CNT 5410 - Fall 2023 - Assignment 2: Fun with Wireshark

Name: Your Name Here

October 2, 2023

This is an individual assignment. Academic integrity violations (i.e., cheating, plagiarism) will be reported to SCCR! The official CISE policy recommended for such offenses is a course grade of E. Additional sanctions may be imposed by SCCR such as marks on your permanent educational transcripts, dismissal or expulsion.

Reminder of the Honor Pledge: On all work submitted for credit by Students at the University of Florida, the following pledge is either required or implied: *"On my honor, I have neither given nor received unauthorized aid in doing this assignment."*

Instructions

Please read the instructions and questions carefully. Write your answers directly in the space provided. Compile the tex document and hand in the resulting PDF as your report.

In this assignment, you will use Wireshark to capture network traffic between your computer and other hosts on the Internet. You will need to install Wireshark on your computer[1]. Please refer to resources specific to your operating system and environment for installation instructions. Make sure that you are able to capture packets on your main network interface.

Wireshark Resources

For this assignment, it will be useful to be familiar with how to use Wireshark. You may find the Wireshark user guide[2] useful. Feel free to use other resources you find on the web.

Initial Trace Capture

With an empty DNS cache, start a new Wireshark capture. Open your Web browser and visit the following url: `cise.ufl.edu`. After the page loads, stop the Wireshark capture.

Note: it is crucial to get a full capture with no caching (e.g., DNS) to be able to properly answer the questions in the assignment. You may also consider clearing your browser cache prior to starting the capture.

[1] `https://www.wireshark.org/download.html`

[2] `https://www.wireshark.org/download/docs/user-guide.pdf`

Problem 1: DNS (20 pts)

Locate the DNS related traffic to `cise.ufl.edu` in your Wireshark capture. Answer the following questions.

Hint: you can type "dns" in the filter bar to display only the DNS related traffic.

1. (1 pts) What is your operating system? What is the version? Is the interface you captured traffic on wired or wireless?

   Your answer here.

2. (2 pts) What is the IP address of your computer?

   Your answer here.

3. (2 pts) What is the IP address of the DNS server?

   Your answer here.

4. (5 pts) List all the relevant DNS requests alongside with their types. If there is more than one request, explain why.

   Your answer here.

5. (5 pts) Focus on the DNS query for the domain `cise.ufl.edu`. Is this query recursive or iterative? (Justify your answer.)

   Your answer here.

6. (5 pts) List the IP address(es) returned for the domain `cise.ufl.edu`. Is the response authoritative? What is the Time to Live?

   Your answer here.

Problem 2: TCP (25 pts)

Using the IP address of the webserver, locate the related traffic. For example, if `A.B.C.D` is the IP address you can use the following filter:

```
ip.src == A.B.C.D or ip.dst == A.B.C.D
```

Answer the following questions.

1. (10 pts) List all of the relevant TCP connections. Specify: the ports, start time, and end time (relative to the beginning of the capture) of each connection.

   Your answer here.

2. (5 pts) Is there a pattern in how port numbers are chosen?

   Your answer here.

3. (5 pts) Why is there more than one connection? Explain their timing. (Justify your answer.)

   Your answer here.

4. (5 pts) What is the TCP sequence number of the SYN packet of the first TCP connection?

   Your answer here.

Problem 3: SSL/TLS, HTTPS (35 pts)

Focus on the SSL/TLS traffic of the first connection. Answer the following questions.

1. (1 pts) What is the TLS version?

   Your answer here.

2. (4 pts) Look at the Client Hello message. What is the random value? What is it used for. (Explain your answer.)

   Your answer here.

3. (5 pts) List **all** the cipher suites in the Client Hello. Are there in any particular order? Are there any weak cipher suites in the list?

   Your answer here.

4. (5 pts) What is the cipher suite that the client and server agreed on? State its name and describe all of its components. (What is the key exchange, encryption, mode of operation, MAC algorithms?)

   Your answer here.

5. (5 pts) Locate the certificate for `cise.ufl.edu`. List the fingerprint of the public key. What is the common name? What is the certificate issuer?

   Your answer here.

6. (5 pts) Is this the only certificate involved in this connection? If so, explain why. If not, what is/are the other certificate(s). (Provide details.)

   Your answer here.

7. (10 pts) After the SSL/TLS handshake is completed, the client and server exchange application data. What is the first HTTP request sent by the client? List all of the HTTP headers in this request including the HTTP version.

   Your answer here.