**Project: Computer Networks**

This is a group project with a maximum of 2 members per group. It is divided into two parts (Part A and Part B), both parts are compulsory. Part A has 60% weight and Part B has 40% weight in the final project marks.

**Part A**

Download Wireshark and install it on your computer. Search for online tutorials and other handy information, such as YouTube videos for using Wireshark apart from the instructions in lab sessions.

**1. Experiment Description**

Write the exact packet capture filter expressions to accomplish the following:

* Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account
* Capture all HTTP traffic to/from Facebook, when you log in to your Facebook account
* Find a popular YouTube video and play it while capturing all traffic to/from YouTube
* After you run Wireshark with the above capture filters and collect the data, do the following:
  + Write a DISPLAY filter expression to count all TCP packets (captured under item #1) that have the flags SYN, PSH, and RST set. Show the fraction of packets that had each flag set.
  + Use a DISPLAY filter expression to separate the packets sent by your computer vs. received from Facebook and YouTube in items #2 and #3 above. Show the fractions for each type.

Note that when sniffing out TCP packets, you will be receiving TCP packets, SSL packets, and HTTP packets. This is because HTTP/SSL run on top of TCP and you capture their packets by default because they are subclasses of TCP packets.

* + So, capture them all and store in a local database.
  + Then use display filters to separate the subset of TCP packets that are also HTTP packets. (You can do this by filtering only packets on port 80).

Note that some of your sessions, e.g., Facebook, may be using secure HTTP (HTTP/SSL or HTTPS), which uses the port number 443.

**2. Captured Data Analysis**

* Count how many TCP packets you received from / sent to Facebook or YouTube, and how many of each were also HTTP packets.
* Determine if any TCP packets with SYN or PSH flags set were sent from your host or received from Facebook/Youtube.

Report all three counts in a table.

* Of course, you may do more. For example, you could find out if any packets had both PSH and RST set, or other flags not listed here.
  + Draw a rough PowerPoint sketch with a timeline of your Youtube session (roughly 5 minutes, or whatever is the duration of your chosen video) and indicate approximately when during the session the packets with SYN or PSH flags occurred. Your timeline should start at the time when the first video packet is received and end when the last video packet is received. You don’t need to draw a precise timeline—just illustrate the relationships.

**Part B**

Implement a virtual private network (VPN) solution that allows remote workers to securely connect to a company's network and access resources. You will be using Cisco Packet Tracer for this part of the Project.

Download Cisco Packet Tracer and install it on your computer. Search for online tutorials and other handy information, such as YouTube videos for using Cisco Packet Tracer apart from the instructions in lab sessions.

Develop a network with at least 5 routers and associated networks configured to be able to communicate with each other with at least 3 servers for different services. Implement a VPN solution for the remote workers to connect to the network and access services.

**Project Report for Part A and Part B**

The report should contain the following information:

**Part A**

* Location where the experiments were run (University campus/lab, home, other) and the type of your computer.
* Exact Wireshark filters used for capture and display.
* To improve the readability of your report, provide the filter expressions in separate lines and use the Courier font to write the filters.
* Explanation for every component of your filter expressions.
* The exact URL for all Youtube videos that you visited for this experiment.
* A table of observed statistics for counting the set flags in captured TCP packets.
* Histogram of the Youtube packet lengths.
* Sketch of the timeline of your Youtube session.
* The list of references used during the data analysis and report preparation, such as websites, blogs, books, etc.

To receive credit, it is not enough just to attach the raw Wireshark data to your report. Instead, you must analyse and discuss the data, and include diagrams and charts. It is critical that your report summarizes the captured data in diagrams, and the narrative provides discussion and explanation of the observations.

**Part B**

The report should contain the following information:

* Set of assumptions about the network set-up.
* Network set-up explanation with details of the networked devices.
* Logic behind your VPN.
* Any information relevant to the network and the project.

The items listed above form just a minimum requirement for the report and can be satisfied to a different degree. Only the students who have performed greatest number of experiments and provided most extensive analysis and discussion of their results in Part A and additional aspects in part B shall receive the top score (100%). The reports that have satisfied all the required items, but only to a bare minimum, shall receive 60% out of 100% of the maximum score.

*Report Submission*

Each group should submit a single project report.

The cover page of the report should include:

⋅ the course title and number

⋅ the project title

⋅ the group members

⋅ the submission date

Optional: To help us assign the grades fairly, you must indicate the breakdown of contributions for each team member.

Submission deadline is 07 January 2023.









