

S5.L3 Mapping di rete/Nmap

OS fingerprint:

```
(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
(kali㉿kali)-[~]
└─$ nmap -O 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-14 02:29 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0016s latency).
Not shown: 979 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
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
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: 08:00:27:65:34:13 (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 15.24 seconds
```

La scansione con l'opzione -O di Nmap, mostrata nell'immagine, ha permesso di identificare il sistema operativo della macchina con IP 192.168.50.101. Questo processo, noto come OS fingerprinting, ha rilevato che il sistema operativo è una versione del kernel Linux tra 2.6.9 e 2.6.33. Questa informazione è utile per determinare potenziali vulnerabilità e configurazioni specifiche del sistema target.

SYN scan:

```
(root@kali)~[/home/kali]
# nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-14 02:29 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00078s latency).
Not shown: 979 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
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
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: 08:00:27:65:34:13 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

L'opzione `-sS` utilizzata con Nmap nell'immagine carica ha eseguito una scansione di tipo SYN, che è una delle tecniche più comuni e veloci per identificare le porte aperte su un host di rete. Questa tecnica specifica manda un pacchetto SYN (che inizia una connessione TCP) a diverse porte dell'host target. Se una porta è aperta, l'host risponde con un pacchetto SYN-ACK, altrimenti risponde con un RST per le porte chiuse.

La scansione ha rilevato diverse porte aperte offrendo servizi come FTP, SSH, Telnet, SMTP, e molti altri, indicando i vari servizi che sono attivi e ascoltano su quelle porte. Questo tipo di scansione è fondamentale per la valutazione della sicurezza, permettendo di capire quali servizi sono esposti su una rete e potenzialmente vulnerabili agli attacchi.

TCP Connect

```
(root@kali)~[/home/kali]
# nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-14 02:30 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0046s latency).
Not shown: 979 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
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
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: 08:00:27:65:34:13 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.83 seconds
```

L'opzione -sT utilizzata in Nmap per la scansione mostrata nell'immagine esegue una scansione TCP connect. A differenza della scansione SYN, la scansione TCP connect utilizza il metodo completo di connessione TCP, il che significa che Nmap completa la connessione TCP a tre vie con il host di destinazione per ogni porta scansionata. Se una porta è aperta, il sistema risponde con un SYN-ACK, seguito da un ACK da parte di Nmap, completando la connessione. Questa tecnica è meno discreta e può essere più facilmente rilevata dai sistemi di rilevamento intrusioni, ma non richiede privilegi di amministratore per essere eseguita. La scansione ha rilevato diverse porte aperte offrendo servizi come FTP, SSH, Telnet, e altri, mostrando quali servizi sono attivi e in ascolto sulle porte del sistema target. Questo tipo di scansione aiuta nella valutazione della sicurezza, rivelando quali porte sono aperte e potenzialmente vulnerabili su un host.

Version Detection:

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-14 02:30 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00069s latency).
Not shown: 979 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)
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
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: 08:00:27:65:34:13 (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 66.55 seconds
```

L'opzione -sV utilizzata in Nmap, come mostrato nell'immagine, serve per eseguire una scansione che determina le versioni dei servizi in esecuzione sulle porte aperte di un host. Questo tipo di scansione è molto utile per identificare specifiche versioni di software in esecuzione, che possono essere confrontate con database di vulnerabilità per scoprire potenziali punti deboli di sicurezza. L'immagine mostra che la scansione ha identificato varie versioni di software come:

- FTP usando vsftpd 2.3.4
- SSH su OpenSSH 4.7p1
- Telnet attraverso telnetd
- SMTP con Postfix

- HTTP con Apache httpd 2.2.8 su Ubuntu
- Samba per condivisione file su NetBIOS
- MySQL versione 5.0.51a-3ubuntu5
- PostgreSQL DB 8.3.0 - 8.3.7
- Apache Tomcat su 8180/tcp

Queste informazioni sono fondamentali per un'amministrazione di sistema sicura e per attività di penetration testing, poiché permettono agli amministratori di sapere esattamente quali versioni di servizi sono in esecuzione e se esistono patch o aggiornamenti necessari per mitigare rischi di sicurezza noti.

OS Fingerprint di windows7 con firewall attivo:

```
(root@kali)-[/home/kali]
# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-14 02:33 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:1E:4A:B5 (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
```

La scansione Nmap mostrata nell'immagine è stata eseguita con l'intento di identificare il sistema operativo di un host con IP 192.168.50.102. Tuttavia, il risultato dell'OS fingerprinting non è stato definitivo a causa dell'attivazione del firewall sulla macchina Windows 7 target.

Dettagli rilevanti:

- Tutte le 1000 porte TCP scansionate sono in stato ignorato perché non hanno risposto, indicando che il firewall potrebbe aver bloccato le richieste di Nmap.
- MAC Address: 08:00:27:1E:4A:B5, che appartiene a una scheda di rete virtuale Oracle VirtualBox.
- Risultato del fingerprinting: Non è stato possibile ottenere dettagli specifici sull'OS a causa di troppe corrispondenze nel database di Nmap, molto probabilmente influenzato dalla non risposta delle porte a causa del firewall.

Questa situazione dimostra come un firewall attivo possa efficacemente ostacolare tentativi di identificazione remota del sistema operativo tramite tecniche come quelle impiegate da Nmap, aumentando la sicurezza del sistema contro attività di scansione non autorizzate.

OS Fingerprint di windows7 con il firewall disattivato:

```
(root@kali)-[/home/kali]
# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-14 02:35 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0017s 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: 08:00:27:1E:4A:B5 (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 15.48 seconds
```

La scansione Nmap mostrata nell'immagine ha rilevato con successo informazioni dettagliate sul sistema operativo della macchina con IP 192.168.50.102, grazie alla disattivazione del firewall. Con il firewall disattivato, Nmap è stato in grado di identificare che l'host sta eseguendo una versione di Windows compatibile con Windows 7 SP0 o SP1, Windows Server 2008 SP1, o Windows Server 2008 R2, o Windows 8, o Windows 8.1 Update 1.

Differenze chiave rispetto alla scansione precedente con il firewall attivo:

1. Porte rilevate aperte: A differenza della precedente scansione, dove tutte le porte erano ignorate a causa del firewall che bloccava le richieste, questa volta Nmap ha potuto identificare diverse porte aperte come NetBIOS, Microsoft-DS, e alcune porte sconosciute.
2. Precisione nel rilevamento: Senza il firewall, Nmap ha potuto effettuare una scansione più accurata, risultando in un rilevamento più preciso del sistema operativo.

Questo dimostra come un firewall possa efficacemente proteggere una macchina impedendo il rilevamento delle porte e delle versioni di servizio, riducendo così la superficie di attacco visibile agli attaccanti. Disattivare il firewall, d'altra parte, espone più informazioni che possono essere utilizzate per identificare vulnerabilità specifiche del sistema.