

## Report nmap

1- Come prima task andiamo ad effettuare delle scansioni su Metasploitable (Ip 192.168.1.102):

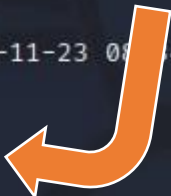
-Prima scansione nmap -O per ricevere informazioni sul sistema operativo.

```
MAC Address: 08:00:27:F0:63:36 (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 15.18 seconds
```

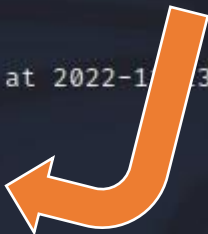
-Seconda scansione nmap -sT stabilisce una connessione completa con il target completando il three-way-handshake. Notiamo come per le porte chiuse ci da come risposta "(conn-refused)".

```
(root@kali)~[/home/kali]
# nmap -sT 192.168.1.102
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 08:34 EST
Nmap scan report for 192.168.1.102
Host is up (0.0039s 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
```



-Terza scansione nmap -sS non stabilisce una connessione completa. E a differenza della tcp connection possiamo vedere come per le porte chiuse ci da come risposta "(reset)"

```
(root@kali)~[/home/kali]
# nmap -sS 192.168.1.102
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 08:33 EST
Nmap scan report for 192.168.1.102
Host is up (0.00018s 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
```



-Quarta scansione nmap -sV ci recupererà la versione relativa ad ogni servizio delle porte aperte eseguendo prima una Tcp connection e poi un grab del banner

```
nmap -sV 192.168.1.102
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 08:35 EST
Nmap scan report for 192.168.1.102
Host is up (0.00015s 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?
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:F0:63:36 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

2- Come seconda task andiamo a effettuare un OS fingerprint di windows 7 (192.168.1.104)

-Con firewall attivo su windows non riesco a recuperare informazioni

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 08:21 EST
Nmap scan report for 192.168.1.104
Host is up (0.00079s latency).
All 1000 scanned ports on 192.168.1.104 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:B9:0D:44 (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 27.08 seconds
```

-Con il firewall disattivato riesco a recuperare informazioni precise

```
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
1 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 16.40 seconds
```

-Come ultimo tentativo sono andato a modificare o ad attivare delle regole nelle impostazioni del firewall riuscendo a recuperare delle informazioni ma poco precise.

```
445/tcp open  microsoft-ds
49154/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:B9:0D:44 (Oracle VirtualBox virtual NIC)
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
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 27.37 seconds
```