Assignment 8: Hands-on with Zeek

Individual Assignment

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.

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.

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.

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.

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.

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

Deliverables: zeek script, relevant zeek log files and a screenshot of the output generated by it for this pcap file.

Deliverables in GC as a tar ball:

- A readable PDF Report with name “ZeekAsg-<RollNo>.PDF”
- Relevant zeek logs and pcap files

PLAGIARISM STATEMENT <Include it in your report>

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:
Date:
Signature: <keep your initials here>