Kirk Turner

CYSE 270: Linux System for Cybersecurity

Lab 11 – Basic Network Configurations

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**.

```
┌──(kirk-turner㉿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 fe80::a00:27ff:fe74:f488  prefixlen 64  scopeid 0x20<link>
        inet6 fd17:625c:f037:2:8d51:d5d2:71b2:9c86  prefixlen 64  scopeid 0x0<global>
        inet6 fd17:625c:f037:2:a00:27ff:fe74:f488  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:74:f4:88  txqueuelen 1000  (Ethernet)
        RX packets 9  bytes 3699 (3.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 4974 (4.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

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

```
┌──(kirk-turner㉿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.

```
┌──(kirk-turner㉿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.)

```
┌──(kirk-turner㉿kali)-[~]
└─$ ping -c 10 ubuntu.com
PING ubuntu.com (185.125.190.20) 56(84) bytes of data.
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=1 ttl=255 time=84.9 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=2 ttl=255 time=85.2 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=3 ttl=255 time=84.3 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=4 ttl=255 time=84.9 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=5 ttl=255 time=84.7 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=6 ttl=255 time=83.9 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=7 ttl=255 time=85.4 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=8 ttl=255 time=85.1 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=9 ttl=255 time=86.8 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=10 ttl=255 time=84.6 ms

── ubuntu.com ping statistics ──
10 packets transmitted, 10 received, 0% packet loss, time 9011ms
rtt min/avg/max/mdev = 83.873/84.977/86.812/0.744 ms
```

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

```
┌──(kirk-turner㉿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.

```
┌──(kirk-turner㉿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.

```
┌──(kirk-turner㉿kali)-[~]
└─$ cat /etc/resolv.conf
# Generated by NetworkManager
search home.local
nameserver 10.0.2.3
```

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**.

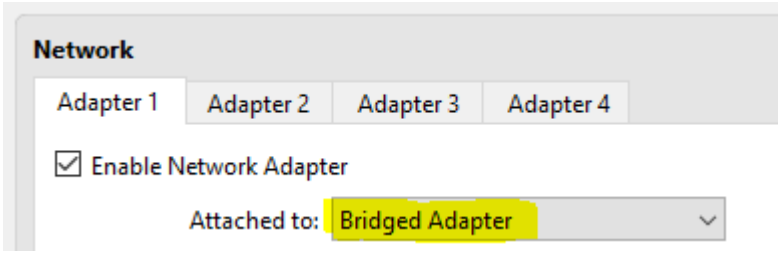
```
┌──(kirk-turner㉿kali)-[~]
└─$ sudo vi /etc/hostname
[sudo] password for kirk-turner:
```

```
┌──(kirk-turner㉿kturn038)-[~]
└─$ cat /etc/hostname
kturn038
```

Kirk Turner

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

Step A.1 (repeated)

```
┌──(kirk-turner㉿kturn038)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.213  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe74:f488  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:74:f4:88  txqueuelen 1000  (Ethernet)
        RX packets 22  bytes 3192 (3.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34  bytes 5166 (5.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

When running the ifconfig command while having my network connection in bridge mode, I noticed that my IP address had changed from 10.0.2.15 to 192.168.1.213.

Step A.2 (repeated)

```
┌──(kirk-turner㉿kturn038)-[~]
└─$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         router.home.loc 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
```

Running the route command changed one destination from 10.0.2.0 to 192.168.1.0, and it also changed one of the gateways from 10.0.2.2 to router.home.loc.

Step A.3 (repeated)

```
┌──(kirk-turner㉿kturn038)-[~]
└─$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

No difference in this step.

Step A.4 (repeated)

```
┌──(kirk-turner㉿kturn038)-[~]
└─$ ping -c 10 ubuntu.com
PING ubuntu.com (185.125.190.20) 56(84) bytes of data.
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=1 ttl=53 time=85.8 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=2 ttl=53 time=85.0 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=3 ttl=53 time=84.5 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=4 ttl=53 time=85.1 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=5 ttl=53 time=85.8 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=6 ttl=53 time=84.4 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=7 ttl=53 time=85.6 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=8 ttl=53 time=84.5 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=9 ttl=53 time=85.3 ms
64 bytes from website-content-cache-1.ps5.canonical.com (185.125.190.20): icmp_seq=10 ttl=53 time=84.4 ms

── ubuntu.com ping statistics ──
10 packets transmitted, 10 received, 0% packet loss, time 9009ms
rtt min/avg/max/mdev = 84.368/85.028/85.823/0.548 ms
```

No difference in this step.

Step A.5 (repeated)

```
┌──(kirk-turner㉿kturn038)-[~]
└─$ host www.odu.edu
www.odu.edu has address 35.170.140.174
```

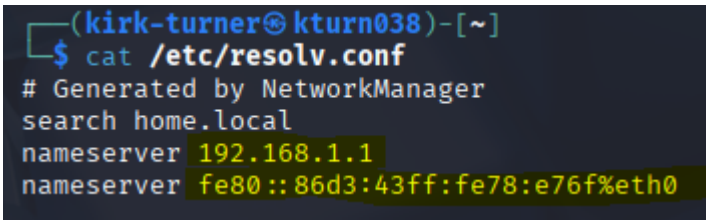
No difference in this step.

Step A.6 (repeated)

```
┌──(kirk-turner㉿kturn038)-[~]
└─$ cat /etc/hostname
kturn038
```

No difference in this step.

Step A.7 (repeated)



In this step, the first nameserver entry had a different IP address (changing from 10.0.2.3 to 192.168.1.1) and had an additional nameserver entry providing an IPv6 address.