Berkeley SCHOOL OF INFORMATION

CTF 1

Full Name: Jason Chow

Date: 9/10/2022

Challenge Name: Swimming Lesson

Browsers use the hypertext transfer protocol (HTTP) to retrieve webpages over the internet. To identify all websites visited during the conference, we must search for all HTTP requests in the PCAP file, which can can do by navigating to 'Statistics' > 'HTTP' > 'Requests'. The filter will output the domain (and sub-domain) of all webpages manually visited by user (i.e. user enters www.<some-domain>.com) and loaded automatically (i.e. ads, images, etc.) when web-page renders.

Analysis: There were (38) unique HTTP requests (by host) identified in file. The first (4) appear to be manually visited by user, while the remaing appears to be loaded automatically when a webpage renders (see appendex for screenshots).

1. www.thewayoftheninja.org
2. www.reddit.com
3. www.facebook.com
4. www.harveycartel.org
5. ninja-game.org
6. www.googletragservices.com
7. www.google-analytics.com
8. www.redditstatic.comlol
9. tpc.googlesyndication.com
10. toyotafr.solution.weborama.fr
11. t.9gag.com
12. static.ak.facebook.com
13. static.adzerk.net
14. secure.adzerk.net

SCHOOL OF INFORMATION, UNIVERSITY OF CALIFORNIA
102 SOUTH HALL #4600, BERKELEY, CA 94720-4600
PH 510.642.1464 FAX 510.642.5814
ISCHOOL.BERKELEY.EDU

15. pubads.g.doubleclick.net
16. platform.twitter.com
17. pixel.redditmedia.com
18. partner.googleadservices.com
19. pagead2.googlesyndication.com
20. miscmedia-9gag-lol.9gaging.com
21. its.tradelab.fr
22. img-9gag-ftw.9cache.com
23. ib.adnxs.com
24. googleads.g.doubleclick.net
25. engine.adzerk.net
26. csi.gstatic.com
27. connect.facebook.net
28. cdn.tradelab.fr
29. cdn.adnxs.com
30. c.thumbs.redditmedia.com
31. b.thumbs.redditmedia.com
32. assets-9gag-ftw.9cache.com
33. ams1.ib.adnxs.com
34. ajax.googleapis.com
35. ajax-9gag-lol.9cache.com
36. adx.g.doubleclick.net
37. a.thumbs.redditmedia.com
38. 9gag.com

Challenge Name: Ping-Pong Precision

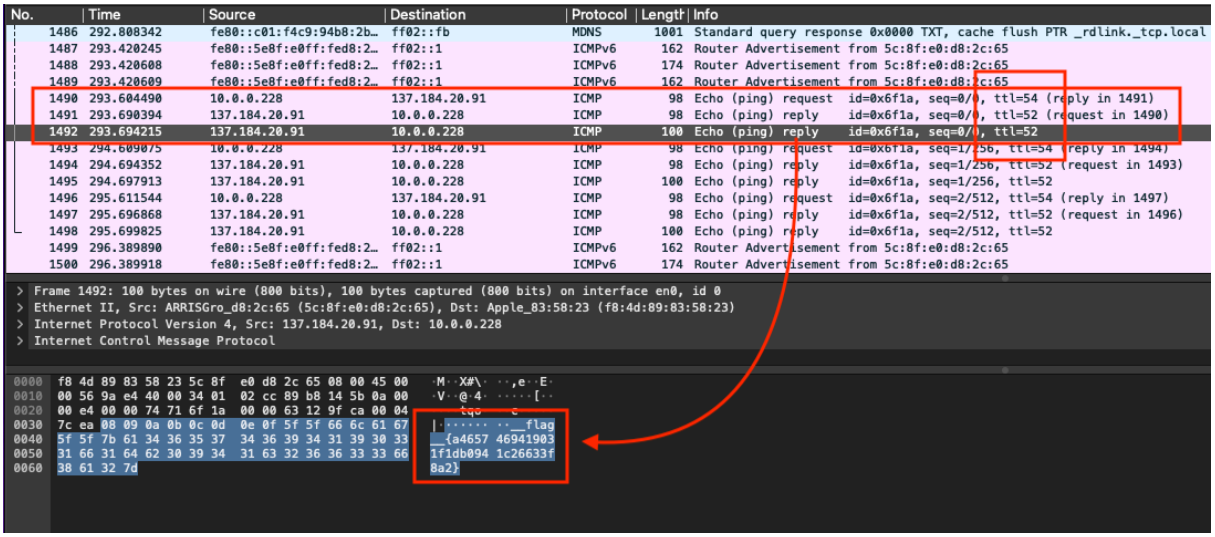
The Ping-Pong Precision challenge builds on the following knowledge: (1) as a packet travels through a router, the router will decrease the packets TTL value by one, and (2) the 'traceroute' utility tells us approximately how many routers exist between a host and desination computer.

To solve the challenge, we first run the 'traceroute.w210.network' command in order to determine the distance / number of routers (or 'hops') between my host computer and CTF system. We add the output (~10-14 hops) with the resulting TTL value the CTF system must receive (TTL = 42) in order to determine a starting TTL value (+/- 5) we should send in our ping command. The successful ping command that recovered flag was 'ping -m 54 w210.network', which means a starting TTL of 54 was required for a resulting TTL value of 42 to arrive at CTF system. Without knowing the distance, we must use a bruteforce approach, which will draw unwanted attention.

Figure 1: Output from 'traceroute w210.network'

```
(base) jasonchow@jchowmbp14 ~ % traceroute w210.network
traceroute to w210.network (137.184.20.91), 64 hops max, 52 byte packets
 1  10.0.0.1 (10.0.0.1)  5.895 ms  5.095 ms  4.982 ms
 2  96.120.90.93 (96.120.90.93)  16.439 ms  14.679 ms  16.144 ms
 3  68.86.248.53 (68.86.248.53)  14.712 ms  14.052 ms  15.004 ms
 4  68.87.194.205 (68.87.194.205)  15.416 ms  23.643 ms  14.847 ms
 5  be-217-rar01.santaclara.ca.sfba.comcast.net (69.139.199.193)  21.231 ms  16.141 ms  15.808 ms
 6  68.87.226.121 (68.87.226.121)  16.096 ms  17.892 ms  21.378 ms
 7  be-299-ar01.santaclara.ca.sfba.comcast.net (68.86.143.93)  18.637 ms  18.407 ms  16.961 ms
 8  lag-14.ear3.sanjose1.level3.net (4.68.72.105)  18.122 ms  15.446 ms  16.734 ms
 9  * * *
10  4.14.218.22 (4.14.218.22)  86.703 ms
    4.14.218.30 (4.14.218.30)  83.285 ms  84.825 ms
11  * * *
12  * * *
13  * * *
14  w210.network (137.184.20.91)  84.658 ms  86.312 ms  83.900 ms
(base) jasonchow@jchowmbp14 ~ % ping -m 55 w210.network
```

Figure 2: Reply from 'ping -m 54 w210.network'



Appendix: All HTTP requests in PCAP file: