

Lab 3 – Metasploitable2 VM and Familiarity with Kali Linux

Seneca

SCHOOL OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

NAME – Student ID	COURSE CODE	WEIGHT
Ishan Aakash Patel - 146151238	CYT130	5%

Homework Objectives

Upon completion of this homework, you will be able to perform the following:

- Download and import Metasploitable2 Virtual Machine (VM);
- Kali Linux commands;

Lab Instructions

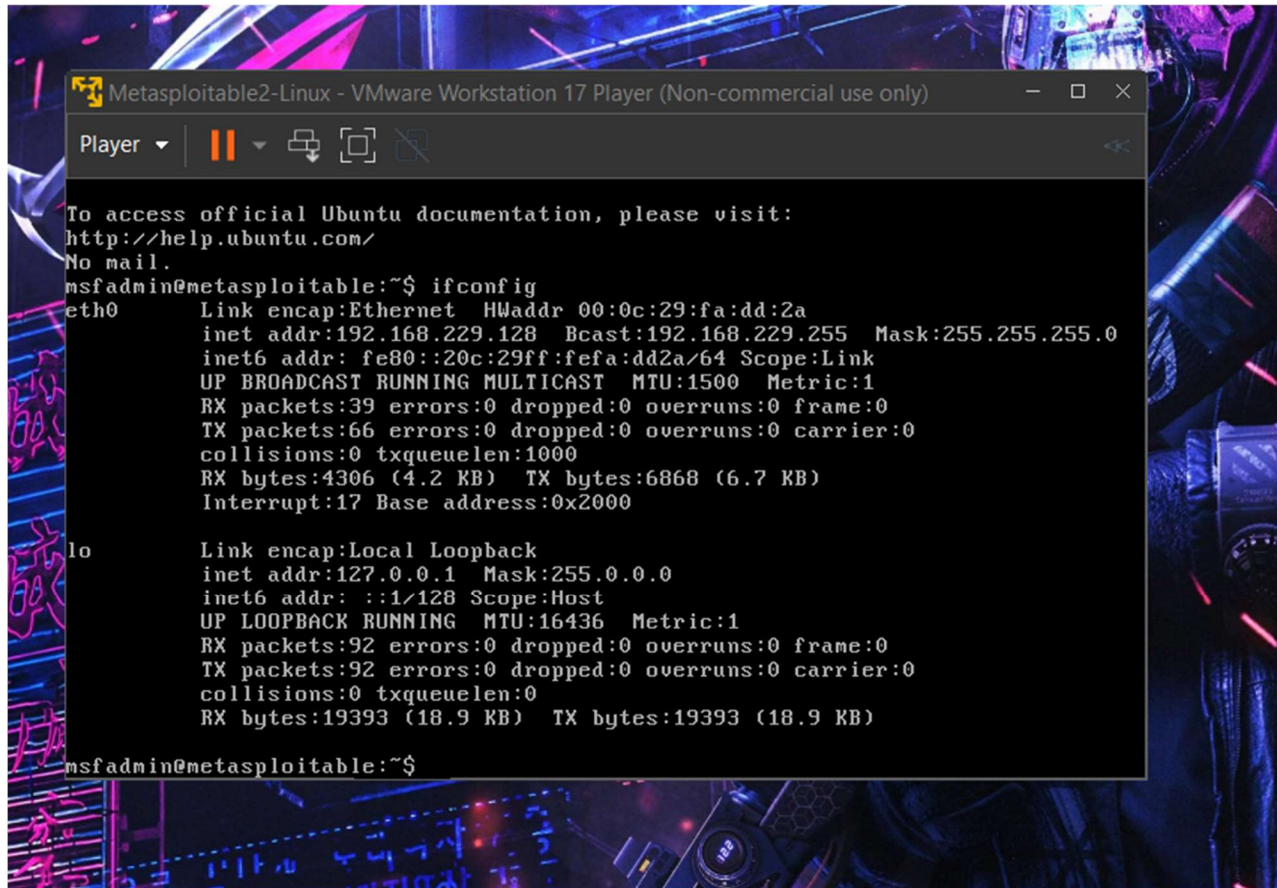
- Install Metasploitable VM;
- Enter your name and student ID above (Example: Michael Smith– 3683xxxx);
- Answer questions and add screenshots into the corresponding questions;
- Save the file on your computer for future reference;
- Save this file again as a “.pdf” file;
- Submit the PDF file with <yourname> <student ID> Lab 3 for grading.

Install Metasploitable VM as per the instruction is Part 1. No need to attach anything here for Part 1.

Moving on to Part 2

1- After logging in, type the following command and attach the screenshot here:

`Ifconfig`



The screenshot shows a terminal window titled "Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)". The terminal displays the output of the `ifconfig` command. The output shows details for the `eth0` and `lo` interfaces. The `eth0` interface is an Ethernet card with IP address `192.168.229.128` and netmask `255.255.255.0`. The `lo` interface is a local loopback with IP address `127.0.0.1` and netmask `255.0.0.0`.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa:dd:2a
          inet addr:192.168.229.128  Bcast:192.168.229.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefa:dd2a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4306 (4.2 KB)  TX bytes:6868 (6.7 KB)
          Interrupt:17 Base address:0x2000

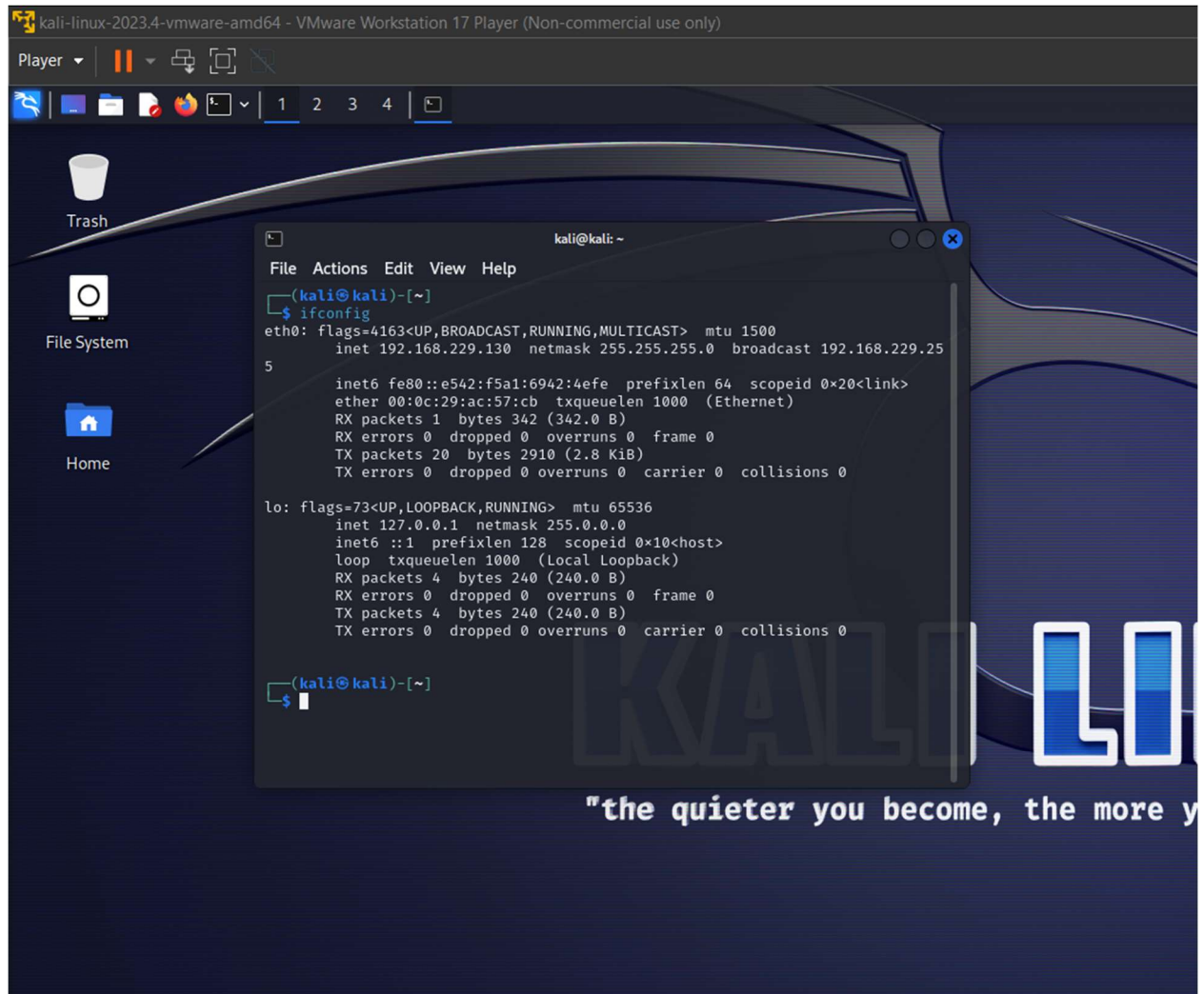
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

- 2- As per indicate in step#6 (in part 2) open Terminal Emulator and type the following command, when prompted type the root password – kali.

`ifconfig`

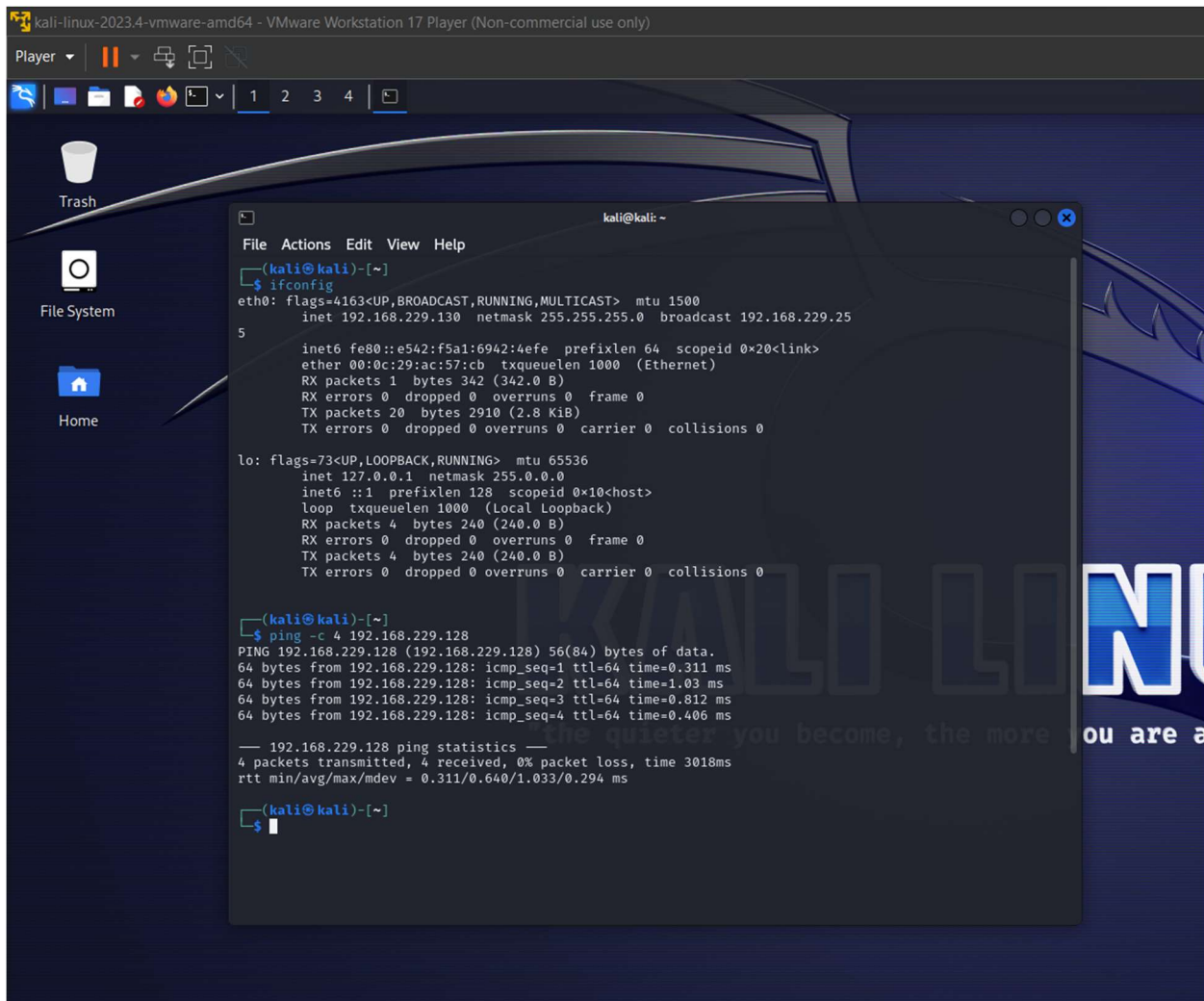
Attach the screenshot here



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the output of the 'ifconfig' command, showing details for the 'eth0' and 'lo' interfaces. The 'eth0' interface is configured with IP 192.168.229.130, netmask 255.255.255.0, and broadcast 192.168.229.255. The 'lo' interface is configured with IP 127.0.0.1 and netmask 255.0.0.0. The terminal window title is 'kali@kali: ~'.

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali)~  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.229.130 netmask 255.255.255.0 broadcast 192.168.229.255  
    5  
    inet6 fe80::e542:f5a1:6942:4efe prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:ac:57:cb txqueuelen 1000 (Ethernet)  
    RX packets 1 bytes 342 (342.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 20 bytes 2910 (2.8 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 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
kali@kali)~  
$
```

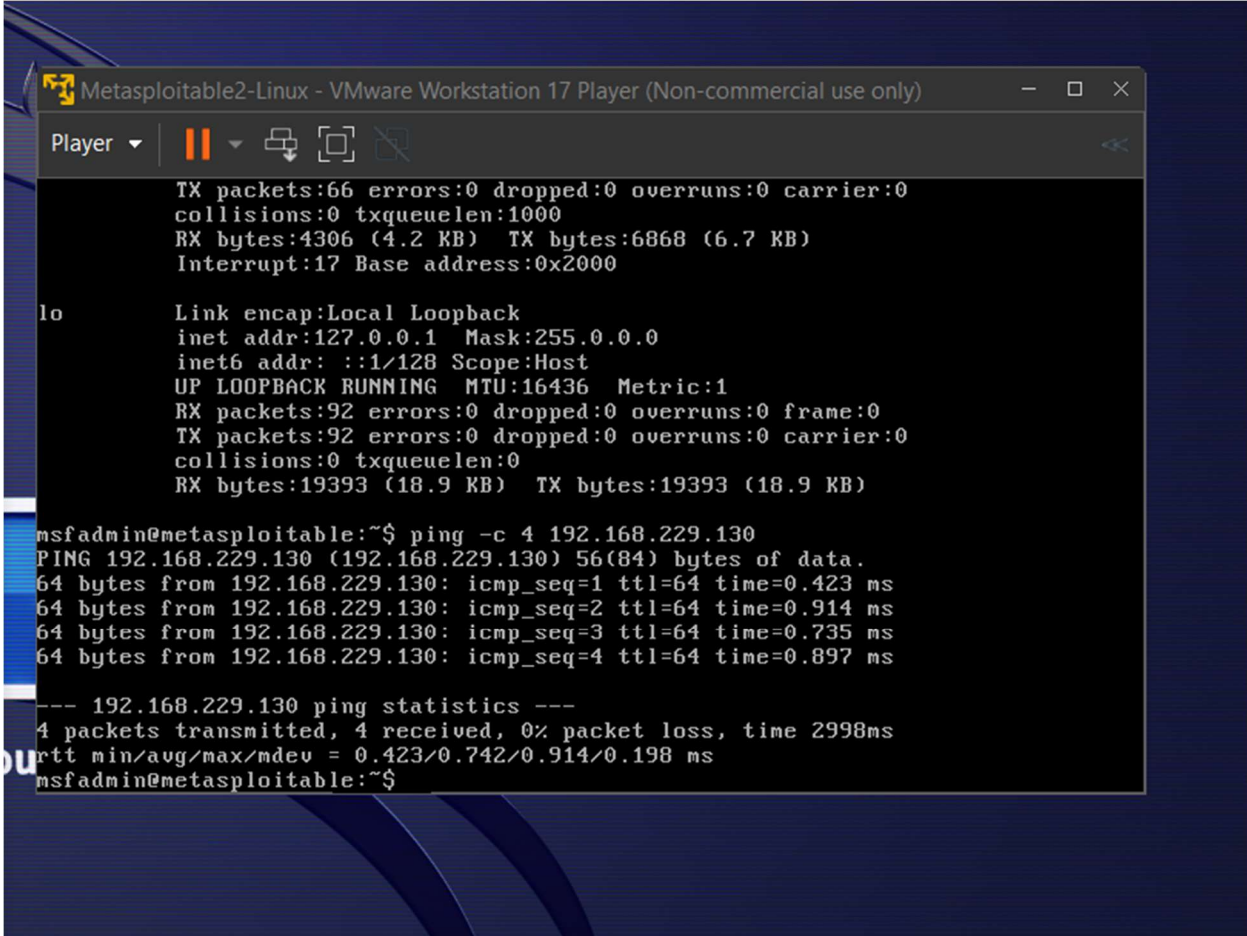
3- Ping Metasploitable from Kali and attach the screenshot below:



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the output of the `ifconfig` command, showing the configuration for the `eth0` and `lo` interfaces. The `eth0` interface is configured with IP `192.168.229.130` and netmask `255.255.255.0`. The `lo` interface is configured with IP `127.0.0.1` and netmask `255.0.0.0`. Below the configuration, the terminal shows the output of a `ping -c 4 192.168.229.128` command, which successfully pings the target IP address.

```
kali@kali: ~  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.229.130 netmask 255.255.255.0 broadcast 192.168.229.255  
    ether 00:0c:29:ac:57:cb txqueuelen 1000 (Ethernet)  
    RX packets 1 bytes 342 (342.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 20 bytes 2910 (2.8 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 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
kali@kali: ~  
$ ping -c 4 192.168.229.128  
PING 192.168.229.128 (192.168.229.128) 56(84) bytes of data:  
64 bytes from 192.168.229.128: icmp_seq=1 ttl=64 time=0.311 ms  
64 bytes from 192.168.229.128: icmp_seq=2 ttl=64 time=1.03 ms  
64 bytes from 192.168.229.128: icmp_seq=3 ttl=64 time=0.812 ms  
64 bytes from 192.168.229.128: icmp_seq=4 ttl=64 time=0.406 ms  
  
— 192.168.229.128 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3018ms  
rtt min/avg/max/mdev = 0.311/0.640/1.033/0.294 ms  
  
kali@kali: ~  
$
```

4- Ping Kali from Metasploitable and attach the screenshot below:



```
Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)
Player
TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4306 (4.2 KB) TX bytes:6868 (6.7 KB)
Interrupt:17 Base address:0x2000

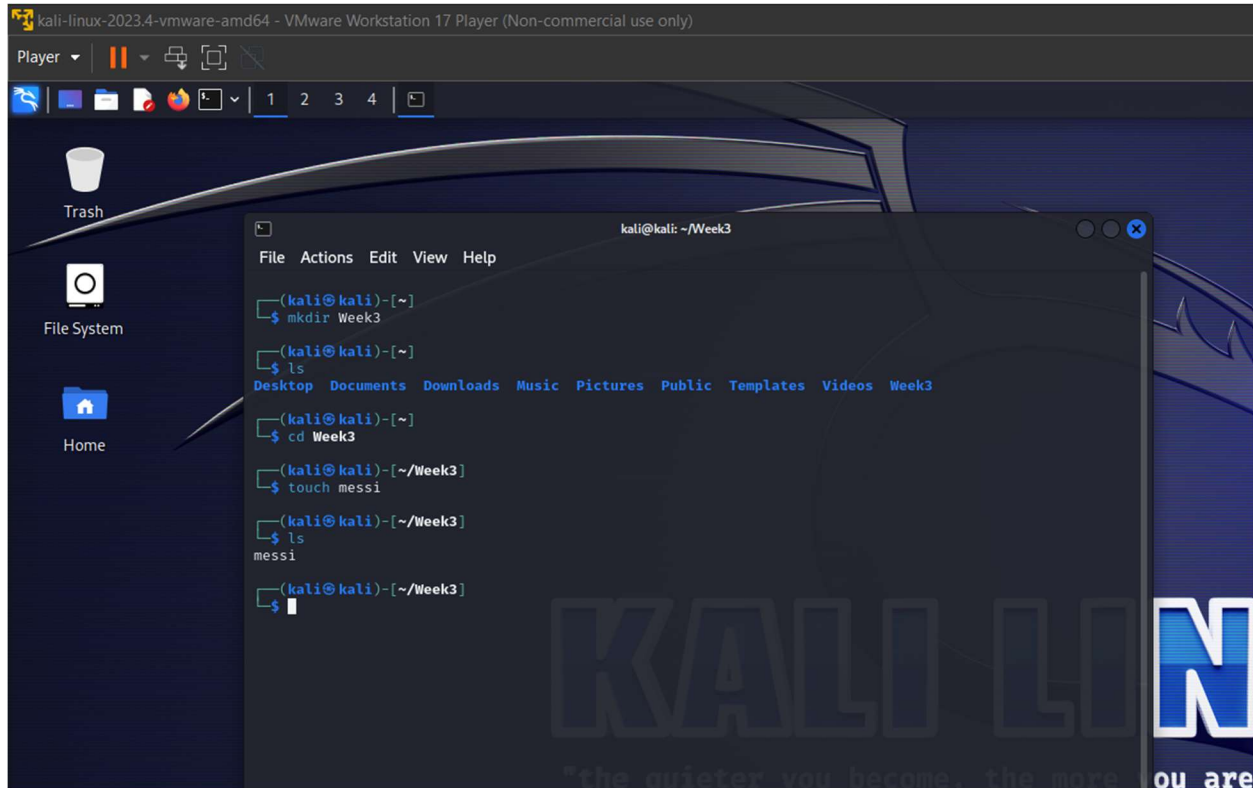
lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:92 errors:0 dropped:0 overruns:0 frame:0
      TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$ ping -c 4 192.168.229.130
PING 192.168.229.130 (192.168.229.130) 56(84) bytes of data.
64 bytes from 192.168.229.130: icmp_seq=1 ttl=64 time=0.423 ms
64 bytes from 192.168.229.130: icmp_seq=2 ttl=64 time=0.914 ms
64 bytes from 192.168.229.130: icmp_seq=3 ttl=64 time=0.735 ms
64 bytes from 192.168.229.130: icmp_seq=4 ttl=64 time=0.897 ms

--- 192.168.229.130 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.423/0.742/0.914/0.198 ms
msfadmin@metasploitable:~$
```

5- On your Kali Linux machine

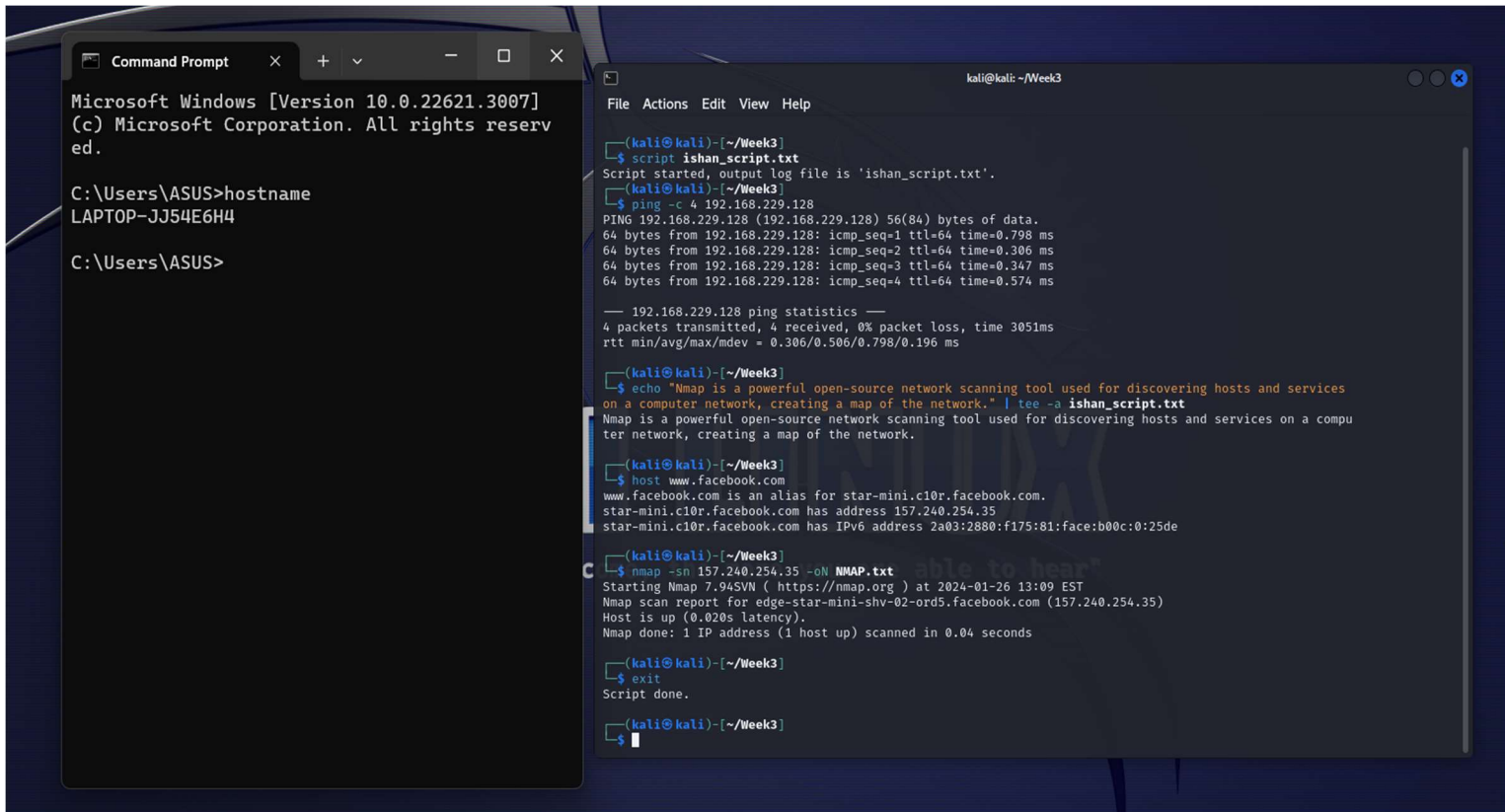
- a. Create a new directory called "Week_3"
- b. Create a new file using "touch". (take screenshot and attach here)



6- What is NMAP?

Nmap is used to scan the network. Basically, we can analyze the packets captured by Nmap and get more information. All the security professionals and experts use Nmap. Using different types of scans, we can get much more information like device discovery, Ip addresses, open ports, services & applications, version detection, etc.

- 7- Run NMAP (Ping scan) – Google for “Nmap ping scan” and output the result to “NMAP.txt”



```
Microsoft Windows [Version 10.0.22621.3007]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ASUS>hostname
LAPTOP-JJ54E6H4

C:\Users\ASUS>
```

```
kali@kali: ~/Week3
File Actions Edit View Help

(kali@kali)-[~/Week3]
$ script ishan_script.txt
Script started, output log file is 'ishan_script.txt'.
(kali@kali)-[~/Week3]
$ ping -c 4 192.168.229.128
PING 192.168.229.128 (192.168.229.128) 56(84) bytes of data:
64 bytes from 192.168.229.128: icmp_seq=1 ttl=64 time=0.798 ms
64 bytes from 192.168.229.128: icmp_seq=2 ttl=64 time=0.306 ms
64 bytes from 192.168.229.128: icmp_seq=3 ttl=64 time=0.347 ms
64 bytes from 192.168.229.128: icmp_seq=4 ttl=64 time=0.574 ms

--- 192.168.229.128 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3051ms
rtt min/avg/max/mdev = 0.306/0.506/0.798/0.196 ms

(kali@kali)-[~/Week3]
$ echo "Nmap is a powerful open-source network scanning tool used for discovering hosts and services on a computer network, creating a map of the network." | tee -a ishan_script.txt
Nmap is a powerful open-source network scanning tool used for discovering hosts and services on a computer network, creating a map of the network.

(kali@kali)-[~/Week3]
$ host www.facebook.com
www.facebook.com is an alias for star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com has address 157.240.254.35
star-mini.c10r.facebook.com has IPv6 address 2a03:2880:f175:81:face:b00c:0:25de

(kali@kali)-[~/Week3]
$ nmap -sn 157.240.254.35 -oN NMAP.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-26 13:09 EST
Nmap scan report for edge-star-mini-shv-02-ord5.facebook.com (157.240.254.35)
Host is up (0.020s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds

(kali@kali)-[~/Week3]
$ exit
Script done.

(kali@kali)-[~/Week3]
$
```

Answer the following questions:

- a. What is the ping command in Unix?

Ping command is simply used to test the other host's network reachability.

- b. What is the ping command on Windows?

Ping works same for windows as well, as it works for unix.

- c. Show the command used to ping 5 times in Unix

ping -c 5 <IP Address>

- d. Show the command used to show IP address in Unix

ifconfig

Submit your Lab



- Doublecheck all your answers.
- Save the file on your computer for future reference.
- Save the file again as a “.pdf” file.
- Submit the PDF file for grading.