CYSE 270: Linux System for Cybersecurity

Lab 11 – Basic Network Configurations

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**.

```
┌──(marshall㉿kali)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 10
00
    link/ether 08:00:27:1a:4f:71 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 86172sec preferred_lft 86172sec
    inet6 fe80::a00:27ff:fe1a:4f71/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(marshall㉿kali)-[~]
└─$
```

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

```
┌──(marshall㉿kali)-[~]
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         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

┌──(marshall㉿kali)-[~]
└─$
```

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

```
┌──(marshall㉿kali)-[~]
└─$ netstat -atn
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State

┌──(marshall㉿kali)-[~]
└─$
```

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.)

```
┌──(marshall㉿kali)-[~]
└─$ ping -c 10 ubuntu.com
PING ubuntu.com (185.125.190.21) 56(84) bytes of data.
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=1 ttl=51 time=
102 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=2 ttl=51 time=
109 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=3 ttl=51 time=
94.8 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=4 ttl=51 time=
95.6 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=5 ttl=51 time=
96.4 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=6 ttl=51 time=
97.2 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=7 ttl=51 time=
96.3 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=8 ttl=51 time=
94.8 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=9 ttl=51 time=
95.1 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=10 ttl=51 time
=98.1 ms

── ubuntu.com ping statistics ──
10 packets transmitted, 10 received, 0% packet loss, time 9136ms
rtt min/avg/max/mdev = 94.778/97.941/108.771/4.204 ms

┌──(marshall㉿kali)-[~]
└─$
```

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

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

┌──(marshall㉿kali)-[~]
└─$
```

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

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

┌──(marshall㉿kali)-[~]
└─$
```

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

system.

```
┌──(marshall㉿kali)-[~]
└─$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 68.105.28.11
nameserver 68.105.29.11
nameserver 68.105.28.12

┌──(marshall㉿kali)-[~]
└─$
```

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**.

```
File  Actions  Edit  View  Help
  ┌──(marshall㉿mbrow096)-[~]
  └─$ cat /etc/hostname
mbrow096

  ┌──(marshall㉿mbrow096)-[~]
  └─$ ▮
```

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).
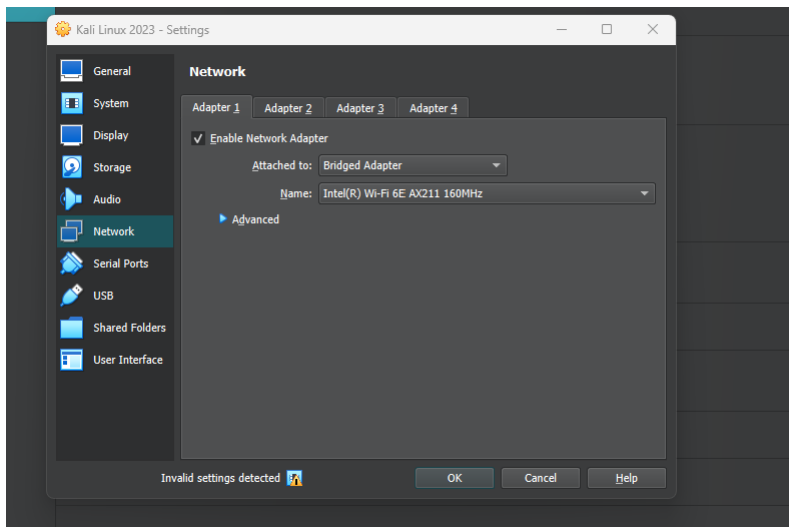
2. Reboot your system, then repeat Steps 1 – 7 in Task A.


```
File  Actions  Edit  View  Help
  ┌──(marshall㉿mbrow096)-[~]
  └─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group defau
lt qlen 1000
    link/ether 08:00:27:1a:4f:71 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.183/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
       valid_lft 172756sec preferred_lft 172756sec
    inet6 2600:8805:4006:d400:5e6b:2fd4:9261:eebc/64 scope global temporary dynamic
       valid_lft 300sec preferred_lft 300sec
    inet6 2600:8805:4006:d400:a00:27ff:fe1a:4f71/64 scope global dynamic mngtmpaddr nop
refixroute
       valid_lft 300sec preferred_lft 300sec
    inet6 fe80::a00:27ff:fe1a:4f71/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

  ┌──(marshall㉿mbrow096)-[~]
  └─$ ▮
```

```
                  valid_lft forever preferred_lft forever
┌──(marshall㉿mbrow096)-[~]
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         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

┌──(marshall㉿mbrow096)-[~]
└─$
```

```
┌──(marshall㉿mbrow096)-[~]
└─$ netstat -atn
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State

┌──(marshall㉿mbrow096)-[~]
└─$
```

```
┌──(marshall㉿mbrow096)-[~]
└─$ ping -c 10 ubuntu.com
PING ubuntu.com(website-content-cache-1.canonical.com (2620:2d:4000:1::26)) 56 data byt
es

── ubuntu.com ping statistics ──
10 packets transmitted, 0 received, 100% packet loss, time 9855ms

┌──(marshall㉿mbrow096)-[~]
└─$
```

```
┌──(marshall㉿mbrow096)-[~]
└─$ host www.odu.edu
www.odu.edu has address 35.170.140.174

┌──(marshall㉿mbrow096)-[~]
└─$
```

```
┌──(marshall㉿mbrow096)-[~]
└─$ cat /etc/hostname
mbrow096

┌──(marshall㉿mbrow096)-[~]
└─$
```

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