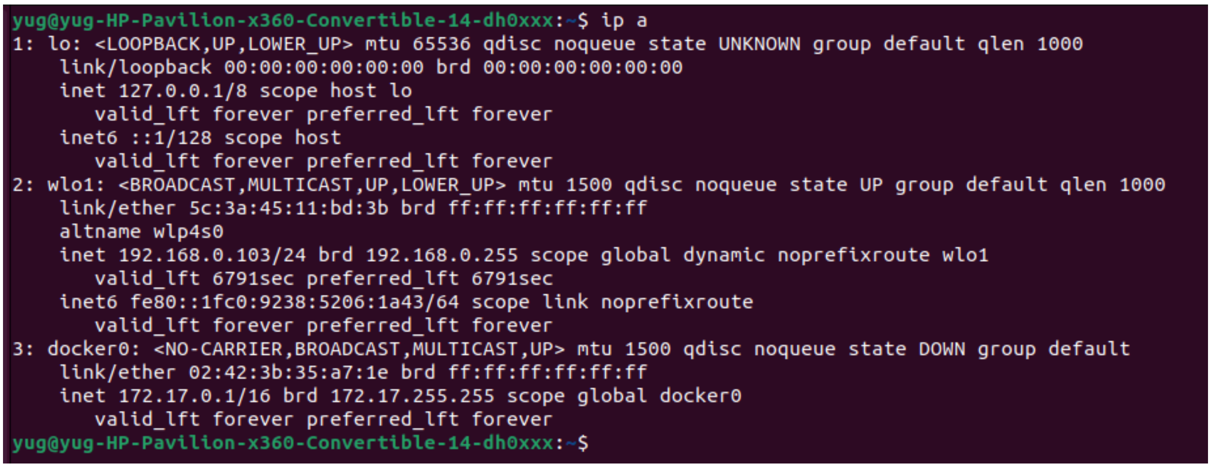
Assignment 8 - Hands on with Zeek

Name - Bhargav Patel
Roll no. - cs23mtech11026

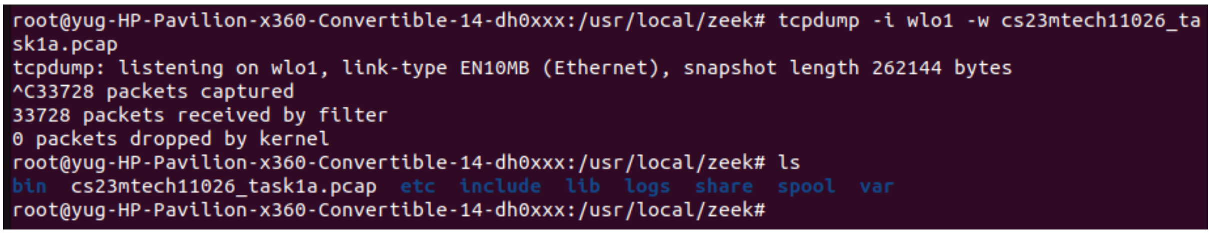
TASK - 1A

1. Checked the interface in which we are going to capture the traffic.



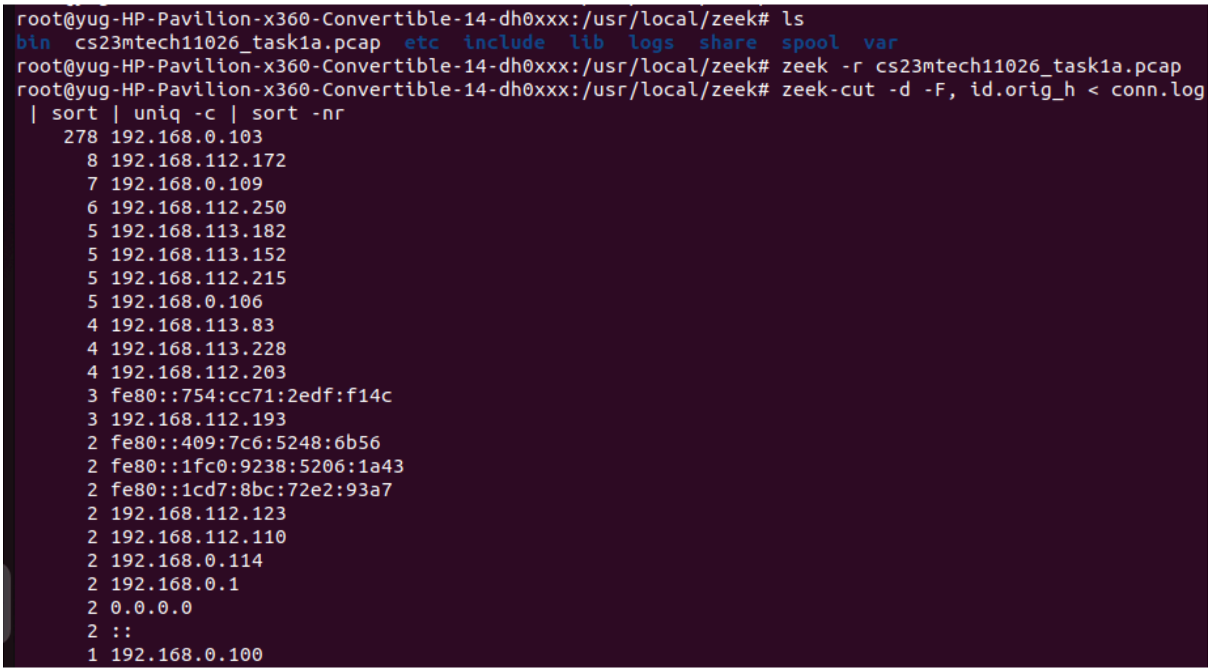
```
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 5c:3a:45:11:bd:3b brd ff:ff:ff:ff:ff:ff
    altname wlp4s0
    inet 192.168.0.103/24 brd 192.168.0.255 scope global dynamic noprefixroute wlo1
       valid_lft 6791sec preferred_lft 6791sec
    inet6 fe80::1fc0:9238:5206:1a43/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:3b:35:a7:1e brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
yug@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:~$
```

2. Captured the traffic for 10 mins and stored in cs23mtech11026_task1a.pcap



```
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# tcpdump -i wlo1 -w cs23mtech11026_ta
sk1a.pcap
tcpdump: listening on wlo1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C33728 packets captured
33728 packets received by filter
0 packets dropped by kernel
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# ls
bin  cs23mtech11026_task1a.pcap  etc  include  lib  logs  share  spool  var
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek#
```

3. To show the source IP addresses that generated the most network traffic and organised them in descending order by using the following sequence of command.
   "zeek -r cs23mtech11026_task1a.pcap"
   "zeek-cut -d -F, id.orig_h < conn.log | sort | uniq -c | sort -nr"

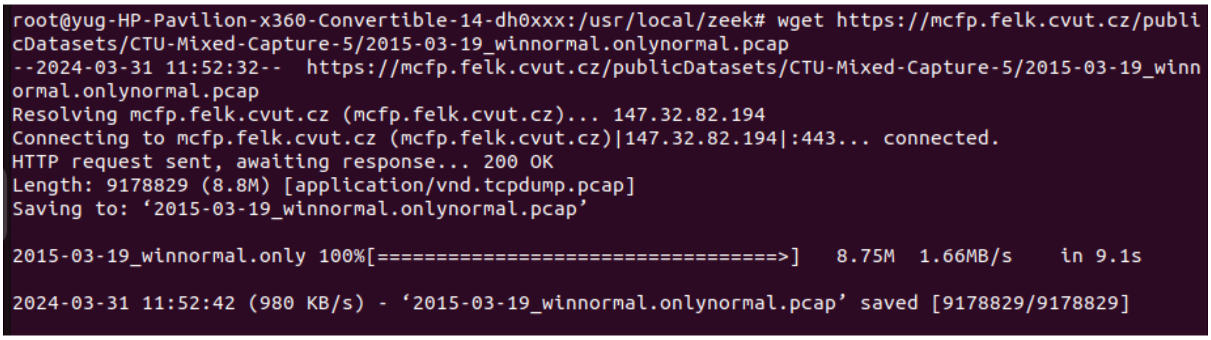


```
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# ls
bin  cs23mtech11026_task1a.pcap  etc  include  lib  logs  share  spool  var
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# zeek -r cs23mtech11026_task1a.pcap
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# zeek-cut -d -F, id.orig_h < conn.log
 | sort | uniq -c | sort -nr
    278 192.168.0.103
      8 192.168.112.172
      7 192.168.0.109
      6 192.168.112.250
      5 192.168.113.182
      5 192.168.113.152
      5 192.168.112.215
      5 192.168.0.106
      4 192.168.113.83
      4 192.168.113.228
      4 192.168.112.203
      3 fe80::754:cc71:2edf:f14c
      3 192.168.112.193
      2 fe80::409:7c6:5248:6b56
      2 fe80::1fc0:9238:5206:1a43
      2 fe80::1cd7:8bc:72e2:93a7
      2 192.168.112.123
      2 192.168.112.110
      2 192.168.0.114
      2 192.168.0.1
      2 0.0.0.0
      2 ::
      1 192.168.0.100
```

TASK - 1B

Link to pcap file that I have used for task 1b-
https://mcfp.felk.cvut.cz/publicDatasets/CTU-Mixed-Capture-5/2015-03-19_winnormal.onlynormal.pcap

1. Downloaded the pcap file using wget

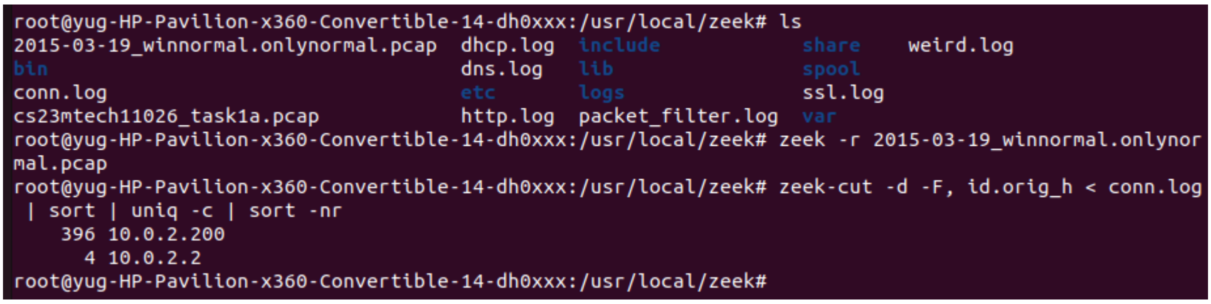


```
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# wget https://mcfp.felk.cvut.cz/publi
cDatasets/CTU-Mixed-Capture-5/2015-03-19_winnormal.onlynormal.pcap
--2024-03-31 11:52:32--  https://mcfp.felk.cvut.cz/publicDatasets/CTU-Mixed-Capture-5/2015-03-19_winn
ormal.onlynormal.pcap
Resolving mcfp.felk.cvut.cz (mcfp.felk.cvut.cz)... 147.32.82.194
Connecting to mcfp.felk.cvut.cz (mcfp.felk.cvut.cz)|147.32.82.194|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9178829 (8.8M) [application/vnd.tcpdump.pcap]
Saving to: ‘2015-03-19_winnormal.onlynormal.pcap’

2015-03-19_winnormal.only 100%[==================================>]   8.75M  1.66MB/s    in 9.1s

2024-03-31 11:52:42 (980 KB/s) - ‘2015-03-19_winnormal.onlynormal.pcap’ saved [9178829/9178829]
```

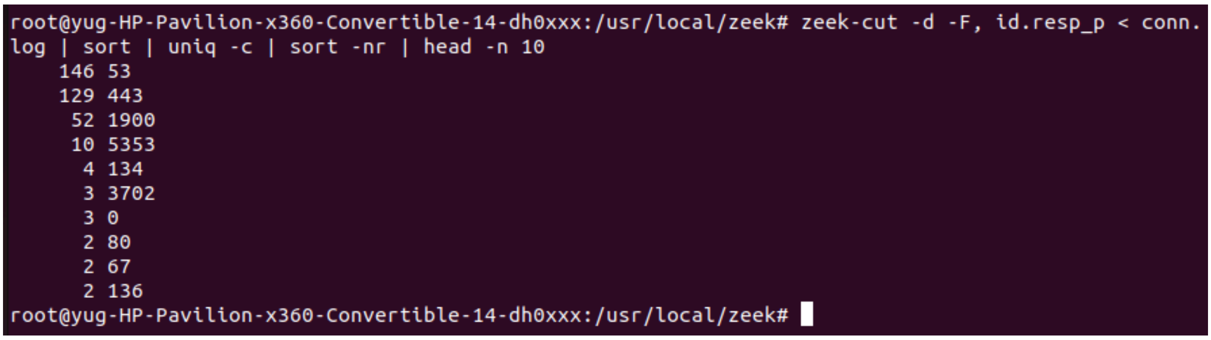
2. Run the same command used in Task 1A in 3rd Step just changing the pcap file name.
   “zeek -r 2015-03-19_winnormal.onlynormal.pcap”
   “zeek-cut -d -F, id.orig_h < conn.log | sort | uniq -c | sort -nr”



```
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# ls
2015-03-19_winnormal.onlynormal.pcap  dhcp.log  include           share    weird.log
bin                                   dns.log   lib               spool
conn.log                              etc       logs              ssl.log
cs23mtech11026_task1a.pcap            http.log  packet_filter.log  var
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# zeek -r 2015-03-19_winnormal.onlynor
mal.pcap
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# zeek-cut -d -F, id.orig_h < conn.log
 | sort | uniq -c | sort -nr
    396 10.0.2.200
      4 10.0.2.2
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek#
```

TASK - 2A

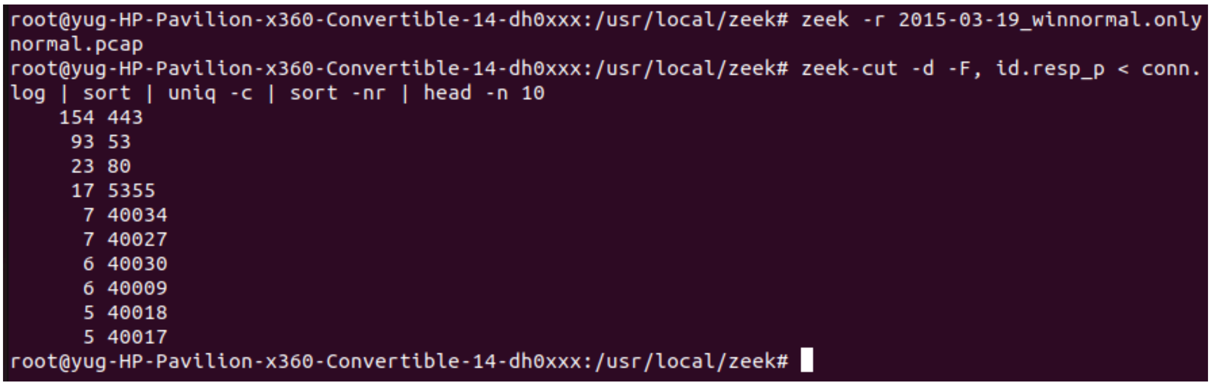
1. Using the same pcap file capture in the Task 1A (cs23mtech11026_task1a.pcap) and sorting according to port as asked in the question using the following command
`“zeek -r cs23mtech11026_task1a.pcap”`
`“zeek-cut -d -F, id.resp_p < conn.log | sort | uniq -c | sort - nr | head -n 10”`



```
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# zeek-cut -d -F, id.resp_p < conn.
log | sort | uniq -c | sort -nr | head -n 10
    146 53
    129 443
     52 1900
     10 5353
      4 134
      3 3702
      3 0
      2 80
      2 67
      2 136
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# 
```

TASK - 2B

1. Using the downloaded pcap file in Task 1B and running the following commands as follows:
`“zeek -r 2015-03-19_winnormal.onlynormal.pcap”`
`“zeek-cut -d -F, id.resp_p < conn.log | sort | uniq -c | sort -nr | head -n 10”`



```
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# zeek -r 2015-03-19_winnormal.only
normal.pcap
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# zeek-cut -d -F, id.resp_p < conn.
log | sort | uniq -c | sort -nr | head -n 10
    154 443
     93 53
     23 80
     17 5355
      7 40034
      7 40027
      6 40030
      6 40009
      5 40018
      5 40017
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# 
```

TASK 3:

1. Zeek script: The below given zeek script first checks if the website has the certificate chain or not. Then taking the end entity certificate and checking if the issuer and subject are the same or not, which ensures that a particular website has a self-signed certificate.

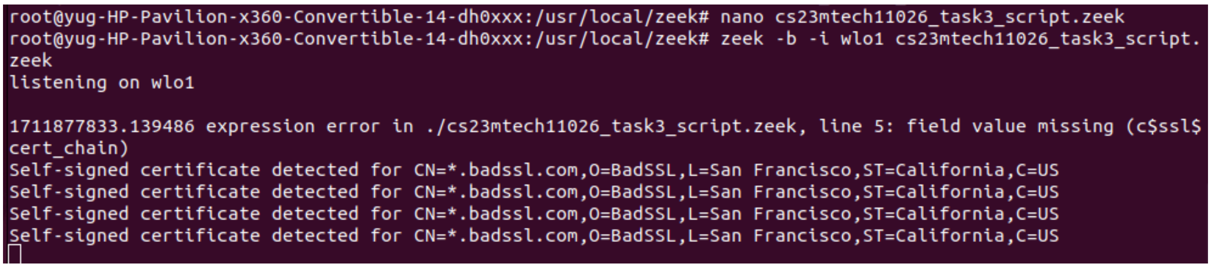
```
@load base/protocols/ssl
event ssl_established(c: connection){
    if (|c$ssl$cert_chain| > 0){
        local end_entity_cert = c$ssl$cert_chain[|c$ssl$cert_chain| - 1];
        if (end_entity_cert$x509$certificate$subject ==
            end_entity_cert$x509$certificate$issuer)
        {
            print fmt("Self-signed certificate detected for %s",
                       end_entity_cert$x509$certificate$subject);
            }
    }
}
```

2. After editing the zeek script using the below given commands to detect that if website have self-signed certificate or not

   (i) Start listening - “zeek -b -i wlo1 cs23mtech11026_task3_script.zeek”

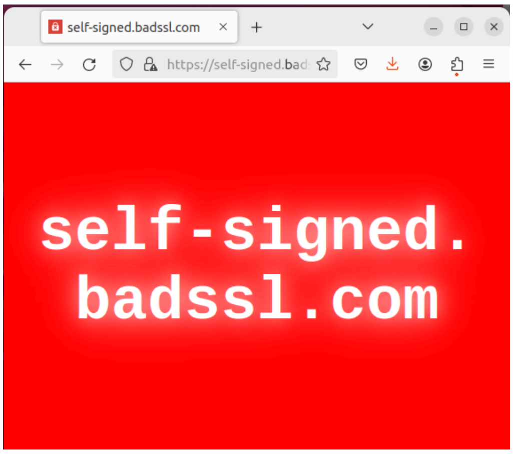
   (ii) Open browser and enter: https://self-signed.badssl.com/

   (iii) Output in the terminal from the zeek script file.



```
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# nano cs23mtech11026_task3_script.zeek
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# zeek -b -i wlo1 cs23mtech11026_task3_script.
zeek
listening on wlo1

1711877833.139486 expression error in ./cs23mtech11026_task3_script.zeek, line 5: field value missing (c$ssl$
cert_chain)
Self-signed certificate detected for CN=*.badssl.com,O=BadSSL,L=San Francisco,ST=California,C=US
Self-signed certificate detected for CN=*.badssl.com,O=BadSSL,L=San Francisco,ST=California,C=US
Self-signed certificate detected for CN=*.badssl.com,O=BadSSL,L=San Francisco,ST=California,C=US
Self-signed certificate detected for CN=*.badssl.com,O=BadSSL,L=San Francisco,ST=California,C=US
```



TASK - 4

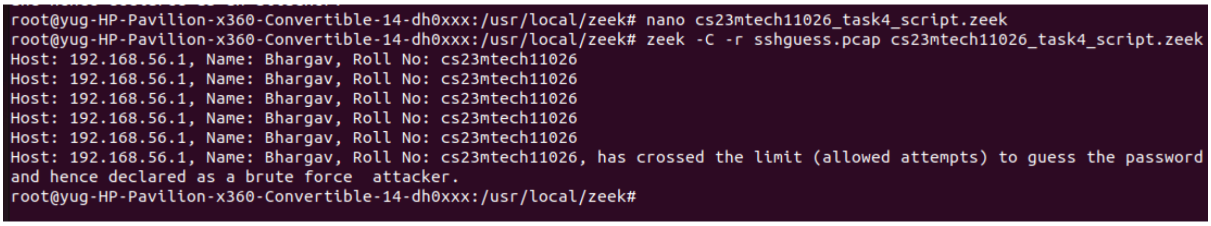
1. Downloading the sshguess.pcap file using this command
   “wget https://github.com/bro/bro/raw/master/testing/btest/Traces/ssh/sshguess.pcap”

2. Creating the zeek script to detect the brute force attacker: The script first checks if the user id is new and assigns it an attempt number 1, if it is old then just increment it and once it crosses the threshold the script declares the host as an brute force attacker.

```
@load base/frameworks/notice
module SSH;
export {
        const THRESHOLD: count = 5 &redef;
}

global attempts: table[addr] of count = table();
event ssh_auth_failed(c: connection) {
        local id = c$id$orig_h;
        if(id !in attempts){
                attempts[id] = 1;
        }
        else {
                attempts[id] += 1;
        }
        if (attempts[id] <= THRESHOLD) {
                print fmt ("Host: %s, Name: Bhargav, Roll No: cs23mtech11026",
                              id);
        }
        if (attempts[id] == THRESHOLD) {
                print fmt ("Host: %s, Name: Bhargav, Roll No: cs23mtech11026,
                              has crossed the limit (allowed attempts) to gues>
        }
}
```

3. Run the below command to detect brute force attack.
   “zeek -C -r sshguess.pcap cs23mtech11026_task4_script.zeek”



```
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# nano cs23mtech11026_task4_script.zeek
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek# zeek -C -r sshguess.pcap cs23mtech11026_task4_script.zeek
Host: 192.168.56.1, Name: Bhargav, Roll No: cs23mtech11026
Host: 192.168.56.1, Name: Bhargav, Roll No: cs23mtech11026
Host: 192.168.56.1, Name: Bhargav, Roll No: cs23mtech11026
Host: 192.168.56.1, Name: Bhargav, Roll No: cs23mtech11026
Host: 192.168.56.1, Name: Bhargav, Roll No: cs23mtech11026
Host: 192.168.56.1, Name: Bhargav, Roll No: cs23mtech11026, has crossed the limit (allowed attempts) to guess the password
and hence declared as a brute force  attacker.
root@yug-HP-Pavilion-x360-Convertible-14-dh0xxx:/usr/local/zeek#
```

PLAGIARISM STATEMENT

I certify that this assignment/report is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this assignment/report has not previously been submitted for assessment in any other course, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that I have not copied in part or whole or otherwise plagiarized the work of other students and/or persons. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, I understand my responsibility to report honor violations by other students if I become aware of it.

Name: Bhargav Patel
Date: 31-03-24
Signature: B.P