

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 be done 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 remaining appears to be loaded automatically when a webpage renders (see appendix 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`

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 destination 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 brute force 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.sanjoel.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'

No.	Time	Source	Destination	Protocol	Length	Info
1486	292.808342	fe80::c01:f4c9:94b8:2b...	ff02::fb	MDNS	1001	Standard query response 0x0000 TXT, cache flush PTR _rdlink_tcp.local
1487	293.420245	fe80::5e8f:e0ff:fed8:2...	ff02::1	ICMPv6	162	Router Advertisement from 5c:8f:e0:d8:2c:65
1488	293.420608	fe80::5e8f:e0ff:fed8:2...	ff02::1	ICMPv6	174	Router Advertisement from 5c:8f:e0:d8:2c:65
1489	293.420609	fe80::5e8f:e0ff:fed8:2...	ff02::1	ICMPv6	162	Router Advertisement from 5c:8f:e0:d8:2c:65
1490	293.604490	10.0.0.228	137.184.20.91	ICMP	98	Echo (ping) request id=0x6f1a, seq=0/0, ttl=54 (reply in 1491)
1491	293.690394	137.184.20.91	10.0.0.228	ICMP	98	Echo (ping) reply id=0x6f1a, seq=0/0, ttl=52 (request in 1490)
1492	293.694215	137.184.20.91	10.0.0.228	ICMP	100	Echo (ping) reply id=0x6f1a, seq=0/0, ttl=52
1493	294.609075	10.0.0.228	137.184.20.91	ICMP	98	Echo (ping) request id=0x6f1a, seq=1/256, ttl=54 (reply in 1494)
1494	294.694352	137.184.20.91	10.0.0.228	ICMP	98	Echo (ping) reply id=0x6f1a, seq=1/256, ttl=52 (request in 1493)
1495	294.697913	137.184.20.91	10.0.0.228	ICMP	100	Echo (ping) reply id=0x6f1a, seq=1/256, ttl=52
1496	295.611544	10.0.0.228	137.184.20.91	ICMP	98	Echo (ping) request id=0x6f1a, seq=2/512, ttl=54 (reply in 1497)
1497	295.696868	137.184.20.91	10.0.0.228	ICMP	98	Echo (ping) reply id=0x6f1a, seq=2/512, ttl=52 (request in 1496)
1498	295.698825	137.184.20.91	10.0.0.228	ICMP	100	Echo (ping) reply id=0x6f1a, seq=2/512, ttl=52
1499	296.389890	fe80::5e8f:e0ff:fed8:2...	ff02::1	ICMPv6	162	Router Advertisement from 5c:8f:e0:d8:2c:65
1500	296.389918	fe80::5e8f:e0ff:fed8:2...	ff02::1	ICMPv6	174	Router Advertisement from 5c:8f:e0:d8:2c:65

> Frame 1492: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface en0, id 0
> Ethernet II, Src: ARRISGro_d8:2c:65 (5c:8f:e0:d8:2c:65), Dst: Apple_83:58:23 (f8:4d:89:83:58:23)
> Internet Protocol Version 4, Src: 137.184.20.91, Dst: 10.0.0.228
> Internet Control Message Protocol

```
0000 f8 4d 89 83 58 23 5c 8f e0 d8 2c 65 00 00 45 00  .M.X#.....E-
0010 00 56 9a e4 40 00 34 01 02 cc 89 08 14 5b 0a 00  .V.@4.....[...
0020 00 e4 00 00 74 71 6f 1a 00 00 63 12 9f ca 00 04  .4c.....
0030 7c ea 00 0a 0b 0c 0d 0e 0f 5f 5f 66 6c 61 67  .l.....flag
0040 5f 5f 7b 61 34 36 35 37 34 36 39 34 31 39 30 33  .{a4657 46941903
0050 31 66 31 64 62 30 39 34 31 63 32 36 36 33 33 66  .1fdb094 1c26633f
0060 38 61 32 7d                                     .8a2}
```

Appendix: All HTTP requests in PCAP file:

