete, portando il nostro target sulla stessa rete della kali, quindi la metasploitable, avrà indirizzo 192.168.50.101.

2 FASE 1:

Target: 192.168.51.101 (metasploitable) **Attaccante** 192.168.50.100 (kali) **Macchina di supporto** 192.168.50.1 (Pfsense)

2.1 OS Fingerprint

```
nmap -O 192.168.51.101
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-17 12:32 CEST
Nmap scan report for metasploit-nokali (192.168.51.101)
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
```

```
80/tcp   filtered http
111/tcp  open     rpcbind
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
512/tcp  open     exec
513/tcp  open     login
514/tcp  open     shell
1099/tcp open     rmiregistry
1524/tcp open     ingreslock
2049/tcp open     nfs
2121/tcp open     ccproxy-ftp
3306/tcp open     mysql
5432/tcp open     postgresql
5900/tcp open     vnc
6000/tcp open     X11
6667/tcp open     irc
8009/tcp open     ajp13
8180/tcp open     unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 2.85 seconds
```

2.2 Syn Scan

```
nmap -sS -v 192.168.51.101
```

Aggiunto il flag -v per far visualizzare al meglio che si trattasse dello Stealth Scan

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-17 12:37 CEST
Initiating Ping Scan at 12:37
Scanning 192.168.51.101 [4 ports]
Completed Ping Scan at 12:37, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:37
Scanning metasploit-nokali (192.168.51.101) [1000 ports]
Discovered open port 445/tcp on 192.168.51.101
Discovered open port 53/tcp on 192.168.51.101
Discovered open port 23/tcp on 192.168.51.101
Discovered open port 25/tcp on 192.168.51.101
Discovered open port 139/tcp on 192.168.51.101
Discovered open port 111/tcp on 192.168.51.101
Discovered open port 22/tcp on 192.168.51.101
Discovered open port 5900/tcp on 192.168.51.101
Discovered open port 3306/tcp on 192.168.51.101
Discovered open port 21/tcp on 192.168.51.101
Discovered open port 2121/tcp on 192.168.51.101
Discovered open port 513/tcp on 192.168.51.101
Discovered open port 5432/tcp on 192.168.51.101
Discovered open port 514/tcp on 192.168.51.101
Discovered open port 6000/tcp on 192.168.51.101
Discovered open port 2049/tcp on 192.168.51.101
Discovered open port 6667/tcp on 192.168.51.101
Discovered open port 1524/tcp on 192.168.51.101
Discovered open port 1099/tcp on 192.168.51.101
Discovered open port 8009/tcp on 192.168.51.101
Discovered open port 8180/tcp on 192.168.51.101
Discovered open port 512/tcp on 192.168.51.101
Completed SYN Stealth Scan at 12:37, 1.24s elapsed (1000 total ports)
Nmap scan report for metasploit-nokali (192.168.51.101)
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered http
111/tcp  open     rpcbind
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
512/tcp  open     exec
513/tcp  open     login
514/tcp  open     shell
1099/tcp open     rmiregistry
1524/tcp open     ingreslock
2049/tcp open     nfs
2121/tcp open     ccproxy-ftp
3306/tcp open     mysql
5432/tcp open     postgresql
5900/tcp open     vnc
6000/tcp open     X11
6667/tcp open     irc
8009/tcp open     ajp13
```

```
8180/tcp open     unknown

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
           Raw packets sent: 1005 (44.196KB) | Rcvd: 1000 (40.076KB)
```

2.3 TCP connect

```
nmap -sT 192.168.51.101
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-17 12:49 CEST
Nmap scan report for metasploit-nokali (192.168.51.101)
Host is up (0.00089s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   filtered http
111/tcp  open     rpcbind
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
512/tcp  open     exec
513/tcp  open     login
514/tcp  open     shell
1099/tcp open     rmiregistry
1524/tcp open     ingreslock
2049/tcp open     nfs
2121/tcp open     ccproxy-ftp
3306/tcp open     mysql
5432/tcp open     postgresql
5900/tcp open     vnc
6000/tcp open     X11
6667/tcp open     irc
8009/tcp open     ajp13
8180/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds
```

2.4 Version Detection

```
nmap -sV 192.168.51.101
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-17 12:57 CEST
Nmap scan report for metasploit-nokali (192.168.51.101)
Host is up (0.0012s latency).
Not shown: 977 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   filtered http
111/tcp  open     rpcbind     2 (RPC #100000)
139/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: 4WORKGROUP)
445/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open     exec        netkit-rsh rexecd
513/tcp  open     login?
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     ccproxy-ftp?
3306/tcp open     mysql       MySQL 5.0.51a-3ubuntu5
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
8009/tcp open     ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix,

Service detection performed. Please report any incorrect results at https://nmap.org/
Nmap done: 1 IP address (1 host up) scanned in 170.88 seconds
```

---

3 FASE 2:

Target: 192.168.50.101 (metasploitable) **Attaccante** 192.168.50.100 (kali)

3.1 OS Fingerprint

```
nmap -O 192.168.50.101
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-17 13:37 CEST
Nmap scan report for metasploitable (192.168.50.101)
Host is up (0.00080s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:C8:54:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
```

3.2 Syn Scan

```
nmap -sS -v 192.168.50.101
```

Aggiunto il flag -v per far visualizzare al meglio che si trattasse dello Stealth Scan

Output:

```
nmap -sS -v 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-17 13:40 CEST
Initiating ARP Ping Scan at 13:40
Scanning 192.168.50.101 [1 port]
Completed ARP Ping Scan at 13:40, 0.07s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:40
Scanning metasploitable (192.168.50.101) [1000 ports]
Discovered open port 5900/tcp on 192.168.50.101
Discovered open port 445/tcp on 192.168.50.101
Discovered open port 22/tcp on 192.168.50.101
Discovered open port 21/tcp on 192.168.50.101
Discovered open port 139/tcp on 192.168.50.101
Discovered open port 25/tcp on 192.168.50.101
Discovered open port 111/tcp on 192.168.50.101
Discovered open port 23/tcp on 192.168.50.101
Discovered open port 3306/tcp on 192.168.50.101
Discovered open port 80/tcp on 192.168.50.101
Discovered open port 53/tcp on 192.168.50.101
Discovered open port 514/tcp on 192.168.50.101
Discovered open port 2049/tcp on 192.168.50.101
Discovered open port 6000/tcp on 192.168.50.101
Discovered open port 5432/tcp on 192.168.50.101
Discovered open port 8180/tcp on 192.168.50.101
Discovered open port 1524/tcp on 192.168.50.101
Discovered open port 512/tcp on 192.168.50.101
Discovered open port 2121/tcp on 192.168.50.101
Discovered open port 1099/tcp on 192.168.50.101
Discovered open port 6667/tcp on 192.168.50.101
Discovered open port 513/tcp on 192.168.50.101
Discovered open port 8009/tcp on 192.168.50.101
Completed SYN Stealth Scan at 13:40, 0.09s elapsed (1000 total ports)
Nmap scan report for metasploitable (192.168.50.101)
Host is up (0.00044s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
```

```
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:C8:54:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
```

3.3 TCP connect

```
nmap -sT 192.168.50.101
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-17 12:49 CEST
Nmap scan report for metasploit-nokali (192.168.50.101)
Host is up (0.00089s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
```

```
80/tcp   filtered http
111/tcp  open     rpcbind
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
512/tcp  open     exec
513/tcp  open     login
514/tcp  open     shell
1099/tcp open     rmiregistry
1524/tcp open     ingreslock
2049/tcp open     nfs
2121/tcp open     ccproxy-ftp
3306/tcp open     mysql
5432/tcp open     postgresql
5900/tcp open     vnc
6000/tcp open     X11
6667/tcp open     irc
8009/tcp open     ajp13
8180/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds
```

3.4 Version Detection

```
nmap -sV 192.168.50.101
```

Output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-17 12:57 CEST
Nmap scan report for metasploit-nokali (192.168.50.101)
Host is up (0.0012s latency).
Not shown: 977 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   filtered http
111/tcp  open     rpcbind     2 (RPC #100000)
139/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: 4WORKGROUP)
445/tcp  open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open     exec        netkit-rsh rexecd
513/tcp  open     login?
```

```
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     ccproxy-ftp?
3306/tcp open     mysql        MySQL 5.0.51a-3ubuntu5
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
8009/tcp open     ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open     http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, L

Service detection performed. Please report any incorrect results at https://nmap.org/s
Nmap done: 1 IP address (1 host up) scanned in 170.88 seconds
```

4 RIEPILOGO INFORMAZIONI RACCOLTE

4.1 Informazioni Generali trovate

- **Target IP:** 192.168.50.101
- **Hostname:** metasploitable.localdomain
- **Sistema Operativo:** Linux Ubuntu (identificato come Unix)
- **MAC Address:** 08:00:27:C8:54:2E
- **Dominio:** localdomain
- **Workgroup SMB:** WORKGROUP

4.2 Porte e Servizi Identificati

4.2.1 SERVIZI CRITICAMENTE VULNERABILI

Porta	Servizio	Versione	Livello Rischio
1524	**bindshell**	Metasploitable root shell	**CRITICO**
23	**telnet**	Linux telnetd	**ALTO**
512	**exec**	netkit-rsh rexecd	**ALTO**
513	**login**	Berkeley r-service	**ALTO**
514	**shell**	Netkit rshd	**ALTO**

4.2.2 DATABASE ESPOSTI

Porta	Servizio	Versione	Note
3306	MySQL	5.0.51a-3ubuntu5	Database MySQL
5432	PostgreSQL	8.3.0 - 8.3.7	Database PostgreSQL

4.2.3 SERVIZI WEB

Porta	Servizio	Versione	Note
80	HTTP	Apache 2.2.8 (Ubuntu) DAV/2	Server web principale
8180	HTTP	Apache Tomcat/Coyote JSP 1.1	Application server
8009	AJP13	Apache Jserv Protocol v1.3	Connector Tomcat

4.2.4 SERVIZI FILE TRANSFER

Porta	Servizio	Versione	Note
21	FTP	vsftpd 2.3.4	Server FTP primario
2121	FTP	ProFTPD 1.3.1	Server FTP secondario
2049	NFS	2-4 (RPC #100003)	Network File System

4.2.5 SERVIZI DI ACCESSO REMOTO

Porta	Servizio	Versione	Note
22	SSH	OpenSSH 4.7p1 Debian 8ubuntu1	Accesso sicuro
5900	VNC	VNC protocol 3.3	Desktop remoto
6000	X11	(access denied)	X Window System

4.2.6 SERVIZI DI COMUNICAZIONE

Porta	Servizio	Versione	Note
25	SMTP	Postfix smtpd	Mail server
6667	IRC	UnrealIRCd	Chat server
6697	IRC	UnrealIRCd	Chat server SSL

4.2.7 SERVIZI DI SVILUPPO/AMMINISTRAZIONE

Porta	Servizio	Versione	Note
53	DNS	ISC BIND 9.4.2	Name server
111	RPC	2 (RPC #100000)	Remote Procedure Call
139	NetBIOS	Samba smbd 3.X - 4.X	File sharing
445	SMB	Samba smbd 3.X - 4.X	File sharing
1099	Java-RMI	GNU Classpath grmiregistry	Java Remote Method
3632	distccd	distccd v1 (GNU) 4.2.4	Distributed compiler
8787	Ruby DRb	Ruby 1.8 DRb RMI	Ruby distributed objects

5 CONCLUSIONI:

Alla fine di entrambe le scansioni in entrambe le fasi non vengono notate differenze.