

Nmap Metasploitable/Wind7

Ernesto Robles

"the quiete

```
(kali㉿kali3) [~/Desktop]
$ fping -a -g 192.168.50.101 192.168.50.106
192.168.50.101
192.168.50.102
192.168.50.103
ICMP Host Unreachable from 192.168.50.102 for ICMP Echo sent to 192.168.50.105
ICMP Host Unreachable from 192.168.50.102 for ICMP Echo sent to 192.168.50.105
ICMP Host Unreachable from 192.168.50.102 for ICMP Echo sent to 192.168.50.105
ICMP Host Unreachable from 192.168.50.102 for ICMP Echo sent to 192.168.50.105
ICMP Host Unreachable from 192.168.50.102 for ICMP Echo sent to 192.168.50.104
ICMP Host Unreachable from 192.168.50.102 for ICMP Echo sent to 192.168.50.104
ICMP Host Unreachable from 192.168.50.102 for ICMP Echo sent to 192.168.50.104
ICMP Host Unreachable from 192.168.50.102 for ICMP Echo sent to 192.168.50.104
ICMP Host Unreachable from 192.168.50.102 for ICMP Echo sent to 192.168.50.106
ICMP Host Unreachable from 192.168.50.102 for ICMP Echo sent to 192.168.50.106
ICMP Host Unreachable from 192.168.50.102 for ICMP Echo sent to 192.168.50.106
ICMP Host Unreachable from 192.168.50.102 for ICMP Echo sent to 192.168.50.106
```

```
(kali㉿kali3) [~/Desktop]
$ |
```

Con il comando fping effettuiamo una scansione delle reti di tutti gli ip attivi che fanno parte di quest'ultima specificando un range di ip da analizzare.

Macchina Kali: 192.168.50.102

Macchina Metaspitable: 192.168.50.101

Macchina Windows7: 192.168.50.103

Con l'uso del comando nmap -o effettuiamo una OS detection, la macchina cossispondete all'indirizzo ip in questione è la Metasploitable possiamo vedere il suo sistema operativo in basso. Alcune macchine potrebbero avere regole che bloccano il traffico ICMP è dunque opportuno eseguire il comando "namp -Pn -O" così facendo possiamo eseguire l'OS fingerprint con luso della 3H.

```
(kali3㉿kali3) [~/Desktop]
$ sudo nmap -O 192.168.50.101
[sudo] password for kali3:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 11:58 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00025s 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: 08:00:27:4A:E1:25 (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 14.47 seconds
```



Con l'uso del comando nmap –sV effettuiamo una scansione dei servizi aperti su un host specifico, inoltre siamo in grado di vedere le versioni dei servizi in esecuzione qui viene usato sulla Metasploitable.

```
(kali3㉿kali3)-[~/Desktop]
$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 12:17 CEST
Stats: 0:00:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 65.22% done; ETC: 12:18 (0:00:11 remaining)
Stats: 0:01:59 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 69.57% done; ETC: 12:20 (0:00:47 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.000062s 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?
25/tcp    open  smtp?
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  ccproxy-ftp?
3306/tcp  open  mysql?
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  unknown
MAC Address: 08:00:27:4A:E1:25 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
(kali㉿kali3) [~/Desktop]
$ sudo nmap -sS 192.168.50.101
[sudo] password for kali3:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 11:08 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000079s 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: 08:00:27:4A:E1:25 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

```
(kali㉿kali3) [~/Desktop]
$ nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 11:35 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00042s 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

Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
```

Con nmap -sS effettuiamo una scansione SYN/ACK che è più veloce rispetto alle altre modalità di scansione ma meno accurata specialmente su reti con dispositivi di sicurezza avanzati o configurazioni particolari.

Con nmap -sT effettuiamo una scansione TCP connect, è più lenta rispetto ad altre modalità di scansione come la scansione SYN ma utile quando si vuole garantire un'accuratezza elevata nella rilevazione dello stato delle porte e a differenza della scansione SYN è facilmente rilevabile.

```
192.168.50....  
└──(kali㉿kali)-[~/Desktop]  
$ sudo nmap -Pn -O 192.168.50.103  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:53 CEST  
Nmap scan report for 192.168.50.103  
Host is up (0.00042s 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: 08:00:27:83:79:1F (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:wind  
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,  
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 15.75 seconds
```

```
└──(kali㉿kali)-[~/Desktop]  
$
```

Con l'uso del comando nmap –Pn –o effettuiamo una OS detection, la macchina corrispondente all'indirizzo ip in questione è Windows possiamo vedere il suo sistema operativo in basso.

In questo caso il firewall di Windows è stato appositamente modificato aggiungendo la regola che permette il traffico ICMP, in una situazione reale però in assenza della regola specifica con l'aggiunta di –PN al comando nmap si effettuerà una 3H al posto del ping.

```
(kali3㉿kali3)-[~/Desktop]
$ sudo nmap -Pn -o 192.168.50.103
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:01 CEST
Nmap scan report for 192.168.50.103
Host is up (0.00060s latency).
All 1000 scanned ports on 192.168.50.103 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:83:79:1F (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 36.95 seconds
```

Con l'uso del comando nmap –Pn –o effettuiamo una OS detection, la macchina cossispondete all'indirizzo ip in questione è Windows e in questo caso è assente la regola nel firewall di Windows che permette il traffico ICMP, anche con l'uso della 3H non abbiamo in ritorno informazioni utili sul OS del host specificato.