

Lab #2: Raspberry PI as Network Monitor using Zeek

Lab Overview

This lab introduces network monitoring tool called zeek, which will be used in our raspberry PI to observe our network traffic and analyze different events in our network.

Requirements

This lab requires properly configured and secure raspberry PI with the proper set up which was done in lab 1. This lab also requires installing zeek which was a bit of trouble at the beginning, but I figured out the way to properly install and configure zeek.

Tasks

1. **PI's local IP and Mac Address:** While doing this lab the following were by IP addresses and MAC address which is obtained by using command **ifconfig** in my raspberry PI terminal.



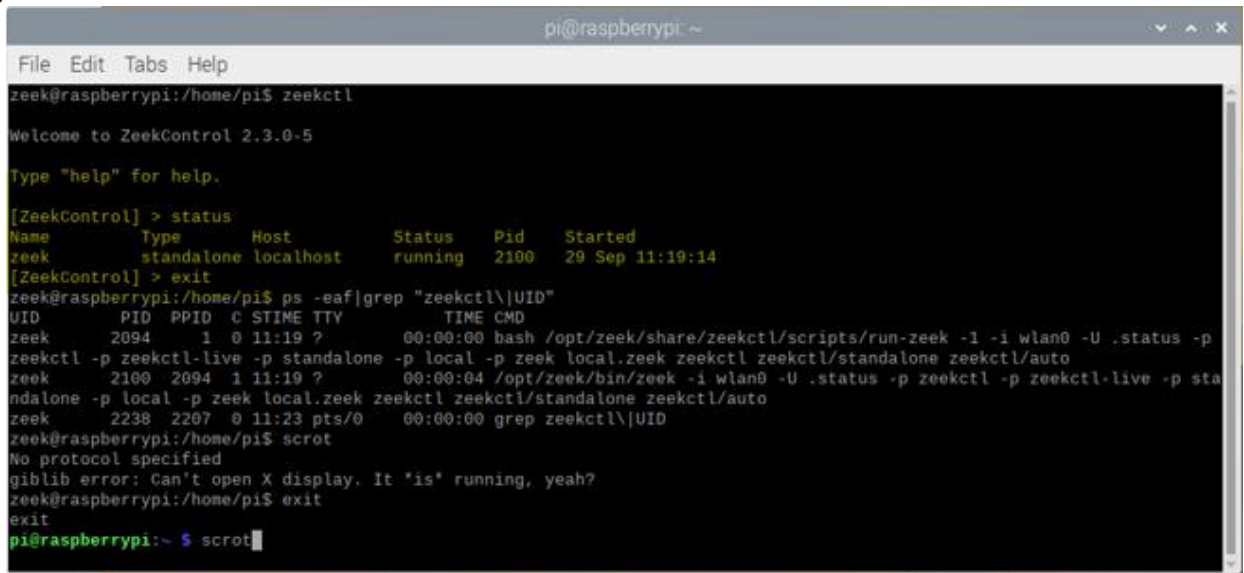
```
pi@raspberrypi:~$ ifconfig
eth0: flags=4096<UP,BROADCAST,MULTICAST> mtu 1500
    ether 88:27:eb:4f:72:d9 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.66 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::c02:9d26:932c:2c8b prefixlen 64 scopeid 0x20<link>
    ether 88:27:eb:4f:72:d9 txqueuelen 1000 (Ethernet)
    RX packets 22020 bytes 23695267 (22.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 13616 bytes 11498706 (10.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

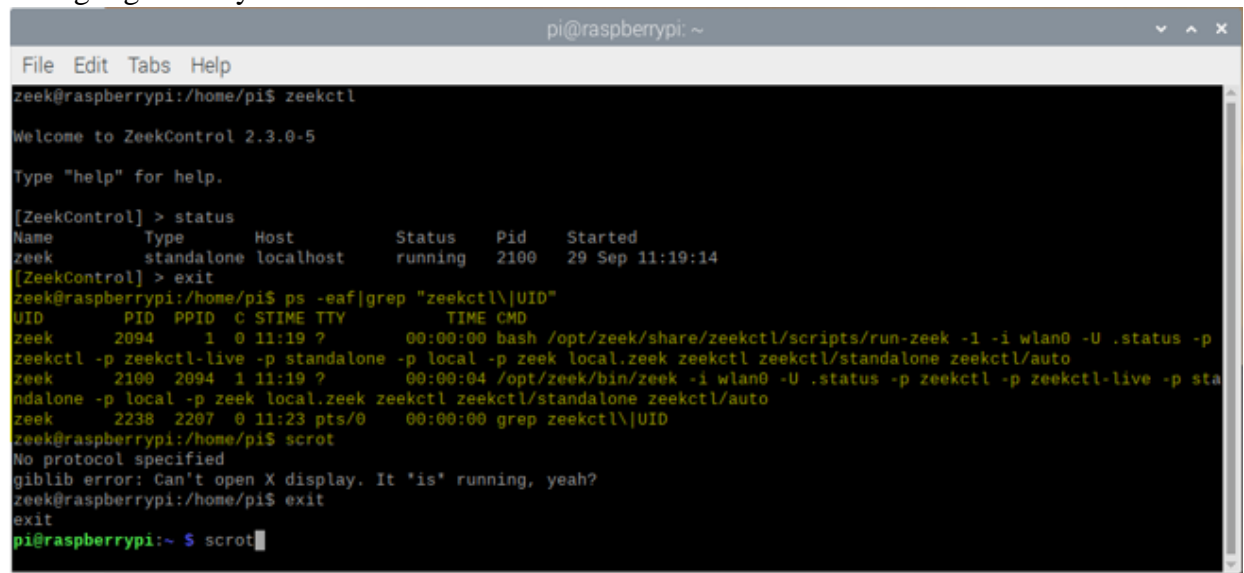
pi@raspberrypi:~$ scrot
```

2. **Zeek Status:** Once the zeek is running, I typed in the command **status** in ZeekControl shell. The zeek was running as we can see in the screenshot below and highlighted in yellow.



```
pi@raspberrypi: ~  
File Edit Tabs Help  
zeek@raspberrypi:/home/pi$ zeekctl  
Welcome to ZeekControl 2.3.0-5  
Type "help" for help.  
[ZeekControl] > status  
Name      Type      Host      Status    Pid      Started  
zeek       standalone localhost running    2100     29 Sep 11:19:14  
[ZeekControl] > exit  
zeek@raspberrypi:/home/pi$ ps -eaf|grep "zeekctl\\|UID"  
UID        PID  PPID  C  STIME TTY          TIME CMD  
zeek       2094      1  0  11:19 ?        00:00:00 bash /opt/zeek/share/zeekctl/scripts/run-zeek -1 -i wlan0 -U .status -p  
zeekctl -p zeekctl-live -p standalone -p local -p zeek local.zeek zeekctl zeekctl/standalone zeekctl/auto  
zeek       2100    2094  1  11:19 ?        00:00:04 /opt/zeek/bin/zeek -i wlan0 -U .status -p zeekctl -p zeekctl-live -p sta  
ndalone -p local -p zeek local.zeek zeekctl zeekctl/standalone zeekctl/auto  
zeek       2238    2207  0  11:23 pts/0    00:00:00 grep zeekctl\\|UID  
zeek@raspberrypi:/home/pi$ scrot  
No protocol specified  
glib error: Can't open X display. It 'is' running, yeah?  
zeek@raspberrypi:/home/pi$ exit  
exit  
pi@raspberrypi:~$ scrot
```

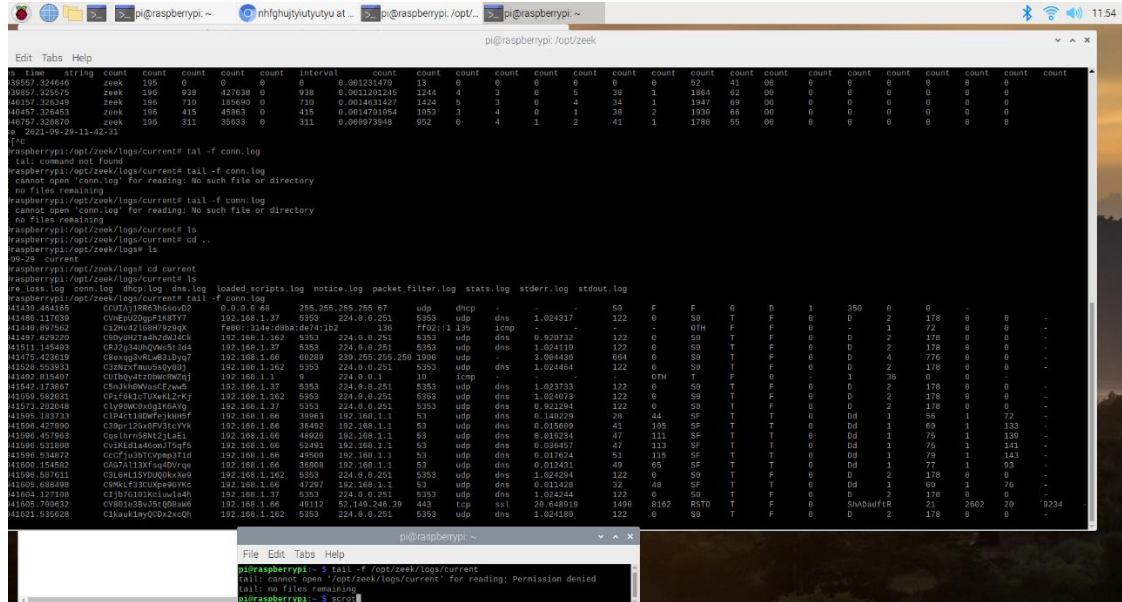
3. **Output of ps -eaf | grep “zeekctl\\|UID”:** While the zeek is up and running I also searched UID of zeekctl file and it was set to user zeek as shown in the screenshot below and highlighted in yellow.



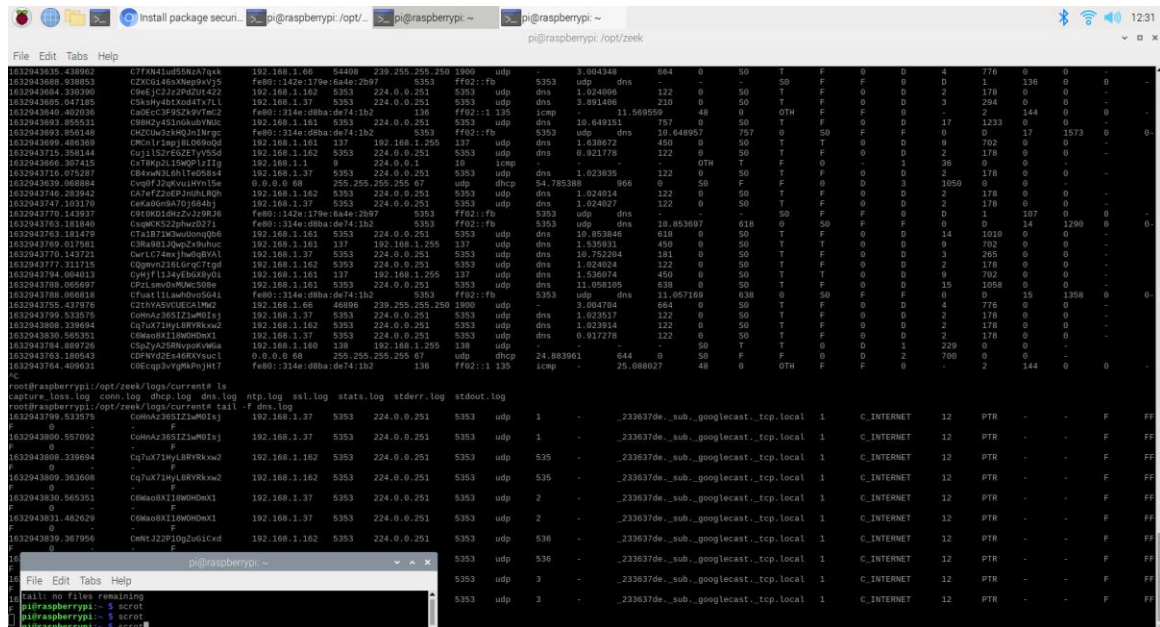
```
pi@raspberrypi: ~  
File Edit Tabs Help  
zeek@raspberrypi:/home/pi$ zeekctl  
Welcome to ZeekControl 2.3.0-5  
Type "help" for help.  
[ZeekControl] > status  
Name      Type      Host      Status    Pid      Started  
zeek       standalone localhost running    2100     29 Sep 11:19:14  
[ZeekControl] > exit  
zeek@raspberrypi:/home/pi$ ps -eaf|grep "zeekctl\\|UID"  
UID        PID  PPID  C  STIME TTY          TIME CMD  
zeek       2094      1  0  11:19 ?        00:00:00 bash /opt/zeek/share/zeekctl/scripts/run-zeek -1 -i wlan0 -U .status -p  
zeekctl -p zeekctl-live -p standalone -p local -p zeek local.zeek zeekctl zeekctl/standalone zeekctl/auto  
zeek       2100    2094  1  11:19 ?        00:00:04 /opt/zeek/bin/zeek -i wlan0 -U .status -p zeekctl -p zeekctl-live -p sta  
ndalone -p local -p zeek local.zeek zeekctl zeekctl/standalone zeekctl/auto  
zeek       2238    2207  0  11:23 pts/0    00:00:00 grep zeekctl\\|UID  
zeek@raspberrypi:/home/pi$ scrot  
No protocol specified  
glib error: Can't open X display. It 'is' running, yeah?  
zeek@raspberrypi:/home/pi$ exit  
exit  
pi@raspberrypi:~$ scrot
```

4. **Events:** For different events and logs, I looked into different log files like conn.log, dns.log, and ssl.log whose screenshots are shown below.

The first event I looked at is the one while I started conn.log where it shows all the logs related to host and target Ip with their signature and ping status. Then, second event I observed is when I connected new device and it showed that in the log. Where IP ending 66 is my PI and the one ending 37 is my phone when I connected my phone and started browsing YouTube.



Third, event I looked at is inside the dns.log file, which contains all the domain name created packets as we can see below where the DNS is using UDP protocol as we can see in the screenshot.



Fourth event I observed was inside ssh.log file. This file was interesting as it showed what I browsed along with Protocol use and DNS name in the plain text as shown in the screenshot below.

pi@raspberrypi: /opt/zeek
13:13

```

File Edit Tabs Help

163294601.989291  CPiFma10NqyVyl1b1  192.168.1.161  137  192.168.1.255  137  udp  dns  1.530844  450  0  S0  T  F  0  0  2  0  762  0  0  -
163294602.027684  C0J1y2z2p21E15v8b  192.168.1.132  5353  224.0.0.251  5353  udp  dns  1.825877  122  0  S0  T  F  0  0  2  2  178  0  0  -
163294604.613630  C0Jwbcxz08Qw02Cq  192.168.1.132  5353  224.0.0.251  5353  udp  dns  1.823620  122  0  S0  T  F  0  0  2  2  178  0  0  -
163294605.516059  C0Jwbcxz08Qw02Cq  192.168.1.37  5353  224.0.0.251  5353  udp  dns  1.024241  122  0  S0  T  F  0  0  2  2  178  0  0  -
163294607.641106  C0Jwbcxz08Qw02Cq  192.168.1.162  5353  224.0.0.251  5353  udp  dns  1.824240  122  0  S0  T  F  0  0  2  2  178  0  0  -
1632946084.33783  C0Jwbcxz08Qw02Cq  192.168.1.37  5353  224.0.0.251  5353  udp  dns  0.822683  122  0  S0  T  F  0  0  2  2  178  0  0  -
163294609.752973  CjGd7Bg5dmPDJA08  192.168.1.166  59435  239.255.255.250  1900  udp  -  3.004744  664  0  S0  T  F  0  0  2  4  776  0  0  -
163294608.488254  C0j1n34z1pYrrYn  192.168.1.88  5353  224.0.0.251  5353  udp  dns  1.822627  450  0  S0  T  F  0  0  2  2  506  0  0  -
1632946078.708740  CjGd4nrfF72Y00b6  F680:114d:1f2c:d392:3b41  5353  f680:1f2c:  1.022202  450  0  S0  T  F  0  0  2  2  846  0  0  -
1632946072.050611  C0w1Scd1fy723H114  192.168.1.161  137  192.168.1.255  137  udp  dns  1.571594  900  0  S0  T  T  0  0  2  18  1404  0  0  -
1632946066.215488  C0fMa2bzdbMwK3eh  192.168.1.161  5353  224.0.0.251  5353  udp  dns  26.827918  1264  0  S0  T  F  0  0  2  29  2076  0  0  -
163294606.219072  C0fMa2bzdbMwK3eh  F680:114d:1f2c:d392:3b41  5353  f680:1f2c:  1.022202  450  0  S0  T  F  0  0  2  2  846  0  0  -
1632946104.614760  C0w02Zb5b8fV7Ue6  192.168.1.355  5353  224.0.0.251  5353  udp  dns  -  50  T  F  0  0  2  1  96  0  0  -
1632946104.615017  C41Hm4M4C0Pm1n1  F680:145d:48f5:2b6f:f7a5  5353  f680:1f2c:  1.022202  450  0  S0  T  F  0  0  2  1  116  0  0  -
1632946104.615252  C044b380f0Pm1n1  192.168.1.161  5353  224.0.0.251  5353  udp  dns  -  50  T  F  0  0  2  1  178  0  0  -
1632946104.617525  Cj8U2z1l683n3j96  F680:11022:7494:2108:4021  5353  f680:1f2c:  1.022202  450  0  S0  T  F  0  0  2  1  144  0  0  -
1632946102.768879  C3BqBg2bMwK3eh  192.168.1.162  5353  224.0.0.251  5353  udp  dns  1.824252  122  0  S0  T  F  0  0  2  2  178  0  0  -
1632946102.769032  C3BqBg2bMwK3eh  192.168.1.37  5353  224.0.0.251  5353  udp  dns  1.823517  122  0  S0  T  F  0  0  2  2  178  0  0  -
1632946133.697447  C0y13z13z3u5uWd  192.168.1.162  5353  224.0.0.251  5353  udp  dns  1.126132  122  0  S0  T  F  0  0  2  2  178  0  0  -
1632946138.612249  C0fMa2bzdbMwK3eh  192.168.1.161  137  192.168.1.255  137  udp  dns  1.696322  900  0  S0  T  T  0  0  2  18  1404  0  0  -
1632946138.612249  C0fMa2bzdbMwK3eh  192.168.1.37  5353  224.0.0.251  5353  udp  dns  1.773844  1231  0  S0  T  F  0  0  2  20  2915  0  0  -
1632946124.278644  C0YncrC1YwM9uWv9  F680:114d:dbba:de74:1b2  5353  f680:1f2c:  1.773179  1231  0  S0  T  F  0  0  2  28  2575  0  0  -
1632946146.497709  C0Yix15TLwq1KdX41  192.168.1.37  5353  224.0.0.251  5353  udp  dns  1.823818  122  0  S0  T  F  0  0  2  2  178  0  0  -
1632946164.622487  C0fC7B451d4e6A03M  192.168.1.162  5353  224.0.0.251  5353  udp  dns  1.824185  122  0  S0  T  F  0  0  2  2  178  0  0  -

```

```

root@raspberrypi: /opt/zeek/logs/current#
root@raspberrypi: /opt/zeek/logs/current# ls
conn.log  dhcp.log  dns.log  stats.log  stderr.log
root@raspberrypi: /opt/zeek/logs/current# cd ..
root@raspberrypi: /opt/zeek/logs# cd current
root@raspberrypi: /opt/zeek/logs/current# ls
conn.log  dhcp.log  dns.log  stats.log  stderr.log  stdout.log
root@raspberrypi: /opt/zeek/logs/current# cd ..
root@raspberrypi: /opt/zeek/logs# cd current
root@raspberrypi: /opt/zeek/logs/current# ls
conn.log  dhcp.log  dns.log  stats.log  stderr.log  stdout.log

```

```

pi@raspberrypi: /opt/zeek

File Edit Tabs Help

pi@raspberrypi:~$ sudo
pi@raspberrypi:~$ sudo
pi@raspberrypi:~$ sudo
pi@raspberrypi:~$ sudo

```