

ESERCIZIO S5/L3

L'esercizio di oggi richiede di eseguire delle scansioni tramite il tool di kali linux nmap su due target diversi, ovvero Metasploitable e Windows 7.

Metasploitable

Os fingerprint:

```
(root@kali) - [/home/kali]
# nmap -O 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 14:26 EST
Nmap scan report for 192.168.50.101
Host is up (0.00032s 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: 08:00:27:56:BC:C9 (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 14.98 seconds
```

questo comando viene utilizzato per ottenere informazioni sul sistema operativo, sullo stato delle porte e dei servizi che ci sono.

Syn scan:

```
(root@kali)-[/home/kali]
# nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 14:29 EST
Nmap scan report for 192.168.50.101
Host is up (0.00037s 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: 08:00:27:56:BC:C9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

L'obiettivo principale di uno scan SYN è quello di ottenere informazioni sulle porte aperte senza stabilire completamente una connessione TCP (quindi non completa il three way handshake), infatti possiamo notare come nella quarta riga alla fine comparirà “(reset)” proprio perché nmap non darà la risposta ack di ritorno.

TCP connect:

```
(root@kali)-[/home/kali]
# nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 14:31 EST
Nmap scan report for 192.168.50.101
Host is up (0.0020s 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: 08:00:27:56:BC:C9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

L'obiettivo principale di uno scan TCP Connect di Nmap è effettivamente quello di stabilire completamente una connessione TCP per determinare lo stato delle porte aperte su un host di destinazione. Questa scansione coinvolge l'inizio del normale handshake TCP, stabilendo una connessione completa con il server. A differenza dello scan SYN, che non completa mai la connessione TCP, lo scan TCP Connect effettua un handshake completo. Questo rende lo scan TCP Connect più intrusivo e più facilmente rilevabile dai sistemi di sicurezza, ma allo stesso tempo fornisce informazioni più affidabili sullo stato delle porte.

Version detection:

```
(root@kali) - [/home/kali]
# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 14:33 EST
Nmap scan report for 192.168.50.101
Host is up (0.00027s 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: 08:00:27:56:BC:C9 (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 66.47 seconds
```

Questo comando viene utilizzato per eseguire una scansione dei servizi in esecuzione su un host, cercando di determinare le versioni specifiche dei servizi e delle applicazioni in ascolto sulle porte aperte. Questo comando aggiunge alla scansione delle informazioni sulla versione dei servizi, consentendo di ottenere dettagli più approfonditi sulle applicazioni in esecuzione su un sistema target.

Windows 7

OS fingerprint:

nmap -O 192.168.50.102

Starting Nmap 7.94SVN (<https://nmap.org>) at 2023-12-20 17:52 EST

Nmap scan report for 192.168.50.102

Host is up (0.00050s latency).

All 1000 scanned ports on 192.168.50.102 are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 08:00:27:07:7D:AB (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 2012, 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 37.37 seconds

Due caratteristiche fondamentali dell'OS fingerprint trovate su Win7 sono sicuramente le 1000 porte trovate ma che non danno risposta e le molteplici versioni del sistema operativo

Il motivo principale del perché le informazioni non sono precise sarà sicuramente all'interno del firewall di Win7 che blocca le connessioni TCP che Kali vuole trasmettere.

Le soluzioni per risolvere questo problema per me sono due:

La soluzione più semplice, ma anche quella che fa sembrare che stiamo barando è cambiare le regole del firewall di Win7 in modo da permettere le connessioni in entrata sotto quel punto di vista;

La seconda soluzione invece è quella di aggiungere un Timing template più alto al comando -O di nmap in modo tale che il firewall non riesca ad individuare per bene quel tipo di connessioni, quindi non bloccandole. La procedura però richiede molto tempo, quindi bisognerà aspettare molti minuti, ore oppure giorni prima di ricevere la risposta al comando -O

Conosciamo vari Timing template di Nmap che variano da -T0 fino a -T5:

-T0= Paranoid scan//Scan molto molto lento

-T1= Sneaky scan// è perfetta per ingannare i firewall

-T2= Polite scan// Non interferisce con il sistema operativo, ma darà meno informazioni

-T3= Normal scan// Lo scan di default di nmap

-T4= Aggressive scan// Da risultati migliori per le reti LAN

-T5= Insane scan// Lo scan più veloce ed aggressivo di tutti

In questo caso per ottenere le informazioni dette prima da parte di Win7 lo scan perfetto è il -T1, in quanto riesce a recuperare tutte le informazioni che ci servono, non facendosi scoprire dal firewall, in un tempo medio/lungo.

Il comando da utilizzare sarà il seguente:

nmap -T1 -O 192.168.50.102