

# Report di Pandolfi Luciano sulla Raccolta Informazioni attraverso comandi da Shell Linux verso Metasploitable

## 1. `nmap -sn -PE 192.168.1.49`

- Esegue una scansione di ping per verificare se il dispositivo con l'indirizzo IP `192.168.1.49` è attivo nella rete (host is up):

`-sn`: Indica una scansione di tipo "ping" senza controllare le porte.

`-PE`: Utilizza il ping ICMP Echo Request per determinare se l'host risponde.

Controlla solo se il dispositivo è online, senza fare altre analisi sulla rete o sulle porte.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sn -PE 192.168.1.49
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 14:44 EST
Nmap scan report for 192.168.1.49 (192.168.1.49)
Host is up (0.0055s latency).
MAC Address: 08:00:27:76:FA:58 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

## 2. `netdiscover -r 192.168.1.49`

- Netdiscover è uno strumento utile per la scoperta di host su reti, utilizzando ARP (Address Resolution Protocol) per scoprire i dispositivi sulla rete.

```
Currently scanning: Finished! | Screen View: Unique Hosts
12 Captured ARP Req/Rep packets, from 12 hosts. Total size: 720
-----
IP                At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.1.1       34:36:54:f1:10:2f    1      60  zte corporation
192.168.1.2       90:31:4b:bb:74:9d    1      60  AltoBeam Inc.
192.168.1.3       24:fc:e5:71:d4:f8    1      60  Samsung Electronics Co.,L
192.168.1.5       9c:1c:37:c3:19:73    1      60  AltoBeam (China) Inc.
192.168.1.6       88:28:7d:81:8f:90    1      60  AltoBeam (China) Inc.
192.168.1.49      08:00:27:76:fa:58    1      60  PCS Systemtechnik GmbH
192.168.1.10      90:31:4b:bb:74:9d    1      60  AltoBeam Inc.
192.168.1.10      9c:1c:37:c3:19:73    1      60  AltoBeam (China) Inc.
192.168.1.29      00:e0:20:2e:0d:70    1      60  TECNOMEN OY
192.168.1.60      c0:35:32:a1:88:d9    1      60  Unknown vendor
192.168.1.16      00:e0:20:2e:0d:70    1      60  TECNOMEN OY
192.168.1.43      00:e0:20:2e:0d:70    1      60  TECNOMEN OY
```

### 3. nmap 192.168.1.49 --top-ports 10 -open

- Utilizza nmap per effettuare una scansione delle prime 10 porte più comuni aperte sul target (192.168.1.49).

Molto rapido per identificare i principali servizi in esecuzione su un sistema, senza dover scansionare tutte le porte.

```
(kali@kali)-[~]
$ sudo nmap 192.168.1.49 --top-ports 10 -open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 15:05 EST
Nmap scan report for 192.168.1.49 (192.168.1.49)
Host is up (0.0047s latency).
Not shown: 3 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:76:FA:58 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

### 4. nmap -sV 192.168.1.49

- Esegue una scansione delle porte identificando i servizi attivi e le relative versioni. È utile per determinare se ci sono vulnerabilità note associate alle versioni dei servizi.

```
$ sudo nmap -sV 192.168.1.49
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 15:06 EST
Nmap scan report for 192.168.1.49 (192.168.1.49)
Host is up (0.00076s 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          OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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?
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:76:FA:58 (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 133.14 seconds
```

## 5. `sudo nmap -sS -sV -T4 192.168.1.49`

- Esegue una scansione SYN (TCP Connect Scan) (`-sS`), non completando il three way handshake, quindi meno invasiva. L'opzione `-sV` identifica i servizi attivi e le loro versioni. L'opzione `-T4` aumenta la velocità della scansione.

```
(kali@kali)-[~]
$ sudo nmap -sS -sV -T4 192.168.1.49
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 15:15 EST
Nmap scan report for 192.168.1.49 (192.168.1.49)
Host is up (0.0055s 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  tcpwrapped
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?
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:76:FA:58 (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 130.89 seconds
```

## 6. `sudo hping3 --scan known 192.168.1.49`

- `hping3` è uno strumento per l'invio di pacchetti personalizzati, con l'opzione `--scan known` esegue una scansione delle porte più comuni.

```
(kali㉿kali)-[~]
└─$ sudo hping3 -V --scan known 192.168.1.49
using eth0, addr: 192.168.1.48, MTU: 1500
Scanning 192.168.1.49 (192.168.1.49), port known
264 ports to scan, use -V to see all the replies
+-----+-----+-----+-----+-----+-----+
|port| serv name | flags | ttl | id | win | len |
+-----+-----+-----+-----+-----+-----+
1  tcpmux    : .. R.A ... 64  0  0  46
2  nbp       : .. R.A ... 64  0  0  46
4  echo      : .. R.A ... 64  0  0  46
6  zip       : .. R.A ... 64  0  0  46
7  echo      : .. R.A ... 64  0  0  46
9  discard   : .. R.A ... 64  0  0  46
11 systat   : .. R.A ... 64  0  0  46
13 daytime  : .. R.A ... 64  0  0  46
15 netstat  : .. R.A ... 64  0  0  46
17 qotd     : .. R.A ... 64  0  0  46
19 chargen  : .. R.A ... 64  0  0  46
20 ftp-data : .. R.A ... 64  0  0  46
37 time     : .. R.A ... 64  0  0  46
43 whois    : .. R.A ... 64  0  0  46
49 tacacs   : .. R.A ... 64  0  0  46
67 bootps   : .. R.A ... 64  0  0  46
68 bootpc   : .. R.A ... 64  0  0  46
69 tftp     : .. R.A ... 64  0  0  46
70 gopher   : .. R.A ... 64  0  0  46
79 finger   : .. R.A ... 64  0  0  46
88 kerberos : .. R.A ... 64  0  0  46
102 iso-tsap : .. R.A ... 64  0  0  46
104 acr-nema : .. R.A ... 64  0  0  46
106 poppassd : .. R.A ... 64  0  0  46
110 pop3     : .. R.A ... 64  0  0  46
113 auth     : .. R.A ... 64  0  0  46
119 nntp     : .. R.A ... 64  0  0  46
123 ntp       : .. R.A ... 64  0  0  46
135 epmap    : .. R.A ... 64  0  0  46
137 netbios-ns : .. R.A ... 64  0  0  46
138 netbios-dgm : .. R.A ... 64  0  0  46
```

## 7. `nc -nvz 192.168.1.49 1-1024`

- Netcat (`nc`) è uno strumento di rete versatile che può essere utilizzato per scansionare porte. L'opzione `-n` impedisce la risoluzione DNS, `-v` attiva la modalità verbosa (per dettagli più specifici), e `-z` fa sì che `nc` esegua solo il tentativo di connessione alle porte senza inviare dati. Questo è utile per testare quali porte sono aperte senza fare una scansione TCP completa.

```
(kali㉿kali)-[~]
└─$ sudo nc -nvz 192.168.1.49 1-1024
[sudo] password for kali:
(UNKNOWN) [192.168.1.49] 514 (shell) open
(UNKNOWN) [192.168.1.49] 513 (login) open
(UNKNOWN) [192.168.1.49] 512 (exec) open
(UNKNOWN) [192.168.1.49] 445 (microsoft-ds) open
(UNKNOWN) [192.168.1.49] 139 (netbios-ssn) open
(UNKNOWN) [192.168.1.49] 111 (sunrpc) open
(UNKNOWN) [192.168.1.49] 80 (http) open
(UNKNOWN) [192.168.1.49] 53 (domain) open
(UNKNOWN) [192.168.1.49] 25 (smtp) open
(UNKNOWN) [192.168.1.49] 23 (telnet) open
(UNKNOWN) [192.168.1.49] 22 (ssh) open
(UNKNOWN) [192.168.1.49] 21 (ftp) open
```

## 8. `sudo nmap -f --mtu=512 192.168.1.49`

- L'opzione `-f` fa sì che nmap invii pacchetti frammentati, mentre l'opzione `--mtu=512` imposta la dimensione massima dei pacchetti a 512 byte. Questa tecnica viene utilizzata per eludere i firewall e i sistemi di rilevamento delle intrusioni (IDS), che potrebbero non riconoscere i pacchetti frammentati.

```
(kali㉿kali)-[~]
$ sudo nmap -f --mtu=512 192.168.1.49
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 15:26 EST
Nmap scan report for 192.168.1.49 (192.168.1.49)
Host is up (0.0095s 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: 08:00:27:76:FA:58 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```

## Riepilogo:

- **Ping Active Hosts:** `nmap -sn -PE 192.168.1.49;`
- **ARP Scan:** `netdiscover -r 192.168.1.49;`
- **Top 10 Ports:** `nmap 192.168.1.49 --top-ports 10;`
- **Stealth SYN Scan with Version Detection:** `sudo nmap -sS -sV -T4 192.168.1.49;`
- **Service Version Scan:** `nmap -sV 192.168.1.49;`
- **Packet-based Stealth Scan:** `sudo hping3 --scan known -V 192.168.1.49;`
- **Port Scanning:** `nc -nvz 192.168.1.49 1-1024;`
- **Firewall Bypass (TCP Fragmentation):** `sudo nmap -f --mtu=512 192.168.1.49.`

