Lab10 HTTP

Lab10 HTTP

1.
Part-A. Look at the file "http-image.pcapng". This captures packets related to downloading a simple image from a website.
Answer the below questions based on this trace. You may want to filter the trace to identify the http packets (filter string: http).

1.1. In the trace, what HTTP method was used to download the image?

Marks: 1
Type: SINGLE_CORRECT_ANSWER

Options:

0) GET
1) POST
2) PUT
3) HEAD

1.2.
In the trace, IP address of the client (where browser is running) corresponds to? Format a.b.c.d (e.g. 10.12.11.34)

Marks: 1
Type: FILL_IN_THE_BLANKS_TYPE

1.3. What browser was used in this exchange and what OS type?

Marks: 1
Type: SINGLE_CORRECT_ANSWER

Options:

0) Internet Explorer, Windows
1) Chrome, Windows
2) Chrome, Ubuntu
3) Mozilla, Ubuntu
4) Command-line wget

1.4. What is the version of the HTTP client software? e.g. 2.3 or 4.2.10

Marks: 1
Type: FILL_IN_THE_BLANKS_TYPE

1.5. What version of HTTP is the Browser and Server running?

Marks: 1
Type: SINGLE_CORRECT_ANSWER

Options:

0) Browser:1.0 and Server 1.0
1) Browser:1.0 and Server 1.1
2) Browser:1.1 and Server 1.0
3) Browser:1.1 and Server 1.1

1.6. What server is being used in the exchange?

Marks: 1
Type: SINGLE_CORRECT_ANSWER

Options:

0) Apache
1) Ngnix
2) Microsoft IIS

1.7. What all status codes from the server do you see in the entire trace? Select all that apply.

Marks: 1
Type: MULTIPLE_CHOICE

Options:

0) 200 OK

1) 301 Moved Permanently

2) 404 Not Found

3) 418 I'm a teapot

4) 502 Bad Gateway

1.8. What was the size of the image that was downloaded? Express it in bytes. Format X (e.g. 11002)

Marks: 1
Type: FLOAT_TYPE

1.9. When was the image last modified? Format YYYY-MM-DD (e.g. 2020-05-20)

Marks: 1
Type: FILL_IN_THE_BLANKS_TYPE

2.

Part-B. Look at the file "http-not-modified.pcapng". This captures packets related to loading and then reloading/refreshing the previous download of an image from a website.
Answer the below questions based on this trace.
Denote the server machine corresponding to the “Not Modified” HTTP response as S, and its IP address as IP_S.
You may want to filter the trace to identify the http packets (filter string: http) or TCP packets or server IP address.

2.1. What is IP_S ? Format a.b.c.d e.g. 29.3.2.50

Marks: 1
Type: FILL_IN_THE_BLANKS_TYPE

2.2. In the packet corresponding to the first load of the image, is there a "If-modified-since" field?

Marks: 1
Type: SINGLE_CORRECT_ANSWER

Options:

0) Yes

1) No

2.3.
In the trace, which client port number is used in the TCP connection corresponding to the first HTTP request/response to load the image?

Marks: 1
Type: FLOAT_TYPE

2.4.
We have seen in the earlier questions that the first GET request results in the download of the image from the server. This response image download would have spanned over many TCP segments (with non-zero bytes in TCP payload). How many such TCP segments were involved in this? *Hint: do not count manually; wireshark does the counting for you: select the relevant HTTP response.*

Marks: 1
Type: FLOAT_TYPE

2.5.
In the trace, which client port number is used in the TCP connection corresponding to the second HTTP request/response to load the image?

Marks: 1
Type: FLOAT_TYPE

2.6.

In the packet corresponding to the second load of the image, there will be an "If-modified-since" field since the image is cached after the first load. What is the content in this field? Format YYYY-MM-DD (e.g. 2020-05-20)

Marks: 1
Type: FILL_IN_THE_BLANKS_TYPE

2.7. Is the HTTP server persistent or non-persistent?

Marks: 1
Type: SINGLE_CORRECT_ANSWER

Options:

0) Persistent

1) Non-persistent

2) Insufficient information in the trace to answer

2.8.
What was the server response code in response to the second request to load the image? Format X (e.g. 200 or 301 or 404)

Marks: 1
Type: FLOAT_TYPE

2.9.
We have seen in the earlier questions in Part-A that the first GET request results in the download of the image from the server. How about the second GET request for the image? Did it involve downloading an image or some part of it?

Marks: 1
Type: SINGLE_CORRECT_ANSWER

Options:

0) Yes

1) No

3.
Part-C. Look at the file "http-html.pcapng". This captures packets related to loading the IITB webpage. Answer the below questions based on this trace. You may want to filter the trace on relevant fields (which you need to figure out on own) to identify relevant packets. You can also use clauses ‘and’ / ‘or’ to combine multiple filter conditions in wireshark.

3.1. In the trace, how many GET requests were sent to download the entire webpage? Format X (e.g. 25)

Marks: 2
Type: FLOAT_TYPE

3.2. What all status codes were returned by the server during the download of the page? Select all that apply.

Marks: 1
Type: MULTIPLE_CHOICE

Options:

0) 200 OK

1) 301 Moved Permanently

2) 404 Not Found

3) 414 Request URI Too Long

4) 401 Unauthorized

3.3. How many TCP connections were established to download the page? Format X (e.g. 1)

Marks: 2
Type: FLOAT_TYPE

3.4.
How many GET requests were sent in a given TCP connection associated with client port of 58414? Format X (e.g. 1)

Marks: 2
Type: FLOAT_TYPE

3.5. Are the TCP connections persistent (as opposed to non persistent)?

Marks: 1
Type: SINGLE_CORRECT_ANSWER

Options:

0) Yes

1) No

3.6. Are the TCP connections pipelined (as opposed to non pipelined)?

Marks: 1
Type: SINGLE_CORRECT_ANSWER

Options:

0) Yes

1) No

3.7.
How many kilo-bytes were downloaded from the server to display the page? Take 1K=1000. Answer to the first decimal place.

Marks: 2
Type: FLOAT_TYPE

3.8. How much time in seconds did it take to load the page? Answer to the first decimal place.

Marks: 2
Type: FLOAT_TYPE

4.
Part-D. Look at the file "http-not-safe.pcapng". This captures a login session and demonstrates why http is not secure and all of us should move to https.
Answer the below questions based on this trace.

4.1.
In the trace, when “http” display filter is applied, what is the packet number of the packet that contains the login details? Format X (e.g. 5)

Marks: 1
Type: FLOAT_TYPE

4.2. What is the HTTP method used to send the login details (username and password)?

Marks: 1
Type: FILL_IN_THE_BLANKS_TYPE

4.3. What is the password used in the authentication? Format string (e.g. hello or 123test)

Marks: 1
Type: FILL_IN_THE_BLANKS_TYPE
