

REPORT

Nel seguente report verranno utilizzati diversi tipi di scansione su Metasploitable e OS fingerprint su Windows 7.

Metasploitable

La prima scansione che andiamo ad eseguire è **OS fingerprint**. Come si vede nell'immagine vengono restituite le porte aperte e il servizio in ascolto di ognuna di esse.

Verso le ultime righe viene specificato il sistema operativo di Metasploitable, ovvero il programma che viene scansionato da Kali Linux. In questo caso Metasploitable utilizza la versione 2.6 del sistema operativo Linux.

```
(root@kali)~[/home/kali]
# nmap -o 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:48 EST
Nmap scan report for 192.168.49.101
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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

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
```

La seconda scansione viene scritta con **sS**: detto anche **SYN scan**, è un metodo meno invasivo rispetto ad sT in quanto nmap, una volta ricevuto il pacchetto SYN/ACK dalla macchina target, non conclude il 3-way-handshake, ma appurato che la porta è aperta chiude la comunicazione, di fatto evitando overload dato dalla creazione del canale.

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:45 EST
Nmap scan report for 192.168.49.101
Host is up (0.0012s 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

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

La terza scansione è detta TCP connect ed è più invasiva della SYN scan , in quanto per controllare se una porta è aperta o meno e recuperare informazioni sul servizio in ascolto, nmap completa tutti i passaggi del 3-way-handshake, stabilendo di fatto un canale.

In questo caso non ci sono differenze tra i due metodi perché non sono presenti sistemi difensivi su Metasploitable e quindi, non essendoci nessun blocco passano tutte le informazioni.

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:46 EST
Nmap scan report for 192.168.49.101
Host is up (0.0024s 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

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
```

L'ultima scansione, oltre le informazioni che abbiamo raccolto con le precedenti, ci restituisce le versioni di ogni porta aperta.

```
(root@kali)~[/home/kali]
# nmap -sV 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:46 EST
Nmap scan report for 192.168.49.101
Host is up (0.0012s 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 rshcd
513/tcp   open  login?
514/tcp   open  tcpwrapped
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Windows 7

Anche in Windows 7 viene eseguito OS fingerprint.

```
(root@kali) ~/home/kali
nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:47 EST
Nmap scan report for 192.168.50.102
Host is up (0.00040s 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: 08:00:27:0D:05:F2 (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 36.80 seconds
```