

In questo report faccio un report riguardo i diversi tipi di scansione di Nmap

1-Metasploitable

i- OS fingerprint

Usando **nmap -O** ip: mi ha mostrato le porte aperte con i nomi di servizi sul target, ci mostra anche il sistema operativo del target nel nostro caso e **Linux_kernel: 2.6**

```
File Actions Edit View Help
(root@kali)-[/home/kali]
# nmap -O 192.168.1.5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:00 EDT
Nmap scan report for 192.168.1.5
Host is up (0.0011s 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: 08:00:27:39:6D:CD (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
```

ii- SYN vs TCP scan:

eseguendo **nmap -sS** per SYN scan e **nmap -sT** per TCP scan me ha risolto

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.1.5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:27 EDT
Nmap scan report for 192.168.1.5
Host is up (0.0017s 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: 08:00:27:39:6D:CD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.51 seconds
```

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.1.5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:26 EDT
Nmap scan report for 192.168.1.5
Host is up (0.0026s 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: 08:00:27:39:6D:CD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds
```

Per poter vedere la differenza ho catturato i pacchetti da wireshark vedendo che SYN scan interrompe la connessione e non termina il **3WH**, mentre TCP scan lo fa
Come mostrato in figura

a- SYN scan: la connessione e terminata prima di completare il **3WH**

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No	Tin	Source	Destination	Protocol	Length	Info
1	0...	PcsCompu_db...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.10
2	1...	PcsCompu_db...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.10
3	4...	192.168.1.10	192.168.1.5	TCP	58	37513 → 23 [SYN] Seq=0 Win=0 Len=0 MSS=1460
4	4...	192.168.1.5	192.168.1.10	TCP	60	23 → 37513 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
5	4...	192.168.1.10	192.168.1.5	TCP	54	37513 → 23 [RST] Seq=1 Win=0 Len=0
6	4...	192.168.1.10	192.168.1.20	TCP	58	38508 → 497 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.1.5 -p 23
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 09:37 EDT
Nmap scan report for 192.168.1.5
Host is up (0.00038s latency).

PORT      STATE SERVICE
23/tcp    open  telnet
MAC Address: 08:00:27:39:6D:CD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds
```

b- TCP Scan

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No	Tin	Source	Destination	Protocol	Length	Info
1	0...	PcsCompu_db...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.10
2	1...	PcsCompu_db...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.10
3	2...	PcsCompu_db...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.10
4	3...	PcsCompu_db...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.10
5	6...	192.168.1.10	192.168.1.5	TCP	74	43244 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
6	6...	192.168.1.5	192.168.1.10	TCP	74	23 → 43244 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
7	6...	192.168.1.10	192.168.1.5	TCP	66	43244 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0
8	6...	192.168.1.10	192.168.1.5	TCP	66	43244 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
9	7...	192.168.1.10	192.168.1.20	TCP	58	38506 → 1027 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.1.5 -p 23
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 09:35 EDT
Nmap scan report for 192.168.1.5
Host is up (0.00044s latency).

PORT      STATE SERVICE
23/tcp    open  telnet
MAC Address: 08:00:27:39:6D:CD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds
```

iii- **Version:** usando **nmap -sV ip**, mi mostra tutte le porte aperte con versioni dei servizi

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.1.5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 10:14 EDT
Nmap scan report for 192.168.1.5
Host is up (0.00049s 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?       detailed info on this state actively (for debugging)
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: 08:00:27:39:6D:CD (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/subm
```

2- Win7

```
File Actions Edit View Help
(root@kali)-[/home/kali]
# nmap -O 192.168.1.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:01 EDT
Nmap scan report for 192.168.1.20
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.1.20 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:09:17:09 (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 37.45 seconds
```