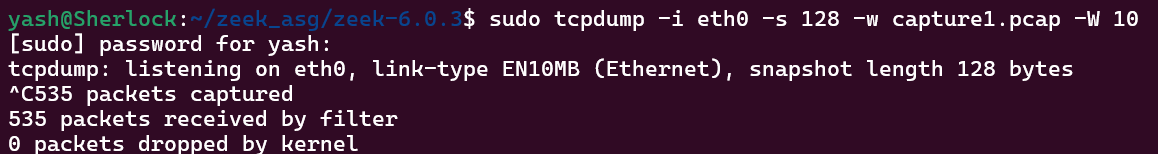
**Assignment 8 : Hands-on with Zeek**

cs23mtech14018 - Yash Shukla

**Task 1A:** Collect network traffic (only packet headers up to MAC layer to reduce the size of pcap file) using tcpdump or wireshark on your personal laptop for 10 mins and show the source IP addresses that generated the most network traffic, organized in descending order using zeek-cut. Deliverables: pcap file generated and relevant zeek log files; A screenshot of zeek-cut and its options used for answering this query and the output generated

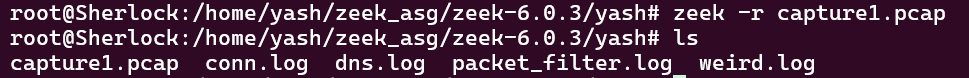
**Solution** :

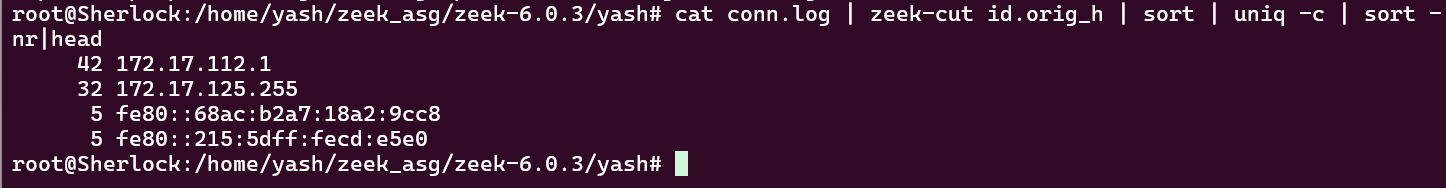
: Command : sudo tcpdump -i eth0 -s 128 -w capture1.pcap -W 10



Run zeek and analyze the captured traffic in the capture1.pcap file.

Using zeek-cut to analyze zeek logs ->





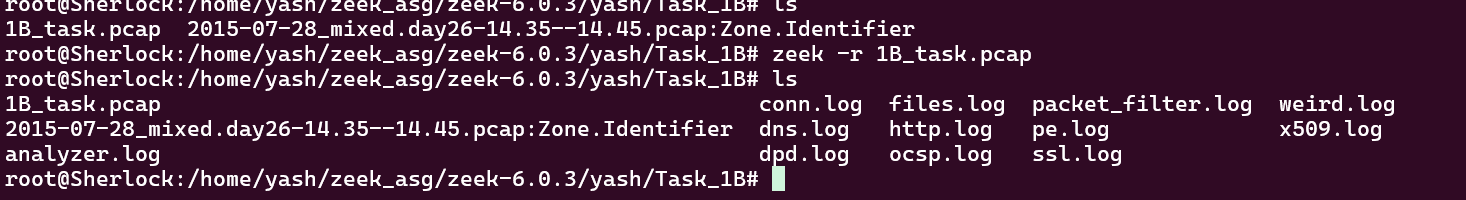
**Task 1B:** Repeat Task 1A by using one of the pcap files from <https://www.stratosphereips.org/datasets-mixed> or <https://www.honeynetproject.com/dataset.html>

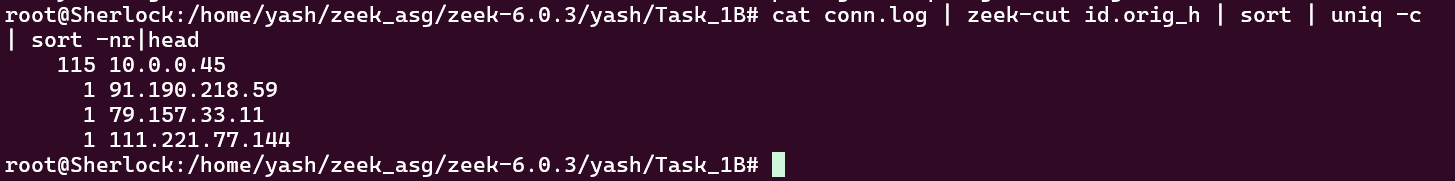
**Deliverables:** link of the pcap file used; A screenshot of zeek-cut and its options used for answering this query and the output generated.

**Solution** :

Link of pcap file used :

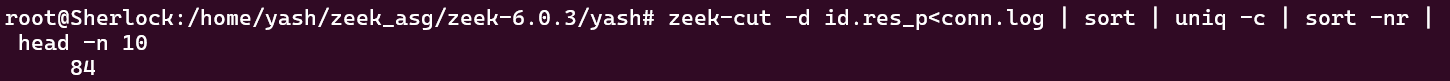
<https://mcfp.felk.cvut.cz/publicDatasets/CTU-Mixed-Capture-1/2015-07-28_mixed.day26-14.35--14.45.pcap>

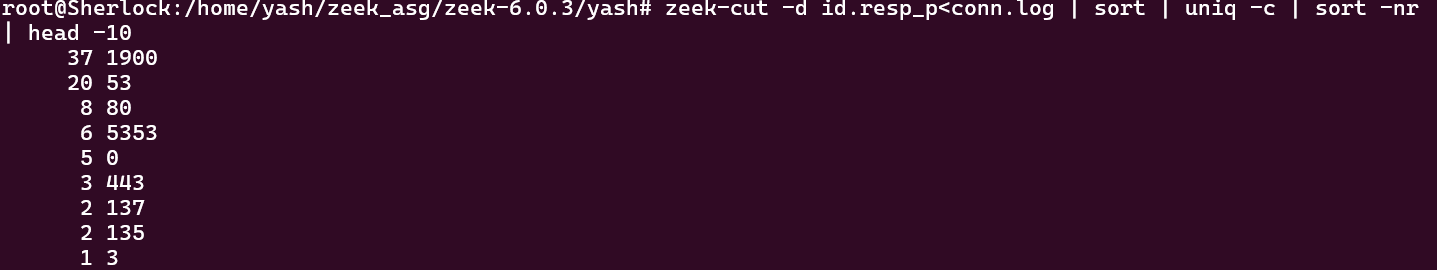




**Task 2A:** Show the 10 destination ports that received the most network traffic,organized in descending order using zeek-cut. Deliverables: Relevant zeek log files and a screenshot of zeek-cut and its options used for answering this query and the output generated.

**Solution** :





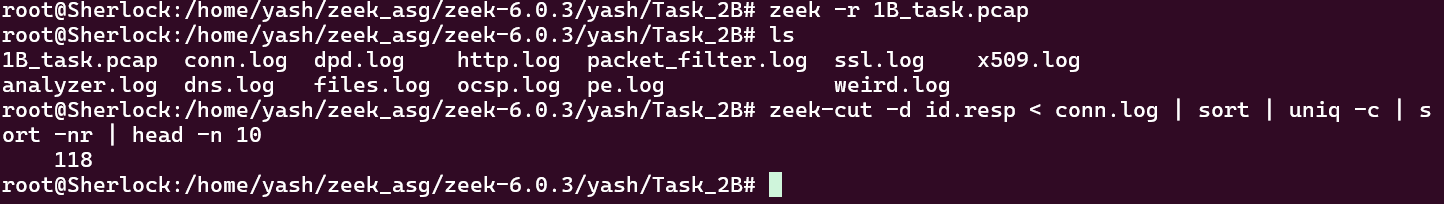
**Task 2B:** Repeat Task 2A by using one of the pcap files from <https://www.stratosphereips.org/datasets-mixed> or <https://www.honeynetproject.com/dataset.html>

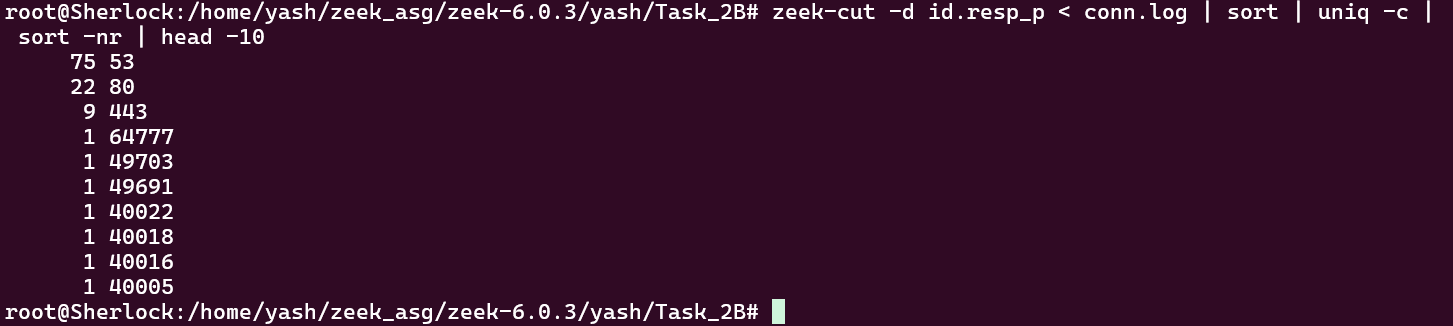
**Deliverables:** link of the pcap file used for completing this task; Relevant zeek log files; A screenshot of zeek-cut and its options used for answering this query and the output generated

**Solution** :

Link of pcap file used :

<https://mcfp.felk.cvut.cz/publicDatasets/CTU-Mixed-Capture-1/2015-07-28_mixed.day26-14.35--14.45.pcap>

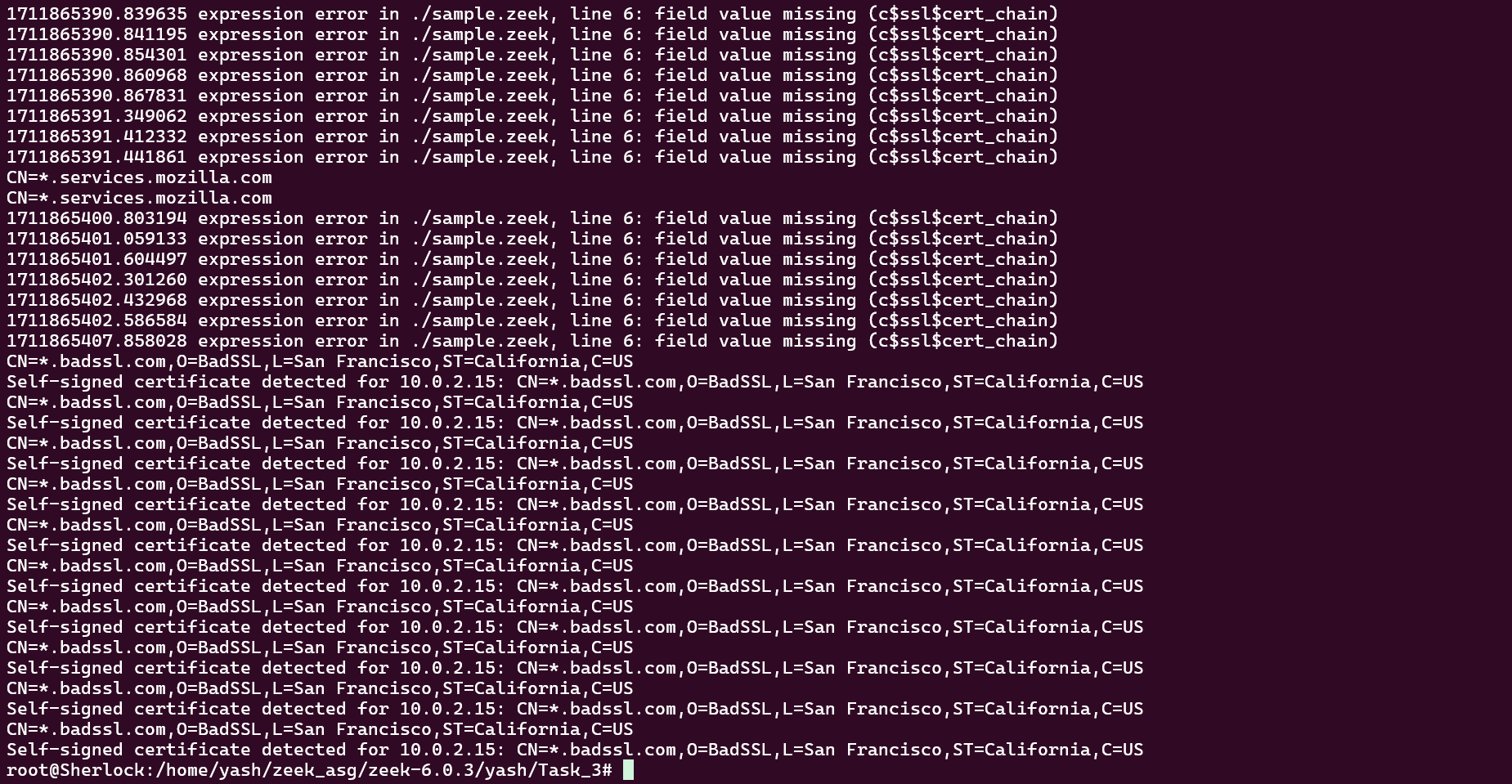




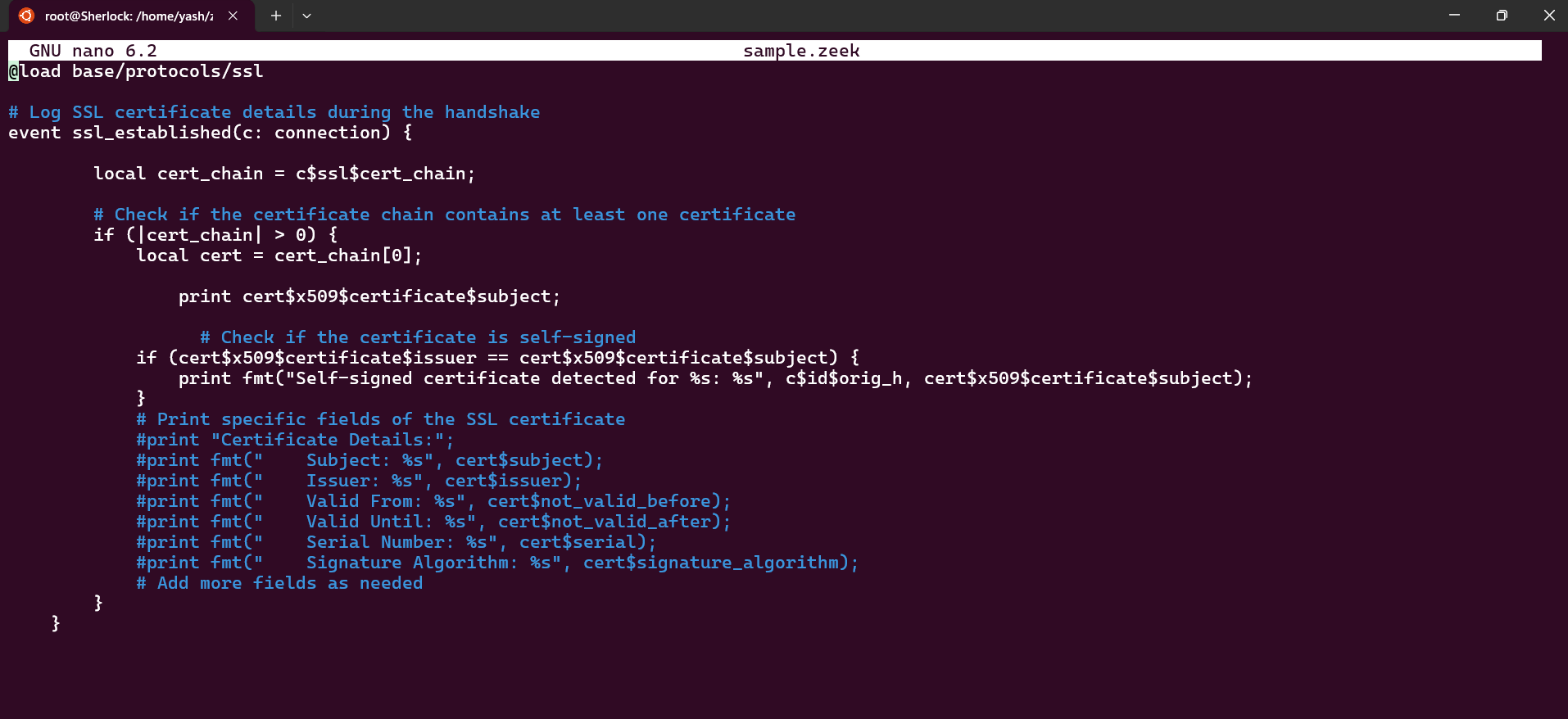
**Task 3:** Write a Zeek script to identify the Self Signed Certificate of the website: <https://self-signed.badssl.com/>

**Deliverables:** zeek script and a screenshot of the output generated by it when you visited this webpage.

**Solution** :



Here is the Code Snippet used to identify the Self Signed Certificate of the Website :



**Zeek Script** :

*@load base/protocols/ssl*

*# Log SSL certificate details during the handshake*

*event ssl\_established(c: connection) {*

*local cert\_chain = c$ssl$cert\_chain;*

*# Check if the certificate chain contains at least one certificate*

*if (|cert\_chain| > 0) {*

*local cert = cert\_chain[0];*

*print cert$x509$certificate$subject;*

*# Check if the certificate is self-signed*

*if (cert$x509$certificate$issuer == cert$x509$certificate$subject) {*

*print fmt("Self-signed certificate detected for %s: %s", c$id$orig\_h, cert$x509$certificate$subject);*

*}*

*# Print specific fields of the SSL certificate*

*#print "Certificate Details:";*

*#print fmt(" Subject: %s", cert$subject);*

*#print fmt(" Issuer: %s", cert$issuer);*

*#print fmt(" Valid From: %s", cert$not\_valid\_before);*

*#print fmt(" Valid Until: %s", cert$not\_valid\_after);*

*#print fmt(" Serial Number: %s", cert$serial);*

*#print fmt(" Signature Algorithm: %s", cert$signature\_algorithm);*

*# Add more fields as needed*

*}*

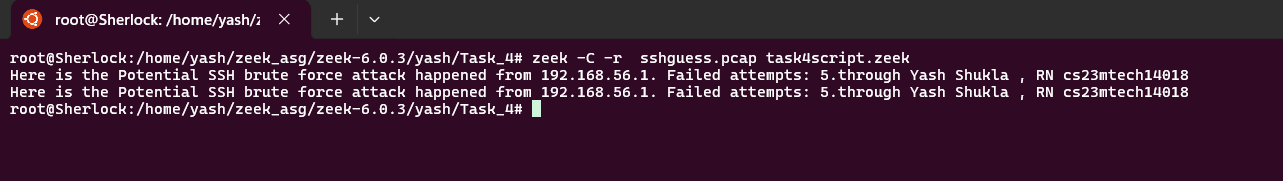
*}*

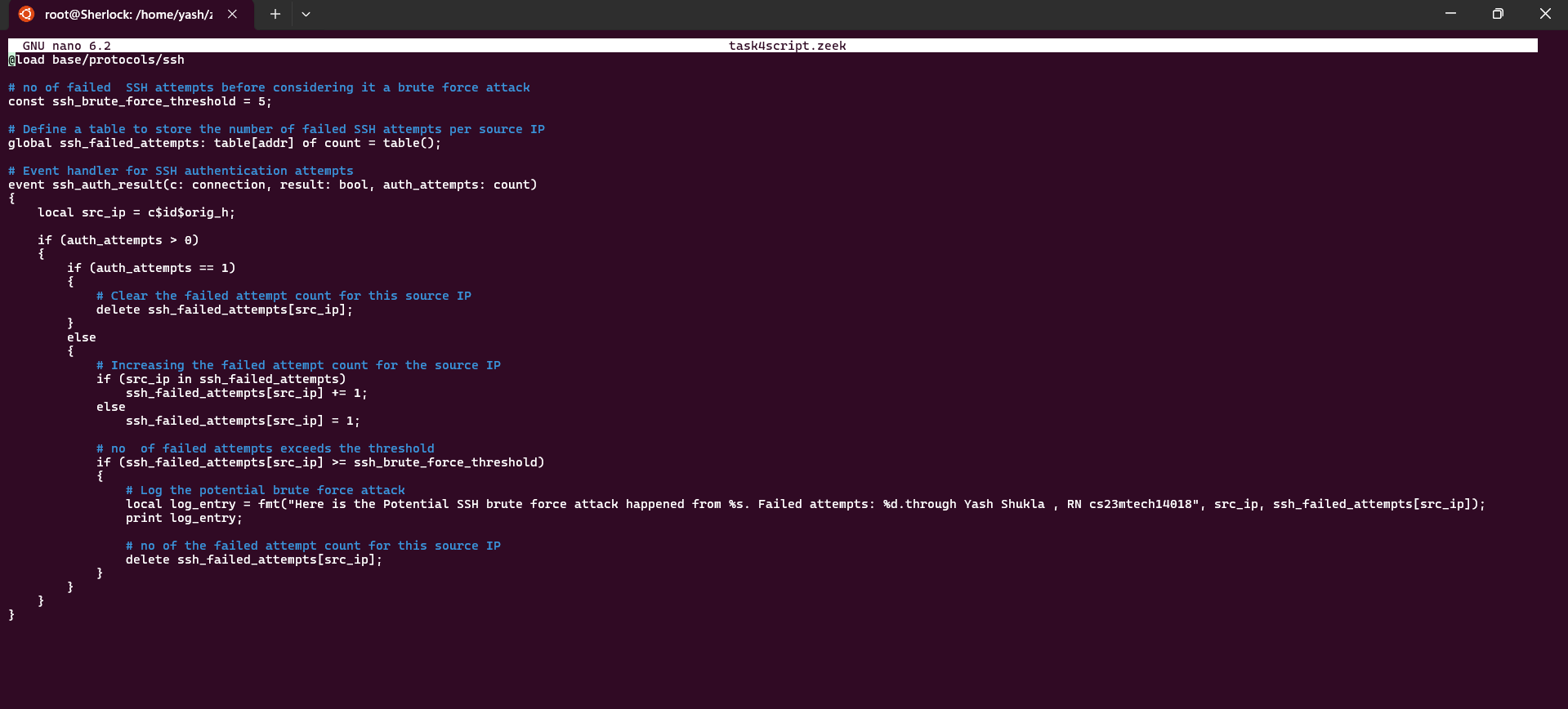
**Explanation** :

**Task 4:** Write a Zeek script to identify the ssh brute force password attacks in the following pcap file. Print the hosts that are guessing ssh passwords along with your name and RollNo in the generated log. <https://github.com/bro/bro/raw/master/testing/btest/Traces/ssh/sshguess.pcap>

**Solution** :

ScreenShot :





Here is the Code Snippet used to identify the ssh brute force password attacks in the pcap file :

**Zeek Script** :

*GNU nano 6.2 task4script.zeek*

*@load base/protocols/ssh*

*# no of failed SSH attempts before considering it a brute force attack*

*const ssh\_brute\_force\_threshold = 5;*

*# Define a table to store the number of failed SSH attempts per source IP*

*global ssh\_failed\_attempts: table[addr] of count = table();*

*# Event handler for SSH authentication attempts*

*event ssh\_auth\_result(c: connection, result: bool, auth\_attempts: count)*

*{*

*local src\_ip = c$id$orig\_h;*

*if (auth\_attempts > 0)*

*{*

*if (auth\_attempts == 1)*

*{*

*# Clear the failed attempt count for this source IP*

*delete ssh\_failed\_attempts[src\_ip];*

*}*

*else*

*{*

*# Increasing the failed attempt count for the source IP*

*if (src\_ip in ssh\_failed\_attempts)*

*ssh\_failed\_attempts[src\_ip] += 1;*

*else*

*ssh\_failed\_attempts[src\_ip] = 1;*

*# no of failed attempts exceeds the threshold*

*if (ssh\_failed\_attempts[src\_ip] >= ssh\_brute\_force\_threshold)*

*{*

*# Log the potential brute force attack*

*local log\_entry = fmt("Here is the Potential SSH brute force attack happened from %s. Failed attempts: %d.through Yash Shukla , RN cs23mtech14018", src\_ip, ssh\_failed\_attempts[src\_ip]);*

*print log\_entry;*

*# no of the failed attempt count for this source IP*

*delete ssh\_failed\_attempts[src\_ip];*

*}*

*}*

*}*

*}*

**Explanation** :

**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: Yash Shukla

Date: 30/03/2024

Signature: Yash Shukla