[CONSEGNA SETTIMANA 5 LEZIONE 3]

Identificazione dei servizi e scansione della rete

La seconda fase di un pentesting è definita come *scansione della rete*, durante la quale ci si avvale del software **nmap,** il quale permette di eseguire diversi tipologie di scansione sulla rete.

Come target oggi useremo la macchina metasploitable e il sistema operativo Windows 10.

IP Metasploitable: 192.168.5.220

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -O 192.168.5.220
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 07:28 EST
Nmap scan report for 192.168.5.220
Host is up (0.00028s 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:BB:C6:4D (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.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.79 seconds
```

Tipologia di scansione : -O

Risultato ottenuto : sistema operativo linux 2.6.x

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV 192.168.5.220
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 07:35 EST
Nmap scan report for 192.168.5.220
Host is up (0.00011s 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:BB:C6:4D (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 65.46 seconds
```

Tipologia di scansione : -sV

Risultato ottenuto : Versione dei servizi in ascolto

Possiamo notare come in entrambe le scansioni siano state elencate tutte le porte aperte e i relativi servizi associati. La differenza sostanziale tra le due scansione risiede nei risultati ottenuti. La prima scansione mirava all ottenere il sistema operativo della macchina, mentre

la seconda cercava nello specifico la versione dei servizi in ascolto. Possiamo notare inoltre che tra le porte aperte, molte sono a rischio di un potenziale attacco (ad esempio la porta 21 ftp o la porta 23 telnet).

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sS 192.168.5.220
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 07:31 EST
Nmap scan report for 192.168.5.220
Host is up (0.000093s 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:BB:C6:4D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sT 192.168.5.220
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 07:33 EST
Nmap scan report for 192.168.5.220
Host is up (0.00018s 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:BB:C6:4D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds
```

Tra le varie tipologie di scansione possiamo trovare -sS, che esegue l'invio solo del pacchetto SYN, per poi terminare con un RESET, questa scansione risulta molto meno invasiva e quindi più difficile da notare.

Un altra scansione, ma che al contrario può risultare più invasiva è -sT che esegue il completo 3-way handshake (SYN - SYN/ACK – ACK), risultando più facile da notare.

Nel caso della scansione sulla macchina metasploitable si può notare che non vi è una differenza tra le due scansioni, se non per la latenza.

IP Windows 11: 192.168.5.243

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.5.243
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 10:30 EST
Nmap scan report for 192.168.5.243
Host is up (0.00026s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: E0:C2:64:2F:48:B5 (Intel Corporate)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1703
OS details: Microsoft Windows 10 1703
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 3.20 seconds
```

Tipologia di scansione : -O

Risultato ottenuto : sistema operativo windows 10

Nel caso della scansione sulla macchina Windows 10, dopo aver temporaneamente disabilitato il firewall, possiamo notare che le porte aperte sono decisamente inferiori. Nel caso non avessi disabilitato il firewall, nmap avrebbe riportato che le porte non hanno dato alcuna risposta (*no-response*)