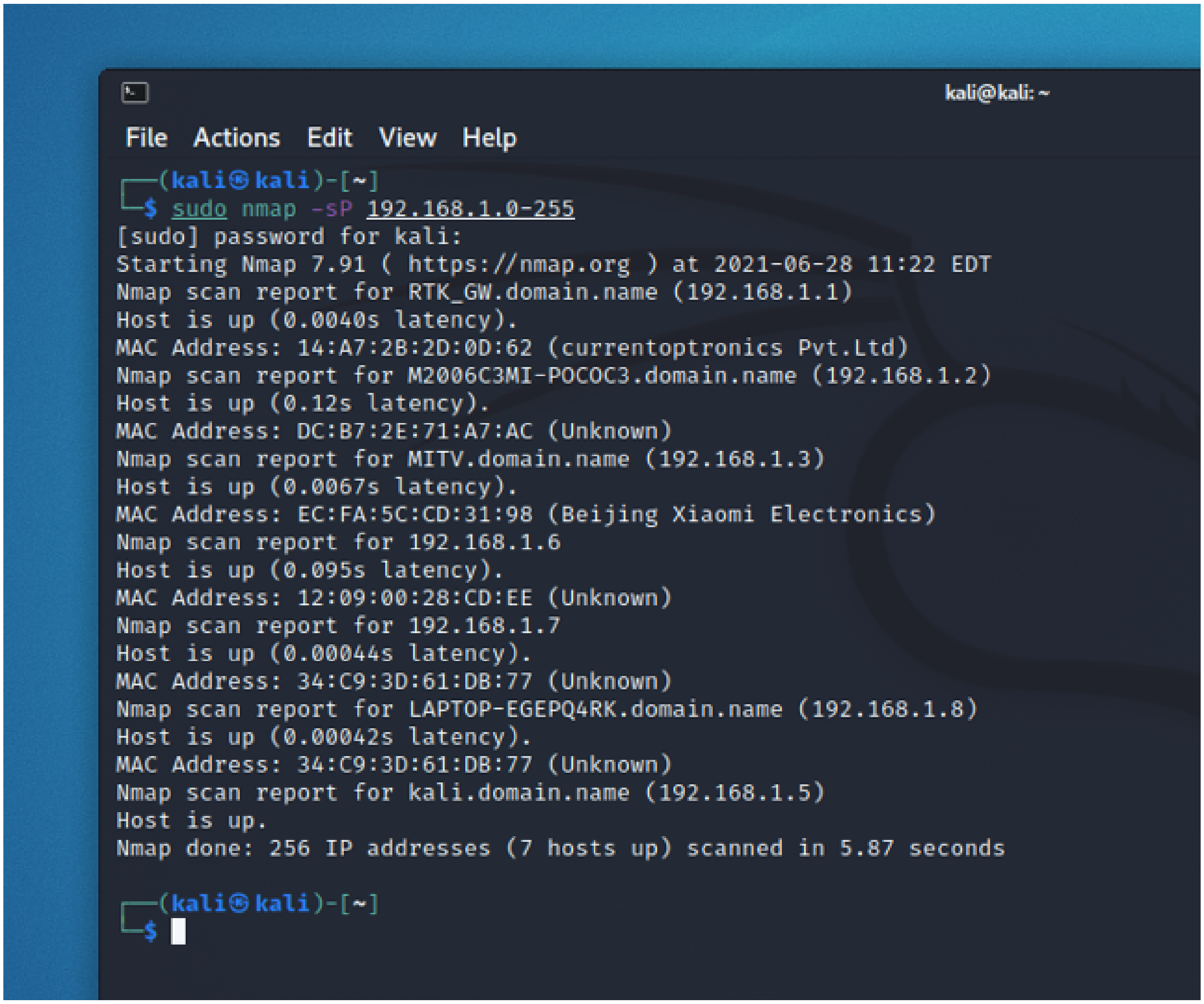
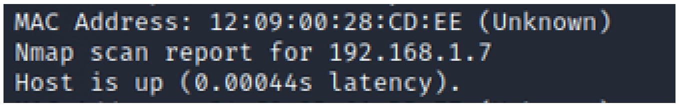
NMAP

STEP 1: Scan the network 192.168.1.0-255



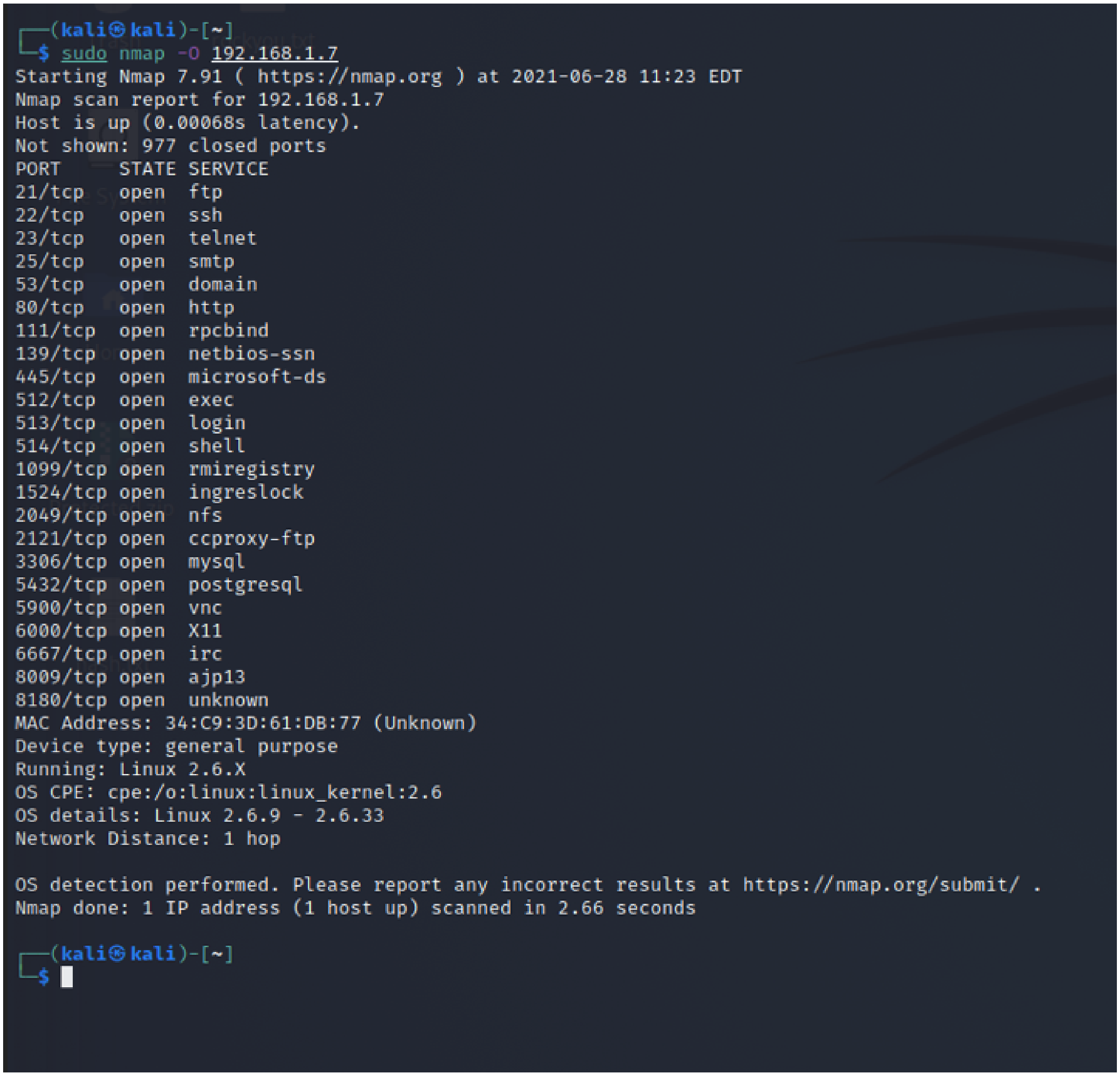
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sP 192.168.1.0-255
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-28 11:22 EDT
Nmap scan report for RTK_GW.domain.name (192.168.1.1)
Host is up (0.0040s latency).
MAC Address: 14:A7:2B:2D:0D:62 (currentoptronics Pvt.Ltd)
Nmap scan report for M2006C3MI-POCOC3.domain.name (192.168.1.2)
Host is up (0.12s latency).
MAC Address: DC:B7:2E:71:A7:AC (Unknown)
Nmap scan report for MITV.domain.name (192.168.1.3)
Host is up (0.0067s latency).
MAC Address: EC:FA:5C:CD:31:98 (Beijing Xiaomi Electronics)
Nmap scan report for 192.168.1.6
Host is up (0.095s latency).
MAC Address: 12:09:00:28:CD:EE (Unknown)
Nmap scan report for 192.168.1.7
Host is up (0.00044s latency).
MAC Address: 34:C9:3D:61:DB:77 (Unknown)
Nmap scan report for LAPTOP-EGEPQ4RK.domain.name (192.168.1.8)
Host is up (0.00042s latency).
MAC Address: 34:C9:3D:61:DB:77 (Unknown)
Nmap scan report for kali.domain.name (192.168.1.5)
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 5.87 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

STEP 2: Finding the IP address of the metasploitable



```
MAC Address: 12:09:00:28:CD:EE (Unknown)
Nmap scan report for 192.168.1.7
Host is up (0.00044s latency).
```

STEP 3 : Scanning the metasploitable



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.7
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-28 11:23 EDT
Nmap scan report for 192.168.1.7
Host is up (0.00068s latency).
Not shown: 977 closed ports
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: 34:C9:3D:61:DB:77 (Unknown)
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 2.66 seconds

┌──(kali㉿kali)-[~]
└─$ 
```