sudo nmap -Pn 192.168.1.* -O

Starting Nmap 7.93 (https://nmap.org) at 2023-08-26 05:22 EDT
Nmap scan report for 192.168.1.2
Host is up (0.00059s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open domain
80/tcp open http
MAC Address: 08:00:27:3C:7D:35 (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: general purpose
Running (JUST GUESSING): FreeBSD 11.X (98%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (98%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.1.102
Host is up (0.00038s latency).
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
49157/tcp open unknown
MAC Address: 08:00:27:25:3C:C6 (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 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

Nmap scan report for 192.168.1.101
Host is up (0.000045s latency).
All 1000 scanned ports on 192.168.1.101 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 11.75 seconds

- in questa maniera abbiamo individuato la macchina windows nella nostra rete: 192.168.1.102

sudo nmap -A 192.168.1.102

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-26 05:25 EDT
Nmap scan report for 192.168.1.102
Host is up (0.00064s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds
(workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:25:3C:C6 (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
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,
Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WINZOZ7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Winzoz7
|   NetBIOS computer name: WINZOZ7\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-07-17T22:00:38+02:00
| smb2-time:
|   date: 2023-07-17T20:00:38
|_  start_date: 2023-07-17T19:24:42
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: WINZOZ7, NetBIOS user: <unknown>, NetBIOS MAC: 080027253cc6
(Oracle VirtualBox virtual NIC)
|_clock-skew: mean: -39d14h05m27s, deviation: 1h09m16s, median: -39d13h25m27s
| smb2-security-mode:
```

| 210:
|_ Message signing enabled but not required

- con questo comando sono riuscito a vedere il servizio di ogni porta aperta e relativa versione, oltre al sistema operativo ed altre informazioni più o meno utili

nmap -oN report1 192.168.1.102
ci permette di salvare il risultato di nmp in report1:
Nmap 7.93 scan initiated Sat Aug 26 05:32:37 2023 as: nmap -oN report1 192.168.1.102
Nmap scan report for 192.168.1.102
Host is up (0.00061s latency).
Not shown: 991 closed tcp ports (conn-refused)
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
49157/tcp open unknown

Nmap done at Sat Aug 26 05:32:39 2023 -- 1 IP address (1 host up) scanned in 2.05 seconds