

Issa Odeh

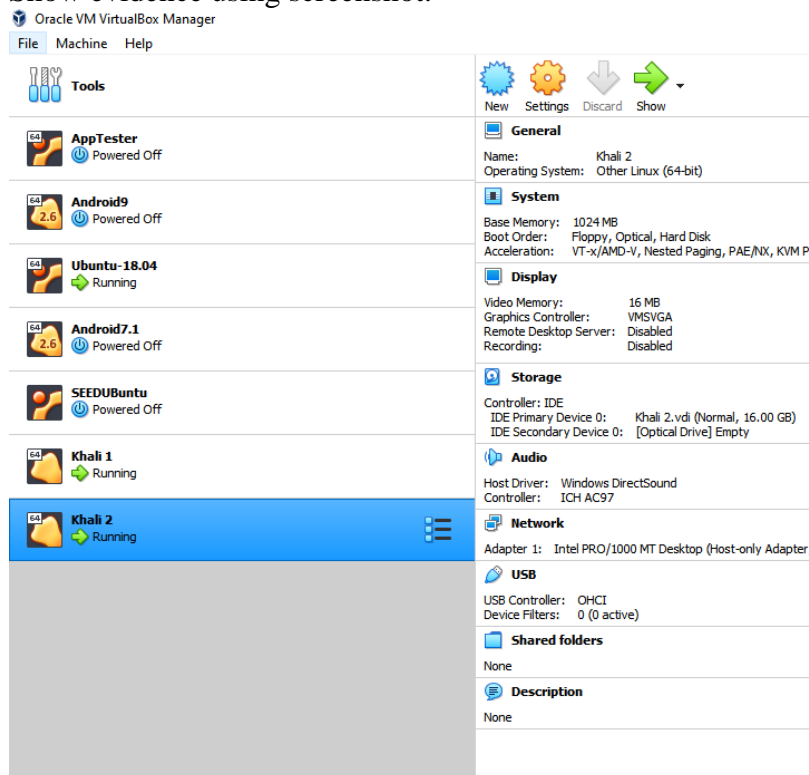
CS 445/645: Internet Security

Instructor: Shahriar Badsha

Assignment 2 (Total 20 points)
Due back on: Wed, Feb 16, 2021

[6] Part 1: Setup:

- 1) Make sure to have two Kali VM and one non-Kali (e.g., Ubuntu Linux) VM. Show evidence using screenshot.



CS 445/645: Internet Security
Homework 2

Due: Tuesday, February 16, 2021
Spring 2021

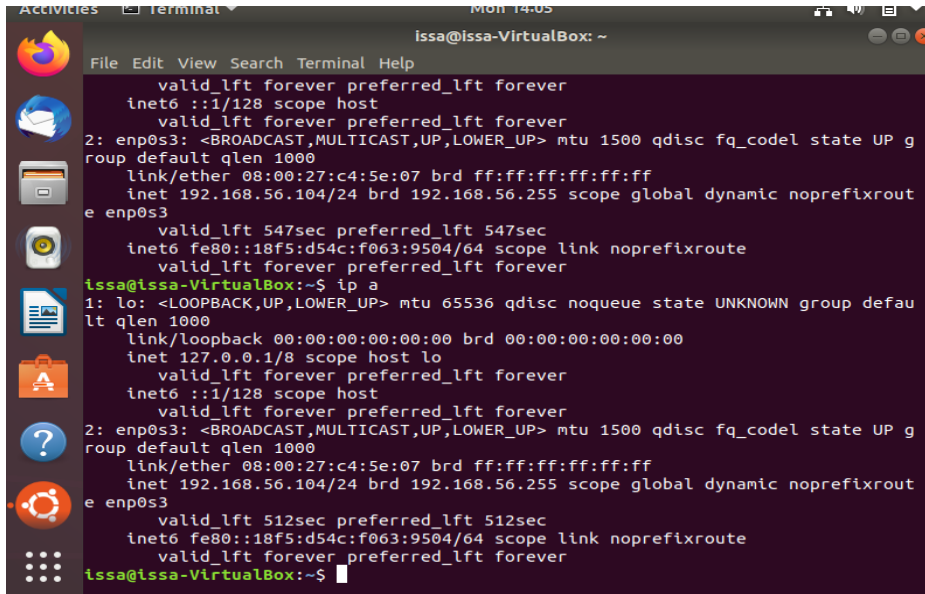
- 2) Make sure they are in the same subnet, i.e., all of them can ping each other. Show evidence using screenshot.

```
issa@kali: ~  
File Actions Edit View Help  
(issa@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.56.103 netmask 255.255.255.0 broadcast 192.168.56.255  
    ether 08:00:27:00:e1:6e txqueuelen 1000 (Ethernet)  
    RX packets 4 bytes 1570 (1.5 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 11 bytes 1142 (1.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 400 (400.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 400 (400.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(issa@kali)-[~]  
$
```

```
File Actions Edit View Help  
(issa@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255  
    ether 08:00:27:a6:3f:c5 txqueuelen 1000 (Ethernet)  
    RX packets 4 bytes 1570 (1.5 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 11 bytes 1142 (1.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 400 (400.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 400 (400.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ip address is 192.168.56.102 in Kali 1

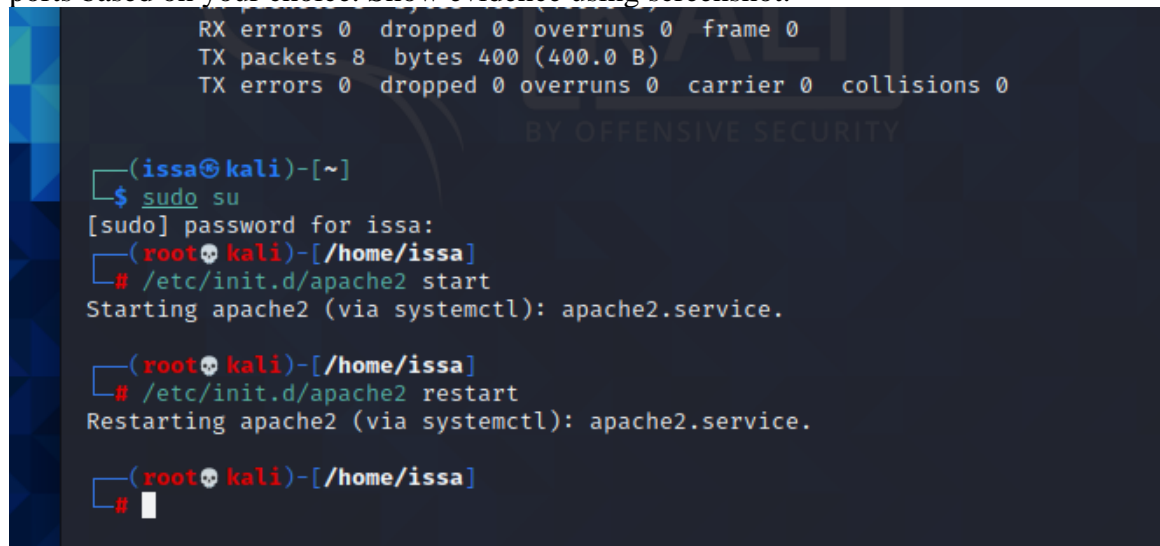
Ip address is 192.168.56.103 in Kali 2



```
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:c4:5e:07 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.104/24 brd 192.168.56.255 scope global dynamic noprefixrout
e enp0s3
        valid_lft 547sec preferred_lft 547sec
    inet6 fe80::18f5:d54c:f063:9504/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
Issa@Issa-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:c4:5e:07 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.104/24 brd 192.168.56.255 scope global dynamic noprefixrout
e enp0s3
        valid_lft 512sec preferred_lft 512sec
    inet6 fe80::18f5:d54c:f063:9504/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
Issa@Issa-VirtualBox:~$
```

Ip address is 192.168.56.104 in the Ubuntu

- 3) Make sure web service is running in one of the target Kali. You can open other ports based on your choice. Show evidence using screenshot.



```
RX errors 0    dropped 0    overruns 0  frame 0
TX packets 8   bytes 400 (400.0 B)
TX errors 0    dropped 0    overruns 0  carrier 0    collisions 0

BY OFFENSIVE SECURITY

(issa@kali)-[~]
$ sudo su
[sudo] password for issa:
(root@kali)-[/home/issa]
# /etc/init.d/apache2 start
Starting apache2 (via systemctl): apache2.service.

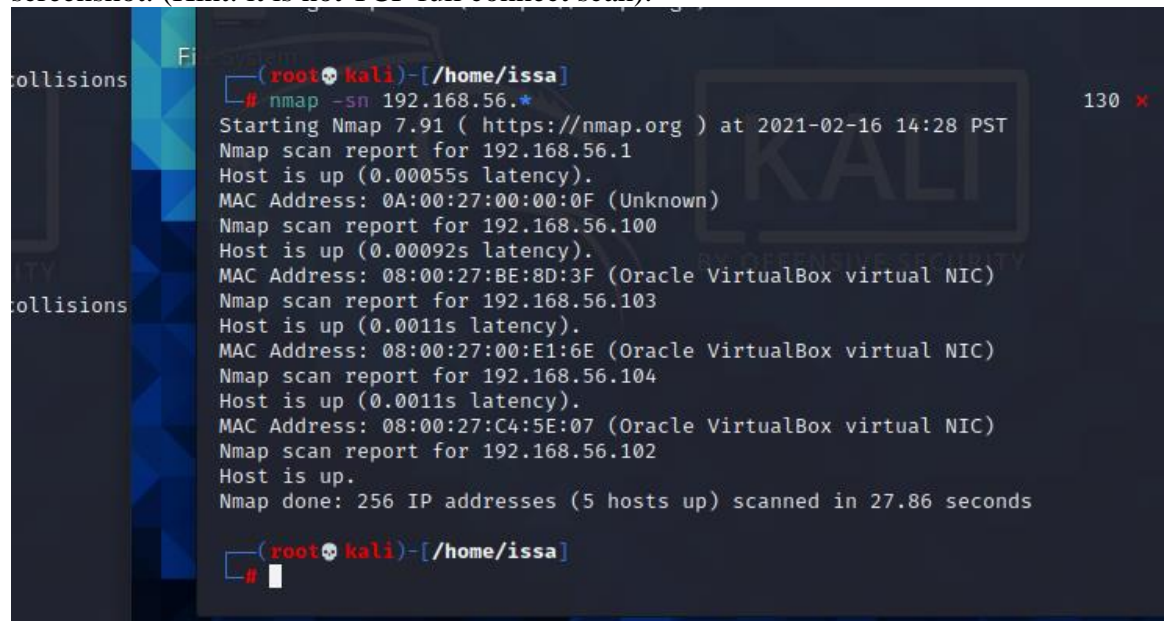
(root@kali)-[/home/issa]
# /etc/init.d/apache2 restart
Restarting apache2 (via systemctl): apache2.service.

(root@kali)-[/home/issa]
#
```

[14] Part 2: Experiment:

- 1) Intruders are able to sweep entire networks looking for targets with nmap. This is usually done with a ping sweep. How can you do ping sweep on your virtual network? Give command(s). How many hosts are up? Show using nmap

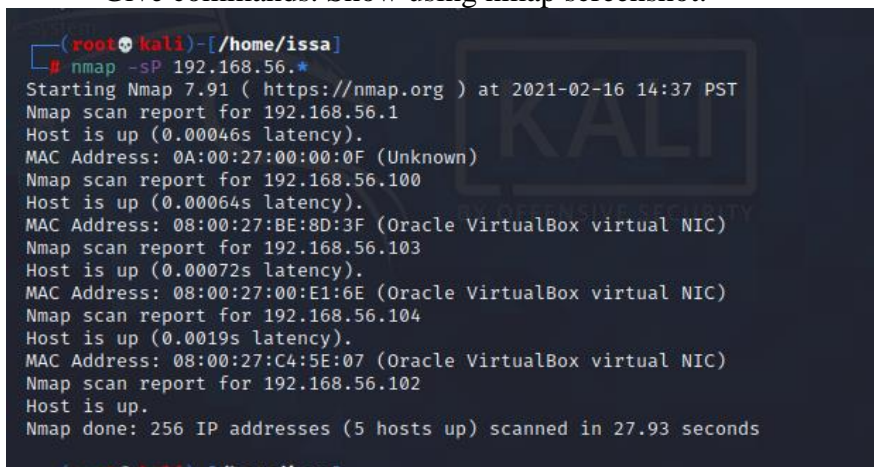
screenshot. (Hint: it is not TCP full connect scan).



```
(root@kali)-[/home/issa]
# nmap -sn 192.168.56.*
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 14:28 PST
Nmap scan report for 192.168.56.1
Host is up (0.00055s latency).
MAC Address: 0A:00:27:00:00:0F (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00092s latency).
MAC Address: 08:00:27:BE:8D:3F (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up (0.0011s latency).
MAC Address: 08:00:27:00:E1:6E (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.104
Host is up (0.0011s latency).
MAC Address: 08:00:27:C4:5E:07 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 27.86 seconds

(root@kali)-[/home/issa]
#
```

- 2) Equipped with previous step, put the live host ip addresses in a file and use the file to probe using nmap. Which ports are open and which services are running? Give commands. Show using nmap screenshot.



```
(root@kali)-[/home/issa]
# nmap -sP 192.168.56.*
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 14:37 PST
Nmap scan report for 192.168.56.1
Host is up (0.00046s latency).
MAC Address: 0A:00:27:00:00:0F (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00064s latency).
MAC Address: 08:00:27:BE:8D:3F (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up (0.00072s latency).
MAC Address: 08:00:27:00:E1:6E (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.104
Host is up (0.0019s latency).
MAC Address: 08:00:27:C4:5E:07 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 27.93 seconds

(root@kali)-[/home/issa]
#
```

```
(root@kali)-[/home/issa]
# nmap -iL file.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 07:32 PST
Nmap scan report for 192.168.56.103
Host is up (0.00024s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:00:E1:6E (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.104
Host is up (0.00023s latency).
All 1000 scanned ports on 192.168.56.104 are closed
MAC Address: 08:00:27:C4:5E:07 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.000070s latency).
All 1000 scanned ports on 192.168.56.102 are closed

Nmap done: 3 IP addresses (3 hosts up) scanned in 26.50 seconds
```

- 3) Find out the versions of services these are running and find out the operating systems. Show using nmap screenshot.

```
Nmap done: 1 IP address (1 host up) scanned in 16.11 seconds

(root@kali)-[/home/issa]
# nmap 192.168.56.103 -sV -O
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-15 23:14 PST
Nmap scan report for 192.168.56.103
Host is up (0.0011s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.46 ((Debian))
MAC Address: 08:00:27:00:E1:6E (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.42 seconds

(root@kali)-[/home/issa]
```



```
File Actions Edit View Help
(root@kali)-[/home/issa]
# nmap 192.168.56.102 -sV -O
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-15 23:17 PST
Nmap scan report for 192.168.56.102
Host is up (0.000076s latency).
All 1000 scanned ports on 192.168.56.102 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.95 seconds

(root@kali)-[/home/issa]
# nmap 192.168.56.104 -sV -O
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-15 23:18 PST
Nmap scan report for 192.168.56.104
Host is up (0.00080s latency).
All 1000 scanned ports on 192.168.56.104 are closed
MAC Address: 08:00:27:C4:5E:07 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.11 seconds

(root@kali)-[/home/issa]
#
```

- 4) Can you create an executable script that will use nmap scans at varying intervals to scan 10 well known ports and print the status of the ports in easy readable manner. Show the script code and show the results using screenshot.

```
File Actions Edit View Help
GNU nano 5.3 file.sh
nmap -p 21 192.168.56.102
nmap -p 22 192.168.56.102
nmap -p 25 192.168.56.102
nmap -p 53 192.168.56.102
nmap -p 80 192.168.56.102
nmap -p 110 192.168.56.102
nmap -p 123 192.168.56.102
nmap -p 143 192.168.56.102
nmap -p 443 192.168.56.102
nmap -p 465 192.168.56.102
```

```
(root@kali)-[/home/issa]
# chmod +x file.sh

(root@kali)-[/home/issa]
# ./file.sh
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 15:04 PST
Nmap scan report for 192.168.56.102
Host is up (0.000038s latency).

PORT      STATE SERVICE
21/tcp    closed ftp

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 15:04 PST
Nmap scan report for 192.168.56.102
Host is up (0.000036s latency).

PORT      STATE SERVICE
22/tcp    closed ssh

Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 15:05 PST
Nmap scan report for 192.168.56.102
Host is up (0.000069s latency).

PORT      STATE SERVICE
25/tcp    closed smtp

Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 15:05 PST
Nmap scan report for 192.168.56.102
Host is up (0.000037s latency).
```

```
PORT      STATE SERVICE
53/tcp    closed domain

Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 15:05 PST
Nmap scan report for 192.168.56.102
Host is up (0.000034s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 15:05 PST
Nmap scan report for 192.168.56.102
Host is up (0.000034s latency).

PORT      STATE SERVICE
110/tcp   closed pop3

Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 15:06 PST
Nmap scan report for 192.168.56.102
Host is up (0.000034s latency).

PORT      STATE SERVICE
123/tcp   closed ntp

Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 15:06 PST
Nmap scan report for 192.168.56.102
Host is up (0.000035s latency).
```

```
Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 15:06 PST
Nmap scan report for 192.168.56.102
Host is up (0.000036s latency).
```

```
PORT      STATE SERVICE
443/tcp   closed https
```

```
Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 15:06 PST
Nmap scan report for 192.168.56.102
Host is up (0.000034s latency).
```

```
PORT      STATE SERVICE
465/tcp   closed smtps
```

```
Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
```