Ivan Fernandez

SER 321 – Summer C

5/25/2021

Assignment 2

Upper Layers of the OSI-Model

1 Sending emails and SMTP

A screenshot of a computer

Description automatically generated with medium confidenceText

Description automatically generatedScreenshots:

1. What filter did you use to catch the traffic and explain why you chose that filter?

I chose the filter tcp.port == 465 because it is the port used to establish communications between the client and the gmail server.

2. What is the standard port for SMTP and why do we use port 465 in the example above?

The standard port for SMTP is port 587 for submissions by mail clients to mail servers. Port 25 is recommended for transmissions between mail servers. Port 465 was used because it uses SSL to encrypt transmissions over the internet; it is for SMTPS. It is also for mail client to mail server communications.

3. Explain each line used in the command line and what it does and why it is needed?

1. echo−ne username | base64 This command is used to encode the username to ensure that it will transmit across the network uncorrupted.

2. echo−ne password | base64 This command is used to encode the password to ensure that it will transmit across the network uncorrupted.

3. openssl s\_client−c r l f−ign\_eof−connect smtp . gmail . com:465 Creates the connection to the google gmail server via tcp port 465.

4. helo gmail . com Ensures that the connection was successful.

5. auth login Login into your gmail account, using base64 encrypted username and password.

6. mail from : [username@gmail . com](mailto:username@gmail%20.%20com) Begins email creation from owner’s email account.

7. rcpt to : [username@gmail . com](mailto:username@gmail%20.%20com) The recipient’s email account.

8. data This command precedes the creation of the email.

9. Subject : Your subject Will create the subject line for the email.

10. Email text goes here . The actual email text is typed into this section.

11. . This period is used to end the email message.

12. quit This closes the connection to the google gmail server.

4. How much back and forth communication do you see for establishing the connection?

We can easily see the three-way handshake, the local tcp port 14410 establishes communications with web server tcp port 465. Three packages can be observed, we can see a [SYN] , [SYN, ACK], and finally an [ACK] from the local port establishing communications with the web server.

5. What is the port your local machine is using between sending the two emails when communicating with the SMTP server?

The port being used is port 14410.

6. Explain who sends the first FIN flag and how the quitting process works.

It can be see that the web server sends the [FIN, ACK] flags first to the local port, the local port then responds with an [ACK]. Application data is sent to the local port, and then port 14410 sends back [FIN, ACK] to port 465. Port 465 then sends [RST] reset flag to port 14410.

3652 531.130032 142.250.141.108 192.168.1.5 TCP 54 465 → 14410 [FIN, ACK] Seq=4194 Ack=1222 Win=66816 Len=0

3653 531.130126 192.168.1.5 142.250.141.108 TCP 54 14410 → 465 [ACK] Seq=1222 Ack=4195 Win=131328 Len=0

3654 531.130213 192.168.1.5 142.250.141.108 TLSv1.3 78 Application Data

3655 531.130286 192.168.1.5 142.250.141.108 TCP 54 14410 → 465 [FIN, ACK] Seq=1246 Ack=4195 Win=131328 Len=0

Graphical user interface, application, table, Excel

Description automatically generated7. Add a screenshot of your Wireshark output and add it to your document.

2 Understanding HTTP

Screenshot 1:

A screenshot of a computer

Description automatically generated with medium confidence

Screenshot 2:

Graphical user interface, text

Description automatically generated

1. Explain the specific API calls you used.

I used the calls:

https://api.github.com/repos/iafernan/assign2git/commits/db64ae38533bd34b4eeed12b66db963c9f682708

<https://api.github.com/repos/iafernan/assign2git/branches?branch=testbranch/commits?per_page=50/>

To get a listing of the commits for the test branch in my assign2git repo on GitHub.

2. Explain the difference between stateless and a state-full communication.

HTTP/HTTPS are stateless protocols, in which a user submits a request to a web browser for example, and HTTP/HTTPS does not save any states of the requests made to any web services. The web service, for example Google, may save information regarding your states and searches, as well as web browser cookies, but the HTTP/HTTPS protocols do not. In short, HTTP/HTTPS does not keep track of your previous web browsing requests or information. In contrast, FTP is a protocol that is stateful, and creates a connection to a server that keeps track and remembers requests that have been made during the session. FTP is unique because it uses two connections to the server to one establish and maintain the connection, and second to send and receive information.

3 Setup your second system and run Server on it

Text

Description automatically generated3.2 Running a simple Java Web Server

3.3 Analyze what happens

Graphical user interface, text, application

Description automatically generated

1. What filter did you use? Explain why you chose that filter.

I chose the filter tcp.port==9000 because that is the port of the Web Server on the second system.

Text

Description automatically generated2. What happens when you are on /random and click the refresh button compared to the browser refresh (you can also use the command line output that the WebServer generates to answer this)?

Graphical user interface

Description automatically generated

The WebServer Received: GET /json HTTP/1.1

449 59.808087 192.168.0.19 3.20.233.20 HTTP 372 GET /json HTTP/1.1

3. What kinds of response codes are you able to get through different requests to your server?

355 46.752836 192.168.0.19 3.20.233.20 TCP 66 11284 → 9000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1

357 46.830405 3.20.233.20 192.168.0.19 TCP 66 9000 → 11284 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK\_PERM=1 WS=128

359 46.830580 192.168.0.19 3.20.233.20 TCP 54 11284 → 9000 [ACK] Seq=1 Ack=1 Win=65536 Len=0

360 46.830737 192.168.0.19 3.20.233.20 HTTP 515 GET / HTTP/1.1

441 59.680668 192.168.0.19 3.20.233.20 HTTP 495 GET /random HTTP/1.1

449 59.808087 192.168.0.19 3.20.233.20 HTTP 372 GET /json HTTP/1.1

4. Explain the response codes you get and why you get them?

Within wireshark, we are able to see multiple local ports connect to the web server during the course of the web browsing session. The TCP three-way handshake is viewable for every port that connects to the web server. We can see various GET requests from the local ports to the server tinted in lime green color, as well as 200 OK HTTP success statuses from the web browsing session.

5. When you do aipOfSecondMachine:9000 take a look what Wireshark generates as a server response. Are you able to find the data that the server sends back to you?

We are able to view the line-based text data:

Graphical user interface, text, application

Description automatically generated

6. Based on the above question explain why HTTPs is now more common than HTTP.

Data with using HTTPS is encrypted, it uses a secure protocol known as Transport Layer Security.

7. What port does the server listen to for HTTP requests in our case and is that the most common port for HTTP?

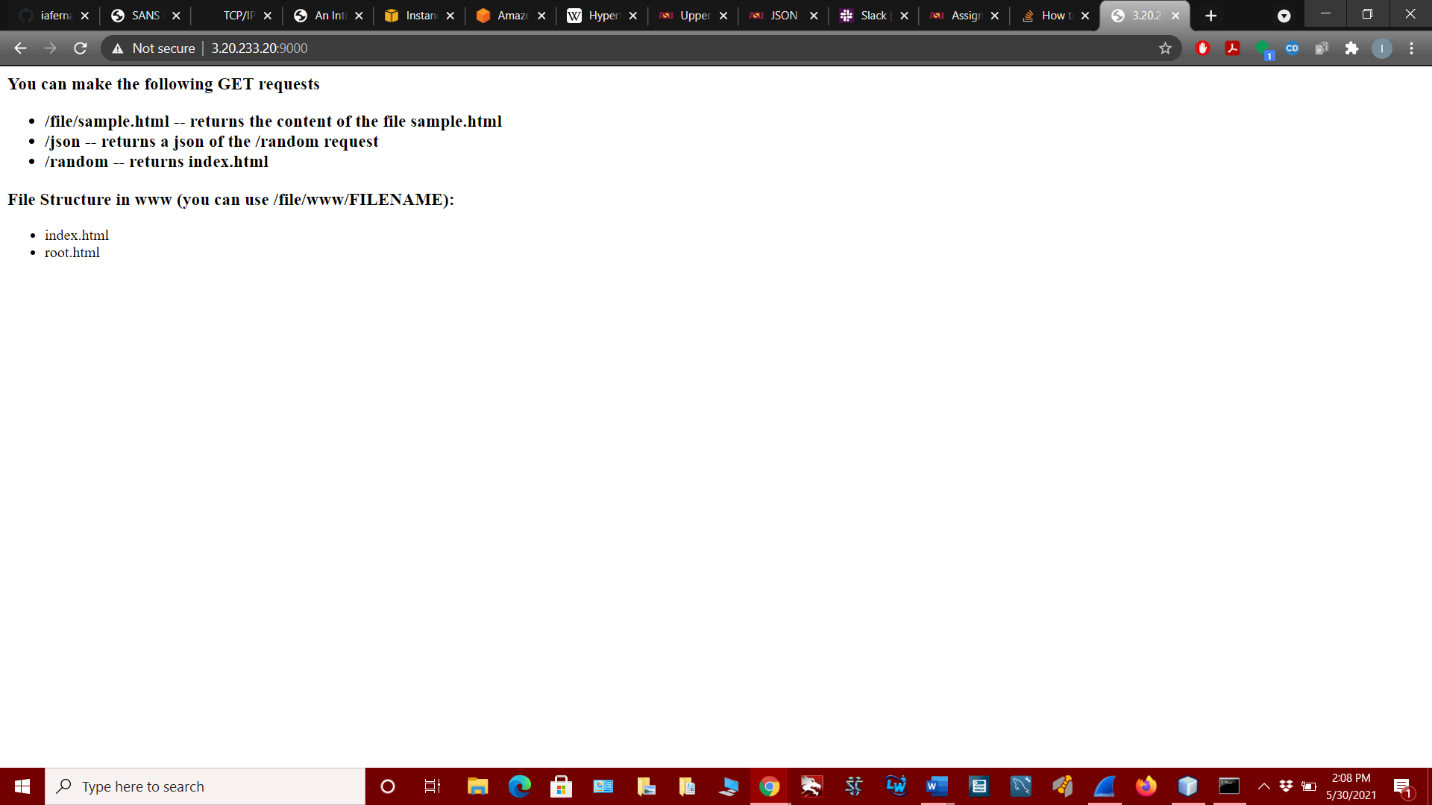
During the web browsing it is interesting to see that multiple local ports connect to the destination web server port 9000. The destination ip is of course the same. This signifies the various processes that are running concurrently as requests are being made to the web server during the web browser session. For example, keeping the home page “alive” while navigating towards other pages/tabs of a website and the various interactions being made within them.

8. What local port is used when sending different requests to the WebServer? How does it differ to the traffic to your SMTP server from part 1?

SMTP made use of one local port for communications whereas http communicated with various local ports when making requests to the webserver.

Graphical user interface, application, table, Excel

Description automatically generated3.4 Setting up a "real" Web server



1. Check your traffic to your Webserver now. What port is the traffic going to now? Is it the same as previously used or is it and should it be different?

It is the same as before.

2. Is it still HTTP or is it now HTTPs? Why?

It is still HTTP.