

Esercitazione 29/04/25

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 delle scansioni TCP connect e SYN?
- Version detection.

E la seguente sul target Windows:

- 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.

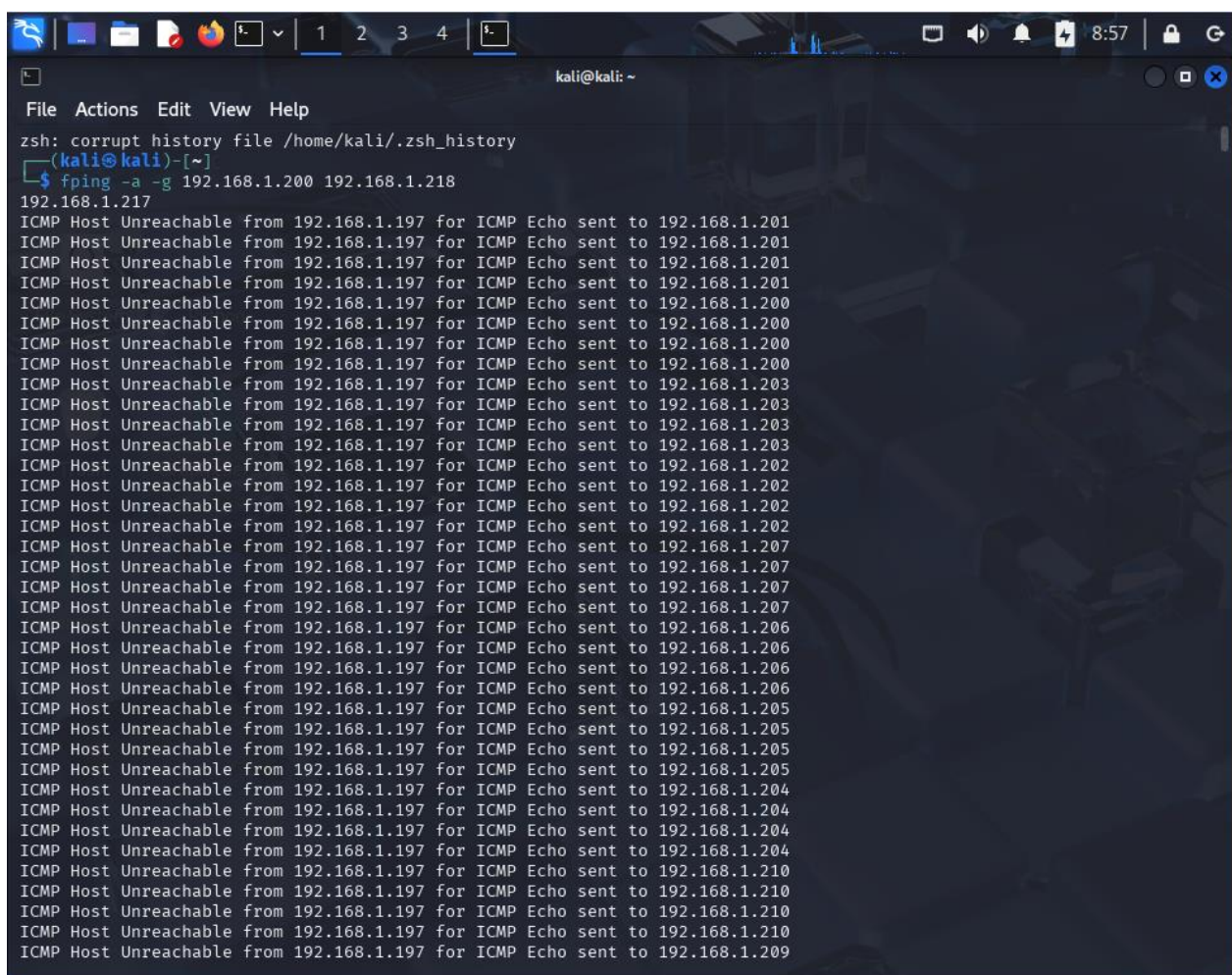
Inizio del report.

Target Metasploitable 2

Per individuare l'indirizzo IP di Metasploitable 2 sul terminale di Kali lancio il comando

fping -a -g 192.168.1.200 192.168.1.218 (indicando il range degli indirizzi IP)

risponde **192.168.1.217**



```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ fping -a -g 192.168.1.200 192.168.1.218  
192.168.1.217  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.201  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.201  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.201  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.201  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.200  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.200  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.200  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.200  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.203  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.203  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.203  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.203  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.202  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.202  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.202  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.202  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.207  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.207  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.207  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.207  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.206  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.206  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.206  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.206  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.205  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.205  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.205  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.205  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.204  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.204  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.204  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.204  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.210  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.210  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.210  
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.210
```

Proseguo ora con l'OS fingerprint.

Lancio da terminale il comando **nmap -O 192.168.1.217**

Il risultato che ottengo mi indica non solo il sistema operativo (Linux) ma anche le porte note che sono aperte.

```
kali@kali: ~  
File Actions Edit View Help  
$ nmap -O 192.168.1.217  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 09:03 EDT  
Nmap scan report for 192.168.1.217  
Host is up (0.00052s 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:AB:F8:47 (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 1.79 seconds
```

Proseguo ora con il Syn Scan.

Lancio da terminale il comando **nmap -sS 192.168.1.217** che non stabilisce una connessione TCP completa ed ottengo questo risultato.

```
(kali@kali)-[~]  
$ nmap -sS 192.168.1.217  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 09:14 EDT  
Nmap scan report for 192.168.1.217  
Host is up (0.00015s 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:AB:F8:47 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

Proseguo poi con il TCP Connect scan.

Lancio il comando **nmap -sT 192.168.1.217** che utilizza la chiamata di sistema per stabilire una connessione TCP completa a ciascuna porta di destinazione.

```
(kali@kali)-[~]
$ nmap -sT 192.168.1.217
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 09:23 EDT
Nmap scan report for 192.168.1.217
Host is up (0.00065s 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:AB:F8:47 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Il risultato può sembrare lo stesso ma quello che cambia tra una scansione ed un'altra è che la scansione -sS è più furtiva e veloce in quanto non stabilisce e chiude connessioni complete e richiede privilegi elevati.

Proseguo ora con la rivelazione dei servizi in esecuzione sulle porte aperte.

Lancio da terminale il comando **nmap -sV 192.168.1.217** per identificare accuratamente i servizi e le versioni.

```

(kali@kali)-[~]
$ nmap -sV 192.168.1.217
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 09:34 EDT
Stats: 0:00:32 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 09:35 (0:00:01 remaining)
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 09:35 (0:00:03 remaining)
Nmap scan report for 192.168.1.217
Host is up (0.00014s 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:AB:F8:47 (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 65.10 seconds

```

Attenzione: le scansioni -sV possono essere rilevate dai sistemi di sicurezza e dai firewall.

Target Windows.

Per individuare l'indirizzo IP di Windows 10 lancio da terminale il comando:

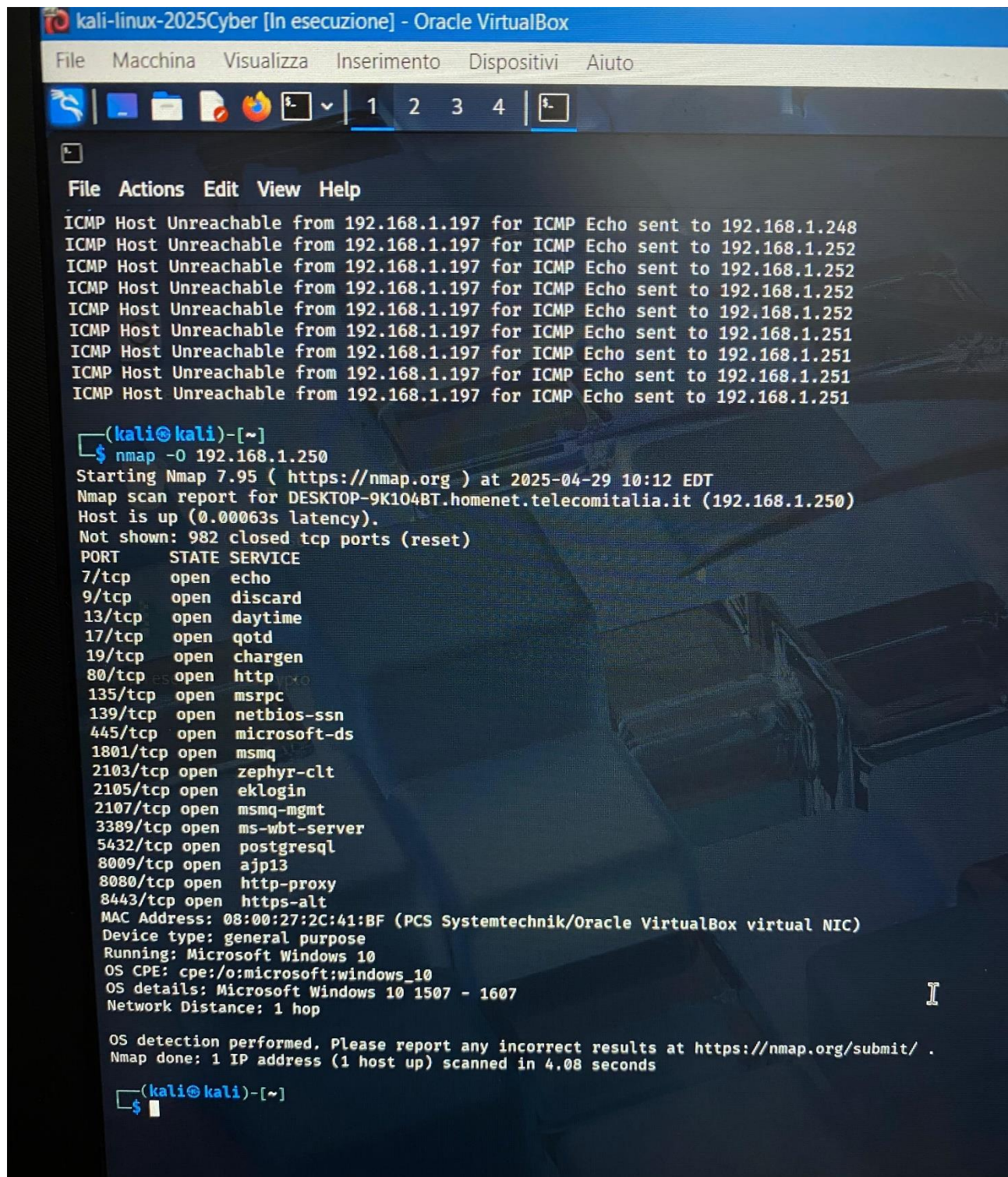
```
fping -a -g 192.168.1.200 192.168.1.252
```

rispondono: 192.168.1.217 (Metasploitable) e 192.168.1.250 (Windows 10)

[illegible]

Proseguo ora con l'OS fingerprint.

Lancio da terminale il comando **nmap -O 192.168.1.250** e ottengo questo risultato.



```
kali-linux-2025Cyber [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

File  Actions  Edit  View  Help
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.248
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.252
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.252
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.252
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.252
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.251
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.251
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.251
ICMP Host Unreachable from 192.168.1.197 for ICMP Echo sent to 192.168.1.251
(kali@kali)-[~]
$ nmap -O 192.168.1.250
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:12 EDT
Nmap scan report for DESKTOP-9K104BT.homenet.telecomitalia.it (192.168.1.250)
Host is up (0.00063s latency).
Not shown: 982 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
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:2C:41:BF (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 4.08 seconds
(kali@kali)-[~]
$
```