22/25 Questions Answered
1 question with unsaved changes

Assignment 6

Q1 Collaborators and Resources Used
0 Points

https://stackoverflow.com/questions/40208051/selenium-using-python-geckodriver-executable-needs-to-be-in-path
https://medium.com/dropout-analytics/selenium-and-geckodriver-on-mac-b411dbfe61bc
link in the comment of professor Blase

Save Answer Last saved on **Feb 16 at 4:45 PM**

Q2 Writeup Question 1
1 Point

uchicago-iot
uchicago-secure
uchicago-guest
uchicago

Save Answer Last saved on **Feb 16 at 4:47 PM**

Q3 Writeup Question 2
1 Point

It tried to visit a website called ocsp.digicert.com having IPv4 protocol. It requests CRL/CACERT Repository (certificate revocation list) within that website
The website need to confirm that the CA been used is not revoked.

Save Answer Last saved on **Feb 16 at 4:52 PM**

Q4 Writeup Question 3
2 Points

This query is answered in 4368, under the section DNS -> Answers -> cs9.wac.phicdn.net: type A, class IN, addr 72.21.91.29

Save Answer Last saved on **Feb 16 at 4:56 PM**

Q5 Writeup Question 4
1 Point

Destination address: 34.120.158.37

Destination address: 54.120.156.57

Save Answer Last saved on **Feb 16 at 4:57 PM**

Q6 Writeup Question 5
1 Point

7 in total

```
5599    22.859900235 192.168.0.100 128.135.24.29 HTTP    523  GET /guavaA/mobile/spr23.html HTTP/1.1
7875    23.248450264 192.168.0.100 128.135.24.29 HTTP    489  GET /guavaA/guavaA.css HTTP/1.1
8042    23.261880528 192.168.0.100 128.135.24.29 HTTP    496  GET /guavaA/mobile/mobile.css HTTP/1.1
8093    23.265721929 192.168.0.100 128.135.24.29 HTTP    480  GET /guavaA/mobile/mobile.js HTTP/1.1
8201    23.277759606 192.168.0.100 128.135.24.29 HTTP    482  GET /guavaA/code/COURSE_CMP.js HTTP/1.1
8206    23.277765260 192.168.0.100 128.135.24.29 HTTP    482  GET /data/course-data-22-23.js HTTP/1.1
9232    23.380851188 192.168.0.100 128.135.24.29 HTTP    490  GET /favicon.ico HTTP/1.1
```

Save Answer Last saved on **Feb 16 at 4:57 PM**

Q7 Writeup Question 6
1 Point

7964

Src Port: 80 (chicago-related-server), Dst Port: 49689(ghost)

Save Answer Last saved on **Feb 16 at 6:01 PM**

Q8 Writeup Question 7
1 Point

890+1779 = 2660

Save Answer Last saved on **Feb 16 at 6:01 PM**

Q9 Writeup Question 8
2 Points

4381 and 4385 are the two steps in network connection. In 4657, client (the ghost) sent SEQ number 1 with TCP length of 430, this led to ACK number from the server as 431 = 430+1. This kind of conversation continues as server keep sending back sum of sequence number and TCP length sent by the client to admit connection

Save Answer Last saved on **Feb 16 at 6:02 PM**

Q10 Writeup Question 9
1 Point

Different one

Src Port: 80 (chicago-related-server), Dst Port: 49697(ghost)

Save Answer Last saved on **Feb 16 at 6:02 PM**

Q11 Writeup Question 10
1 Point

The incoming port from the server is always 80 while ghost's port seems to increase sequentially

```
5599	22.859900235 192.168.0.100 128.135.24.29 HTTP	523  GET /guavaA/mobile/spr23.html HTTP/1.1
Src: 49689, Des: 80
7875	23.248450264 192.168.0.100 128.135.24.29 HTTP	489  GET /guavaA/guavaA.css HTTP/1.1
Src: 49695, Des: 80
8042	23.261880528 192.168.0.100 128.135.24.29 HTTP	496  GET /guavaA/mobile/mobile.css HTTP/1.1
Src: 49696, Des: 80
8093	23.265721929 192.168.0.100 128.135.24.29 HTTP	480  GET /guavaA/mobile/mobile.js HTTP/1.1
Src: 49697, Des: 80
8201	23.277759606 192.168.0.100 128.135.24.29 HTTP	482  GET /guavaA/code/COURSE_CMP.js HTTP/1.1
Src: 49698, Des: 80
8206	23.277765260 192.168.0.100 128.135.24.29 HTTP	482  GET /data/course-data-22-23.js HTTP/1.1
9232	23.380851188 192.168.0.100 128.135.24.29 HTTP	490  GET /favicon.ico HTTP/1.1
```

Save Answer Last saved on **Feb 16 at 5:03 PM**

Q12 Writeup Question 11
2 Points

Ghost is tried to close connection with 34.160.144.191 (which is what FIN doing, ACK is just the acknowledgement required to send after initial connection)

Save Answer Last saved on **Feb 16 at 5:03 PM**

Q13 Writeup Question 12
2 Points

www.google.com

He's searching "how to steal rare plants from blase"

It might be caused by TCP Dup ACK which means there's missing data

Save Answer Last saved on **Feb 16 at 5:03 PM**

Q14 Writeup Question 13
1 Point

104.123.153.192
Internet Protocol Version 4, Src: 192.168.0.100, Dst: 128.135.11.239

Save Answer Last saved on **Feb 16 at 5:03 PM**

Q15 Writeup Question 14
2 Points

Host: computersecurityclass.com\r\n
I determined it in In row No.30770, hyperlink transfer protocol

Save Answer Last saved on **Feb 16 at 5:04 PM**

Q16 Writeup Question 15
2 Points

https://computersecurityclass.com/4645316182537493008.html In No.30770, hyperlink transfer protocol, full-url section

Save Answer Last saved on **Feb 16 at 5:04 PM**

Q17 Writeup Question 16
2 Points

There's a continuous transformation of data (identified by TLS application data) between the ghost and server accompanied by ACK to keep ensuring connection. In the beginning there's a handshake, and in the end there's some [FIN, ACK] and retransmission that marks the termination and completion of the data transfer.

Save Answer Last saved on **Feb 16 at 5:23 PM**

Q18 Writeup Question 17
5 Points

https://computersecurityclass.com/4645316182537493008.html

Save Answer Last saved on **Feb 16 at 5:17 PM**

Q19 Writeup Question 18
3 Points

I added up all relative sequence numbers in [FIN, ACK] message coming from the server (not the ghost) because it represents the total amount of data gotten sent (minus retransmission fin ack data), open the two possible websites and use wireshark to record their traffic; then I do the same calculation and pick the one that has closer total amount of data.

Save Answer ***Unsaved Changes**

Q20 Writeup Question 19
4 Points

We can use rule-out method if a website contains a huge amount of URL links.
1. In general, a website with more information (media, photos, etc.) tends to send out a much larger amount of information, and vice versa. We can thus calculate a mean number of data for different kinds of websites. (there might also be other kinds of pattern a categories of websites may be like)
2. it would be better if there's a way to get the leaking decrypted message directly (like what we found out from the HTTP of ghost's visit record)

Save Answer Last saved on **Feb 16 at 5:21 PM**

Q21 Step 3 Code (submitted on Canvas)
12 Points

Save Answer

Q22 Writeup Question 20
3 Points

1. delete record of the first two websites (which we've already known)
2. I delete all ACK message (the only data we want is TLS with [ACK, FIN] message flag
3. I delete all retransmission message which won't affect the final calculation of data
4. Separate data into a sequence of JSON file, the separation is determined by the existence of a message [FIN, ACK] and a "Client hello" message after it
5. store the separated files into a directory

Save Answer Last saved on **Feb 16 at 5:27 PM**

Q23 Step 4 code (submitted on Canvas)
30 Points

Save Answer

Q24 Writeup Question 21
5 Points

From step 3 I already got the data transmitted for every website ghosts visit & the second websites he visited.
Here's what I do:
1. Sum() function (line 72) to determine the number of total data been transmitted
2. use function url_grabber to record all URL links presented in that known websites into an arr of string
3. open wireshark, use function RUN (line 91) to open up every URL links. Record all data, doing similar preprocessing to them (as in step 3, parse them into different json files, one represent one webpage), use SUM to compare sum of each websites with the real one. Pick the one with smallest error, continue with it and change it into a known website

Save Answer Last saved on **Feb 16 at 5:33 PM**

Q25 Writeup Question 22
15 Points

Enter your answer here

Save Answer Last saved on **Feb 16 at 5:35 PM**

Save All Answers

Submit & View Submission ›