Armira Nance

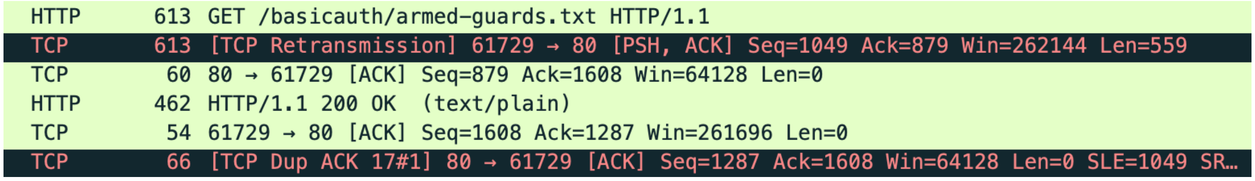
FA 2023

CS 338: Computer Security

HTTP Basic Authentication Assignment

In an attempt to understand what's happening on the backend when we perform HTTP basic authentication, I took captures of two different instances of me performing the same actions. Generally, I'm just navigating to the website, then clicking through the links from bottom to top, not including the homepage link at the very top. For one of these captures, I forgot to uncache the credentials so I was logged in almost as soon as I navigated to the page. For the other, I intentionally went back and cleared my cache in order to see how that affected the transmission data my packet sniffer caught.

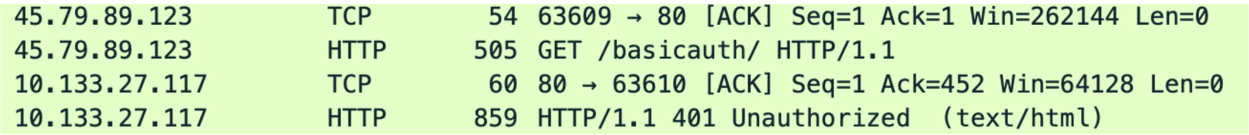
Looking at the packets sniffed out when I was signed in automatically, I immediately notice that two TCP handshakes are initiated back-to-back. The first is sent from port 61729 to port 80 and the second is sent from port 61730 to port 80. Both handshakes are completed successfully, though I wonder why there were two instead of one, as the handshakes are completely identical outside of the different initiating ports. Once the handshake is completed, there's a GET request for the webpage we're looking for, which is accepted and we receive a success code of 200. When I clicked the link at the bottom of the page (link 1), there was a GET request for the information on that page, which was accepted and displayed in the browser. I navigated back and attempted to navigate to the second link from the bottom of the page (link 2). There was a GET request for link 2 that was accepted and the page was displayed, but the packets looked peculiar for this part. I noticed that there were two red-colored entries, one of them labeled “TCP Retransmission.” After conducting further research, it appears that this entry came about because a packet was retransmitted after the expiration of the acknowledgement (the third part of our TCP-handshake). It seems that this is something that can happen when there’s a lot of information being transmitted at once and the network gets congested, so I wonder if this was caused in part because I moved very quickly when I navigated from link 1 to the homepage then link 2. I think it’s a plausible idea, because I hesitated before clicking link 1 and the final link (link 3) and this error didn’t come up for those distinct sets of packets.



```
HTTP      613  GET /basicauth/armed-guards.txt HTTP/1.1
TCP       613  [TCP Retransmission] 61729 → 80 [PSH, ACK] Seq=1049 Ack=879 Win=262144 Len=559
TCP        60  80 → 61729 [ACK] Seq=879 Ack=1608 Win=64128 Len=0
HTTP      462  HTTP/1.1 200 OK  (text/plain)
TCP        54  61729 → 80 [ACK] Seq=1608 Ack=1287 Win=261696 Len=0
TCP        66  [TCP Dup ACK 17#1] 80 → 61729 [ACK] Seq=1287 Ack=1608 Win=64128 Len=0 SLE=1049 SR…
```

After this, the only notable event was the TCP Keep-Alive, which basically just maintained the connection and verified that it’s still alive.

Looking at the other packet capture, there’s not much difference. There were still two separate TCP-handshakes, and only one port between the two that was actually used. The primary difference that I found is that when I entered the password or username incorrectly, the packets reflected that the website could not display the contents of the webpage, because I was unauthorized (thus, it returned a 404 failure code).



```
45.79.89.123          TCP        54  63609 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
45.79.89.123          HTTP      505  GET /basicauth/ HTTP/1.1
10.133.27.117         TCP        60  80 → 63610 [ACK] Seq=1 Ack=452 Win=64128 Len=0
10.133.27.117         HTTP      859  HTTP/1.1 401 Unauthorized  (text/html)
```