



## Traccia:

Tecniche di scansione con Nmap Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

OS fingerprint

Syn Scan

TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN? Version detection

## **Svolgimento:**

Scansione nmap -O per tentare di identificare il S.O. sulla macchina target... In questo caso l'identificazione non riesce ad identificare precisamente il sistema.

```
-(kali⊛kali)-[~]
 -$ <u>sudo</u> nmap -0 192.168.1.199
[sudo] password for kali:
Starting Nmap 7.94 (https://nmap.org) at 2024-01-19 13:33 EST
Nmap scan report for 192.168.1.199
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
      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: 08:00:27:9C:24:72 (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 18.35 seconds
```

## Scansione con nmap -sS

```
-(kali⊛kali)-[~]
└─$ <u>sudo</u> nmap -sS 192.168.1.199
Starting Nmap 7.94 (https://nmap.org) at 2024-01-19 13:42 EST
Nmap scan report for 192.168.1.199
Host is up (0.00058s 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: 08:00:27:9C:24:72 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 17.13 seconds
```

Scansione nmap -sT con completamento del threeWAY...

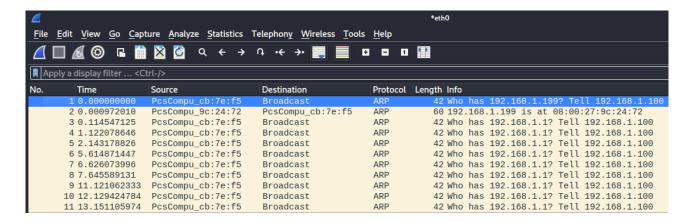
```
-(kali⊛kali)-[~]
<u>sudo</u> nmap -sT 192.168.1.199
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 13:45 EST
Nmap scan report for 192.168.1.199
Host is up (0.0072s latency).
Not shown: 977 closed tcp ports (conn-refused)
        STATE SERVICE
PORT
21/tcp
       open ftp
22/tcp open ssh
23/tcp 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: 08:00:27:9C:24:72 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 16.92 seconds
```

```
$ <u>sudo</u> nmap -sV 192.168.1.199
Starting Nmap 7.94 (https://nmap.org) at 2024-01-19 13:49 EST Nmap scan report for 192.168.1.199
Host is up (0.00041s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
            open ftp
22/tcp
                                   OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
Linux telnetd
           open
                   ssh
23/tcp
                    telnet
           open
25/tcp
            open
                    smtp
                                    Postfix smtpd
                                    ISC BIND 9.4.2
53/tcp
           open
                    domain
                                    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
80/tcp
           open
111/tcp
139/tcp
           open
                    rpcbind
                                    2 (RPC #100000)
                   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
           open
445/tcp
           open
512/tcp open
513/tcp open
                                    netkit-rsh rexecd
                    login?
514/tcp open
                    shell
                                    Netkit rshd
1099/tcp open
1524/tcp open
2049/tcp open
                                    GNU Classpath grmiregistry
                    java-rmi
                    bindshell
                                    Metasploitable root shell
                                    2-4 (RPC #100003)
2121/tcp open
                                    ProFTPD 1.3.1
 3306/tcp open
                    mysql
                                    MySQL 5.0.51a-3ubuntu5
                                   PostgreSQL DB 8.3.0 - 8.3.7 VNC (protocol 3.3)
5432/tcp open
                    postgresql
5900/tcp open
6000/tcp open
                                    (access denied)
6667/tcp open
                   irc
                                    UnrealIRCd
8009/tcp open
                   ajp13
                                   Apache Jserv (Protocol v1.3)
Apache Tomcat/Coyote JSP engine 1.1
8180/tcp open http
MAC Address: 08:00:27:9C:24:72 (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 116.33 seconds
```

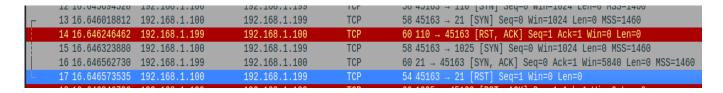
## Di seguito vengono allegate le catture fatte con WireShark per vedere la differenza tra una scan che non completa il threeWay ed una che lo cpmpleta

Le macchine sono sulla stessa rete 192.168.1.0/24

Cattura dei pacchetti ARP che cercano il target



Prendendo da esempio la porta 21 vediamo che dopo il SYN e il SYN ACK viene inviato un RST



Prendiamo da esempio la porta 22 e vediamo il completamento del threeWay

_					
4	12 16.627124380	192.168.1.100	192.168.1.199	TCP	74 52806 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1326365134 T
	13 16.627352332	192.168.1.100	192.168.1.199	TCP	74 41766 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1326365134
	14 16.627535544	192.168.1.100	192.168.1.199	TCP	74 36710 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1326365134
	15 16.627679080 1	192.168.1.100	192.168.1.199		74 47568 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1326365134 T
	16 16.627821655	192.168.1.199	192.168.1.100	TCP	74 22 → 52806 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=21
	17 16.627842633 1	192.168.1.100	192.168.1.199	TCP	66 52806 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1326365135 TSecr=215934
	40 40 007054045	100 100 1 100	100 100 1 100	TOD	