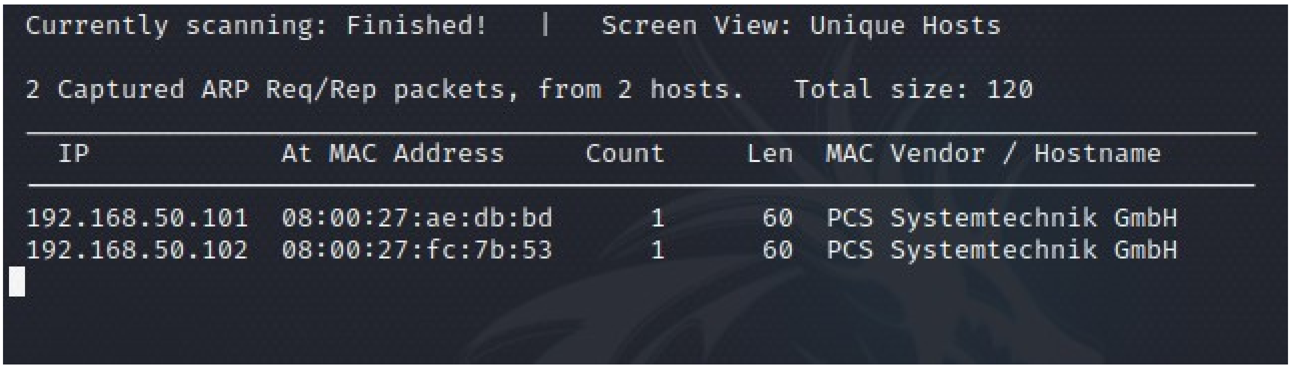
Nmap

Tools: Nmap, Netdiscover

Obbiettivi:
- Target: Metasploitable
  Scansionare:
  1) OS fingerprint,
  2) Syn Scan,
  3) TCP connect,
  4) Version detection.
- Target: Windows 7
  Scansionare: OS fingerprint

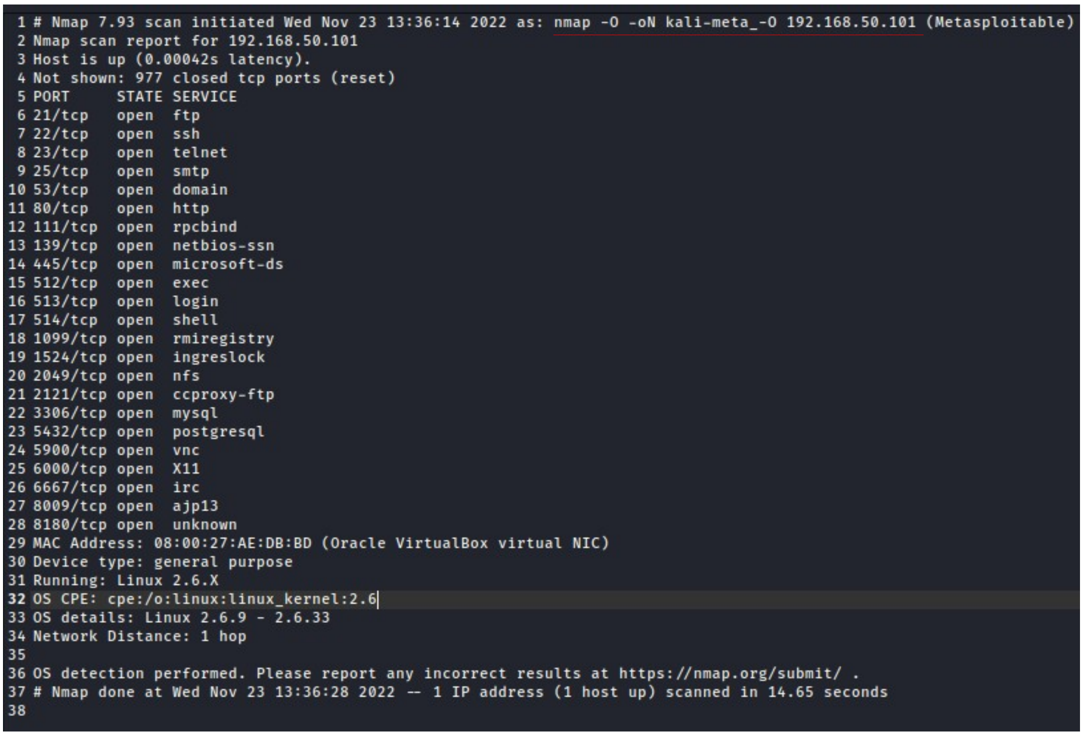
Per trovare i dispositivi sulla rete usiamo Netdiscover
con il comando: “netdiscover -r 192.168.50.0/24”



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

 2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 120
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.50.101  08:00:27:ae:db:bd      1      60  PCS Systemtechnik GmbH
 192.168.50.102  08:00:27:fc:7b:53      1      60  PCS Systemtechnik GmbH
```

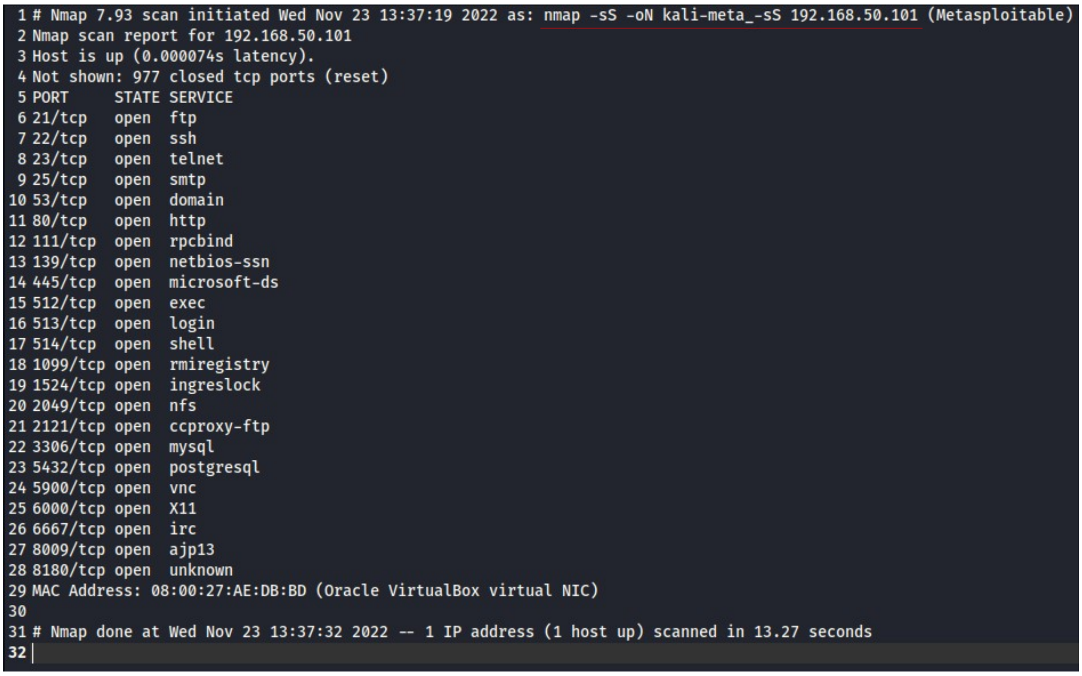
Abbiamo scoperto 2 dispositivi collegati nella nostra rete, una di queste è Metasploitable e l’altra è Windows 7, per identificarle useremo nmap.

Target: Metasploitable; Scan type: Operating System fingerprint;
comando utilizzato per effettuare la scansione: “nmap -O <metasploitable_ip>”
informazioni scoperte: Port, Services, MAC address, Operating System version e Network Distance
tempo impiegato per la scansione: 14.65 secondi.



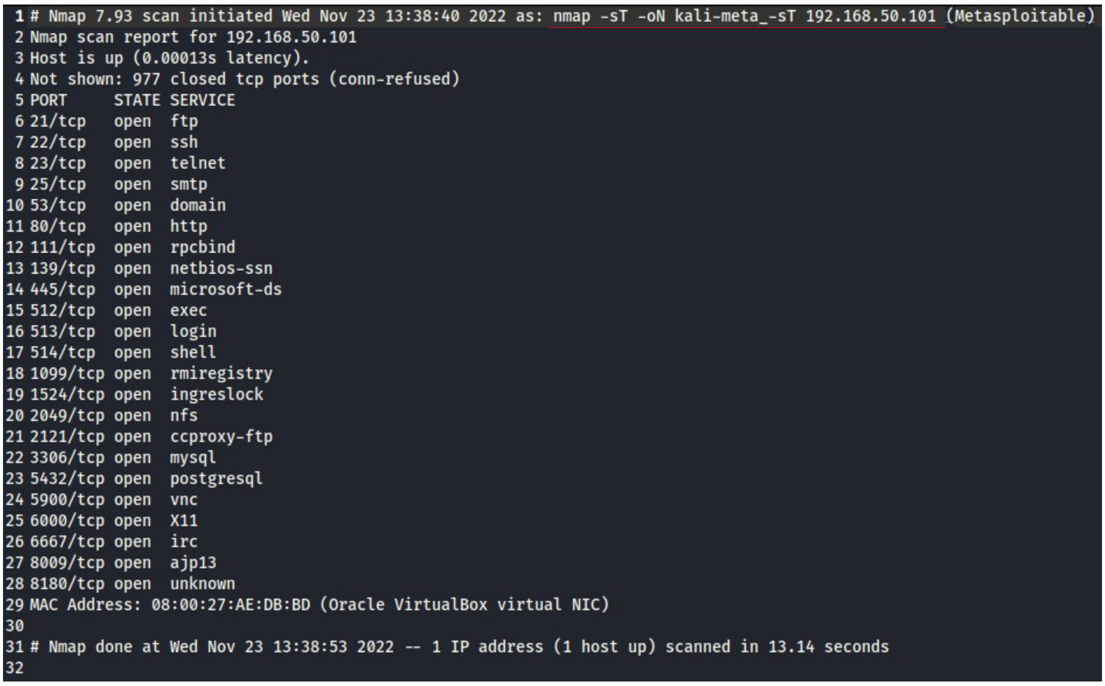
```
# Nmap 7.93 scan initiated Wed Nov 23 13:36:14 2022 as: nmap -O -oN kali-meta_-O 192.168.50.101 (Metasploitable)
Nmap scan report for 192.168.50.101
Host is up (0.00042s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
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:AE:DB:BD (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 at Wed Nov 23 13:36:28 2022 -- 1 IP address (1 host up) scanned in 14.65 seconds
```

Target: Metasploitable; Scan type: SynScan;
comando usato per la scansione: “nmap -sS <metasploitable_ip>”
info scoperte: Ports, Services, MAC address
tempo impiegato per la scansione: 13.27 secondi.



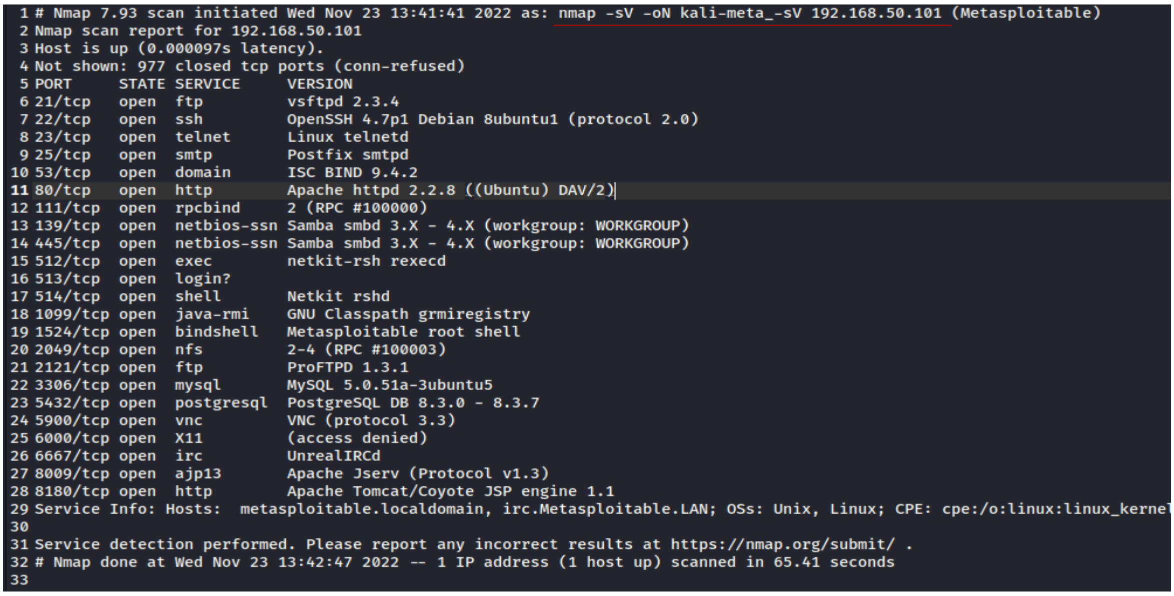
```
# Nmap 7.93 scan initiated Wed Nov 23 13:37:19 2022 as: nmap -sS -oN kali-meta_-sS 192.168.50.101 (Metasploitable)
Nmap scan report for 192.168.50.101
Host is up (0.000074s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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:AE:DB:BD (Oracle VirtualBox virtual NIC)

# Nmap done at Wed Nov 23 13:37:32 2022 -- 1 IP address (1 host up) scanned in 13.27 seconds
```

Target: Metasploitable; Scan type: TCP connect;
comando usato per la scansione: “nmap -sT <metasploitable_ip>”
info scoperte: Ports, Services, MAC address
tempo: 13.14 secondi



```
# Nmap 7.93 scan initiated Wed Nov 23 13:38:40 2022 as: nmap -sT -oN kali-meta_-sT 192.168.50.101 (Metasploitable)
Nmap scan report for 192.168.50.101
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (conn-refused)
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:AE:DB:BD (Oracle VirtualBox virtual NIC)

# Nmap done at Wed Nov 23 13:38:53 2022 -- 1 IP address (1 host up) scanned in 13.14 seconds

```

Target: Metasploitable; Scan type: Version Detection;
comando usato per la scansione: “nmap -sV <metasploitable_ip>”
info scoperte: Ports, Services, Service Versions, Host Service Info, OS
tempo: 65.41 secondi

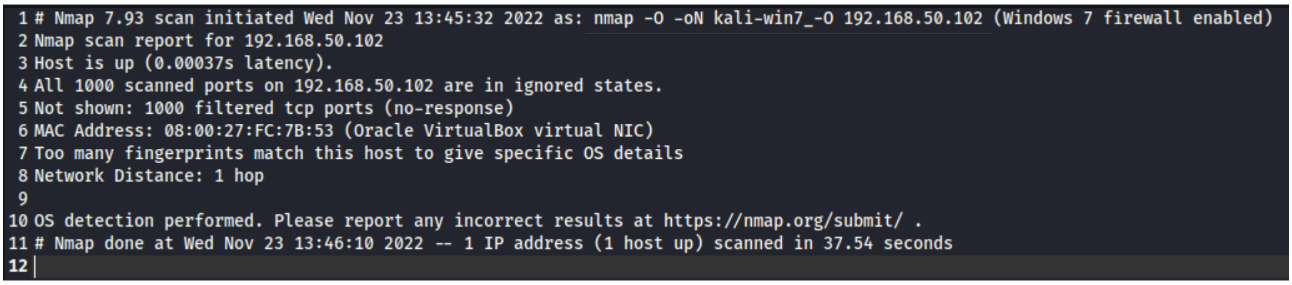


```
# Nmap 7.93 scan initiated Wed Nov 23 13:41:41 2022 as: nmap -sV -oN kali-meta_-sV 192.168.50.101 (Metasploitable)
Nmap scan report for 192.168.50.101
Host is up (0.000097s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Nov 23 13:42:47 2022 -- 1 IP address (1 host up) scanned in 65.41 seconds

```

Target	Scan Type	tempo	ports	services	Service Versions	MAC	OS	OS Version
192.168.50.101	-O	14.65	23	22	/	si	si	si
192.168.50.101	-sS	13.27	23	22	/	si	/	/
192.168.50.101	-sT	13.14	23	22	/	si	/	/
192.168.50.101	-sV	65.41	23	23	22	/	si	/

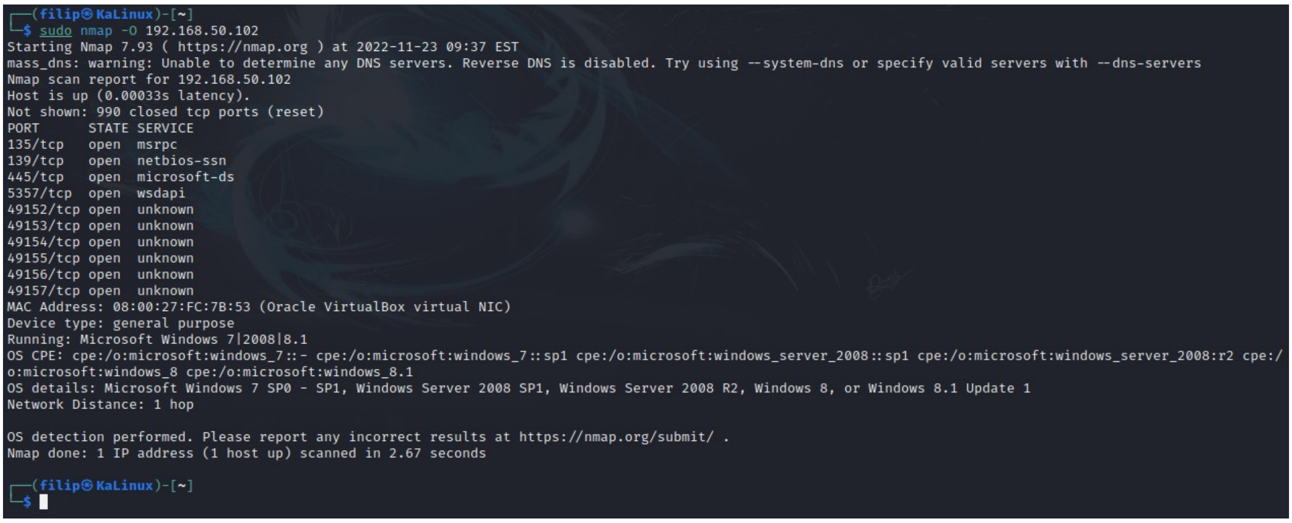
Target: Windows 7; Scan type: OS fingerprint;
comando usato per la scansione: “nmap -O <windows7_ip>”
info scoperte: MAC address, Network Distance
tempo: 37.54

Win7 firewall abilitato:
tutti 1000 port di default (piu usati) sono filtrati



```
# Nmap 7.93 scan initiated Wed Nov 23 13:45:32 2022 as: nmap -O -oN kali-win7_-O 192.168.50.102 (Windows 7 firewall enabled)
Nmap scan report for 192.168.50.102
Host is up (0.00037s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:FC:7B:53 (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 at Wed Nov 23 13:46:10 2022 -- 1 IP address (1 host up) scanned in 37.54 seconds

```

Win7 firewall disabilitato:
info scoperte: Ports, Services, MAC address, OS, OS version, Netword Distance
tempo: 2.67

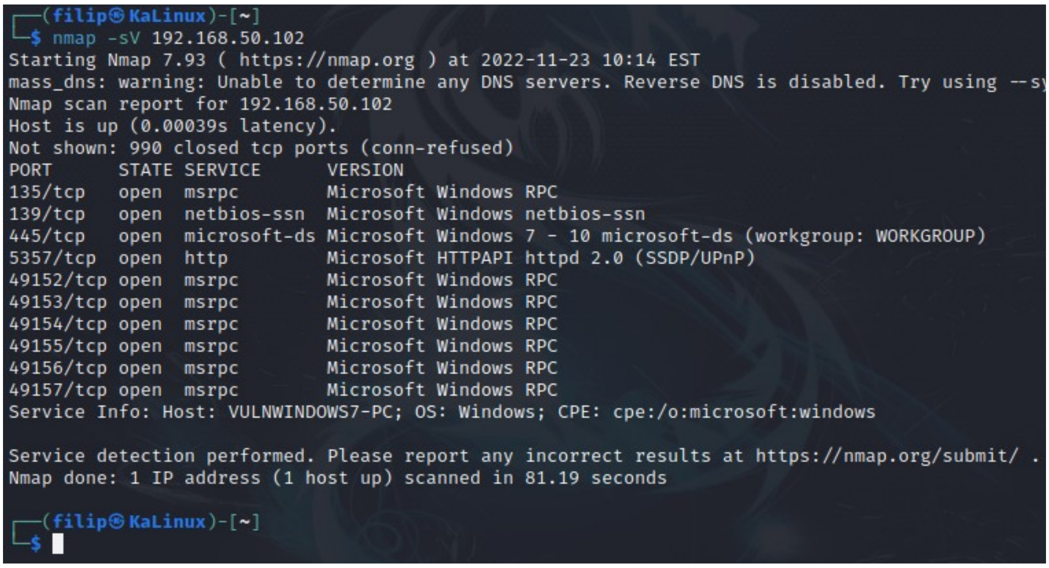


```
┌──(filip㉿KaLinux)-[~]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 09:37 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.00033s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
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:FC:7B:53 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.67 seconds

┌──(filip㉿KaLinux)-[~]
└─$ 
```

Target	Firewall	Scan Type	Tempo	Ports	Services	Service Version	MAC	OS	OS Version
192.168.50.102	si	-O	37.54	/	/	/	si	/	/
192.168.50.102	no	-O	2.67	10	si	/	si	si	si
192.168.50.102	no	-sV	81.19	10	si	si	/	/	/

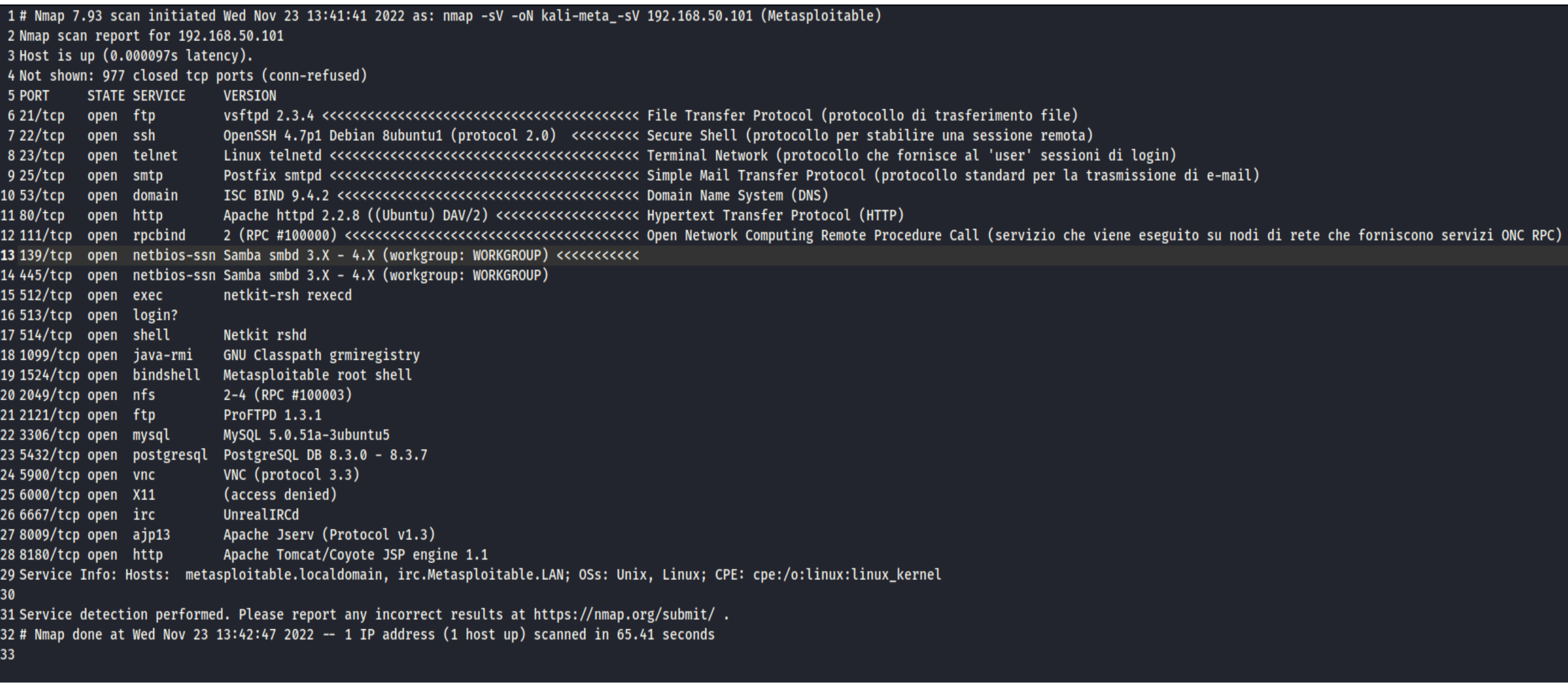
VM	IP	OS	Porte Aperte	Servizi in ascolto & versione
Kali	192.168.50.100	Linux Debian	/	/
Meta.	192.168.50.101	Linux Kernel	23	22
Win7	192.168.50.102	Microsoft Win7	10	10

Win7 = Version scan con nmap:



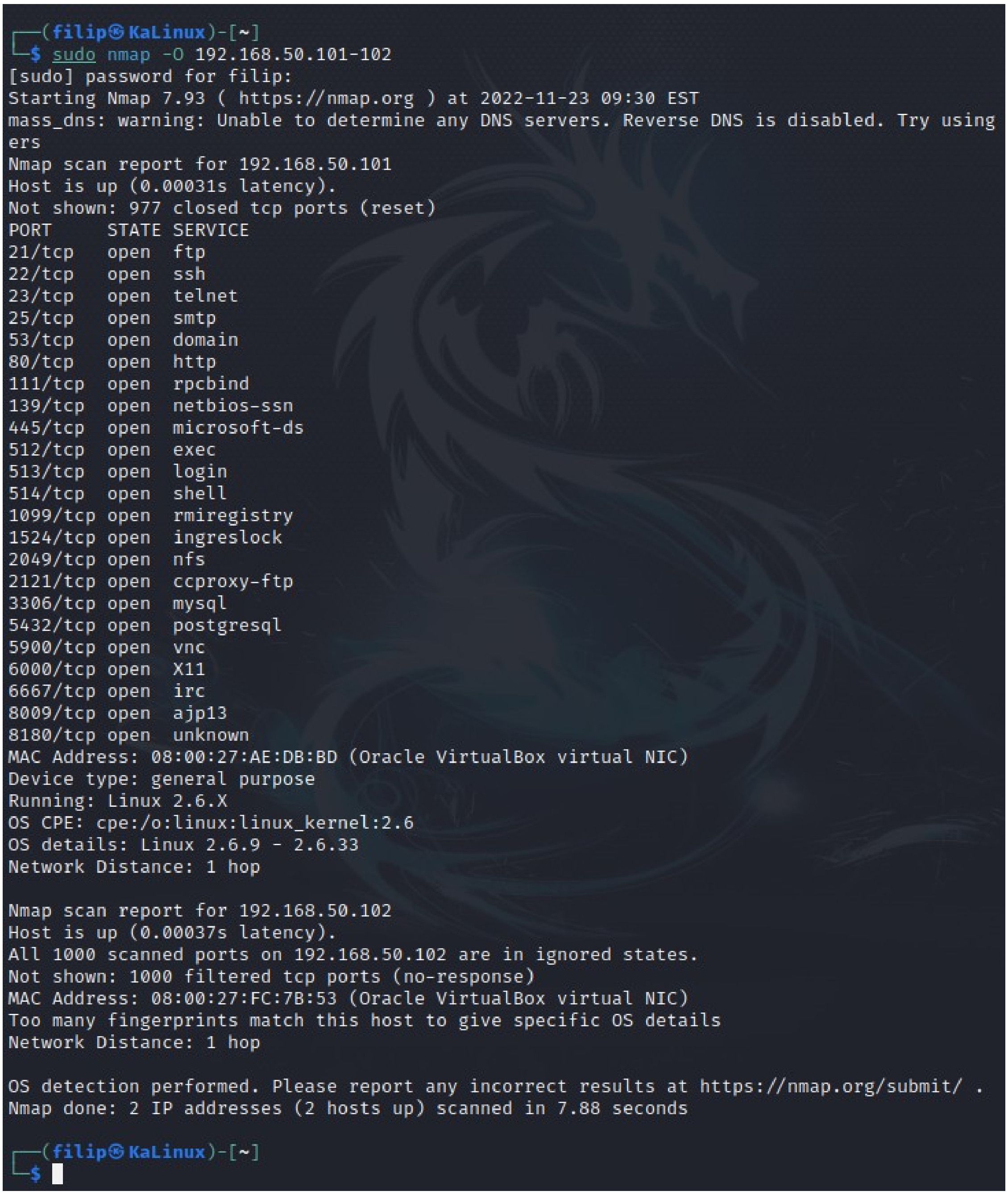
```
┌──(filip㉿KaLinux)-[~]
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 10:14 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --sy
Nmap scan report for 192.168.50.102
Host is up (0.00039s latency).
Not shown: 990 closed tcp ports (conn-refused)
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 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
Service Info: Host: VULNWINDOWS7-PC; 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 81.19 seconds

┌──(filip㉿KaLinux)-[~]
└─$ 
```

Descrizione dei servizi



```
# Nmap 7.93 scan initiated Wed Nov 23 13:41:41 2022 as: nmap -sV -oN kali-meta_-sV 192.168.50.101 (Metasploitable)
Nmap scan report for 192.168.50.101
Host is up (0.000097s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4 <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< File Transfer Protocol (protocollo di trasferimento file)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  <<<<<<<<< Secure Shell (protocollo per stabilire una sessione remota)
23/tcp   open  telnet      Linux telnetd <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< Terminal Network (protocollo che fornisce al 'user' sessioni di login)
25/tcp   open  smtp        Postfix smtpd <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< Simple Mail Transfer Protocol (protocollo standard per la trasmissione di e-mail)
53/tcp   open  domain      ISC BIND 9.4.2 <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< Domain Name System (DNS)
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2) <<<<<<<<<<<<<<<<<<< Hypertext Transfer Protocol (HTTP)
111/tcp  open  rpcbind     2 (RPC #100000) <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< Open Network Computing Remote Procedure Call (servizio che viene eseguito su nodi di rete che forniscono servizi ONC RPC)
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Nov 23 13:42:47 2022 -- 1 IP address (1 host up) scanned in 65.41 seconds

```

Extra: visto che abbiamo usato lo stesso comando per Meta e Win7, potevamo fare 1 comando per entrambe le macchine



```
┌──(filip㉿KaLinux)-[~]
└─$ sudo nmap -O 192.168.50.101-102
[sudo] password for filip:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 09:30 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
ers
Nmap scan report for 192.168.50.101
Host is up (0.00031s 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:AE:DB:BD (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

Nmap scan report for 192.168.50.102
Host is up (0.00037s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:FC:7B:53 (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: 2 IP addresses (2 hosts up) scanned in 7.88 seconds

┌──(filip㉿KaLinux)-[~]
└─$ 
```