Gabriele Di giampietro **Data 23/11/2022**

- **Obbiettivo: Effettuare delle scansioni con "nmap" su due nostre VM collegate su linea interna: per Metasploitable eseguire OS fingerprint, Syn scan, TCP scan e Versione detection. Per Windows 7 eseguire solamente l'OS fingerprint e valutarne i risultati con possibili soluzioni.**

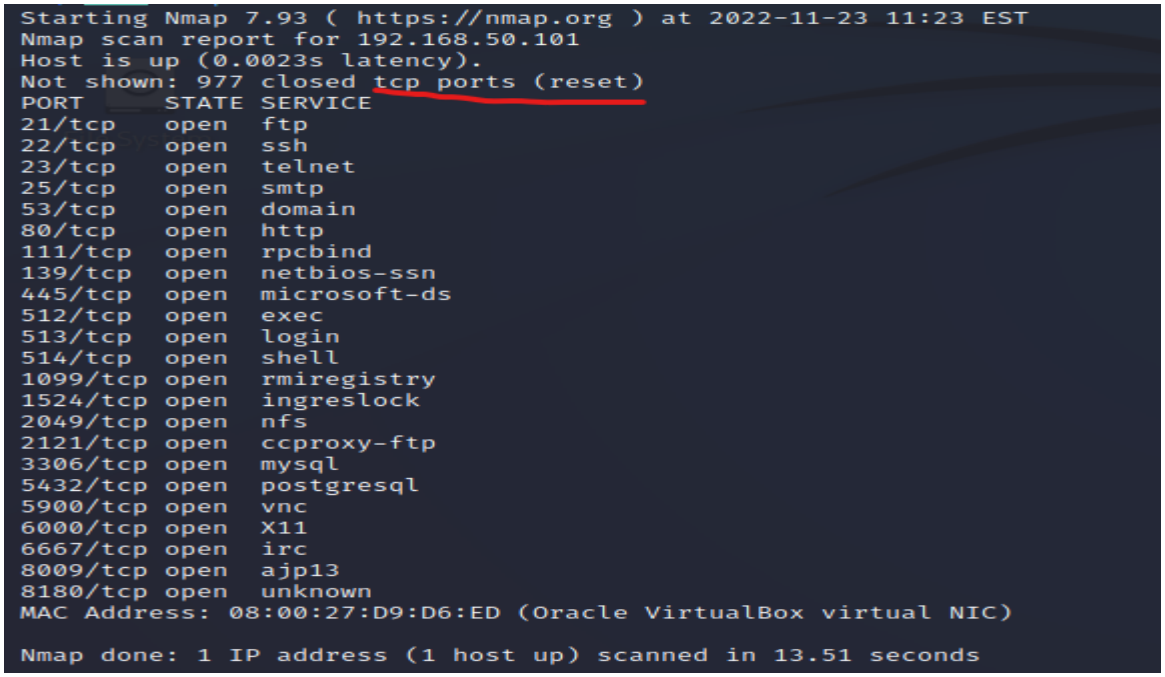
Metasploitable ip 192.168.50.101 OS fingerprint:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O -T5 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 11:20 EST
Nmap scan report for 192.168.50.101
Host is up (0.0020s 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:D9:D6:ED (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
```

Metasploitable ip 192.168.50.101 Syn scan:

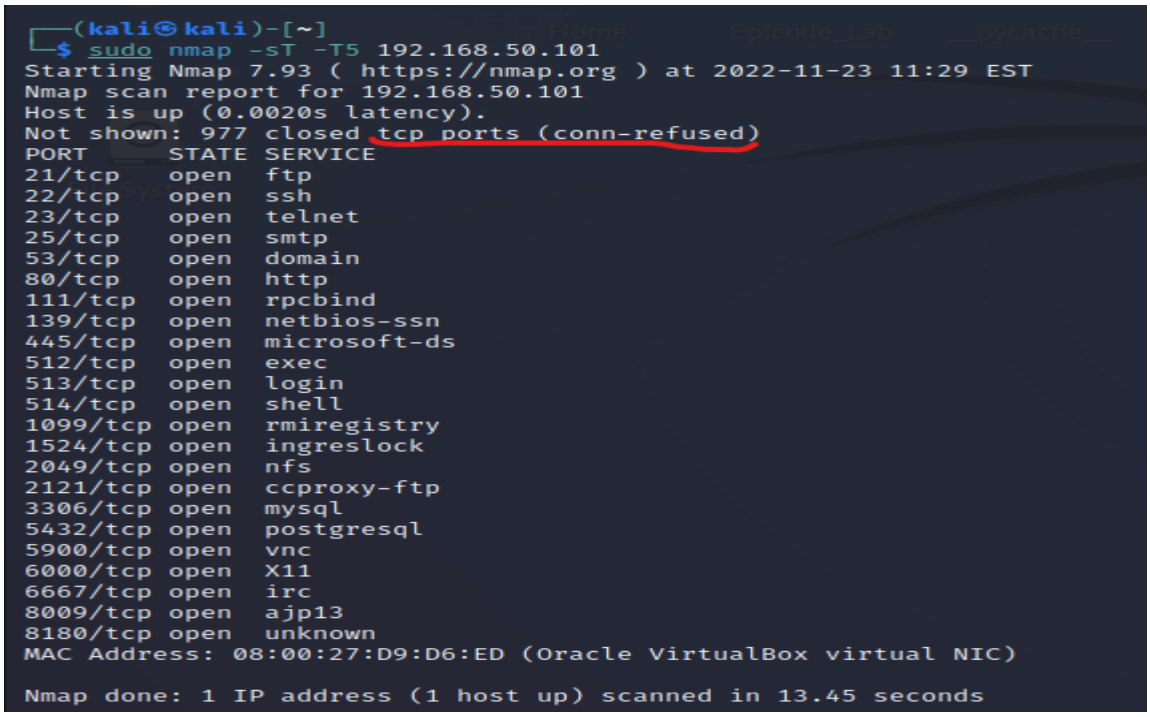
Andiamo ad effettuare una scansione Syn e quindi meno invasiva, infatti in questo caso la connessione controllerà solamente le porte aperte e poi la connessione verrà resettata come vediamo sottolineato in rosso.



Metasploitable ip 192.168.50.101 TCP scan:

Comando: nmap -sV -sT -T5 192.168.50.101

In questo caso abbiamo una scansione più aggressiva, infatti oltre a controllare le porte aperte si crea una connessione, completando il SYN/ACK come vediamo sottolineato in rosso.



Metasploitable ip 192.168.50.101 Version detection:

Andiamo ad enumerare le versioni dei servizi in ascolto.

```
└─$ sudo nmap -sV -T5 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 11:34 EST
Nmap scan report for 192.168.50.101
Host is up (0.0022s 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:D9:D6:ED (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 66.36 seconds
```

Metasploitable ip 192.168.50.101 Tipologia Sistema operativo:

Attraverso l'utilizzo degli scripts di nmap andiamo ad ricevere informazioni più dettagliate sul tipo di sistema operativo utilizzato dal nostro target, sottolineato in rosso.

```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb-os-discovery -T5 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 11:41 EST
Nmap scan report for 192.168.50.101
Host is up (0.0065s 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: 2022-11-23T11:41:42-05:00

Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
```

Windows 7 ip 192.168.50.102 OS fingerprint (Firewall attivo)

Scansionando la macchina Windows 7 con firewall attivo non ci dà risultati.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O -T5 192.168.50.102
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 11:47 EST
Nmap scan report for 192.168.50.102
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:8F:46:75 (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 https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.90 seconds
```

Windows 7 ip 192.168.50.102 OS fingerprint (Firewall disattivato):

In questo caso riceviamo delle informazioni dalla macchina.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O -T5 192.168.50.102
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 11:51 EST
Nmap scan report for 192.168.50.102
Host is up (0.0023s 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: 08:00:27:8F:46:75 (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 15.81 seconds
```

Windows 7 ip 192.168.50.102 **Soluzione OS fingerprint (Firewall attivo):**

L'unica soluzione per bypassare il firewall è quella di cambiare le regole del firewall stesso, permettendoci l'accesso cosa che possiamo vedere infatti scansionando le porte 80 e 443 dove ci risulta filtred e quindi con accesso bloccato. Perché come abbiamo visto soltanto con il firewall disattivato riusciamo ad ottenere informazioni.