Old Dominion University
Major: Cybersecurity
Name: Michael Greene
ID: 01213114

CYSE 270: Linux System for Cybersecurity

Lab 12 – Advanced Network configurations

Old Dominion University
Major: Cybersecurity
Name: Michael Greene
ID: 01213114

Scenario: You, as a network admin, are going to set up your Ubuntu VM as a gateway to provide Internet access to another client Ubuntu VM. The client VM needs to be in the same internal network as the gateway (**as shown in Figure 1**). Once the connection is ready, you need to configure the firewall to secure the network properly. The following requirements need to be satisfied to receive full credits.

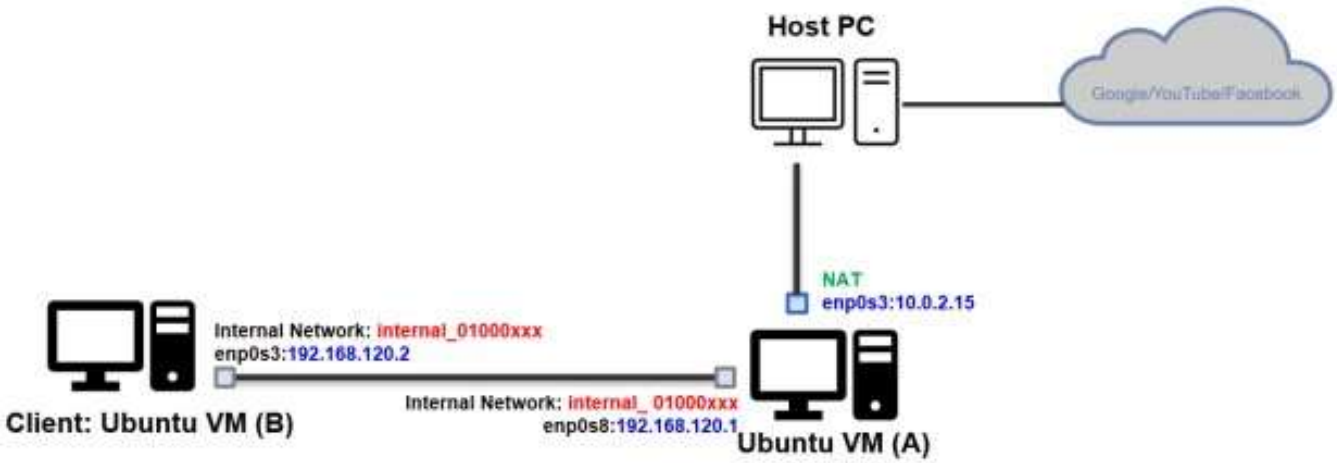


Figure 1 Desired Network Topology

Please note that you need to customize the value in the fields marked in RED above.

Please configure the network with the following requirement:

Old Dominion University
Major: Cybersecurity
Name: Michael Greene
ID: 01213114

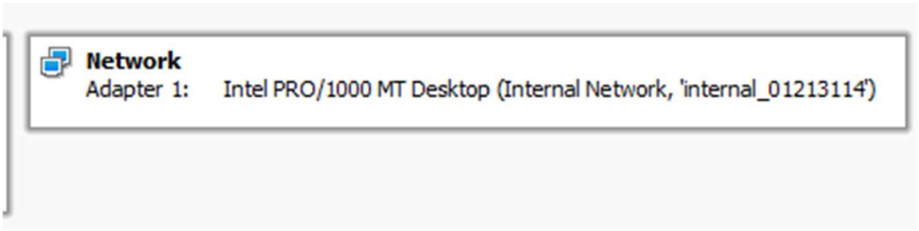
Task A –Network Configuration (**60 points**)

1. In the virtual box setting, connect two VMs in the same internal network, “internal_{UIN}”.

Replace {UIN} with your real UIN.

VM(A)

VM(B)



2. Change the hostname of the Client VM to “{MIDAS}-Client.” **Replace {MIDAS} with your real MIDAS.**

```
michael@michael-VirtualBox:~$ sudo hostnamectl set-hostname mgree034-Client
[sudo] password for michael:
michael@michael-VirtualBox:~$ hostnamectl
 Static hostname: mgree034-Client
       Icon name: computer-vm
         Chassis: vm
      Machine ID: 712e59fb681945e1871ab56ab879231d
         Boot ID: 56b61b4dc37e48278402f6878e1eb4d6
  Virtualization: oracle
Operating System: Ubuntu 22.04.1 LTS
          Kernel: Linux 5.15.0-47-generic
    Architecture: x86-64
 Hardware Vendor: innotek GmbH
  Hardware Model: VirtualBox
```

Old Dominion University
Major: Cybersecurity
Name: Michael Greene
ID: 01213114

3. Configure the temporary IP address on the Gateway Ubuntu, as shown in Figure 1.

```
michael@michael-VirtualBox:~$ sudo ifconfig enp0s8 192.168.120.1
[sudo] password for michael:
michael@michael-VirtualBox:~$ ifconfig
enp0s3: 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::eb83:3690:aaf2:fee7  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1b:68:af  txqueuelen 1000  (Ethernet)
        RX packets 240892  bytes 359460134 (359.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20986  bytes 1325160 (1.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.120.1  netmask 255.255.255.0  broadcast 192.168.120.255
        inet6 fe80::ba22:f26f:2967:cec5  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:3a:70:4e  txqueuelen 1000  (Ethernet)
        RX packets 58  bytes 12315 (12.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 124  bytes 20421 (20.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

4. Configure the temporary IP address, routing table, and DNS server on Client VM as shown in Figure 1.

```
michael@mgree034-Client:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.120.2  netmask 255.255.255.0  broadcast 192.168.120.255
        inet6 fe80::a00:27ff:fe05:f94b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:05:f9:4b  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 77  bytes 9030 (9.0 KB)
        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 148  bytes 12668 (12.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 148  bytes 12668 (12.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Old Dominion University
Major: Cybersecurity
Name: Michael Greene
ID: 01213114

```
michael@mgree034-Client:~$ sudo route add default gw 192.168.120.1
[sudo] password for michael:
michael@mgree034-Client:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.120.1   0.0.0.0         UG    0      0        0 enp0s3
```

```
michael@mgree034-Client:~$ ping 192.168.120.1
PING 192.168.120.1 (192.168.120.1) 56(84) bytes of data.
64 bytes from 192.168.120.1: icmp_seq=1 ttl=64 time=0.193 ms
64 bytes from 192.168.120.1: icmp_seq=2 ttl=64 time=0.199 ms
64 bytes from 192.168.120.1: icmp_seq=3 ttl=64 time=0.222 ms
^C
--- 192.168.120.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2026ms
rtt min/avg/max/mdev = 0.193/0.204/0.222/0.012 ms
```

```
michael@mgree034-Client:~$ sudo vi /etc/resolv.conf
michael@mgree034-Client:~$ tail -3 /etc/resolv.conf
nameserver 8.8.8.8
options edns0 trust-ad
search .
```

5. Configure gateway Ubuntu to forward the traffic (also NAT configuration) from the Client to the Internet.

```
michael@michael-VirtualBox:~$ sudo iptables -t nat -A POSTROUTING -o enp0s3 -j
MASQUERADE
michael@michael-VirtualBox:~$ sudo iptables -A FORWARD -i enp0s3 -o enp0s8 -m s
tate --state RELATED,ESTABLISHED -j ACCEPT
michael@michael-VirtualBox:~$ sudo iptables -A FORWARD enp0s8 -o enp0s3 -j ACCE
PT
Bad argument `enp0s8'
Try `iptables -h' or 'iptables --help' for more information.
michael@michael-VirtualBox:~$ sudo iptables -A FORWARD -i enp0s8 -o enp0s3 -j A
CCEPT
```

```
michael@michael-VirtualBox:~$ su root
Password:
root@michael-VirtualBox:/home/michael# echo 1 >/proc/sys/net/ipv4/ip_forward
root@michael-VirtualBox:/home/michael# cat >/proc/sys/net/ipv4/ip_forward
```

Old Dominion University
Major: Cybersecurity
Name: Michael Greene
ID: 01213114

6. Test your ping connection to 8.8.8.8 and www.google.com, respectively.

```
michael@mgree034-Client:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=37.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=37.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=44.9 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=112 time=34.5 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 34.535/38.679/44.882/3.800 ms
michael@mgree034-Client:~$ ping www.google.com
PING www.google.com (142.250.189.100) 56(84) bytes of data.
64 bytes from atl26s29-in-f4.1e100.net (142.250.189.100): icmp_seq=1 ttl=112 ti
me=38.8 ms
64 bytes from atl26s29-in-f4.1e100.net (142.250.189.100): icmp_seq=2 ttl=112 ti
me=39.6 ms
64 bytes from atl26s29-in-f4.1e100.net (142.250.189.100): icmp_seq=3 ttl=112 ti
me=34.1 ms
64 bytes from atl26s29-in-f4.1e100.net (142.250.189.100): icmp_seq=4 ttl=112 ti
me=37.6 ms
64 bytes from atl26s29-in-f4.1e100.net (142.250.189.100): icmp_seq=5 ttl=112 ti
me=47.6 ms
64 bytes from atl26s29-in-f4.1e100.net (142.250.189.100): icmp_seq=6 ttl=112 ti
me=36.6 ms
```

Task B –Firewall Configuration (**40 points**)

1. Configure the iptables on the gateway Ubuntu to block all the inbound ICMP packets from the Client VM.

```
michael@michael-VirtualBox:~$ sudo iptables -A INPUT -s 192.168.120.2 -p icmp -
j DROP
```

2. Configure the iptables on the gateway Ubuntu to block all the outbound ICMP packets that originated from the gateway Ubuntu itself.

```
michael@michael-VirtualBox:~$ sudo iptables -A OUTPUT -d 192.168.120.1 -p icmp
-j DROP
```

Extra credit:

Set the permanent IP address on the Client Ubuntu based on the above network topology.

```
michael@mgree034-Client:~$ sudo vim /etc/netplan/01-network-manager-all.yaml
```

Old Dominion University
Major: Cybersecurity
Name: Michael Greene
ID: 01213114

```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4:no
    addresses:
      - 192.168.120.2/24
    gateway4: 192.168.120.1
    nameservers: [8.8.8.8]
```