Assignment 8: Hands-on with Zeek

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.

Commands:

1. **tcpdump -i wlo1 -w task.pcap -s 0 -G 600**
2. **zeek -r task.pcap**
3. **cat conn.log | zeek-cut conn.log id.orig_h | sort | uniq -c | sort -rn**

zeek-cut for Task1A:
options used: conn.log and id.orig_h

```
root@sreyash-mohanty-1-0:/home/sreyash-mohanty/Desktop/NS_ZEEK/TASK-1# cat conn.log | zeek-cut conn.log id.orig_h | sort | uniq -c | sort -rn
     85         192.168.29.64
     72         192.168.29.206
     63         fe80::83ce:242b:98fc:7615
     33         2405:201:c004:5066:e55d:8d74:942c:c5c4
     17         fe80::4e22:f3ff:feda:fd28
     13         192.168.29.59
     10         192.168.29.101
     10         192.168.29.1
      8         fe80::8987:e73:813f:2dce
      6         fe80::ce9:dc0:789e:fa07
      6         fe80::144a:6b80:5bda:4f7b
      6         fd52:ee59:318:f047:c4be:cea1:be47:a413
      6         192.168.29.47
      6         192.168.29.11
      5         fe80::fcd5:5918:fe1d:ce2d
      2         192.168.29.23
      2         0.0.0.0
      1         fe80::8872:c3ff:fe8c:b6bd
root@sreyash-mohanty-1-0:/home/sreyash-mohanty/Desktop/NS_ZEEK/TASK-1#
```

Top source IP addresses generating the most network traffic

Task 1B: Repeat Task 1A by using one of the pcap files from https://www.stratosphereips.org/datasets-mixed

Link to the pcap file used for Task 1B:
https://mcfp.felk.cvut.cz/publicDatasets/CTU-Mixed-Capture-1/

-> 2015-07-28_mixed.day26-14.35--14.45.pcap

```
root@sreyash-mohanty-1-0:/home/sreyash-mohanty/Desktop/NS_ZEEK/TASK-2/TASK2B# cat conn.log | zeek-cut conn.log id.orig_h | sort | uniq -c | sort -rn
    115         10.0.0.45
      1         91.190.218.59
      1         79.157.33.11
      1         111.221.77.144
```

Top source IP addresses generating the most network traffic

Commands:

1. **tcpdump -i wlo1 -w task.pcap -s 0 -G 600**
2. **zeek -r task.pcap**
3. **cat conn.log | zeek-cut conn.log id.resp_p | sort | uniq -c | sort -rn**

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.

zeek-cut for Task2A:
options used: conn.log and id.resp_p

```
root@sreyash-mohanty-1-0:/home/sreyash-mohanty/Desktop/NS_ZEEK/TASK-2# cat conn.log | zeek-cut conn.log id.resp_p | sort | uniq -c | sort -rn | head -n 10
     94         5353
     88         5355
     55         53
     29         443
     18         1900
     17         137
     15         136
      6         7
      6         3
      5         133
```

Top 10 destination ports receiving the most network traffic

Task 2B: Repeat Task 2A by using one of the pcap files from https://www.stratosphereips.org/datasets-mixed

Link to the pcap file used for Task 1B:
https://mcfp.felk.cvut.cz/publicDatasets/CTU-Mixed-Capture-1/

-> 2015-07-28_mixed.day26-14.35--14.45.pcap

```
root@sreyash-mohanty-1-0:/home/sreyash-mohanty/Desktop/NS_ZEEK/TASK-2/TASK2B# cat conn.log | zeek-cut conn.log id.resp_p | sort | uniq -c | sort -rn
     75         53
     22         80
      9         443
      1         64777
      1         49703
      1         49691
      1         40022
      1         40018
      1         40016
      1         40005
      1         37671
      1         3702
      1         1900
      1         17500
      1         1
```

Top 10 destination ports receiving the most traffic

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

Firstly, used tcpdump to capture network traffic on **wlo1** interface to the specified website using:

tcpdump -i wlo1 -w task3.pcap host self-signed.badssl.com

This generated a pcap file which contained network traffic to the given website (https://self-signed.badssl.com/) only.

Command: zeek -C -r task3.pcap task3.zeek

```
root@sreyash-mohanty-1-0:/home/sreyash-mohanty/Desktop/NS_ZEEK/TASK-3# zeek -C -r task3.pcap task3.zeek
Self-signed certificate detected for website with IP address 104.154.89.105
Self-signed certificate detected for website with IP address 104.154.89.105
```

Self-signed certificate detected for the website (IP address)

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.

Download pcap from:

https://github.com/bro/bro/raw/master/testing/btest/Traces/ssh/sshguess.pcap

Command: zeek -C -r sshguess.pcap task4.zeek

```
root@sreyash-mohanty-1-0:/home/sreyash-mohanty/Desktop/NS_ZEEK/TASK-4# zeek -C -r sshguess.pcap task4.zeek
Potential SSH brute force attempt detected from 192.168.56.1 to 192.168.56.103 (Attempt 20) - Sreyash Mohanty, RollNo. CS23MTECH14015
Potential SSH brute force attempt detected from 192.168.56.1 to 192.168.56.103 (Attempt 21) - Sreyash Mohanty, RollNo. CS23MTECH14015
Potential SSH brute force attempt detected from 192.168.56.1 to 192.168.56.103 (Attempt 22) - Sreyash Mohanty, RollNo. CS23MTECH14015
Potential SSH brute force attempt detected from 192.168.56.1 to 192.168.56.103 (Attempt 23) - Sreyash Mohanty, RollNo. CS23MTECH14015
Potential SSH brute force attempt detected from 192.168.56.1 to 192.168.56.103 (Attempt 24) - Sreyash Mohanty, RollNo. CS23MTECH14015
Potential SSH brute force attempt detected from 192.168.56.1 to 192.168.56.103 (Attempt 25) - Sreyash Mohanty, RollNo. CS23MTECH14015
Potential SSH brute force attempt detected from 192.168.56.1 to 192.168.56.103 (Attempt 26) - Sreyash Mohanty, RollNo. CS23MTECH14015
Potential SSH brute force attempt detected from 192.168.56.1 to 192.168.56.103 (Attempt 27) - Sreyash Mohanty, RollNo. CS23MTECH14015
Potential SSH brute force attempt detected from 192.168.56.1 to 192.168.56.103 (Attempt 28) - Sreyash Mohanty, RollNo. CS23MTECH14015
```

SSH brute force attempt detected and warned after 20 failed attempts

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: Sreyash Mohanty
Date: 30/03/2024
Signature: Sreyash