

OS FINGER PRINT W7

```
(root@kali)-[~]
└─# sudo nmap -Pn -O 192.168.5.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 09:10 EDT
Nmap scan report for 192.168.5.102
Host is up (0.00022s latency). Please report any incorrect results a
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49158/tcp  open  unknown
MAC Address: 08:00:27:58:F0:A4 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:
microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cp
e:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows S
erver 2008 R2, Windows 8, or Windows 8.1 Update 1
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 16.22 seconds
```

IP:	192.168.5.101	
OS:	W7	
PORTE APERTE:	135/msrpc	porta usata per le comunicazioni
	139/netbios-ssn	porta usata per le comunicazioni di rete, usata
		in passato.
	445/microsoft-ds	porta usata per il protocollo SMB (Server
		Message Block) su reti Windows.

Qui possiamo osservare che il comando nmap scannerizza ip di W7 e mostra sia le porte aperte, il servizio ed il sistema operativo del dispositivo

OS FINGER PRINT META

```
(root@kali)~[~] # sudo nmap -Pn -O 192.168.5.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 09:09 EDT
Nmap scan report for 192.168.5.101
Host is up (0.00020s 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/desktop
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:C0:6A:C7 (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 15.22 seconds
```

IP: 192.168.5.101

OS: W7

PORTE APERTE: tutte quella nell'immagine, che vengono ad essere le porte piu comuni.

Qui possiamo osservare che il comando nmap scannerizza ip di META e mostra sia le porte aperte, il servizio ed il sistema operativo del dispositivo. Addifferenza di W7, Meta mostra piu porte aperte.

SYN SCAN META

```
(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sS 192.168.5.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 09:19 EDT
Nmap scan report for 192.168.5.101
Host is up (0.000075s 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:C0:6A:C7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.50 seconds
```

Comando nmap, usando il metodo “sS”, scannerizza le porte aperte in modo meno invasivo.

Il pacchetto non conclude il 3 way handshake, si interrompe nella fase SYN/ACK, per rimandare indietro NON ACK ma RST(reset).

TCP CONNECTION META

```
(kali㉿kali)-[~/Desktop]
$ sudo nmap -sT 192.168.5.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 09:36 EDT
Nmap scan report for 192.168.5.101
Host is up (0.00028s 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:C0:6A:C7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.47 seconds
```

Comando nmap, usando il metodo “sT”, scannerizza le porte aperte ni modo molto invasivo/rumoroso.

Il pacchetto conclude il 3 way handshake, a differenza del “sS”, quindi recupera info sullo stato della porta, ma crea grosse congestioni di rete per quanto invasivo sia.

VERSION DETECTION META

```
(kali@kali)~[~/Desktop]
$ sudo nmap -sV 192.168.5.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 09:43 EDT
Nmap scan report for 192.168.5.101
Host is up (0.00015s 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  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  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:C0:6A:C7 (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 25.22 seconds
```

Comando nmap, usando il metodo “sV” esegue ua scansione abilitando la feature di “version detection”, grazie alla quale oltre al servizio recuperiamo anche la versione e relativi dettagli.