Logan Gutierrez

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**.

```
┌──(lgut㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd17:625c:f037:2:7320:691f:ab8f:7b2d  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fe4a:4a3d  prefixlen 64  scopeid 0x20<link>
        inet6 fd17:625c:f037:2:a00:27ff:fe4a:4a3d  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:4a:4a:3d  txqueuelen 1000  (Ethernet)
        RX packets 11  bytes 3991 (3.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34  bytes 5394 (5.2 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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

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

```
┌──(lgut㉿kali)-[~]
└─$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.0.2.2        0.0.0.0         UG    100    0        0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

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

```
┌──(lgut㉿kali)-[~]
└─$ netstat -p TCP
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
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   PID/Program name     Path
unix  3      [ ]         STREAM     CONNECTED     9605     1164/wrapper-2.0
unix  3      [ ]         STREAM     CONNECTED     11052    926/dbus-daemon      /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     8650     932/gnome-keyring-d
unix  3      [ ]         STREAM     CONNECTED     10690    927/pipewire         /run/user/1000/pipewire-0
unix  3      [ ]         STREAM     CONNECTED     9783     926/dbus-daemon      /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     9064     -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     9618     926/dbus-daemon      /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     9797     1242/agent
unix  3      [ ]         STREAM     CONNECTED     8967     1031/VBoxClient
unix  3      [ ]         STREAM     CONNECTED     11051    1565/xdg-desktop-po
unix  3      [ ]         STREAM     CONNECTED     10722    926/dbus-daemon      /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     8678     -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     9782     1242/agent
```

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.)

```
┌──(lgut㉿kali)-[~]
└─$ 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=105 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=3 ttl=255 time=105 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=4 ttl=255 time=109 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=5 ttl=255 time=170 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=6 ttl=255 time=105 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=7 ttl=255 time=102 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=8 ttl=255 time=134 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=9 ttl=255 time=159 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=10 ttl=255 time=105 ms

── ubuntu.com ping statistics ──
10 packets transmitted, 10 received, 0% packet loss, time 9010ms
rtt min/avg/max/mdev = 95.247/118.813/169.937/24.809 ms
```

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

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

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

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

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

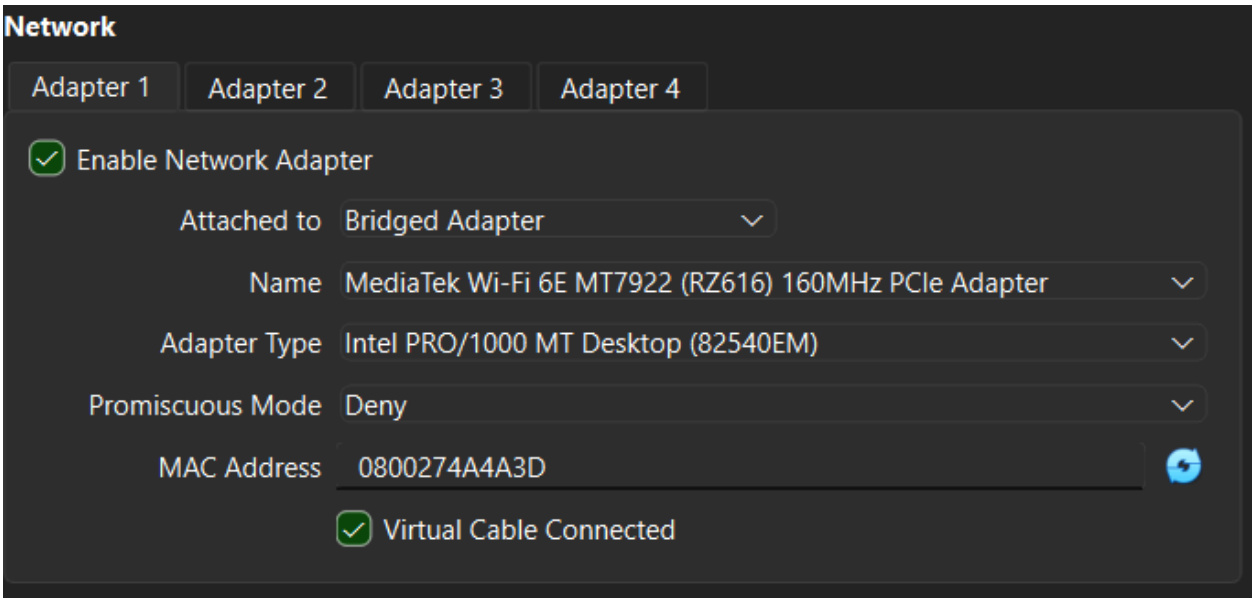
```
┌──(lgut㉿kali)-[~]
└─$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 68.105.28.11
nameserver 68.105.29.11
nameserver fd17:625c:f037:2::3
```

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**.

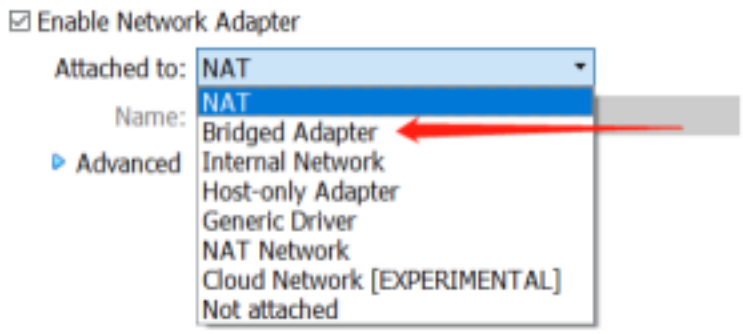
```
┌──(lgut㉿lguti005)-[~]
└─$ cat /etc/hostname
lguti005
```

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.




```
┌──(lgut㉿lguti005)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.240  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fd1f:3474:114d:10ca:a00:27ff:fe4a:4a3d  prefixlen 64  scopeid 0×0<global>
        inet6 2600:8805:5c08:2000:a00:27ff:fe4a:4a3d  prefixlen 64  scopeid 0×0<global>
        inet6 fd1f:3474:114d:10ca:40bf:2c92:c5a6:78b3  prefixlen 64  scopeid 0×0<global>
        inet6 2600:8805:5c08:2000:a2d5:396b:8c9d:3b1f  prefixlen 64  scopeid 0×0<global>
        inet6 fe80::a00:27ff:fe4a:4a3d  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:4a:4a:3d  txqueuelen 1000  (Ethernet)
        RX packets 432  bytes 65581 (64.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 685  bytes 91530 (89.3 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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The ip addresses were changed

```
┌──(lgut㉿lguti005)-[~]
└─$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.0.1     0.0.0.0         UG    100    0        0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

Route table changed due to different ips

```
┌──(lgut㉿lguti005)-[~]
└─$ netstat -p TCP
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 192.168.0.240:bootpc    192.168.0.1:bootps      ESTABLISHED -
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  3      [ ]         STREAM     CONNECTED     9307     1012/dbus-daemon     /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     10137    -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     9241     1081/xfce4-panel
unix  3      [ ]         STREAM     CONNECTED     10449    1410/obexd
unix  3      [ ]         STREAM     CONNECTED     8870     1023/at-spi2-regist
unix  3      [ ]         STREAM     CONNECTED     9529     1176/xiccd
unix  3      [ ]         STREAM     CONNECTED     8663     958/VBoxClient
unix  3      [ ]         STREAM     CONNECTED     10171    1337/gvfs-mtp-volum
unix  3      [ ]         STREAM     CONNECTED     9314     -                    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     9230     1095/wrapper-2.0
unix  3      [ ]         STREAM     CONNECTED     9570     -                    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     8574     868/dbus-daemon      /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     10462    -                    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     8869     -                    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     10379    1012/dbus-daemon     /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     10172    868/dbus-daemon      /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     9319     1109/wrapper-2.0
unix  3      [ ]         STREAM     CONNECTED     9523     -                    @/tmp/.X11-unix/X0
```

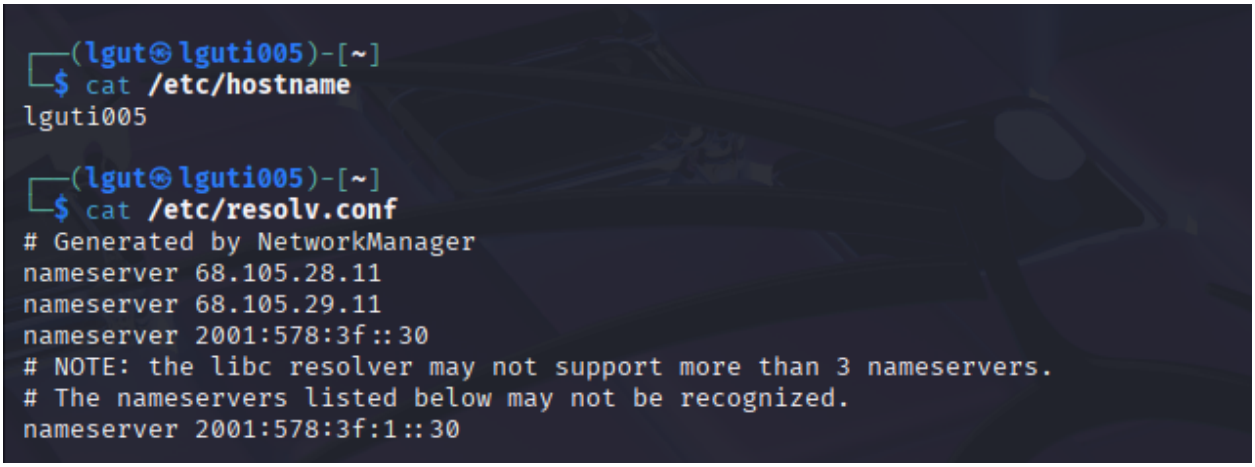
```
┌──(lgut㉿lguti005)-[~]
└─$ ping -c 10 ubuntu.com
PING ubuntu.com (2620:2d:4000:1::26) 56 data bytes

── ubuntu.com ping statistics ──
10 packets transmitted, 0 received, 100% packet loss, time 9196ms
```

The packets were not received when running the command

```
┌──(lgut㉿lguti005)-[~]
└─$ host www.odu.edu
www.odu.edu has address 35.170.140.174
```

```
┌──(lgut㉿lguti005)-[~]
└─$ cat /etc/hostname
lguti005
```

Logan Gutierrez



Has different nameservers