Lab #2: Raspberry PI as Network Monitor using Zeek

Lab Overview

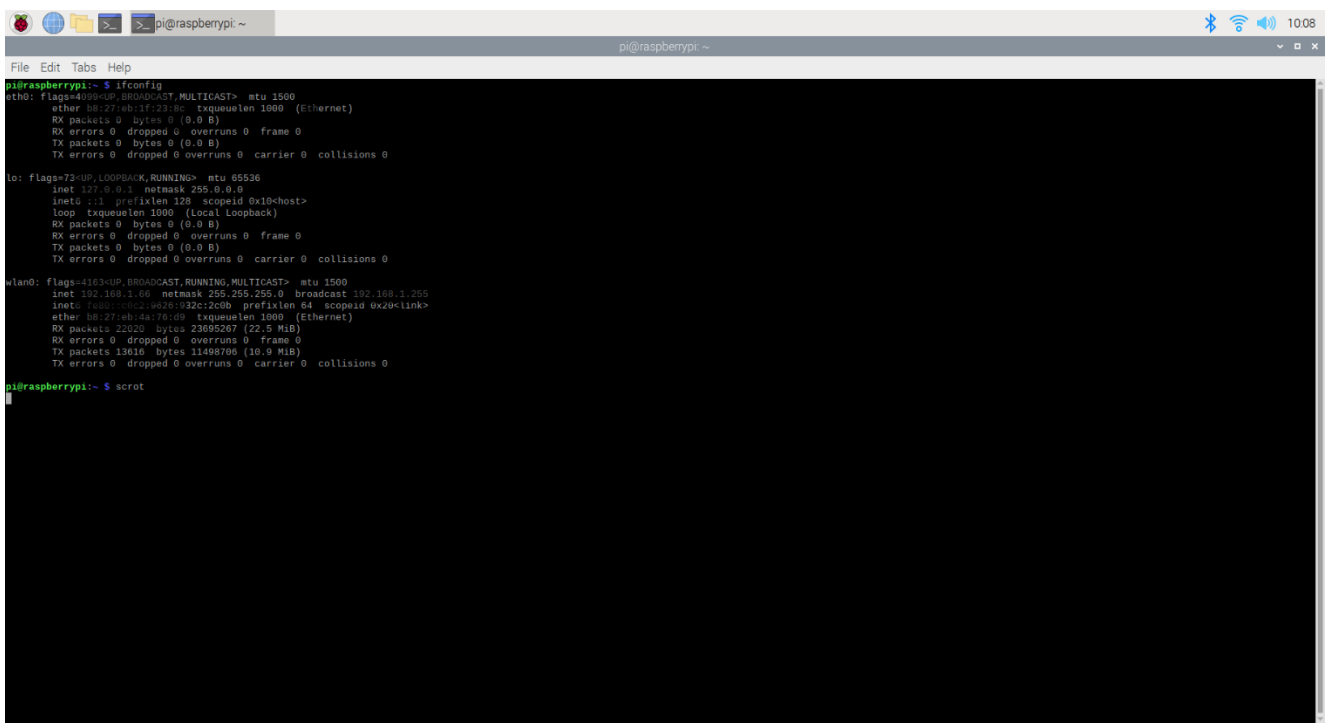
This lab introduces network monitoring tool called zeek, which will be used in our raspberry PI to observe our network traffic and analyze different events in our network.

Requirements

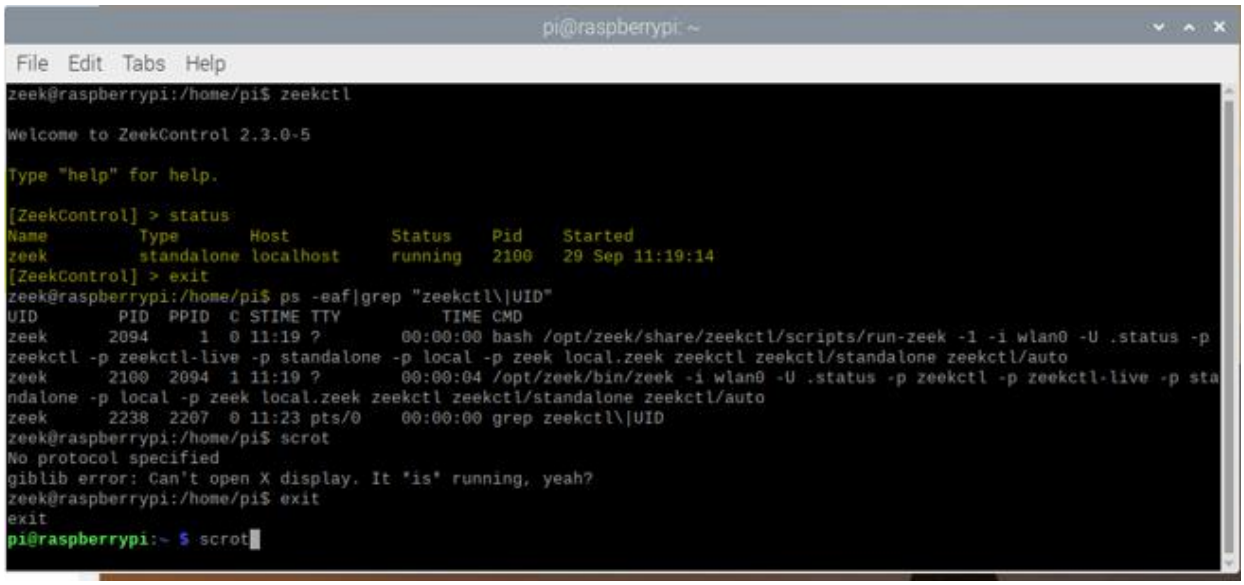
This lab requires properly configured and secure raspberry PI with the proper set up which was done in lab 1. This lab also requires installing zeek which was a bit of trouble at the beginning, but I figured out the way to properly install and configure zeek.

Tasks

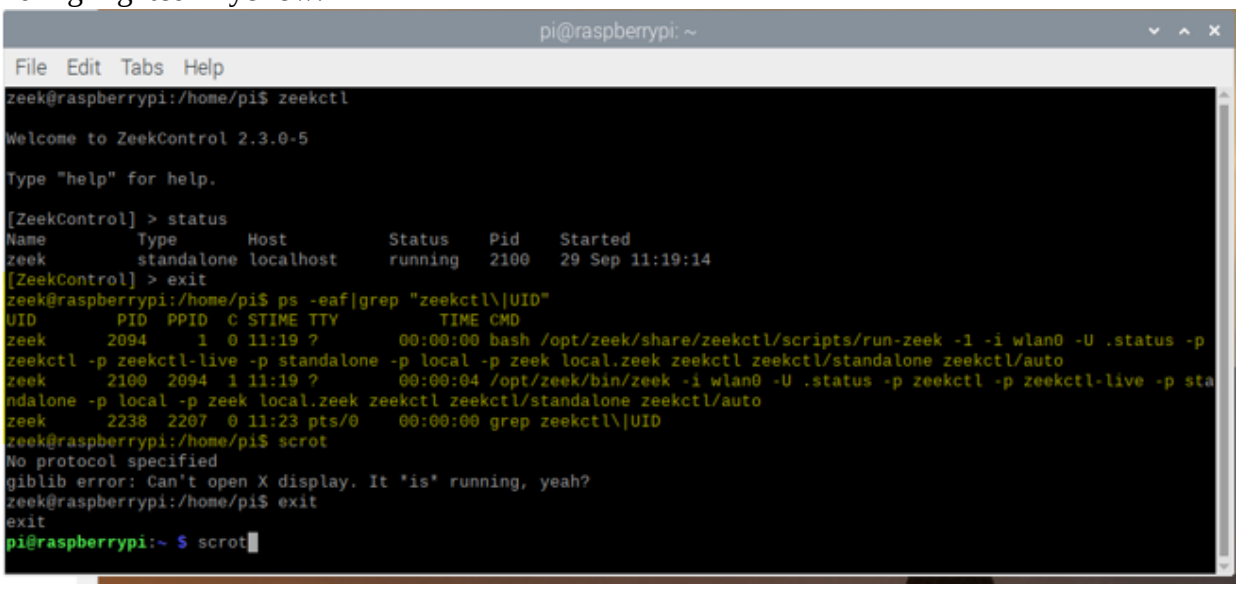
1. **PI's local IP and Mac Address:** While doing this lab the following were by IP addresses and MAC address which is obtained by using command **ifconfig** in my raspberry PI terminal.



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.

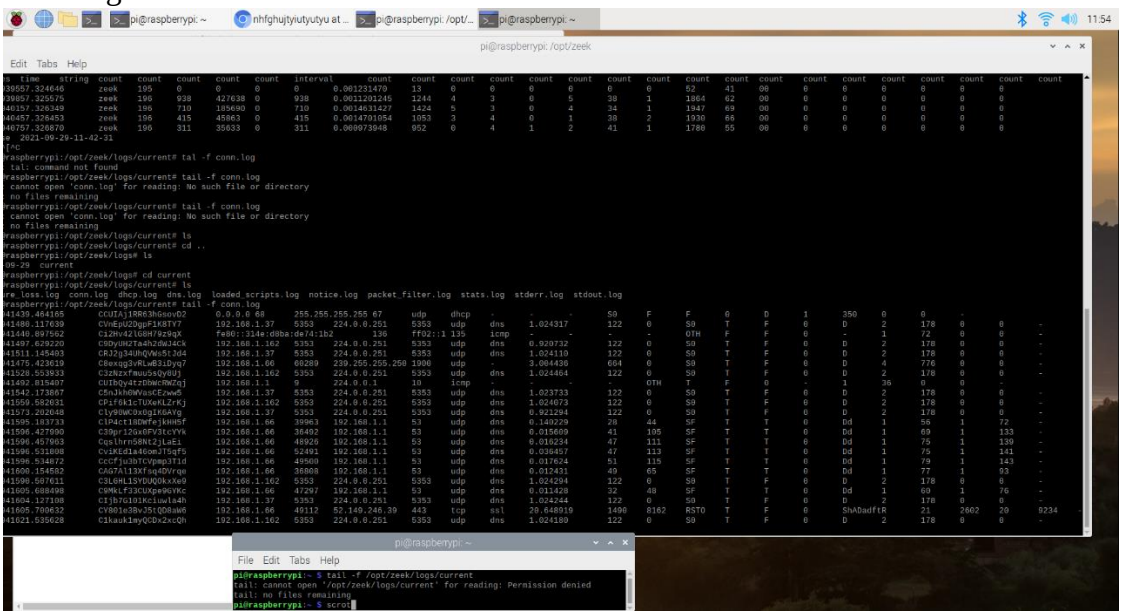


3. **Output of ps -eaf | grep "zeekctl\|UID":** While the zeek is up and running I also searched UID of zeekctl file and it was set to user zeek as shown in the screenshot below and highlighted in yellow.

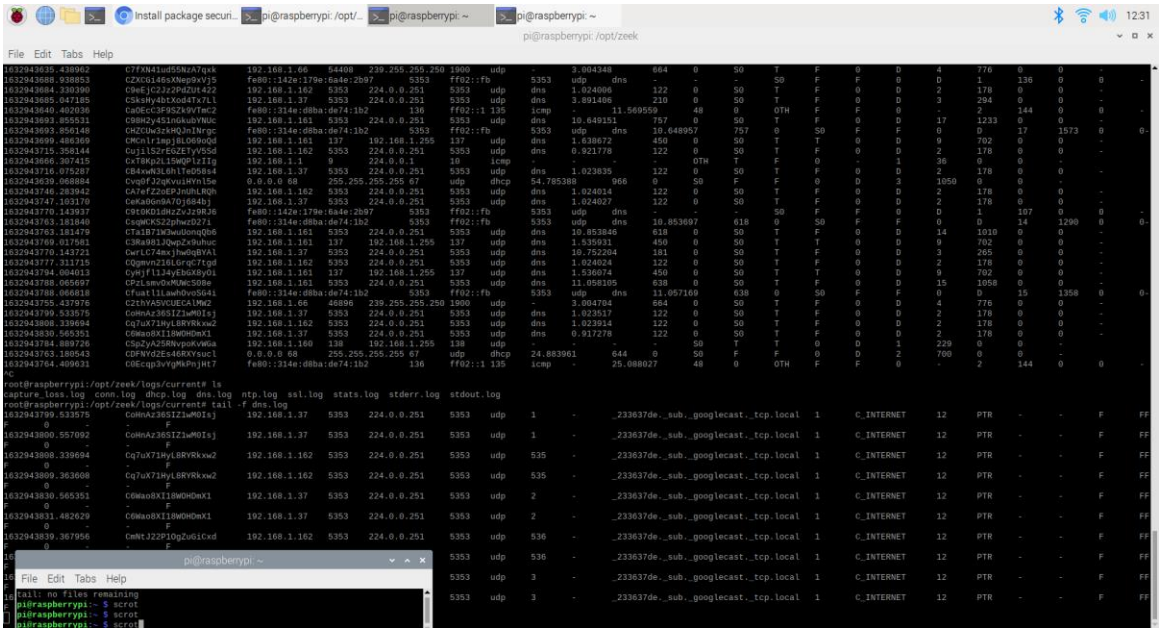


4. **Events**: For different events and logs, I looked into different log files like conn.log, dns.log, and ssl.log whose screenshots are shown below.

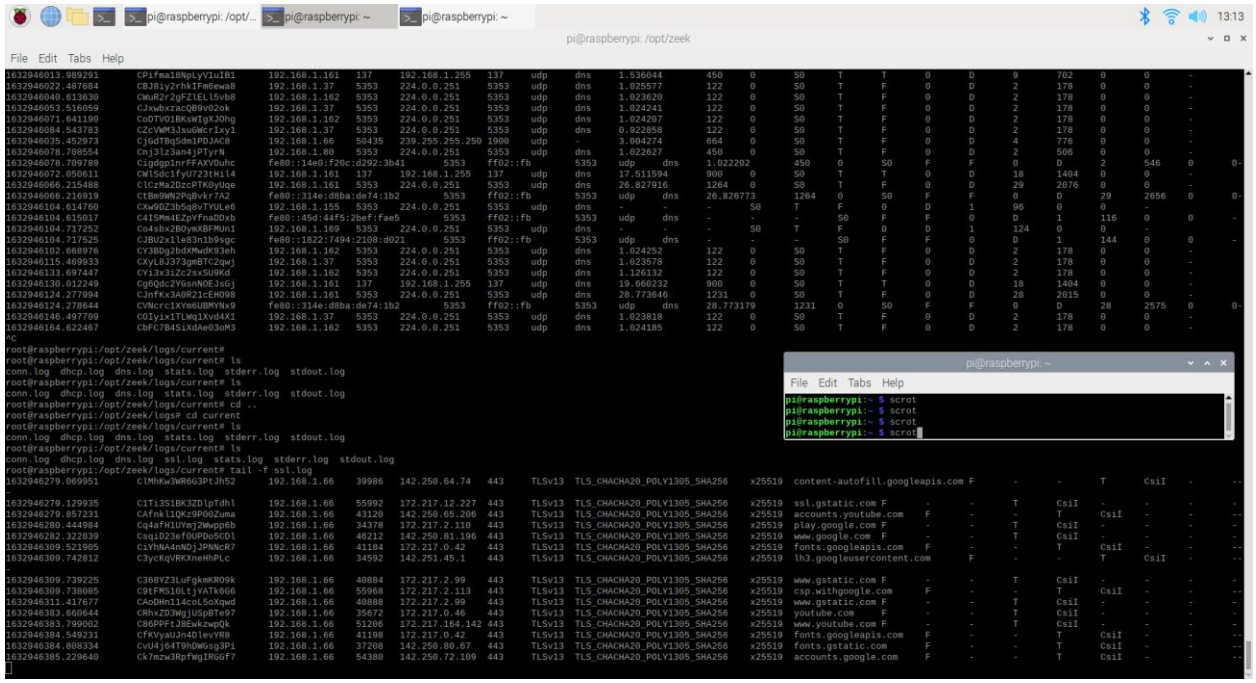
The first event I looked at is the one while I started conn.log where it shows all the logs related to host and target Ip with their signature and ping status. Then, second event I observed is when I connected new device and it showed that in the log. Where IP ending 66 is my PI and the one ending 37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



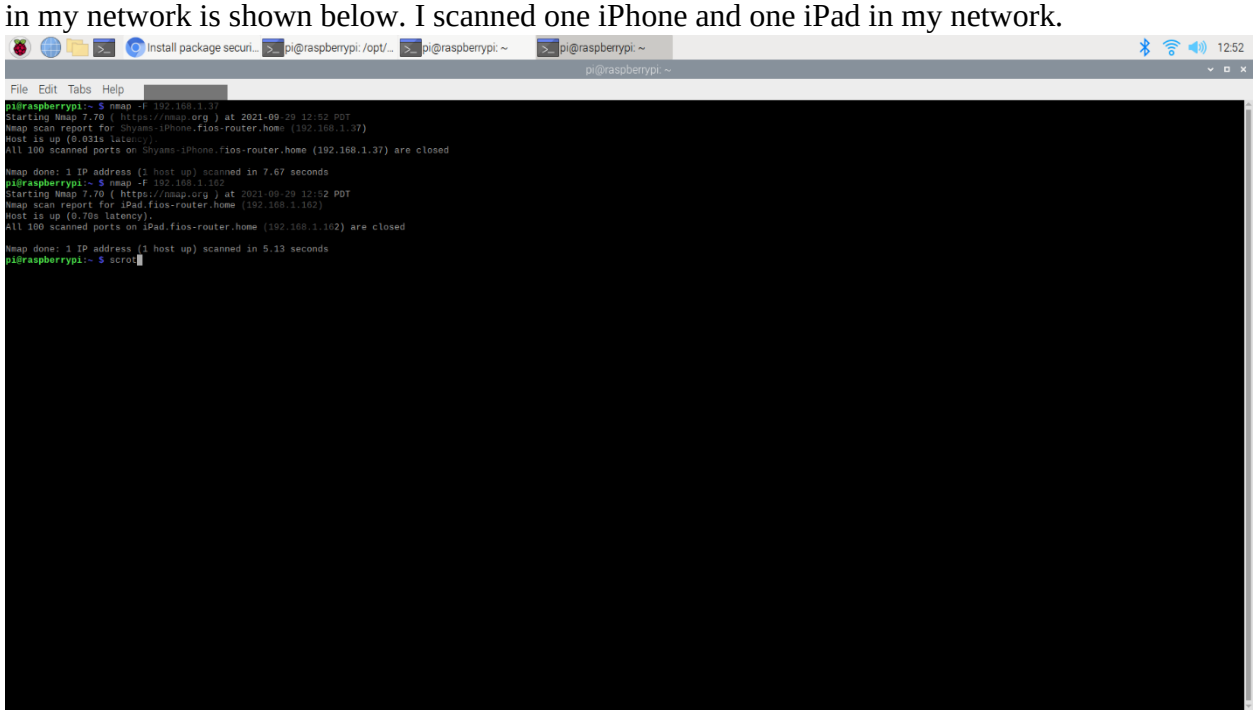
Third, event I looked at is inside the dns.log file, which contains all the domain name created packets as we can see below where the DNS is using UDP protocol as we can see in the screenshot.



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.



5. **Port Scan of different device in network**: I used nmap to scan two different devices in my network and saw if any ports were open, the result of the port scan of different device in my network is shown below. I scanned one iPhone and one iPad in my network.



6. **Analysis of a unique event**: For the analysis of a unique event, I took an example from the ssh.log file which I found was the interesting log file as we can see what site is being browsed by the device. As we can see in the screenshot below, when I typed youtube.com, from my PI with IP 198.168.1.66 the SSL connection was started and it led

me to IP 172.217.164.142 form port 443. Along with the connection we can see that the unique certificate is created for each event which can be seen in second column. This led me to www.youtube.com as we can see in the screenshot. It loaded all the fonts required and the prompted me to do account login as we can see in the screenshot. Thus, From the screenshot below we can see the SSH log along with the sites being browsed.