ASSIGNMENT

INTERNET PROTOCOL LAB

NAME: **RAHUL RAJ**

REGNO: **CB.EN.P2CYS22011**

TASK 1:

Docker- compose command.

```
┌──(root💀kali)-[/home/kali/Desktop/Labsetup]
└─# docker-compose build
VPN_Client uses an image, skipping
Host1 uses an image, skipping
Host2 uses an image, skipping
Router uses an image, skipping

┌──(root💀kali)-[/home/kali/Desktop/Labsetup]
└─# docker-compose up
\Creating network "net-10.9.0.0" with the default driver
Creating network "net-192.168.60.0" with the default driver
Pulling VPN_Client (handsonsecurity/seed-ubuntu:large) ...
large: Pulling from handsonsecurity/seed-ubuntu
da7391352a9b: Pull complete
14428a6d4bcd: Pull complete
2c2d948710f2: Pull complete
b5e99359ad22: Pull complete
3d2251ac1552: Pull complete
1059cf087055: Pull complete
b2afee800091: Pull complete
c2ff2446bab7: Pull complete
4c584b5784bd: Pull complete
Digest: sha256:41efab02008f016a7936d9cadfbe8238146d07c1c12b39cd63c3e73a0297c07a
Status: Downloaded newer image for handsonsecurity/seed-ubuntu:large
Creating host-192.168.60.5  ... done
Creating server-router      ... done
Creating client-10.9.0.5    ... done
Creating host-192.168.60.6  ... done
Attaching to client-10.9.0.5, host-192.168.60.6, host-192.168.60.5, server-router
host-192.168.60.5 |  * Starting internet superserver inetd                [ OK ]
host-192.168.60.6 |  * Starting internet superserver inetd                [ OK ]
```

```
┌──(root💀kali)-[/home/kali/Desktop/Labsetup]
└─# docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED          STATUS          PORTS     NAMES
c2d5a7cb3b31   handsonsecurity/seed-ubuntu:large    "bash -c ' ip route …"   52 seconds ago   Up 42 seconds             host-192.168.60.6
77df85f6a743   handsonsecurity/seed-ubuntu:large    "bash -c ' tail -f /…"   52 seconds ago   Up 42 seconds             client-10.9.0.5
e629a7e46f24   handsonsecurity/seed-ubuntu:large    "bash -c ' ip route …"   52 seconds ago   Up 42 seconds             server-router
24c3868831e9   handsonsecurity/seed-ubuntu:large    "bash -c ' ip route …"   52 seconds ago   Up 42 seconds             host-192.168.60.5
```

Login as server

```
┌(  root  💀  kali  )-[  /home/kali/Desktop/Labsetup            ]
└─#  docker    exec    -it   e629a7e46f24       /bin/bash
root@e629a7e46f24:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=64 time=0.342 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=64 time=0.092 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=64 time=0.104 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=64 time=0.097 ms
^C
--- 192.168.60.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3080ms
rtt min/avg/max/mdev = 0.092/0.158/0.342/0.105 ms
root@e629a7e46f24:/# ping 192.168.60.6
PING 192.168.60.6 (192.168.60.6) 56(84) bytes of data.
64 bytes from 192.168.60.6: icmp_seq=1 ttl=64 time=0.222 ms
64 bytes from 192.168.60.6: icmp_seq=2 ttl=64 time=0.096 ms
64 bytes from 192.168.60.6: icmp_seq=3 ttl=64 time=0.100 ms
64 bytes from 192.168.60.6: icmp_seq=4 ttl=64 time=0.098 ms
^C
--- 192.168.60.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3066ms
rtt min/avg/max/mdev = 0.096/0.129/0.222/0.053 ms
root@e629a7e46f24:/#
```

Login as client

```
┌──(root💀kali)-[/home/kali/Desktop/Labsetup]
└─# docker exec n-it 77df85f6a743
Error: No such container: n-it

┌──(root💀kali)-[/home/kali/Desktop/Labsetup]
└─# docker exec -it 77df85f6a743 /bin/bash
root@77df85f6a743:/#
```

```
root@77df85f6a743:/# ping 192.168.60.6
PING 192.168.60.6 (192.168.60.6) 56(84) bytes of data.
^C
--- 192.168.60.6 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3058ms

root@77df85f6a743:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
^C
--- 192.168.60.5 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2047ms

root@77df85f6a743:/#
```

Tcpdump for a host

```
root@c2d5a7cb3b31:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=64 time=0.273 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=64 time=0.111 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=64 time=0.107 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=64 time=0.124 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=64 time=0.116 ms
^C
--- 192.168.60.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4078ms
rtt min/avg/max/mdev = 0.107/0.146/0.273/0.063 ms
root@c2d5a7cb3b31:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
^C
--- 10.9.0.5 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5100ms

root@c2d5a7cb3b31:/# ping 10.9.0.11
PING 10.9.0.11 (10.9.0.11) 56(84) bytes of data.
64 bytes from 10.9.0.11: icmp_seq=1 ttl=64 time=0.182 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.104 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.105 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.106 ms
^C
--- 10.9.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3058ms
rtt min/avg/max/mdev = 0.104/0.124/0.182/0.033 ms
root@c2d5a7cb3b31:/#
```

```
┌──(root💀kali)-[/home/kali/Desktop/Labsetup]
└─# docker exec -it c2d5a7cb3b31 /bin/bash
root@c2d5a7cb3b31:/# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
23:45:40.463684 IP c2d5a7cb3b31 > host-192.168.60.5.net-192.168.60.0: ICMP echo request, id 6, seq 1, length 64
23:45:40.463903 IP host-192.168.60.5.net-192.168.60.0 > c2d5a7cb3b31: ICMP echo reply, id 6, seq 1, length 64
23:45:41.468868 IP c2d5a7cb3b31 > host-192.168.60.5.net-192.168.60.0: ICMP echo request, id 6, seq 2, length 64
23:45:41.468932 IP host-192.168.60.5.net-192.168.60.0 > c2d5a7cb3b31: ICMP echo reply, id 6, seq 2, length 64
23:45:42.492057 IP c2d5a7cb3b31 > host-192.168.60.5.net-192.168.60.0: ICMP echo request, id 6, seq 3, length 64
23:45:42.492121 IP host-192.168.60.5.net-192.168.60.0 > c2d5a7cb3b31: ICMP echo reply, id 6, seq 3, length 64
23:45:43.516061 IP c2d5a7cb3b31 > host-192.168.60.5.net-192.168.60.0: ICMP echo request, id 6, seq 4, length 64
23:45:43.516143 IP host-192.168.60.5.net-192.168.60.0 > c2d5a7cb3b31: ICMP echo reply, id 6, seq 4, length 64
23:45:44.541441 IP c2d5a7cb3b31 > host-192.168.60.5.net-192.168.60.0: ICMP echo request, id 6, seq 5, length 64
23:45:44.541508 IP host-192.168.60.5.net-192.168.60.0 > c2d5a7cb3b31: ICMP echo reply, id 6, seq 5, length 64
23:45:45.500272 ARP, Request who-has host-192.168.60.5.net-192.168.60.0 tell c2d5a7cb3b31, length 28
23:45:45.500387 ARP, Request who-has c2d5a7cb3b31 tell host-192.168.60.5.net-192.168.60.0, length 28
23:45:45.500399 ARP, Reply c2d5a7cb3b31 is-at 02:42:c0:a8:3c:06 (oui Unknown), length 28
23:45:45.500411 ARP, Reply host-192.168.60.5.net-192.168.60.0 is-at 02:42:c0:a8:3c:05 (oui Unknown), length 28
23:46:09.652202 IP c2d5a7cb3b31 > 10.9.0.5: ICMP echo request, id 7, seq 1, length 64
23:46:09.652682 IP c2d5a7cb3b31.48457 > 192.168.23.80.domain: 6655+ PTR? 5.0.9.10.in-addr.arpa. (39)
23:46:10.652669 IP c2d5a7cb3b31 > 10.9.0.5: ICMP echo request, id 7, seq 2, length 64
23:46:11.679602 IP c2d5a7cb3b31 > 10.9.0.5: ICMP echo request, id 7, seq 3, length 64
23:46:12.703802 IP c2d5a7cb3b31 > 10.9.0.5: ICMP echo request, id 7, seq 4, length 64
23:46:13.724463 IP c2d5a7cb3b31 > 10.9.0.5: ICMP echo request, id 7, seq 5, length 64
23:46:14.658949 IP c2d5a7cb3b31.49106 > 192.168.23.80.domain: 6655+ PTR? 5.0.9.10.in-addr.arpa. (39)
23:46:14.684139 ARP, Request who-has server-router.net-192.168.60.0 tell c2d5a7cb3b31, length 28
23:46:14.684348 ARP, Reply server-router.net-192.168.60.0 is-at 02:42:c0:a8:3c:0b (oui Unknown), length 28
```

Login as client and copy the program tun.py

```
root@77df85f6a743:/# cd volumnes
bash: cd: volumnes: No such file or directory
root@77df85f6a743:/# cd volumes
root@77df85f6a743:/volumes# nano tun.py
root@77df85f6a743:/volumes# chmod a+x tun.py
root@77df85f6a743:/volumes# tun.py
Interface Name: akhil0
```

```
root@77df85f6a743:/# ip addr
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
2: akhil0: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN group def
ault qlen 500
    link/none
8: eth0@if9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP gr
oup default
    link/ether 02:42:0a:09:00:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.5/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
root@77df85f6a743:/# ip addr add 192.168.53.99 dev akhil0
root@77df85f6a743:/# ip addr
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
2: akhil0: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN group def
ault qlen 500
    link/none
    inet 192.168.53.99/32 scope global akhil0
       valid_lft forever preferred_lft forever
8: eth0@if9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP gr
oup default
    link/ether 02:42:0a:09:00:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.5/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
```

```python
#!/usr/bin/env python3

import fcntl
import struct
import os
import time
from scapy.all import *

TUNSETIFF = 0x400454ca
IFF_TUN   = 0x0001
IFF_TAP   = 0x0002
IFF_NO_PI = 0x1000

# Create the tun interface
tun = os.open("/dev/net/tun", os.O_RDWR)
ifr = struct.pack('16sH', b'akhil%d', IFF_TUN | IFF_NO_PI)
ifname_bytes  = fcntl.ioctl(tun, TUNSETIFF, ifr)

# Get the interface name
ifname = ifname_bytes.decode('UTF-8')[:16].strip("\x00")
print("Interface Name: {}".format(ifname))

while True:
    time.sleep(10)
```

This can be also done by adding command to the program

```python
#!/usr/bin/env python3

import fcntl
import struct
import os
import time
from scapy.all import *

TUNSETIFF = 0x400454ca
IFF_TUN   = 0x0001
IFF_TAP   = 0x0002
IFF_NO_PI = 0x1000

# Create the tun interface
tun = os.open("/dev/net/tun", os.O_RDWR)
ifr = struct.pack('16sH', b'akhil%d', IFF_TUN | IFF_NO_PI)
ifname_bytes  = fcntl.ioctl(tun, TUNSETIFF, ifr)

# Get the interface name
ifname = ifname_bytes.decode('UTF-8')[:16].strip("\x00")
print("Interface Name: {}".format(ifname))

os.system("ip addr add 192.168.53.99/24 dev {}".format(ifname))
os.system("ip link set dev {} up".format(ifname))
while True:
    time.sleep(10)
```

```
root@77df85f6a743:/# ip addr
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
3: akhil0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast st
ate UNKNOWN group default qlen 500
    link/none
    inet 192.168.53.99/24 scope global akhil0
       valid_lft forever preferred_lft forever
8: eth0@if9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP gr
oup default
    link/ether 02:42:0a:09:00:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.5/24 brd 10.9.0.255 scope global eth0
       valid_lft forever preferred_lft forever
```