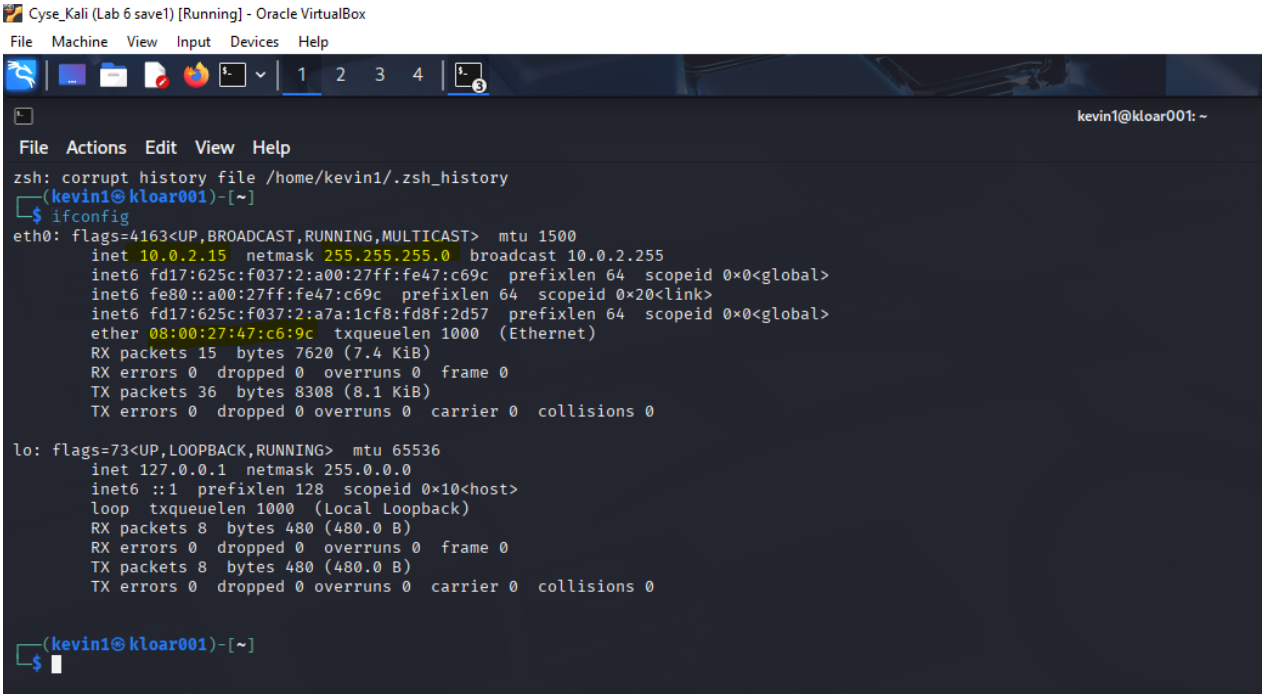
CYSE 270: Linux System for Cybersecurity

Lab 11 – Basic Network Configurations

CYSE 270: Linux System for Cybersecurity You can use either Ubuntu VM or Kali Linux VM to complete the following tasks.

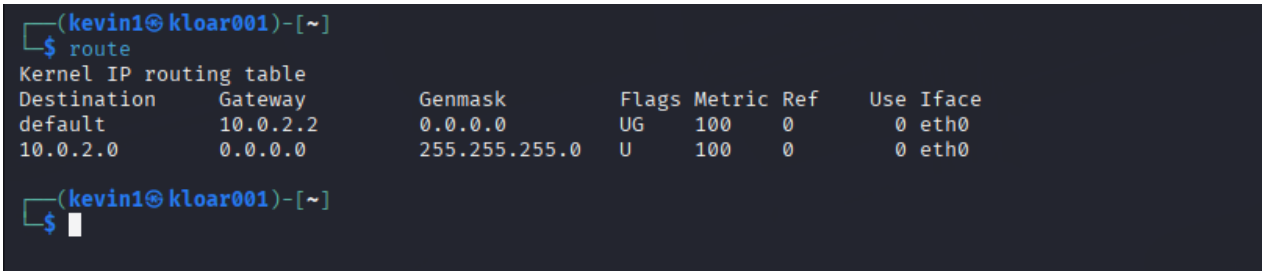
Task A – Explore Network Configurations (8 * 5 = 40 Points)
{{{{{{{{{Connect your VM in the NAT mode}}}}}}}}}

1. Use the correct **ifconfig** command to display the current network configuration. **Highlight your IP address, MAC address, and the network mask**.



With the "ifconfig" command, it displays the current network configuration.

2. Use the correct **route** command to display the current routing table.



The "route" command displays the routing table.

3. Use the **netstat** command to list current TCP connections.

```
┌──(kevin1㉿kloar001)-[~]
└─$ netstat TCP
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 10.0.2.15:bootpc        10.0.2.2:bootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     8103
unix  3      [ ]         STREAM     CONNECTED     9819
unix  3      [ ]         STREAM     CONNECTED     6865     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     8091     /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     8164     @/tmp/.ICE-unix/983
unix  3      [ ]         STREAM     CONNECTED     9036     @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     12489    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     8144     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     11320
unix  3      [ ]         STREAM     CONNECTED     8132
unix  3      [ ]         STREAM     CONNECTED     10048
unix  3      [ ]         STREAM     CONNECTED     11448    @/tmp/.ICE-unix/983
unix  3      [ ]         STREAM     CONNECTED     11319
unix  3      [ ]         STREAM     CONNECTED     9909     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     9553
unix  3      [ ]         STREAM     CONNECTED     11350
unix  3      [ ]         STREAM     CONNECTED     8093     /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     12483    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     11330
unix  3      [ ]         STREAM     CONNECTED     8081
unix  3      [ ]         STREAM     CONNECTED     12355    @/tmp/.X11-unix/X0
```

The “netstat TCP” command displays the current TCP connections.

4. Use the **ping** command to determine if the ubuntu.com system is accessible via the network. (Use the correct option to send 10 ping requests only.)

```
┌──(kevin1㉿kloar001)-[~]
└─$ ping -c 10 ubuntu.com
PING ubuntu.com (185.125.190.29) 56(84) bytes of data.
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=1 ttl=255 time=95.2 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=2 ttl=255 time=97.0 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=3 ttl=255 time=93.2 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=4 ttl=255 time=90.8 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=5 ttl=255 time=91.3 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=6 ttl=255 time=93.0 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=7 ttl=255 time=89.8 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=8 ttl=255 time=93.5 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=9 ttl=255 time=90.8 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=10 ttl=255 time=94.6 ms

── ubuntu.com ping statistics ──
10 packets transmitted, 10 received, 0% packet loss, time 9680ms
rtt min/avg/max/mdev = 89.810/92.927/97.009/2.161 ms

┌──(kevin1㉿kloar001)-[~]
```

After using the "ping" command, it displays that the 10 ping requests were transmitted.

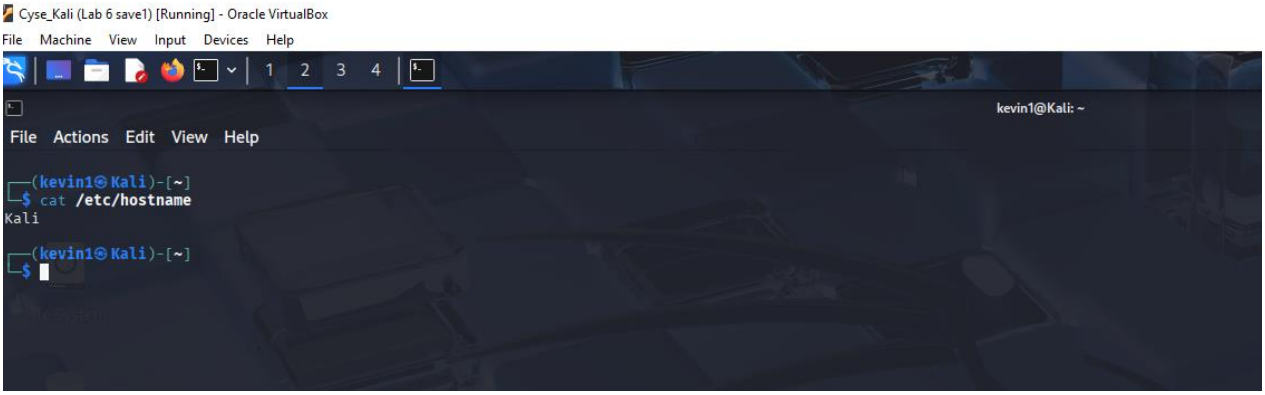
5. Use the **host** command to perform a DNS query on www.odu.edu

```
┌──(kevin1㉿kloar001)-[~]
└─$ host www.odu.edu
www.odu.edu has address 35.170.140.174

┌──(kevin1㉿kloar001)-[~]
└─$
```

After using the "host" command, it could reach its destination.

6. Use the **cat** command to display the contents of the file that contains the system's hostname.

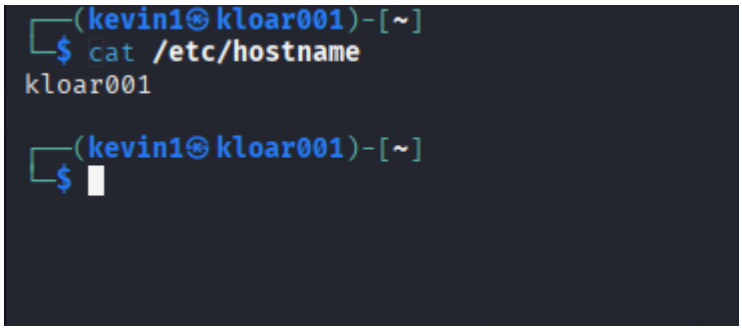


After using the "cat" command, followed by the path of the system's hostname will display the hostname.

7. 7. Use the **cat** command to display the contents of the file that contains the DNS servers for this system.

Using the "cat" command and the path of the file for the DNS server of the system, it displays the contents of it.

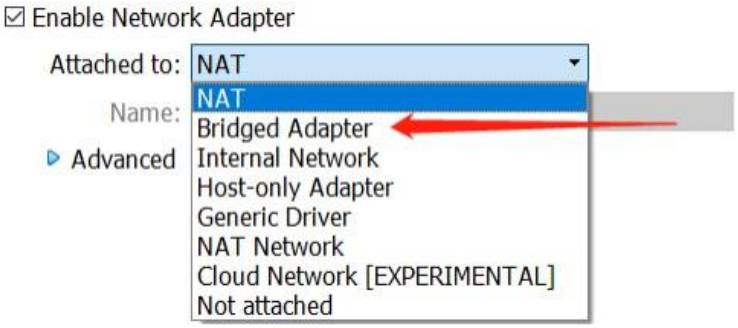
8. Edit the same file you display in the previous step, set the system's hostname to your MIDAS ID permanently. Reboot system and **repeat step 6**.

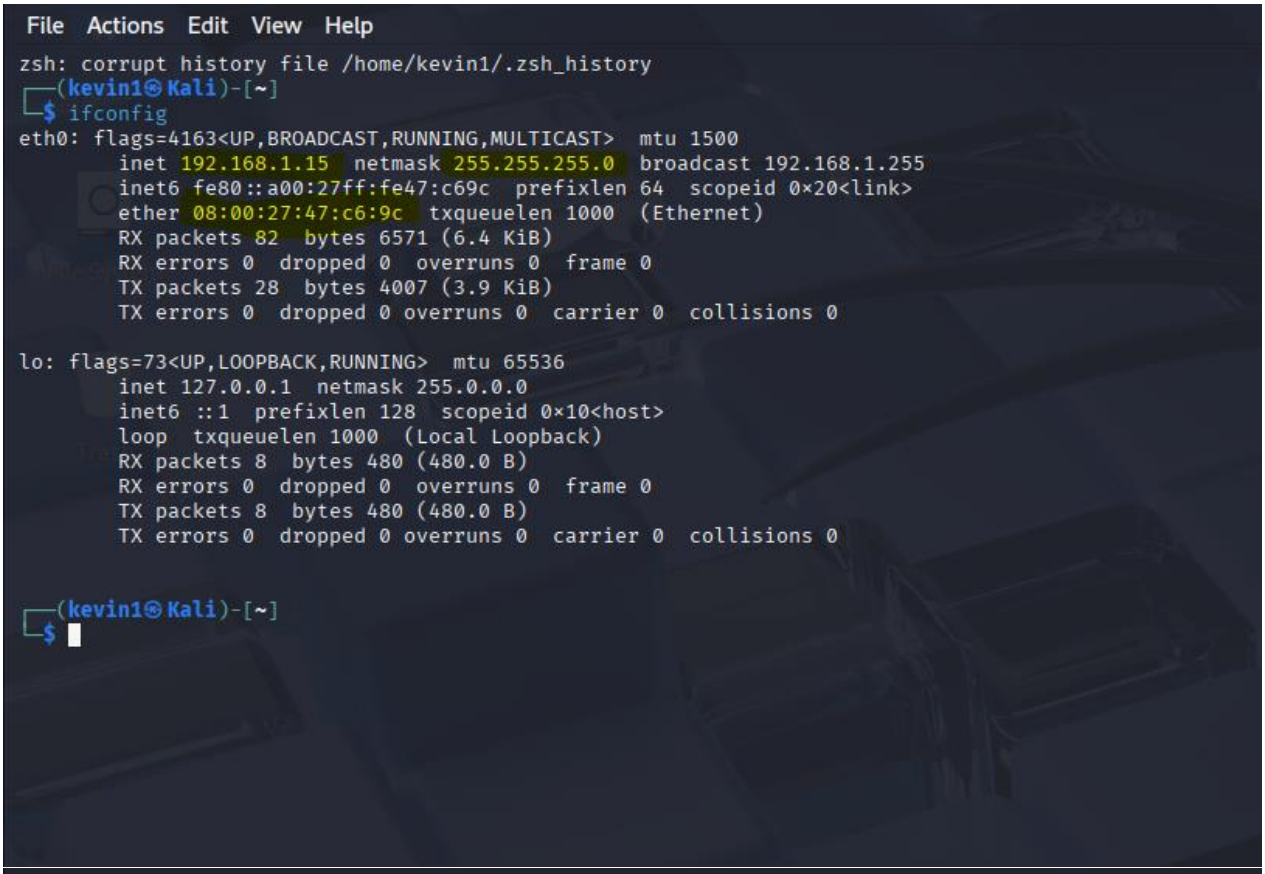


As root user (sudo) with the following "vim /etc/hostname" allows me to edit the file to my Midas ID. After changing the name and rebooting the system, the new name appears when repeating step 6.

Task B – A Different Network Setting (3 * 20 = 60 Points)

1. Change the VM network connection from NAT to the bridge mode (you will lose your Internet connection if you are connected to the ODU campus Wi-Fi network, but it is okay).
2. Reboot your system, then repeat Steps 1 – 7 in Task A.
3. Highlight the differences at the end of each step and discuss what do you find.


Enable Network Adapter
Attached to:
NAT
Name:
Advanced
NAT
Bridged Adapter
Internal Network
Host-only Adapter
Generic Driver
NAT Network
Cloud Network [EXPERIMENTAL]
Not attached




```
┌──(kevin1㉿kloar001)-[~]
└─$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.1.1     0.0.0.0         UG    100    0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0

┌──(kevin1㉿kloar001)-[~]
└─$
```

```
┌──(kevin1㉿kloar001)-[~]
└─$ netstat TCP
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 192.168.1.15:bootpc     192.168.1.1:bootps      ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     12662
unix  3      [ ]         STREAM     CONNECTED     13408
unix  3      [ ]         STREAM     CONNECTED     7897
unix  3      [ ]         STREAM     CONNECTED     11054    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     9893
unix  3      [ ]         STREAM     CONNECTED     11804
unix  3      [ ]         STREAM     CONNECTED     11494
unix  3      [ ]         STREAM     CONNECTED     4987
unix  3      [ ]         STREAM     CONNECTED     12372    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     1003     /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     15421
unix  3      [ ]         STREAM     CONNECTED     5997
unix  3      [ ]         STREAM     CONNECTED     13314
unix  3      [ ]         STREAM     CONNECTED     9771
```

```
┌──(kevin1㉿kloar001)-[~]
└─$ ping -c 10 ubuntu.com
PING ubuntu.com (185.125.190.21) 56(84) bytes of data.

— ubuntu.com ping statistics —
10 packets transmitted, 0 received, 100% packet loss, time 9201ms


┌──(kevin1㉿kloar001)-[~]
└─$
```

```
┌──(kevin1㉿kloar001)-[~]
└─$ host www.odu.edu
www.odu.edu has address 35.170.140.174

┌──(kevin1㉿kloar001)-[~]
└─$
```

```
┌──(kevin1㉿kloar001)-[~]
└─$ cat /etc/hostname
kloar001

┌──(kevin1㉿kloar001)-[~]
└─$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 192.168.1.1

┌──(kevin1㉿kloar001)-[~]
└─$
```

After repeating steps 1-7 with the network mode changed to bridged mode, there were several different changes. The addresses for the network information and the tables route have changed. Then for the ping command, ubuntu could no longer receive the ping.

Reflection

In this lab, I did basic network commands in the command line. There wasn't any challenges in this lab as the requirements to complete it were straightforward. The key concepts I learned from this lab is that it could be used for troubleshooting methods (ex. using the ping command to test if the device can communicate to the website).