21 FEBBRAIO 2024

REPORT - EPICODE

S5L3

PRESENTED BY

Alessandro Marasca

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 SYN?
- Version detection.

E la seguente sul target Windows 7:

- OS fingerprint.

02 - TECNICHE DI SCANSIONE CON NMAP

OS FINGERPRINT

SYN SCAN

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 15:08 EST
Nmap scan report for 192.168.49.101
Host is up (0.28s 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

Nmap done: 1 IP address (1 host up) scanned in 2.06 seconds
```

TCP

Nmap - ST completa il 3-way-handshake, creando così il canale. Recupera info sullo stato della porta, è dunque una tecnica di scanning più identificabile e che su grosse reti potrebbe creare congestioni di rete.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 15:07 EST
Nmap scan report for 192.168.49.101
Host is up (0.032s 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

Nmap done: 1 IP address (1 host up) scanned in 1.95 seconds
```

WINDOWS - OS DETECTION

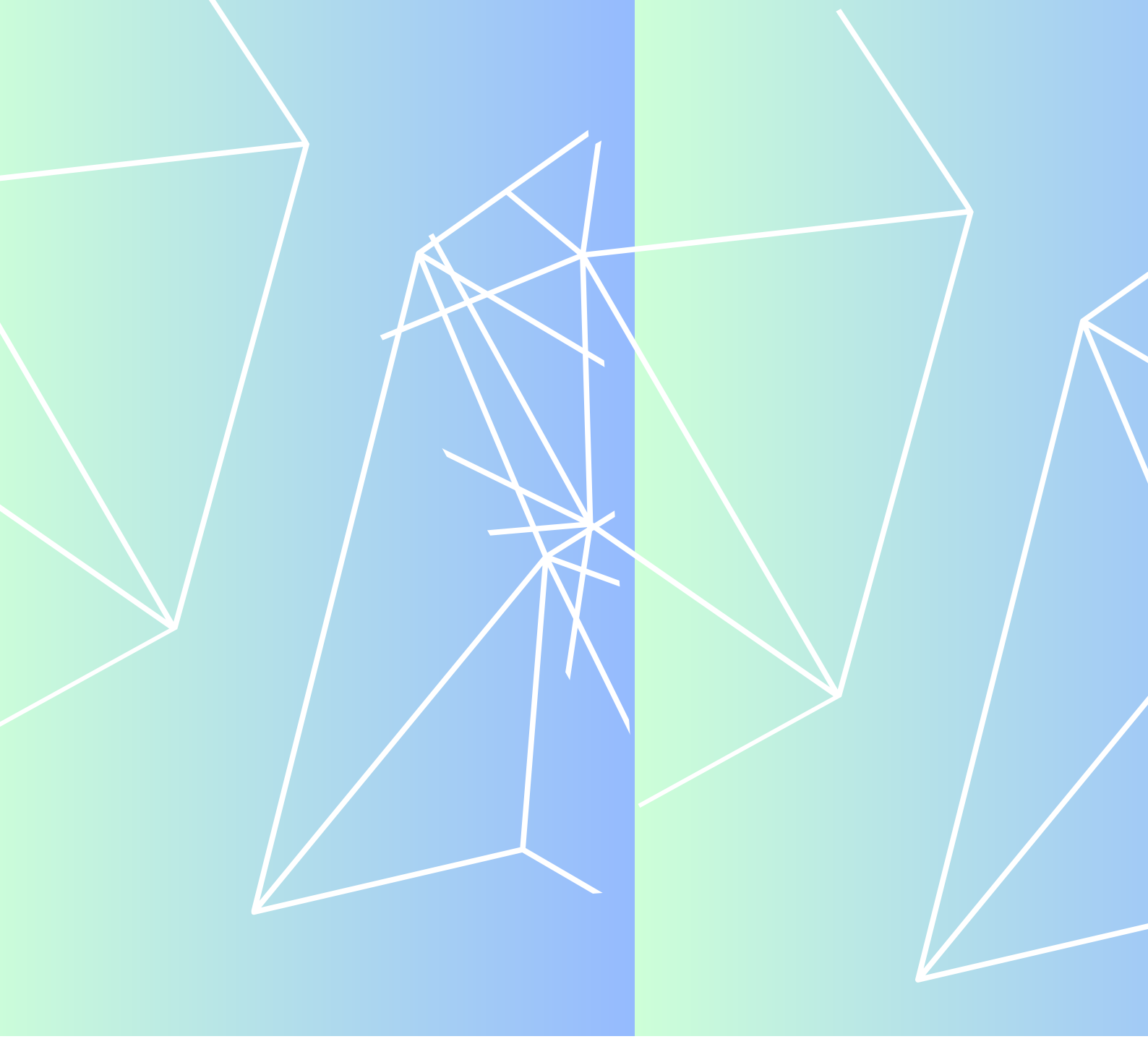
Procediamo con l'identificazione OS di Windows, agisce allo stesso modo di Meta, andando a rintracciare lo stato delle porte dall'IP di Windows e notiamo una differenza: la presenza dei ***demoni:*** un programma eseguito in background, cioè senza che sia sotto il controllo diretto dell'utente, tipicamente fornendo un servizio all'utente. Principalmente viene utilizzato sui server ma anche su normali PC.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 15:53 EST
Nmap scan report for 192.168.50.102
Host is up (0.0015s 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
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:0A:A3:AD (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:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 15:55 EST
Nmap scan report for 192.168.50.102
Host is up (0.00075s 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)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
MAC Address: 08:00:27:0A:A3:AD (Oracle VirtualBox virtual NIC)
Service Info: Host: ALE-PC; 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 60.81 seconds
```



Alessandro Marasca

Epicode

S5L3 - CS0124