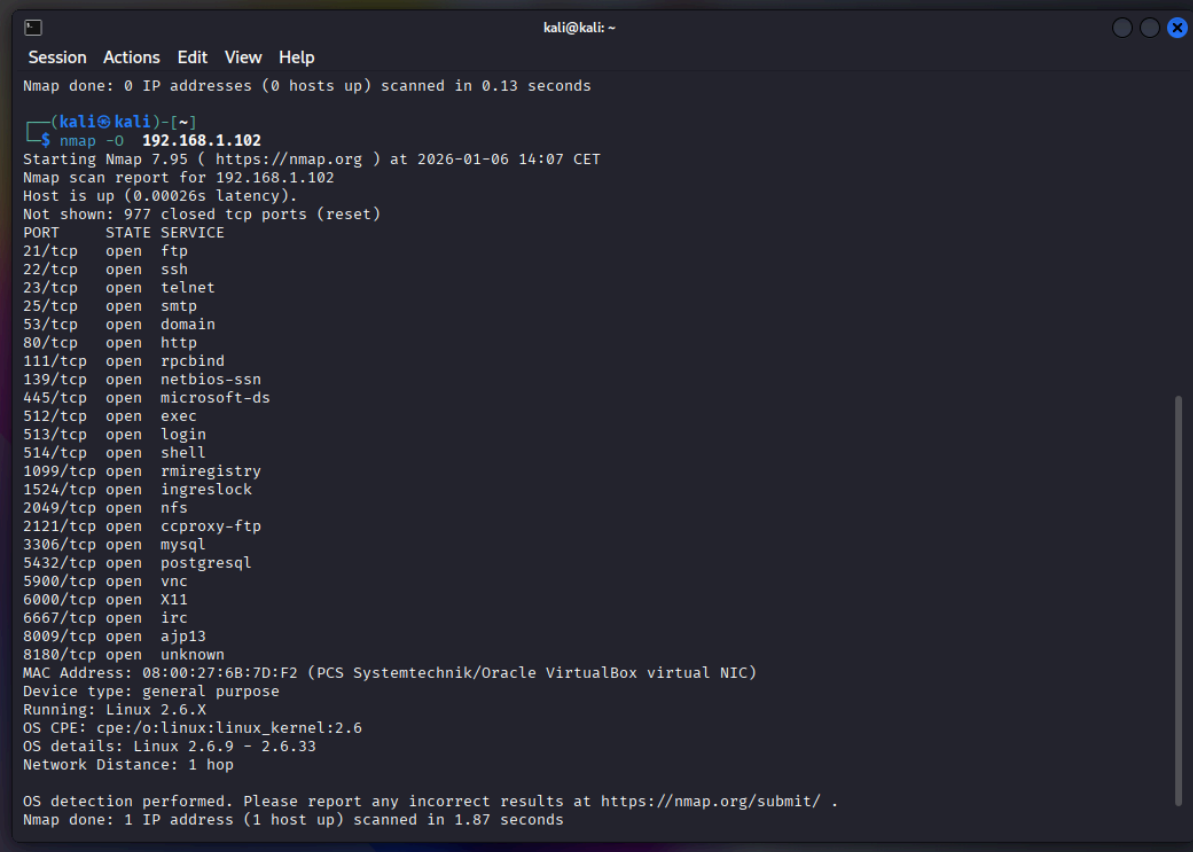


Report per scansione NMap su Target Metasploitable

Obbiettivo :

Si decide di raccogliere informazioni su un **target Metasploitable** di Ip **192.168.1.102**

- Os FingerPrint : determina il sistema operativo che è in esecuzione sul target :
 - Comando : `nmap -O 192.168.1.102`



```
kali@kali: ~  
Session Actions Edit View Help  
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.13 seconds  
  
(kali@kali)-[~]  
$ nmap -O 192.168.1.102  
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 14:07 CET  
Nmap scan report for 192.168.1.102  
Host is up (0.00026s 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: 08:00:27:6B:7D:F2 (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 1.87 seconds
```

Come si può vedere il **sistema operativo** della Meta è :

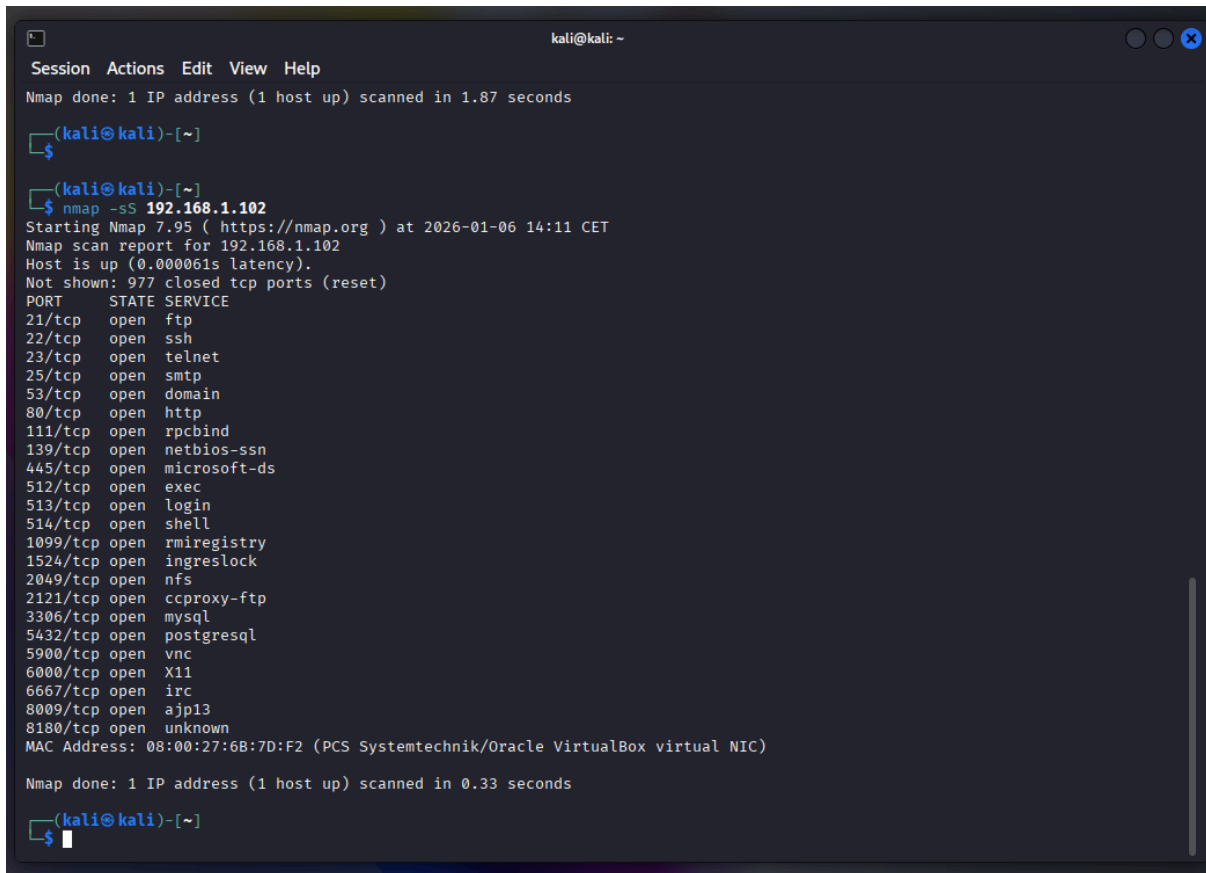
Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

● Syn Scan :

- Comando : `nmap -sS 192.168.1.102`



The screenshot shows a terminal window titled 'kali@kali: ~'. The window contains the output of an Nmap SYN scan. The first scan attempt shows 'Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds'. The second scan attempt, initiated by the command `nmap -sS 192.168.1.102`, shows 'Starting Nmap 7.95 (https://nmap.org) at 2026-01-06 14:11 CET'. The scan report for 192.168.1.102 indicates the host is up with a latency of 0.000061s. It lists 21 open ports with their corresponding services: 21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 25/tcp (smtp), 53/tcp (domain), 80/tcp (http), 111/tcp (rpcbind), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 512/tcp (exec), 513/tcp (login), 514/tcp (shell), 1099/tcp (rmiregistry), 1524/tcp (ingreslock), 2049/tcp (nfs), 2121/tcp (ccproxy-ftp), 3306/tcp (mysql), 5432/tcp (postgresql), 5900/tcp (vnc), 6000/tcp (X11), 6667/tcp (irc), 8009/tcp (ajp13), and 8180/tcp (unknown). The scan concludes with 'Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds'.

```
kali@kali: ~
Session Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds

(kali@kali)-[~]
$

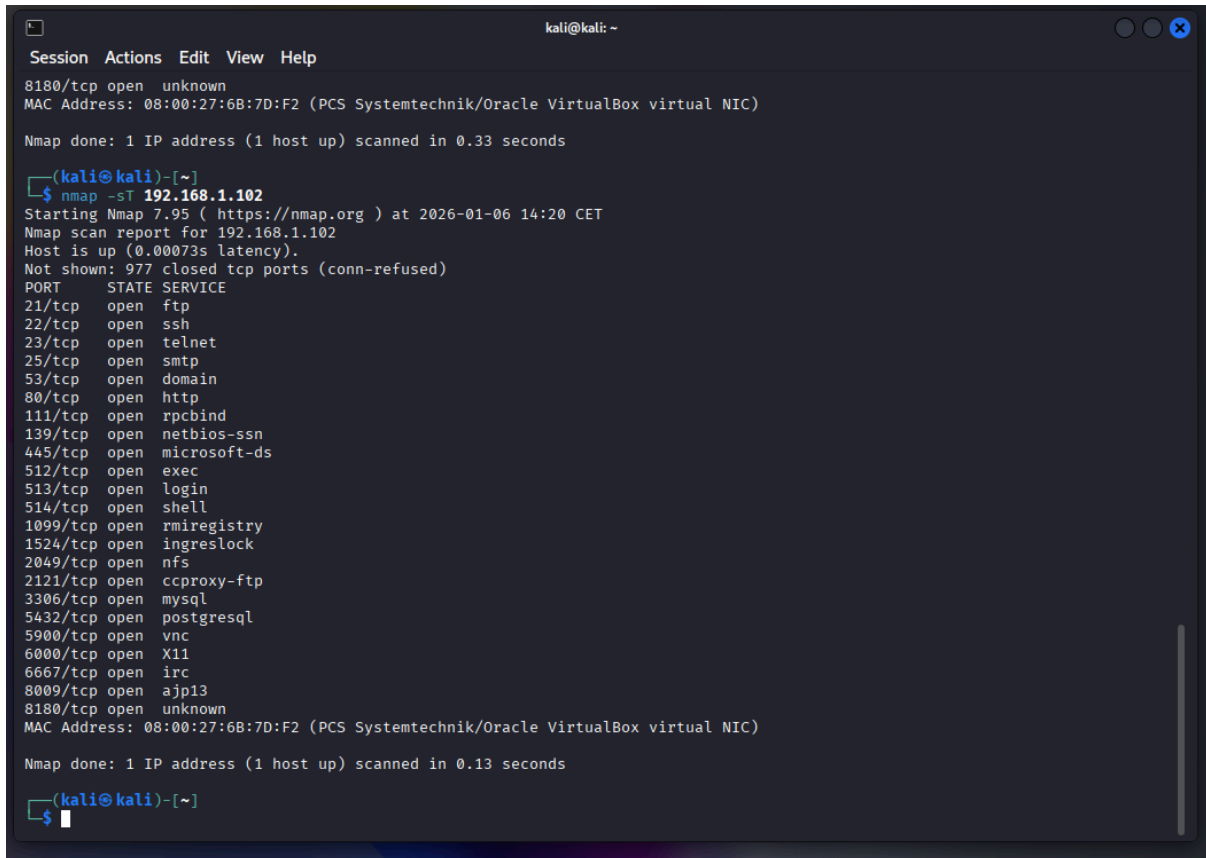
(kali@kali)-[~]
$ nmap -sS 192.168.1.102
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 14:11 CET
Nmap scan report for 192.168.1.102
Host is up (0.000061s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    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: 08:00:27:6B:7D:F2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

(kali@kali)-[~]
$
```

● Tcp Connect :

- Comando : `nmap -sT 192.168.1.102`



```
kali@kali: ~  
Session Actions Edit View Help  
8180/tcp open unknown  
MAC Address: 08:00:27:6B:7D:F2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds  
  
(kali@kali)-[~]  
$ nmap -sT 192.168.1.102  
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 14:20 CET  
Nmap scan report for 192.168.1.102  
Host is up (0.00073s 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: 08:00:27:6B:7D:F2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds  
  
(kali@kali)-[~]  
$
```

Differenza tra i due :

Nessuna differenza nella porte trovate aperte. L'unica differenza consiste nel metodo utilizzato per controllare la porta.

SYN Scan : reset

TCP Connect Scan : Conn-refused

● Version Detected

- Comando : `nmap -sV 192.168.1.102`

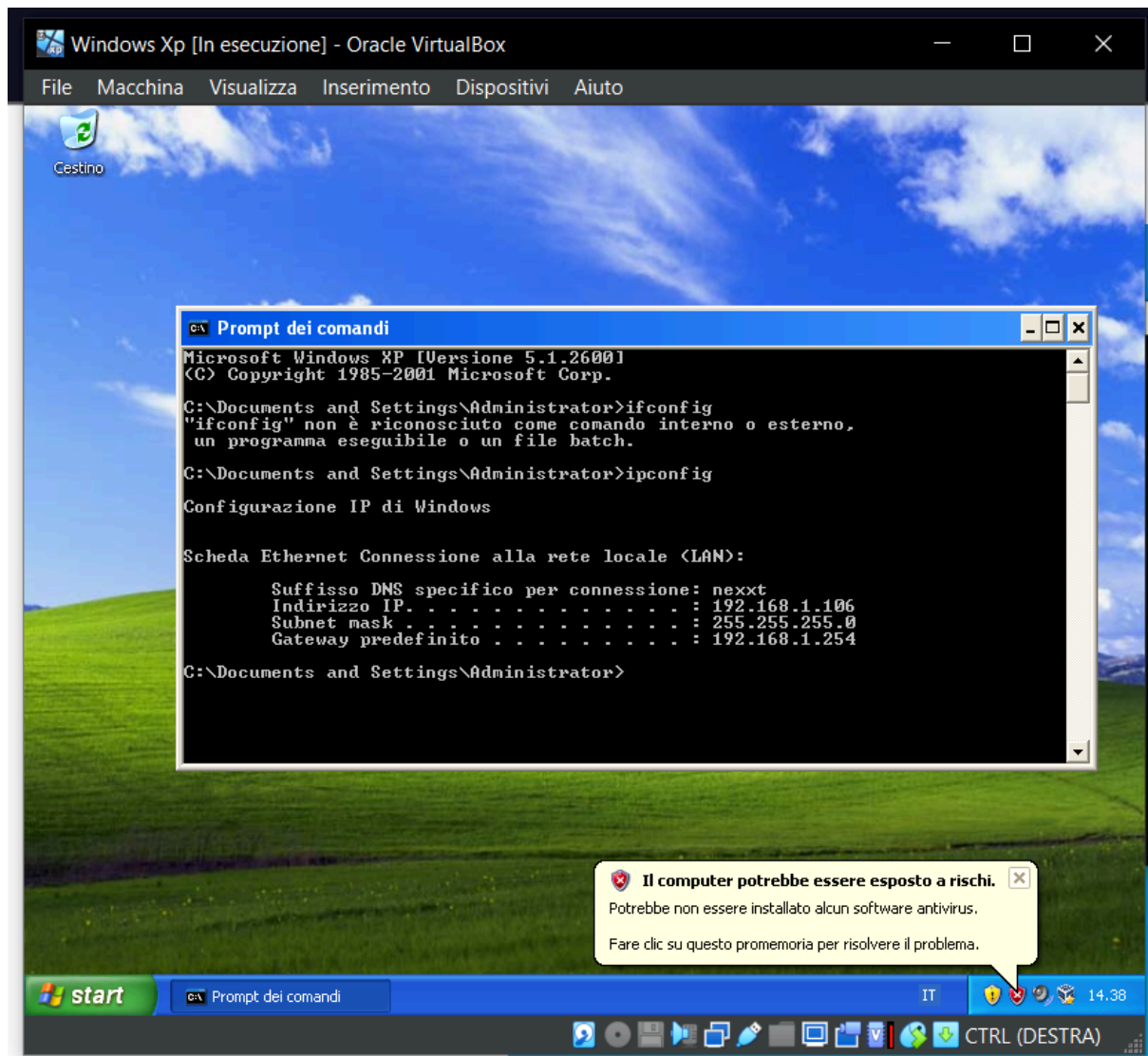
```
kali@kali: ~  
Session Actions Edit View Help  
  
(kali@kali)-[~]  
$ nmap -sV 192.168.1.102  
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 14:28 CET  
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 86.96% done; ETC: 14:28 (0:00:02 remaining)  
Nmap scan report for 192.168.1.102  
Host is up (0.0013s 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         netkit-rsh rexecd  
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: 08:00:27:68:7D:F2 (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 11.63 seconds  
  
(kali@kali)-[~]  
$
```

Obbiettivo :

Si decide di raccogliere informazioni su un **target Windows XP** di Ip **192.168.1.106**

- Os FingerPrint : determina il sistema operativo ch   e in esecuzione sul target :
 - Comando : `nmap -O 192.168.1.106`

```
kali@kali: ~  
Session Actions Edit View Help  
^C  
--- 169.254.179.73 ping statistics ---  
104 packets transmitted, 0 received, 100% packet loss, time 106953ms  
  
(kali@kali)-[~]  
$ ping 192.168.1.106  
PING 192.168.1.106 (192.168.1.106) 56(84) bytes of data:  
64 bytes from 192.168.1.106: icmp_seq=1 ttl=128 time=0.713 ms  
64 bytes from 192.168.1.106: icmp_seq=2 ttl=128 time=0.284 ms  
64 bytes from 192.168.1.106: icmp_seq=3 ttl=128 time=0.317 ms  
64 bytes from 192.168.1.106: icmp_seq=4 ttl=128 time=0.349 ms  
^C  
--- 192.168.1.106 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3058ms  
rtt min/avg/max/mdev = 0.284/0.415/0.713/0.173 ms  
  
(kali@kali)-[~]  
$ nmap -O 192.168.1.106  
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 14:36 CET  
Nmap scan report for 192.168.1.106  
Host is up (0.00037s 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 (PCS Systemtechnik/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%), Microsoft 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 SP2 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 10.47 seconds  
  
(kali@kali)-[~]  
$
```



Indirizzo ip, Subnet Mask e Gateway predefonito della macchina Windows Xp