U1W2L – Report

map e scansione dei servizi

Richieste:

- Sul target Metasploitable:
  - OS fingerprint.
  - Syn Scan.
  - TCP connect
  - Version detection.
  - Identificazione differenze TCE e Syn Scan
- Sul target Windows:
  - OS fingerprint.

Svolgimento:

Anzitutto ho provveduto a collegare tutte le VM in scheda bridge, avviandole per poter far partire i test.

Tramite il comando ifconfig, eseguito sulla Metasploitable, ne ho individuato l'IP, ovvero 192.168.1.11.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:77:c7:3b
          inet addr:192.168.1.11  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe77:c73b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8019 (7.8 KB)  TX bytes:7119 (6.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)
```

Conoscendo l'IP della macchina, ho proceduto con i test dalla macchina sorgente, Kali Linux, IP 192.168.1.9, andando a eseguire anzitutto una OS fingerprint sulla Metasploitable.

L'OS fingerprint è una tecnica fondamentale nella Cybersecurity, attraverso la quale si può identificare il sistema operativo e la versione dello stesso di una macchina bersaglio. Questa identificazione avviene tramite l'analisi delle risposte ai pacchetti di rete, sia all'invio diretto, che con l'analisi del traffico.

Il risultato da me ottenuto è stato il seguente:

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.1.11
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:00 EST
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.11)
Host is up (0.0030s 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: 08:00:27:77:C7:3B (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.47 seconds
```

Il sistema operativo della macchina Metasploitable è stato correttamente identificato come Linux. Oltre a ciò, questa scansione ha identificato anche le porte aperte sulla macchina che, essendo di test e volutamente vulnerabile, ne presenta diverse, identificando anche parte dei servizi.

Come da richiesta, ho poi provveduto a effettuare una Syn Scan, lanciando il comando nmap -sS. Questo comando effettua un 3-way-handshake, ponendovi però fine prima dell'invio del proprio ACK. Così facendo, l'handshake TCP non si conclude e l'evento viene loggato dalla macchina target come errore.

È un metodo che verifica se una porta è aperta o meno, considerato meno congestionante a livello di rete.

I risultati ottenuti sono stati i seguenti:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.11
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:19 EST
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.11)
Host is up (0.010s 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: 08:00:27:77:C7:3B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
```

A seguito di questa scansione, ho effettuato la sua gemella, la nmap -sT, una TCP scan che, diversamente dalla Syn Scan, completa il 3-way-handshake.
Questa scansione produce più rumore a livello di rete e, essendo che la connessione viene stabilita, viene loggata dalla macchina bersaglio ed è più facilmente rilevabile.

A livello di risultati, però, le due scansioni non presentano differenze: entrambe loggano le porte aperte e i servizi dietro ad esse.

A seguire i risultati della TCP scan:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.1.11
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:20 EST
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.11)
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: 08:00:27:77:C7:3B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

A seguito di queste scansioni, ho proceduto a effettuare un'operazione di banner grabbing. Lanciando il comando nmap -sV, infatti, nmap raccoglie informazioni in merito a un servizio eseguito su una determinata porta e rileva la versione di questo. Ciò avviene tramite la lettura di messaggi di benvenuto o automatici inviati dal servizio quando viene stabilita una connessione.

Vengono inviati pacchetti probe (di sonda) per poter analizzare le risposte, confrontandole poi con un database di firme note per identificare così servizio e versione.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.11
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 13:59 EST
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.11)
Host is up (0.0019s 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?
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:77:C7:3B (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 106.71 seconds
```

Per quello che riguarda Windows, la macchina analizzata è stata una VM con installato Windows 10.

Ho anzitutto eseguito il comando ipconfig per individuarne l'IP.

```
C:\Users\user>ipconfig

Configurazione IP di Windows


Scheda Ethernet Ethernet:

   Suffisso DNS specifico per connessione: homenet.telecomitalia.it
   Indirizzo IPv4. . . . . . . . . . . . . : 192.168.1.13
   Subnet mask . . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . . : 192.168.1.1

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 . . . . . . . . . . . . . . . . . . . . : 2001:0:2851:782c:2c12:2721:a8f4:2e2a
   Indirizzo IPv6 locale rispetto al collegamento . . . . : fe80::2c12:2721:a8f4:2e2a%5
   Gateway predefinito . . . . . . . . . . . . . . . . . : ::

Scheda Tunnel isatap.homenet.telecomitalia.it:

   Stato supporto. . . . . . . . . . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione: homenet.telecomitalia.it

C:\Users\user>
```

Dalla Kali ho poi provveduto a eseguire una OS fingerprinting del sistema, ottenendo questa risposta:

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.1.13
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 14:13 EST
Nmap scan report for DESKTOP-9K1O4BT.homenet.telecomitalia.it (192.168.1.13)
Host is up (0.0024s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
5432/tcp open  postgresql
8009/tcp open  ajp13
8080/tcp open  http-proxy
8443/tcp open  https-alt
MAC Address: 08:00:27:2F:59:68 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 1.46 seconds
```

Il sistema è stato correttamente individuato come Windows 10, sono state inoltre individuate le porte aperte.