Indian Institute of Technology Kanpur
Department of Computer Science and Engineering
CS628 Computer System Security - Fall 2023
Instructor - Angshuman Karmakar
Assignment 4 – Packet Capture Analysis

Problem Statement: You are provided with two **.PCAP** files that contain network traffic captured during web attacks involving SQL injection and Cross-Site Scripting (XSS). As a network analyst, your task is to analyze the provided **.PCAP** files and extract insights from the attacks. You can perform packet capture analysis using the ***Wireshark*** tool [1] by uploading the provided packet capture files and initiating your analysis [2].

Deliverables:

To obtain the files for your assignment, please execute the following command in the terminal from your desktop. You will find the "Assignment4.zip" file by running the command:

$ wget 172.29.233.235:8000/Assignment4.zip

After downloading the files to your desktop, proceed to unzip them. Inside the unzipped directory, you will find three files:

1. **PCAP1.pcapng** - This file contains the network traffic captured during the SQL injection Attack.
2. **PCAP2.pcapng** - This file contains the network traffic captured during the XSS Attack.
3. **Assignment4.docx** - This is the final submission file. Please rename this file as **"YourRollNo_Assignment4.docx"**
   - Inside this document, you will find **20** questions designed to test your packet capture analysis skills. To open the document, use ***LibreOffice***.
   - For most of the questions, you are required to provide an answer along with a screenshot to confirm your response. To take the screenshot, use the ***ScreenShot*** tool.
   - For a few questions, you need to provide an explanation to support your answer. In such cases, a screenshot is not required. You will be explicitly informed when a question falls into this category, indicated by the statement "(Screenshot is not required)" at the end of that specific question.
   - Once you have answered all the questions, please access the following link from your web browser inside your lab VM machine: (http://172.29.233.235/), and upload the file "YourRollNo_Assignment4.docx."

Grading Schema - Total 60 Marks

1. A correct answer to a given question accounts for **2 marks**.
2. Providing an appropriate screenshot that supports your correct answer accounts for **1 mark.**
3. For explanation-based questions, a correct answer along with proper reasoning accounts for **3 marks.**

Instructions to access the Lab VM machine for the assignment

1. Connect to your iitk wifi network before you open the url sent to your mail. (https://172.29.233.235/). (preferably)
2. Open the url in any of your browser and login with your credentials (sent to your mail).
3. You will then have access to the UBUNTU 20.04 machine with user cs628. By giving the password as cs628 (cs is small), you can access the machine.

Instructions for Report Making: (Use the following template)

1. **Normal Text - Style** → Ubuntu**, Word Size** → 12
2. **Figure Name/Description - Style** → Ubuntu**, Word Size -** 12

Important Note: Justify all the lines in the submission document. You are expected to write every sentence in your own words. You should not rely on manpages. Your report will be thoroughly checked in turnitin and other AI tools for plagiarism. If the plagiarism is more than **20%** your submission is not considered for grading.

Caution: Once you have access to the machine, **everything will be recorded and logged.** You can do whatever that is required to solve the assignment, but if you were found doing anything out of scope, there is a reduction in your marks by **half**. You will only be evaluated with **half of the respective assignment marks.**

Submission Deadline: 23:55 of 13-11-2023 (Hard Deadline)

References:

[1] WireShark Tool: https://www.wireshark.org/

[2] WireShark Basics Tutorial: https://www.javatpoint.com/wireshark