Indian Institute of Technology Hyderabad

Department of Computer Science and Engineering

Assignment on Zeek

Network Security Monitor

Course: **Network Security - CS6903** **Submission Deadline: March 7th, 2025 11:59PM**

Zeek Network Traffic Analysis and Security Detection

Instructions:

- **This is an individual assignment**. Therefore, Teams/Collaboration are not allowed and is strictly forbidden.
- Total Marks of this assignment is 30.
- Ensure all deliverables are submitted in the required format on Google Classroom before the deadline, i.e., **March 7th, 2025 11:59PM [*No Extensions]**
- **Late submissions will receive a penalty of 100%, meaning all late submissions will be awarded 0 (zero) marks.**
- **If any student is found to have shared their work with another student, both will receive 0 (zero) for this assignment, followed by a one-grade reduction for this course. For example, if the final grade for the course is B, it will be reduced to B-.**

Task 1: Network Traffic Collection and Analysis [7 Marks]

Task 1A: Capture network traffic on your personal laptop and analyze the most active source IPs.

Instructions:

- Use `tcpdump` or `Wireshark` to collect network traffic for 10 minutes (capture only packet headers up to the MAC layer to minimize the PCAP file size).
- Process the captured PCAP file using `Zeek` and extract the source IP addresses that generated the most network traffic in descending order using `zeek-cut`.

Deliverables:

- Captured PCAP file and relevant Zeek log files.
- A screenshot of the `zeek-cut` command, its options, and the output.

Task 1B: Perform the same analysis using a publicly available PCAP dataset.

Instructions:

- Select a PCAP file from one of the following sources:
  - **Stratosphere IPS Datasets**: https://www.stratosphereips.org/datasets-mixed
  - **Honeynet Project Datasets**: https://www.honeynetproject.com/dataset.html

- Process the selected PCAP file using Zeek and extract the most active source IPs.

Deliverables:

- Link to the PCAP file used.
- A screenshot of the `zeek-cut` command, its options, and the output.

Task 2: Destination Port Analysis [7 Marks]

Task 2A: Identify the top 10 destination ports receiving the most network traffic.

Instructions:

- Process the Zeek logs generated from Task 1A.
- Use `zeek-cut` to extract and organize the destination ports in descending order of traffic volume.

Deliverables:

- Relevant Zeek log files.
- A screenshot of the `zeek-cut` command, its options, and the output.

Task 2B: Perform the same analysis using a publicly available PCAP dataset.

Instructions:

- Select a PCAP file from one of the following sources:
  - **Stratosphere IPS Datasets**: https://www.stratosphereips.org/datasets-mixed
  - **Honeynet Project Datasets**: https://www.honeynetproject.com/dataset.html
- Process the selected PCAP file using Zeek and extract the top 10 destination ports receiving the most traffic.

Deliverables:

- Link to the PCAP file used.
- Relevant Zeek log files.
- A screenshot of `zeek-cut` command, its options, and the output.

Task 3: Identifying Self-Signed Certificates [7 Marks]

Instructions:

- Write a Zeek script to analyze SSL traffic and detect self-signed certificates.
- Test the script by visiting **Self-Signed BadSSL**: https://self-signed.badssl.com/.

Deliverables:

- Zeek script.
- A screenshot of the script's output when visiting the webpage.

Task 4: Detecting SSH Brute-Force Attacks [9 Marks]

Instructions:

- Download and analyze the following **SSH Brute-Force PCAP** file: https://github.com/bro/bro/raw/master/testing/btest/Traces/ssh/sshguess.pcap.
- Write a Zeek script to identify SSH hosts performing brute-force attacks in the given PCAP file.
- Print the detected attacking hosts along with your name and Roll No. in the generated log.

Deliverables:

- Zeek script.
- Relevant Zeek log files.
- A screenshot of the output generated by the script.

Deliverables in Google Classroom as a tarball:

Submit a tarball (`.tar.gz/.zip/`) named as `ZeekAsg-<RollNo>.tar` or `ZeekAsg-<RollNo>.zip` containing:

- A readable **PDF Report** named `Report-<RollNo>.pdf` with explanations, **screenshots**, and findings.
- All **Zeek log files** generated during the analysis.
- **Links to PCAP files** you downloaded and used using links provided by us.
- Any **PCAP files captured by you** during the task (not the downloaded ones).
- Anti-Plagiarism Statement (see below).

Anti-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 `<RollNo>`**:**
Date:
Signature: `<keep your initials here>`