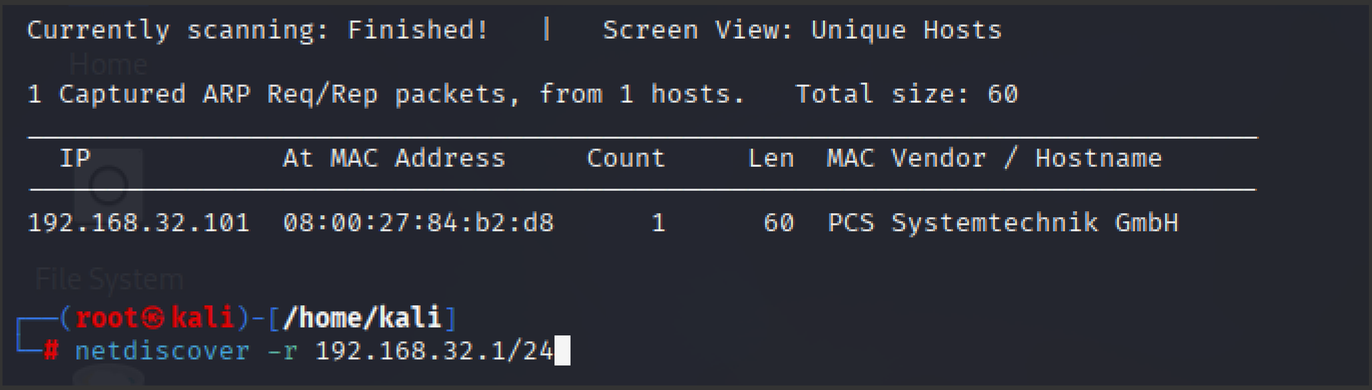
Come per l'esercizio precedente, si andrà ad utilizzare Nmap per ottenere informazioni su una macchina, in questo caso con Windows.

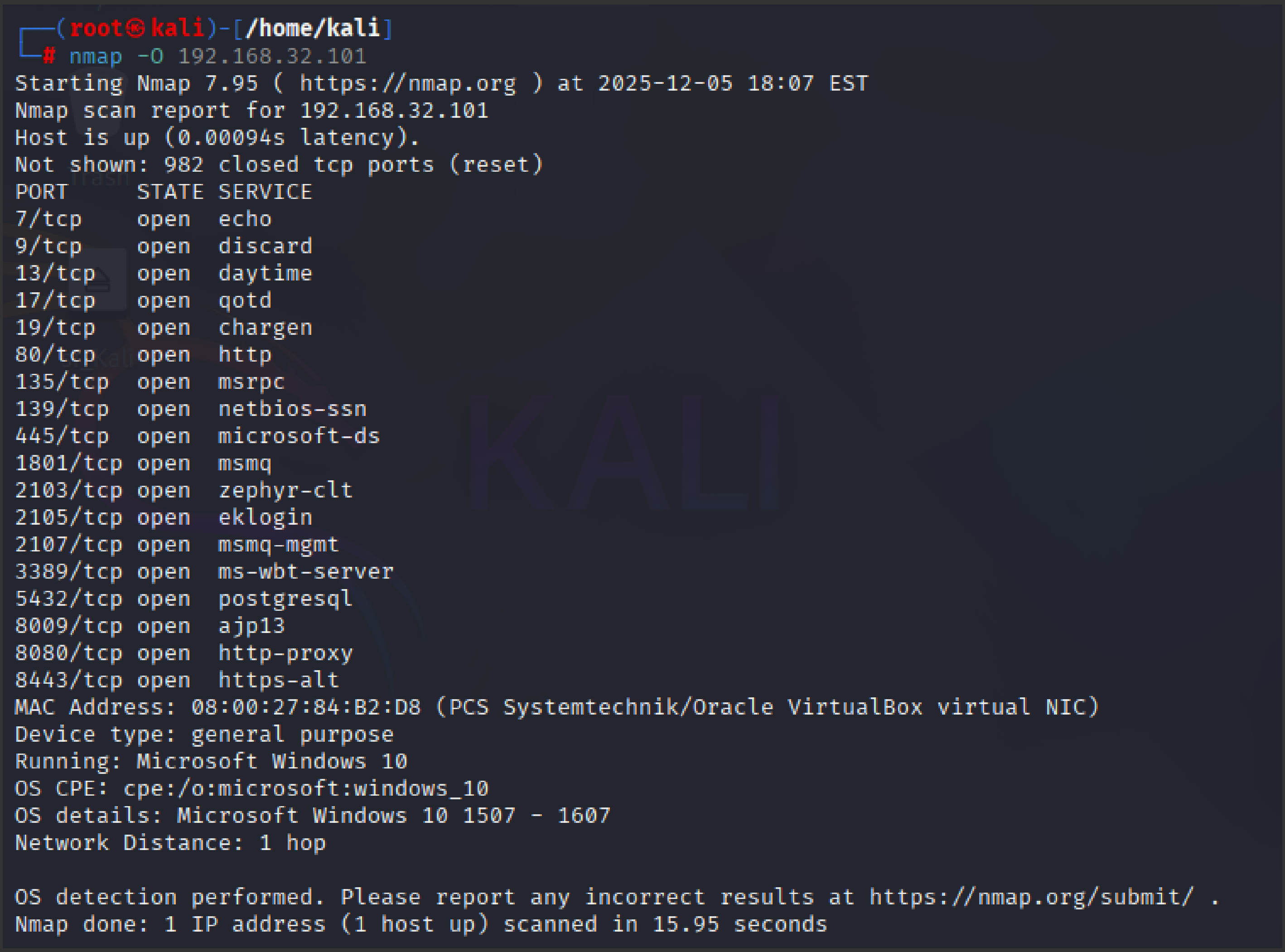
Con Netdiscover -r, o in alternativa con Nmap -sn -PE, si andranno a mostrare gli host attivi in un determinato range.

Ip attivo trovato: 192.168.32.1011 (Ip Windows)



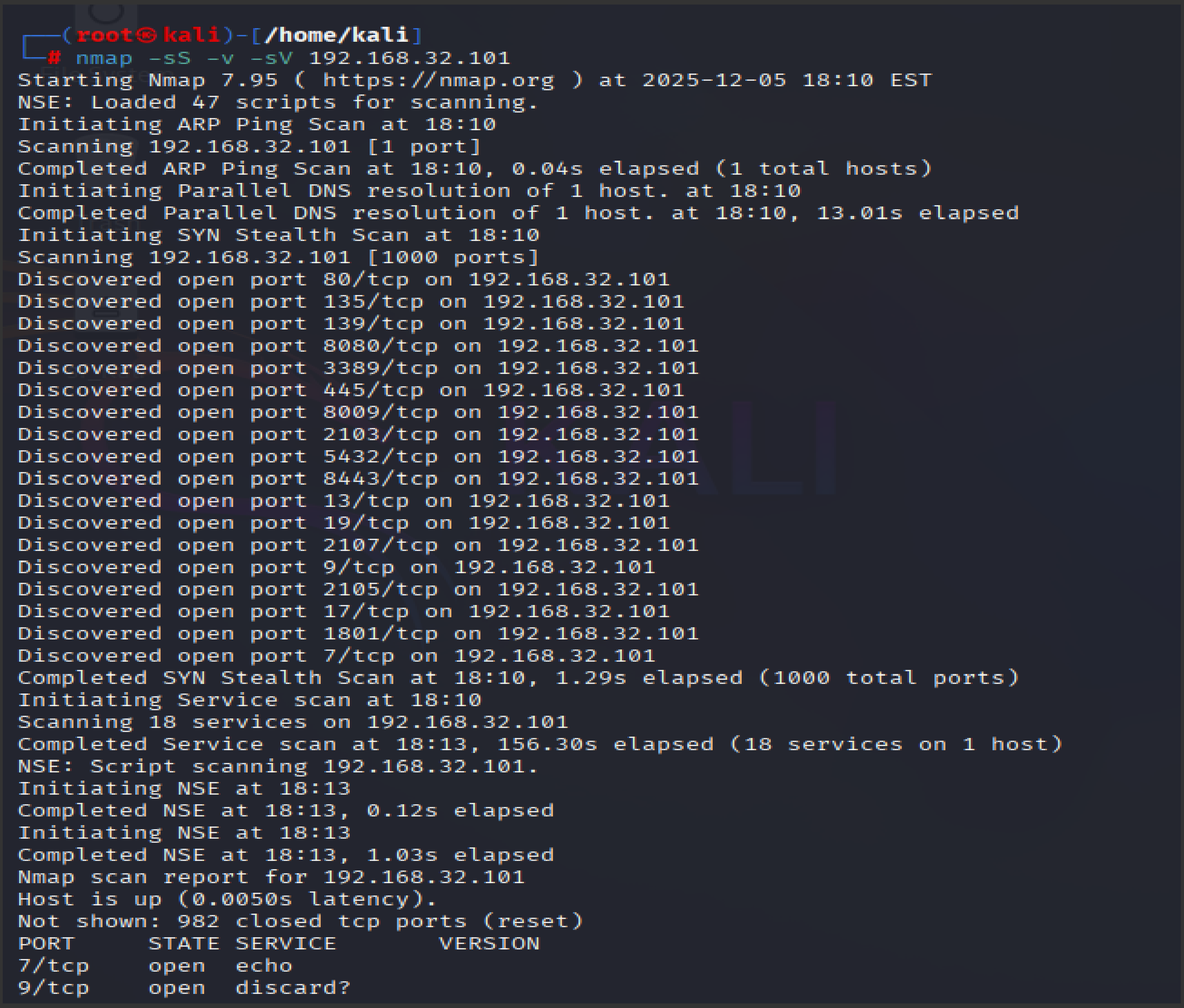
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.32.101  08:00:27:84:b2:d8      1       60  PCS Systemtechnik GmbH


┌──(root㉿kali)-[/home/kali]
└─# netdiscover -r 192.168.32.1/24
```

Con Nmap -O si visualizzano le porte aperte, e la versione del Sistema Operativo.

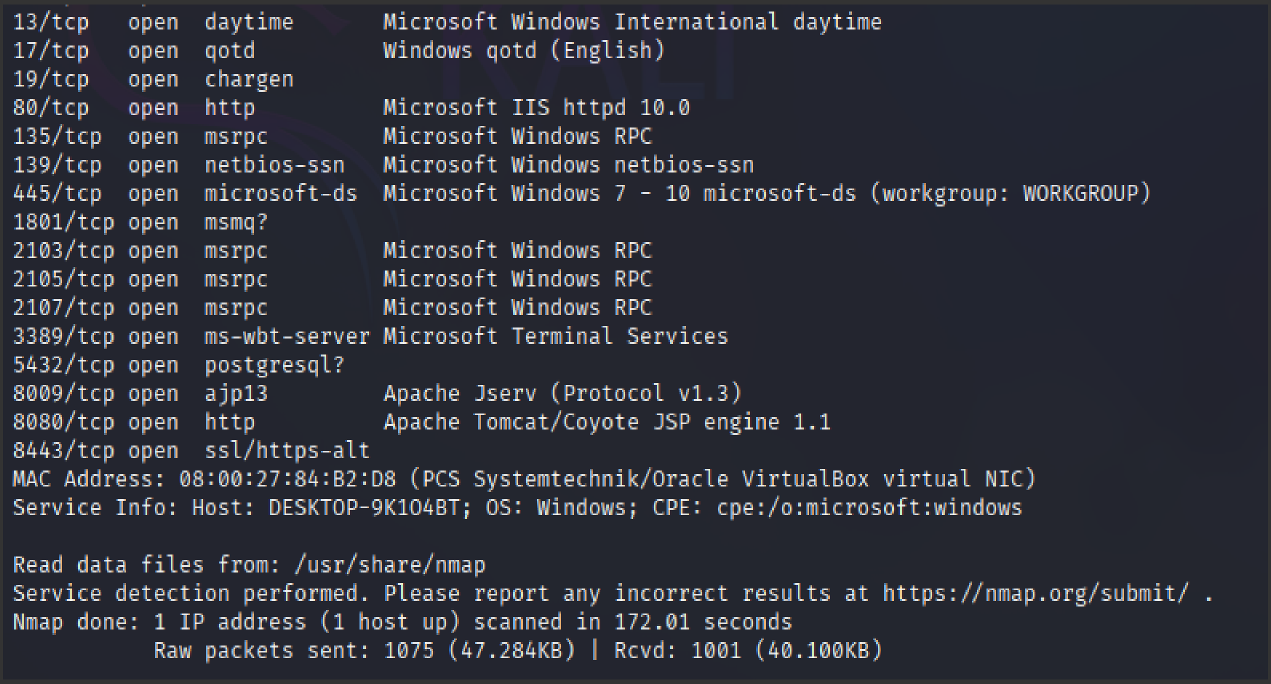


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.32.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 18:07 EST
Nmap scan report for 192.168.32.101
Host is up (0.00094s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
5432/tcp open  postgresql
8009/tcp open  ajp13
8080/tcp open  http-proxy
8443/tcp open  https-alt
MAC Address: 08:00:27:84:B2:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 15.95 seconds
```

Con il Syn Scan tramite Nmap -sS -v -sV si visualizzeranno i servizi attivi, e le loro versioni.

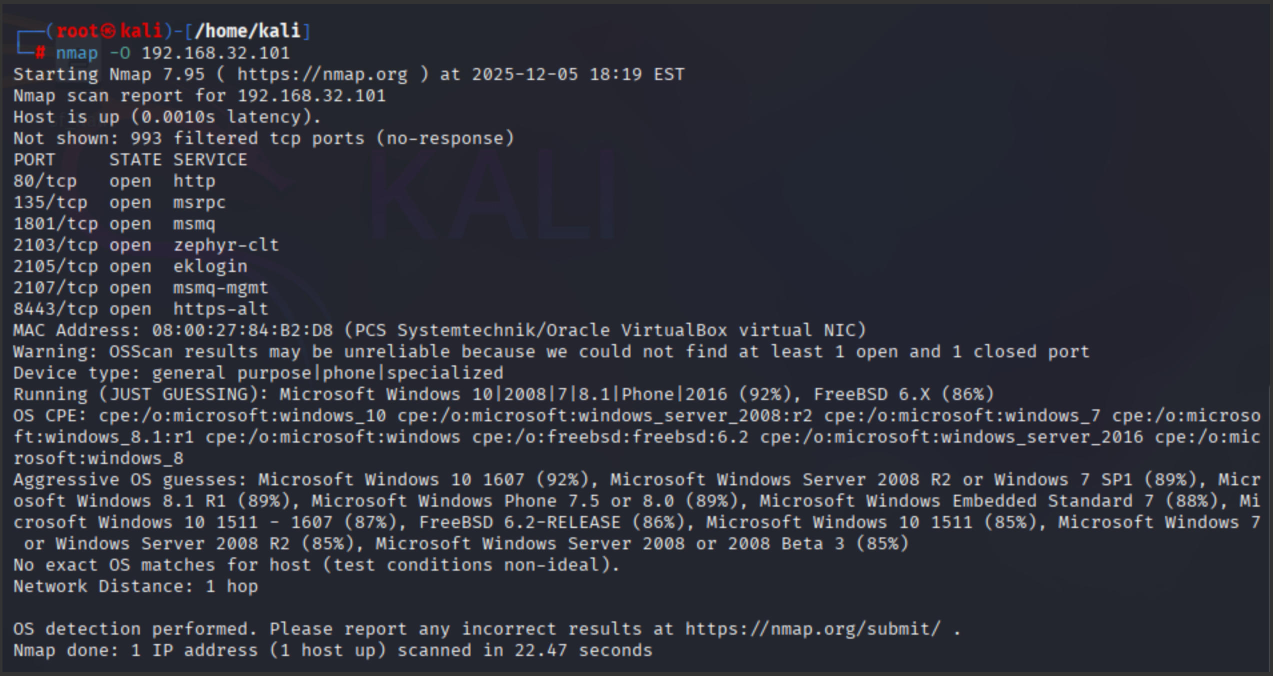


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -v -sV 192.168.32.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 18:10 EST
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 18:10
Scanning 192.168.32.101 [1 port]
Completed ARP Ping Scan at 18:10, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:10
Completed Parallel DNS resolution of 1 host. at 18:10, 13.01s elapsed
Initiating SYN Stealth Scan at 18:10
Scanning 192.168.32.101 [1000 ports]
Discovered open port 80/tcp on 192.168.32.101
Discovered open port 135/tcp on 192.168.32.101
Discovered open port 139/tcp on 192.168.32.101
Discovered open port 8080/tcp on 192.168.32.101
Discovered open port 3389/tcp on 192.168.32.101
Discovered open port 445/tcp on 192.168.32.101
Discovered open port 8009/tcp on 192.168.32.101
Discovered open port 2103/tcp on 192.168.32.101
Discovered open port 5432/tcp on 192.168.32.101
Discovered open port 8443/tcp on 192.168.32.101
Discovered open port 13/tcp on 192.168.32.101
Discovered open port 19/tcp on 192.168.32.101
Discovered open port 2107/tcp on 192.168.32.101
Discovered open port 9/tcp on 192.168.32.101
Discovered open port 2105/tcp on 192.168.32.101
Discovered open port 17/tcp on 192.168.32.101
Discovered open port 1801/tcp on 192.168.32.101
Discovered open port 7/tcp on 192.168.32.101
Completed SYN Stealth Scan at 18:10, 1.29s elapsed (1000 total ports)
Initiating Service scan at 18:10
Scanning 18 services on 192.168.32.101
Completed Service scan at 18:13, 156.30s elapsed (18 services on 1 host)
NSE: Script scanning 192.168.32.101.
Initiating NSE at 18:13
Completed NSE at 18:13, 0.12s elapsed
Initiating NSE at 18:13
Completed NSE at 18:13, 1.03s elapsed
Nmap scan report for 192.168.32.101
Host is up (0.0050s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
7/tcp    open  echo
9/tcp    open  discard?
```

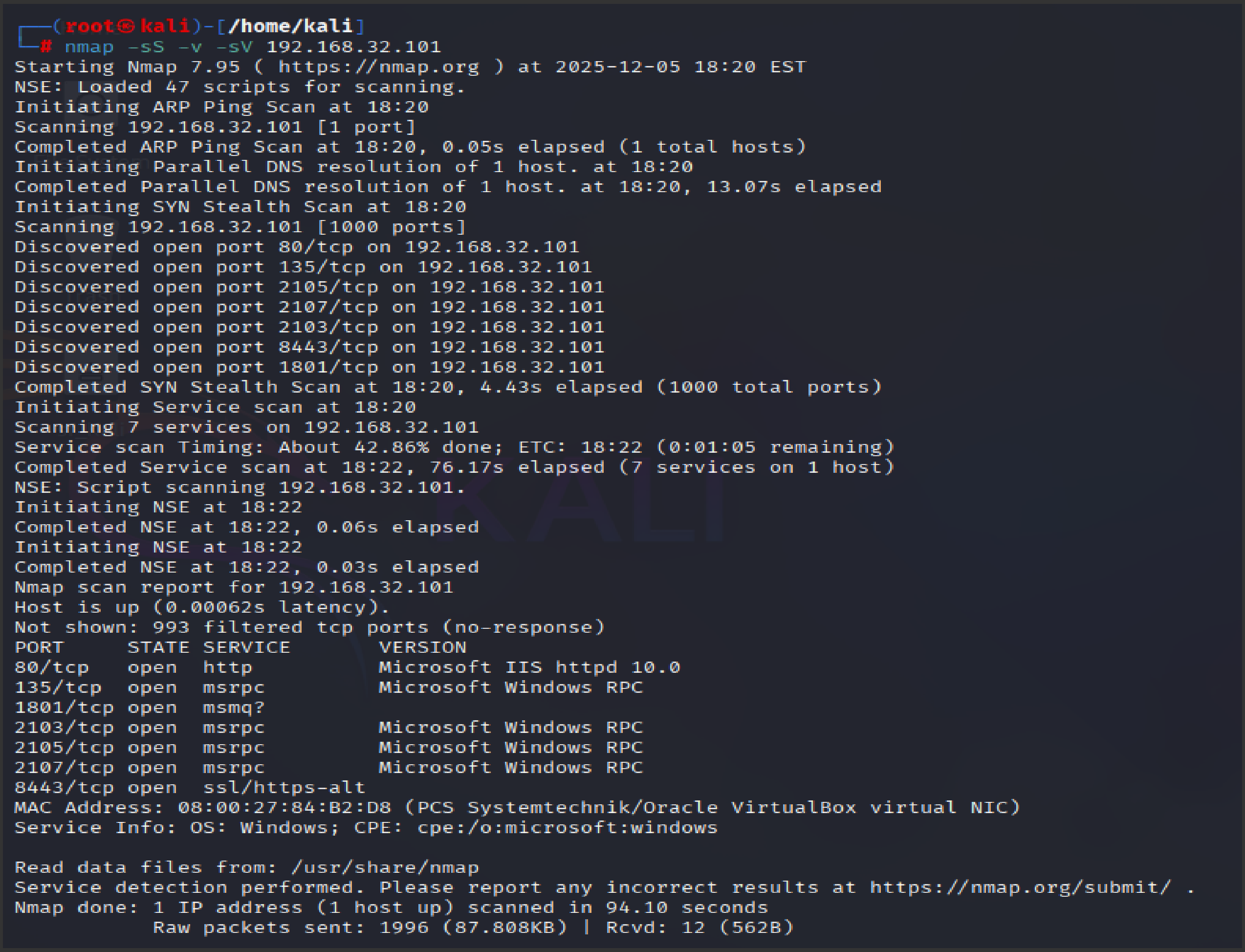


```
13/tcp   open  daytime       Microsoft Windows International daytime
17/tcp   open  qotd          Windows qotd (English)
19/tcp   open  chargen
80/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
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
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5432/tcp open  postgresql?
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:84:B2:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 172.01 seconds
           Raw packets sent: 1075 (47.284KB) | Rcvd: 1001 (40.100KB)
```

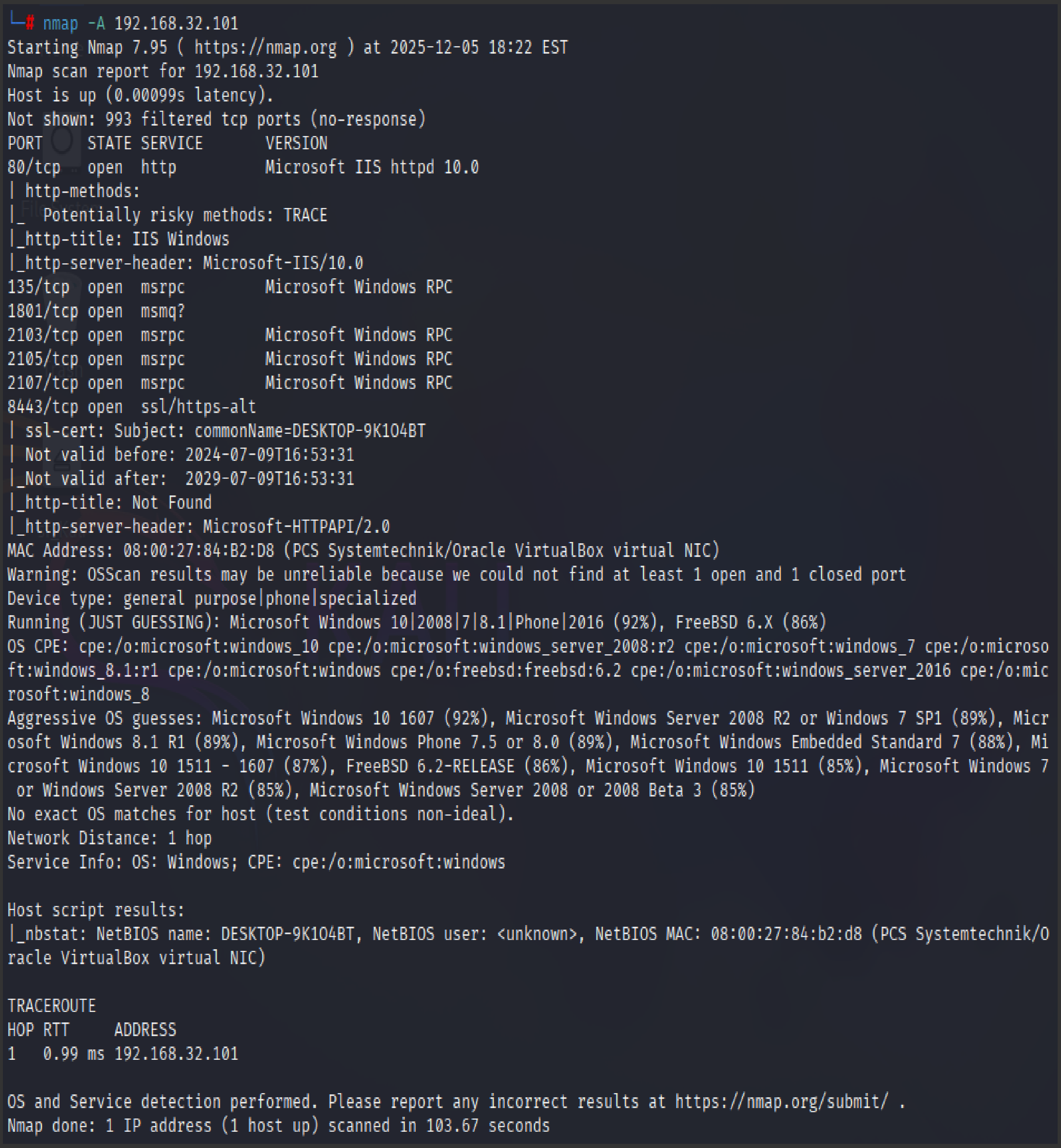
Con il Firewall attivato invece si possono notare meno servizi esposti.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.32.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 18:19 EST
Nmap scan report for 192.168.32.101
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: 08:00:27:84:B2:D8 (PCS Systemtechnik/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|phone|specialized
Running (JUST GUESSING): Microsoft Windows 10|2008|7|8.1|Phone|2016 (92%), FreeBSD 6.X (86%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microso
ft:windows_8.1:r1 cpe:/o:microsoft:windows cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_server_2016 cpe:/o:mic
rosoft:windows_8
Aggressive OS guesses: Microsoft Windows 10 1607 (92%), Microsoft Windows Server 2008 R2 or Windows 7 SP1 (89%), Micr
osoft Windows 8.1 R1 (89%), Microsoft Windows Phone 7.5 or 8.0 (89%), Microsoft Windows Embedded Standard 7 (88%), Mi
crosoft Windows 10 1511 - 1607 (87%), FreeBSD 6.2-RELEASE (86%), Microsoft Windows 10 1511 (85%), Microsoft Windows 7
 or Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 or 2008 Beta 3 (85%)
No exact OS matches for host (test conditions non-ideal).
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 22.47 seconds
```



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -v -sV 192.168.32.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 18:20 EST
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 18:20
Scanning 192.168.32.101 [1 port]
Completed ARP Ping Scan at 18:20, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:20
Completed Parallel DNS resolution of 1 host. at 18:20, 13.07s elapsed
Initiating SYN Stealth Scan at 18:20
Scanning 192.168.32.101 [1000 ports]
Discovered open port 80/tcp on 192.168.32.101
Discovered open port 135/tcp on 192.168.32.101
Discovered open port 2105/tcp on 192.168.32.101
Discovered open port 2107/tcp on 192.168.32.101
Discovered open port 2103/tcp on 192.168.32.101
Discovered open port 8443/tcp on 192.168.32.101
Discovered open port 1801/tcp on 192.168.32.101
Completed SYN Stealth Scan at 18:20, 4.43s elapsed (1000 total ports)
Initiating Service scan at 18:20
Scanning 7 services on 192.168.32.101
Service scan Timing: About 42.86% done; ETC: 18:22 (0:01:05 remaining)
Completed Service scan at 18:22, 76.17s elapsed (7 services on 1 host)
NSE: Script scanning 192.168.32.101.
Initiating NSE at 18:22
Completed NSE at 18:22, 0.06s elapsed
Initiating NSE at 18:22
Completed NSE at 18:22, 0.03s elapsed
Nmap scan report for 192.168.32.101
Host is up (0.00062s 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: 08:00:27:84:B2:D8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 94.10 seconds
           Raw packets sent: 1996 (87.808KB) | Rcvd: 12 (562B)
```



```
└─# nmap -A 192.168.32.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 18:22 EST
Nmap scan report for 192.168.32.101
Host is up (0.00099s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows
|_http-server-header: Microsoft-IIS/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
| ssl-cert: Subject: commonName=DESKTOP-9K1O4BT
| Not valid before: 2024-07-09T16:53:31
|_Not valid after:  2029-07-09T16:53:31
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 08:00:27:84:B2:D8 (PCS Systemtechnik/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|phone|specialized
Running (JUST GUESSING): Microsoft Windows 10|2008|7|8.1|Phone|2016 (92%), FreeBSD 6.X (86%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microso
ft:windows_8.1:r1 cpe:/o:microsoft:windows cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_server_2016 cpe:/o:mic
rosoft:windows_8
Aggressive OS guesses: Microsoft Windows 10 1607 (92%), Microsoft Windows Server 2008 R2 or Windows 7 SP1 (89%), Micr
osoft Windows 8.1 R1 (89%), Microsoft Windows Phone 7.5 or 8.0 (89%), Microsoft Windows Embedded Standard 7 (88%), Mi
crosoft Windows 10 1511 - 1607 (87%), FreeBSD 6.2-RELEASE (86%), Microsoft Windows 10 1511 (85%), Microsoft Windows 7
 or Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 or 2008 Beta 3 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: DESKTOP-9K1O4BT, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:84:b2:d8 (PCS Systemtechnik/O
racle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT     ADDRESS
1   0.99 ms 192.168.32.101

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 103.67 seconds
```