Identificazione servizi e scansione (Nmap)

Target: Metasploitable2 192.168.30.200

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O  192.168.30.200
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 09:10 EST
Nmap scan report for 192.168.30.200
Host is up (0.00032s 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: 08:00:27:6B:CE:22 (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.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.69 seconds
```

Con questa prima scansione possiamo ottenere informazioni circa le porte ed i servizi attivi su esse, inoltre possiamo anche estrapolare il sistema operativo della vittima.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.30.200 --script smb-os-discovery
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 10:15 EST
Nmap scan report for 192.168.30.200
Host is up (0.00027s 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

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: 2023-02-22T10:15:53-05:00

Nmap done: 1 IP address (1 host up) scanned in 13.36 seconds
```

Invocando lo script smb-os-discovery otteniamo un' analisi dettagliata sul sistema operativo vittima

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV  192.168.30.200
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 09:41 EST
Nmap scan report for 192.168.30.200
Host is up (0.000099s 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       OpenBSD or Solaris rlogind
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: 08:00:27:6B:CE:22 (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 24.71 seconds
```

Applicando invece la flag -sV otteniamo oltre ai demoni dei servizi in ascolto sulle porte anche la versione del servizio stesso oltretutto otteniamo anche maggiori informazioni sul sistema operativo della macchina scansionata.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS  192.168.30.200
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 10:12 EST
Nmap scan report for 192.168.30.200
Host is up (0.00012s 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: 08:00:27:6B:CE:22 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT  192.168.30.200
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 10:11 EST
Nmap scan report for 192.168.30.200
Host is up (0.00021s 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: 08:00:27:6B:CE:22 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds
```

Facendo la scansione SYN possiamo notare a differenza di quella completa, la mancanza della specifica (conn-refused) nelle porte che sono state bloccate, dato che la prima non conclude il thre-hand-handshake ed invia il reset dopo l'eventuale risposta.

Per quanto riguarda windows, il firewall blocca tutte le connessioni in entrata quindi non possiamo utilizzare un metodo convenzionale per scansionare le porte, quindi un modo per aggirare questo problema sarebbe abbattere il firewall o aggiungere delle regole più permissive.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT  192.168.30.150
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 09:52 EST
Nmap scan report for 192.168.30.150
Host is up (0.00030s latency).
All 1000 scanned ports on 192.168.30.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:7F:0A:13 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 36.70 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS  192.168.30.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 09:53 EST
Nmap scan report for 192.168.30.150
Host is up (0.00027s latency).
All 1000 scanned ports on 192.168.30.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:7F:0A:13 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 37.72 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O  192.168.30.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-22 09:04 EST
Nmap scan report for 192.168.30.150
Host is up (0.00034s latency).
Not shown: 991 filtered tcp ports (no-response)
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
MAC Address: 08:00:27:7F:0A:13 (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
:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft W
08 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 19.40 seconds
```