REPORT TECNICO

SCANSIONE DEI SERVIZI CON NMAP

Redatto da: *Nicolò Calì Cybersecurity Student*

Data: 06/01/2026

1. Introduzione

1.1 Obiettivo dell'Attività

L’obiettivo dell’esercitazione di oggi è quello di eseguire una serie di scansioni con il tool Nmap già installato sulla nostra Kali.

La scansione avverrà su due diverse Macchine Target:

- *Metasploitable*
- *Windows 10 pro.*

Le scansioni che verranno eseguite sono le seguenti:

- *OS fingerprint*
- *Syn Scan*
- *TCP connect*
- *Version detection*

1.2 Scopo

Lo scopo della nostra simulazione è quello di raccogliere quante più informazioni possibili al fine di individuare, nelle nostre macchine bersaglio, potenziali vulnerabilità.

2. Ambiente di Lavoro e Strumenti

Per effettuare le nostre scansioni lavoreremo in un ambiente di test su Virtualbox in cui sono presenti le seguenti macchine virtuali:

2.1 Macchine Virtuali

- **Macchina Attaccante:** Kali Linux 2025.3
- **Prima Macchina Vittima:** Metasploitable2
- **Seconda Macchina Vittima:** Windows 10 pro

2.2 Strumenti

- Nmap: Usato per le scansioni.

3. Attività Tecnica e Metodologia

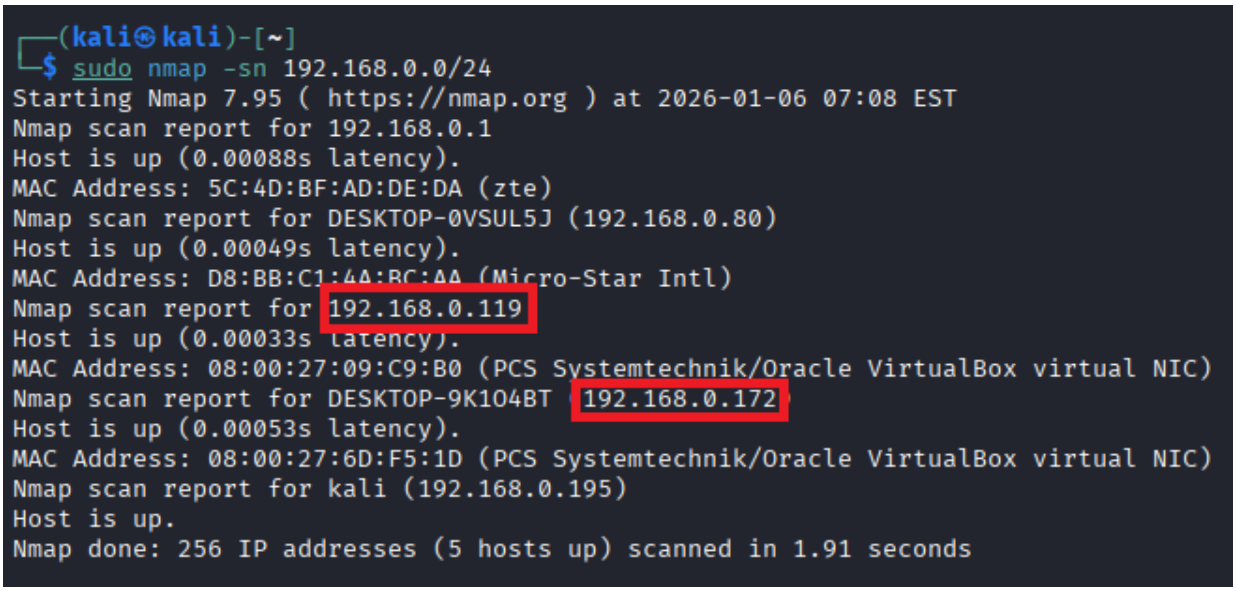
Per Prima di poter procedere con le nostre scansioni è necessario conoscere gli indirizzi IPv4 delle due macchine bersaglio.

Per farlo accendiamo le nostre VM e dal terminale digitiamo i seguenti comandi:

- *Kali: “ip a” oppure “ifconfig” → IP: 192.168.0.195/24*
- *Metasploitable: “ifconfig” → IP: 192.168.0.119/24*
- *Windows: “ipconfig” → IP: 192.168.0.172/24*

Una volta ottenuti i nostri indirizzi IP andremo ad ottenere l’elenco degli host presenti nella stessa rete LAN digitando nel terminale della Kali il seguente comando:

sudo nmap -sn 192.168.0.0/24



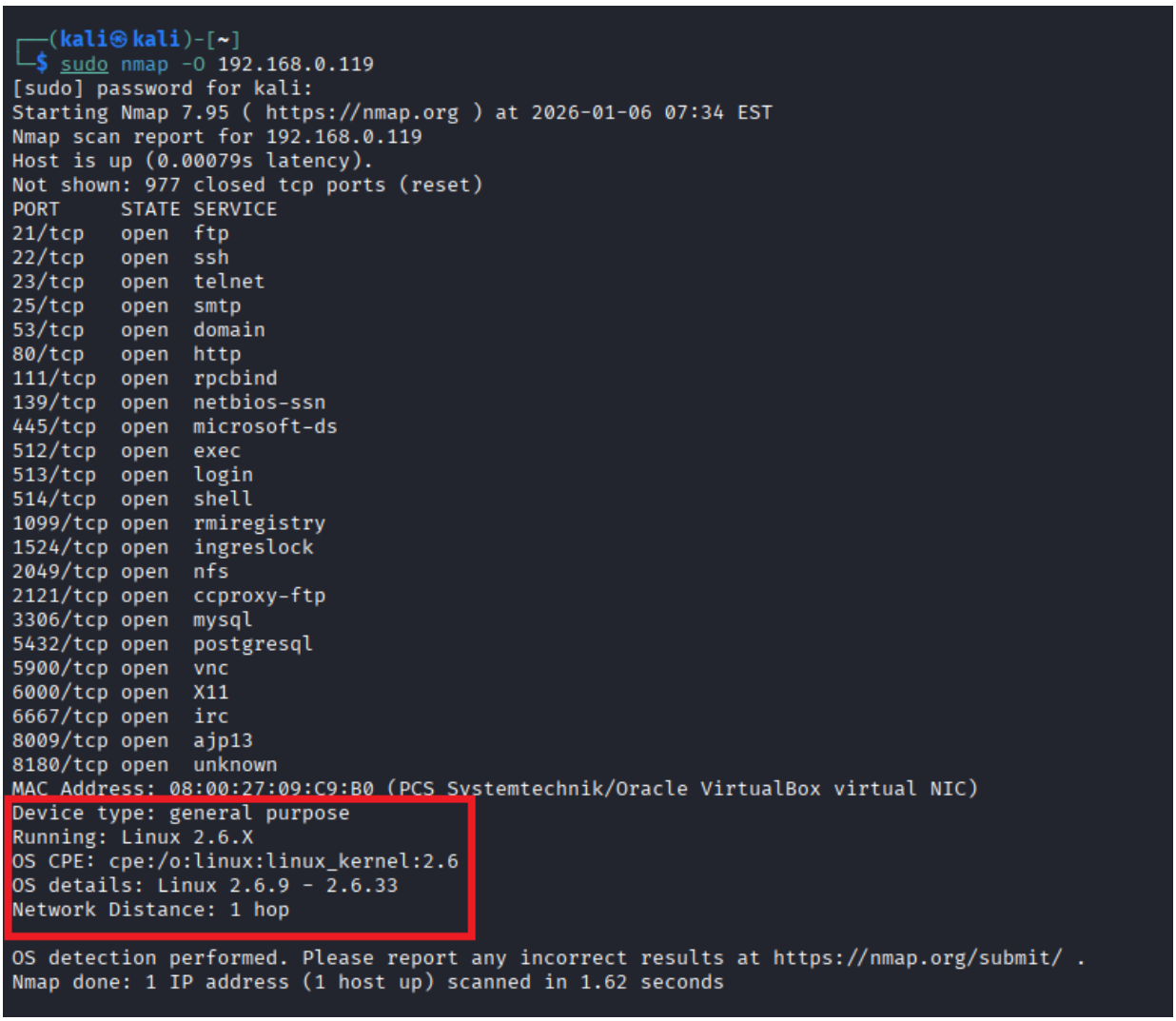
Adesso che sappiamo con certezza che i nostri dispositivi comunicano fra loro possiamo procedere con la raccolta di informazioni per mezzo delle scansioni con Nmap.

3.1 Scansione Os fingerprint

La scansione “Os fingerprint” ci permette, per mezzo del tool Nmap, di andare a verificare il tipo di sistema operativo che è installato nella macchina target.

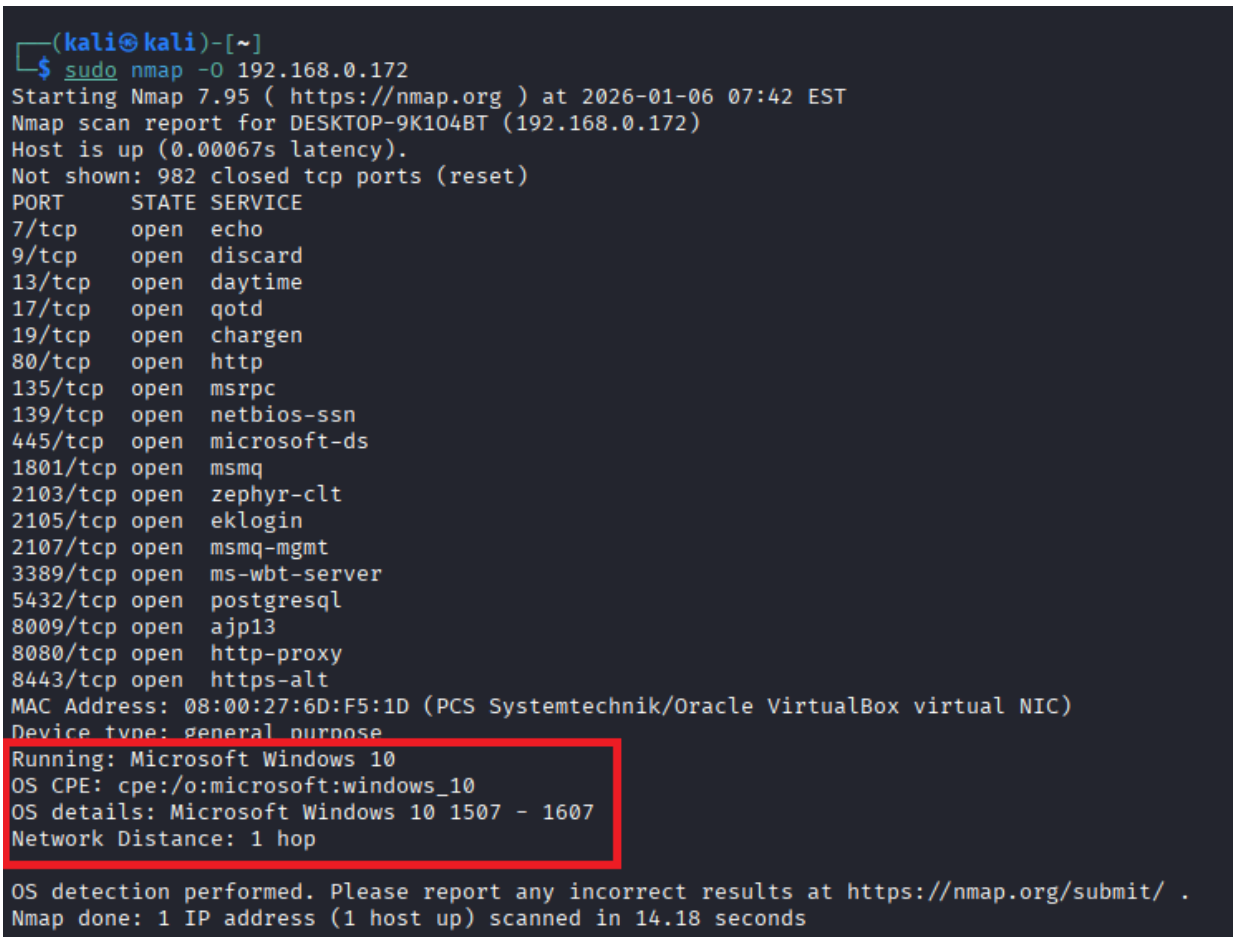
- *Comando lanciato:* `sudo nmap -O [targetIP]`
- *Osservazione:* Dovremo essere in grado di vedere il tipo di sistema operativo installato nelle macchine che andremo a bersagliare.

Os fingerprint su Metasploitable → sudo nmap -O 192.168.0.119



Come possiamo vedere Nmap ci restituisce come output alcuni importanti dettagli tra cui il sistema operativo del nostro target: **Linux 2.6.X**

Os fingerprint su Windows 10 pro → sudo nmap -O 192.168.0.172



Come output questa volta avremo che il sistema operativo utilizzato dal nostro secondo bersaglio è un **Windows 10**.

3.2 Scansione Syn Scan

La scansione "Syn Scan" consiste nell'inviare pacchetti SYN e nell'attendere una risposta SYN/ACK sfruttando una connessione parziale "half-open".

Si tratta di un tipo di scansione veloce e meno rilevabile.

- *Comando lanciato:* sudo nmap -sS [targetIP]
- *Osservazione:*
  - → *Se riceve una risposta SYN/ACK allora la porta è aperta.*
  - → *Se riceve una risposta RST (Reset) allora la porta è chiusa.*

Eseguiremo la scansione solo su metasploitable lanciando il seguente comando:

sudo nmap -sS 192.168.0.119

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.0.119
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 08:02 EST
Nmap scan report for 192.168.0.119
Host is up (0.000080s 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: 08:00:27:09:C9:B0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

Come output ci darà delle informazioni preziose:

- ***PORT*** *→ indica il numero della porta ed il tipo (es. TCP, UDP…);*
- ***STATE*** *→ indica se la porta è aperta o chiusa;*
- ***SERVICE*** *→ indica il servizio attivo su quella porta (ftp, telnet, http, ssh etc..)*

3.2 Scansione TCP connect

La scansione "TCP connect", a differenza del Syn Scan, completa tutta la 3-way handshake TCP in quanto viene utilizzata la funzione connect().

Questo tipo di scansione non richiede nessun privilegio particolare per essere eseguito tuttavia risulta molto meno "silenziosa" rispetto al Syn scan in quanto genera un maggiore traffico sulla rete.

- *Comando lanciato:* sudo nmap -sT [targetIP]

Eseguiremo la scansione solo su metasploitable lanciando il seguente comando:

sudo nmap -sT 192.168.0.119

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.0.119
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 08:38 EST
Nmap scan report for 192.168.0.119
Host is up (0.000084s 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: 08:00:27:09:C9:B0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

Come possiamo notare TCP scan produrrà lo stesso identico output di SYN scan.

Differenze tra SYN scan e TCP scan

Caratteristiche	SYN Scan	TCP Scan
Velocità	Più rapido	Più lento
Rumorosità	Poco traffico di rete generato	Più traffico di rete generato
Visibilità	Difficile da rilevare	Facile da rilevare
Permessi root	si	no

3.2 Version detection

La scansione “Version detection” permette di andare a localizzare su ogni porta aperta i servizi (Http, ssh, telnet,) e le loro versioni (Apache httpd 2.2.8, OpenSSH 4.7p1).

- *Comando lanciato:* sudo nmap -sV [targetIP]

Eseguiremo la scansione solo su metasploitable lanciando il seguente comando:

sudo nmap -sV 192.168.0.119

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.0.119
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 09:20 EST
Nmap scan report for 192.168.0.119
Host is up (0.000049s 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?
513/tcp  open  login?
514/tcp  open  shell?
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
1 service unrecognized despite returning data. If you know the service/version, pl
SF-Port514-TCP:V=7.95%I=7%D=1/6%Time=695D1A3D%P=x86_64-pc-linux-gnu%r(NULL
SF:,2B,"\x01Couldn't\x20get\x20address\x20for\x20your\x20host\x20\(kali\)\
SF:n");
MAC Address: 08:00:27:09:C9:B0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Uni

Service detection performed. Please report any incorrect results at https://nmap.o
Nmap done: 1 IP address (1 host up) scanned in 65.34 seconds
```

Come output avremo:

- ***PORT*** *→ indica il numero della porta ed il tipo (es. TCP, UDP…);*
- ***STATE*** *→ indica se la porta è aperta o chiusa;*
- ***SERVICE*** *→ indica il servizio attivo su quella porta (ftp, telnet, http, ssh etc..)*
- ***VERSION*** *→ indica la versione del servizio su quella specifica porta.*

4. Conclusioni

L'analisi con Nmap ha evidenziato tre aspetti fondamentali per la sicurezza dei sistemi: :

- **Identificazione delle Vulnerabilità:** Su Metasploitable sono emersi servizi datati dimostrando come il *Version Detection* sia cruciale per individuare falle di sicurezza
- **Discrezione dell'Analisi:** Il confronto ha confermato che la *SYN Scan* (-sS) è preferibile alla *TCP Connect* per ridurre l'impatto sulla rete e la visibilità nei log di sistema.
- **Contestualizzazione del Rischio:** La corretta distinzione tra Linux e Windows 10 permette di focalizzare la ricerca delle vulnerabilità specifiche per l'architettura del sistema operativo in uso.