

## SCANSIONE SERVIZI CON NMAP

Come primo passo, ci viene chiesto di trovare il sistema operativo della macchina Metasploitable con IP 192.168.32.102; usiamo il comando `-O` di nmap per scoprirlo:

```
(kali@kali)~$ sudo su
[sudo] password for kali:
(root@kali)~$ # nmap -O 192.168.32.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 04:42 EST
Nmap scan report for 192.168.32.102
Host is up (0.00057s 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:E2:A5:64 (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 14.98 seconds
```

Sempre su Meta, usiamo il comando `-sS` per effettuare lo scan meno invasivo delle porte in modo da poter trovare i servizi attivi sull' host scelto:

```
(root@kali)~$ # nmap -sS 192.168.32.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 04:44 EST
Nmap scan report for 192.168.32.102
Host is up (0.00037s 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:E2:A5:64 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.33 seconds
```

Con lo scan `-sT`, chiamato anche TCP connect, otteniamo comunque lo stesso risultato dello scan precedente, ma il metodo è molto più invasivo in quanto stabilisce direttamente una connessione con l'host, a differenza del `-sS` che dropa lo scan una volta che ha ricevuto la risposta:

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.32.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 04:53 EST
Nmap scan report for 192.168.32.102
Host is up (0.0093s 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:E2:A5:64 (Oracle VirtualBox virtual NIC)

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

Ultimo scan da effettuare è quello per scoprire le versioni dei servizi attivi su macchina Meta, utilizziamo qui il comando `-sV` sempre da nmap:

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.32.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 06:15 EST
Nmap scan report for 192.168.32.102
Host is up (0.00026s 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:E2:A5:64 (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 66.00 seconds
```

Per poter effettuare scan verso la macchina Windows, va prima aggiunta una policy su Windows Firewall che permetta alla macchina Kali di comunicare;

Lanciando il comando per scoprire il sistema operativo di Windows, nmap non ha trovato subito la giusta versione, ma ha fatto delle supposizioni:

```
(root@kali) ~/home/kali
# nmap -O 192.168.32.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 05:03 EST
Nmap scan report for 192.168.32.101
Host is up (0.00071s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:44:8F:FC (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::-professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::-cp
e:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2
008 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 20.64 seconds
```

In questo caso ho risolto facendo lo scan aggressivo -A ( si può usare anche lo script smb-os-discovery):

```
Host script results:
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
|_ NetBIOS name: ALESSIO-PC, NetBIOS user: unknown, NetBIOS MAC: 08:00:27:44:8f:fc (Oracle VirtualBox virtual NIC)
smb-os-discovery:
| OS: Windows 7 Home Premium 7601 Service Pack 1 (Windows 7 Home Premium 6.1)
| OS CPE: cpe:/o:microsoft:windows_7::sp1
| Computer name: ALESSIO-PC
| NetBIOS computer name: ALESSIO-PC\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2022-11-23T10:22:53+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb-time:
|   date: 2022-11-23T09:22:53
|_ start_date: 2022-11-23T09:02:41
|_ clock-skew: mean: -1h20m01s, deviation: 34m38s, median: -1h00m01s

TRACEROUTE
HOP RTT ADDRESS
1 0.79 ms 192.168.32.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.56 seconds
```