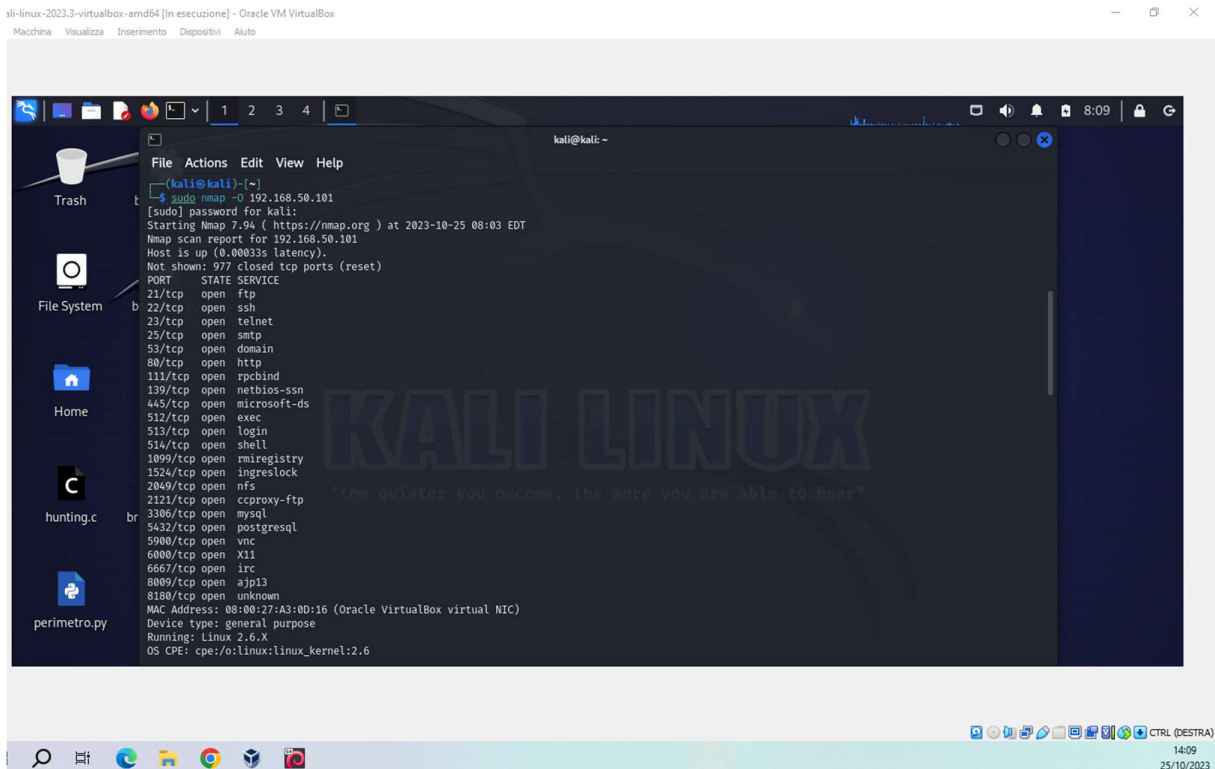


NMAP

L'esercizio di oggi prevedeva di familiarizzare con alcune tecniche di scansione di Nmap.

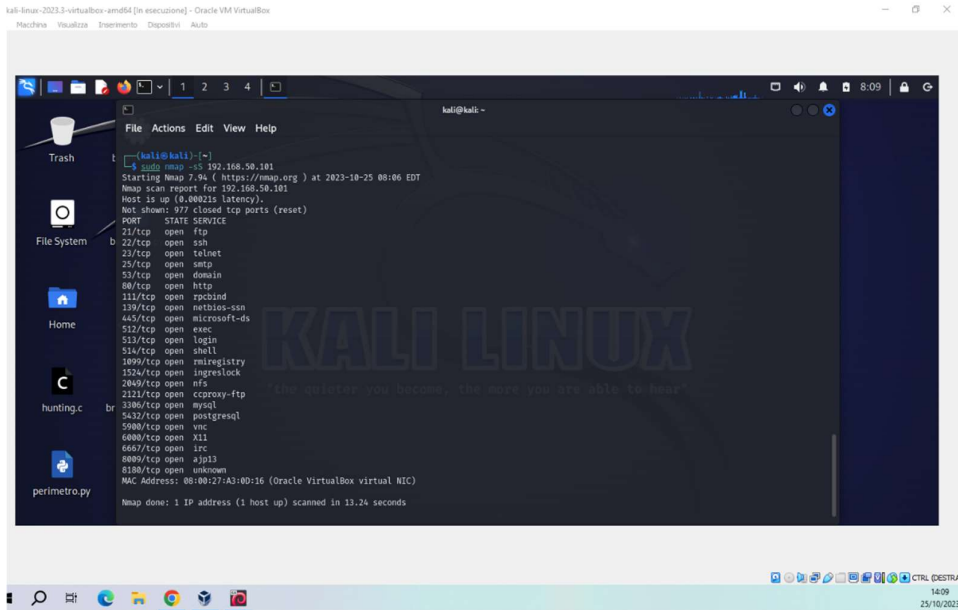
Ho eseguito le scansioni su Metasploitable (IP: 192.168.50.101) e Windows7 (IP: 192.168.50.103).

Con il comando `nmap -O` ho visto il sistema operativo di Metasploitable, ovvero Linux.



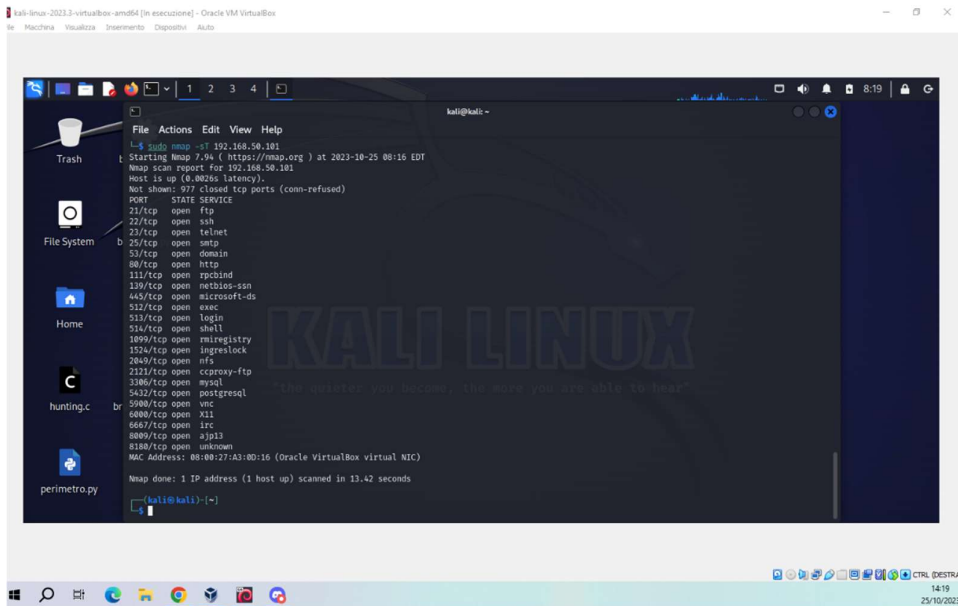
```
File Actions Edit View Help
kali@kali:~$ sudo nmap -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 08:03 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0003s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    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:A3:00:16 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

Con il comando `nmap -sS` e `-sT` ho fatto la scansione delle porte aperte. La differenza tra i due comandi è che il primo è meno attendibile e meno invasivo perché una volta che riceve il pacchetto SYN/ACK dalla macchina target, non conclude il “3-way-handshake”, ma chiude la comunicazione; però riesce lo stesso a recuperare informazioni riguardanti le porte. `-sT` invece completa il “3-way-handshake” ed è molto più invasivo.



```
kali@kali:~$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 08:06 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0021s 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
1899/tcp  open  mircregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6880/tcp  open  x11
6667/tcp  open  irc
8889/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:A3:0D:16 (Oracle VirtualBox virtual NIC)

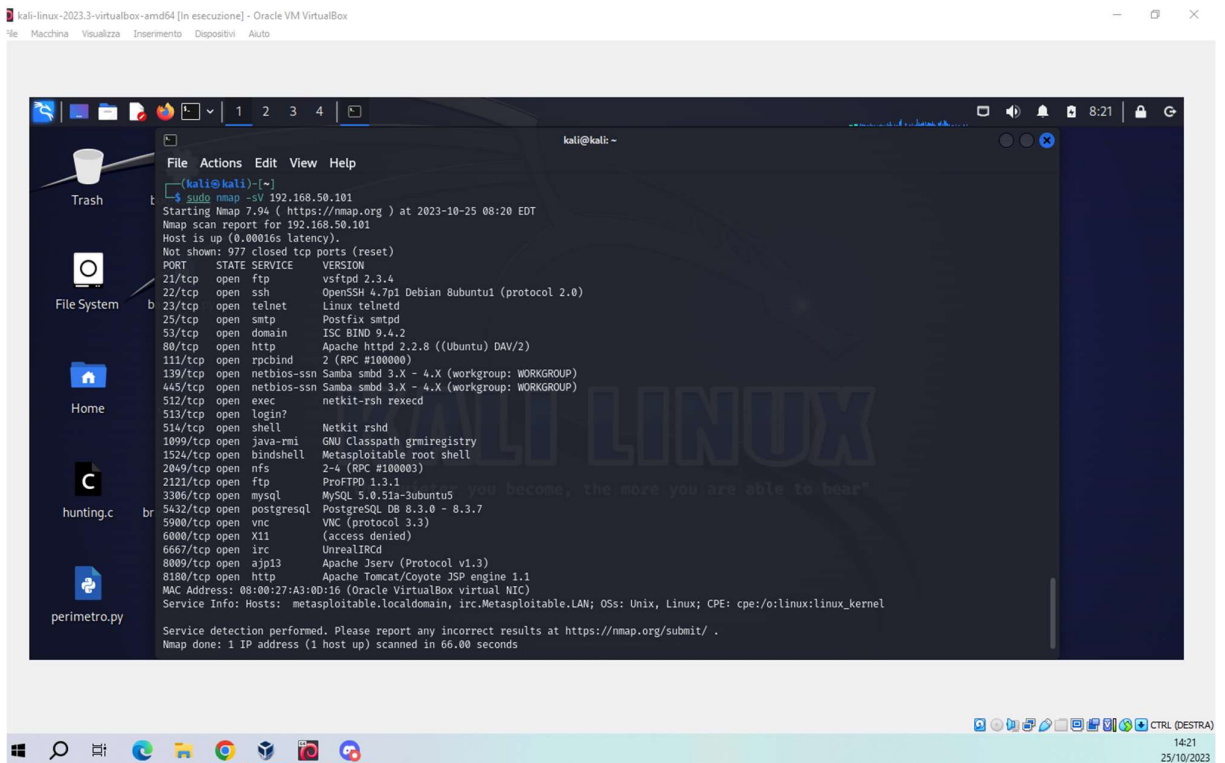
Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
```



```
kali@kali:~$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 08:16 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0026s 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
1899/tcp  open  mircregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6880/tcp  open  x11
6667/tcp  open  irc
8889/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:A3:0D:16 (Oracle VirtualBox virtual NIC)

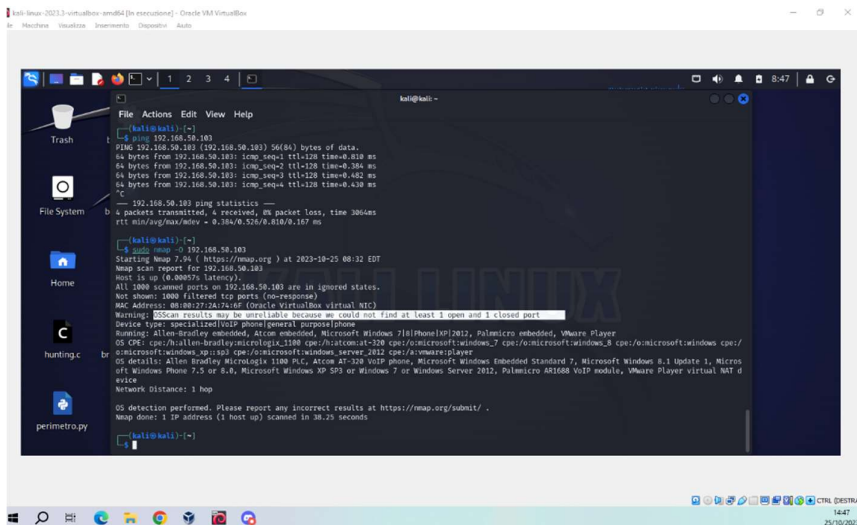
Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds
```

Con il comando nmap -sV ho fatto la scansione dei servizi in ascolto con la loro versione.



```
kali@kali: ~  
File Actions Edit View Help  
t (kali@kali)~  
t $ nmap -sV 192.168.50.101  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 08:20 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.00016s 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 gmicregistry  
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  
8080/tcp  open  ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
MAC Address: 08:00:27:A3:0D:16 (Oracle VirtualBox virtual NIC)  
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: 1 IP address (1 host up) scanned in 66.00 seconds
```

Sul secondo IP invece ho utilizzato lo stesso comando per vedere il sistema operativo. Il comando ha dato come output che c'è un sistema windows sull'IP, ma non abbiamo delle informazioni precise perché c'è un firewall. Per poterlo aggirare si potrebbe usare il comando -T1 così che gli scan sono parecchio lenti e poco invasivi e quindi diminuisce la probabilità di essere intercettati. Con -T1 però ci vorrebbe troppo tempo per effettuare la scansione.



```
kali@kali: ~  
File Actions Edit View Help  
t (kali@kali)~  
t $ nmap -sV 192.168.50.102  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 08:32 EDT  
Nmap scan report for 192.168.50.102  
Host is up (0.00057s 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:A3:0D:16 (Oracle VirtualBox virtual NIC)  
Warning: 00:00:27:A3:0D:16 (Oracle VirtualBox virtual NIC) could not find at least 3 open and 3 closed ports  
Device type: Specialized (VLAN) phone (general purpose) phone  
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7 (Phone) XP2012, PalmSecure embedded, VMware Player  
OS CPE: cpe:/o:allen-bradley:embedded, cpe:/o:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_xp  
OS details: Allen Bradley Micrologix 1500 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, PalmSecure AR1688 VoIP module, VMware Player virtual NAT 4  
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 38.25 seconds
```