Report S5L2 - Nmap

Introduzione

L’esercizio richiede di effettuare delle scansioni di servizi tramite Nmap.
Le scansioni saranno effettuate dal terminale della kali, e si andranno ad effettuare:

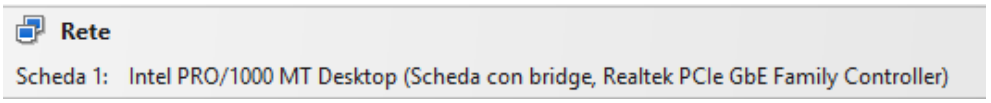
- Sulla VM **metaspoitable**:
    - OS Fingerprint;
    - Syn Scan;
    - TCP Connect;
    - Version Detection.

- Sulla VM **Windows 10**:
    - OS Fingerprint.

Nmap (Network Mapper) è uno strumento open-source estremamente potente e versatile per la scansione della rete e l'identificazione dei dispositivi e dei servizi.
Funzionalità principali di Nmap:

- Scansione degli Host: Identifica gli host attivi all'interno di una rete;
- Identificazione dei Servizi: Rileva i servizi in esecuzione su ciascun host, inclusi i numeri di porta e i protocolli;
- Rilevamento dei Sistemi Operativi: Utilizza varie tecniche di fingerprinting per determinare il sistema operativo in esecuzione su un host;
- Scansione delle Vulnerabilità: Può essere utilizzato per identificare potenziali vulnerabilità nei dispositivi e nei servizi rilevati.

Il primo step è quello di impostare tutte le macchine virtuali in modo da averne 3 connesse in Bridge con la scheda di rete dell’host.



Controllare l’indirizzo IP delle 3 macchine attraverso la console:

```
Last login: Tue Jan  6 13:33:04 EST 2026 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 20

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast ql
    link/ether 08:00:27:1a:d4:54 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.127/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe1a:d454/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

```
Prompt dei comandi
C:\Users\user>ipconfig

Configurazione IP di Windows


Scheda Ethernet Ethernet:

   Suffisso DNS specifico per connessione:
   Indirizzo IPv4. . . . . . . . . . . . : 192.168.1.125
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . : 192.168.1.1

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 . . . . . . . . . . . . . . . . . . . . : 2001:0:2851:782c:2039:1621:68b6:71b1
   Indirizzo IPv6 locale rispetto al collegamento . . : fe80::2039:1621:68b6:71b1%5
   Gateway predefinito . . . . . . . . . : ::
```

```
1  2  3  4
kali@kali: ~
Session  Actions  Edit  View  Help
  command 'ifconfig' from deb net-tools
Try: sudo apt install <deb name>

┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group de
fault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:63:b0:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.126/24 brd 192.168.1.255 scope global dynamic noprefixrou
te eth0
       valid_lft 40500sec preferred_lft 40500sec
    inet6 fe80::9934:39ab:244:b8a1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$
```

Prima di avviare le attività di scansione, è stata verificata la raggiungibilità degli host all'interno della sottorete. La mappatura degli asset ha confermato la seguente distribuzione degli indirizzi IP:

- **Windows 10:** 192.168.1.125;
- **Metasploitable**: 192.168.1.127;
- **Kali Linux**: 192.168.1.126.

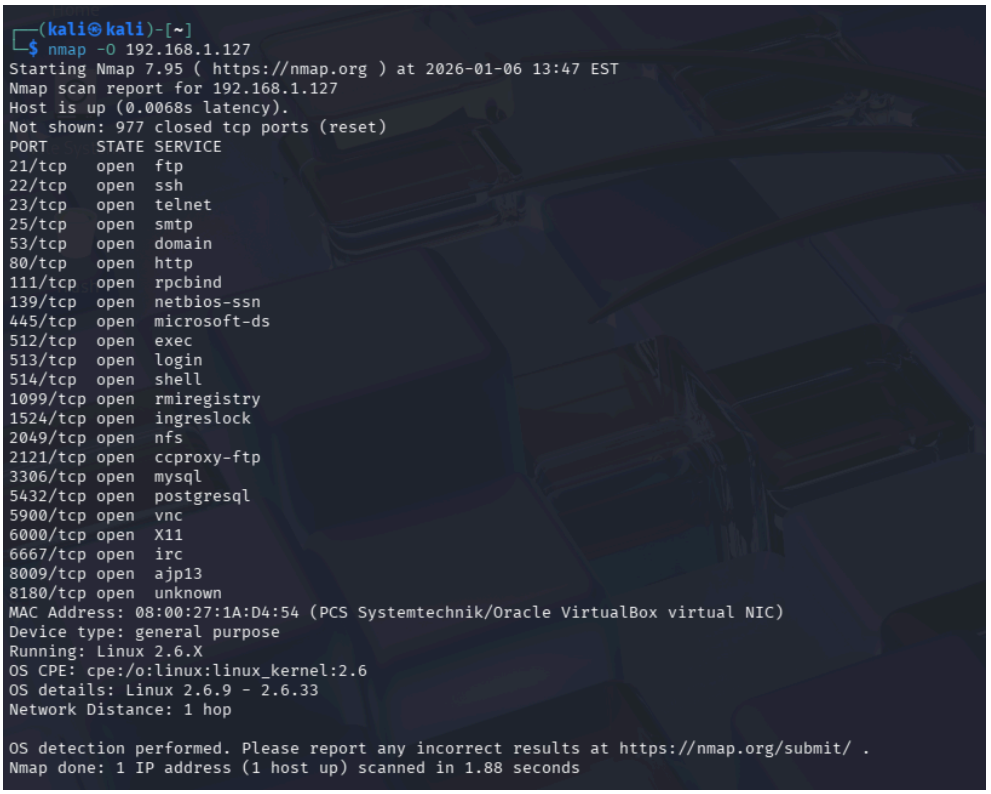
Gli indirizzi IP ci saranno necessari per indirizzare i nostri scan, una volta fatto questo si può procedere con le scansioni.

Target 1: Metasploitable 2

In questa fase abbiamo testato la macchina vulnerabile per eccellenza per osservare come risponde a scansioni aggressive.

A. OS Fingerprinting

L'**OS Fingerprinting** è la tecnica che Nmap utilizza per determinare il sistema operativo del target senza che questo lo dichiari esplicitamente.
Comando: sudo nmap -O 192.168.1.127

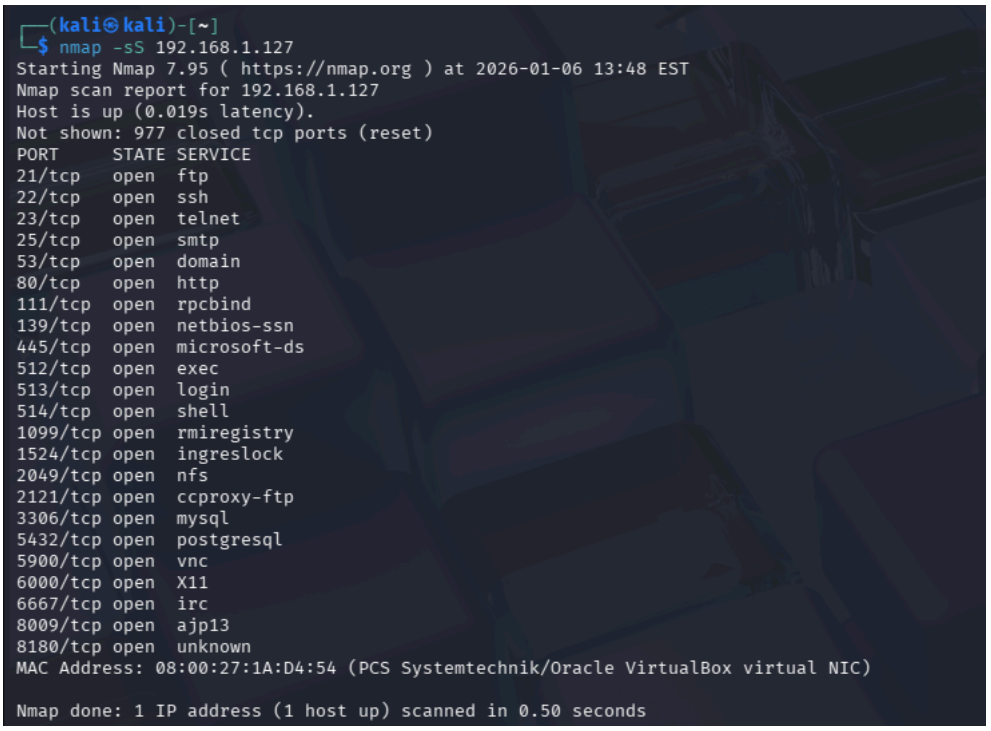


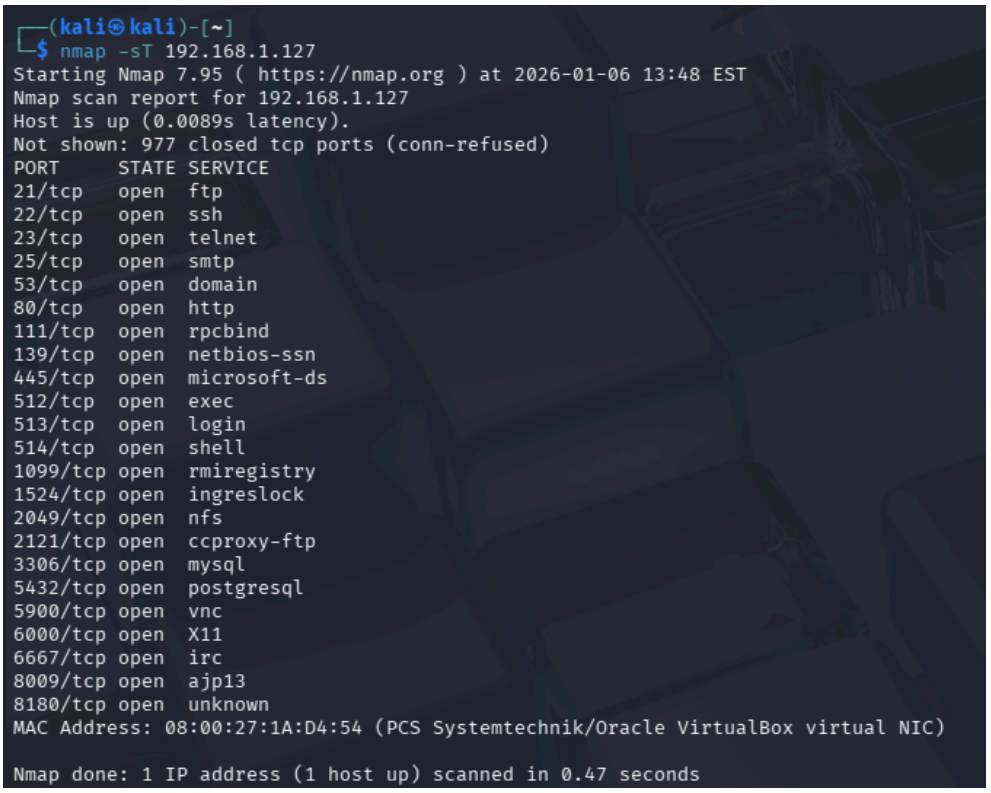
Il comando quindi ci darà come risultato
OS details: Linux 2.6.9 - 2.6.33

B. SYN Scan vs TCP Connect Scan

Comandi:

- *SYN scan*: nmap -sS 192.168.1.127
- *TCP scan*: nmap -sT 192.168.1.127.





Il SYN scan e il TCP scan mostrano sostanzialmente lo stesso risultato, la differenza tra i due risiede nelle performance e nella visibilità.

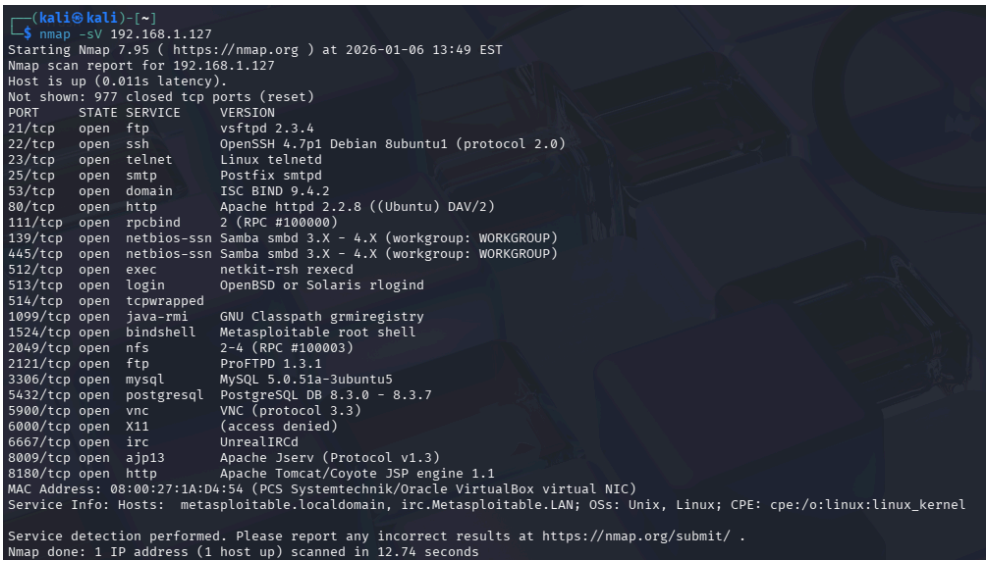
Il **SYN scan** infatti è più rapido del **TCP scan** ed anche meno visibile.
Se analizzassimo il traffico con ***Wireshark***, vedremmo che il TCP Connect lascia tracce complete nei log dei servizi (es. un server HTTP loggherà una connessione), mentre il SYN scan no, in quanto non completa il **Three-Way Handshake**.

Il **Three-Way Handshake** è la "stretta di mano" in **tre passaggi** necessaria per stabilire una connessione affidabile tra due computer.

1. **SYN (Synchronize):** Il Client invia un pacchetto per dire: *"Ehi, vorrei connettermi alla porta X, ecco il mio numero di sequenza"*.
2. **SYN-ACK (Synchronize-Acknowledge):** Se la porta è aperta, il Server risponde: *"Ricevuto! Anche io sono pronto, ecco il mio numero di sequenza"*.
3. **ACK (Acknowledge):** Il Client risponde: *"Ok, ho ricevuto tutto, ora iniziamo a scambiare dati"*.

Il SYN Scan è chiamato infatti anche **"Half-Open Scan"** (scansione semi-aperta) proprio perché interrompe bruscamente la procedura dell'handshake al secondo passaggio.

C. Version Detection
La **Version Detection** è il processo con cui Nmap cerca di capire esattamente **quale software** e **quale versione** specifica stanno girando su una porta aperta.
Comando: nmap -sV 192.168.1.127



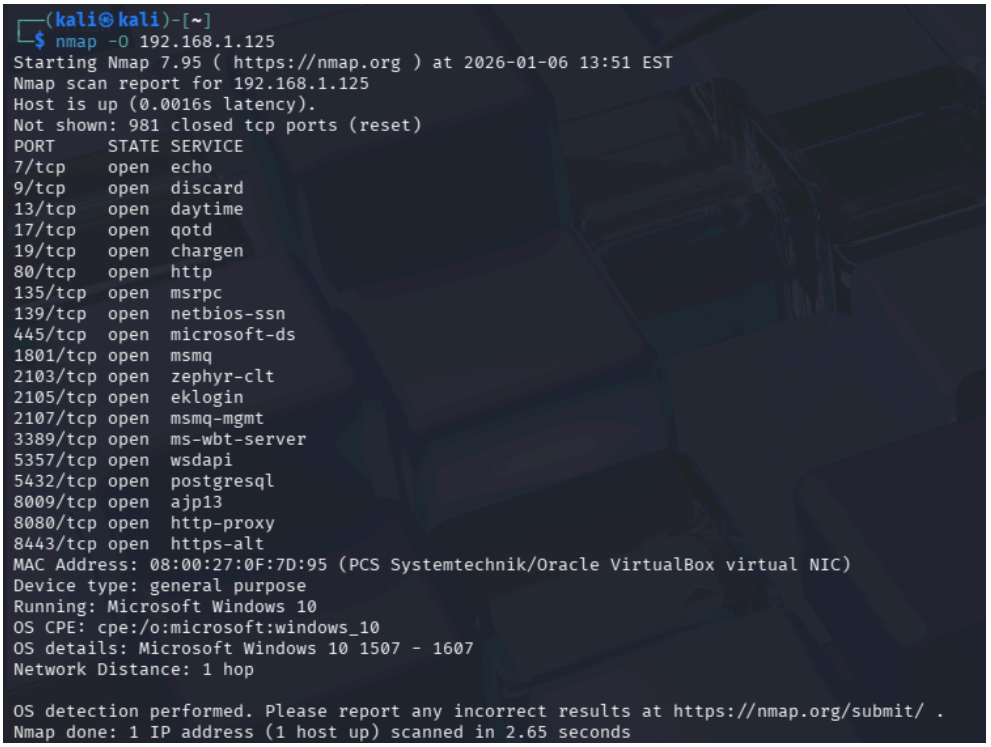
Come possiamo notare dallo screenshot, questo processo ci ha fornito informazioni su quale software e quale versione giri su una determinata porta.
Prendiamo come esempio la **porta 3306** che ospita il servizio **mysql** con la versione **MySQL 5.0.51a-3ubuntu5.**

Target 2: Windows

Ora si effettuerà l'OS Fingerprinting su Windows10 per confrontarne le differenze.

A. OS Fingerprinting

Comando: sudo nmap -O 192.168.1.125



Contrariamente a quanto avviene solitamente con i target **Windows**, caratterizzati da poche porte aperte e firewall restrittivi che costringono **Nmap** a formulare delle stime (**Guess**), in questo test l'identificazione è risultata univoca. La presenza di servizi accessibili ha permesso a **Nmap** di raccogliere un numero sufficiente di campioni (*fingerprints*), portando a un'identificazione certa del sistema come **Microsoft Windows 10 (versioni 1507 - 1607)** senza la necessità di proporre ipotesi alternative.