

Scansione dei servizi con Nmap – Pratica S5/L2

1. Introduzione

L'esercitazione ha avuto come obiettivo l'analisi dei servizi esposti da sistemi target mediante l'utilizzo dello strumento Nmap, al fine di identificare il sistema operativo, le porte aperte e i servizi in ascolto. L'attività si colloca nella fase di reconnaissance e service enumeration di un penetration test.

2. Ambiente di laboratorio

L'ambiente di laboratorio è stato realizzato su piattaforma **Oracle VirtualBox** e comprende più macchine virtuali configurate all'interno di un contesto di rete controllato.

La macchina **Kali Linux** è utilizzata per l'esecuzione delle attività di scansione, mentre **Metasploitable2** e una macchina virtuale **Windows** rappresentano i sistemi target oggetto dell'esercitazione. È inoltre presente un sistema **pfSense**, mantenuto da un precedente laboratorio e utilizzato esclusivamente come router per consentire alla macchina Kali Linux l'accesso a Internet; tale sistema non è coinvolto nelle attività di scansione previste dall'esercitazione.

Le macchine virtuali risultano configurate all'interno dello stesso segmento di rete locale, consentendo la comunicazione tra Kali Linux e i sistemi target.

Configurazione di rete e indirizzamento IP

Sistema	Indirizzo IP	Subnet
Kali Linux	192.168.50.151	/24
Metasploitable2	192.168.50.101	/24
Windows 10	192.168.50.153	/24
Pfsense	192.168.50.1	/24

3. Attività di scansione

Le attività di scansione sono state effettuate utilizzando lo strumento **Nmap**, applicando differenti tecniche con l'obiettivo di identificare il sistema operativo dei target, le porte aperte e i servizi in ascolto.

Le scansioni sono state eseguite dalla macchina Kali Linux nei confronti dei sistemi target presenti nel segmento di rete locale.

Le tecniche adottate includono:

- OS Fingerprinting
- SYN Scan
- TCP Connect Scan
- Version Detection

Nei paragrafi seguenti vengono descritti i comandi utilizzati e i risultati ottenuti per ciascun target.

3.1 OS Fingerprinting – Target Metasploitable2

Per l'identificazione del sistema operativo del target Metasploitable2 è stata utilizzata la funzionalità di **OS fingerprinting** di Nmap, che consente di stimare il sistema operativo analizzando il comportamento dello stack TCP/IP del target.

Il comando utilizzato è il seguente:

```
sudo nmap -O 192.168.50.101
```

Di seguito è riportato l'output ottenuto dall'esecuzione del comando sulla macchina Kali Linux:

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-11 17:57 EST
Nmap scan report for 192.168.50.101
Host is up (0.00061s 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:D6:14:8D (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 2.01 seconds
```

Dall'analisi dell'output è possibile stimare che il sistema operativo del target sia un **Linux con kernel 2.6.x**, con un intervallo di versione compreso tra **2.6.9** e **2.6.33**. L'identificazione è basata su tecniche di fingerprinting attivo e deve essere considerata una stima probabilistica.

Il comando utilizzato è il seguente:

```
sudo nmap -sS 192.168.50.101
```

Di seguito è riportato l'output ottenuto dall'esecuzione del comando sulla macchina Kali Linux:

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-11 19:27 EST
Nmap scan report for 192.168.50.101
Host is up (0.000075s 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:D6:14:8D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

La scansione ha evidenziato la presenza di numerose porte TCP aperte e relativi servizi in ascolto, confermando l'ampia superficie di attacco del sistema Metasploitable2.

L'utilizzo della SYN scan consente di ottenere tali informazioni senza completare il three-way handshake TCP, rendendo la tecnica meno invasiva e più discreta rispetto a una TCP Connect scan.

3.3 TCP Connect Scan – Target Metasploitable2

Al fine di confrontare i risultati ottenuti con la SYN scan, è stata eseguita una **TCP Connect Scan**, tecnica che utilizza la chiamata di sistema `connect()` per stabilire una connessione TCP completa con il target.

Il comando utilizzato è il seguente:

```
sudo nmap -sT 192.168.50.101
```

Di seguito è riportato l'output ottenuto dall'esecuzione del comando sulla macchina Kali Linux:

```
(kali@kali)~[~]
$ sudo nmap -sT 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-11 20:11 EST
Nmap scan report for 192.168.50.101
Host is up (0.00064s 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    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:D6:14:8D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

La TCP Connect scan ha restituito un elenco di porte aperte e servizi in ascolto sovrapponibile a quanto rilevato tramite SYN scan. La differenza principale risiede nel comportamento della scansione, che in questo caso completa il **three-way handshake TCP**, risultando più invasiva e maggiormente rilevabile dal sistema target.

Confronto tra SYN Scan e TCP Connect Scan

I risultati ottenuti tramite TCP Connect scan risultano **coerenti e sovrapponibili** a quelli emersi dalla precedente SYN scan in termini di porte aperte e servizi individuati. Tuttavia, le due tecniche presentano differenze significative dal punto di vista operativo: mentre la **SYN scan non completa il three-way handshake TCP** e risulta quindi più discreta e meno facilmente rilevabile, la **TCP Connect scan stabilisce una connessione completa con il target**, rendendola più invasiva e maggiormente soggetta a logging.

La scelta tra le due tecniche dipende dal contesto operativo e dal livello di privilegio disponibile sul sistema di scansione.

3.4 Version Detection – Target Metasploitable2

Per identificare i servizi in ascolto e le relative versioni applicative sul target Metasploitable2 è stata eseguita una **Version Detection**, tecnica che consente a Nmap di interrogare attivamente i servizi individuati sulle porte aperte e di analizzarne i banner di risposta.

Il comando utilizzato è il seguente:

```
sudo nmap -sV 192.168.50.101
```

Di seguito è riportato l'output ottenuto dall'esecuzione del comando sulla macchina Kali Linux:

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-11 20:46 EST
Nmap scan report for 192.168.50.101
Host is up (0.000074s 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    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  tcpwrapped
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
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?
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:D6:14:8D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 144.42 seconds
```


La Version Detection ha consentito di identificare in modo dettagliato i servizi in esecuzione e le relative versioni software, evidenziando la presenza di numerosi servizi obsoleti e intenzionalmente vulnerabili. Le informazioni ottenute risultano particolarmente rilevanti in quanto permettono di correlare i servizi individuati a potenziali vulnerabilità note, rappresentando un passaggio fondamentale per le successive fasi di vulnerability assessment.

3.5 OS Fingerprinting – Target Windows

Per l'identificazione del sistema operativo del target Windows è stata eseguita una scansione di **OS fingerprinting** tramite Nmap, al fine di stimare il sistema operativo in esecuzione analizzando il comportamento dello stack TCP/IP.

Il comando utilizzato è il seguente:

```
sudo nmap -O 192.168.50.153
```

Di seguito è riportato l'output ottenuto dall'esecuzione del comando sulla macchina Kali Linux:

```
(kali@kali)-[~]
└─$ sudo nmap -O 192.168.50.153
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-12 21:43 EST
Nmap scan report for 192.168.50.153
Host is up (0.00083s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:77:1B:C9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 2.92 seconds
```

L'OS fingerprinting ha consentito di identificare il sistema target come **Microsoft Windows 10**, con una stima di versione compresa tra **1507** e **1607**.

Come per le precedenti scansioni, il risultato deve essere interpretato come una stima basata su tecniche di fingerprinting attivo, la cui accuratezza dipende dai servizi esposti e dalla configurazione del sistema.

4. Conclusioni

L'attività di laboratorio ha permesso di applicare le principali tecniche di scansione offerte da Nmap, consentendo l'identificazione dei sistemi operativi, delle porte aperte e dei servizi in ascolto sui target analizzati.

Le scansioni SYN e TCP Connect hanno prodotto risultati equivalenti in termini di porte rilevate, evidenziando come le differenze tra le tecniche siano principalmente di natura operativa.

La Version Detection ha fornito informazioni dettagliate sui servizi e sulle versioni applicative, risultando fondamentale per una corretta valutazione della superficie di attacco.