

NMAP

Traccia: Tecniche di scansione con Nmap 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 7: OS fingerprint

A valle delle scansioni è prevista la produzione di un report contenente le seguenti info (dove disponibili):

IP.

Sistema Operativo.

Porte Aperte.

Servizi in ascolto con versione.

Quesito extra (al completamento dei quesiti sopra): Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

Iniziamo con Kali e Meta.

Per prima cosa usiamo NMAP per effettuare l'OS Fingerprinting sulla macchina meta con IP 192.168.50.105

```
metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
-bash: s: command not found
msfadmin@metasploitable:~$ if config
>
>
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:76:0c:d9
          inet addr:192.168.50.105  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe76:cd9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5615 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5643 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:406285 (396.7 KB)  TX bytes:363514 (354.9 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:391 errors:0 dropped:0 overruns:0 frame:0
          TX packets:391 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:85534 (83.5 KB)  TX bytes:85534 (83.5 KB)

msfadmin@metasploitable:~$
```

```

(kali@kali)-[~]
$ sudo nmap -O 192.168.50.105
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 09:07 EDT
Nmap scan report for 192.168.50.105
Host is up (0.00095s 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: 08:00:27:76:0C:D9 (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 14.63 seconds

```

Test eseguito con successo, ci riporta il sistema operativo di Metasploitable.

Poi eseguiamo una scansione Syn, per vedere se la macchina risponde.

```

(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 09:12 EDT
Nmap scan report for 192.168.50.105
Host is up (0.00084s 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: 08:00:27:76:0C:D9 (Oracle VirtualBox virtual NIC)

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

```

La macchina ha risposto e si è sincronizzata con il pacchetto SYN. Ora vediamo se ci sono differenze con un ciclo TCP completo.

```
(kali㉿kali)-[~]
$ sudo nmap -sT 192.168.50.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 09:15 EDT
Nmap scan report for 192.168.50.105
Host is up (0.0031s 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: 08:00:27:76:0C:D9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.63 seconds
```

Come ci si aspettava, non ci sono differenze sostanziali se non qualche millesimo di secondo in più, dato che il ciclo completo effettua anche invio di SYN/ACK e di ACK.

Ora vediamo le versioni del software e dei servizi sulla macchina di meta.

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.50.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 09:17 EDT
Nmap scan report for 192.168.50.105
Host is up (0.0012s 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?
25/tcp    open  smtp?
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?
514/tcp   open  shell?
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  ccproxy-ftp?
3306/tcp  open  mysql?
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: 08:00:27:76:0C:D9 (Oracle VirtualBox virtual NIC)
Service Info: Host: 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 193.33 seconds
```

Adesso passiamo all' OS Fingerprinting della macchina Windows con IP 192.168.50.102

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.

C:\Users\ vboxuser>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::8471:cafe:bb70:52a7%11
    Indirizzo IPv4. . . . . : 192.168.50.102
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.50.1

Scheda Tunnel isatap.{7FFEC7C0-D516-4AA8-A796-B75FAF6EE458}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

C:\Users\ vboxuser>$
```

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 09:27 EDT
Nmap scan report for win.epi (192.168.50.102)
Host is up (0.00089s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:50:F9:A1 (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|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
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 6.26 seconds
```

Come possiamo vedere, l'OS fingerprinting è avvenuto con successo ma nmap segnala che 997 porte siano filtrate, molto probabilmente vengono filtrate dal firewall di windows che è configurato di default.

Proviamo ad utilizzare uno dei metodi visti a lezione per aggirare il firewall di windows.

Utilizziamo la Sneaky scan del Timing di NMAP per cercare di aggirare il firewall.

```
sudo nmap -T1 192.168.50.102
```

Così facendo effettueremo una scansione lenta che però è anche meno invasiva e ha la possibilità di aggirare i sistemi di protezione come IDS, IPS e Firewall a difesa della macchina target. Ovviamente questo tipo di scansione non è una panacea che aggirerà tutti gli ostacoli: molto dipende dalla configurazione di difesa della macchina, se i dispositivi a protezione della rete sono sensibili, quasi sicuramente questo metodo non funzionerà.