

Relazione: tecniche di scansione con Nmap

1. Introduzione

Per esplorare le funzionalità offerte da **Nmap**, è possibile visualizzare la guida dei comandi digitando:

```
nmap -h
```

Questo comando elenca tutte le opzioni disponibili per effettuare:

- Scansioni TCP/UDP
- Identificazione del sistema operativo
- Rilevamento delle versioni dei servizi
- Uso di script NSE
- Analisi avanzate su host, rete e firewall

2. Ambiente di test

Le scansioni sono state effettuate da una macchina **Kali Linux** su una rete interna simulata in UTM. I target erano:

- **Metasploitable** – IP: 192.168.20.20
- **Windows** – IP: 192.168.20.30

3. Scansioni effettuate Metasploitable IP: 192.168.20.20

- OS Fingerprint → nmap -O 192.168.20.20
- SYN Scan → nmap -sS 192.168.20.20
- TCP Connect Scan → nmap -sT 192.168.20.20
- Version Detection → nmap -sV 192.168.20.20

```
Kali Linux
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -O 192.168.20.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 12:48 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.20.20
Host is up (0.0013s 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: 7A:A7:42:D3:74:56 (Unknown)
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
(kali㉿kali)-[~]
```

```
Kali Linux
File Actions Edit View Help
(kali㉿kali)-[~]
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
(kali㉿kali)-[~]
$ nmap -sS 192.168.20.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 13:15 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.20.20
Host is up (0.00068s 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: 7A:A7:42:D3:74:56 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
(kali㉿kali)-[~]
```

```
Kali Linux
File Actions Edit View Help
kali㉿kali: ~
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 7A:A7:42:D3:74:56 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

(kali㉿kali)-[~]
$ nmap -sT 192.168.20.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 13:18 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.20.20
Host is up (0.0012s 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  cccproxy-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: 7A:A7:42:D3:74:56 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

(kali㉿kali)-[~]
$
```

```
Kali Linux
File Actions Edit View Help
kali㉿kali: ~
MAC Address: 7A:A7:42:D3:74:56 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

(kali㉿kali)-[~]
$ nmap -sV 192.168.20.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 13:18 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.20.20
Host is up (0.00036s 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        Netkit rshd
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
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: 7A:A7:42:D3:74:56 (Unknown)
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 52.63 seconds

(kali㉿kali)-[~]
$
```

Confronto tecnico tra SYN Scan e TCP Connect Scan

Durante l'attività pratica, sono state effettuate due delle più comuni tecniche di scansione offerte da Nmap: la **SYN scan**(-sS) e la **TCP connect scan** (-sT). Questi due approcci sono fondamentali per l'identificazione delle porte aperte su un host, ma si differenziano profondamente per comportamento, impatto e requisiti.

SYN Scan (-sS)

La SYN scan è conosciuta anche come "**half-open scan**" perché invia un pacchetto **SYN** e attende un'eventuale risposta **SYN-ACK** dal target, **senza mai completare il three-way handshake** TCP. In caso di risposta positiva, la porta viene marcata come "open" e Nmap **invia un pacchetto RST** (Reset) per interrompere la connessione prima che venga stabilita.

Caratteristiche principali:

- **Stealth:** la connessione non viene mai completata, il che la rende più difficile da rilevare da parte di firewall e sistemi di intrusion detection (IDS).
- **Veloce ed efficiente:** permette scansioni più rapide rispetto ad altri metodi.

TCP Connect Scan (-sT)

La TCP Connect scan utilizza le normali **chiamate di sistema** (socket) per effettuare il **three-way handshake completo**(SYN → SYN-ACK → ACK). È più "rumorosa", poiché stabilisce una vera e propria connessione TCP con il servizio target.

Caratteristiche principali:

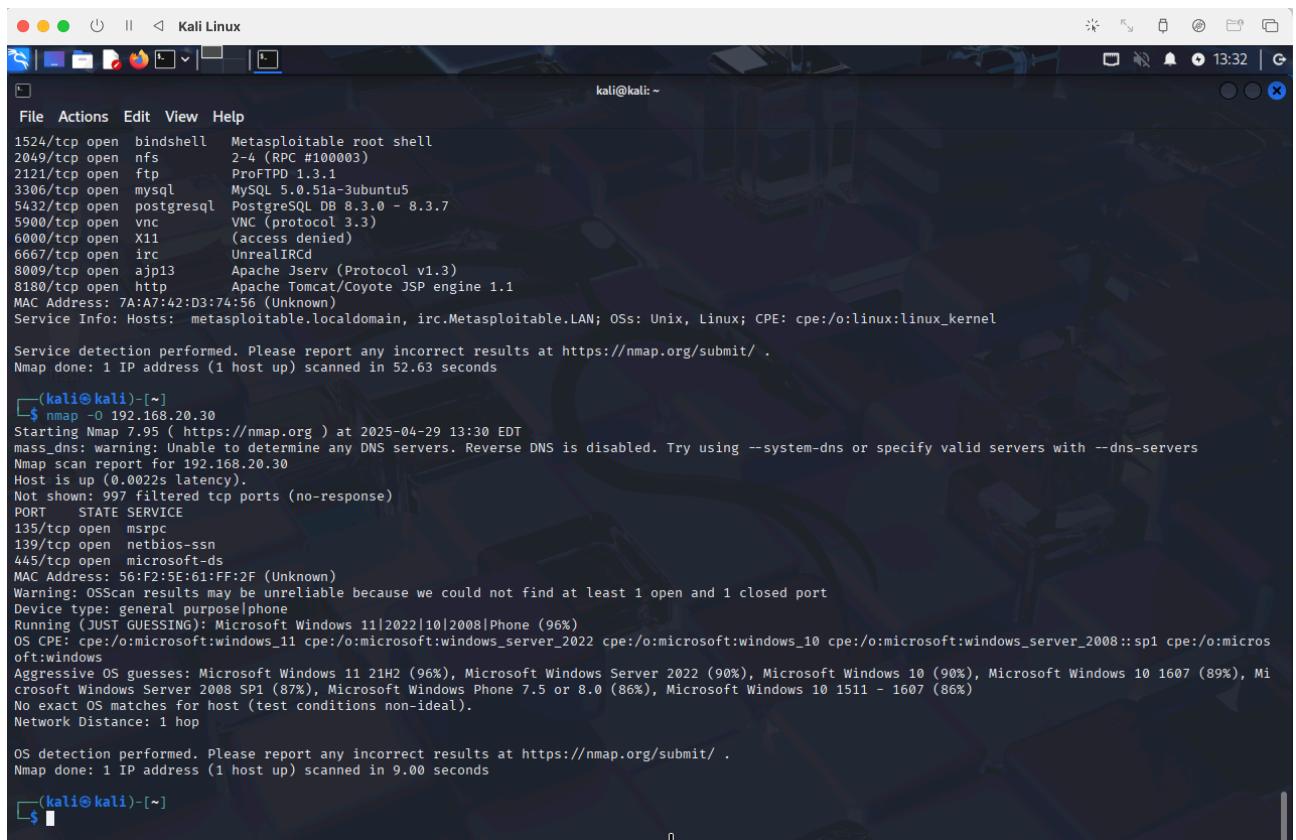
- **Rilevabile:** essendo una connessione vera e propria, è facilmente intercettabile da firewall, router e IDS.
- **Più lenta:** ogni connessione viene aperta e chiusa, il che comporta un maggior overhead.

Entrambe le tecniche hanno restituito **risultati coerenti** durante le scansioni contro il target Metasploitable, rilevando le stesse porte aperte e offrendo una mappa completa dei servizi in ascolto. Tuttavia, è fondamentale comprendere il contesto di utilizzo:

- Se l'obiettivo è **rimanere inosservati**, la **SYN scan** è preferibile.
- Se si lavora in ambienti **con privilegi limitati** (o senza root), la **TCP connect** è una valida alternativa, anche se più evidente.

4. Scansioni effettuate Windows IP: 192.168.20.30

- **OS Fingerprint** → nmap -O 192.168.20.30



```
kali㉿kali: ~
File Actions Edit View Help
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: 7A:A7:42:D3:74:56 (Unknown)
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 52.63 seconds

(kali㉿kali)-[~]
$ nmap -O 192.168.20.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 13:30 EDT
mass dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.20.30
Host is up (0.0022s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 56:F2:5E:61:FF:2F (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 11|2022|10|2008|Phone (96%)
OS CPE: cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_server_2022 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows
Aggressive OS guesses: Microsoft Windows 11 21H2 (96%), Microsoft Windows Server 2022 (90%), Microsoft Windows 10 (90%), Microsoft Windows 10 1607 (89%), Microsoft Windows Server 2008 SP1 (87%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windows 10 1511 - 1607 (86%)
No exact OS matches for host (test conditions non-ideal).
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 9.00 seconds
```

5. Conclusione

L'esercizio ha permesso di applicare in modo pratico le principali tecniche di scansione di rete tramite Nmap, consolidando la capacità di analisi delle porte aperte, dei servizi attivi e dei sistemi operativi dei target.

Sono stati scansionati due sistemi differenti:

- **Metasploitable**, con numerosi servizi vulnerabili esposti.
- **Windows**, con una configurazione di rete più protetta e con meno porte aperte.

Le scansioni sono state condotte utilizzando diversi metodi (-sS, -sT, -sV, -O), mettendo in evidenza le caratteristiche, i vantaggi e le limitazioni di ogni tecnica.

È stata inoltre osservata l'efficacia di Nmap anche senza l'uso di privilegi elevati, confermando la sua flessibilità operativa.

Complessivamente, l'attività ha rinforzato la comprensione del funzionamento delle scansioni TCP, delle tecniche stealth, e dell'importanza di interpretare correttamente i risultati ottenuti in diversi contesti di rete.

6. Considerazioni Aggiuntive

L'esercizio ha evidenziato l'importanza di una corretta impostazione della rete di test per il buon esito delle scansioni.

La semplicità con cui è stato possibile identificare porte e servizi su Metasploitable ha confermato che un ambiente volutamente vulnerabile facilita l'apprendimento delle tecniche di analisi.

Nel caso del sistema Windows, è stato interessante osservare come un numero limitato di porte aperte e l'adozione di configurazioni di default più sicure abbiano reso la scansione meno dettagliata, evidenziando le differenze tra un sistema progettato per la sicurezza e uno volutamente esposto.

Infine, la possibilità di eseguire le scansioni senza privilegi elevati su Kali Linux ha semplificato il lavoro pratico, ma è importante ricordare che in ambienti produttivi reali potrebbe essere necessario disporre di permessi amministrativi per ottenere risultati completi.

Nel complesso, l'attività ha fornito una base solida per l'utilizzo di Nmap e ha preparato il terreno per futuri approfondimenti nell'ambito della sicurezza delle reti.