

REPORT S3/L1

Scansione dei servizi on Nmap

Traccia

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint.
- Syn Scan.
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection.

E la seguente sul target Windows:

- OS fingerprint.

Svolgimento

Controlliamo le impostazioni di rete delle macchine di Kali e Metasploitable in modo che entrambe si trovino sulla stessa rete. Assegniamo i seguenti indirizzi alle macchine:

- 192.168.20.4 per Kali Linux
- 192.168.20.5 per Metasploitable2

Eseguiamo i comandi visti a lezione per scansionare il S.O. Metasploitable2 da Kali Linux.

Per l'OS fingerprint lanciamo il comando: `sudo nmap -O 192.168.20.5`

```
(kali@kali)-[~]
└─$ sudo nmap -O 192.168.20.5
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 09:02 EST
Nmap scan report for 192.168.20.5
Host is up (0.076s 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), Linux 2.6.20 - 2.6.24 (Ubuntu 7.04 - 8.04)
Network Distance: 2 hops
```

Figura 1. OS Fingerprint di Metasploitable2

Possiamo vedere che alla terz'ultima riga del risultato possiamo leggere **OS CPE:**
linux_kernel:2.6 che è esattamente il kernel di Metasploitable2.

Per il syn scan lanciamo: `sudo nmap-sS 192.168.20.5`

```
(kali@kali)-[~]  
$ sudo nmap -sS 192.168.20.5  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 09:04 EST  
Nmap scan report for 192.168.20.5  
Host is up (0.13s 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 9.85 seconds
```

Figura 2. Syn Scan di Metasploitable2

Per il TCP connect lanciamo: `sudo nmap-sT 192.168.20.5`

```
(kali㉿kali)-[~]  
$ sudo nmap -sT 192.168.20.5  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 09:08 EST  
Nmap scan report for 192.168.20.5  
Host is up (0.057s 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 10.95 seconds
```

Figura 3. TCP connect su Metasploitable2

Dopo l'esecuzione di questo comando non notiamo differenze nel risultato con il precedente.

Per il version detection lanciamo: `sudo nmap-sV 192.168.20.5`

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.20.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 09:09 EST
Nmap scan report for 192.168.20.5
Host is up (0.19s 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  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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.86 seconds
```

Figura 4. Version detection su Metasploitable2

Per eseguire il version detection su windows lanciamo la VM di Windows 10 e anche su questo sistema impostiamo manualmente l'indirizzo IP in modo che Kali e Windows siano sulla stessa rete.

Assegniamo rispettivamente:

- 192.168.1.50 a Kali
- 192.168.1.30 a Windows

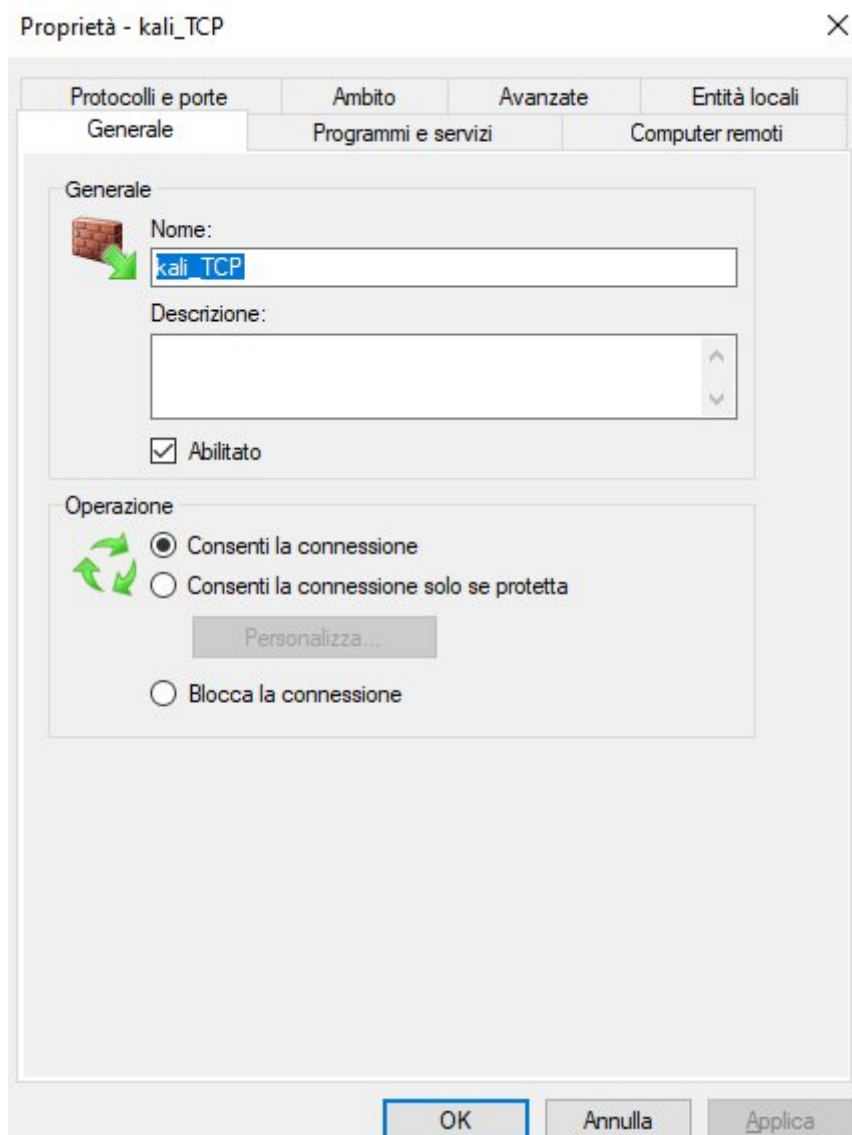
Proviamo il comando `sudo nmap-sV 192.168.1.30`, otteniamo come risposta l'errore riportato in figura:

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.1.30
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 10:12 EST
Nmap scan report for 192.168.1.30
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.1.30 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:A7:57:A9 (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: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft
Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2
012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device
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 35.14 seconds
```

Questo ci fa capire che, anche se i due sistemi sono nella stessa rete, Windows non è “raggiungibile”. Proviamo ad aggiungere delle regole firewall su Windows così da permettere la comunicazione con il protocollo TCP, che viene utilizzato da nmap.

Impostiamo la regola sia in entrata che in uscita, come in figura:



A questo punto ripetiamo il comando ed otteniamo:

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.1.30
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 10:16 EST
Nmap scan report for 192.168.1.30
Host is up (0.0045s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:A7:57:A9 (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
Running (JUST GUESSING): Microsoft Windows 2019|10 (90%)
OS CPE: cpe:/o:microsoft:windows_10
Aggressive OS guesses: Microsoft Windows Server 2019 (90%), Microsoft Windows 10 1909 (88%)
No exact OS matches for host (test conditions non-ideal).
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 21.71 seconds
```

Possiamo vedere che l'identificazione del S.O. è andata a buon fine al 90%.