Obiettivo

L'obiettivo dell'esercizio è esplorare e comprendere le principali tecniche di scansione offerte da Nmap.

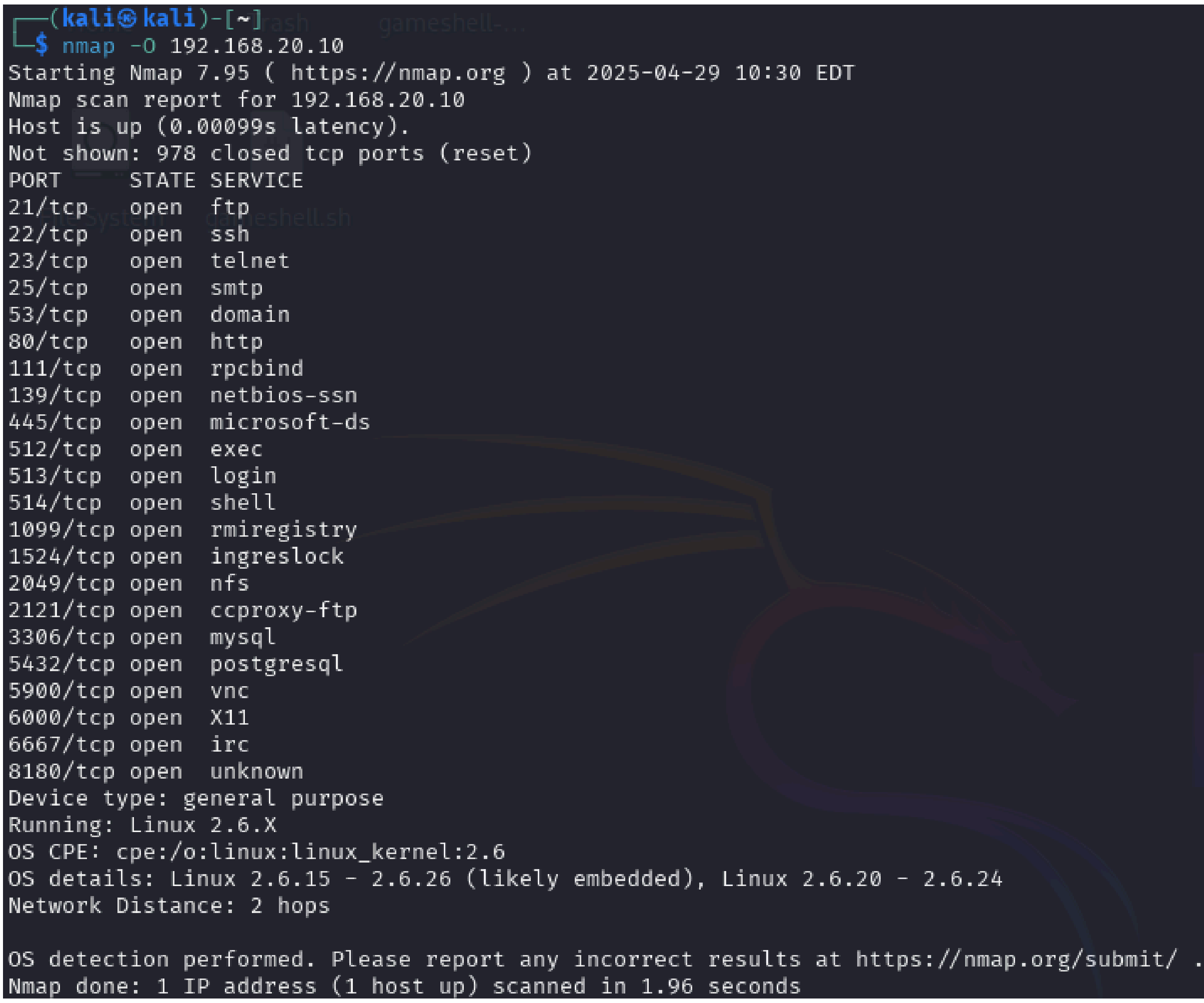
Attraverso diverse modalità (SYN, TCP Connect, Version Detection e OS Fingerprint), vengono analizzati due target: una macchina vulnerabile (Metasploitable) e un sistema Windows.

Lo scopo è identificare informazioni critiche come IP, sistema operativo, porte aperte e servizi in ascolto, valutando anche le differenze tra le varie tecniche di scansione.

Target 1: Metasploitable

Ip: 192.168.20.10

1. **OS Fingerprint**
   a. **Comando usato:** nmap -O 192.168.20.10
   b. **Risultati:**



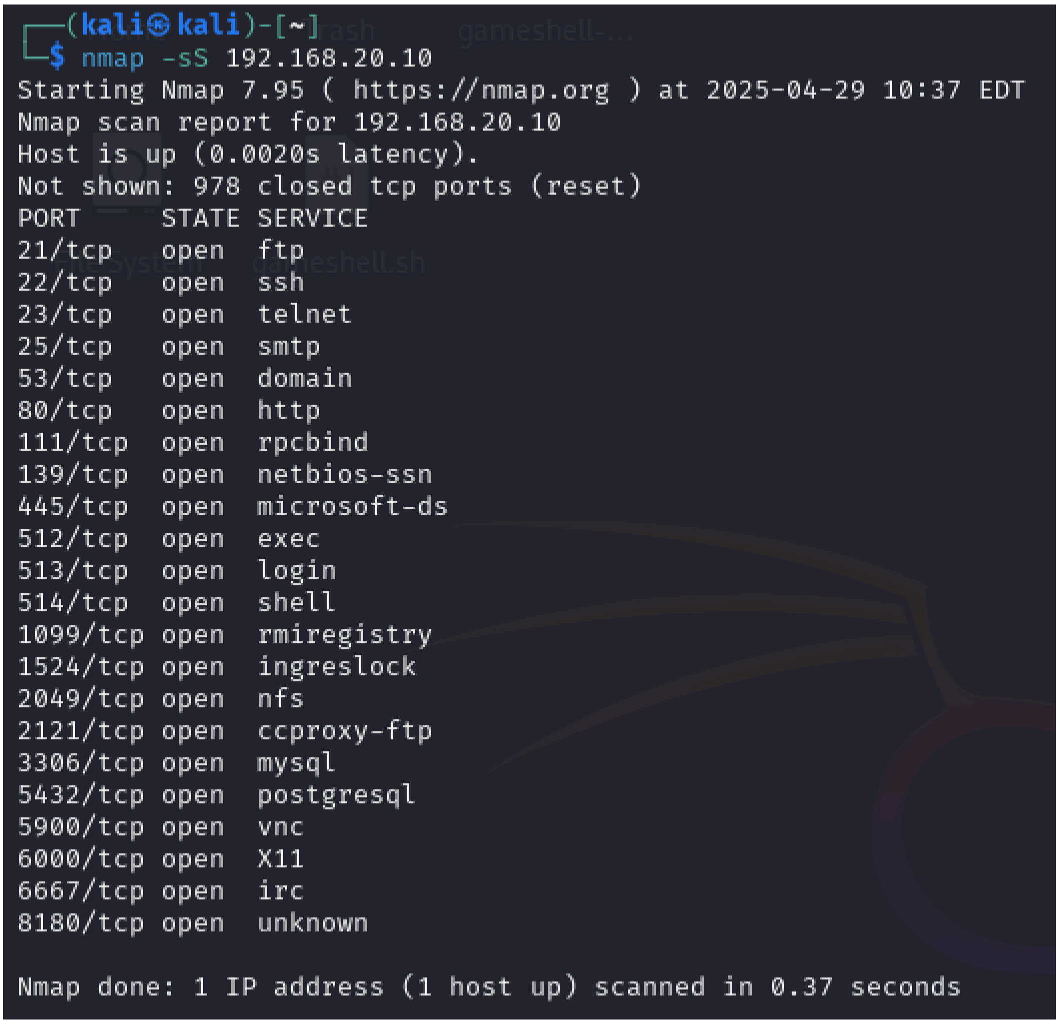
```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.20.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:30 EDT
Nmap scan report for 192.168.20.10
Host is up (0.00099s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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
8180/tcp open  unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.20 - 2.6.24
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.96 seconds
```

Il comando nmap ha rivelato il sistema operativo Linux versione 2.6.X con X variabile tra .15 e .26.

Nell'output abbiamo anche una lista di porte aperte di metasploitable, tra cui alcune critiche.

    c. **note:** OS FingerPrint rivela il sistema operativo target analizzando le risposte e confrontandole con un database. (ogni versione di ogni sistema operativo potrebbe presentare differenze nel modo in cui risponde alle richieste)

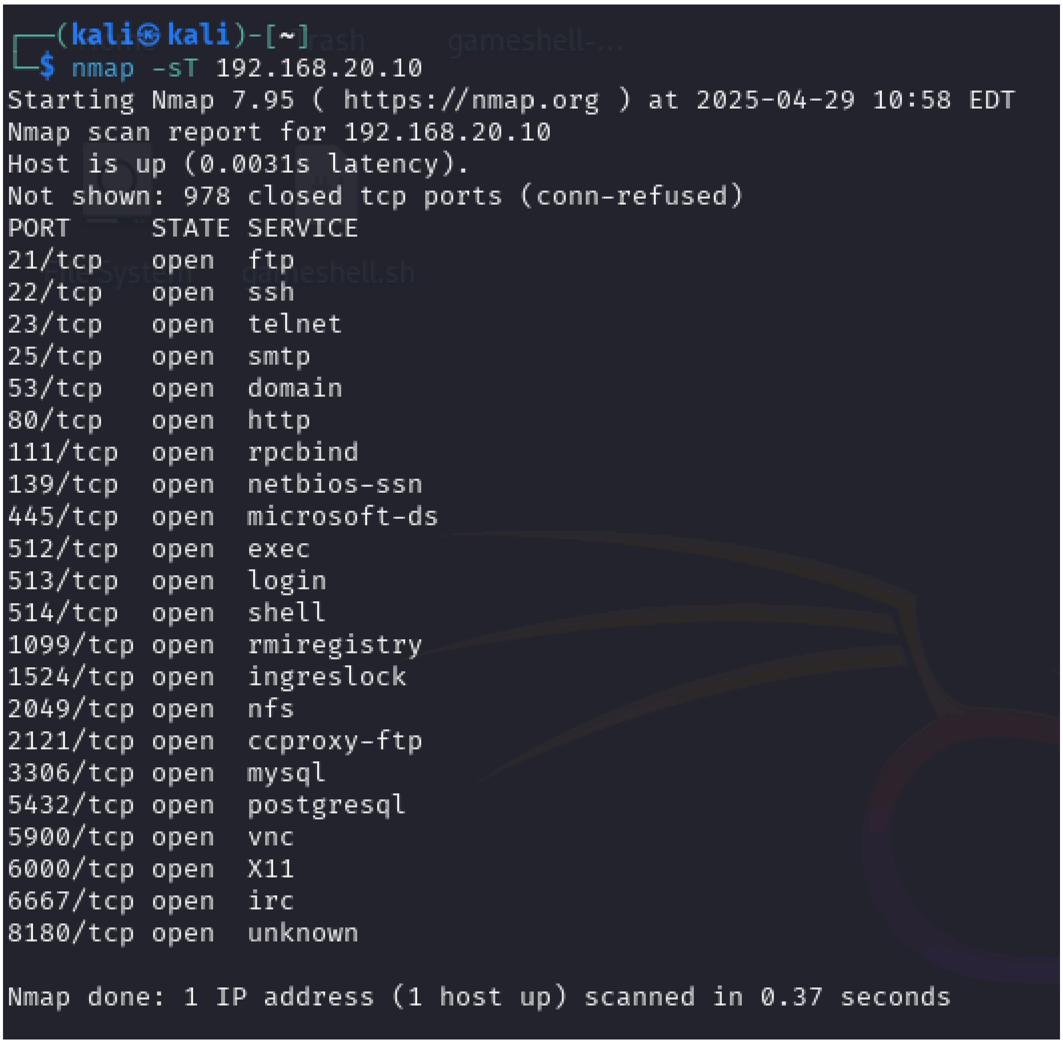
2. **SYN Scan**
    a. **Comando usato:** nmap -sS 192.168.20.10
    b. **Risultati:**



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.20.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:37 EDT
Nmap scan report for 192.168.20.10
Host is up (0.0020s latency).
Not shown: 978 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
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

    c. **note:** il SYN Scan invia pacchetti SYN (inizio connessione TCP) e analizza le risposte, non viene loggato dal sistema target.

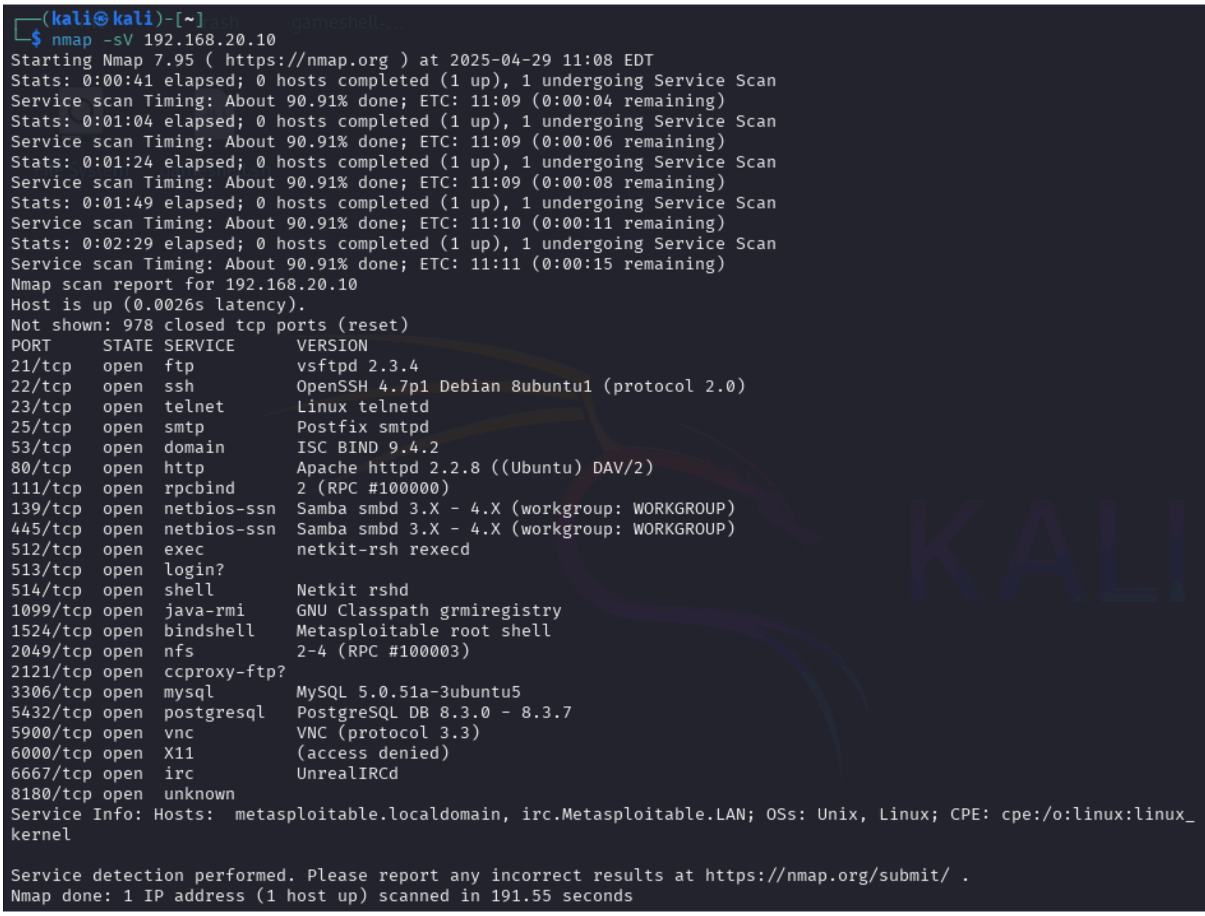
3. **TCP Connect Scan**
    a. **Comando usato:** nmap -sT 192.168.20.10
    b. **Risultati:**



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.20.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 10:58 EDT
Nmap scan report for 192.168.20.10
Host is up (0.0031s latency).
Not shown: 978 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
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

c. **differenze rispetto a SYS Scan:**
   Il TCP Connect Scan esegue una connessione completa TCP (SYN, SYN-ACK, ACK) e non richiede privilegi speciali. E’ utile quando si vogliono fare scansioni RAW come su windows senza privilegi di admin.

4. **Version Detection**
   a. **Comando usato:** namp -sV 192.168.20.10
   b. **Risultati:**



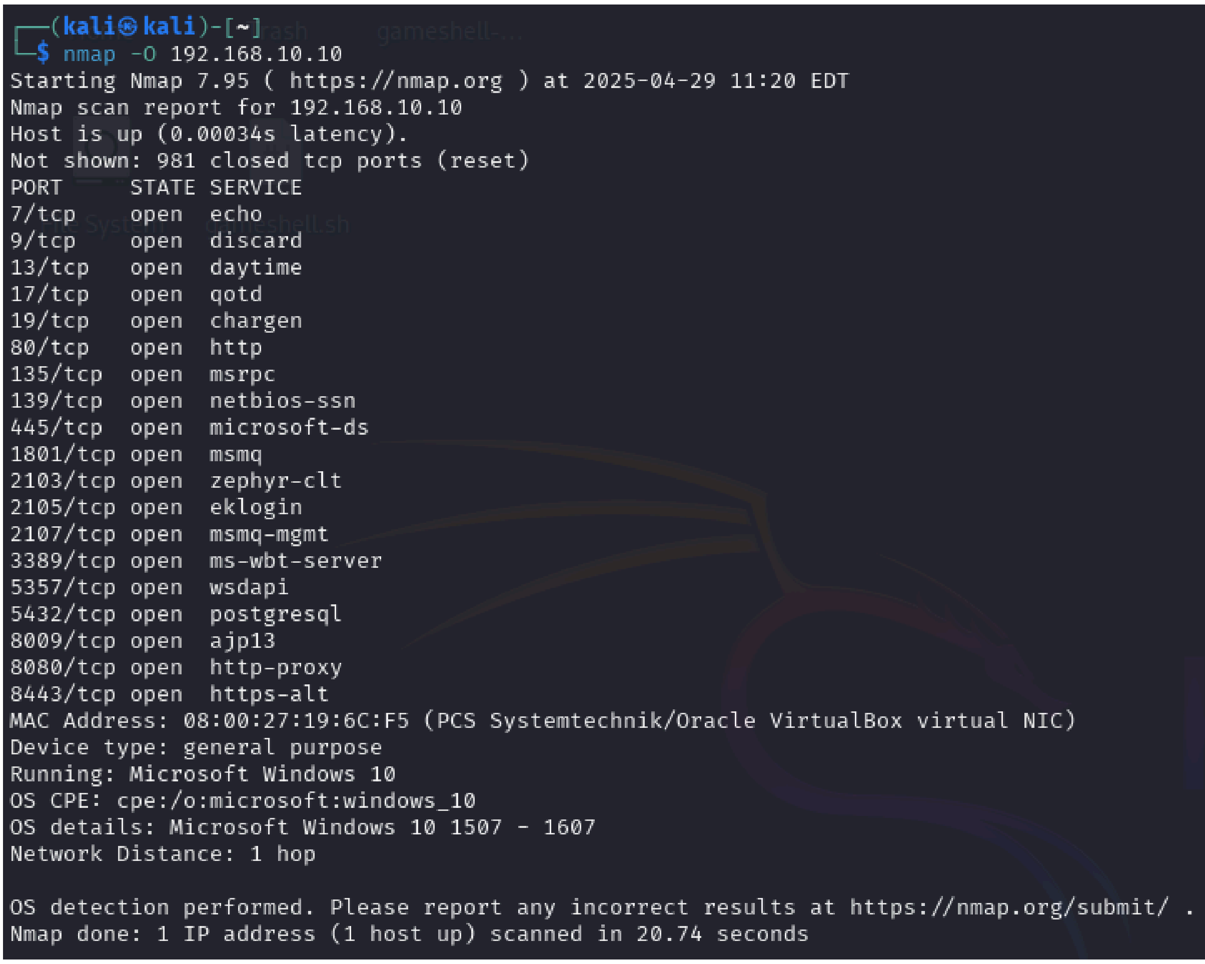
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.20.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 11:08 EDT
Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 90.91% done; ETC: 11:09 (0:00:04 remaining)
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 90.91% done; ETC: 11:09 (0:00:06 remaining)
Stats: 0:01:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 90.91% done; ETC: 11:09 (0:00:08 remaining)
Stats: 0:01:49 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 90.91% done; ETC: 11:10 (0:00:11 remaining)
Stats: 0:02:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 90.91% done; ETC: 11:11 (0:00:15 remaining)
Nmap scan report for 192.168.20.10
Host is up (0.0026s latency).
Not shown: 978 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        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
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       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
8180/tcp open  unknown
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 191.55 seconds
```

c. **note:** Il funzionamento e’ analogo a quello dell’OS FingerPrint. E’ utile quando si vuole sapere se ci sono versioni deprecate di servizi vulnerabili.

Target 2: Windows metasploitable

Ip: 192.168.10.10

1. **OS FingerPrint**
   a. **Comando usato:** nmap -O 192.168.10.10
   b. **Risultati:**



```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.10.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 11:20 EDT
Nmap scan report for 192.168.10.10
Host is up (0.00034s 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: 08:00:27:19:6C:F5 (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 20.74 seconds
```

Il comando ha rivelato con successo il sistema operativo target, Windows 10.

Riepilogo finale

Target	IP	OS Identificato	Porte aperte	Servizi + versione
metasploitable	192.168.20.10	linux 2.6.X 15 <= X <= 26	21 22 23 25 53 80 111	vsftpd 2.3.4 openSSH 4.7p1 linux telnet postfix smtp ISC BIND 9.4.2 apache httpd 2.2.8 RPC 2

			139 445 512 513 514 1099 1524 2049 2121 3306 5432 5900 6000 6667 8180	samba smbd 3.x - 4.x samba smbd 3.x - 4.x netkit-rsh rexecd / netkit-rsh GNU classpath grmiregistry metasploitable root shell 2-4 RCP / mySQL 5.0.51a-3ubuntu5 postgreSQL DB 8.3.0 - 8.3.7 VNC (protocol 3.3) / unrealIRCd unknown service
windows	192.168.10.10	windows 10	7 9 13 17 19 80 135 139 445 1801 2103 2105 2107 3389 5357 5432 8009 8080 8443	echo discard? daytime qotd chargen httpd 10.0 RPC netbios-ssn microsoft-ds msmq? RPC RPC RPC ms-wbt-server httpd 2.0 postgresql? apache Jserv v1.3 apache tomcat / coyote JSP engine 1.1 ssl/https-alt