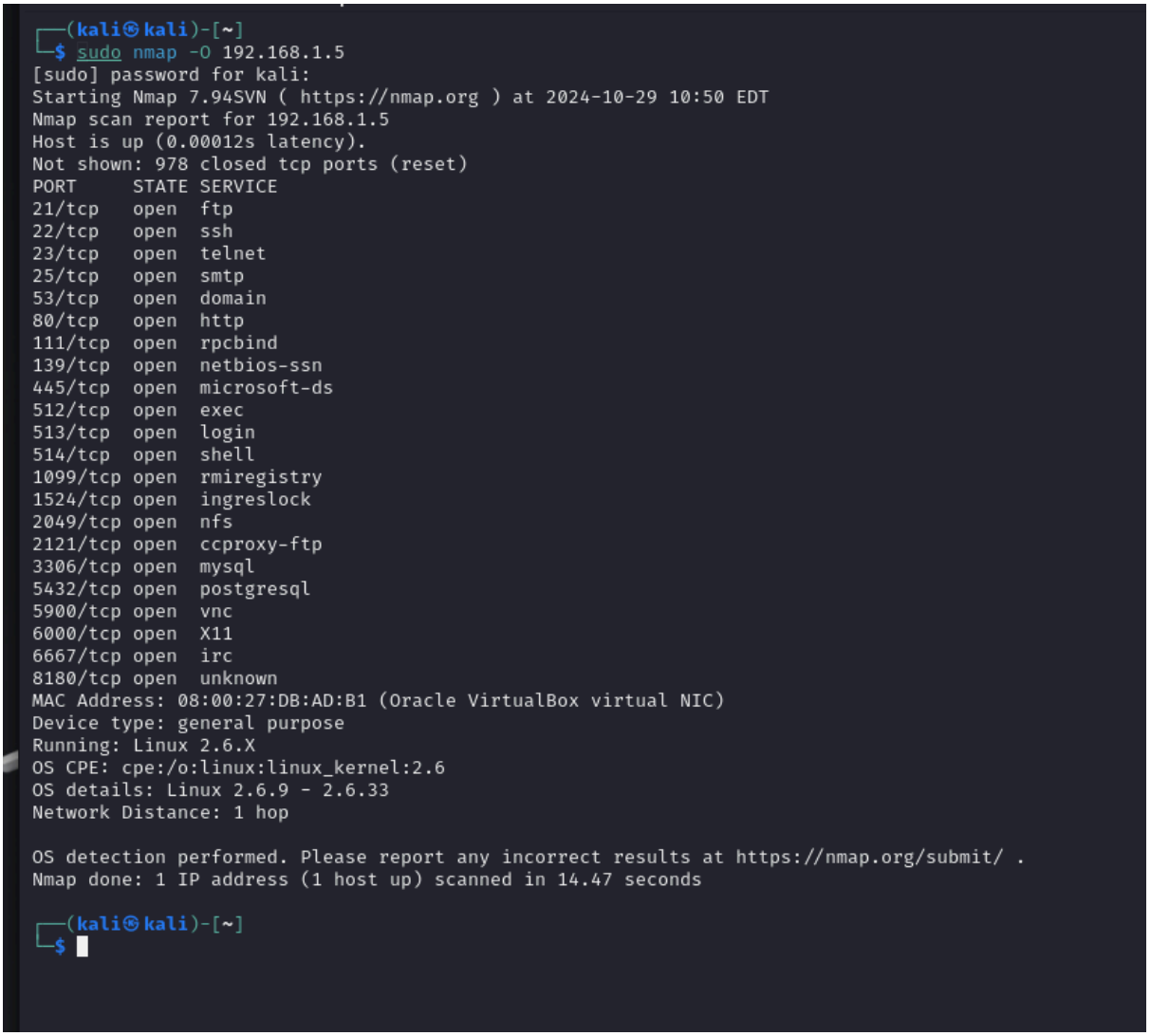
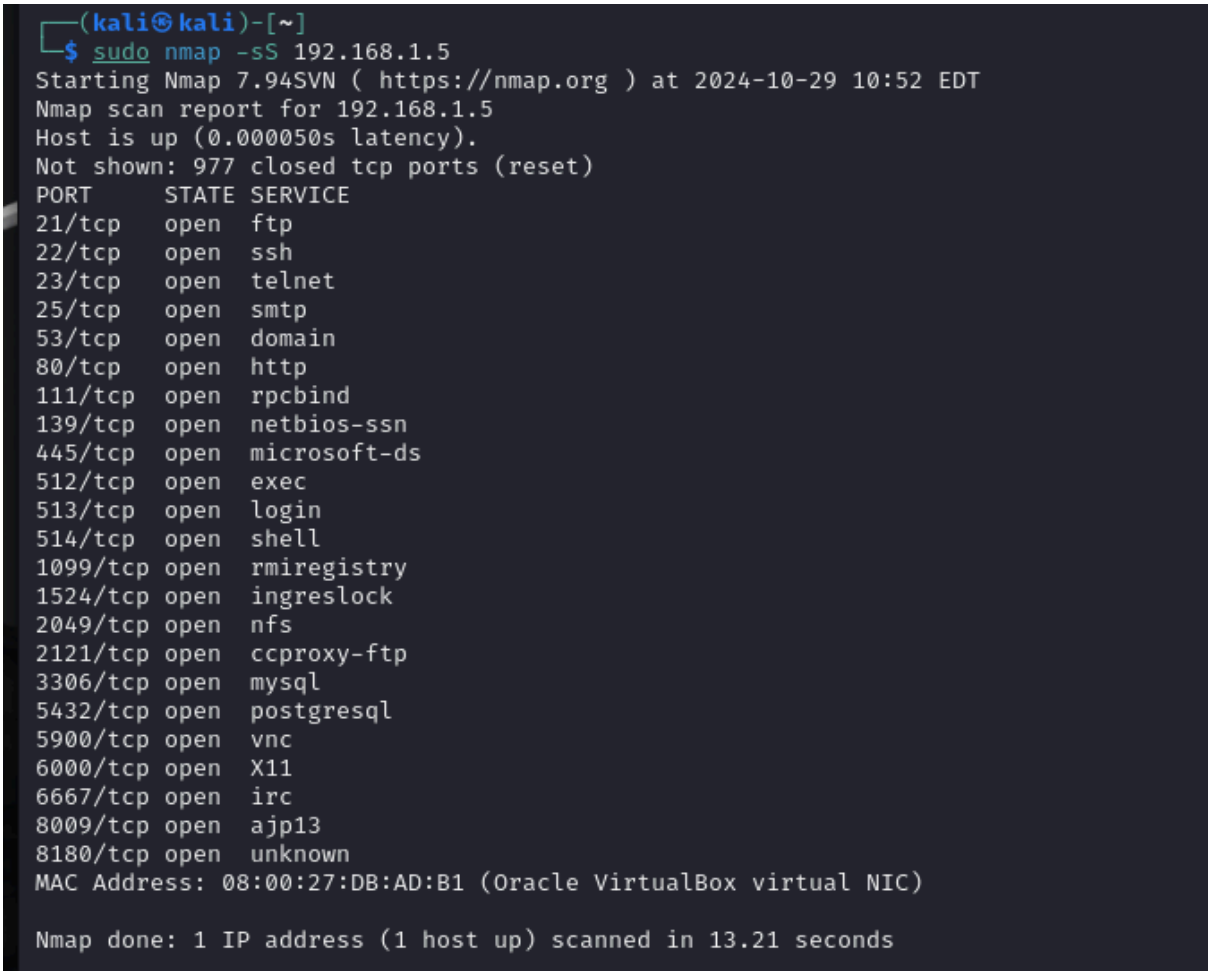
Esercizio S5L2 - Nmap e raccolta informazioni

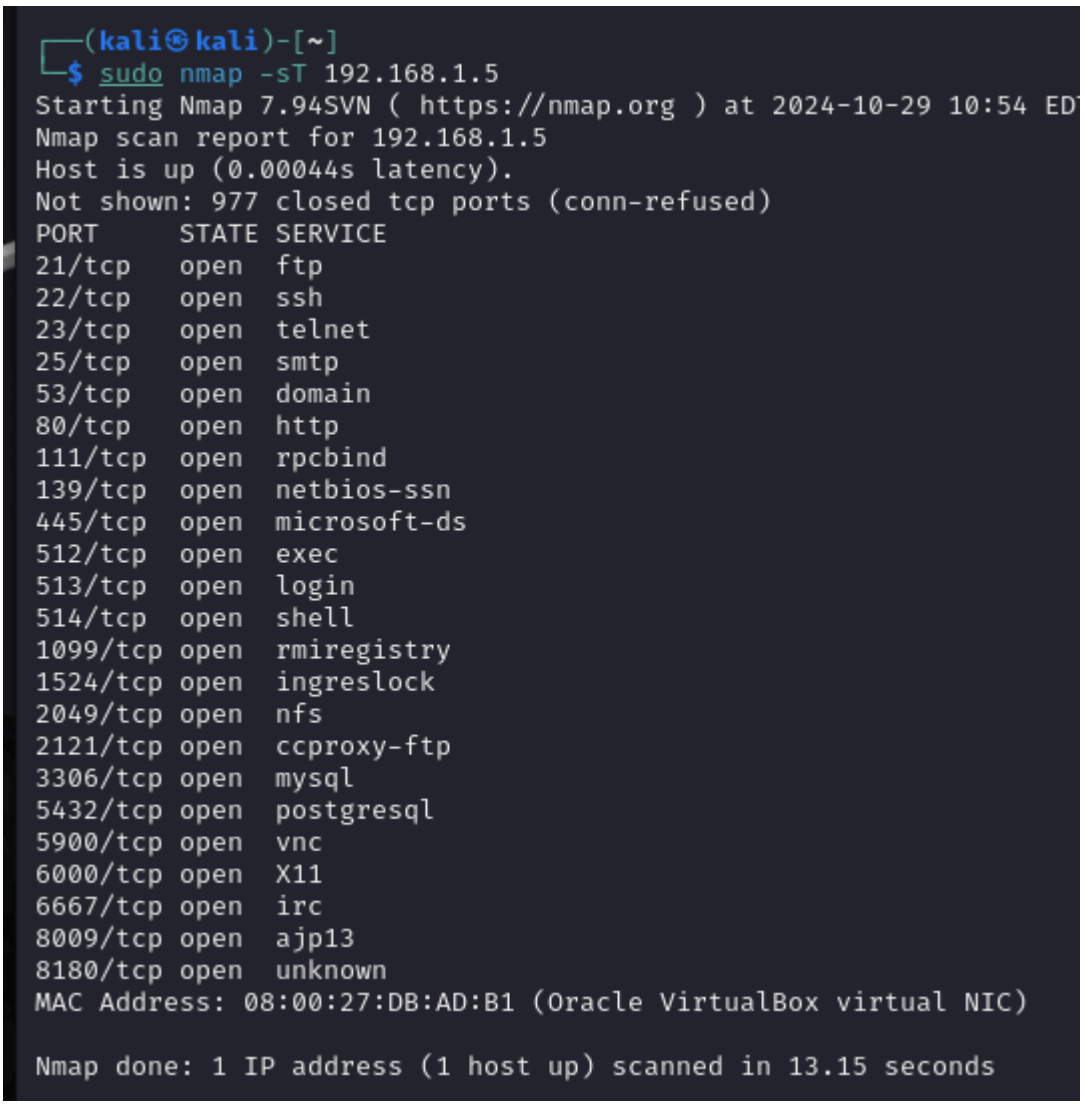
L'esercizio di oggi richiedeva l'impiego di Nmap per capirne il funzionamento e fare partica con il processo di raccolta informazioni attraverso Kali Linux verso la macchina Metasploitable e il nostro sistema Windows.



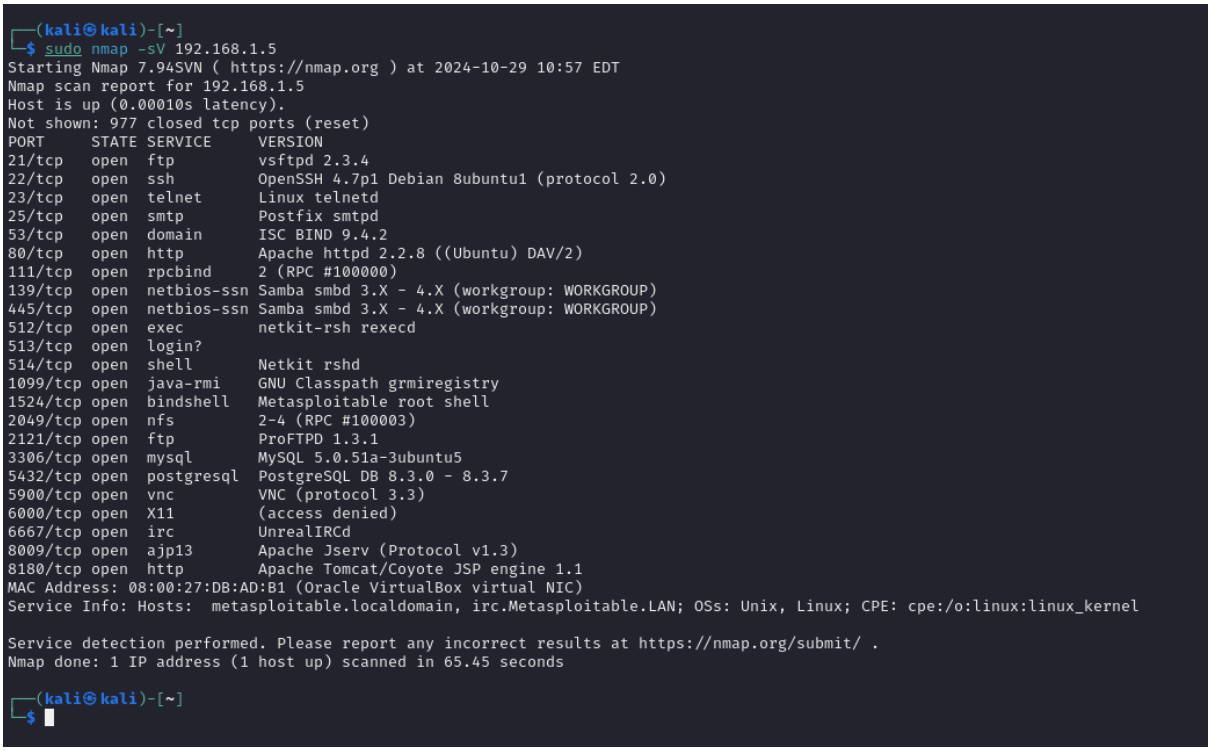
Il primo comando, `nmap -O`, eseguito sulla macchina Metasploitable2, ha rivelato un sistema operativo Linux. Questo risultato conferma che la macchina è un ambiente progettato per test di penetrazione, utile per l'apprendimento delle vulnerabilità e delle tecniche di attacco sui sistemi Unix-lik



Il secondo comando, `nmap -sS`, lanciato su Metasploitable2, ha trovato molte porte aperte, inclusi i servizi FTP, SSH e Telnet. Questa scansione, nota come SYN scan, è veloce e furtiva, consentendo di identificare i servizi attivi senza stabilire connessioni complete, utile per raccogliere informazioni sui sistemi.



Il terzo comando ha invece evidenziato le stesse porte aperte dello scan SYN ma attraverso il protocollo TCP completo; la differenza col SYN scan è in sostanza che potrebbe allertare dei sistemi di sicurezza, come ad esempio un IDS.



Il quarto comando, `nmap -sV`, eseguito su Metasploitable2, ha fornito un elenco di servizi attivi con le loro versioni. Tra i risultati figurano FTP, SSH, Telnet e HTTP. Questa scansione è utile per identificare potenziali vulnerabilità associate a versioni specifiche di software, facilitando l'analisi delle minacce.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.197
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 11:00 EDT
Nmap scan report for 192.168.1.197
Host is up (0.00013s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1042/tcp open  afrog
1043/tcp open  boinc
MAC Address: 04:33:C2:0B:AB:D0 (Intel Corporate)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/29%OT=135%CT=1%CU=38756%PV=Y%DS=1%DC=D%G=Y%M=043
OS:3C2%TM=6720F89D%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=102%TI=I%CI=I
OS:%II=I%SS=S%TS=U)SEQ(SP=104%GCD=5%ISR=102%TI=I%CI=I%II=I%SS=S%TS=U)OPS(O1
OS:=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5B4NW8NNS%O6=M5B4
OS:NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y%T=8
OS:0%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(
OS:R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F
OS:=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=
OS:0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=
OS:164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

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 24.03 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O --osscan-guess 192.168.1.197
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 11:06 EDT
Nmap scan report for 192.168.1.197
Host is up (0.000099s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1042/tcp open  afrog
1043/tcp open  boinc
MAC Address: 04:33:C2:0B:AB:D0 (Intel Corporate)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
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 15.50 seconds
```

Il quinto comando, `nmap -0`, utilizzato sul mio sistema operativo Windows, ha restituito risultati generici, indicando che Nmap non era riuscito a identificare correttamente la versione del sistema. Questo può succedere a causa di protezioni attive o configurazioni di rete che limitano la visibilità delle informazioni del sistema. A questo punto ho deciso di utilizzare –osscan guess, per migliorare i risultati: effettivamente così ha correttamente identificato il sistema operativo Windows 10.

IP Kali - 192.168.1.25
IP Metasploitable2 (cambiato post build week dopo configurazione per pfsense) - 192.168.1.5
IP Windows 10 - 192.168.1.197
IP Gateway - 192.168.1.1

Lista porte aperte su Metasploitable 2:

```
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
8180/tcp open  unknown
```

Lista servizi aperti su Metasploitable2:

```
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

Sistemi operativi rilevati:

Metasploitable2
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

Windows10 (dopo –osscan-guess)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop