

Os fingerprint

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.50.101/24
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 15:56 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0013s 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  cproxy-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: 08:00:27:06:E0:32 (Oracle VM VirtualBox virtual NIC)
```

```
(kali㉿kali)-[~]
File Actions Edit View Help
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:06:E0:32 (Oracle VM 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

Nmap scan report for 192.168.50.102
Host is up (0.0014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
MAC Address: 08:00:27:A1:81:43 (Oracle VM VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
Network Distance: 1 hop

Nmap scan report for 192.168.50.100
Host is up (0.000073s latency).
All 1000 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
```

```
OS CPE: cpe:/o:microsoft:windows_ / cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
Network Distance: 1 hop

Nmap scan report for 192.168.50.100
Host is up (0.000073s latency).
All 1000 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 14.94 seconds

(kali㉿kali)-[~]
$
```

Syn Scan

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.50.101/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 16:04 CEST
Nmap scan report for 192.168.50.101
Host is up (0.000675s 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  cproxy-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: 08:00:27:06:E0:32 (Oracle VM VirtualBox virtual NIC)
```

```
File Actions Edit View Help
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  cproxy-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: 08:00:27:06:E0:32 (Oracle VM VirtualBox virtual NIC)

Nmap scan report for 192.168.50.102
Host is up (0.0012s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
MAC Address: 08:00:27:A1:81:43 (Oracle VM VirtualBox virtual NIC)

Nmap scan report for 192.168.50.100
Host is up (0.000023s latency).
All 1000 scanned ports on 192.168.50.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 13.63 seconds

(kali㉿kali)-[~]
$
```

TCP + trovare le differenze con Syn scan

```
(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 16:09 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0012s 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: 08:00:27:06:E0:32 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

TCP + SYN SCAN

TCP

- Tempo di latenza 0,0012
- Porte chiuse = conn-refused 977
- MAC ADDRESS = non è molto rilevato
- Durata scannone = 0,39 sec.

SYN SCAN

- Tempo di latenza 0,0067
- Porte chiuse = reset 977
- MAC ADDRESS = è molto rilevato
- Durata scannone = 13,36 sec

Version detection

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 17:46 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0008s 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 smtd
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  shell        Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2 (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: 08:00:27:06:E0:32 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
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: 08:00:27:06:E0:32 (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 12.35 seconds
```

OS fingerprint Windows

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-26 18:05 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0019s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:A1:81:43 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
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 14.22 seconds
```

- IP = 192.168.50.102

- S.O = Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0

- Porte aperte = 135/Tcp

139/Tcp

445/Tcp

- Servizi in ascolto con versione = msrpc → 135

netbios-ssn → 139

microsoft-ds → 445

} Microsoft.

Extra

Se una porta chiusa, il risultato è inaffidabile, che è necessario per un'analisi precisa nel rilevamento del S.O.