Farhad Ahmed
Network Security
Professor McCoy
02/19/19

Lab 01 – DHCP Starvation Attack Using Python/ScaPy

This lab was designed to show the effectiveness of launching a DoS attack on a DHCP server by starving it of available IP's within a range. To start this lab, the first thing that needed to be done was reset the EXT-Router's dhcpd.leases files. Before the attack these files appeared as shown below.

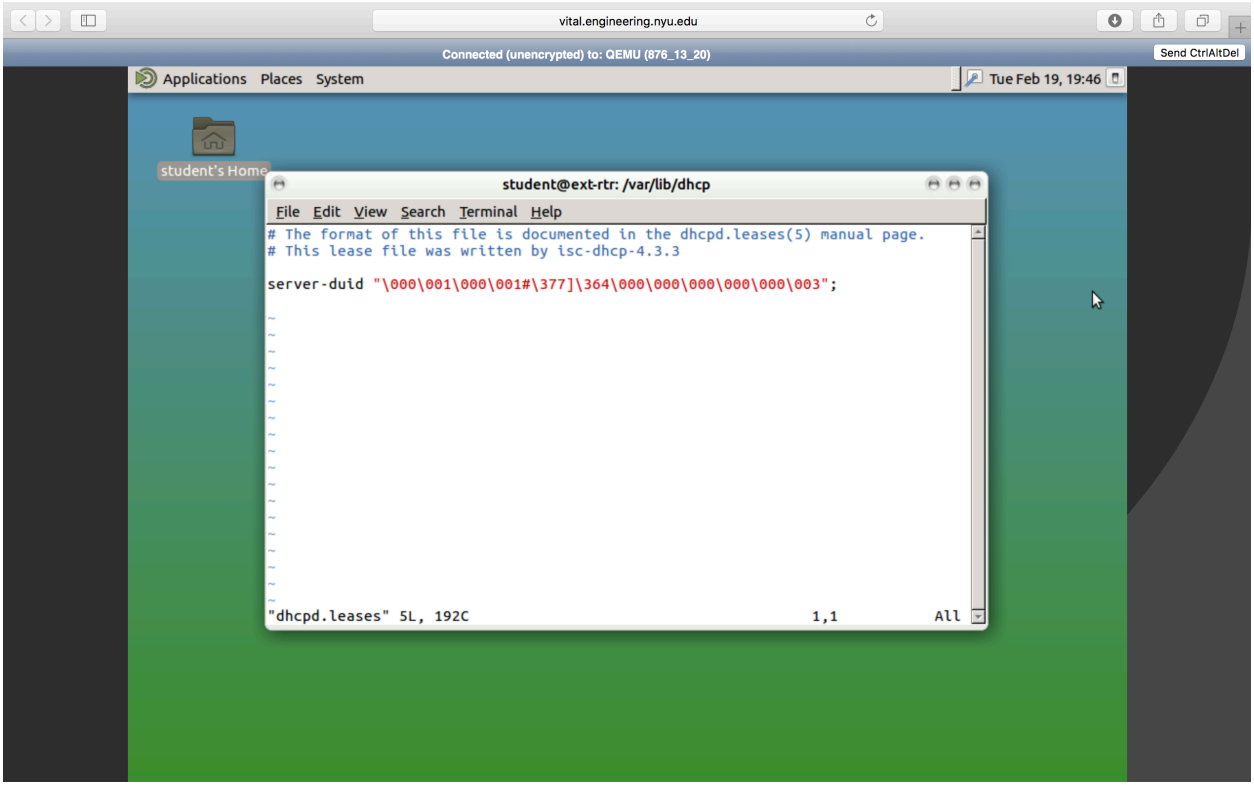


Figure 1. *dhcpd.leases file contents*

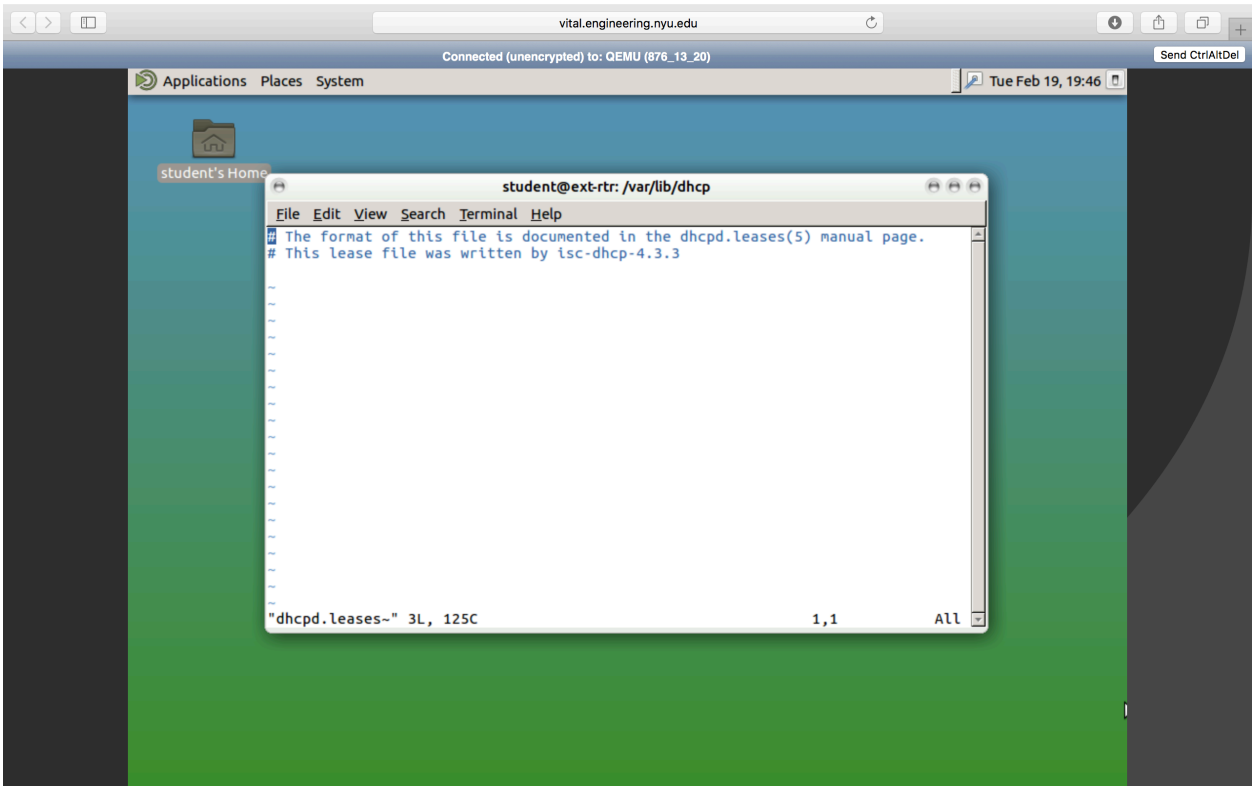


Figure 2. *dhcpd.leases~ file contents*

The next step was to boot the Kali Linux machine and write a Python script using the ScaPy library. This script loops through a range of 100 to 200 and adds that to the subnet to assemble a proper IP address (10.10.11.xxx). A new MAC address is also generated and a packet is put together using these two. The packets are sent to the server and the handshake results as incomplete which bounds the packet to the IP. After doing this for 100 addresses, there is none left for legitimate users.

Running the script, output to the terminal everytime a packet was sent and also displayed the IP address that the loop was on.

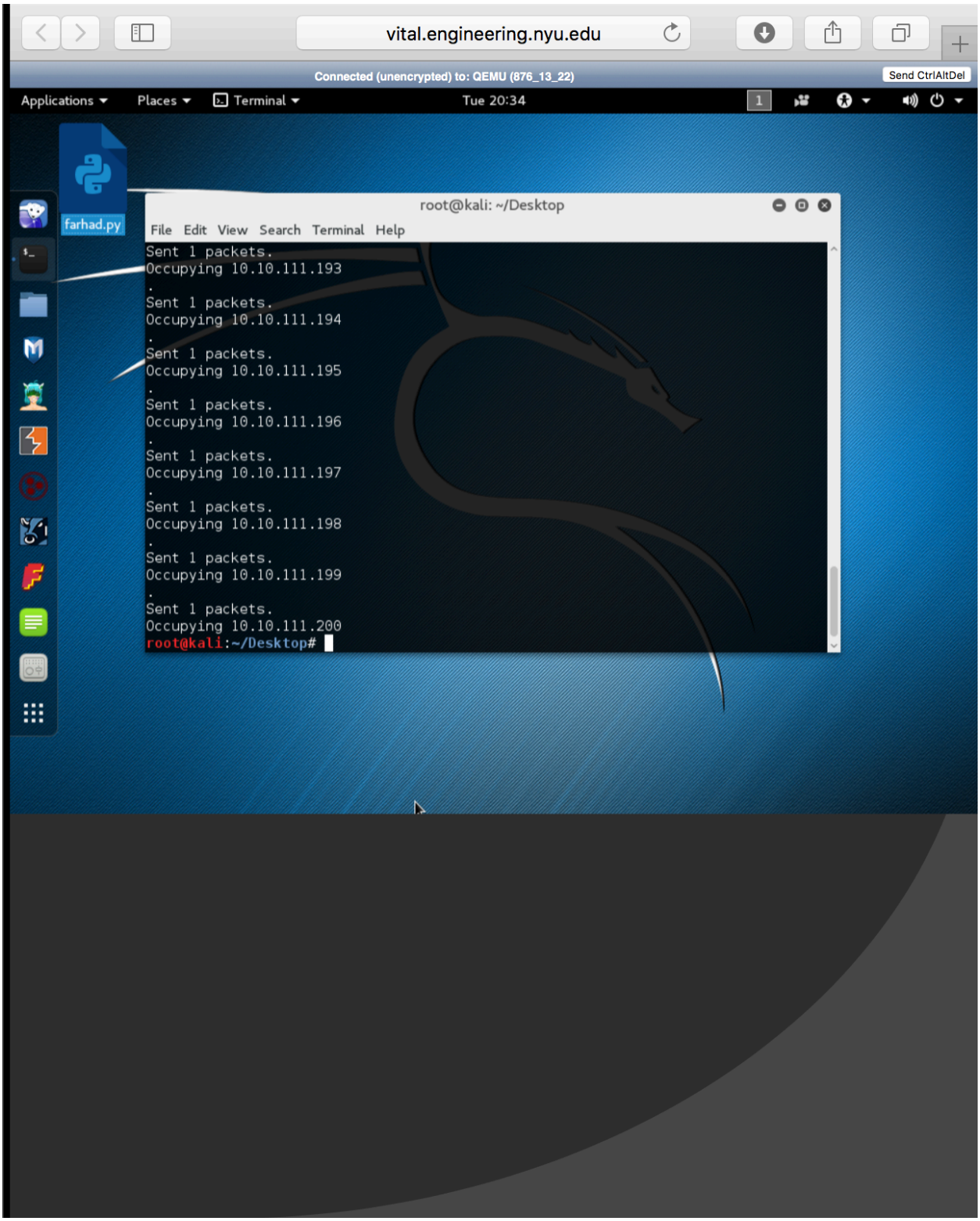


Figure 3. *Terminal output from running starve.py*

Trying to access the server through ipconfig on the Windows XP VM, revealed that the IP address and subnet was 0.0.0.0. Running ipconfig/renew returned a message indicating that the request had timed out.

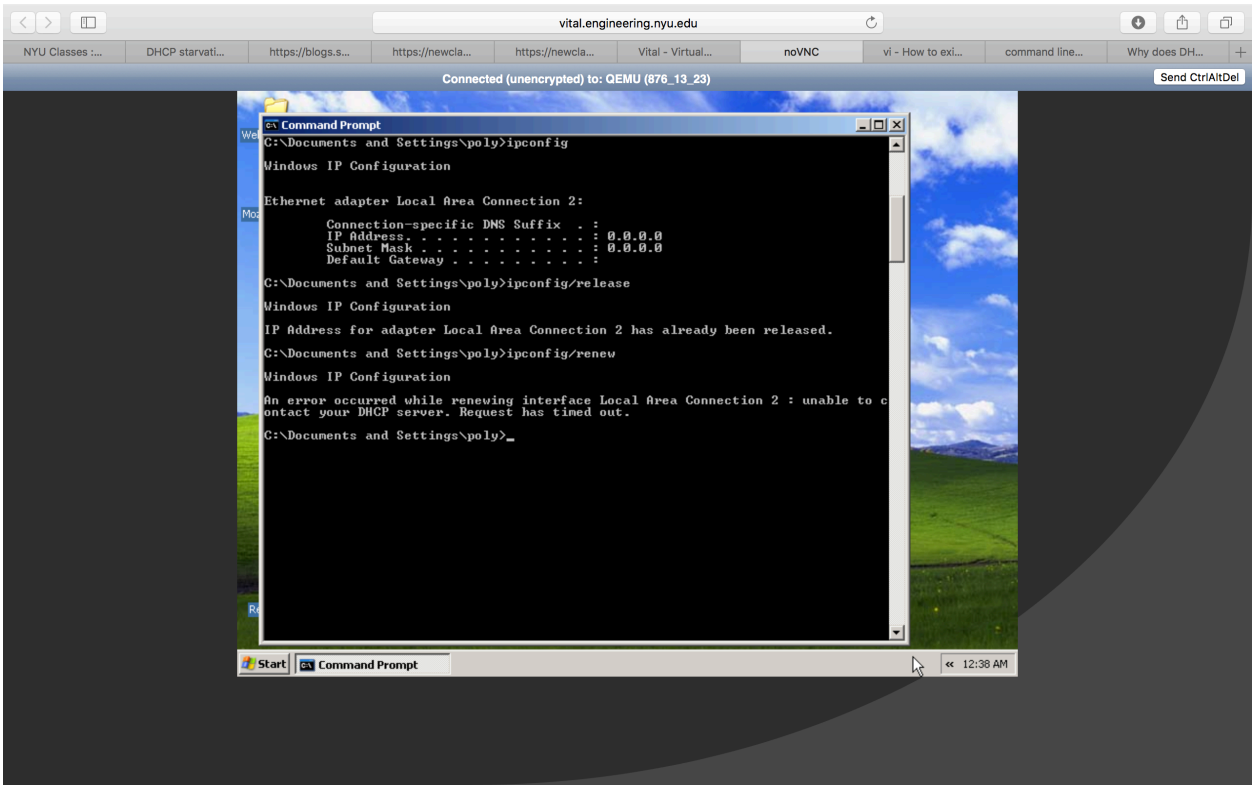
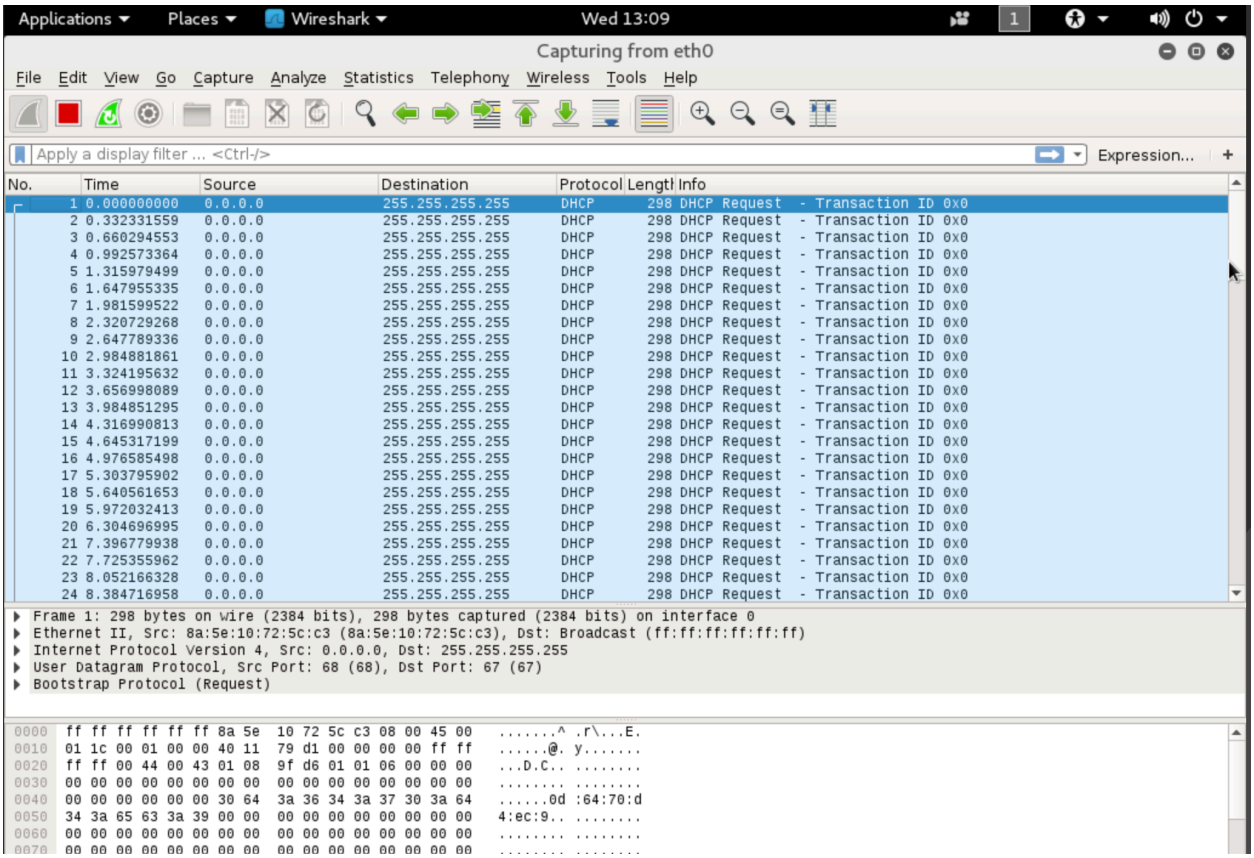
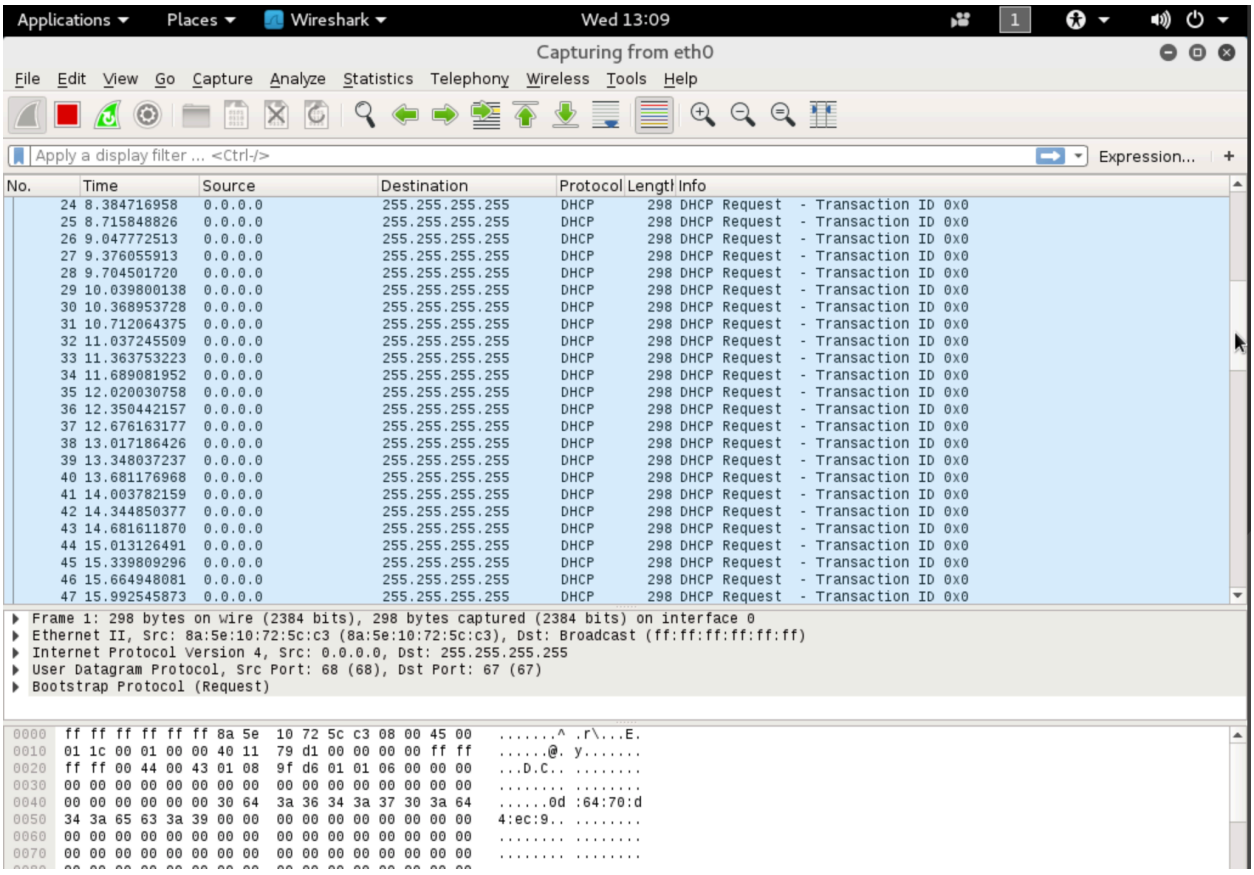


Figure 4. *Victim is unable to access server.*

Capturing the packets during the execution of the script was somewhat difficult due to problems with running WireShark within the VM. Wireshark would frequently close after opening the program and selecting the connection to sniff packets on. Sometimes it would even close in the middle of running the starve.py script. However, I was able to screenshot some of the packets before the program could close.


Applications
Places
Wireshark
Wed 13:09
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000000 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
2 0.332331559 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
3 0.660294553 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
4 0.992573364 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
5 1.315979499 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
6 1.647955335 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
7 1.981599522 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
8 2.320729268 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
9 2.647789336 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
10 2.984881861 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
11 3.324195632 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
12 3.656998089 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
13 3.984851295 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
14 4.316990813 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
15 4.645317199 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
16 4.976585498 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
17 5.303795902 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
18 5.640561653 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
19 5.972032413 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
20 6.304696995 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
21 7.396779938 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
22 7.725355962 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
23 8.052166328 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
24 8.384716958 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
Frame 1: 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface 0
Ethernet II, Src: 8a:5e:10:72:5c:c3 (8a:5e:10:72:5c:c3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
Bootstrap Protocol (Request)
0000 ff ff ff ff ff ff 8a 5e 10 72 5c c3 08 00 45 00 ....^ .r\...E.
0010 01 1c 00 01 00 00 40 11 79 d1 00 00 00 00 ff ff ......@. y.......
0020 ff ff 00 44 00 43 01 08 9f d6 01 01 06 00 00 00 ...D.C.. ....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0040 00 00 00 00 00 00 30 64 3a 36 34 3a 37 30 3a 64 ......0d :64:70:d
0050 34 3a 65 63 3a 39 00 00 00 00 00 00 00 00 00 00 4:ec:9.. ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....


Applications
Places
Wireshark
Wed 13:09
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
24 8.384716958 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
25 8.715848826 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
26 9.047772513 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
27 9.376055913 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
28 9.704501720 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
29 10.039800138 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
30 10.368953728 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
31 10.712064375 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
32 11.037245509 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
33 11.363753223 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
34 11.689081952 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
35 12.020030758 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
36 12.350442157 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
37 12.676163177 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
38 13.017186426 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
39 13.348037237 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
40 13.681176968 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
41 14.003782159 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
42 14.344850377 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
43 14.681611870 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
44 15.013126491 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
45 15.339809296 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
46 15.664948081 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
47 15.992545873 0.0.0.0 255.255.255.255 DHCP 298 DHCP Request - Transaction ID 0x0
Frame 1: 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface 0
Ethernet II, Src: 8a:5e:10:72:5c:c3 (8a:5e:10:72:5c:c3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
Bootstrap Protocol (Request)
0000 ff ff ff ff ff ff 8a 5e 10 72 5c c3 08 00 45 00 ....^ .r\...E.
0010 01 1c 00 01 00 00 40 11 79 d1 00 00 00 00 ff ff ......@. y.......
0020 ff ff 00 44 00 43 01 08 9f d6 01 01 06 00 00 00 ...D.C.. ....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0040 00 00 00 00 00 00 30 64 3a 36 34 3a 37 30 3a 64 ......0d :64:70:d
0050 34 3a 65 63 3a 39 00 00 00 00 00 00 00 00 00 00 4:ec:9.. ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....

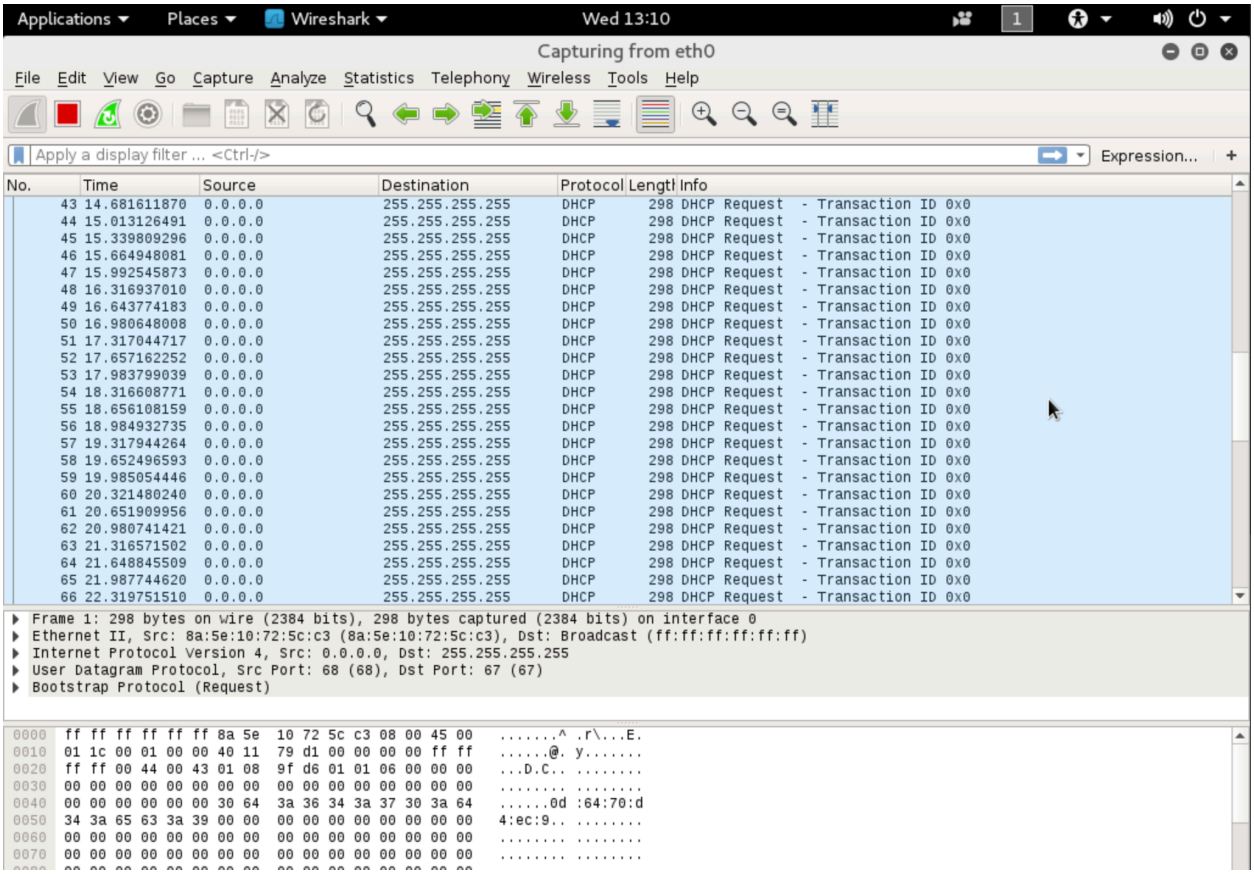


Figure 5. *Wireshark packets being captured.*

After running the starvation script, the dhcpd file on the EXT-Router had been updated as seen below.

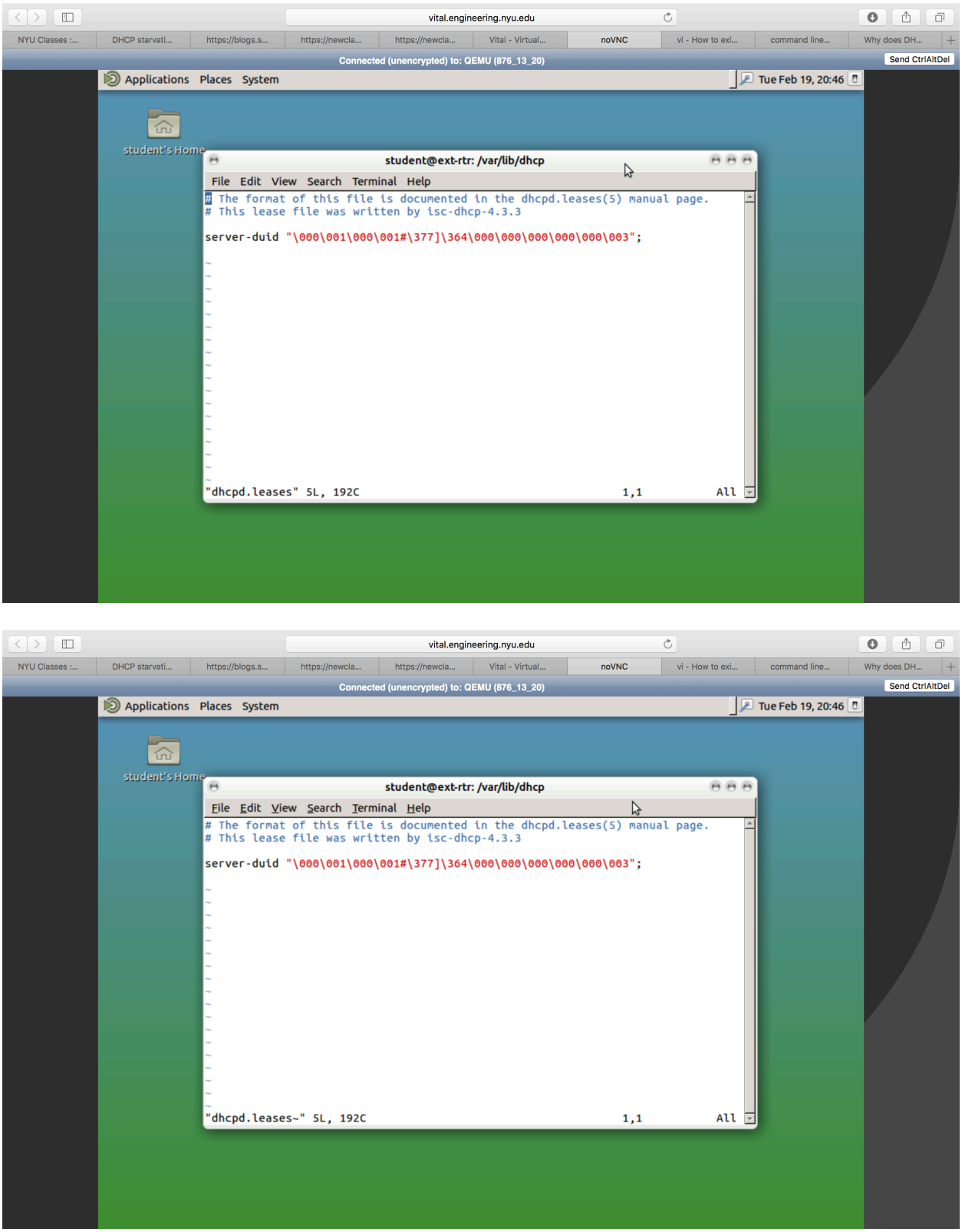


Figure 6. *dhcpd.leases files changed after running attack script.*