2DT905 Assignment 1 - Wireshark

Note: The maximum size of the submission should be 3 pages, not including title and reference pages. Include cropped screenshots when it is beneficial to your explanations.

Objective: The objective of this lab is to get familiar with the packet sniffer tool “Wireshark” and conduct a packet capture and packet analysis for various tasks related to TCP/IP and HTTP protocol.

Getting started:

- Launch Wireshark
- Get familiar with Wireshark (if you haven’t used it before) Please don’t start the packet capture yet, briefly read how it works and study the interface of Wireshark.
- In the capture screen, select the appropriate interface for capturing traffic that traverses the Internet.
- Click on the start button and begin packet capturing.

Problem 1 - Basic information about TCP/IP protocol

You will use Wireshark to capture packets from your Network Interface Card (NIC). These are the steps you will need to perform.

- Close all running windows and applications that generate network traffic (web browsers, email programs, background downloads, etc) to minimize the amount of traffic captured.
- Open a web browser which preferably has a blank homepage.
- Start a packet capture with Wireshark on the appropriate interface
- Type www.google.com in the URL bar of the browser. Leave it open for about 30-40 seconds.
- Stop the packet capture and save it as Assignment1_TCPwireshark.pcapng

Answer the following questions:

- T1-1: What are the different protocols listed in the protocol window of your system? Name some of these and very briefly explain them.
- T1-2: Perform a general packet capture for 20 minutes of web browsing, how many IPv4 and IPv6 **conversations** are there? In addition, what is the IP address of the DNS server you are connecting to? Briefly explain your reasoning as to why there is a different amount of IPv4 and IPv6 conversations and explain why this DNS server is used.
- T1-3: Type "udp" in the "Apply a display filter" section of Wireshark and hit Enter. Which protocols are used? Briefly explain what they do.

Problem 2 - Basic information about HTTP

To perform the following task(s), you will need to know how to clear your browser cache and ensure that it is cleared and re-clear it during some sections of this part. Clear the cache now.

Start a packet capture on the appropriate interface. In a separate window, open a web browser and enter the following: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

- T2-1: Please note down the IP address of your machine and the destination machine. What do you observe in the HTTP request message?
- T2-2: Observe and write down the details of the HTTP response message such as status code, content length and modified last time. Briefly explain each of these with a few sentences or less.

Problem 3 - GET request/response interaction

To perform the following task(s), you will need to know how to clear your browser cache and ensure that it is cleared and re-clear it during some sections of this part. Clear the cache now.

Start a packet capture on the appropriate interface. In a separate window, open a web browser and enter the following: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

Stop the packet capture and filter for "http" only to only see HTTP conversations.

- T3-1: Write down interesting observations for the GET request and response messages. Provide a brief overview of what is happening.

Problem 4 - Getting a longer document from the server

To perform the following task(s), you will need to know how to clear your browser cache and ensure that it is cleared and re-clear it during some sections of this part. Clear the cache now.

Start a packet capture on the appropriate interface. In a separate window, open a web browser and enter the following: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

Stop the packet capture and filter for "http" only to only see HTTP conversations.

- T4-1: As you are retrieving long document, how many request packets are sent from the client to the server? Briefly explain why the packet lengths are what they are.
- T4-2: . Write down your understanding on how the HTTP long file is supported by underlying TCP.
- T4-3: Inspect the packet which contains the status code and HTTP reason phrase. Provide a brief explanation of these.

Problem 5 - Getting a password protected document over HTTP

To perform the following task(s), you will need to know how to clear your browser cache and ensure that it is cleared and re-clear it during some sections of this part. Clear the cache now.

In this problem, you are trying to access a secured file stored on a UMass server. USername is: "wireshark-students" and the password is "network".

Start a packet capture on the appropriate interface. In a separate window, open a web browser and enter the following: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

Stop the packet capture and filter for "http" only to only see HTTP conversations.

- T5-1: Wire down your interesting observations for the request and response messages while performing this task. Provide a brief explanation of what is happening. Are there any problems with the password protection?

References

- http://www.wireshark.org
- HTTP1.1 standard, viewable here: http://www.ietf.org/rfc/rfc2616.txt
- J. F. Kurose and K.W. Ross, “Computer Networking: A Top-Down Approach featuring the Internet”

Submission

- One pdf containing all answers

The pdf name should have a format like the following:

"yourlnucode_2DT905_assign1.pdf" A valid example would be

"ls223qx_2DT905_assign1.pdf"