Report di Scansione Nmap

1. Obbiettivo

Effettuare le seguenti scansioni sul target Metasploitable e su reti differenti, facoltativamente ripetere le scansione con il target nella stessa rete attaccante.

- Scenario Iniziale: Target e Attaccante su reti differenti.
- Scenario Facoltativo: Target e Attaccante su stessa rete.

2. Configurazione dell' Ambiente

2.1 Ambiente di Rete

- Macchina Firewall:
- Sistema operativo: pfSense - CE
- RETE LAN: 192.168.50.0/24
- RETE DMZ: 192.168.51.0/24 (RETE DIFFERENTE)
- DNS: epic-pfsense.epicode

LAN	↑	autoselect	192.168.50.1
DMZ	↑	autoselect	192.168.51.1

- Macchina Attaccante:
- Sistema operativo: Kali Linux
- IP: 192.168.50.100
- DNS: epic-kali.epicode

- Macchina Target:
- Sistema operativo: Metasploitable - Linux
- IP LAN: 192.168.50.101
- IP DMZ: 192.168.51.101 (RETE DIFFERENTE)
- DNS: epic-metasploitable.epicode

2.2 Strumenti Utilizzati

- Nmap v7.95
- Virtualizzazione: Vmware ESXi

3. Scansioni Effettuate e Risultati

3.1 OS Fingerprint

Comandi utilizzati:

nmap -O 192.168.51.101 (RETE DIFFERENTE)

```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 16:34 CET
Nmap scan report for 192.168.51.101
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
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
it/ .
Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds
```

nmap -O 192.168.50.101 (STESSA RETE)

```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 16:56 CET
Nmap scan report for Epic-Metasploitable.epicode (192.168.50.101)
Host is up (0.00025s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
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: 00:0C:29:F9:38:77 (VMware)
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 htt
it/ .
Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```

Differenze:

- Rete Differente:
  1. OS Fingerprint meno accurato
  2. Trova anche la porta 53 (DNS Server)
  3. Si notano 2 hop (essendo in rete differente)

- Stessa Rete:
  1. Scopre il MAC
  2. OS Fingerprint piu accurato rispetto a una rete differente.

Il resto dei risultati sono uguali.

3.2 SYN Scan

Comandi utilizzati:

nmap -sS -p- 192.168.51.101 (RETE DIFFERENTE)

```
┌──(root㉿kali)-[~]
└─# nmap -sS -p- 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 16:36 CET
Nmap scan report for 192.168.51.101
Host is up (0.00035s latency).
Not shown: 65505 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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
37801/tcp open  unknown
44257/tcp open  unknown
48183/tcp open  unknown
48966/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.51 seconds
```

nmap -sS -p- 192.168.50.101 (STESSA RETE)

```
┌──(root㉿kali)-[~]
└─# nmap -sS -p- 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 17:05 CET
Nmap scan report for Epic-Metasploitable.epicode (192.168.50.101)
Host is up (0.00035s latency).
Not shown: 65505 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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
33332/tcp open  unknown
34836/tcp open  unknown
37559/tcp open  unknown
54830/tcp open  unknown
MAC Address: 00:0C:29:F9:38:77 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.53 seconds
```

Differenze: TRA UNA RETE E L'ALTRA, LE ULTIME 4 PORTE SONO DIFFERENTI)

- Rete Differente: 1. Ultime 4 porte: 37 801, 44 257, 48 183, 48 966.

- Stessa Rete: 1. Ultime 4 porte: 33 332, 34 836, 37 559, 54 830.

Il resto dei risultati sono uguali.

3.3 TCP Connect Scan

Comando utilizzato:

nmap -sT -p- 192.168.51.101 (RETE DIFFERENTE)

```
┌──(root㉿kali)-[~]
└─# nmap -sT -p- 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 16:41 CET
Nmap scan report for 192.168.51.101
Host is up (0.00046s latency).
Not shown: 65505 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    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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
37801/tcp open  unknown
44257/tcp open  unknown
48183/tcp open  unknown
48966/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 3.69 seconds
```

nmap -sT -p- 192.168.50.101 (STESSA RETE)

```
┌──(root㉿kali)-[~]
└─# nmap -sT -p- 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 17:10 CET
Nmap scan report for Epic-Metasploitable.epicode (192.168.50.101)
Host is up (0.00036s latency).
Not shown: 65505 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    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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
33332/tcp open  unknown
34836/tcp open  unknown
37559/tcp open  unknown
54830/tcp open  unknown
MAC Address: 00:0C:29:F9:38:77 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.50 seconds
```

Differenze:

1. Anche qui le ultime 4 porte cambiano

3.4 Version Detection

Comandi utilizzati:

nmap -sV -p- 192.168.51.101 (RETE DIFFERENTE)

```
┌──(root㉿kali)-[~]
└─# nmap -sV -p- 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 16:42 CET
Nmap scan report for 192.168.51.101
Host is up (0.00041s 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 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
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  unknown
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
37801/tcp open  java-rmi     GNU Classpath grmiregistry
44257/tcp open  status       1 (RPC #100024)
48183/tcp open  nlockmgr     1-4 (RPC #100021)
48966/tcp open  mountd       1-3 (RPC #100005)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Uni
 Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.o
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 175.16 seconds
```

nmap -sV -p- 192.168.50.101 (STESSA RETE)

```
┌──(root㉿kali)-[~]
└─# nmap -sV -p- 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 17:13 CET
Nmap scan report for Epic-Metasploitable.epicode (192.168.50.101)
Host is up (0.00039s 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 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  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/drb)
33332/tcp open  java-rmi     GNU Classpath grmiregistry
34836/tcp open  mountd       1-3 (RPC #100005)
37559/tcp open  status       1 (RPC #100024)
54830/tcp open  nlockmgr     1-4 (RPC #100021)
MAC Address: 00:0C:29:F9:38:77 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Un
 Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 151.05 seconds
```

Differenze:

1. Nella rete Interna si scopre il servizio FTP **ProFTPD 1.3.1** sulla porta 2121
2. Anche qui le ultime porte sono differenti
3. Tempo di scansione diverso, la rete interna rivolve prima, dovendo usare un solo hop.

5. Conclusioni

Sintesi dei risultati:

- La SYN scan è risultata più veloce e stealth rispetto alla TCP connect.
- Le configurazioni di rete hanno avuto un impatto sui risultati hop e tempistihe di scan.
- Le ultime 4 porte esposte di Metasploitable cambiano in rete differente e stessa rete.

Francsesco Rinaldi