

## 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.**

```
(cody@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:a00:27ff:fee7:a0c prefixlen 64 scopeid 0<global>
    inet6 fd17:625c:f037:2:e480:a352:7a68:91e9 prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fee7:a0c prefixlen 64 scopeid 0<link>
    ether 08:00:27:e7:0a:0c txqueuelen 1000 (Ethernet)
    RX packets 11 bytes 3991 (3.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 34 bytes 5414 (5.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
(cody@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:a00:27ff:fee7:a0c prefixlen 64 scopeid 0<global>
    inet6 fd17:625c:f037:2:e480:a352:7a68:91e9 prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fee7:a0c prefixlen 64 scopeid 0<link>
    ether 08:00:27:e7:0a:0c txqueuelen 1000 (Ethernet)
    RX packets 11 bytes 3991 (3.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 34 bytes 5414 (5.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

```
(cody@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.

```
(cody@kali)-[~]
$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
```

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.)

```
(cody@kali)-[~]
$ ping -c 10 ubuntu.com
PING ubuntu.com (185.125.190.20) 56(84) bytes of data.

— ubuntu.com ping statistics —
10 packets transmitted, 0 received, 100% packet loss, time 9204ms
```

5. Use the **host** command to perform a DNS query on [www.odu.edu](http://www.odu.edu)

```
(cody@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.

```
(cody@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.

```
(cody@kali)-[~]  
$ cat /etc/resolv.conf  
# Generated by NetworkManager  
nameserver 68.105.28.11  
nameserver 68.105.29.11  
nameserver 68.105.28.12  
# NOTE: the libc resolver may not support more than 3 nameservers.  
# The nameservers listed below may not be recognized.  
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**.

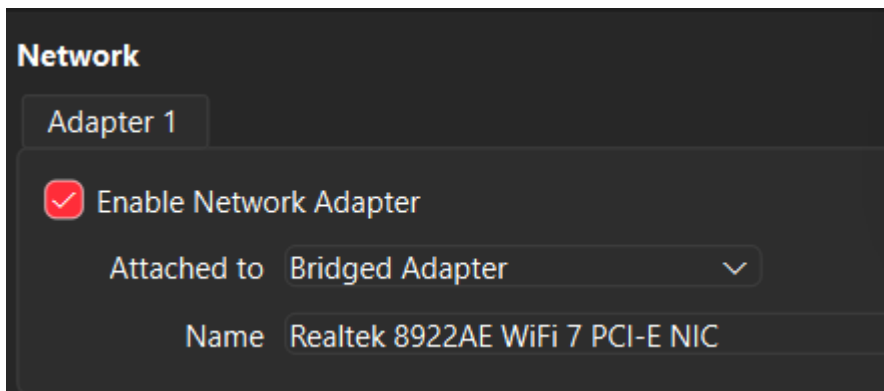
```
(cody@kali)-[~]  
$ sudo vi /etc/hosts  
[sudo] password for cody:
```

```
127.0.0.1    localhost  
127.0.1.1    cgreg017
```

```
(cody@cgreg017)-[~]  
$ cat /etc/hostname  
cgreg017
```

## **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.

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.108 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 2600:8805:1fd0:5300::82b prefixlen 128 scopeid 0<global>
    inet6 2600:8805:1fd0:5300:215e:785c:2da1:2ef prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fee7:a0c prefixlen 64 scopeid 0<link>
    inet6 2600:8805:1fd0:5300:a00:27ff:fee7:a0c prefixlen 64 scopeid 0<global>
    ether 08:00:27:e7:0a:0c txqueuelen 1000 (Ethernet)
    RX packets 69 bytes 11867 (11.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 135 bytes 19767 (19.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.108 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 2600:8805:1fd0:5300::82b prefixlen 128 scopeid 0<global>
    inet6 2600:8805:1fd0:5300:215e:785c:2da1:2ef prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fee7:a0c prefixlen 64 scopeid 0<link>
    inet6 2600:8805:1fd0:5300:a00:27ff:fee7:a0c prefixlen 64 scopeid 0<global>
    ether 08:00:27:e7:0a:0c txqueuelen 1000 (Ethernet)
    RX packets 69 bytes 11867 (11.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 135 bytes 19767 (19.3 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
```

```
(cody@cgreg017)-[~]
$ 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
```

```
(cody@cgreg017)-[~]
$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
```



```
(cody@Cgreg017)-[~]
$ 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 9197ms
```

```
(cody@Cgreg017)-[~]
$ host www.odu.edu
www.odu.edu has address 35.170.140.174
```

```
(cody@Cgreg017)-[~]
$ cat /etc/hostname
Cgreg017
```

```
(cody@Cgreg017)-[~]
$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 68.105.28.11
nameserver 68.105.29.11
nameserver 68.105.28.12
# NOTE: the libc resolver may not support more than 3 nameservers.
# The nameservers listed below may not be recognized.
nameserver 2001:578:3f::30
nameserver 2001:578:3f:1::30
```

3. Highlight the differences at the end of each step and discuss what do you find.

Ifconfig: Ip address and broadcast changed from Kali's private IP that everyone that users are defaulted too. It changed to my personal IP from COX. The Mac address stayed the same since it's my laptop's given address.

Route: the route changed since my IP changed to my ISP

Ping: The ping changed from pinging IPV4 to IPV6, I believe this happened because my Internet is IPV6 and it's trying to communicate through IPV6.

Cat /etc/resolv.conf: the unrecognized nameservers changed from private to public, but the three nameservers stayed the same.