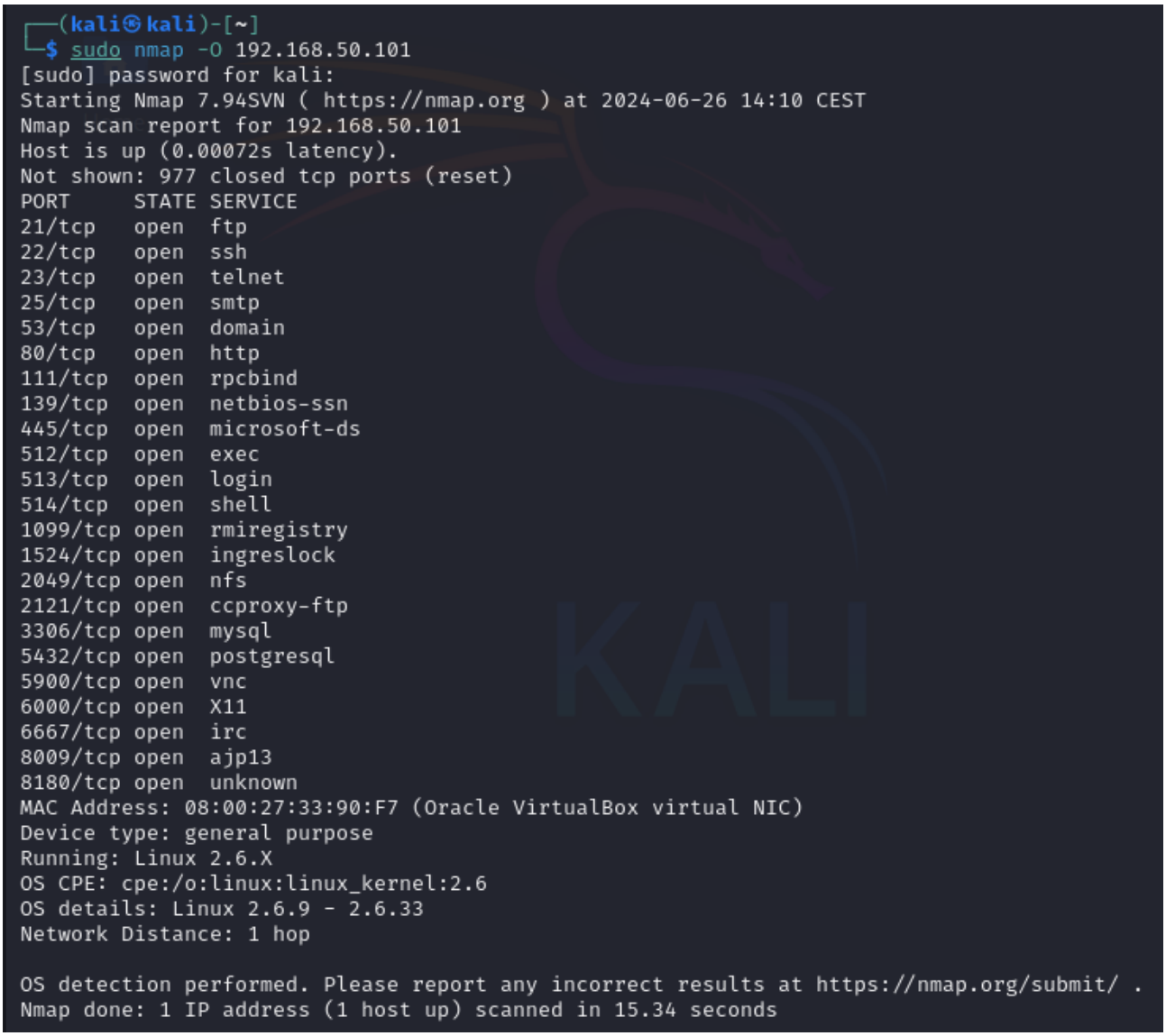
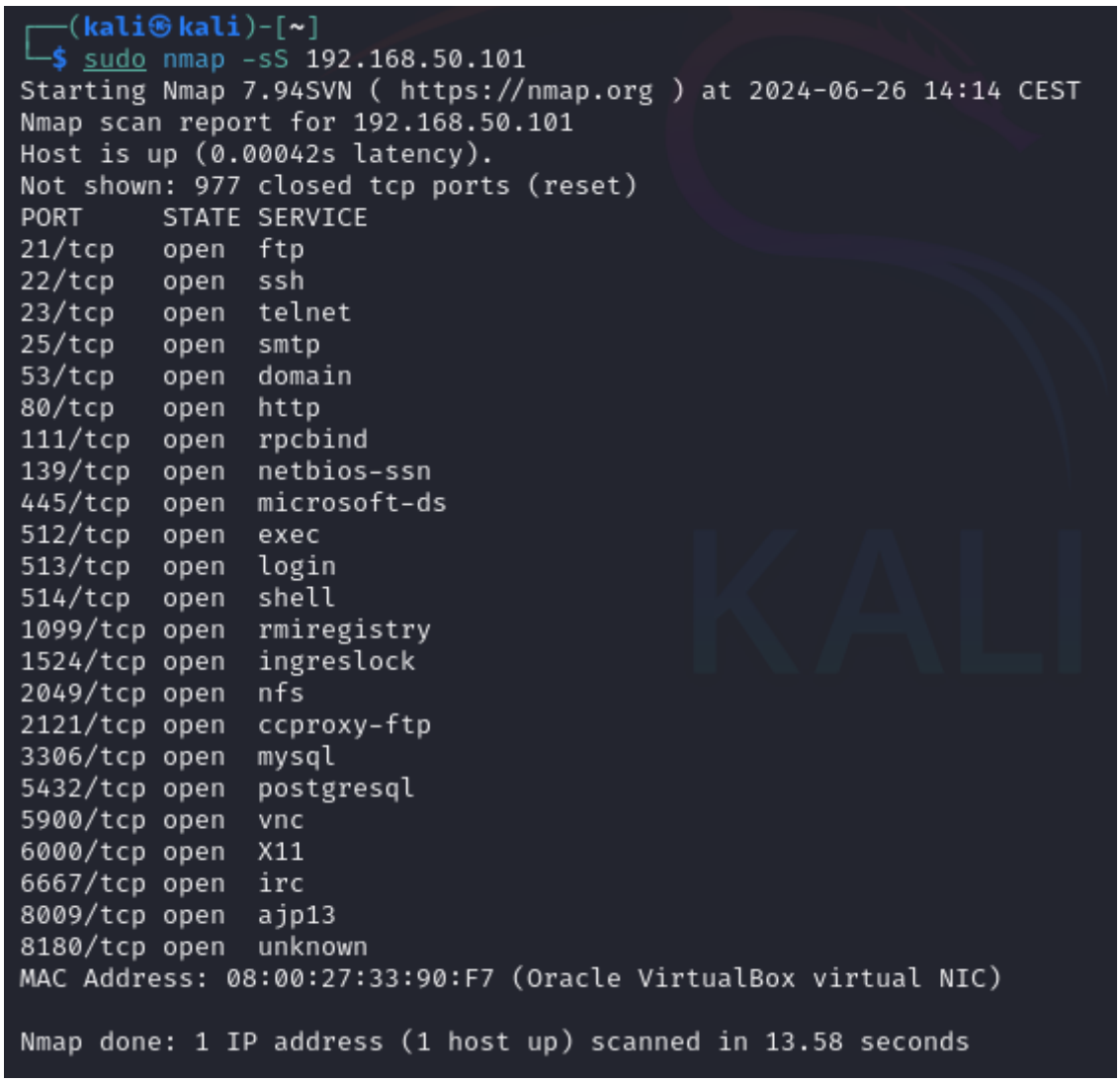
REPORT NMAP

Consegna U2-S5-L3

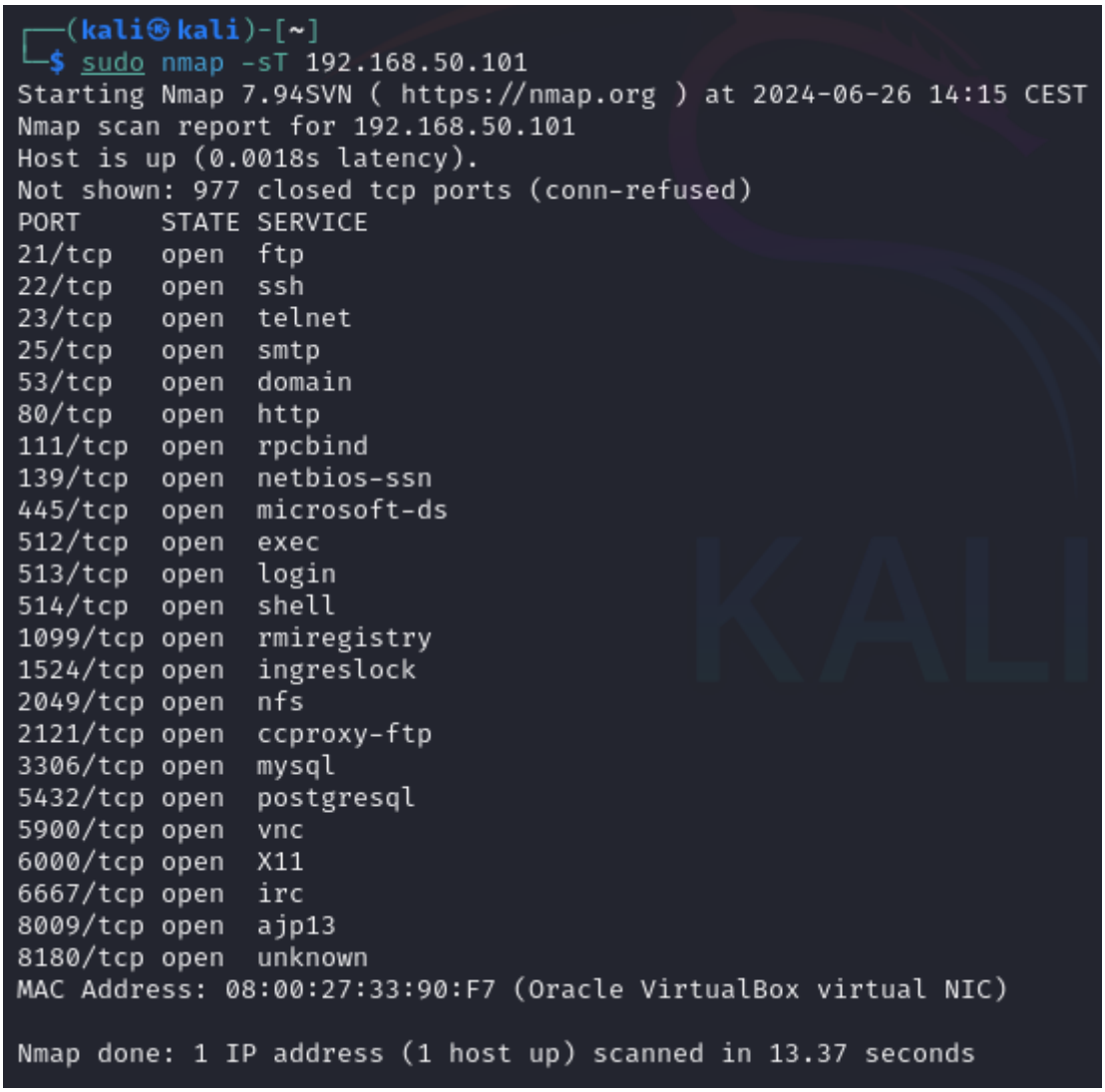
- **OS Fingerprint su Metasploitable**



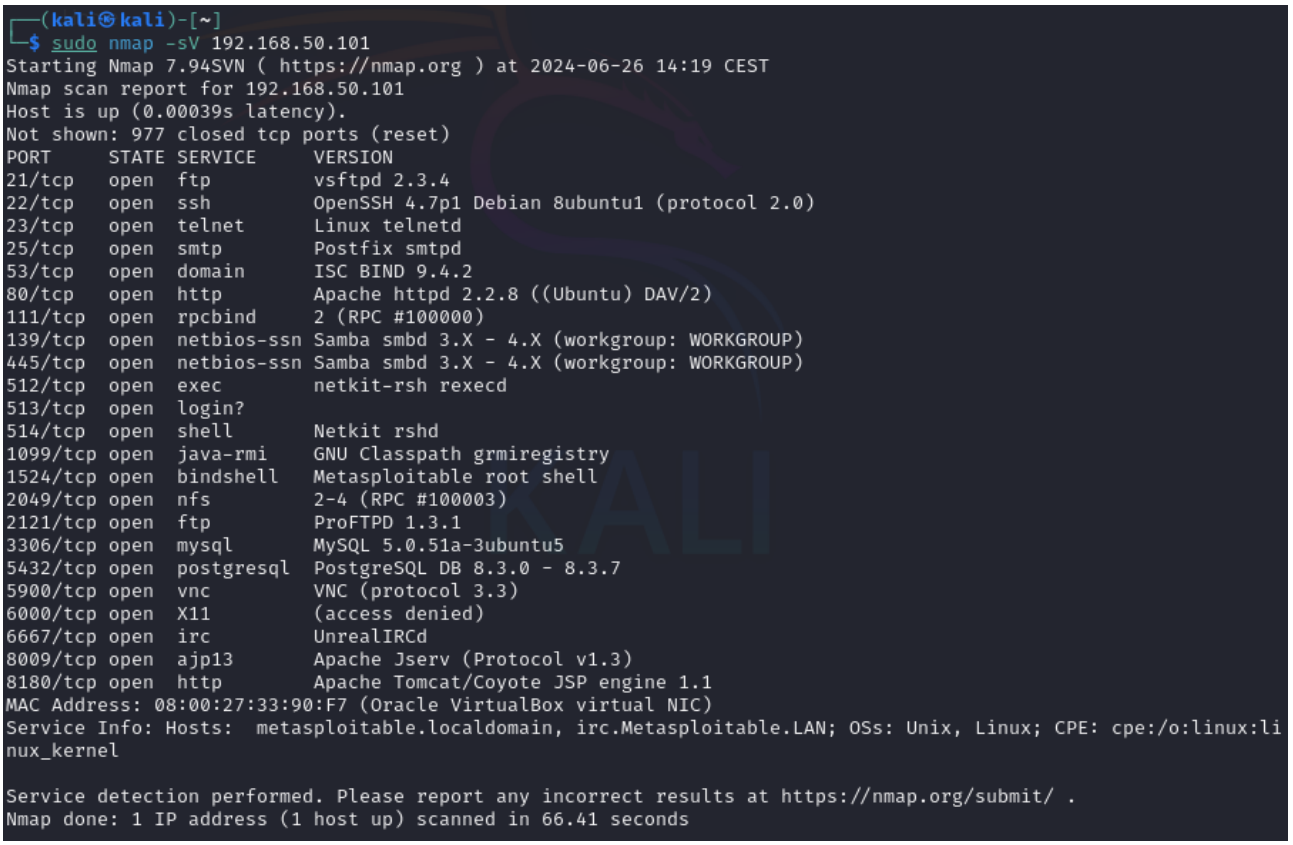
- **Syn Scan su Metasploitable**



- **TCP Connect su Metasploitable**



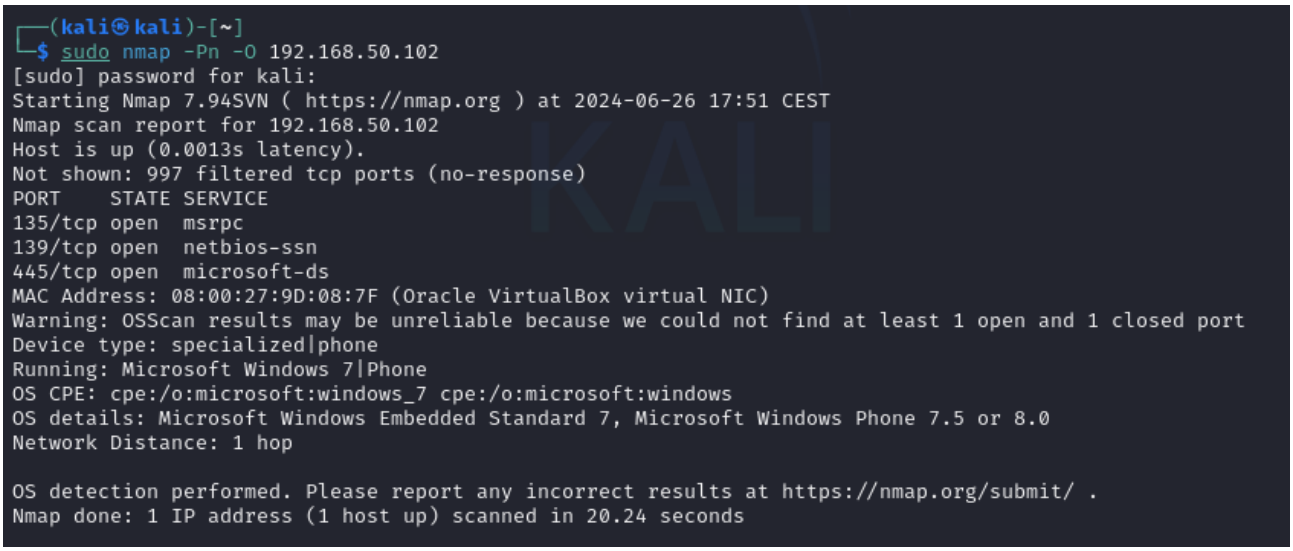
- **Version Detection su Metasploitable**



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 14:19 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00039s 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: 08:00:27:33:90:F7 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:li
nux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.41 seconds
```

- **OS Fingerprint su Windows 7**



- **Report finale**

- **Metasploitable**:
  Sistema operativo: basato su Linux kernel 2.6.9 – 2.6.33
  IP: 192.168.50.101
  Porte aperte:
  - 21/tcp → ftp
  - 22/tcp → ssh
  - 23/tcp → telnet
  - 25/tcp → smtp
  - 53/tcp → domain
  - 80/tcp → http
  - 111/tcp → rpcbind
  - 139/tcp → netbios-ssn
  - 445/tcp → microsoft-ds
  - 512/tcp → exec
  - 513/tcp → login
  - 514/tcp → shell
  - 1099/tcp → rmiregistry
  - 1524/tcp → ingreslock
  - 2049/tcp → nfs

2121/tcp → ccproxy-ftp
3306/tcp → mysql
5432/tcp → postgresql
5900/tcp → vnc
6000/tcp → X11
6667/tcp → irc
8009/tcp → ajp13
8180/tcp → unknown

Versione dei servizi:

ftp	→	vsftpd 2.3.4
ssh	→	OpenSSH 4.7p1
telnet	→	Linux telnetd
smtp	→	Postfix smtpd
domain	→	ISC BIND 9.4.2
http	→	Apache httpd 2.2.8
rpcbind	→	2
netbios-ssn	→	Samba smbd 3.x -4.x
exec	→	netkit-rsh rexecd
login	→	
shell	→	Netkit rshd
java-rmi	→	GNU Classpath grmiregistry
bindshell	→	Metasploitable root shell
nfs	→	2-4
ftp	→	ProFTPD 1.3.1
mysql	→	MySQL 5.0.51°
postgresql	→	PostgreSQL DB 8.3.0 – 8.3.7
vnc	→	VNC 3.3
X11	→	(access denied)
Irc	→	UnrealIRCd
ajp13	→	Apache Jserv 1.3
http	→	Apache Tomcat/Coyote JSP engine 1.1

- **Windows 7:**
  Sistema operativo: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5/8.0
  IP: 192.168.50.102
  Porte aperte:
  135/tcp → msrpc
  139/tcp → netbios-ds
  445/tcp → microsoft-ds

  Affinchè nmap possa scansire correttamente il sistema Windows 7, è necessario aggiungere lo switch “-Pn” al comando da terminale.