IP LAB EXPERIMENT – 3 [CYS 2022 - 2024] **20-10-2022**

(Note: Total 25 marks for this lab assignment which includes 20 marks + 3 marks for your presentation + 2 marks for your report)

For each of the following steps describe your results, give the syntax of the command you used, and, where appropriate, the output produced. Include screen captures as needed in your output. Be sure to label your results carefully and organize your results in the order of steps as given here and answer each question in your report.

1. Let's begin our exploration of HTTP by downloading a very simple HTML file - one that is very short and contains no embedded objects. Do the following:

1. Start up your web browser.

2. Start the Wireshark packet sniffer, as described in the Introductory lab (but don't yet begin packet capture). Enter "http" (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We're only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).

3. Wait more than one minute (we'll see why shortly), and then begin Wireshark packet capture.

4. Enter the following into your browser

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

Your browser should display a very simple, one-line HTML file.

5. Stop Wireshark packet capture.

By looking at the information in the HTTP GET and response messages, answer the following questions.

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

2. What languages (if any) do your browser indicate that it can accept to the server? 3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

4. What is the status code returned from the server to your browser?

5. When was the HTML file that you are retrieving last modified at the server?

6. How many bytes of content are being returned to your browser?

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

---

2. Before performing the steps below, ensure your browser's cache is empty.

• Start up your web browser, and make sure your browser's cache is cleared, as discussed above.

• Start up the Wireshark packet sniffer

• Enter the following URL into your browser

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

Your browser should display a very simple five-line HTML file.

Quickly enter the same URL into your browser again (or simply select the refresh button on your browser)

• Stop Wireshark packet capture and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

Answer the following questions:

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? What information follows the "IF-MODIFIED-SINCE:" header?

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the file's contents? Explain.

---

3. Start up your web browser, and make sure your browser's cache is cleared, as discussed above.

• Start up the Wireshark packet sniffer

• Enter the following URL into your browser

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

Your browser should display the rather lengthy US Bill of Rights.

• Stop Wireshark packet capture and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed.

Answer the following questions:

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

14. What is the status code and phrase in the response?

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

---

4. Finally, let's try visiting a website that is password-protected and examining the sequence of HTTP messages exchanged for such a site. The URL http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html is password protected. The username is "Wireshark-students" (without the quotes), and the password is "network" (again, without the quotes). So, let's access this "secure" password-protected site.

Go Through this link before answering this question: HTTP Authentication Schemes (userland.com)

Do the following:

• Make sure your browser's cache is cleared, as discussed above, and close your browser. Then, start up your browser

• Start up the Wireshark packet sniffer

• Enter the following URL into your browser http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html Type the requested username and password into the pop-up box.

• Stop Wireshark packet capture and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

Answer the following questions:

16. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

17. When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?