Submission Week # 2
SNSkies

Muhammad Usman

Task 1

Library   ✕

🔍 Type here to search   ▼

⊟ 🖥 My Computer
    📋 kali-linux-2025.2-vmware
    📋 Ubuntu Admin 64-bit
    📋 Ubuntu Server 64 bit
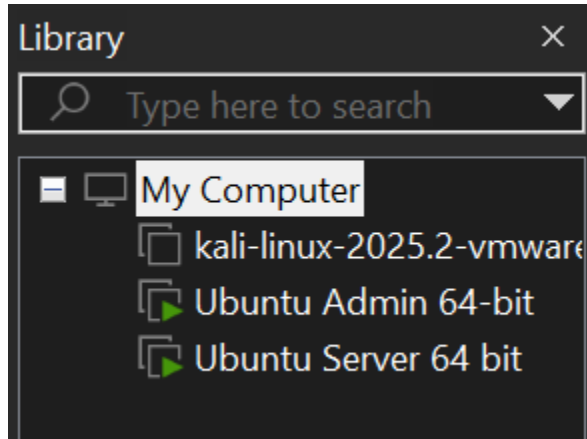
Admin VM

```
usman@usman-virtual-machine: ~/Desktop

usman@usman-virtual-machine:~/Desktop$ sudo cat /etc/netplan/*.yaml
[sudo] password for usman:
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens33:
      addresses:
        - 192.168.56.20/24
      routes:
        - to: default
          via: 192.168.56.1
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
usman@usman-virtual-machine:~/Desktop$
```

```
usman@usman-virtual-machine: ~/Desktop

usman@usman-virtual-machine:~/Desktop$ ip a
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
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:0c:c9:79 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.56.20/24 brd 192.168.56.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe0c:c979/64 scope link
       valid_lft forever preferred_lft forever
```

Server VM

```
usman@usman:~$ sudo cat /etc/netplan/*.yaml
[sudo] password for usman:
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  version: 2
  ethernets:
    ens33:
      addresses:
        - 192.168.56.10/24
      routes:
        - to: default
          via: 192.168.56.1
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]

usman@usman:~$ _
```

```
usman@usman:~$ ip a
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
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:6b:05:fa brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.56.10/24 brd 192.168.56.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe6b:5fa/64 scope link
       valid_lft forever preferred_lft forever
```

Verify with ip a and cross-VM ping

Server to Admin

```
usman@usman:~$ ping 192.168.56.20
PING 192.168.56.20 (192.168.56.20) 56(84) bytes of data.
64 bytes from 192.168.56.20: icmp_seq=1 ttl=64 time=1.38 ms
64 bytes from 192.168.56.20: icmp_seq=2 ttl=64 time=2.22 ms
64 bytes from 192.168.56.20: icmp_seq=3 ttl=64 time=2.46 ms
64 bytes from 192.168.56.20: icmp_seq=4 ttl=64 time=2.47 ms
64 bytes from 192.168.56.20: icmp_seq=5 ttl=64 time=2.51 ms
^C
--- 192.168.56.20 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 1.383/2.208/2.514/0.425 ms
usman@usman:~$ _
```

Admin to Server

```
usman@usman-virtual-machine:~/Desktop$ ping 192.168.56.10
PING 192.168.56.10 (192.168.56.10) 56(84) bytes of data.
64 bytes from 192.168.56.10: icmp_seq=1 ttl=64 time=1.10 ms
64 bytes from 192.168.56.10: icmp_seq=2 ttl=64 time=2.46 ms
64 bytes from 192.168.56.10: icmp_seq=3 ttl=64 time=2.36 ms
64 bytes from 192.168.56.10: icmp_seq=4 ttl=64 time=2.51 ms
64 bytes from 192.168.56.10: icmp_seq=5 ttl=64 time=1.94 ms
^C
--- 192.168.56.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 1.099/2.075/2.510/0.527 ms
usman@usman-virtual-machine:~/Desktop$
```

IP Allocations

Component	IP Address
infra-server VM	192.168.56.10
admin-tools VM	192.168.56.20
Dummy Gateway	192.168.56.1

Task 2

Docker PS

Server

```
usman@usman:~$ docker ps -a
CONTAINER ID   IMAGE    COMMAND              CREATED         STATUS          PORTS
                        NAMES
b60bd6d4ac10   nginx    "/docker-entrypoint.…"   14 minutes ago  Up 14 minutes   0.0.0.0:8080->80/
tcp, :::8080->80/tcp   web
usman@usman:~$
```
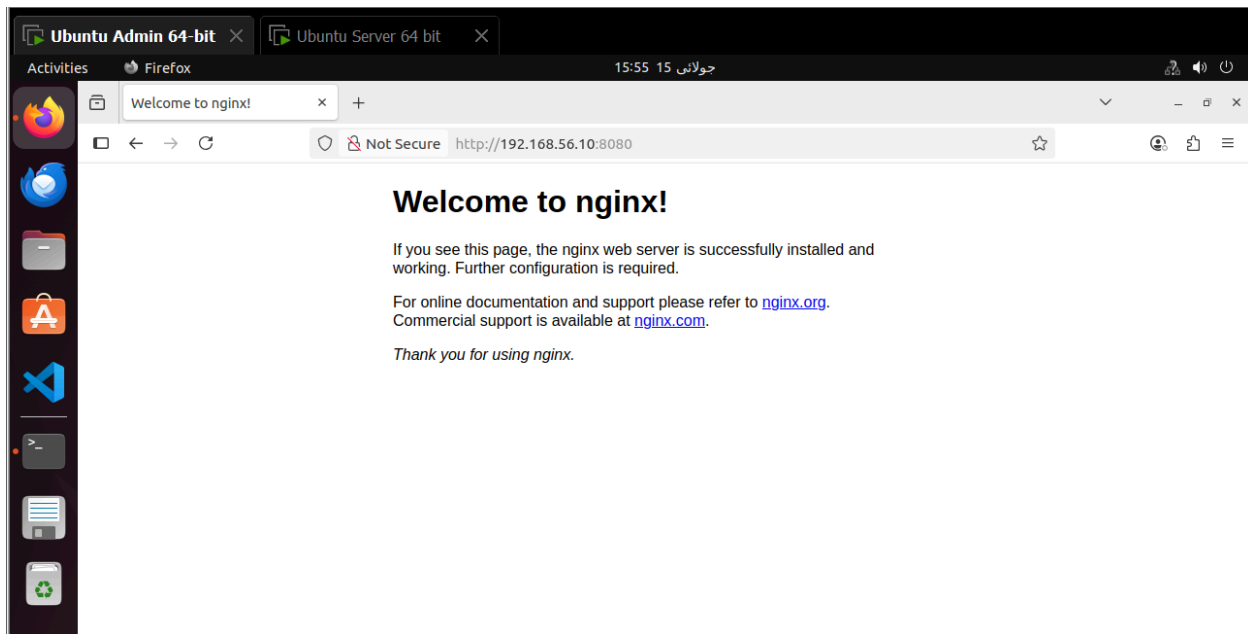
Admin

```
usman@usman-virtual-machine:~/Desktop$ docker ps -a
CONTAINER ID   IMAGE             COMMAND              CREATED         STATUS
         PORTS                                                 NAMES
be709379263b   balabit/syslog-ng   "/usr/local/bin/entr…"   16 minutes ago  Up 16 minutes (h
ealthy)   601/tcp, 0.0.0.0:514->514/udp, [::]:514->514/udp, 6514/tcp   logger
usman@usman-virtual-machine:~/Desktop$
```

IP Allocations

Component	IP Address	Container Name	Service	Port Mapping
Nginx container	172.20.0.10	web	Nginx	8080:80
Syslog-NG container	172.21.0.20	logger	Syslog-NG	514:514/udp

From Server VM

```
usman@usman:~$ logger --server 192.168.56.20 --port 514 "testing from server"
usman@usman:~$ _
```

From Admin VM

```
usman@usman-virtual-machine:~/Desktop$ docker start logger
logger
usman@usman-virtual-machine:~/Desktop$ logger --server 192.168.56.20 --port 514 "From Same VM"
usman@usman-virtual-machine:~/Desktop$ logger --server 172.21.0.20 --port 514 "Using Container IP"
usman@usman-virtual-machine:~/Desktop$ docker logs logger
```

Logs

```
Jul 16 08:24:37 192.168.56.20 1 2025-07-16T13:24:37.334064+05:00 usman-virtual-machine usman - - [timeQuality tzKnown="1" isSynced="0"] From Same VM
Jul 16 08:25:02 172.21.0.1 1 2025-07-16T13:25:02.923374+05:00 usman-virtual-machine usman - - [timeQuality tzKnown="1" isSynced="0"] Using Container IP
Jul 16 08:25:39 192.168.56.10 1 2025-07-16T08:25:40.329492+00:00 usman usman - - [timeQuality tzKnown="1" isSynced="0"] testing from server
usman@usman-virtual-machine:~/Desktop$
```

```
y tzKnown="1" isSynced="0"] From Same VM
zKnown="1" isSynced="0"] Using Container IP
Synced="0"] testing from server
```

Docker Container for Server VM

```
docker network create --subnet=172.20.0.0/24 web-net
docker run -d --name web \
--network web-net --ip 172.20.0.10 \
-p 8080:80 nginx
```

Docker Container for Admin VM

```
docker network create --subnet=172.21.0.0/24 log-net
docker run -d --name logger\
        --network log-net\
        --ip 172.21.0.20\
        -p 514:514/udp\
        -v "$PWD/syslog-ng.conf:/etc/syslog-ng/syslog-ng.conf" \
        balabit/syslog-ng
```

Task 3

```
usman@usman-virtual-machine:~/Desktop/task/Task2$ sudo python3 set_ip.py --ip 192.168.56.10/24 --gw 192.168.56.1 --iface enp0s3
[sudo] password for usman:
[2025-07-16 15:25:35] Applying static IP 192.168.56.10/24 on enp0s3 with gateway 192.168.56.1
[2025-07-16 15:25:35] Netplan config written to /etc/netplan/01-netcfg.yaml

** (generate:4806): WARNING **: 15:25:35.495: `gateway4` has been deprecated, use default routes instead.
See the 'Default routes' section of the documentation for more details.

** (generate:4806): WARNING **: 15:25:35.496: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan configuratio
ble by others.

** (process:4802): WARNING **: 15:25:38.113: `gateway4` has been deprecated, use default routes instead.
See the 'Default routes' section of the documentation for more details.

** (process:4802): WARNING **: 15:25:38.119: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan configuration
le by others.

** (process:4802): WARNING **: 15:25:40.504: `gateway4` has been deprecated, use default routes instead.
See the 'Default routes' section of the documentation for more details.

** (process:4802): WARNING **: 15:25:40.505: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan configuration
le by others.

** (process:4802): WARNING **: 15:25:40.505: `gateway4` has been deprecated, use default routes instead.
See the 'Default routes' section of the documentation for more details.

** (process:4802): WARNING **: 15:25:40.505: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan configuration
le by others.
[2025-07-16 15:25:40] Netplan applied successfully
usman@usman-virtual-machine:~/Desktop/task/Task2$ sudo cat /var/log/ip-config.log
[2025-07-16 15:25:35] Applying static IP 192.168.56.10/24 on enp0s3 with gateway 192.168.56.1
[2025-07-16 15:25:35] Netplan config written to /etc/netplan/01-netcfg.yaml
[2025-07-16 15:25:40] Netplan applied successfully
usman@usman-virtual-machine:~/Desktop/task/Task2$
```

Script B monitor.py (Revamped for split-VM use)

```
🐍 monitor.py          ≡ healthcheck.log  ✕

Task2 > ≡ healthcheck.log
   1    [2025-07-15 17:05:43] PING web 192.168.56.10 OK | HTTP 200 OK | SYSLOG FAIL
   2    [2025-07-16 10:42:35] PING 192.168.56.10 OK | HTTP FAIL | SYSLOG RECEIVED
   3    [2025-07-16 10:42:38] PING 192.168.56.10 OK | HTTP FAIL | SYSLOG RECEIVED
   4    [2025-07-16 10:45:21] PING 192.168.56.10 OK | HTTP 200 OK | SYSLOG RECEIVED
   5    [2025-07-16 10:45:24] PING 192.168.56.10 OK | HTTP 200 OK | SYSLOG RECEIVED
   6    [2025-07-16 11:16:46] PING 192.168.56.10 OK | HTTP 200 OK | SYSLOG RECEIVED
   7    [2025-07-16 11:16:49] PING 192.168.56.10 OK | HTTP 200 OK | SYSLOG RECEIVED
   8    [2025-07-16 11:37:42] PING 192.168.56.10 OK | HTTP 200 OK | SYSLOG RECEIVED
   9    |
  10
```