Fingerprint

```
┌──(root㉿kali)-[/home/marco]
└─# nmap -O 192.168.50.110
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-03 20:10 CEST
Nmap scan report for 192.168.50.110
Host is up (0.00064s latency).

All 1000 scanned ports on 192.168.50.110 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 08:00:27:24:88:18 (Oracle VirtualBox virtual NIC)

Too many fingerprints match this host to give specific OS details
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 37.06 seconds
```

```
┌──(root㉿kali)-[/home/marco]
└─# nmap 192.168.50.110 --script smb-os-discovery
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-03 20:14 CEST
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 32.00% done; ETC: 20:15 (0:00:15 remaining)

Nmap scan report for 192.168.50.110
Host is up (0.00024s latency).

All 1000 scanned ports on 192.168.50.110 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 08:00:27:24:88:18 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.57 seconds
```

Syn Scan + Version Scan + Fingerprint

```
┌──(root㉿kali)-[/home/marco]
└─# nmap -sS -sV -O 192.168.50.110
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-03 20:13 CEST
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 82.00% done; ETC: 20:13 (0:00:04 remaining)
Nmap scan report for 192.168.50.110
Host is up (0.00049s latency).

All 1000 scanned ports on 192.168.50.110 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 08:00:27:24:88:18 (Oracle VirtualBox virtual NIC)

Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.20 seconds
```

Scansione porta 88

```
┌──(root㉿kali)-[/home/marco]
└─# nmap -sS -v -g 88  192.168.50.110
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-03 20:08 CEST

Initiating ARP Ping Scan at 20:08
Scanning 192.168.50.110 [1 port]
Completed ARP Ping Scan at 20:08, 0.04s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 20:08
Completed Parallel DNS resolution of 1 host. at 20:09, 13.00s elapsed

Initiating SYN Stealth Scan at 20:09
Scanning 192.168.50.110 [1000 ports]
Completed SYN Stealth Scan at 20:09, 21.24s elapsed (1000 total ports)

Nmap scan report for 192.168.50.110
Host is up (0.00064s latency).

All 1000 scanned ports on 192.168.50.110 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 08:00:27:24:88:18 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 34.36 seconds
Raw packets sent: 2001 (88.028KB) | Rcvd: 1 (28B)
```

```
┌──(root㉿kali)-[/home/marco]
└─# nmap -sS -T4 -v -g 88 192.168.50.110
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-03 20:26 CEST
Initiating ARP Ping Scan at 20:26
Scanning 192.168.50.110 [1 port]
Completed ARP Ping Scan at 20:26, 0.05s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 20:26
Completed Parallel DNS resolution of 1 host. at 20:26, 13.00s elapsed
Initiating SYN Stealth Scan at 20:26
Scanning 192.168.50.110 [1000 ports]
Completed SYN Stealth Scan at 20:27, 21.26s elapsed (1000 total ports)

Nmap scan report for 192.168.50.110
Host is up (0.00045s latency).
All 1000 scanned ports on 192.168.50.110 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:24:88:18 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 34.40 seconds
Raw packets sent: 2001 (88.028KB) | Rcvd: 1 (28B)
```

```
┌──(marco㉿kali)-[~]
└─$ sudo nmap -mtu 24 -p 88 192.168.50.110
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 20:49 CEST
Nmap scan report for 192.168.50.110
Host is up (0.00064s latency).

PORT   STATE    SERVICE
88/tcp filtered kerberos-sec

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

Scansione porta 80

```
┌──(root㉿kali)-[/home/marco]
└─# nmap 192.168.50.110 --source-port 80
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-03 20:20 CEST
Nmap scan report for 192.168.50.110
Host is up (0.00062s latency).
All 1000 scanned ports on 192.168.50.110 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:24:88:18 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.38 seconds
```

Scansione porte da 1 a 100 T4

```
┌──(root㉿kali)-[/home/marco]
└─# nmap -sF -p1-100 -T4 192.168.50.110
```

Starting Nmap 7.93 (https://nmap.org) at 2023-05-03 20:52 CEST
Nmap scan report for 192.168.50.110
Host is up (0.00061s latency).
All 100 scanned ports on 192.168.50.110 are in ignored states.
Not shown: 100 open|filtered tcp ports (no-response)
MAC Address: 08:00:27:24:88:18 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.20 seconds

Scansione senza ping

```
┌──(root㉿kali)-[/home/marco]
└─# nmap -sS -v -v -Pn 192.168.50.110
```

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 (https://nmap.org) at 2023-05-03 20:53 CEST
Initiating ARP Ping Scan at 20:53
Scanning 192.168.50.110 [1 port]
Completed ARP Ping Scan at 20:53, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:53
Completed Parallel DNS resolution of 1 host. at 20:53, 13.00s elapsed
Initiating SYN Stealth Scan at 20:53
Scanning 192.168.50.110 [1000 ports]
Completed SYN Stealth Scan at 20:54, 21.25s elapsed (1000 total ports)
Nmap scan report for 192.168.50.110
Host is up, received arp-response (0.00046s latency).
Scanned at 2023-05-03 20:53:51 CEST for 21s
All 1000 scanned ports on 192.168.50.110 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:24:88:18 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 34.38 seconds
Raw packets sent: 2001 (88.028KB) | Rcvd: 1 (28B)

….includo la porta 88

```
┌──(root㉿kali)-[/home/marco]
└─# nmap -sS -v -v -Pn -g 88  192.168.50.110
```

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 (https://nmap.org) at 2023-05-03 20:56 CEST
Initiating ARP Ping Scan at 20:56
Scanning 192.168.50.110 [1 port]
Completed ARP Ping Scan at 20:56, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:56
Completed Parallel DNS resolution of 1 host. at 20:56, 13.00s elapsed
Initiating SYN Stealth Scan at 20:56
Scanning 192.168.50.110 [1000 ports]
Completed SYN Stealth Scan at 20:56, 21.31s elapsed (1000 total ports)

Nmap scan report for 192.168.50.110
Host is up, received arp-response (0.00037s latency).
Scanned at 2023-05-03 20:56:22 CEST for 21s
All 1000 scanned ports on 192.168.50.110 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:24:88:18 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 34.45 seconds
Raw packets sent: 2001 (88.028KB) | Rcvd: 1 (28B)

Scan con Packet trace

┌──(root㉿kali)-[/home/marco]
└─# **nmap -vv -sn -PE -T4 --packet-trace 192.168.50.110**
Starting Nmap 7.93 (https://nmap.org) at 2023-05-03 20:59 CEST
Initiating ARP Ping Scan at 20:59
Scanning 192.168.50.110 [1 port]
SENT (0.0307s) ARP who-has 192.168.50.110 tell 192.168.50.100
RCVD (0.0313s) ARP reply 192.168.50.110 is-at 08:00:27:24:88:18
Completed ARP Ping Scan at 20:59, 0.03s elapsed (1 total hosts)
NSOCK INFO [0.0700s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.0700s] nsock_connect_udp(): UDP connection requested to 192.168.1.103:53 (IOD #1) EID 8
NSOCK INFO [0.0700s] nsock_read(): Read request from IOD #1 [192.168.1.103:53] (timeout: -1ms) EID 18
NSOCK INFO [0.0700s] nsock_iod_new2(): nsock_iod_new (IOD #2)
NSOCK INFO [0.0700s] nsock_connect_udp(): UDP connection requested to 192.168.1.1:53 (IOD #2) EID 24
NSOCK INFO [0.0700s] nsock_read(): Read request from IOD #2 [192.168.1.1:53] (timeout: -1ms) EID 34
Initiating Parallel DNS resolution of 1 host. at 20:59
NSOCK INFO [0.0700s] nsock_write(): Write request for 45 bytes to IOD #1 EID 43 [192.168.1.103:53]
NSOCK INFO [0.0700s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.1.103:53]
NSOCK INFO [0.0700s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 43 [192.168.1.103:53]
NSOCK INFO [0.0700s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 24 [192.168.1.1:53]
NSOCK INFO [2.5740s] nsock_write(): Write request for 45 bytes to IOD #1 EID 51 [192.168.1.103:53]
NSOCK INFO [2.5740s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 51 [192.168.1.103:53]
NSOCK INFO [6.5760s] nsock_write(): Write request for 45 bytes to IOD #2 EID 59 [192.168.1.1:53]
NSOCK INFO [6.5760s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 59 [192.168.1.1:53]
NSOCK INFO [9.0760s] nsock_write(): Write request for 45 bytes to IOD #2 EID 67 [192.168.1.1:53]

NSOCK INFO [9.0760s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 67 [192.168.1.1:53]
Completed Parallel DNS resolution of 1 host. at 20:59, 13.01s elapsed
NSOCK INFO [13.0750s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [13.0750s] nevent_delete(): nevent_delete on event #18 (type READ)
NSOCK INFO [13.0750s] nsock_iod_delete(): nsock_iod_delete (IOD #2)
NSOCK INFO [13.0750s] nevent_delete(): nevent_delete on event #34 (type READ)
Nmap scan report for 192.168.50.110
Host is up, received arp-response (0.00067s latency).
MAC Address: 08:00:27:24:88:18 (Oracle VirtualBox virtual NIC)
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
Raw packets sent: 1 (28B) | Rcvd: 1 (28B)

Scan con controllo dimensione pacchetto (24 e 16 byte)

```
┌──(marco㉿kali)-[~]
└─$ sudo nmap --mtu 24 192.168.50.110
```
Starting Nmap 7.93 (https://nmap.org) at 2023-05-03 21:12 CEST
Nmap scan report for 192.168.50.110
Host is up (0.00056s latency).
All 1000 scanned ports on 192.168.50.110 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:24:88:18 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.37 seconds

```
┌──(marco㉿kali)-[~]
└─$ sudo nmap --mtu 16  192.168.50.110
```
Starting Nmap 7.93 (https://nmap.org) at 2023-05-03 21:13 CEST
Nmap scan report for 192.168.50.110
Host is up (0.00060s latency).
All 1000 scanned ports on 192.168.50.110 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:24:88:18 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.40 seconds

Scan senza ping T1

```
┌──(root㉿kali)-[/home/marco]
└─# nmap -Pn -T1 192.168.50.110
```
Starting Nmap 7.93 (https://nmap.org) at 2023-05-04 06:32 CEST
Stats: 0:00:15 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 0.00% done
Stats: 1:39:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.65% done; ETC: 14:54 (6:43:11 remaining)
Stats: 3:29:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 41.65% done; ETC: 14:53 (4:52:23 remaining)
Stats: 4:02:56 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 48.40% done; ETC: 14:53 (4:18:30 remaining)
Stats: 6:05:32 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 72.90% done; ETC: 14:53 (2:15:43 remaining)
Stats: 7:25:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 88.95% done; ETC: 14:53 (0:55:20 remaining)
Stats: 7:59:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 95.75% done; ETC: 14:53 (0:21:17 remaining)
Nmap scan report for 192.168.50.110
Host is up (0.0015s latency).
All 1000 scanned ports on 192.168.50.110 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:24:88:18 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 30069.68 seconds

```
┌──(marco㉿kali)-[~]
└─$ sudo nmap -mtu 24 -p 8080 192.168.50.110
```
[sudo] password di marco:
Starting Nmap 7.93 (https://nmap.org) at 2023-05-05 19:16 CEST
Nmap scan report for 192.168.50.110
Host is up (0.0037s latency).

PORT STATE SERVICE
8080/tcp filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds

```
┌──(marco㉿kali)-[~]
└─$ sudo nmap -mtu 24 -p 443 192.168.50.110
```
Starting Nmap 7.93 (https://nmap.org) at 2023-05-05 19:19 CEST
Nmap scan report for 192.168.50.110
Host is up (0.00030s latency).

PORT STATE SERVICE
443/tcp filtered https
MAC Address: 08:00:27:24:88:18 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds

REPORT

IP: 192.168.50.110

S.O.: Too many fingerprints match this host to give specific OS details

MAC Address: 08:00:27:24:88:18 (Oracle VirtualBox virtual NIC)

PORTE APERTE:
TUTTE FILTRATE (FIREWALL)

ad esempio:
88/tcp filtered kerberos-sec
443/tcp filtered https
8080/tcp filtered http-proxy