Traccia: Tecniche di scansione con Nmap

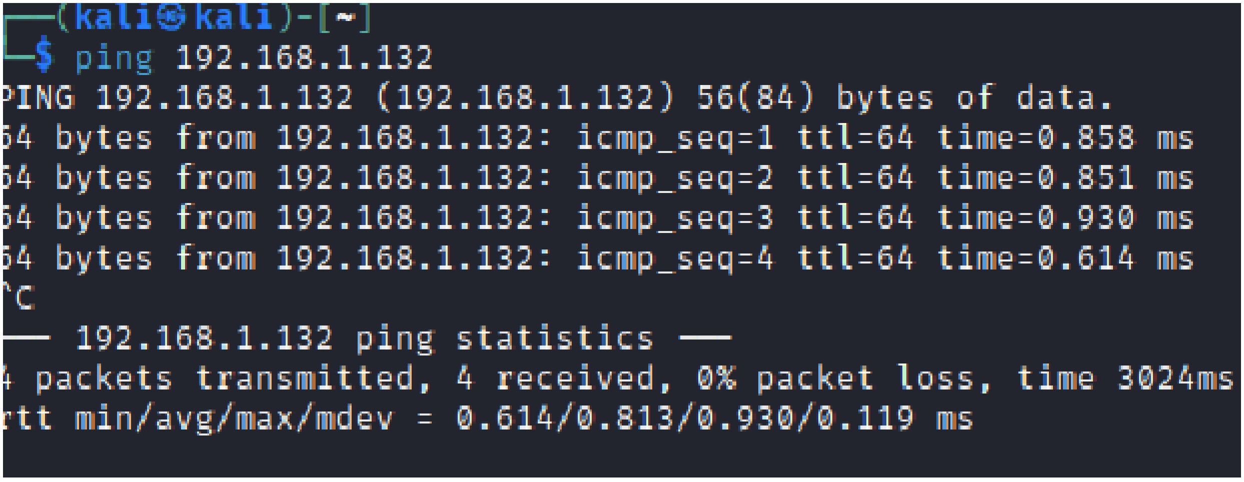
Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- 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:
- OS fingerprint.

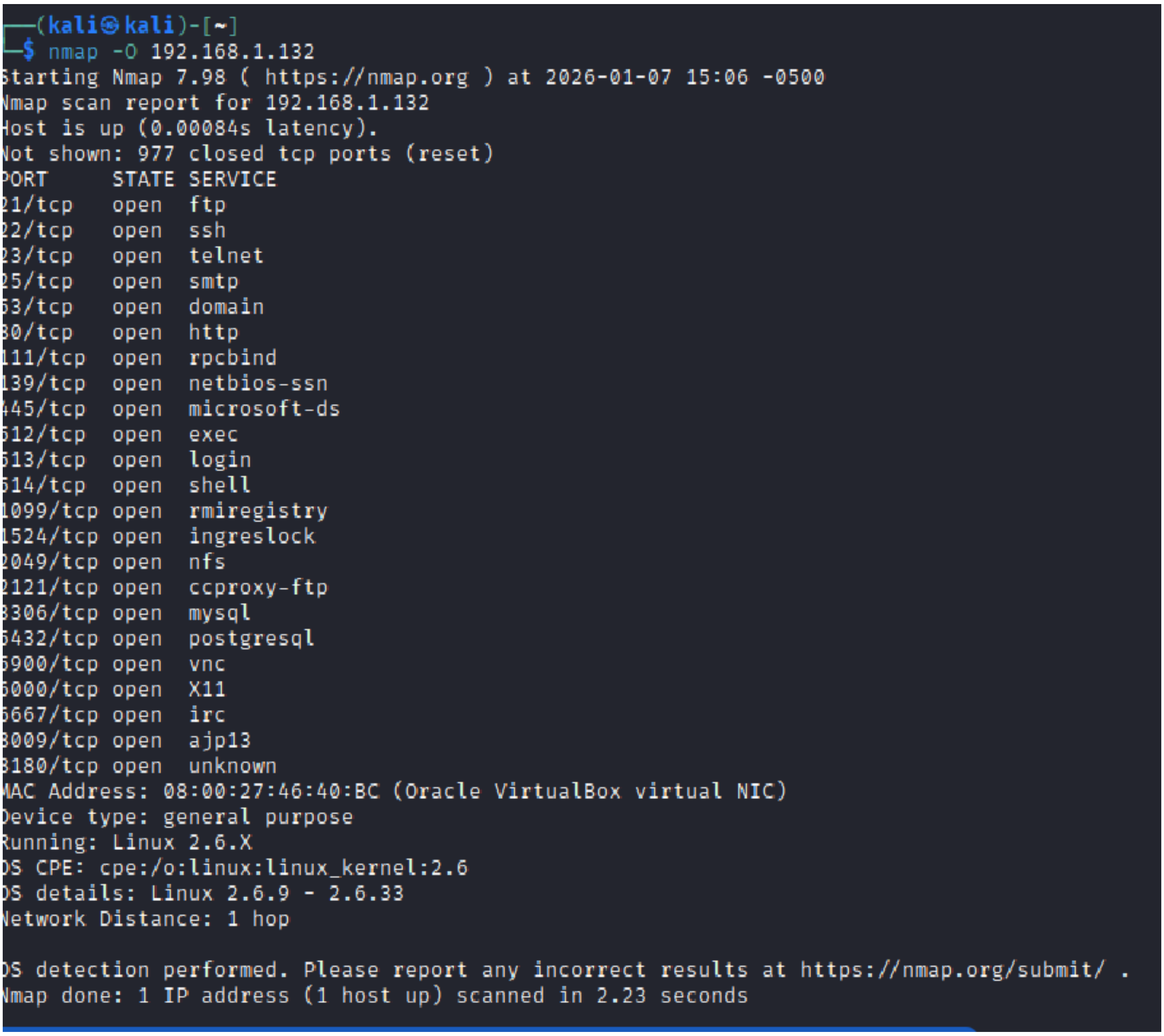
ESECUZIONE

Dopo aver collegato le due Macchine Virtuali Kali e Metasploitable eseguo le scansioni dal terminale Kali

- OS fingerprint. Nmap -O 192.168.1.132

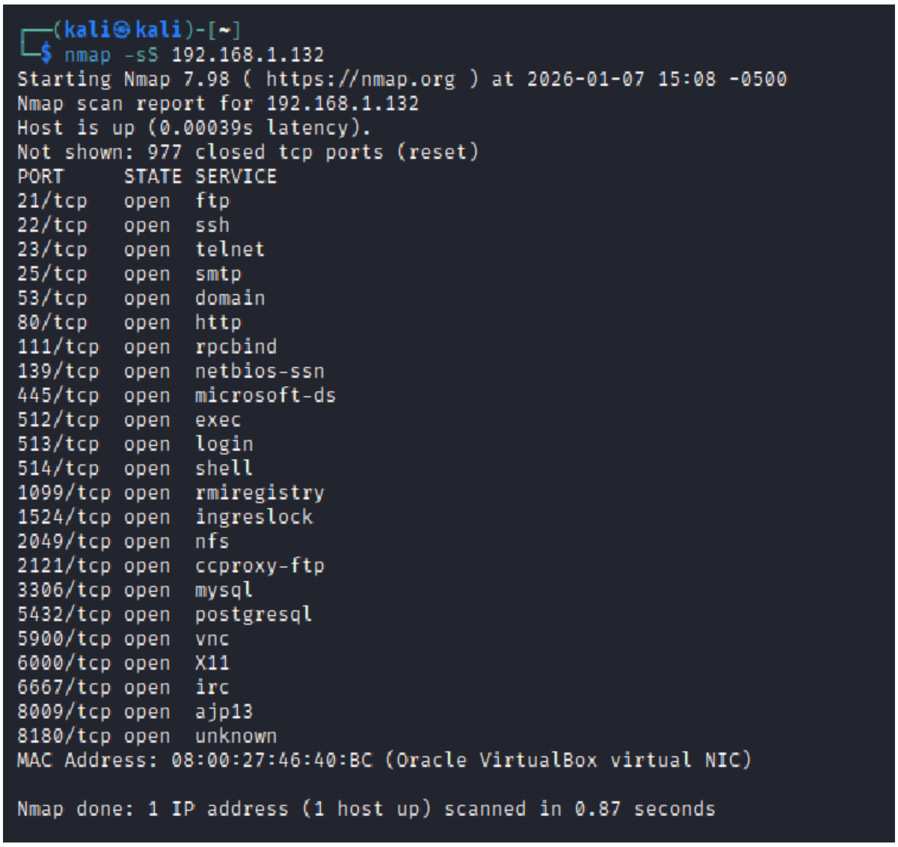


```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.132
PING 192.168.1.132 (192.168.1.132) 56(84) bytes of data.
64 bytes from 192.168.1.132: icmp_seq=1 ttl=64 time=0.858 ms
64 bytes from 192.168.1.132: icmp_seq=2 ttl=64 time=0.851 ms
64 bytes from 192.168.1.132: icmp_seq=3 ttl=64 time=0.930 ms
64 bytes from 192.168.1.132: icmp_seq=4 ttl=64 time=0.614 ms
^C
─── 192.168.1.132 ping statistics ───
4 packets transmitted, 4 received, 0% packet loss, time 3024ms
rtt min/avg/max/mdev = 0.614/0.813/0.930/0.119 ms
```



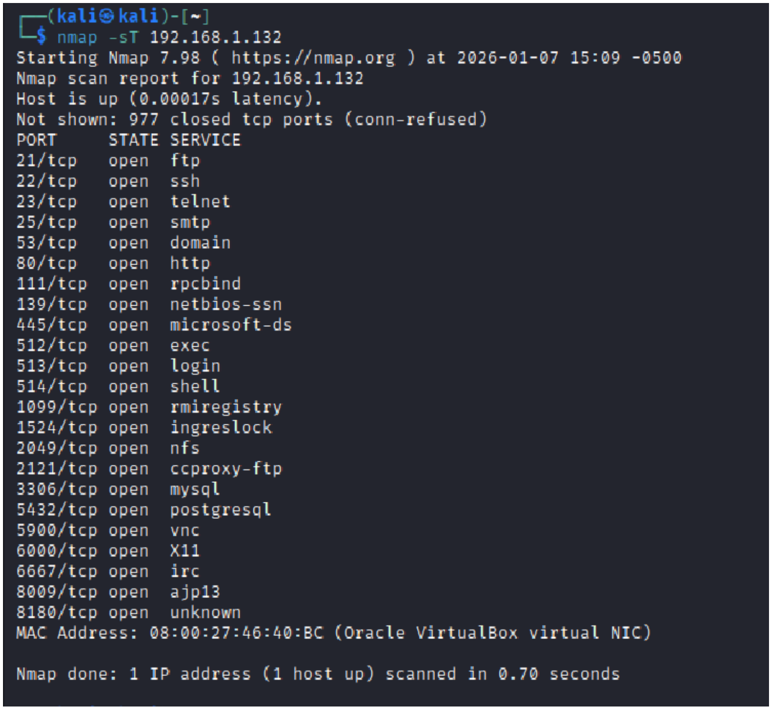
```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.1.132
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-07 15:06 -0500
Nmap scan report for 192.168.1.132
Host is up (0.00084s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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: 08:00:27:46:40:BC (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 2.23 seconds
```

- Syn Scan. Nmap -sS 192.168.1.132 come da immagine sottostante.



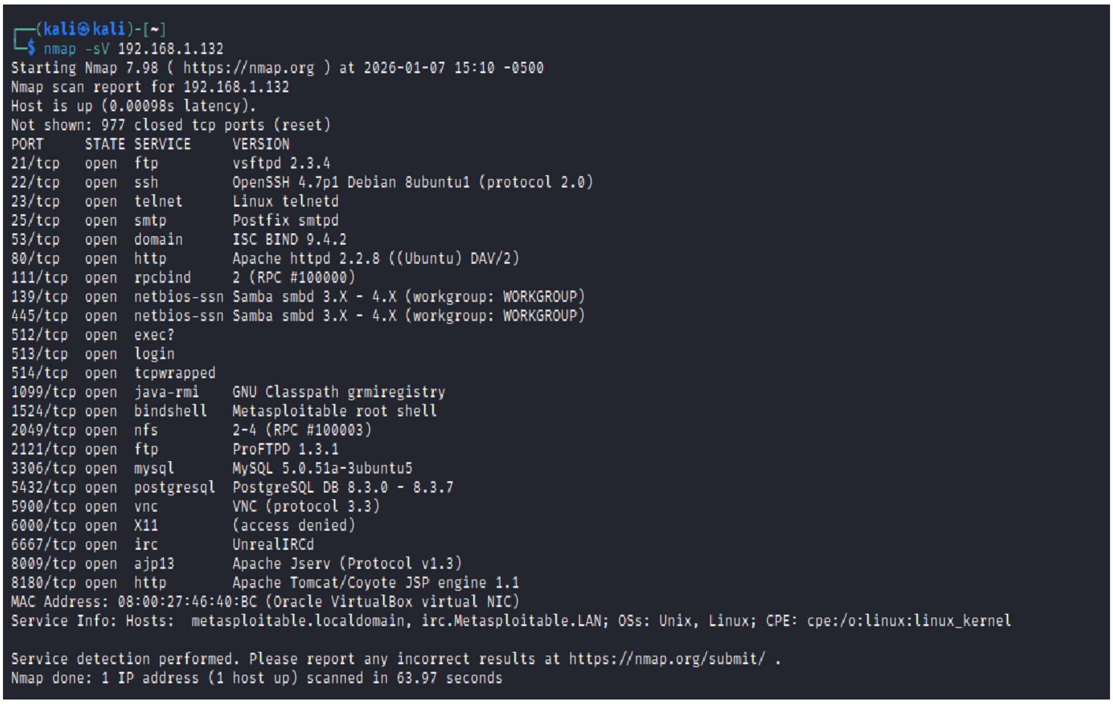
```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.1.132
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-07 15:08 -0500
Nmap scan report for 192.168.1.132
Host is up (0.00039s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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: 08:00:27:46:40:BC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds
```

- TCP connect nmap -sT 192.168.1.132 eseguendo la scansione più velocemente dello scan precedente



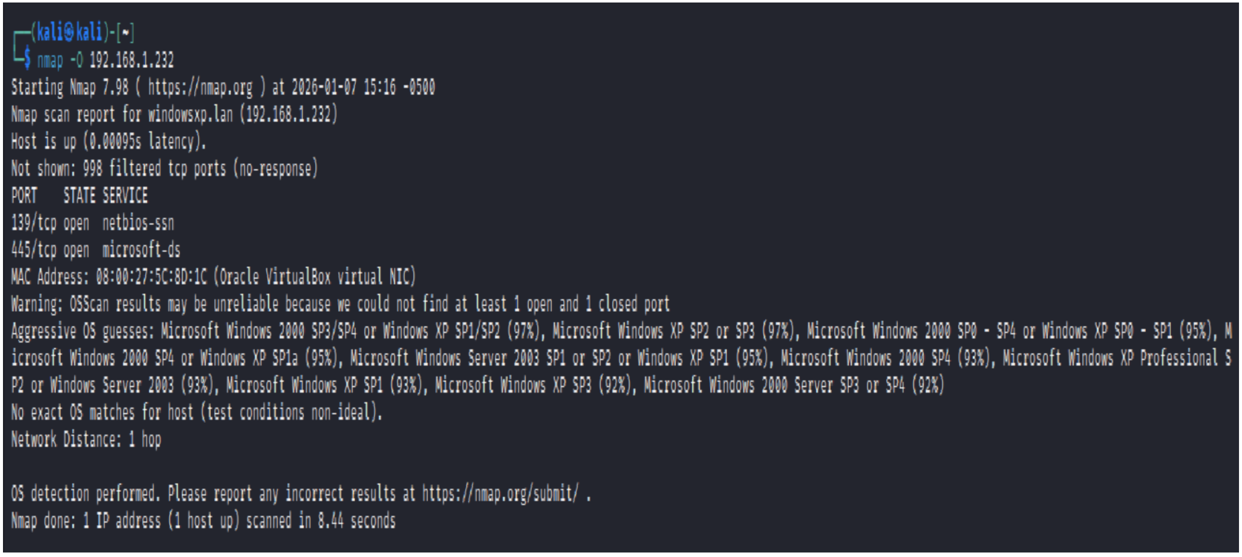
```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.1.132
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-07 15:09 -0500
Nmap scan report for 192.168.1.132
Host is up (0.00017s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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: 08:00:27:46:40:BC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
```

- Version detection. Nmap -sV 192.168.1.132

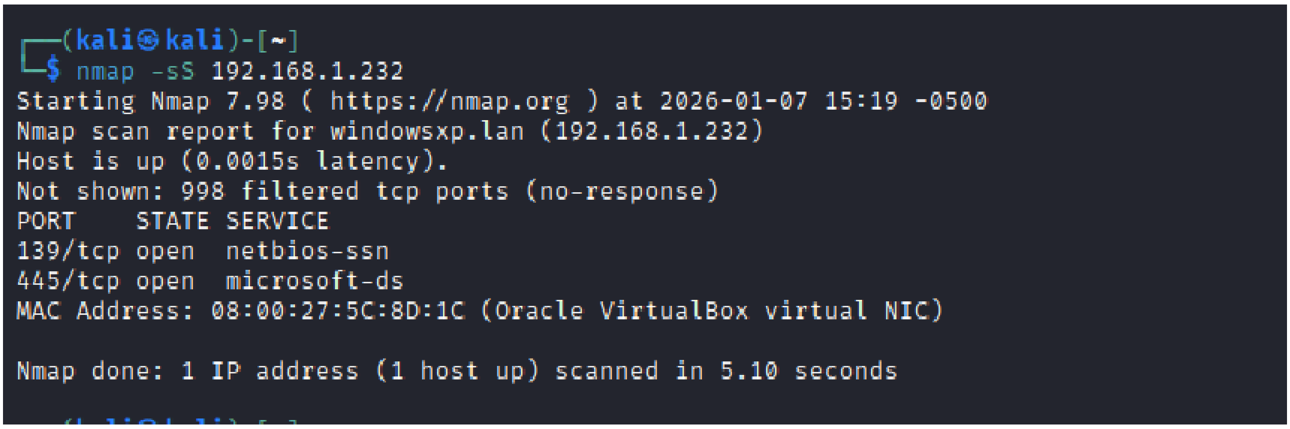


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.132
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-07 15:10 -0500
Nmap scan report for 192.168.1.132
Host is up (0.00098s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   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
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: 08:00:27:46:40:BC (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 63.97 seconds
```

Su Windows XP ip 192.168.1.232 eseguo OS fingerprint rilevando un Sistema Operativo Windows in un range di opzioni e un Syn scan



```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.1.232
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-07 15:16 -0500
Nmap scan report for windowsxp.lan (192.168.1.232)
Host is up (0.00095s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 2000 SP3/SP4 or Windows XP SP1/SP2 (97%), Microsoft Windows XP SP2 or SP3 (97%), Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1 (95%), M
icrosoft Windows 2000 SP4 or Windows XP SP1a (95%), Microsoft Windows Server 2003 SP1 or SP2 or Windows XP SP1 (95%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows XP Professional S
P2 or Windows Server 2003 (93%), Microsoft Windows XP SP1 (93%), Microsoft Windows XP SP3 (92%), Microsoft Windows 2000 Server SP3 or SP4 (92%)
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 8.44 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.1.232
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-07 15:19 -0500
Nmap scan report for windowsxp.lan (192.168.1.232)
Host is up (0.0015s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.10 seconds
```