

Tecniche di scansione con Nmap su target Metasploitable:

- OS fingerprint
- Syn scan
- TCP connect
- version detection

Tecniche di scansione con Nmap su target Windows 7:

- OS fingerprint

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)~[~]  
$ sudo nmap -O 192.168.32.101  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 18:54 CET  
Nmap scan report for 192.168.32.101  
Host is up (0.00053s 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:F4:08:97 (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 http://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 16.27 seconds  
  
(kali@kali)~[~]  
$
```

Tecnica OS fingerprint da VM Kali sulla VM Metasploitable

Da VM Kali, attraverso il port scanner Nmap, si esegue il processo: *OS fingerprint*, sulla VM Metasploitable, stimando il sistema operativo del target, ispezionando i pacchetti di risposta ricevuti e confrontandoli con le informazioni in suo possesso.

Da terminale si esegue il comando: `sudo nmap -O 192.168.32.101` .

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo nmap -sS 192.168.32.101  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 19:08 CET  
Nmap scan report for 192.168.32.101  
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  
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:F4:08:97 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.84 seconds  
  
(kali@kali)-[~]  
$
```

Tecnica SYN scan da VM Kali sulla VM Metasploitable

Da VM Kali, attraverso il port scanner Nmap, si esegue la tecnica: *SYN scan*, sulla VM Metasploitable, una scansione furtiva in quanto non stabilisce una connessione completa con essa ma, recupera solo le informazioni riguardo le porte aperte.

Da terminale si esegue il comando: `sudo nmap -sS 192.168.32.101` .

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo nmap -sT 192.168.32.101  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 19:21 CET  
Nmap scan report for 192.168.32.101  
Host is up (0.0020s 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:F4:08:97 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds  
  
(kali@kali)-[~]  
$
```

Tecnica TCP connect da VM Kali sulla VM Metasploitable

Da VM Kali, attraverso il port scanner Nmap, si esegue la tecnica: *TCP connect*, sulla VM Metasploitable, una scansione che viene registrata nel log delle applicazioni che ascoltano sulla rete target, in quanto stabilisce una connessione con il demone in ascolto, completando il *three-way-handshake*.

Da terminale si esegue il comando: `sudo nmap -sT 192.168.32.101` .

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo nmap -sV 192.168.32.101  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 20:04 CET  
Nmap scan report for 192.168.32.101  
Host is up (0.00025s 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: WORKGRO  
UP)  
445/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGRO  
UP)  
512/tcp   open  exec          netkit-rsh rexecd  
513/tcp   open  login?        Netkit rshd  
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:F4:08:97 (Oracle VirtualBox virtual NIC)  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitabl  
e.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 67.26 seconds  
  
(kali@kali)-[~]  
$
```

Tecnica version detection da VM Kali sulla VM Metasploitable

Da VM Kali, attraverso il port scanner Nmap, si esegue la tecnica: *version detection*, sulla VM Metasploitable, una scansione TCP con l'aggiunta di specifici test per la rivelazione dei servizi in ascolto su una porta, ma, anch'essa, è più tosto facile da rilevare, in quanto genera molto traffico di rete.

Da terminale si esegue il comando: `sudo nmap -sV 192.168.32.101` .


```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo nmap -O 192.168.32.102  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 20:12 CET  
Nmap scan report for 192.168.32.102  
Host is up (0.00070s 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:D7:B6:F5 (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 http  
s://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 40.90 seconds  
  
(kali@kali)-[~]  
$
```

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo nmap -O 192.168.32.102  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-23 20:17 CET  
Nmap scan report for 192.168.32.102  
Host is up (0.00075s latency).  
Not shown: 990 closed tcp ports (reset)  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
5357/tcp   open  wsdapi  
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:D7:B6:F5 (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::s  
p1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windo  
ws_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windo  
ws_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 http  
s://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 17.24 seconds  
  
(kali@kali)-[~]  
$
```

Tecnica OS fingerprint da VM Kali sulla VM Windows 7

Da VM Kali, attraverso il port scanner Nmap, si esegue il processo: *OS fingerprint*, sulla VM Windows 7, stimando il sistema operativo del target, ispezionando i pacchetti di risposta ricevuti e confrontandoli con le informazioni in suo possesso ma, come mostrato nell'immagine a sinistra, a causa del firewall di Windows attivo, la scansione risulta impossibile, mentre, a firewall disattivato, come mostrato nell'immagine a destra, la scansione risulta completa.

Da terminale si esegue il comando: `sudo nmap -O 192.168.32.102` .