MAPPING NET & SERVICES

Nel Seguente report si affronteranno le **Tecniche di scansione con Nmap** sul target **Metasploitable**, con l'obiettivo di identificare sistema operativo, porte aperte e servizi esposti.
Le tecniche applicate consentono di analizzare la superficie d'attacco del sistema e di raccogliere informazioni utili per le successive fasi di valutazione della sicurezza.

6-JAN-26
CYBER SECURITY

AMIN EL KASSIMI
PAOLO RAMPINO

OS FINGERPRINT

In questa sezione si fara l'**Identificazione del Sistema Operativo:** Utile per capire quale sistema operativo è in esecuzione su un host remoto, il che può essere utile per la gestione della rete, la sicurezza e la pianificazione delle vulnerabilità.

"nmap -O"

Funzione:
Esegue una "OS Detection" (rilevazione del sistema operativo).

Descrizione:
Questo tipo di scansione tenta di determinare quale sistema operativo (e talvolta quale versione) è in esecuzione su un host remoto.

Come Funziona:
Nmap invia una serie di pacchetti specifici all'host di destinazione e analizza le risposte. La combinazione delle caratteristiche di queste risposte (come i tempi, i contenuti e i flag dei pacchetti TCP/IP) viene confrontata con un database di firme di sistemi operativi noti per identificare il sistema operativo del target.

In sintesi, la scansione mostra quattro cose fondamentali:

Prima: l'host è attivo e raggiungibile.
Nmap conferma che l'IP risponde e che la latenza è minima. È una macchina nella tua rete locale (1 hop), tipicamente una VM.
Seconda: **una quantità anomala di servizi in ascolto**.
Vedi **oltre 20 porte TCP aperte**, molte delle quali oggi sarebbero considerate radioattive:

- Servizi in chiaro e legacy: ftp (21), telnet (23), rsh/rlogin (512–514)
- Servizi di posta: smtp (25)
- Web: http (80)
- File sharing e RPC: rpcbind (111), nfs (2049)
- Windows services esposti su Linux: netbios (139), smb (445)
- Database senza restrizioni apparenti: mysql (3306), postgresql (5432)
- Servizi "esotici" e storicamente bucabili: distcc (3632), ingreslock (1524), vnc (5900), X11 (6000), irc (6667)

Seconda: **una quantità anomala di servizi in ascolto**.
Vedi **oltre 20 porte TCP aperte**, molte delle quali oggi sarebbero considerate radioattive:

- Servizi in chiaro e legacy: ftp (21), telnet (23), rsh/rlogin (512–514)
- Servizi di posta: smtp (25)
- Web: http (80)
- File sharing e RPC: rpcbind (111), nfs (2049)
- Windows services esposti su Linux: netbios (139), smb (445)
- Database senza restrizioni apparenti: mysql (3306), postgresql (5432)
- Servizi "esotici" e storicamente bucabili: distcc (3632), ingreslock (1524), vnc (5900), X11 (6000), irc (6667)

Terza: fingerprinting del sistema operativo riuscito.
Nmap identifica:

- **OS**: Linux
- **Kernel**: 2.6.x (range 2.6.9 – 2.6.33)
- **CPE**: cpe:/o:linux:linux_kernel:2.6

Quarta: contesto virtualizzato.
Il MAC address rivela una **VirtualBox NIC**, quindi sei quasi certamente davanti a una VM da laboratorio, non a un host reale esposto per errore.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -O 10.0.2.3
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-10 19:47 CET
Nmap scan report for 10.0.2.3
Host is up (0.0021s 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: 08:00:27:59:35:43 (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 1.73 seconds
```

SYN SCA

In questa sezione si effettua la **scansione delle porte TCP**: è utile per individuare quali servizi sono in ascolto su un host remoto, informazione fondamentale per l'analisi della superficie d'attacco e la valutazione della sicurezza.

"nmap -sS"

Funzione:
Esegue una **TCP SYN Scan** (scansione SYN, detta anche half-open).

Descrizione:
Questo tipo di scansione consente di determinare lo stato delle porte TCP senza stabilire una connessione completa con il target. È una delle tecniche di scansione più utilizzate perché rapida, affidabile e relativamente discreta.

Come Funziona:
Nmap invia un pacchetto **SYN** a ciascuna porta del sistema bersaglio, simulando l'inizio di una connessione TCP. In base alla risposta ricevuta, Nmap determina lo stato della porta:

- **SYN/ACK** → la porta è **open**
- **RST** → la porta è **closed**
- **Nessuna risposta / ICMP unreachable** → la porta è **filtered**

La connessione non viene mai completata, poiché Nmap non invia l'ACK finale del three-way handshake.

La scansione conferma che **l'host è attivo** (Host is up) con latenza molto bassa: sei sulla stessa rete, probabilmente una VM Metasploitable.

Nmap indica che **977 porte TCP sono chiuse** e rispondono con **RST**. Questo è importante: significa che il target risponde correttamente ai SYN, quindi non c'è un firewall che filtra aggressivamente il traffico TCP.

Sono state rilevate **numerose porte aperte**, ognuna associata a un servizio noto. In particolare:

- **Servizi di accesso remoto insicuri**:
  ftp (21), telnet (23), rsh/rlogin (512–514)
  Tutti trasmettono credenziali in chiaro.

- **Servizi di rete e file sharing**:
  rpcbind (111), nfs (2049), netbios (139), smb (445)
  Tipici bersagli per enumeration e accesso non autenticato su sistemi legacy.

- **Servizi web e applicativi**:
  http (80), ajp13 (8009), unknown (8180)
  Indicano la presenza di web server e servizi applicativi ausiliari.

- **Database esposti**:
  mysql (3306), postgresql (5432)
  Raramente dovrebbero essere accessibili senza restrizioni.

- **Servizi grafici e desktop remoto**:
  vnc (5900), X11 (6000)
  Estremamente pericolosi se non protetti.

- **Servizi vari e storicamente vulnerabili**:
  smtp (25), irc (6667), distcc (ingreslock 1524)

La presenza di così tanti servizi **aperti contemporaneamente** è un segnale inequivocabile di una macchina **intenzionalmente vulnerabile**, non di un sistema reale in produzione.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sS 10.0.2.3
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-17 12:41 CET
Nmap scan report for 10.0.2.3
Host is up (0.0031s 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: 08:00:27:59:35:43 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

DIFFERENZE TCP CONNECT E SYN

TCP connect su Metasploitable - come ci aspettavamo non ci sono differenze rispetto alla scansione SYN - l'unica differenza è nel metodo utilizzato per effettuare il check sulla porta.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sT 10.0.2.3
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-17 12:47 CET
Nmap scan report for 10.0.2.3
Host is up (0.011s 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: 08:00:27:59:35:43 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

VERSION DETECTION

In questa sezione si effettua l'**identificazione dei servizi e delle loro versioni**: è utile per capire **quale software è in esecuzione sulle porte aperte**, informazione fondamentale per l'analisi delle vulnerabilità e la pianificazione delle fasi successive del penetration test.

"nmap -sV"

Funzione:
Esegue la **rilevazione delle versioni dei servizi** (*service version detection*).

Descrizione:
L'opzione -sV permette a Nmap di identificare **il servizio in ascolto su una porta aperta e la sua versione**, andando oltre il semplice numero di porta.
Questa tecnica è una forma avanzata di **banner grabbing**, utile per associare i servizi individuati a vulnerabilità note.

Come funziona:
Dopo aver individuato le porte aperte, Nmap invia una serie di **probe specifiche** ai servizi in ascolto.
Le risposte ricevute vengono analizzate e confrontate con un **database di firme** per determinare:

- il tipo di servizio (es. Apache, OpenSSH, MySQL)
- la versione del software
- eventuali informazioni aggiuntive come protocollo o sistema operativo stimato

Il processo si basa sul comportamento del servizio e sui dati restituiti (banner, errori, risposte standard o non standard), consentendo a Nmap di fornire un'identificazione più accurata rispetto al semplice port scanning.

Nmap conferma di nuovo che l'host è attivo e che **977 porte TCP sono chiuse**. Fin qui nulla di nuovo. La differenza sta nel contenuto delle porte aperte: ora ogni servizio ha **nome e versione precisa**.

Per esempio:

- **FTP (21)** → vsftpd 2.3.4
  Versione famigerata: esiste un backdoor pubblico e ben documentato.

- **SSH (22)** → OpenSSH 4.7p1 Debian/Ubuntu
  Versione molto datata, utile per fingerprinting e attacchi mirati.

- **HTTP (80)** → Apache httpd 2.2.8 (Ubuntu)
  Web server legacy con moduli DAV attivi.

- **SMB (139/445)** → Samba smbd 3.X – 4.X
  Storicamente ricchissimo di vulnerabilità.

- **MySQL (3306)** → MySQL 5.0.51a
  Versione obsoleta, spesso con credenziali deboli o exploit noti.

- **PostgreSQL (5432)** → PostgreSQL 8.3.x
  Anche qui: versione preistorica in termini di sicurezza.

Ma il dato più interessante non è solo *quanto siano vecchi i servizi*, è **cosa Nmap riesce a dedurre dal loro comportamento**.

Alcuni esempi chiave:

- 1524/tcp → **bindshell – "Metasploitable root shell"**
  Qui Nmap ti sta praticamente urlando: *"questa è una backdoor"*.

- 1099/tcp → Java RMI registry
  Superficie ideale per exploit Java legacy.

- 8180/tcp → Apache Tomcat / Coyote JSP engine
  Porta applicativa spesso dimenticata dai sysadmin.

- 8009/tcp → AJP13
  Storicamente sfruttato per accessi non autorizzati.

In fondo all'output compare anche una **sintesi intelligente**:

- OS stimato: **Unix / Linux**
- Hostname: metasploitable.localdomain
- Kernel Linux (CPE identificato)

Questo significa che -sV ha incrociato le risposte dei servizi per **rafforzare l'OS fingerprinting**, anche senza usare -O.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV  10.0.2.3
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-17 12:49 CET
Nmap scan report for 10.0.2.3
Host is up (0.00069s 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 rexecd
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       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:59:35:43 (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 11.53 seconds
```

CONCLUSIONE

Le scansioni effettuate hanno permesso di ottenere una visione completa e dettagliata del target Metasploitable, evidenziando un sistema intenzionalmente vulnerabile con un'ampia superficie d'attacco. L'OS fingerprinting ha fornito una stima attendibile del sistema operativo in uso, mentre le scansioni SYN e TCP Connect hanno consentito di identificare le porte aperte, mostrando risultati coerenti tra loro ma con differenze in termini di rumorosità e modalità di interazione con il target. La versione detection ha infine rivelato servizi obsoleti e configurazioni insicure, confermando come l'enumerazione rappresenti una fase fondamentale per comprendere il contesto del sistema e pianificare in modo efficace le successive attività di analisi e testing della sicurezza.