W11D4 - Nmap target Windows

Target: Macchina Windows 10 - IP:192.168.50.102

scansione Nmap SYN Scan - "*nmap -sS 192.168.50.102*"

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-25 15:16 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00053s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
8443/tcp open  https-alt
MAC Address: 08:00:27:F6:0D:8F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.53 seconds
```

scansione Nmap OS Fingerprint - "*nmap -O 192.168.50.102*"

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-25 14:51 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00049s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
8443/tcp open  https-alt
MAC Address: 08:00:27:F6:0D:8F (PCS Systemtechnik/Oracle VirtualBo
Warning: OSScan results may be unreliable because we could not fin
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 10|2008|7|8.1|Phone|Vis
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_serve
Aggressive OS guesses: Microsoft Windows 10 1607 (91%), Microsoft
rosoft Windows 10 1511 (85%), Microsoft Windows 7 or Windows Serve
0 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 23.23 seconds
```

scansione Nmap TCP Connect - *“nmap -sT 192.168.50.102”*

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-25 15:17 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0010s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
8443/tcp open  https-alt
MAC Address: 08:00:27:F6:0D:8F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.92 seconds
```

scansione Nmap Version Detection - *“nmap -sV 192.168.50.102”*

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-25 15:18 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00026s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:F6:0D:8F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 94.13 seconds
```