

## Task 1: Network Setup

We set up the environment as follows:

```
(root@kali)~[~/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)~[~/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-192.168.60.6 ... done
Creating host-192.168.60.5 ... done
Creating client-10.9.0.5 ... done
Creating server-router ... done
Attaching to client-10.9.0.5, host-192.168.60.5, server-router, host-192.168.60.6
host-192.168.60.5 | * Starting internet superserver inetd          [ OK ]
host-192.168.60.6 | * Starting internet superserver inetd          [ OK ]
```

```
(root@kali)~[~/home/kali]
# docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS
PORTS         NAMES
8e8b861b1822   handsonsecurity/seed-ubuntu:large   "bash -c ' ip route ..." About a minute ago Up About a minute
server-router
2adb10cdb40a   handsonsecurity/seed-ubuntu:large   "bash -c ' tail -f /..." About a minute ago Up About a minute
client-10.9.0.5
a5041b1442c4   handsonsecurity/seed-ubuntu:large   "bash -c ' ip route ..." About a minute ago Up About a minute
host-192.168.60.5
adf271d51dc5   handsonsecurity/seed-ubuntu:large   "bash -c ' ip route ..." About a minute ago Up About a minute
host-192.168.60.6
```

From server to both the hosts

```
root@8e8b861b1822:/# 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=0.180 ms
64 bytes from 192.168.60.6: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 192.168.60.6: icmp_seq=3 ttl=64 time=0.049 ms
64 bytes from 192.168.60.6: icmp_seq=4 ttl=64 time=0.050 ms
64 bytes from 192.168.60.6: icmp_seq=5 ttl=64 time=0.061 ms
^C
--- 192.168.60.6 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4075ms
rtt min/avg/max/mdev = 0.049/0.078/0.180/0.050 ms
root@8e8b861b1822:/# 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=0.274 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=64 time=0.077 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=64 time=0.081 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=64 time=0.277 ms
^C
--- 192.168.60.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3270ms
rtt min/avg/max/mdev = 0.077/0.177/0.277/0.098 ms
```

From client to server

```
root@2adb10cdb40a:/# 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=0.172 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.091 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.049 ms
64 bytes from 10.9.0.11: icmp_seq=4 ttl=64 time=0.057 ms
^C
--- 10.9.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3081ms
rtt min/avg/max/mdev = 0.049/0.092/0.172/0.048 ms
root@2adb10cdb40a:/#
```

Run tcpdump on server to capture all the traffic

```
root@8e8b861b1822:/# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:16:38.239528 IP client-10.9.0.5.net-10.9.0.0 > 8e8b861b1822: ICMP echo request, id 8, seq 1, length 64
13:16:38.239547 IP 8e8b861b1822 > client-10.9.0.5.net-10.9.0.0: ICMP echo reply, id 8, seq 1, length 64
13:16:39.243597 IP client-10.9.0.5.net-10.9.0.0 > 8e8b861b1822: ICMP echo request, id 8, seq 2, length 64
13:16:39.243625 IP 8e8b861b1822 > client-10.9.0.5.net-10.9.0.0: ICMP echo reply, id 8, seq 2, length 64
13:16:40.643062 IP client-10.9.0.5.net-10.9.0.0 > 8e8b861b1822: ICMP echo request, id 8, seq 3, length 64
13:16:40.643075 IP 8e8b861b1822 > client-10.9.0.5.net-10.9.0.0: ICMP echo reply, id 8, seq 3, length 64
13:16:43.403891 ARP, Request who-has client-10.9.0.5.net-10.9.0.0 tell 8e8b861b1822, length 28
13:16:43.403990 ARP, Request who-has 8e8b861b1822 tell client-10.9.0.5.net-10.9.0.0, length 28
13:16:43.403994 ARP, Reply 8e8b861b1822 is-at 02:42:0a:09:00:0b (oui Unknown), length 28
13:16:43.403996 ARP, Reply client-10.9.0.5.net-10.9.0.0 is-at 02:42:0a:09:00:05 (oui Unknown), length 28
```

## Task 2: Create and Configure TUN Interface:

### Task 2.a: Name of the Interface:

From client –

```
root@8e8b861b1822:~# 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
2: tun0: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 500
    link/none
12: eth1@if13: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:a8:3c:0b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.60.11/24 brd 192.168.60.255 scope global eth1
        valid_lft forever preferred_lft forever
14: eth0@if15: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:0b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.11/24 brd 10.9.0.255 scope global eth0
        valid_lft forever preferred_lft forever
root@8e8b861b1822:~#
```

```
root@2adb10cdb40a:~# exit
exit

(root@kali) ~ - [~/home/kali]
# docker exec -it 8e8b861b1822 /bin/bash
root@8e8b861b1822:~# nano tun.py
root@8e8b861b1822:~# python3 tun.py
Interface Name: tun0
^
```

```
#!/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'shebu%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)
```

```
root@8e8b861b1822:~# 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
2: shebu0: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 500
    link/none
12: eth1@if13: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:a8:3c:0b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.60.11/24 brd 192.168.60.255 scope global eth1
        valid_lft forever preferred_lft forever
14: eth0@if15: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:0b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.11/24 brd 10.9.0.255 scope global eth0
        valid_lft forever preferred_lft forever
root@8e8b861b1822:~#
```

```
root@2adb10cdb40a:~# exit
exit

(root@kali) ~ - [~/home/kali]
# docker exec -it 8e8b861b1822 /bin/bash
root@8e8b861b1822:~# nano tun.py
root@8e8b861b1822:~# python3 tun.py
Interface Name: tun0
^CTraceback (most recent call last):
  File "tun.py", line 24, in <module>
    time.sleep(10)
KeyboardInterrupt

root@8e8b861b1822:~# python3 tun.py
Interface Name: shebu0
^
```

Task 2.b: Set up the TUN Interface: First, we added the ip address manually using the command- ip addr add and command – ip link set up to bring up the interface:



```

root@8e8b861b1822:/# ip addr add 192.168.53.99/24 dev shebu0
root@8e8b861b1822:/# 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
4: shebu0: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 500
    link/none
    inet 192.168.53.99/24 scope global shebu0
        valid_lft forever preferred_lft forever
12: eth1@if13: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:a8:3c:0b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.60.11/24 brd 192.168.60.255 scope global eth1
        valid_lft forever preferred_lft forever
14: eth0@if15: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:0b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.11/24 brd 10.9.0.255 scope global eth0
        valid_lft forever preferred_lft forever
root@8e8b861b1822:/#

```

```

root@8e8b861b1822:/
# python3 tun.py
Interface Name: shebu0

```

```

root@8e8b861b1822:/# ip link set dev shebu0 up
root@8e8b861b1822:/# 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
5: shebu0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 500
    link/none
12: eth1@if13: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:a8:3c:0b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.60.11/24 brd 192.168.60.255 scope global eth1
        valid_lft forever preferred_lft forever
14: eth0@if15: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:0b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.11/24 brd 10.9.0.255 scope global eth0
        valid_lft forever preferred_lft forever
root@8e8b861b1822:/#

```

```

root@8e8b861b1822:/
# python3 tun.py
Interface Name: shebu0

```

Also, this is done automatically by adding the commands to the code:

```

# Create the tun interface
tun = os.open("/dev/net/tun", os.O_RDWR)
ifr = struct.pack('16sH', b'shebu%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@8e8b861b1822:/# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    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
6: shebu0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc
    state UNKNOWN group default qlen 500
    link/none
    inet 192.168.53.99/24 scope global shebu0
        valid lft forever preferred lft forever
12: eth1@if13: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noq

```

Task 2.c: Read from the TUN Interface:

Code:

```

ifr = struct.pack('16s', b'shebu0', 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:
    packet=os.read(tun, 2048)
    if packet:
        ip=IP(packet)
        print(ip.summary())

while True:
    time.sleep(10)

```

First, On Host U, we ping a host in the 192.168.53.0/24 network. Specifically, we ping the 192.168.53.1 network. As the interface is not yet configured to get a reply back, we can see that packets were not received back. However, being in the same LAN network, the packets get sent successfully.

```

root@deeb5999b181:/# 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
7: shebu0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 500
    link/none
    inet 192.168.53.99/24 scope global shebu0
        valid lft forever preferred lft forever
30: eth0@if31: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group 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@deeb5999b181:/# ping 192.168.53.1
PING 192.168.53.1 (192.168.53.1) 56(84) bytes of data.
^C
  -- 192.168.53.1 ping statistics --
  5 packets transmitted, 0 received, 100% packet loss, time 400ms

root@deeb5999b181:/#

root@deeb5999b181:/# python3 tun.py
Interface Name: shebu0
<bound method Packet.summary of <IP version=4 ihl=5 tos=0x0 len=84 id=6383 flags=DF frag=0 ttl=64 proto=icmp chksum=0x365>
src=192.168.53.99 dst=192.168.53.1 [<ICMP type=echo-request code=0 chksum=0xbdec id=0x4 seq=0x1 |<raw |load> \xaa\xab\xbc\x00\x00\x00\x00\x01\x0c\x00\x00\x00\x00\x00\x00\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f |<#56> \(')+, ..., /01234567' ]>>>
<bound method Packet.summary of <IP version=4 ihl=5 tos=0x0 len=84 id=6313 flags=DF frag=0 ttl=64 proto=icmp chksum=0x362d
src=192.168.53.99 dst=192.168.53.1 [<ICMP type=echo-request code=0 chksum=0xbdb0 id=0x4 seq=0x2 |<raw |load> \xaa\xab\xbc\x00\x00\x00\x00\x00\x0c\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f |<#56> \(')+, ..., /01234567' ]>>>
<bound method Packet.summary of <IP version=4 ihl=5 tos=0x0 len=84 id=6586 flags=DF frag=0 ttl=64 proto=icmp chksum=0x353a
src=192.168.53.99 dst=192.168.53.1 [<ICMP type=echo-request code=0 chksum=0xbdb0 id=0x4 seq=0x3 |<raw |load> \xaa\xab\xbc\x00\x00\x00\x00\x0c\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f |<#56> \(')+, ..., /01234567' ]>>>
<bound method Packet.summary of <IP version=4 ihl=5 tos=0x0 len=84 id=6699 flags=DF frag=0 ttl=64 proto=icmp chksum=0x34c9
src=192.168.53.99 dst=192.168.53.1 [<ICMP type=echo-request code=0 chksum=0xb9fac id=0x4 seq=0x4 |<raw |load> \xaa\xab\xbc\x00\x00\x00\x00\x0c\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f |<#56> \(')+, ..., /01234567' ]>>>
<bound method Packet.summary of <IP version=4 ihl=5 tos=0x0 len=84 id=6836 flags=DF frag=0 ttl=64 proto=icmp chksum=0x3448
src=192.168.53.99 dst=192.168.53.1 [<ICMP type=echo-request code=0 chksum=0xb9fac id=0x4 seq=0x5 |<raw |load> \xaa\xab\xbc\x00\x00\x00\x00\x0c\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f |<#56> \(')+, ..., /01234567' ]>>>

```

Now, on Host U, we ping a host in the internal network 192.168.60.0/24. Specifically, we ping the 192.168.60.5 network. Similar to before, we can see that no packets are received. However, in this case, no packets were sent out as well due to which the client

side screen is blank as it tried sending out packets to network outside of the host network which is unreachable

```
root@deeb5999b181:/# 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 ---
18 packets transmitted, 0 received, 100% packet loss, time 17409ms

root@deeb5999b181:/#
```

```
root@deeb5999b181:/#
Interface Name:
```

## Task 2.d: Write to the TUN Interface

We modified the code so that a spoofed packet is sent out with src IP as 192.168.53.3 :

```
while True:
    packet = os.read(tun, 2048)
    if packet:
        ip = IP(packet)
        print(ip.summary)

        newip = IP(src='192.168.53.3', dst=ip.src)
        newpkt = newip/ip.payload
        os.write(tun, bytes(newpkt))
```

We run the code to see that packets were sent and received successfully

```
root@deeb5999b181:/# ping 192.168.53.3
PING 192.168.53.3 (192.168.53.3) 56(84) bytes of data.
64 bytes from 192.168.53.3: icmp_seq=1 ttl=64 time=2.37 ms
64 bytes from 192.168.53.3: icmp_seq=2 ttl=64 time=2.21 ms
64 bytes from 192.168.53.3: icmp_seq=3 ttl=64 time=7.78 ms
^C
--- 192.168.53.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.207/4.120/7.780/2.588 ms
root@deeb5999b181:/#
```

```
root@deeb5999b181:/# python3 tun.py
Interface Name: shebu0
^CTraceback (most recent call last):
  File "tun.py", line 27, in <module>
    packet = os.read(tun, 2048)
KeyboardInterrupt

root@deeb5999b181:/# nano tun.py
root@deeb5999b181:/# python3 tun.py
Interface Name: shebu0
<bound method Packet.summary of <IP version=4 ihl=5 tos=0 len=84 id=61050 flags=0 seq=0 chksum=0 src=192.168.53.99 dst=192.168.53.3 |<ICMP type=echo-request d=0xc seq=0*1 |<Raw load='t\xcc7\xbb\x00\x00\x00na\x02\x00\x00\x00\x00\x10\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&'()*+,-./01234567' |>>>
<bound method Packet.summary of <IP version=4 ihl=5 tos=0 len=84 id=61051 flags=0 seq=0 chksum=0 src=192.168.53.99 dst=192.168.53.3 |<ICMP type=echo-reply code=0 seq=0*1 |<Raw load='t\xcc7\xbb\x00\x00\x00na\x02\x00\x00\x00\x00\x10\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&'()*+,-./01234567' |>>>
```

Instead of writing an IP packet to the interface, we modify the code to write some arbitrary data to the interface to send it as bytes:

```
while True:
    packet = os.read(tun, 2048)
    if packet:
        ip = IP(packet)
        print(ip.summary)

        newip = IP(src='192.168.53.3', dst=ip.src)
        newpkt = newip/ip.payload
        arb_data = b'Any arbitrary data'
        os.write(tun, arb_data)
```



We run the code to see the output as follows:

```
root@deeb5999b181:/# ping 192.168.53.3
PING 192.168.53.3 (192.168.53.3) 56(84) bytes of data.
^C
--- 192.168.53.3 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2058ms

root@deeb5999b181:/#

root@deeb5999b181:/# python3 tun.py
Interface Name: shebu0
<bound method Packet.summary of <IP version=4 ihl=5 tos=0x0 len=84 id=34580 flags=DF frag=0
ttl=64 proto=icmp chksum=0xc7dd src=192.168.53.99 dst=192.168.53.3 |<ICMP type=echo-reques
t code=0 chksum=0x2531 id=0xf seq=0x1 |<Raw load='\xc5\xd9\xbb\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !'#$%&\'
()*+,-./01234567' |>>>>
<bound method Packet.summary of <IP version=4 ihl=5 tos=0x0 len=84 id=34705 flags=DF frag=0
ttl=64 proto=icmp chksum=0xc760 src=192.168.53.99 dst=192.168.53.3 |<ICMP type=echo-reques
t code=0 chksum=0xc8ac id=0xf seq=0x2 |<Raw load='\xc5\xd9\xbb\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !'#$%&\'
()*+,-./01234567' |>>>>
<bound method Packet.summary of <IP version=4 ihl=5 tos=0x0 len=84 id=34875 flags=DF frag=0
ttl=64 proto=icmp chksum=0xc6b6 src=192.168.53.99 dst=192.168.53.3 |<ICMP type=echo-reques
t code=0 chksum=0x734b id=0xf seq=0x3 |<Raw load='\xc6\xd9\xbb\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !'#$%&\'
()*+,-./01234567' |>>>>
^C

root@deeb5999b181:/# tcpdump -i shebu0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on shebu0, link-type RAW (Raw IP), capture size 262144 bytes
09:09:24.503603 IP 192.168.53.99 > 192.168.53.3: ICMP echo request, id 15, seq 1, length 64
09:09:24.505526 IP [ilp]
09:09:25.537104 IP 192.168.53.99 > 192.168.53.3: ICMP echo request, id 15, seq 2, length 64
09:09:25.546465 IP [ilp]
09:09:26.561774 IP 192.168.53.99 > 192.168.53.3: ICMP echo request, id 15, seq 3, length 64
09:09:26.569333 IP [ilp]
```

Task 3: Send the IP Packet to VPN Server Through a Tunnel Tun-server.py code:

```
root@5021b92cb001:/# python3 tun_server.py
10.9.0.5:44425 -> 0.0.0.0:9090
Inside: 192.168.53.99 -> 192.168.53.3
Traceback (most recent call last):
  File "tun_server.py", line 16, in <module>
    os.write(tun, bytes(pkt))
NameError: name 'tun' is not defined
root@5021b92cb001:/#

root@deeb5999b181:/# python3 tun_client.py
Interface Name: tun0
^CTraceback (most recent call last):
  File "tun_client.py", line 31, in <module>
    packet = os.read(tun, 2048)
KeyboardInterrupt

root@deeb5999b181:/# nano tun_client.py
root@deeb5999b181:/# python3 tun_client.py
Interface Name: tun0

root@kali:/home/kali
File Actions Edit View Help
(kali@kali)-[~]
└─$ su root
Password:
(root@kali)-[/home/kali]
└─$ docker exec -it deeb5999b181 /bin/bash
root@deeb5999b181:/# ping 192.168.53.3
PING 192.168.53.3 (192.168.53.3) 56(84) bytes of data.
^C
--- 192.168.53.3 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6128ms

root@deeb5999b181:/# ping 192.168.53.3
PING 192.168.53.3 (192.168.53.3) 56(84) bytes of data.
^C
--- 192.168.53.3 ping statistics ---
20 packets transmitted, 0 received, 100% packet loss, time 19447ms

root@deeb5999b181:/# ping 192.168.53.3
PING 192.168.53.3 (192.168.53.3) 56(84) bytes of data.
```