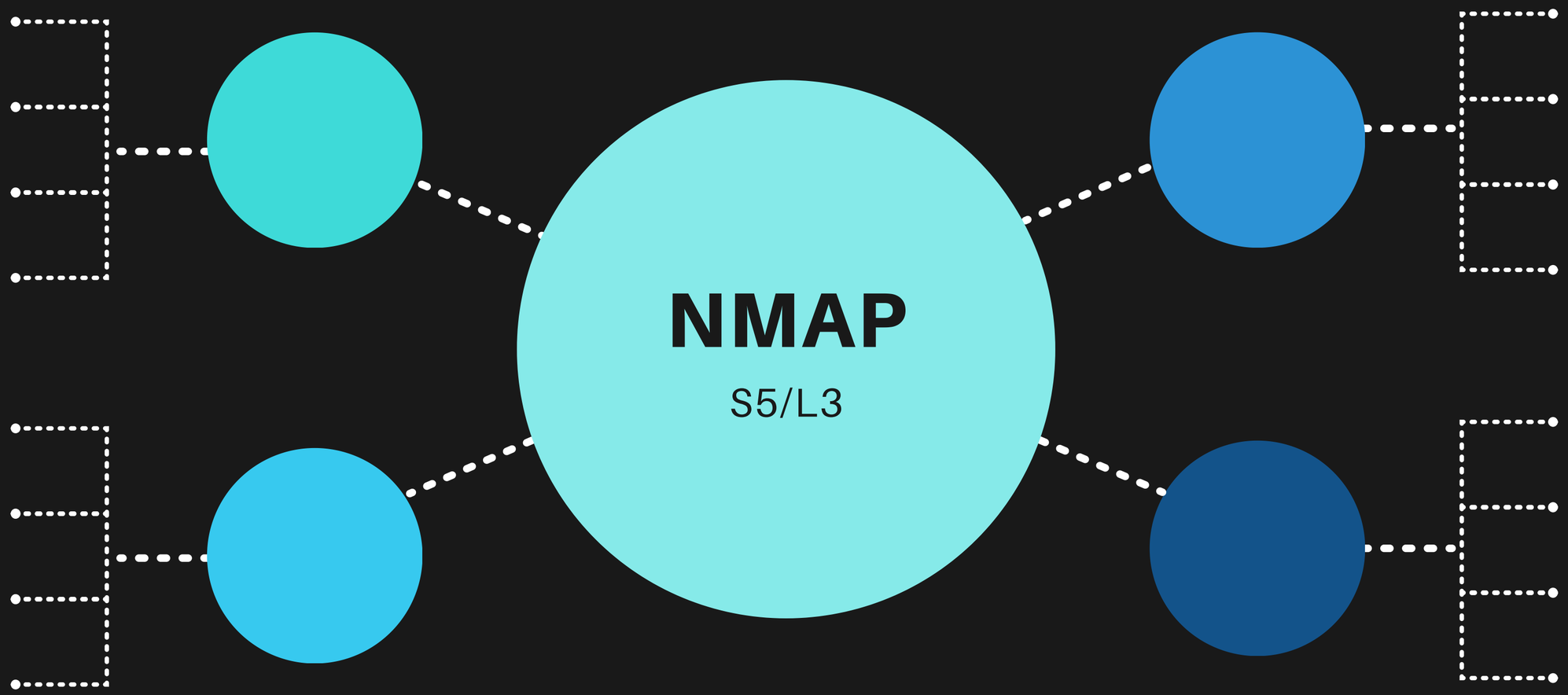
NMAP
S5/L3

SCANSIONE SU

Metasploitable2

OS fingerprint

```
└─$ sudo nmap -O 192.168.50.100
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 05:25 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00034s 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: 08:00:27:6D:5F:CB (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 14.60 seconds
```

L'OS fingerprinting è una tecnica utilizzata per determinare il sistema operativo in esecuzione su un host di rete. Questo processo si basa sull'analisi dei pacchetti di rete inviati da un host di destinazione e sulle risposte ricevute per determinare caratteristiche uniche del sistema operativo.
Quando un host di rete comunica con altri dispositivi sulla rete, invia e riceve pacchetti di dati. Ogni sistema operativo ha delle peculiarità nell'implementazione dei protocolli di rete e nelle risposte ai pacchetti. L'OS fingerprinting sfrutta queste differenze per tentare di identificare il sistema operativo.

Risultato:

- IP: 192.168.50.101
- Sistema Operativo: Linux (basato sulle risposte ai pacchetti di rete)

SCANSIONE SU

Metasploitable2

SYN Scan

```
└─$ sudo nmap -sS 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 05:26 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00027s 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: 08:00:27:6D:5F:CB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds
```

Lo "SYN Scan" è una tecnica di scansione delle porte utilizzata per individuare le porte aperte su un host di destinazione. Questa tecnica è una delle modalità più comuni di scansione delle porte e viene eseguita utilizzando il protocollo TCP (Transmission Control Protocol).
Non completa mai la procedura di connessione TCP, quindi non stabilisce mai una connessione completa con l'host di destinazione. Questo lo rende più difficile da rilevare rispetto ad altre tecniche di scansione delle porte. Tuttavia, è possibile che alcuni sistemi di sicurezza o firewall rilevino e blocchino questa attività se configurati correttamente.

Risultato:

- Porte Aperte: Tutte le porte analizzate risultano aperte pronte per accettare connessioni in arrivo, questo può comportare un grave rischio per la sicurezza.

SCANSIONE SU

Metasploitable2

```
└─$ sudo nmap -sT 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 05:27 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0011s 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: 08:00:27:6D:5F:CB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

TCP connect

Il "TCP Connect" è una tecnica di scansione delle porte utilizzata per individuare le porte aperte su un host di destinazione. Questo metodo di scansione delle porte implica l'utilizzo del protocollo TCP (Transmission Control Protocol) per stabilire una connessione completa con le porte dell'host per determinare se sono aperte o chiuse.
Il TCP Connect Scan è una tecnica affidabile e precisa per individuare le porte aperte su un host. Tuttavia, richiede più tempo rispetto ad altre tecniche di scansione delle porte, poiché stabilisce una connessione completa con ciascuna porta da testare. Questo metodo di scansione è più probabile che venga rilevato dai sistemi di sicurezza, poiché lascia tracce nel registro delle connessioni TCP dell'host di destinazione.

Risultato:

- Porte Aperte: Tutte le porte analizzate risultano aperte
- Differenze con SYN Scan: Nessuna differenza significativa nei risultati, entrambe le scansioni indicano tutte le porte aperte. La differenza principale risiede nel metodo utilizzato per stabilire le connessioni.

SCANSIONE SU

Metasploitable2

Version detection

```
└─$ sudo nmap -sV  192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 05:28 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00018s 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?
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: 08:00:27:6D:5F:CB (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, L
inux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.60 seconds
```

Il "Version Detection" è una tecnica utilizzata durante la scansione di porte per identificare la versione dei servizi in esecuzione su un host di destinazione. Questa tecnica è utile perché consente di determinare non solo se una porta è aperta o chiusa, ma anche quale specifica versione del servizio è in esecuzione su quella porta.
Il Version Detection è utile per gli amministratori di rete e per gli attaccanti che vogliono ottenere informazioni dettagliate sui servizi in esecuzione su un host di destinazione.

Risultato:

- IP: 192.168.50.101
- Porte Aperte e Servizi in Ascolto:
  - Porta 21: vsftpd 2.3.4
  - Porta 22: OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
  - Porta 23: telnetd
  - Porta 25: Postfix smtpd
  - Porta 53: ISC BIND 9.4.2
  - Porta 80: Apache httpd 2.2.8 ((Ubuntu) DAV/2)
  - Porta 139: Samba smbd 3.X
  - Porta 445: Samba smbd 3.X
  - Porta 3306: MySQL 5.0.51a-3ubuntu5
  - Porta 5432: PostgreSQL DB 8.3.0 - 8.3.7

SCANSIONE SU

Windows 7

OS fingerprint

```
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 09:57 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00055s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:09:64:48 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
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 37.06 seconds
```

```
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 09:53 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00088s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:09:64:48 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:
/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.
1 Update 1
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 15.56 seconds
```

L'OS fingerprinting è stato eseguito per determinare il sistema operativo in esecuzione sull'host Windows 7. Sono stati effettuati due tentativi, uno con il firewall attivo e uno con il firewall disattivato.

Risultato con Firewall Attivo:

- IP: Non specificato
- Sistema Operativo: Impossibile determinare (presumibilmente bloccato dal firewall)

Risultato con Firewall Disattivato:

- IP: Non specificato
- Sistema Operativo: Windows 7
- Porte Aperte: 9 porte aperte, 991 porte chiuse

QUESITO EXTRA

Windows 7

OS fingerprint

La scansione con il firewall attivo non ha permesso l'identificazione del sistema operativo e ha limitato la visibilità delle porte aperte a causa delle protezioni del firewall. Quando il firewall è stato disattivato, Nmap è riuscito a identificare il sistema operativo e le porte aperte.

Soluzione per Continuare le Scansioni:

- Disattivare il Firewall: Come già fatto, disattivare il firewall consente di ottenere risultati più completi. Tuttavia, questo potrebbe non essere sempre pratico in ambienti di produzione.
- Configurare il Firewall per la Scansione: Configurare eccezioni nel firewall per consentire la scansione delle porte specifiche.
- Utilizzare Tecniche Avanzate di Scansione: Tecniche come l'aggiramento dei firewall (e.g., scansioni fragili) o l'uso di proxy per evitare il rilevamento.