

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.**

```
(pmacm001@kali-270)-[~]
└─$ 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:fe02:a4f prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:02:0a:4f txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 590 (590.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 23 bytes 3100 (3.0 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 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

```
(pmacm001@kali-270)-[~]
└─$ 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.

```
(pmacm001@kali-270)-[~]
└─$ netstat
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 20057 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 20718 /run/dbus/system_bus_socket
unix 3 [ ] STREAM CONNECTED 20100
unix 3 [ ] STREAM CONNECTED 20646 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 19735 @/tmp/.X11-unix/X0
unix 3 [ ] STREAM CONNECTED 20033
unix 2 [ ] DGRAM CONNECTED 17818
unix 3 [ ] STREAM CONNECTED 20667 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 20779 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 20237
unix 3 [ ] STREAM CONNECTED 20050
unix 3 [ ] STREAM CONNECTED 19369
unix 3 [ ] STREAM CONNECTED 17828 /run/dbus/system_bus_socket
unix 3 [ ] STREAM CONNECTED 17238 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 17182 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 17343
unix 3 [ ] STREAM CONNECTED 20215
unix 3 [ ] STREAM CONNECTED 20617 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 21057 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 20471 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 20127 @/tmp/.ICE-unix/943
unix 3 [ ] STREAM CONNECTED 19826
unix 3 [ ] STREAM CONNECTED 19425 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 19949 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 20089 @/tmp/.ICE-unix/943
unix 3 [ ] STREAM CONNECTED 20376 @/tmp/.ICE-unix/943
unix 3 [ ] STREAM CONNECTED 19686
unix 3 [ ] STREAM CONNECTED 20417 @/tmp/.X11-unix/X0
unix 3 [ ] STREAM CONNECTED 20374 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 20020 @/tmp/.X11-unix/X0
```

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.)

```
(pmacm001@kali-270)-[~]
$ ping -c 10 www.ubuntu.com
PING www.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=55 time=111 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=2 ttl=55 time=119 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=3 ttl=55 time=137 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=4 ttl=55 time=98.8 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=5 ttl=55 time=127 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=6 ttl=55 time=93.5 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=7 ttl=55 time=96.6 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=8 ttl=55 time=100 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=9 ttl=55 time=94.8 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=10 ttl=55 time=104 ms

--- www.ubuntu.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9006ms
rtt min/avg/max/mdev = 93.530/108.218/136.719/14.122 ms
```

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

```
(pmacm001@kali-270)-[~]
$ 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.

```
(pmacm001@kali-270)-[~]
$ cat /etc/hostname
kali-270
```

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

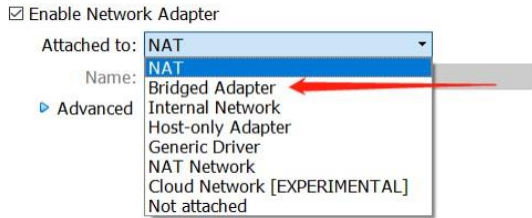
```
(pmacm001@kali-270)-[~]
$ cat /etc/resolv.conf
# Generated by NetworkManager
search fios-router.home
nameserver 192.168.1.1
```

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.**

```
(pmacm001@pmacm001)-[~]
$ cat /etc/hostname
pmacm001
```

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.



Step 1: We can clearly see that the network/ip address has changed from part A.

```

(pmacm001@pmacm001)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.176 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe02:a4f prefixlen 64 scopeid 0<link>
    ether 08:00:27:02:0a:4f txqueuelen 1000 (Ethernet)
    RX packets 125 bytes 38292 (37.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 44 bytes 14142 (13.8 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<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
  
```

Step 2: We see that the gateway has changed when compared to part A.

```

(pmacm001@pmacm001)-[~]
└─$ route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default Fios_Quantum_Ga 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
  
```

Step 3: We notice that both the local and foreign addresses change to reflect the change in network adapter.

```

(pmacm001@pmacm001)-[~]
└─$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
udp 0 0 pmacm001.fios-ro:bootpc Fios_Quantum_Gat:bootps ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags Type State I-Node Path
unix 3 [ ] STREAM CONNECTED 19353
unix 3 [ ] STREAM CONNECTED 17059 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 19753 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 20425
unix 2 [ ] DGRAM 19979
unix 3 [ ] STREAM CONNECTED 20477 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 20631
unix 3 [ ] STREAM CONNECTED 20103 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 19683 /run/user/1000/bus
unix 2 [ ] DGRAM 17437
unix 3 [ ] DGRAM CONNECTED 16028
unix 3 [ ] STREAM CONNECTED 19806
unix 3 [ ] STREAM CONNECTED 20051
unix 3 [ ] STREAM CONNECTED 18630
unix 3 [ ] STREAM CONNECTED 19857 /run/user/1000/pipewire-0
unix 3 [ ] STREAM CONNECTED 19645 /run/user/1000/at-spi-bu
s_0
unix 3 [ ] STREAM CONNECTED 20271
unix 3 [ ] STREAM CONNECTED 19612 @/tmp/.ICE-unix/865
unix 3 [ ] STREAM CONNECTED 19358
unix 3 [ ] STREAM CONNECTED 18953 /run/user/1000/bus
unix 2 [ ] DGRAM 18632
unix 3 [ ] STREAM CONNECTED 19723
  
```

Step 4: Nothing of note here, output of ping command looks the same as part A.

```
(pmacm001@pmacm001)-[~]
--$ ping -c 10 www.ubuntu.com
PING www.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=58 time=94.6 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=2 ttl=58 time=99.1 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=3 ttl=58 time=91.7 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=4 ttl=58 time=95.1 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=5 ttl=58 time=95.7 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=6 ttl=58 time=88.9 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=7 ttl=58 time=92.2 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=8 ttl=58 time=90.6 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=9 ttl=58 time=92.7 ms
64 bytes from website-content-cache-2.ps5.canonical.com (185.125.190.21): icmp_seq=10 ttl=58 time=95.2 ms

-- www.ubuntu.com ping statistics --
10 packets transmitted, 10 received, 0% packet loss, time 9010ms
rtt min/avg/max/mdev = 88.909/94.185/99.085/2.731 ms
```

Steps 5 & 6: Main difference is that the host name was changed from kali-270 to pmacm001

```
(pmacm001@pmacm001)-[~]
--$ host www.odu.edu
www.odu.edu has address 35.170.140.174

(pmactm001@pmacm001)-[~]
--$ cat /etc/hostname
pmacm001
```

Step 7: No change from part A.

```
(pmacm001@pmacm001)-[~]
--$ cat /etc/resolv.conf
# Generated by NetworkManager
search fios-router.home
nameserver 192.168.1.1
```