PROGETTO W3L3

Nmap

Uno sguardo alle scansioni con Nmap verso una macchina metaspoit e windows 7

Siamo andati ad effettuare diversi tipi di scansioni sulle nostre due macchine virtuali, e nelle prossime slide andremo a snocciolare i temi toccati.
Importante precisazione, ci sono state diverse difficoltà dovute al firewall di windows7, il quale bloccando il protocollo ICMP non permetteva l'utilizzo del ping verso la nostra macchina virtuale.
Nelle prossime slide vedremo i seguenti tipi di scansioni:

- OS fingerprint
- Syn Scan
- TCP connect
- Version detection.

OS FINGERSPRINTIG:

Per identificare un sistema operativo, bisogna inviare delle richieste di rete all'host in oggetto e successivamente studiare le risposte ricevute. È possibile risalire ai sistemi operativi dalle risposte che inviano a determinate richieste, grazie a delle piccole differenze che i diversi sistemi operativi (Windows, Linux, macOS) presentano nell'implementazione dello stack di rete.
Questa tecnica prende appunto il nome di fingersprinting ed è sempre comunque una stima che si ottiene facendo un riscontro è quindi normale avere una determinata percentuale di probabilità.

OS FINGERSPRINTING META

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -O 192.168.1.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-25 09:24 EDT
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.9)
Host is up (0.0078s 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:F5:52:7D (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.9 - 2.6.24 (97%), Linux 2.6.9 - 2.6.30 (97%), Linux 2.6.9 - 2.6.33 (97%), Linux 2.6.13 - 2.6.32 (97%), Linux 2.6.9 (97%), Linux 2.6.24 - 2.6.28 (96%), Linux 2.6.18 - 2.6.32 (96%), Linux 2.6.22 - 2.6.23
(96%), Linux 2.6.18 (Debian 4, VMware) (96%), Linux 2.6.23 (95%)
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 5.13 seconds
```

Qui con il comando nmap -O iP_target siamo andati a definire il probabile sistema operativo della nostra macchina meta, come possiamo vedere c'è il 97% di possibilità che si tratti di un sistema Linux con versione 2.6.9.
nmap ha provveduto ad ordinare i risultati in base alla probabilità

PRIMO TENTATIVO FINGERPRINTING W7

Qui siamo andati ad effettuare un primo tentativo di fingerprinting su windows 7 e il risultato ottenuto è il seguente:

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -O 192.168.1.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-25 09:26 EDT
Nmap scan report for win7.homenet.telecomitalia.it (192.168.1.10)
Host is up (0.00090s latency).
All 1000 scanned ports on win7.homenet.telecomitalia.it (192.168.1.10) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:05:6C:73 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
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 35.00 seconds
```

SECONDO TENTATIVO FINGERPRINTING W7

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -Pn -O 192.168.1.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-25 09:29 EDT
Nmap scan report for win7.homenet.telecomitalia.it (192.168.1.10)
Host is up (0.0016s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
MAC Address: 08:00:27:05:6C:73 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
```

In questo secondo tentativo siamo riusciti a stabilire il possibile Sistema operativo, tramite il comando “nmap -Pn -O iP_Target”.

Ciò avviene perchè spesso una macchina potrebbe essere attiva ma non rispondere al ping, ad esempio se c’è una regola firewall che blocca il traffico ICMP. Con il nostro comando siamo quindi andati ad agirare questa regola.

SYN SCAN W7

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sS 192.168.1.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-25 09:33 EDT
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 62.55% done; ETC: 09:35 (0:00:29 remaining)
Stats: 0:03:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 73.35% done; ETC: 09:37 (0:01:01 remaining)
Stats: 0:03:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 73.45% done; ETC: 09:37 (0:01:01 remaining)
Stats: 0:03:34 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 76.35% done; ETC: 09:38 (0:01:03 remaining)
Stats: 0:04:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 83.65% done; ETC: 09:39 (0:00:55 remaining)
Stats: 0:06:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 94.65% done; ETC: 09:40 (0:00:23 remaining)
Stats: 0:07:46 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.65% done; ETC: 09:41 (0:00:02 remaining)
Stats: 0:11:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 09:45 (0:00:00 remaining)
Nmap scan report for 192.168.1.10
Host is up (0.0019s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
MAC Address: 08:00:27:05:6C:73 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1010.59 seconds
```

è un metodo meno invasivo rispetto ad altri scan in quanto nmap, una volta ricevuto il pacchetto SYN/ACK dalla macchina target, non conclude il 3-way-handshake, ma appurato che la porta è aperta chiude la comunicazione, di fatto evitando overload dato dalla creazione del canale.

SYN SCAN META

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sS 192.168.1.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-25 09:33 EDT
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.9)
Host is up (0.015s 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:F5:52:7D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
```

TCP CONNECT W7

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sT 192.168.1.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-25 09:55 EDT
Nmap scan report for 192.168.1.10
Host is up (0.0026s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
MAC Address: 08:00:27:05:6C:73 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.62 seconds
```

è il metodo di scansione più invasivo, in quanto per controllare se una porta è aperta o meno e recuperare informazioni sul servizio in ascolto, nmap completa tutti i passaggi del 3-way-handshake, stabilendo di fatto un canale.

TCP CONNECT META

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sT 192.168.1.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-25 09:54 EDT
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.9)
Host is up (0.016s 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:F5:52:7D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

VERSION SCAN W7

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV 192.168.1.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-25 10:08 EDT
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 10:09 (0:01:12 remaining)
Nmap scan report for win7.homenet.telecomitalia.it (192.168.1.10)
Host is up (0.00089s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:05:6C:73 (Oracle VirtualBox virtual NIC)
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.14 seconds
```

è a tutti gli effetti una scansione TCP connect con l'aggiunta di specifici test per la rilevazione dei servizi in ascolto su una porto. Così come la scansione TCP connect è piuttosto facile da rilevare in quanto genera molto traffico di rete.

VERSION SCAN META

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sV 192.168.1.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-25 10:06 EDT
Stats: 0:01:05 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 10:07 (0:00:03 remaining)
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.9)
Host is up (0.0024s 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:F5:52:7D (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 89.22 seconds
```