

## **Scansione dei servizi con Nmap**

### **Descrizione dell'ambiente**

I test descritti di seguito sono stati effettuati attraverso un laboratorio realizzato con VirtualBox, all'interno del quale si trovano tre macchine virtuali che hanno degli indirizzi IP statici e connesse alla stessa rete interna:

- Kali Linux (192.168.50.100);
- Metasploitable 2 (192.168.50.101);
- Windows 7 (192.168.50.102).

### **Cosa si andrà a fare**

Ho effettuato delle scansioni con Kali Linux utilizzando Nmap, ovvero un software per la scansione di porte di rete. Come target, pertanto, sono stati scelti Metasploitable 2 e Windows 7.

## Prima scansione

La prima scansione l'ho effettuata su Metasploitable 2.

Da Kali, ho lanciato il comando

```
nmap -O 192.168.50.101
```

attraverso il quale riesco a determinare il sistema operativo e la versione di quest'ultimo in esecuzione su uno specifico host.

Infatti, l'output ricevuto è il seguente

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)~  
# nmap -O 192.168.50.101  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:37 CEST  
Nmap scan report for 192.168.50.101  
Host is up (0.0090s 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: 08:00:27:4A:AD:67 (Oracle VirtualBox virtual NIC)  
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).  
TCP/IP fingerprint:  
OS:SCAN(V=7.94%E=4%D=10/25%OT=21%CT=1%CU=34571%PV=Y%DS=1%DC=D%G=Y%M=080027%  
OS:TM=65390C0A%P=x86_64-pc-linux-gnu)SEQ(SP=C3%GCD=1%ISR=CB%TI=Z%CI=Z%II=I%  
OS:TS=5)SEQ(SP=C4%GCD=1%ISR=CB%TI=Z%CI=Z%II=I%TS=5)OPS(O1=M5B4ST11NW7%O2=M5  
OS:B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(  
OS:W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0  
OS:%O=M5B4NNSNW7%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R  
OS:=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M5B4ST11NW7%RD=0%Q=)T4(R=Y%DF=Y%T=40  
OS:%W=0%A=Z%F=R%O=0%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=0%RD=0%Q  
OS:=)T6(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=0%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A  
OS:=S+%F=AR%O=0%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%R  
OS:UCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)  
  
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 24.75 seconds  
(root@kali)~  
#
```

dal quale si può dedurre che:

- l'host 192.168.50.101 è in esecuzione e ha una latenza di 0,009 secondi;
- l'host ha 101 porte aperte, 977 porte chiuse e 0 porte filtrate;
- le porte aperte includono:
  - 21/tcp (FTP)

- 22/tcp (SSH)
  - 23/tcp (Telnet)
  - 25/tcp (SMTP)
  - 53/tcp (Domain)
  - 80/tcp (HTTP)
  - 111/tcp (RPCbind)
  - 139/tcp (NetBIOS-ssn)
  - 445/tcp (Microsoft-ds)
  - 512/tcp (Exec)
  - 513/tcp (Login shell)
  - 1099/tcp (Remiregistry)
  - 1524/tcp (Ingreslock)
  - 2049/tcp (Nfs)
  - 2121/tcp (Ccproxy-ftp)
  - 3306/tcp (Mysql)
  - 5432/tcp (Postgresql)
  - 5900/tcp (X11)
  - 6667/tcp (1rc)
  - 8009/tcp (Ajp13)
  - 8180/tcp (Ajp13)
  - 8180/tcp (Sconosciuto)
- l'host è probabilmente in esecuzione su un sistema operativo Linux, ma non è possibile determinare con certezza il sistema operativo specifico.

In base a questo output, è possibile ipotizzare che l'host sia un server web o un server di file. Le porte aperte 21, 80, 443 e 5900 sono spesso utilizzate per questi tipi di server. La porta 22 è spesso utilizzata per l'accesso SSH, che può essere utilizzato per eseguire comandi sul sistema. La porta 25 è spesso utilizzata per l'invio di e-mail. Le porte 139 e 445 sono spesso utilizzate per la condivisione di file e stampanti su reti Windows.

Ho poi lanciato il comando

*`nmap -sS 192.168.50.101`*

attraverso il quale sono andato ad eseguire una scansione di porte TCP SYN. La scansione SYN è una tecnica di scansione delle porte che invia un pacchetto SYN a una porta specifica. Se il server risponde con un

pacchetto SYN+ACK, la porta è aperta. Se il server risponde con un pacchetto RST, la porta è chiusa.

La scansione SYN è una tecnica di scansione poco affidabile, abbastanza rilevabile e poco intensiva in quanto a spreco di risorse.

L'output ricevuto è il seguente

```
(root@kali)-[~]
# nmap -sS 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:39 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0061s 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: 08:00:27:4A:AD:67 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.59 seconds

(root@kali)-[~]
#
```

dal quale è possibile dedurre quanto segue:

- l'host ha una latenza di 0,0061 secondi;
- il MAC address dell'host è 08:00:27:4A:AD:67. Questo MAC address è associato a una scheda di rete virtuale Oracle VirtualBox. Questo indica che l'host è probabilmente un sistema virtuale in esecuzione su un computer host.

Successivamente ho lanciato il comando

```
nmap -sT 192.168.50.101
```

il quale esegue una scansione SYN su un host o una rete. Lo scan SYN è stealth, il che significa che è meno probabile che venga rilevato da un firewall. Inoltre è più intensiva rispetto al comando precedente.

Il suo output includerà una colonna “Stato” per ogni porta. Gli stati possibili sono:

- Open: la porta è aperta;
- Closed: la porta è chiusa;
- Filtered: la porta è filtrata da un firewall o da un IDS;
- Unreachable: il server non è raggiungibile;
- Open|Filtered: la porta è aperta o filtrata.

L’output ricevuto infatti è il seguente

```
(root@kali)-[~]
# nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:42 CEST
Nmap scan report for 192.168.50.101
Host is up (0.010s 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: 08:00:27:4A:AD:67 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.54 seconds

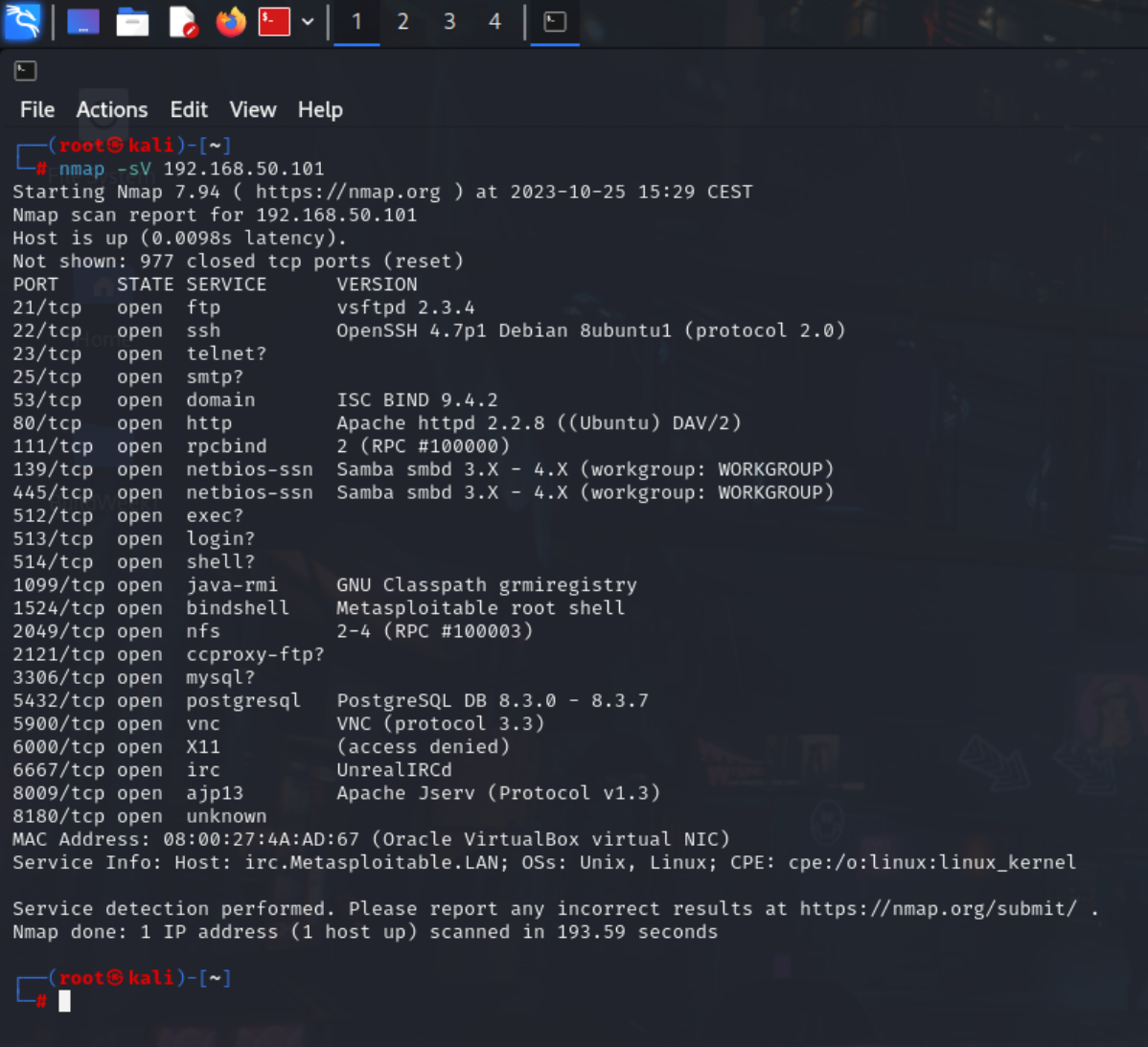
(root@kali)-[~]
#
```

Infine, ho lanciato il comando

```
nmap -sV 192.168.50.101
```

il quale esegue uno scan di versione su un host o una rete. Questo tipo di scansione tenta di identificare il sistema operativo, il servizio e la versione del software in esecuzione su ogni porta aperta.

L'output è il seguente



```
(root@kali)~# nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:29 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0098s 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?
25/tcp    open  smtp?
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?
513/tcp   open  login?
514/tcp   open  shell?
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  ccproxy-ftp?
3306/tcp  open  mysql?
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  unknown
MAC Address: 08:00:27:4A:AD:67 (Oracle VirtualBox virtual NIC)
Service Info: Host: 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 193.59 seconds

(root@kali)~#
```

## Seconda scansione

Il target per la seconda scansione è Windows 7. C'è da dire che ho dovuto disattivare il firewall per poter scansionare adeguatamente questa macchina.

In questo caso ho eseguito il comando

`nmap -O 192.168.50.102`

L'output è il seguente

```
root@kali:~# nmap -O 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:42 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0012s 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:C8:83:05 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7/2008/8.1
OS CPE: cpe:/o:microsoft:windows_7::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 15.39 seconds
root@kali:~#
```

dal quale si può dedurre che:

- l'host è in esecuzione e ha un tempo di latenza di 0,00125 secondi;
- sono presenti 991 porte chiuse, ma non vengono visualizzate;
- sono presenti 5 porte aperte:
  - 135/tcp: msrpc;
  - 139/tcp: netbios-ssn;
  - 445/tcp:microsoft-ds;
  - 49152/tcp: sconosciuto;
  - 49153/tcp: sconosciuto.
- l'indirizzo MAC dell'host è 08:00:27:C8:83:25;
- il tipo di dispositivo è generale;
- il sistema operativo è Microsoft Windows 7/2008 R2;
- la versione del sistema operativo è una delle seguenti:
  - Microsoft Windows 7 SP1;
  - Microsoft Windows Server 2008 SP1;
  - Microsoft Windows Server 2008 R2;
  - Microsoft Windows 8;
  - Microsoft Windows 8.1 Update 1;
- la distanza di rete è di 1 hop.

Inoltre, si può dedurre che l'host è probabilmente un computer desktop o un server. Le porte aperte indicano che l'host esegue servizi come Microsoft RPC, NetBIOS e Microsoft Active Directory.

**END**