

Report di Scansione con Nmap

1. Introduzione

L'obiettivo di questo report è analizzare i risultati delle scansioni Nmap effettuate su un sistema target (Metasploitable) utilizzando diverse tecniche. Le scansioni mirano a raccogliere informazioni sui servizi attivi, porte aperte, sistema operativo e versioni dei software in esecuzione. Le configurazioni di rete includono:

- **Scenario iniziale:** target e attaccante su due reti diverse.
- **Scenario facoltativo:** target e attaccante sulla stessa rete.

2. Configurazione dell' Ambiente

2.1 Ambiente di Rete

- Macchina Firewall:



- Sistema operativo: pfSense - CE
- RETE 1: 192.168.50.0/24
- RETE 2: 192.168.51.0/24
- DNS: epic-pfsense.epicode

- Macchina Attaccante:

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

- Macchina Target:

- Sistema operativo: Metasploitable - Linux
- IP: 192.168.51.101
- IP Stessa rete: 192.168.50.101
- DNS: epic-metasploitable.epicode

 LAN	↑	autoselect	192.168.50.1
 DMZ	↑	autoselect	192.168.51.1

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_
link/ether 00:0c:29:f9:38:77 brd ff
inet 192.168.51.101/24 brd 192.168.
inet6 fe80::20c:29ff:fe9:3877/64 s
valid_lft forever preferred_lft
eth1: <BROADCAST,MULTICAST,UP,LOWER_
link/ether 00:0c:29:f9:38:81 brd ff
inet 192.168.50.101/24 brd 192.168.
inet6 fe80::20c:29ff:fe9:3881/64 s
valid_lft forever preferred_lft
```

Figura 1: Schede Metasploitable

2.2 Strumenti Utilizzati

- Nmap v7.95
- Virtualizzazione: Vmware ESXi

3. Scansioni Effettuate e Risultati

3.1 OS Fingerprint

Comandi utilizzati:

`nmap -O 192.168.50.101`

```
(root@kali)-[/home/kali]
# nmap -O 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org )
Nmap scan report for 192.168.50.101
Host is up (0.00020s 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: 00:0C:29:F9:38:81 (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
```

`nmap -O 192.168.51.101`

```
(root@kali)-[/home/kali]
# nmap -O 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-1
Nmap scan report for Epic-Metasploitable.epicode (192.168.51.101)
Host is up (0.00035s 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
```

Differenze:

1. La scansione nella stessa rete scopre il Mac Address, ha una latenza inferiore, un tempo di scansione inferiore, 1 solo hop e l'OS Fingerprint è più accurato
2. Sulla stessa rete c'è una latenza inferiore
3. Sulla stessa rete troviamo 1 solo hop, rispetto ai 2 hop della rete 51.0
4. Il tempo di scansione varia, nella stessa rete è più veloce
5. La rete differente risolve il DNS

3.2 SYN Scan

Comandi utilizzati:

nmap -sS -p- 192.168.50.101 (Stessa Rete)

```
(root@kali)-[/home/kali]
# nmap -sS -p- 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 21:45
Nmap scan report for 192.168.50.101
Host is up (0.00037s 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
46260/tcp open  unknown
48348/tcp open  unknown
54350/tcp open  unknown
60066/tcp open  unknown
MAC Address: 00:0C:29:F9:38:81 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.63 seconds
```

nmap -sS -p- 192.168.51.101 (Rete Differente)

```
(root@kali)-[/home/kali]
# nmap -sS -p- 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 21:45
Nmap scan report for Epic-Metasploitable.epicode (192.168.5
Host is up (0.00040s 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
46260/tcp open  unknown
48348/tcp open  unknown
54350/tcp open  unknown
60066/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 3.76 seconds
```

Differenze:

1. Durata Scansione Differente
3. Trovate 30 porte aperte
4. Nella stessa rete si scopre il MAC

3.3 TCP Connect Scan

Comando utilizzato:

```
nmap -sT -p- 192.168.50.101
```

```
(root@kali)~[/home/kali]
# nmap -sT -p- 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-20 10:00:00
Nmap scan report for 192.168.50.101
Host is up (0.00037s 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
46260/tcp open  unknown
48348/tcp open  unknown
54350/tcp open  unknown
60066/tcp open  unknown
MAC Address: 00:0C:29:F9:38:81 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.54 s
```

```
nmap -sT -p- 192.168.51.101
```

```
(root@kali)~[/home/kali]
# nmap -sT -p- 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-20 10:00:00
Nmap scan report for Epic-Metasploitable.epicode (192.168.51.101)
Host is up (0.00052s 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
46260/tcp open  unknown
48348/tcp open  unknown
54350/tcp open  unknown
60066/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 3.71 s
```

Differenze:

1. Con la scansione TCP si ricevono le stesse porte aperte per entrambi le reti, Incluse le ULTIME 4 Porte
2. Tempi di scansione differenti
3. Mac Address

3.4 Version Detection

Comandi utilizzati:

nmap -sV -p- 192.168.51.101

nmap -sV -p- 192.168.51.101

```
(root@kali)-[/home/kali]
# nmap -sV -p- 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 22:06 CET
Nmap scan report for 192.168.51.101
Host is up (0.00034s 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/drbb)
46260/tcp open  mountd       1-3 (RPC #100005)
48348/tcp open  nlockmgr     1-4 (RPC #100021)
54350/tcp open  java-rmi     GNU Classpath grmiregistry
60066/tcp open  status       1 (RPC #100024)
MAC Address: 00:0C:29:F9:38:81 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix; o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 150.99 seconds
```

```
(root@kali)-[/home/kali]
# nmap -sV -p- 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 22:10 CET
Nmap scan report for Epic-Metasploitable.epicode (192.168.51.101)
Host is up (0.00060s 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  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
46260/tcp open  mountd       1-3 (RPC #100005)
48348/tcp open  nlockmgr     1-4 (RPC #100021)
54350/tcp open  java-rmi     GNU Classpath grmiregistry
60066/tcp open  status       1 (RPC #100024)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix; o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 175.17 seconds
```

Differenze:

1. Nella rete Interna si scopre il servizio FTP **ProFTPD 1.3.1** sulla porta 2121
2. Tempi di scansione differenti
3. Mac Address

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 tempistiche di scan.

Considerazioni finali:

- In scenari reali, la scelta della tecnica e della configurazione di rete può influenzare l'efficacia delle scansioni.
- L'importanza di considerare restrizioni di rete e firewall nel planning delle scansioni.