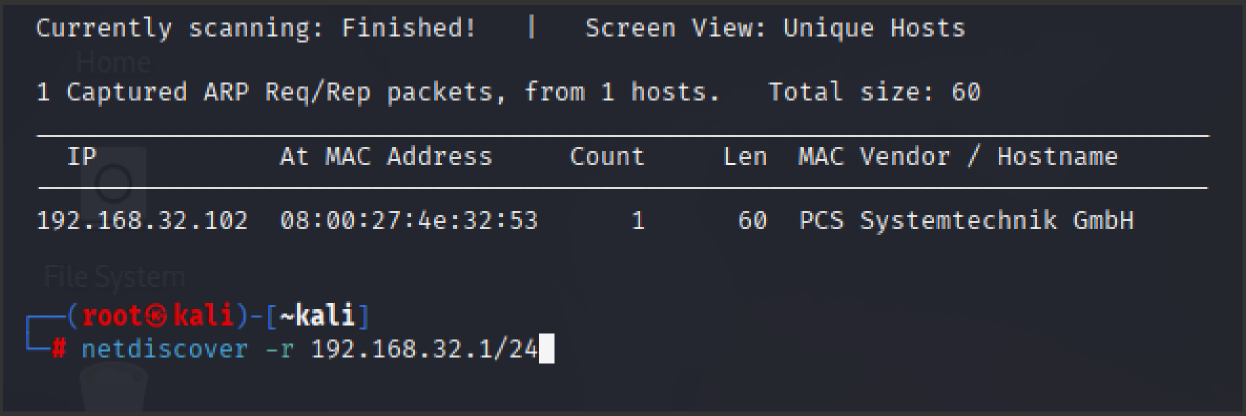
Con Netdiscover -r, o in alternativa con Nmap -sn -PE, si andranno a mostrare gli host attivi in un determinato range.

Ip attivo trovato: 192.168.32.102 (Ip Meta)

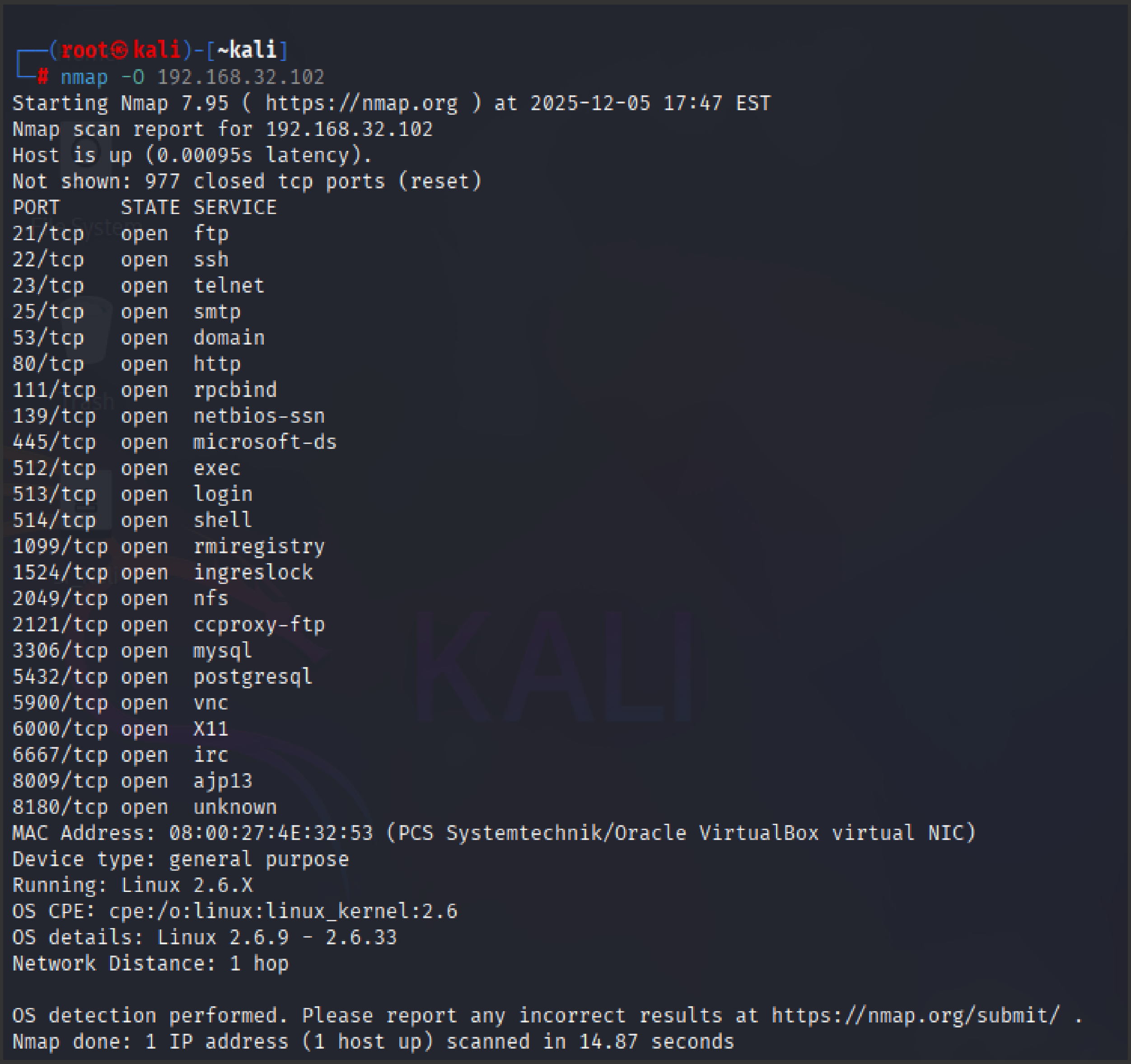


```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.32.102  08:00:27:4e:32:53      1      60  PCS Systemtechnik GmbH

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

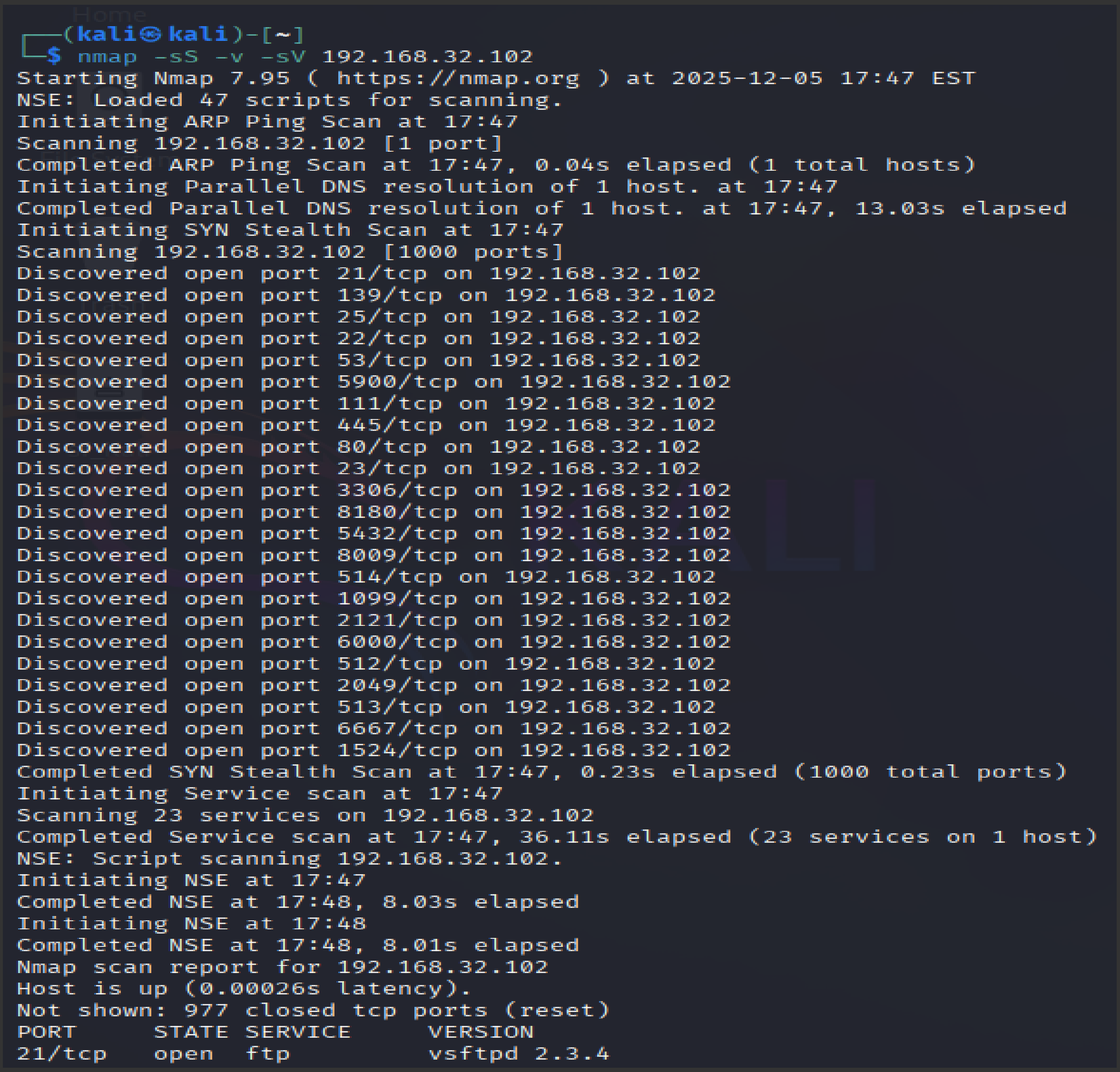
Con Nmap -O si visualizzano le porte aperte, e la versione del Sistema Operativo.



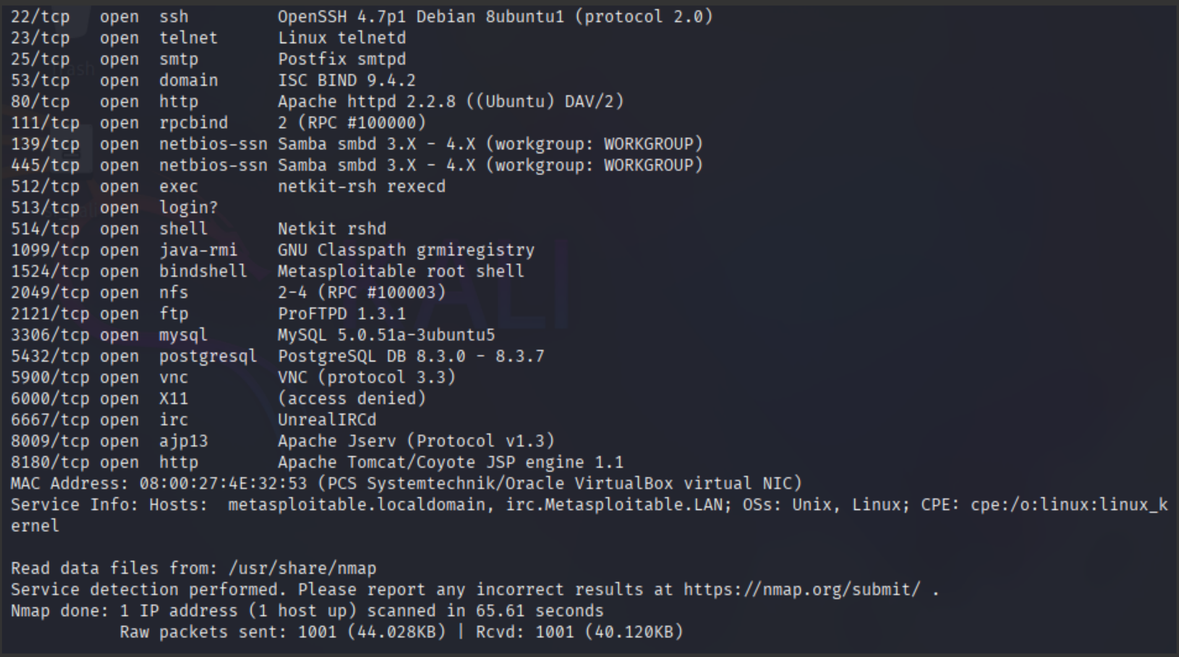
```
┌──(root㉿kali)-[~kali]
└─# nmap -O 192.168.32.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 17:47 EST
Nmap scan report for 192.168.32.102
Host is up (0.00095s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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: 08:00:27:4E:32:53 (PCS Systemtechnik/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 14.87 seconds
```

Con il Syn Scan tramite Nmap -sS -v -sV si visualizzeranno i servizi attivi, e le loro versioni.
In alternativa, con Nmap -A sarebbe possibile eseguire una scansione più dettagliata in cui sono comprese più informazioni contemporaneamente.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -v -sV 192.168.32.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 17:47 EST
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 17:47
Scanning 192.168.32.102 [1 port]
Completed ARP Ping Scan at 17:47, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:47
Completed Parallel DNS resolution of 1 host. at 17:47, 13.03s elapsed
Initiating SYN Stealth Scan at 17:47
Scanning 192.168.32.102 [1000 ports]
Discovered open port 21/tcp on 192.168.32.102
Discovered open port 139/tcp on 192.168.32.102
Discovered open port 25/tcp on 192.168.32.102
Discovered open port 22/tcp on 192.168.32.102
Discovered open port 53/tcp on 192.168.32.102
Discovered open port 5900/tcp on 192.168.32.102
Discovered open port 111/tcp on 192.168.32.102
Discovered open port 445/tcp on 192.168.32.102
Discovered open port 80/tcp on 192.168.32.102
Discovered open port 23/tcp on 192.168.32.102
Discovered open port 3306/tcp on 192.168.32.102
Discovered open port 8180/tcp on 192.168.32.102
Discovered open port 5432/tcp on 192.168.32.102
Discovered open port 8009/tcp on 192.168.32.102
Discovered open port 514/tcp on 192.168.32.102
Discovered open port 1099/tcp on 192.168.32.102
Discovered open port 2121/tcp on 192.168.32.102
Discovered open port 6000/tcp on 192.168.32.102
Discovered open port 512/tcp on 192.168.32.102
Discovered open port 2049/tcp on 192.168.32.102
Discovered open port 513/tcp on 192.168.32.102
Discovered open port 6667/tcp on 192.168.32.102
Discovered open port 1524/tcp on 192.168.32.102
Completed SYN Stealth Scan at 17:47, 0.23s elapsed (1000 total ports)
Initiating Service scan at 17:47
Scanning 23 services on 192.168.32.102
Completed Service scan at 17:47, 36.11s elapsed (23 services on 1 host)
NSE: Script scanning 192.168.32.102.
Initiating NSE at 17:47
Completed NSE at 17:48, 8.03s elapsed
Initiating NSE at 17:48
Completed NSE at 17:48, 8.01s elapsed
Nmap scan report for 192.168.32.102
Host is up (0.00026s 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?
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: 08:00:27:4E:32:53 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_k
ernel

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 65.61 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
```