Section 5: Scanning

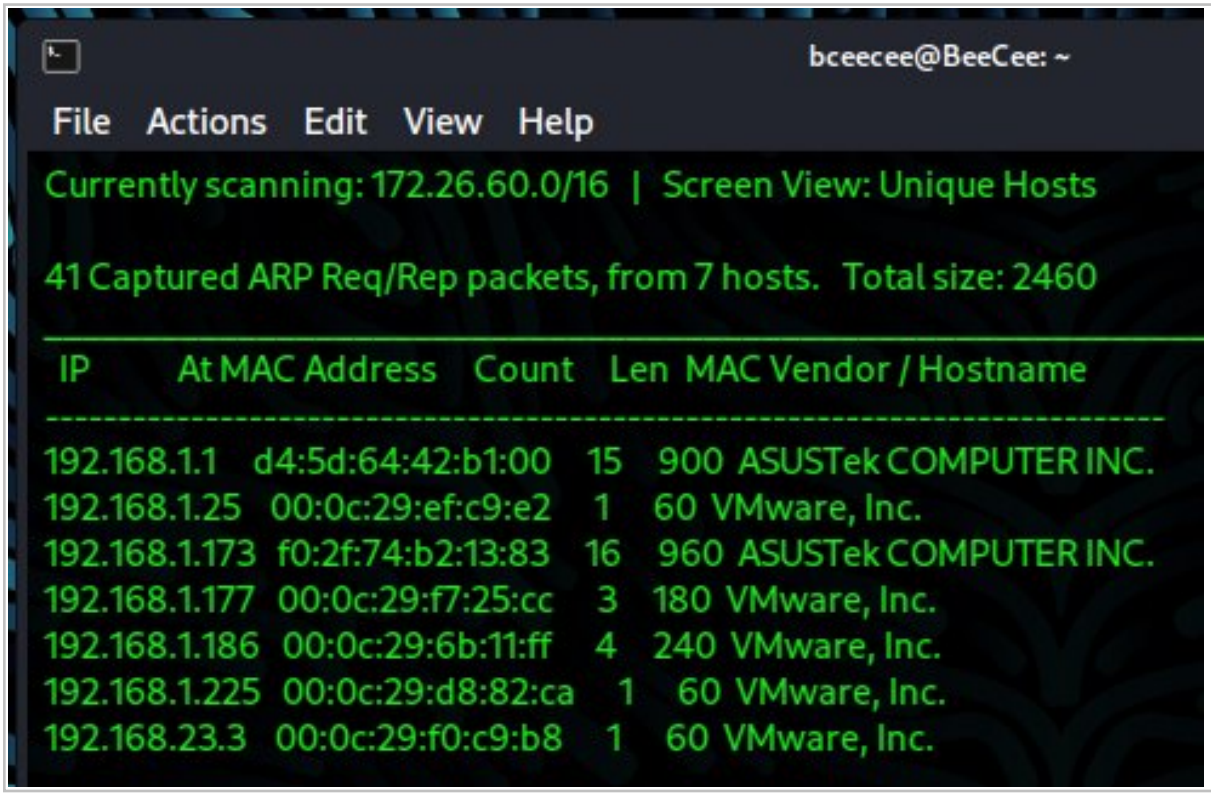
Name: BC

Choose screenshots for each lab that best illustrates your completion of the lab. Submit by clicking the box and locating the screenshot. Use a black-on-white color scheme for all Terminal sessions.

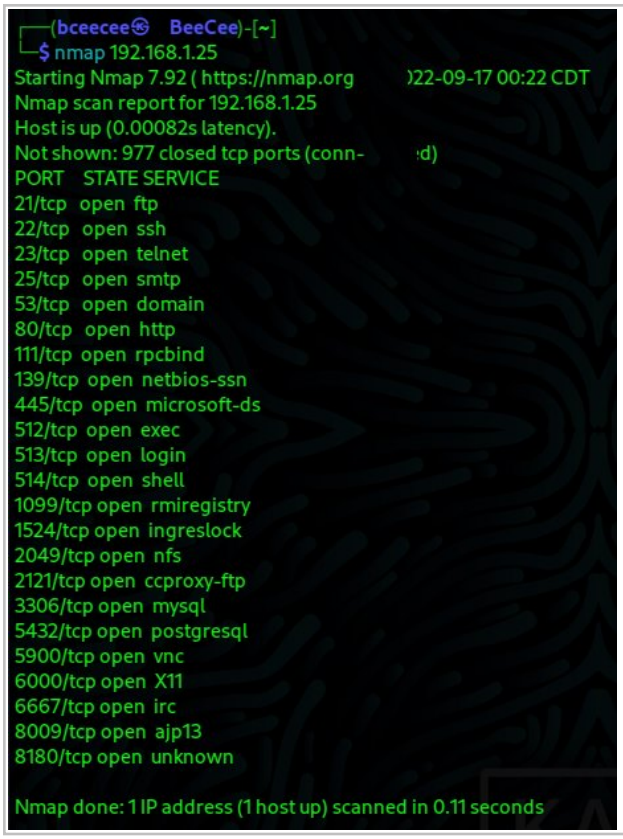
Lab 1: Download and install Metasploitable2 as a VM. Configure internal network settings (37)

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:ef:c9:e2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::20c:29ff:feef:c9e2/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ping -c3 192.168.1.110
PING 192.168.1.110 (192.168.1.110) 56(84) bytes of data.
64 bytes from 192.168.1.110: icmp_seq=1 ttl=64 time=0.289 ms
64 bytes from 192.168.1.110: icmp_seq=2 ttl=64 time=0.445 ms
64 bytes from 192.168.1.110: icmp_seq=3 ttl=64 time=0.433 ms

--- 192.168.1.110 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.289/0.389/0.445/0.070 ms
msfadmin@metasploitable:~$ _
```

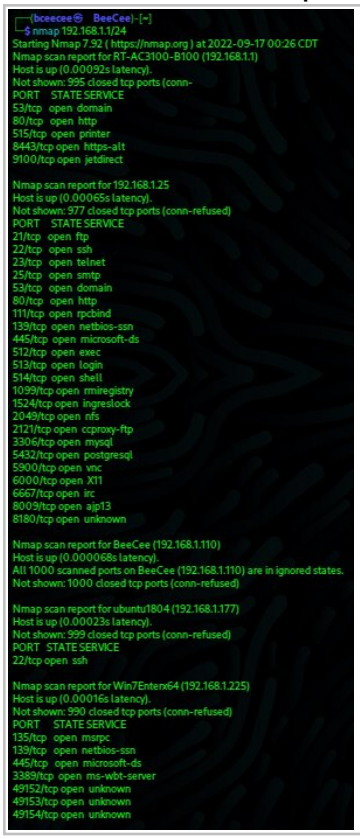
Lab 2: Start several lab VMs. Use netdiscover on Kali VM to find the other VMs (38)



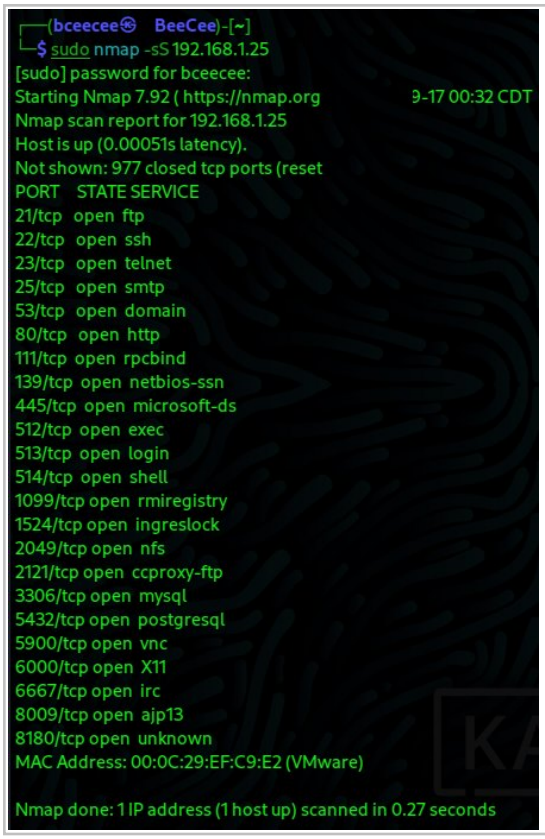
Lab 3: Run a basic nmap scan against the Metasploitable2 VM (39)



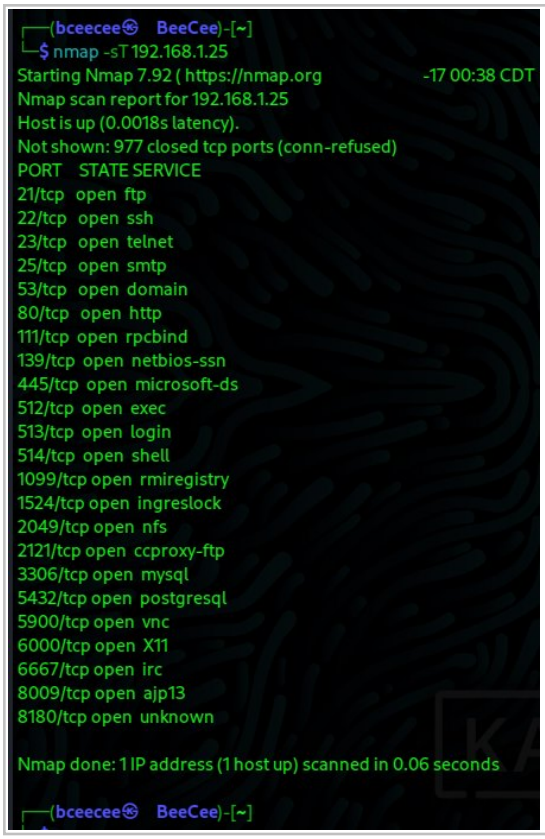
Lab 4: Run an nmap scan against your entire subnet (39)



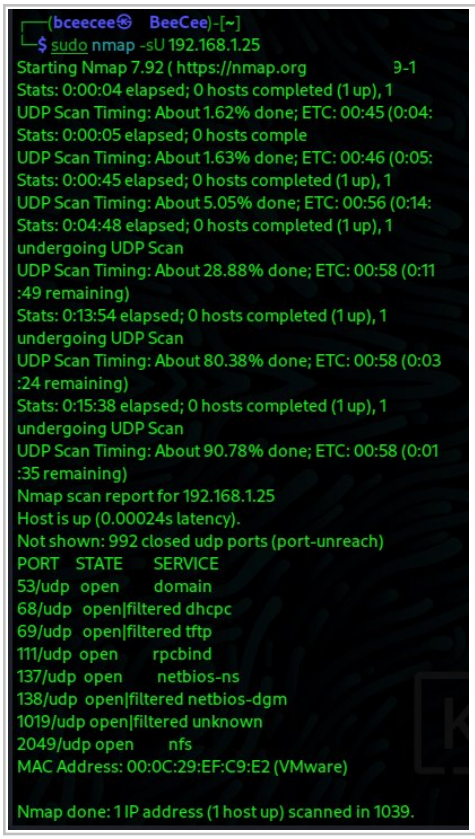
Lab 5: Conduct a TCP SYN scan from Kalia against Metasploitable2 (40)



Lab 6: Conduct a TCP CONNECT scan from Kalia against Metasploitable2 (40)

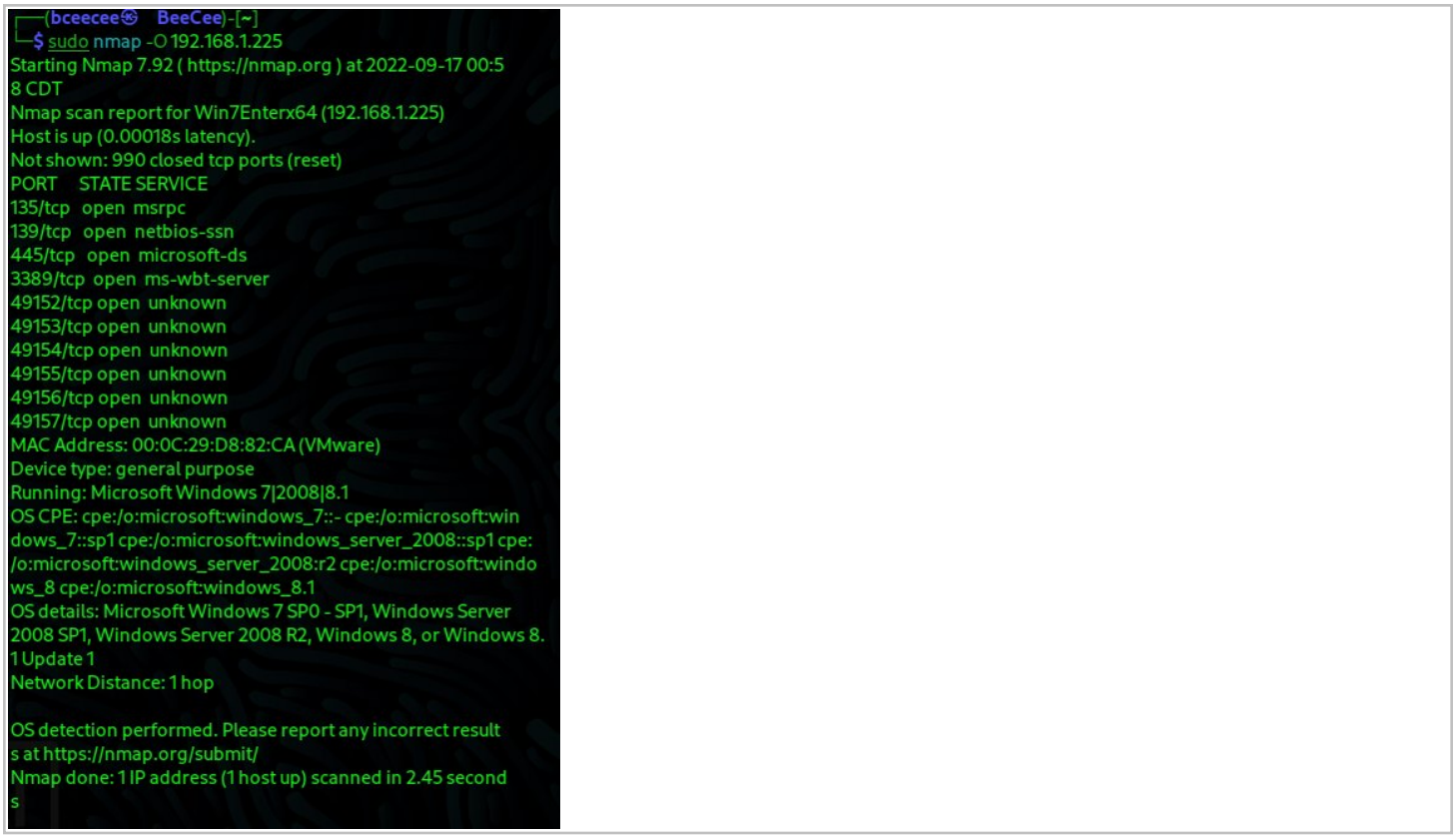


Lab 7: Conduct a UDP scan from Kalia against Metasploitable2 (40)

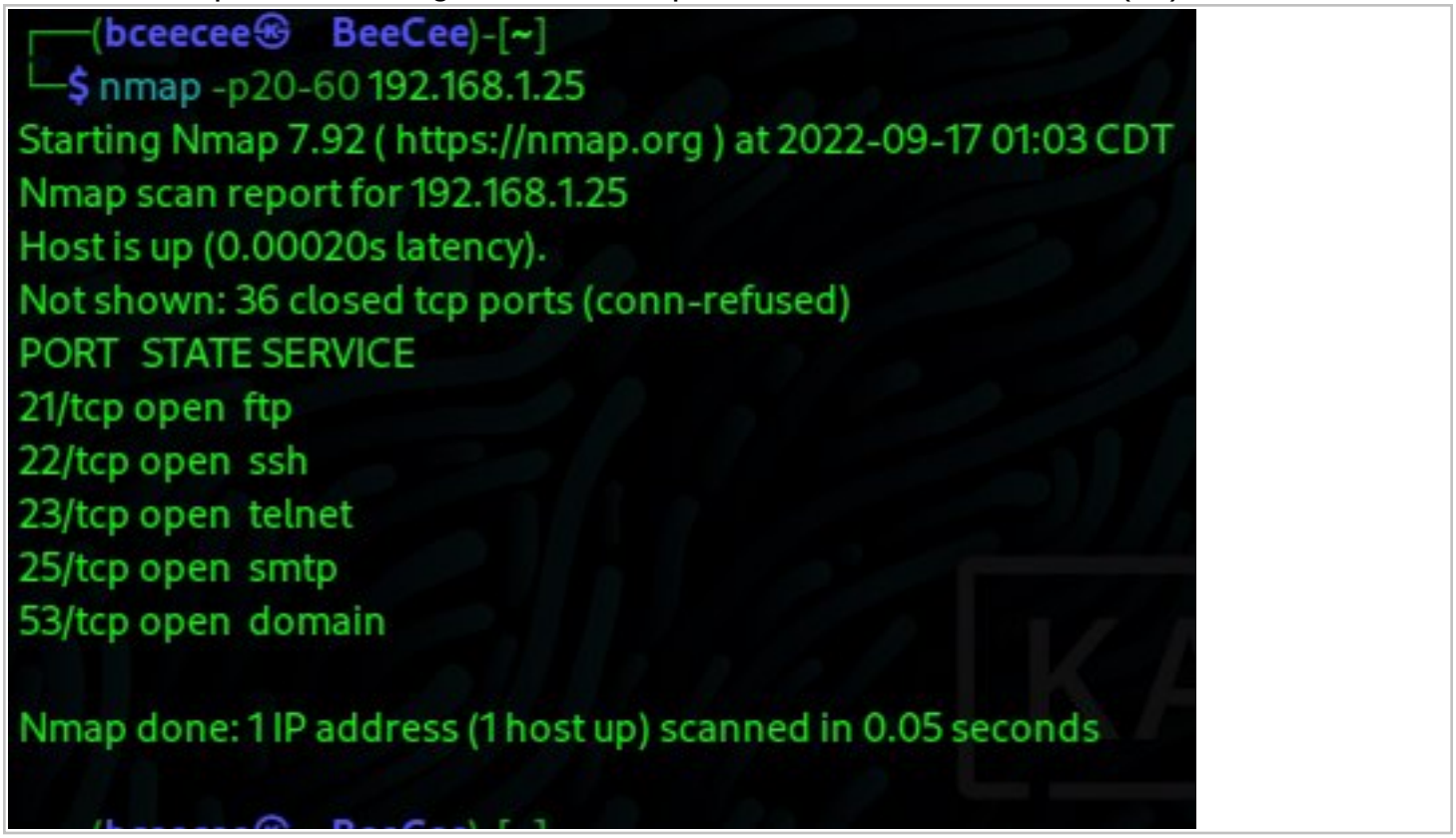


Lab 8: Conduct a TCP XMAS scan from Kalia against Metasploitable2 (40)

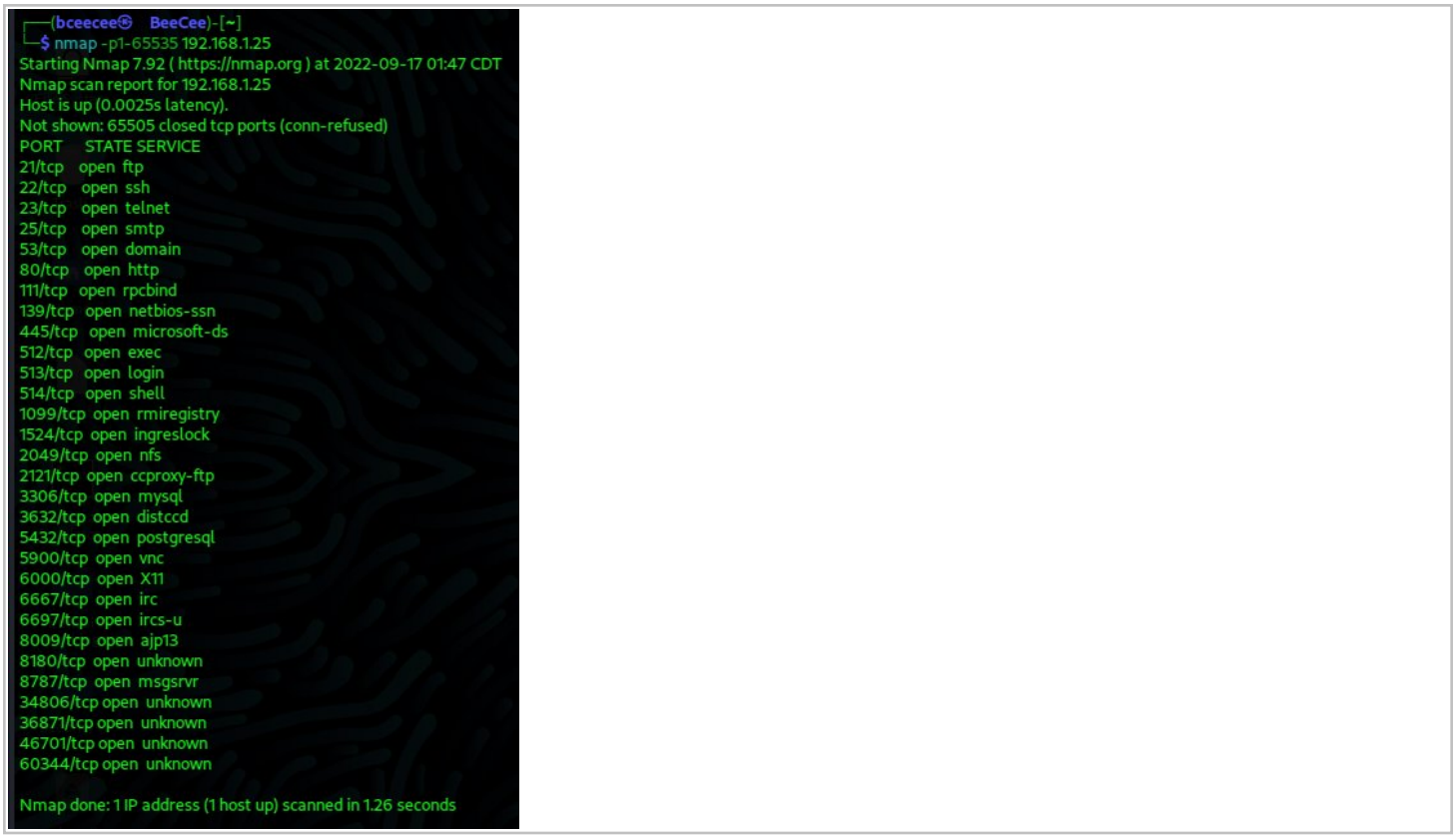
Lab 9: Determine the operating system running on Windows 7 VM from Kali VM (42)



Lab 10: Scan ports 20 through 60 on Metasploitable2 VM from Kali VM (44)

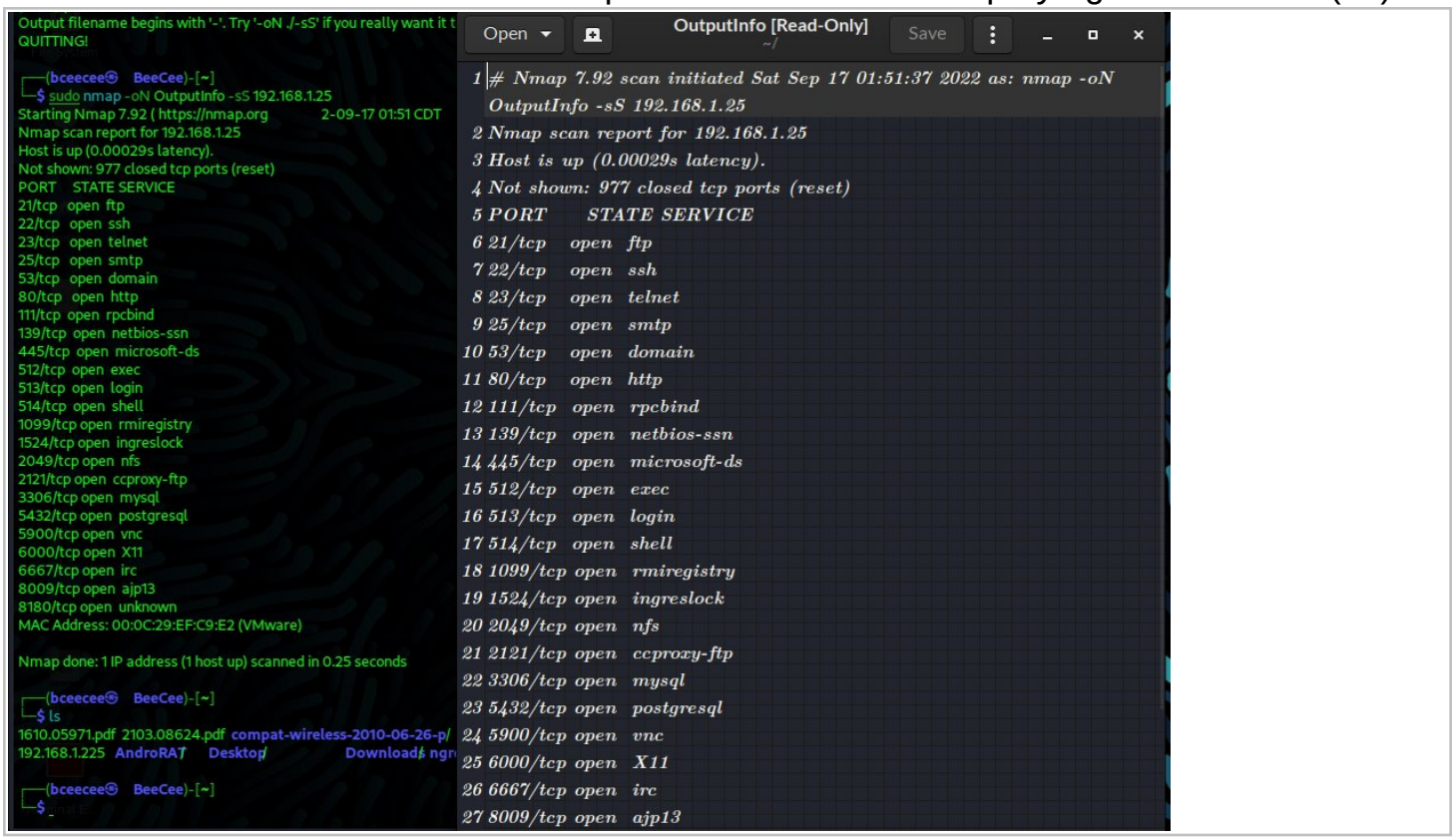


Lab 11: Scan all ports on Metasploitable2 from Kali (44)



```
┌──(bceecee㉿ BeeCee)-[~]
└─$ nmap -p1-65535 192.168.1.25
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-17 01:47 CDT
Nmap scan report for 192.168.1.25
Host is up (0.0025s latency).
Not shown: 65505 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
3632/tcp open  distccd
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
6697/tcp open  ircs-u
8009/tcp open  ajp13
8180/tcp open  unknown
8787/tcp open  msgsrvr
34806/tcp open  unknown
36871/tcp open  unknown
46701/tcp open  unknown
60344/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
```

Lab 12: Save a TCP SYN scan of Metasploitable2 while also displaying on the screen (44)

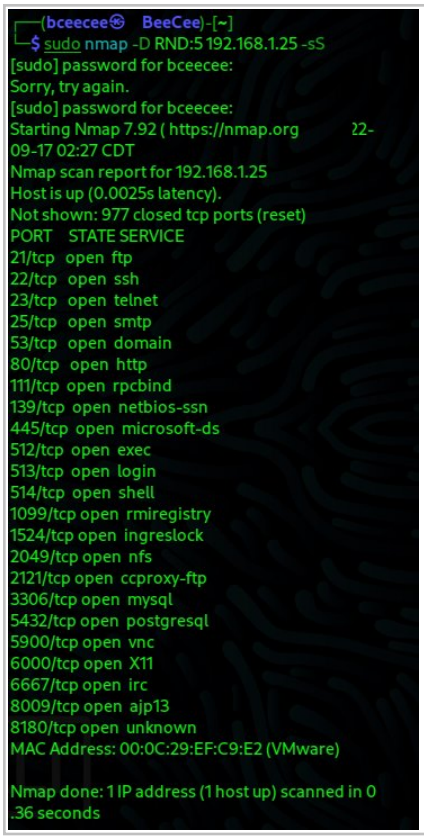


```
Output filename begins with '-'. Try '-oN ./-sS' if you really want it t
QUITTING!

┌──(bceecee㉿ BeeCee)-[~]
└─$ sudo nmap -oN OutputInfo -sS 192.168.1.25
Starting Nmap 7.92 ( https://nmap.org )          2-09-17 01:51 CDT
Nmap scan report for 192.168.1.25
Host is up (0.00029s 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: 00:0C:29:EF:C9:E2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds

┌──(bceecee㉿ BeeCee)-[~]
└─$ ls
1610.05971.pdf  2103.08624.pdf  compat-wireless-2010-06-26-p/
192.168.1.225   AndroRAT        Desktop/                      Downloads ngr

┌──(bceecee㉿ BeeCee)-[~]
└─$
```

Open OutputInfo [Read-Only] ~/ Save

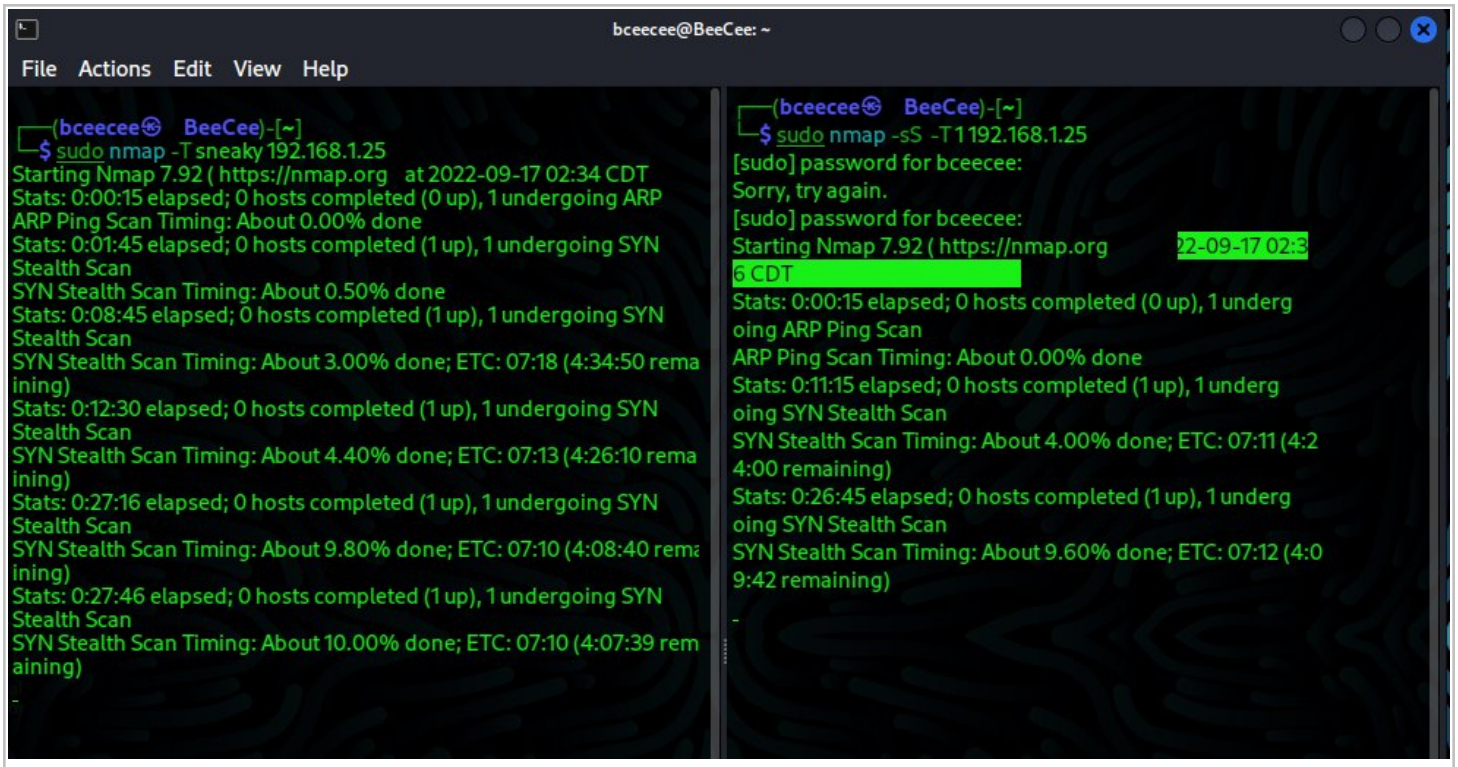
```
1 # Nmap 7.92 scan initiated Sat Sep 17 01:51:37 2022 as: nmap -oN
  OutputInfo -sS 192.168.1.25
2 Nmap scan report for 192.168.1.25
3 Host is up (0.00029s latency).
4 Not shown: 977 closed tcp ports (reset)
5 PORT     STATE SERVICE
6 21/tcp   open  ftp
7 22/tcp   open  ssh
8 23/tcp   open  telnet
9 25/tcp   open  smtp
10 53/tcp  open  domain
11 80/tcp  open  http
12 111/tcp  open  rpcbind
13 139/tcp  open  netbios-ssn
14 445/tcp  open  microsoft-ds
15 512/tcp  open  exec
16 513/tcp  open  login
17 514/tcp  open  shell
18 1099/tcp open  rmiregistry
19 1524/tcp open  ingreslock
20 2049/tcp open  nfs
21 2121/tcp open  ccproxy-ftp
22 3306/tcp open  mysql
23 5432/tcp open  postgresql
24 5900/tcp open  vnc
25 6000/tcp open  X11
26 6667/tcp open  irc
27 8009/tcp open  ajp13
```

Lab 13: Scan Metasploitable2 using five random source IP addresses on Internal LAN (46)



Lab 14: Scan Metasploitable2 using a defined set of source IP addresses on Internal LAN (46)

Lab 15: Run a sneaky TCP SYN scan against Exploitable2 VM (47)



This tool may take several hours to complete. You may capture the results after a half hour if you wish for your screenshot. Press the up arrow to see the status.