Scansione dei servizi con Nmap

Richieste:

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**:

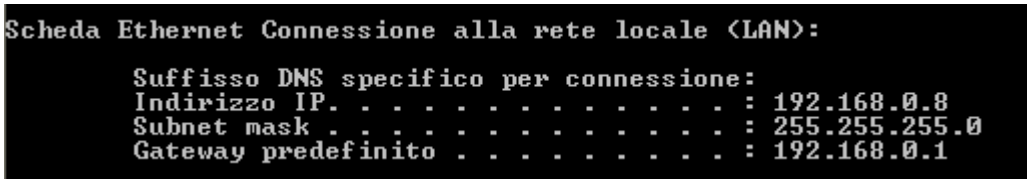
- OS fingerprint.

1.RILEVAMENTO INDIRIZZI IP MACCHINE

Prima di effettuare qualsiasi scansione,ho rilevato gli **indirizzi IP** delle due macchine:

- ***Metasploitable: 192.168.0.10/24***

- ***WindowsXp: 192.168.0.8/24***



Una volta acquisiti gli indirizzi e fatto l'accesso alla **kali,**ho aperto il terminale per effettuare le scansioni attraverso **Nmap**(strumento per scansionare la rete ed identificare dispositivi e servizi).

2.SCANSIONE METASPLOITABLE

2.1)OS FINGERPRINT

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.0.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:42 EST
Nmap scan report for 192.168.0.10 (192.168.0.10)
Host is up (0.0018s 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:AB:F7:BD (PCS Systemtechnik/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
```

Scrivendo ***nmap –O 192.168.0.10***,risulta che il sistema Operativo della ***Metasploitable*** è nel range tra ***Linux 2.6.9 e Linux 2.6.33***

2.2)SYN SCAN E TCP CONNECT

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.0.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:43 EST
Nmap scan report for 192.168.0.10 (192.168.0.10)
Host is up (0.00087s 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:AB:F7:BD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.0.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:43 EST
Nmap scan report for 192.168.0.10 (192.168.0.10)
Host is up (0.020s 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:AB:F7:BD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

Scrivendo ***nmap –sS 192.168.0.10***, mostra lo stato delle diverse porte e stessa cosa vale anche per il TCP CONNECT (***nmap –sT 192.168.0.10***) ma con una piccola differenza.

Principalmente le due si differenziano nella scansione delle porte ovvero:

- Nel SYN: nmap **non** completa il 3-way-handshake ma al momento del SYN/ACK da parte del target, lo chiude con un pacchetto **RST(reset)** in modo da diminuire la possibilità di essere rilevati da parte della macchina target.
- Nel TCP: nmap invece completa il 3-way-handshake ma questo aumenta la possibilità di essere rilevati

2.3)VERSION DETECTION

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.0.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:44 EST
Nmap scan report for 192.168.0.10 (192.168.0.10)
Host is up (0.011s 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?
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
MAC Address: 08:00:27:AB:F7:BD (PCS Systemtechnik/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 64.16 seconds
```

Scrivendo ***nmap –sV 192.168.0.10,*** è stata data una lista di tutte le versioni dei servizi in ascolto,questo sarà utile per la fase del **penetration testing.**

3)SCANSIONE WINDOWS

3.1)OS FINGERPRINT

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.0.8
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:47 EST
Nmap scan report for 192.168.0.8 (192.168.0.8)
Host is up (0.0042s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 2000 SP3/SP4 or Windows XP SP1/SP2 (97%), Microsoft Windows XP SP2 or SP3 (97%)
s XP SP1 (95%), Microsoft Windows 2000 SP4 or Windows XP SP1a (94%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows
icrosoft Windows 2000 Server SP3 or SP4 (92%)
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 8.76 seconds
```

Scrivendo ***nmap –O 192.168.0.8***, risulta che la versione della macchina target **Windows** è un ***Windows XP SP1/SP2***