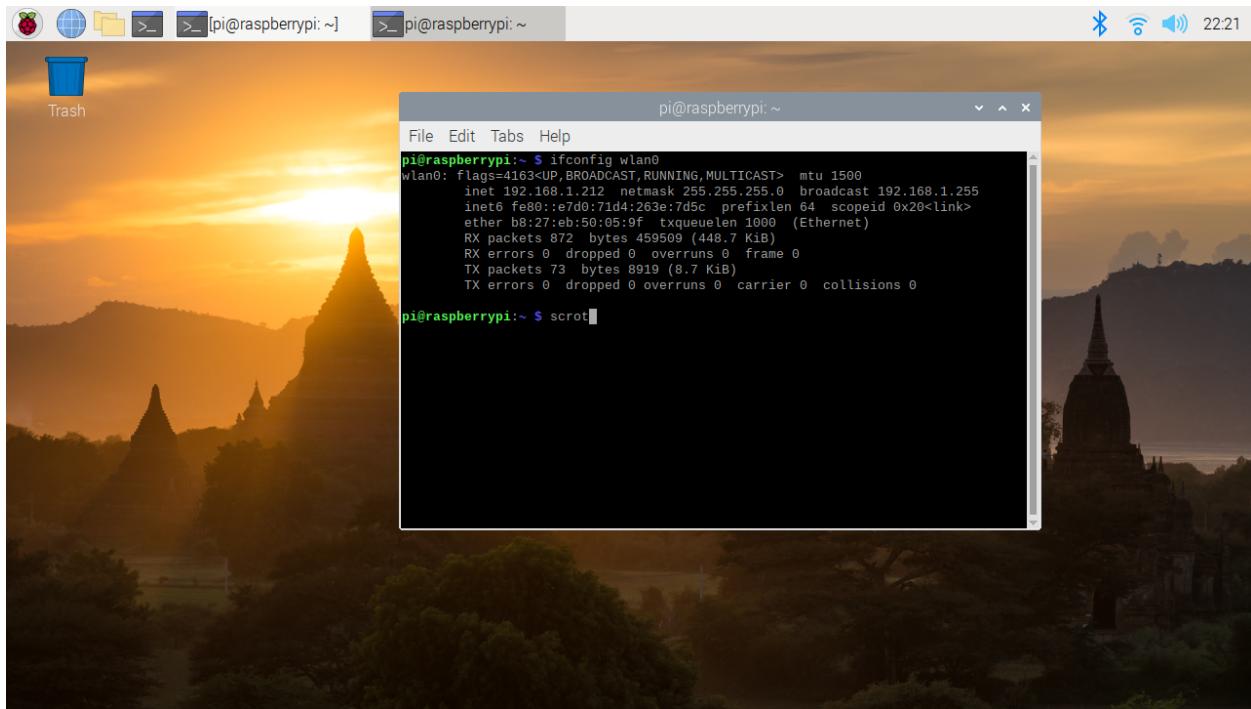
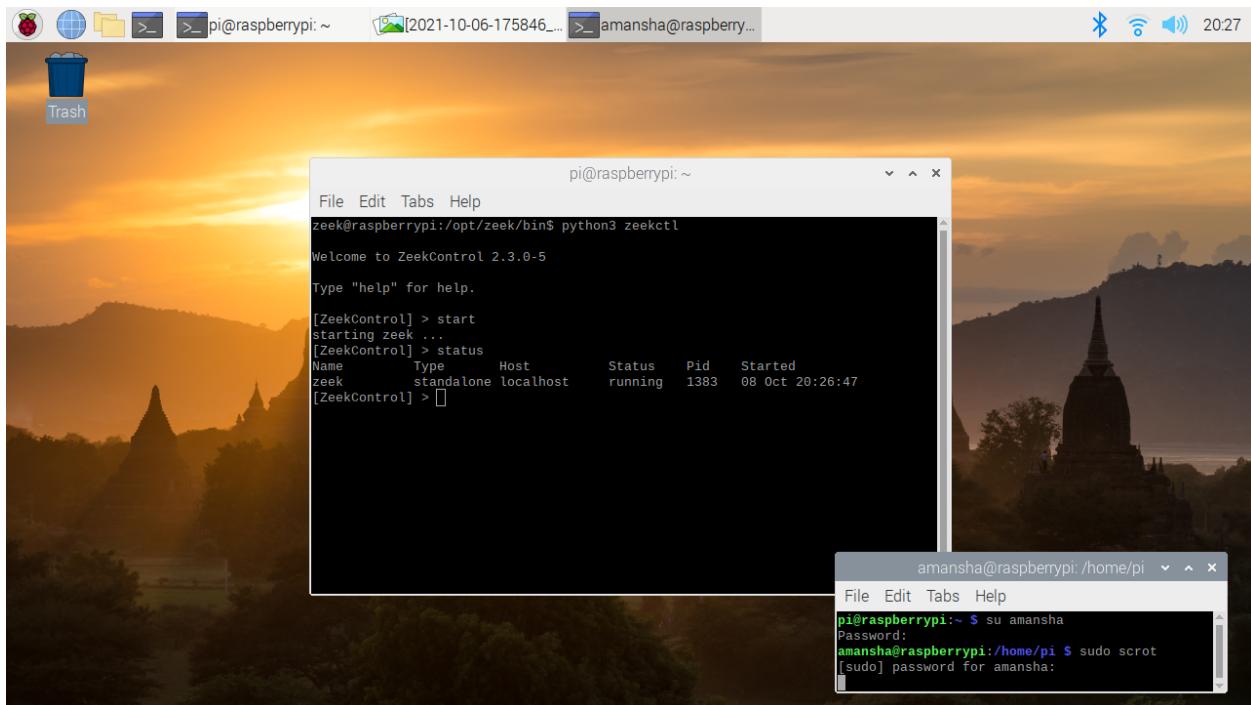


Amir Mansha
Lab #2

2.



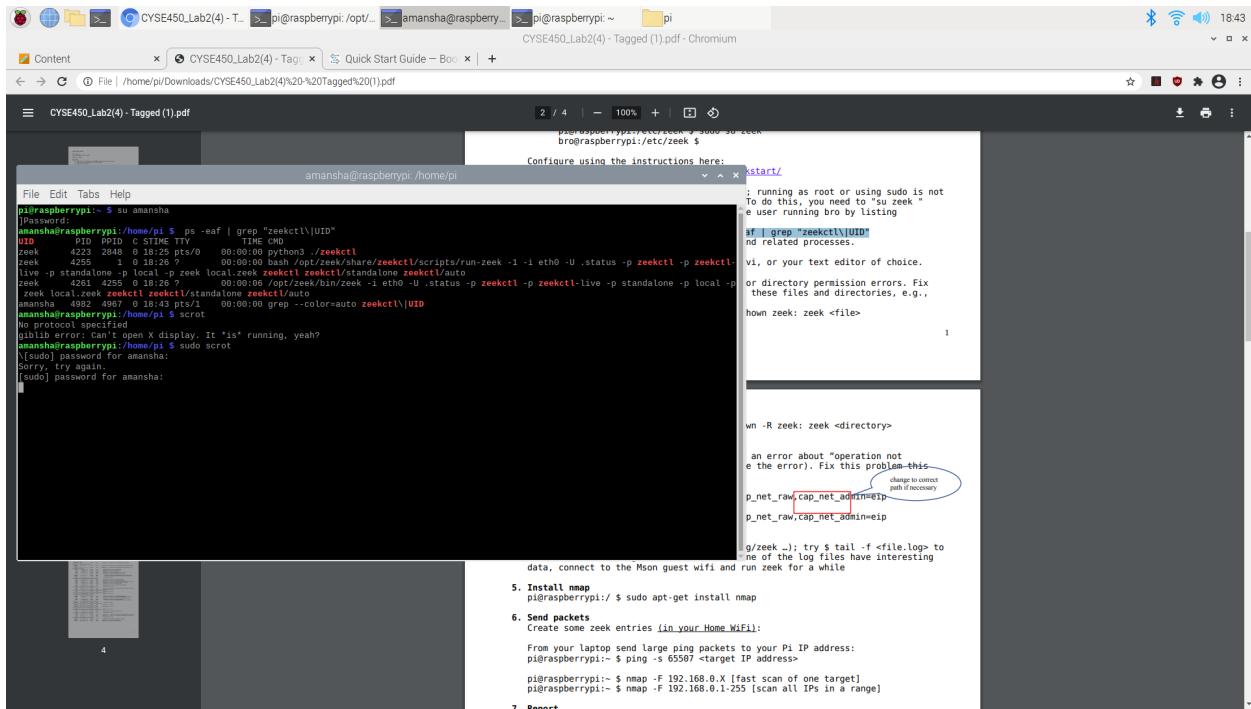
3.



Amir Mansha

Lab #2

4.



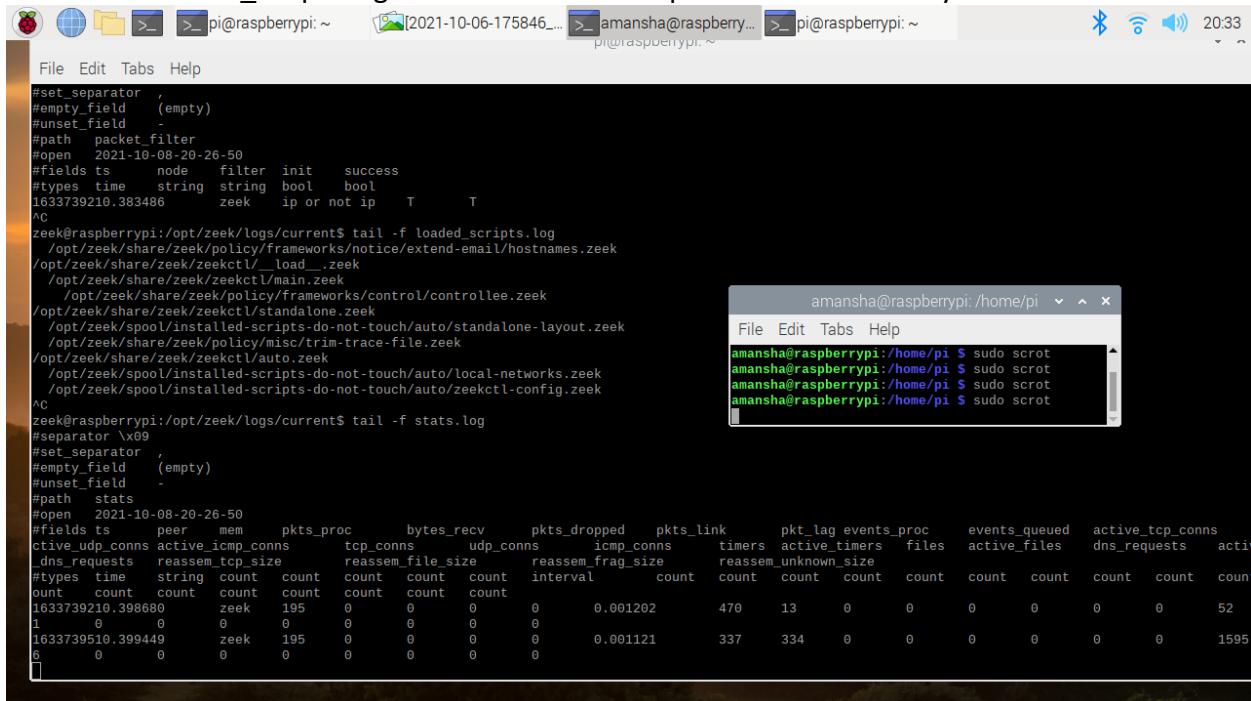
The screenshot shows a Chromium browser window displaying a PDF titled 'CYSE450_Lab2(4)-Tagged(1).pdf'. The PDF content includes a terminal session on a Raspberry Pi running Raspbian. The terminal shows the user attempting to run Zeek as root or sudo, which fails due to permission errors. A specific error message is highlighted with a red circle: 'an error about "operation not supported by the error". Fix this problem - this change to correct path if necessary'. The terminal also shows the user trying to install nmap and sending packets to a target IP address.

```
pi@raspberrypi: ~$ su amansha
[pi@raspberrypi: /home/pi]$ ps -ef | grep "zeekctl|UID"
UID      PID  PPID  C STIME TT%  TIME CMD
zeek     4223  2848  0 16:25 pts/0    00:00:00 python3 ./zeekctl
zeek     4255  1  0 16:26 ?    00:00:00 bash /opt/zeek/share/zeekctl/scripts/run-zeek -i eth0 -U .status -p zeekctl -p zeekctl
[...]
zeekctl standalone zeekctl/standalone zeekctl/auto
zeek local.zeek zeekctl zeekctl/standalone zeekctl/auto
amansha 4982 4967  0 16:43 pts/1    00:00:00 grep --color=auto zeekctl|UID
pi@raspberrypi: /home/pi$ scrot
[...]
glibib: Can't open X display. It 'is' running, yeah?
amansha@raspberrypi: /home/pi$ sudo scrot
Xlib:  extension "Composite" not present
Sorry, try again.
[sudo] password for amansha:
```

5.

5.

I think the Loaded_scripts.log file means all the scripts that are loaded by zeek.



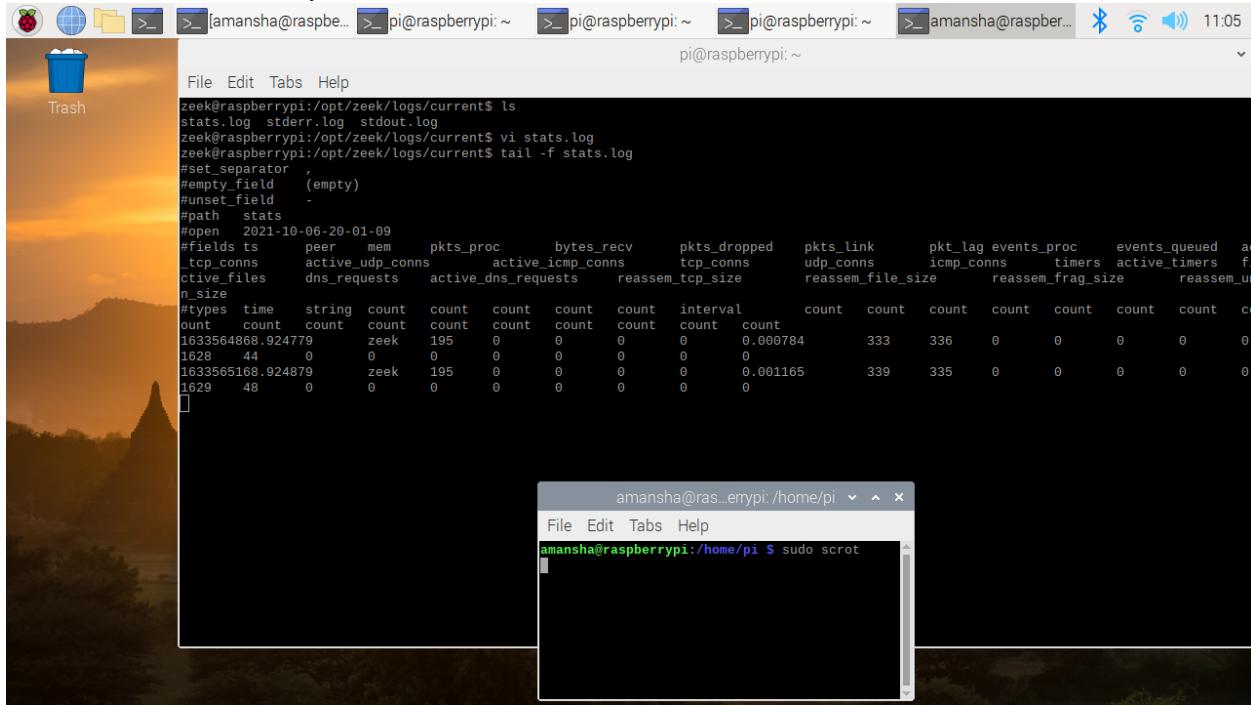
The screenshot shows a terminal window on a Raspberry Pi. The user has run the command 'tail -f loaded_scripts.log' to view the contents of the 'loaded_scripts.log' file. The log file lists several Zeek scripts and their configuration details. Below the log, another terminal window shows the user running the 'scrot' command multiple times to capture screenshots of the terminal session.

```
#set_separator '
#empty_field (empty)
#unset_field -
#path packet_filter
#open 2021-10-08-20-26-50
#fields ts node filter init success
#types time string string bool bool
1633739210.383486 zeek ip or not ip T T
^C
zeek@raspberrypi:/opt/zeek/logs/current$ tail -f loaded_scripts.log
/opt/zeek/share/zeek/policy/frameworks/notice/extend-email/hostnames.zeek
/opt/zeek/share/zeek/zeekctl/_load_zeek
/opt/zeek/share/zeek/zeekctl/main.zeek
/opt/zeek/share/zeek/policy/control/controllee.zeek
/opt/zeek/share/zeek/zeekctl/standalone.zeek
/opt/zeek/spool/installed-scripts/do-not-touch/auto/standalone-layout.zeek
/opt/zeek/share/zeek/policy/misc/trim-trace-file.zeek
/opt/zeek/share/zeek/zeekctl/auto.zeek
/opt/zeek/spool/installed-scripts/do-not-touch/auto/local-networks.zeek
/opt/zeek/spool/installed-scripts/do-not-touch/auto/zeekctl-config.zeek
^C
zeek@raspberrypi:/opt/zeek/logs/current$ tail -f stats.log
#separator \x09
#set_separator '
#empty_field (empty)
#unset_field -
#path stats
#open 2021-10-08-20-26-50
#fields ts peer mem pkts_recv bytes_recv pkts_dropped pkts_link pkt_lag events_proc events_queued active_tcp_conns
active_udp_conns active_icmp_conns tcp_conns udp_conns icmp_conns timers active_timers files active_files dns_requests active
dns_requests reassem_tcp_size reassem_file_size reassem_frag_size reassem_unknown_size
#types time string count count count count interval count count
1633739210.398680 zeek 195 0 0 0 0 0 0.001202 470 13 0 0 0 0 0 0 52
1633739510.399449 zeek 195 0 0 0 0 0 0.001121 337 334 0 0 0 0 0 0 1595
6 0 0 0 0 0 0 0 0
```

File Edit Tabs Help
amansha@raspberrypi: /home/pi \$ sudo scrot
amansha@raspberrypi: /home/pi \$ sudo scrot
amansha@raspberrypi: /home/pi \$ sudo scrot
amansha@raspberrypi: /home/pi \$ sudo scrot

Amir Mansha
Lab #2

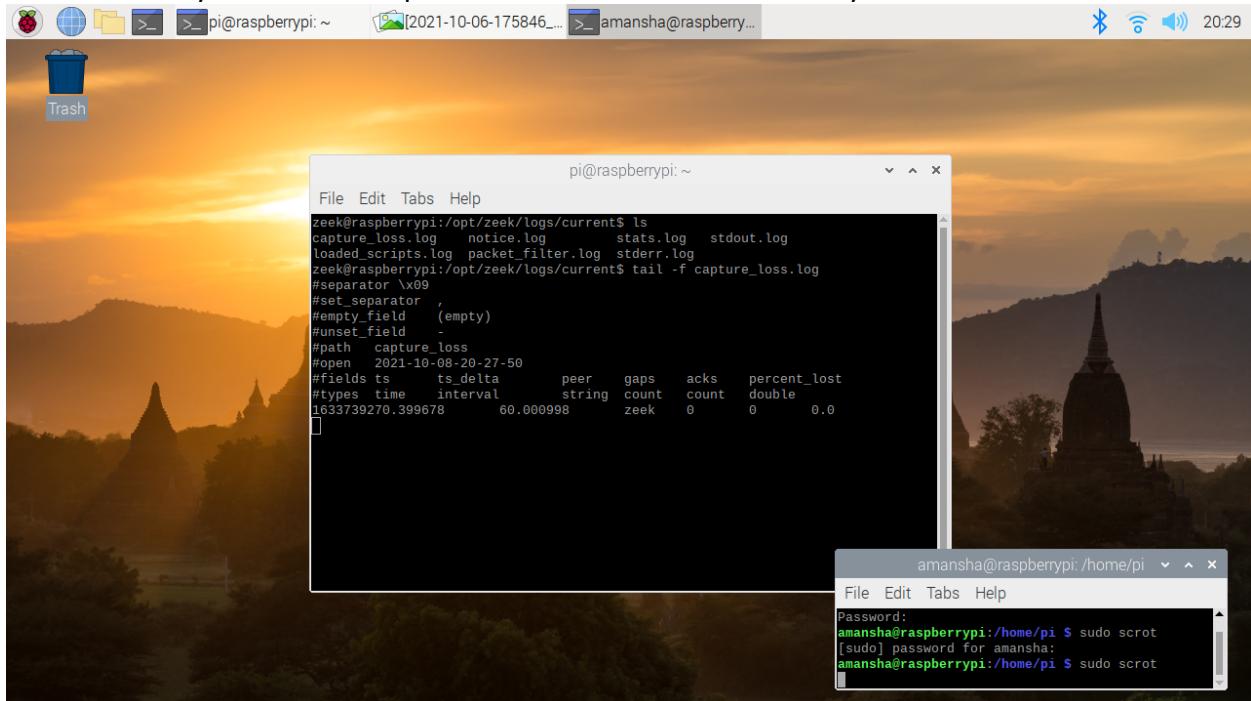
In the stats.log file there are 2 events. I think it means it logged 2 packets and their statistics such as their time stamp and time interval.



```
zeek@raspberrypi:/opt/zeek/logs/current$ ls
stats.log stderr.log stdout.log
zeek@raspberrypi:/opt/zeek/logs/current$ tail -f stats.log
#separator ,
#empty_field  (empty)
#unset_field -
#path  stats
#open 2021-10-06-20-01-09
#fields ts peer mem pkts_proc bytes_recv pkts_dropped pkts_link pkt_lag events_proc events_queued ac
_ltcp_conn active_udp_conn active_icmp_conn tcp_conn udp_conn icmp_conn timers active_timers f
ctive_files dns_requests active_dns_requests reassem_tcp_size reassem_file_size reassem_frag_size reassem_ur
n_size
#types time string count count count count count interval count count count count count count count count
count count count count count count count count count count count count count count count count count count
1633564868.924779 zeek 195 0 0 0 0 0 0.000784 333 336 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1628 44 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1633565108.924879 zeek 195 0 0 0 0 0 0.001165 339 335 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1629 48 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

```
amansha@raspberrypi:/home/pi $ sudo scrot
```

There is 1 event in the capture_loss.log file that I think it means the when the packet loss of the time rate. It says the timestamp and the time interval of the delay.



```
zeek@raspberrypi:/opt/zeek/logs/current$ ls
capture_loss.log notice.log stats.log stderr.log
loaded_scripts.log packet_filter.log stderr.log
zeek@raspberrypi:/opt/zeek/logs/current$ tail -f capture_loss.log
#separator \x09
#empty_field  (empty)
#unset_field -
#path  capture_loss
#open 2021-10-08-20-27-50
#fields ts ts_delta peer gaps acks percent_lost
#types time interval string count count double
1633739270.399678 60.000998 zeek 0 0 0.0
```

```
amansha@raspberrypi:/home/pi $ sudo scrot
```

```
Password: amansha@raspberrypi:/home/pi $ sudo scrot
[sudo] password for amansha:
amansha@raspberrypi:/home/pi $ sudo scrot
```

Amir Mansha
Lab #2

6.
I port scanned my sister's laptop.

```
pi@raspberrypi:~ $ su amansha
Password:
amansha@raspberrypi:/home/pi $ sudo scrot
[sudo] password for amansha:

pi@raspberrypi:~ $ nmap -F 192.168.1.153
Starting Nmap 7.70 ( https://nmap.org ) at 2021-10-08 10:51 EDT
Nmap scan report for 192.168.1.153
Host is up (0.022s latency).
All 100 scanned ports on 192.168.1.153 are closed

Nmap done: 1 IP address (1 host up) scanned in 2.83 seconds
pi@raspberrypi:~ $ nmap -F 192.168.1.202
Starting Nmap 7.70 ( https://nmap.org ) at 2021-10-08 10:52 EDT
Nmap scan report for 192.168.1.202
Host is up (0.0086s latency).
Not shown: 94 closed ports
PORT      STATE     SERVICE
106/tcp   filtered pop3pw
515/tcp   filtered printer
3000/tcp  filtered ppp
3128/tcp  filtered squid-http
5900/tcp  filtered vnc
8009/tcp  filtered ajp13

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
```

Amir Mansha
Lab #2

7.

In the notice.log file, it means what zeek notices when things are unusual. Since I was in a isolated home network, zeek did not pick up that much traffic.