

# SCANSIONE DEI SERVIZI CON NMAP

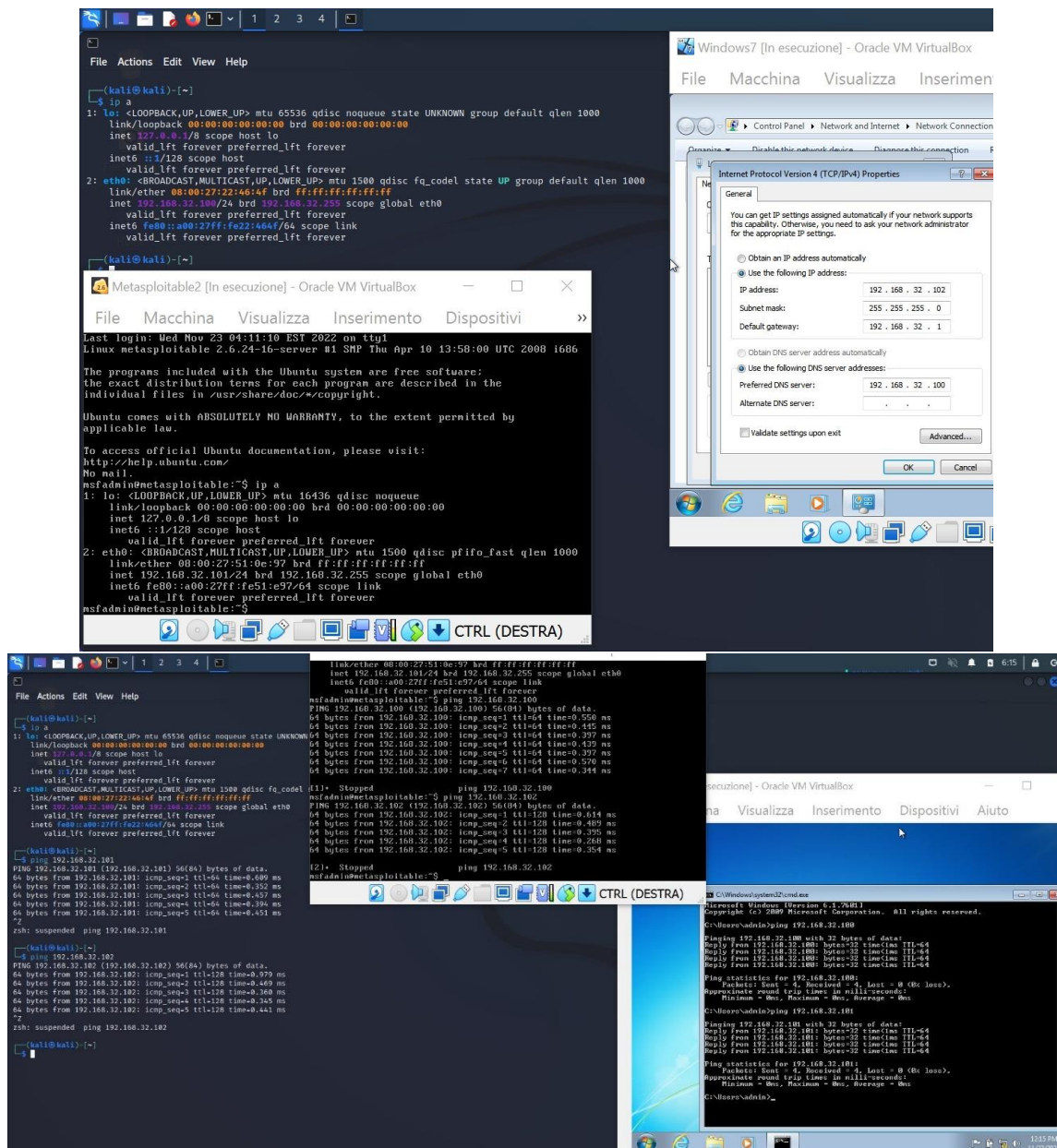
Nell'esercizio di oggi dovremmo effettuare delle scansioni sui target Metasploitable2 e Windows7.

Su Metasploitable2 dovremmo fare scan di:

- OS fingerprint
- SYN scan
- TCP connect
- Version detection

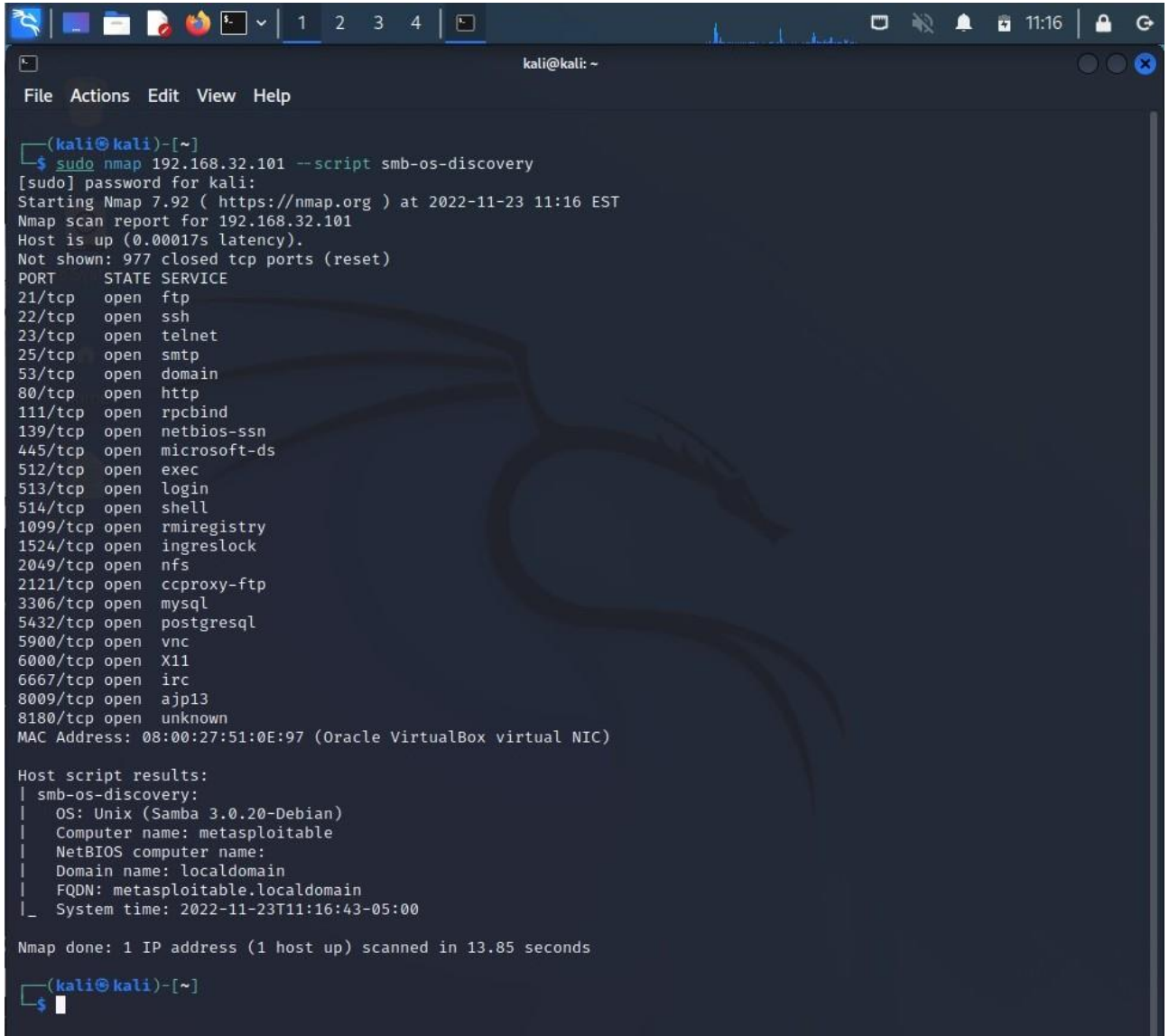
Su Windows7 dovremmo fare una OS fingerprint scan.

Prima di tutto abbiamo impostato le tre macchine (Kali, Metasploitable2, Windows7) sulla stessa rete, controllando il ping tra di esse.



Una volta impostate le tre macchine, siamo andati ad effettuare le scansioni di Metasploitable2 con nmap, tramite i comandi:

- Nmap "IP target" --script smb-os-discovery per l'utilizzo della feature di OS fingerprint:



```
(kali@kali)-[~]
$ sudo nmap 192.168.32.101 --script smb-os-discovery
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 11:16 EST
Nmap scan report for 192.168.32.101
Host is up (0.00017s 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: 08:00:27:51:0E:97 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-11-23T11:16:43-05:00

Nmap done: 1 IP address (1 host up) scanned in 13.85 seconds
(kali@kali)-[~]
$
```

Nmap recupera delle informazioni dalle risposte ricevute e le confronta con quelle in suo possesso per stimare il sistema operativo utilizzato.

Qui possiamo vedere che l'OS utilizzato da Metasploitable2 è Unix (Samba 3.0.20-Debian)

- -sS per la SYN scan (stealth scan):

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.32.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 05:28 EST
Nmap scan report for 192.168.32.101
Host is up (0.00019s 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: 08:00:27:51:0E:97 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
(kali@kali)-[~]
$
```

La scansione verifica lo stato delle porte analizzando le risposte date durante il 3-way-handshake senza però terminarlo; si fermerà alla fase di SYN+ACK avendo la certezza che la porta sia aperta.

- -sT per la scansione TCP connect:

```
(kali@kali)-[~]
$ sudo nmap -sT 192.168.32.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 05:31 EST
Nmap scan report for 192.168.32.101
Host is up (0.0018s 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: 08:00:27:51:0E:97 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
(kali@kali)-[~]
$
```

La scansione verifica lo stato delle porte analizzando le risposte completando il 3-way-handshake; in caso di risposta RST/ACK la porta risulterà chiusa e, a differenza della

scansione con -sS, per le porte chiuse darà "conn-refused" in quanto il 3-way-handshake non verrà concluso.

- -sV per la scansione version detection:

```
(kali@kali)-[~]
$ sudo nmap -sV -sT 192.168.32.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 05:46 EST
Nmap scan report for 192.168.32.101
Host is up (0.00068s latency).
Not shown: 977 closed tcp ports (conn-refused)
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: 08:00:27:51:0E:97 (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 66.24 seconds
```

Nmap eseguirà una scansione TCP connect abilitando però la feature di version detection, andando ad identificare la versione e relativi dettagli dei servizi tramite il banner grabbing.

Siamo ora andati ad effettuare la scansione di OS fingerprint su Windows7:

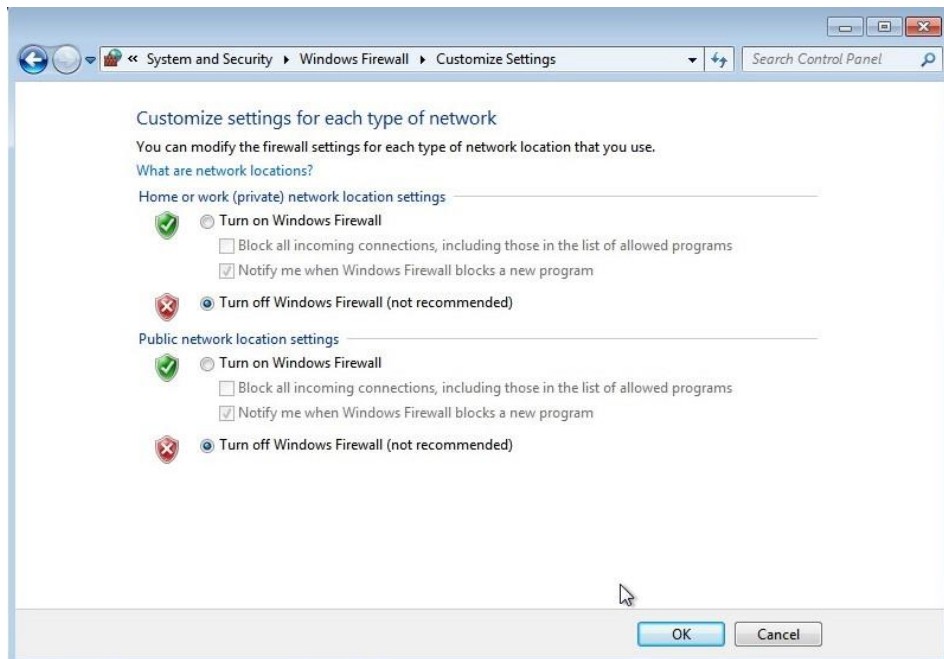
```
(kali@kali)-[~]
$ sudo nmap -O 192.168.32.102
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 06:02 EST
Nmap scan report for 192.168.32.102
Host is up (0.00052s latency).
All 1000 scanned ports on 192.168.32.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:E7:08:B4 (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 41.23 seconds

(kali@kali)-[~]
$
```

Come possiamo vedere non risulta possibile verificare il sistema operativo utilizzato, andremo quindi a disabilitare i FireWall di Windows7 e andremo a riprovare la scansione:





```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.32.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 05:49 EST
Nmap scan report for 192.168.32.102
Host is up (0.00044s 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:E7:08:B4 (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:windows_server_2008::sp1 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 16.55 seconds

(kali㉿kali)-[~]
$
```

Com'è possibile vedere adesso possiamo visualizzare il sistema operativo utilizzato, in questo caso Microsoft Windows 7|2008|8.1 .