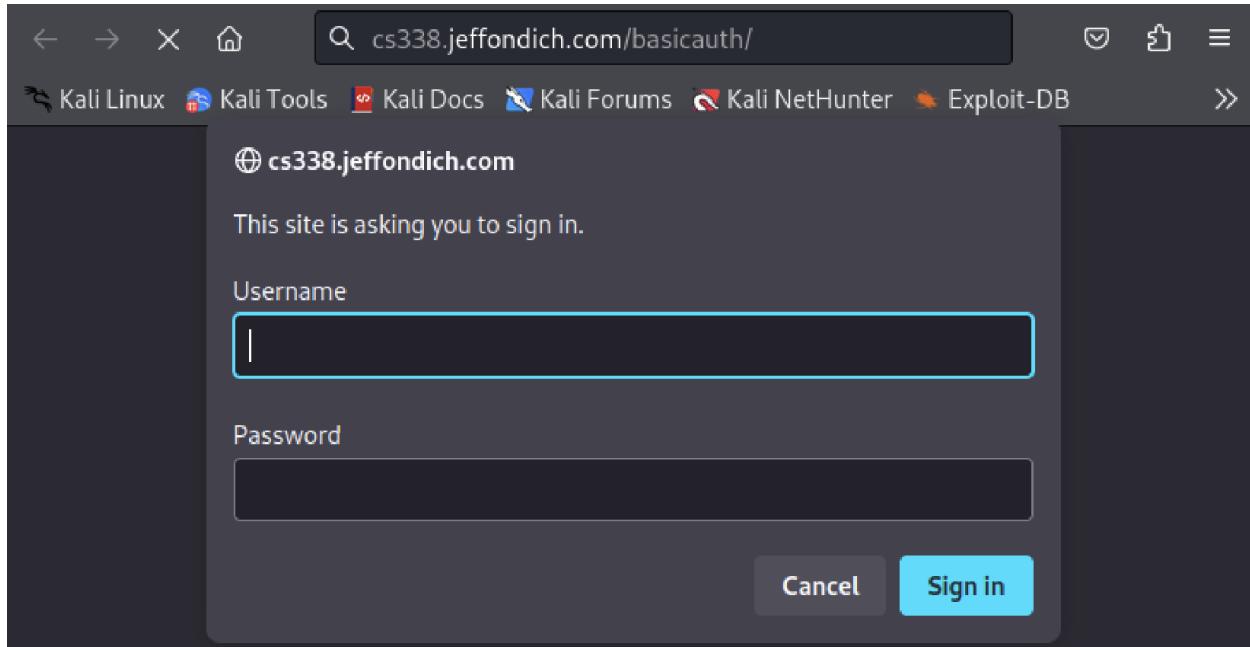


After some difficulty and professor consultation, I managed to open Wireshark on the ethernet interface (for me `eth0`) and filter to the target site's IP address.



From there I opened Firefox on Kali and submitted the URL for the target page, and was greeted with the authentication pop-up.



I input our credentials to gain access to the page, and then hopped over to Wireshark to stop sniffing and analyze the packets.

The first thing that was interesting was that my browser had apparently opened up two ports, 57672 and 57686, to the server's port 80. Jeff said this was likely to handle different kinds of incoming packets more quickly.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.64.2	45.79.89.123	TCP	74	57672 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
2	0.000066981	192.168.64.2	45.79.89.123	TCP	74	57686 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
3	0.052205387	45.79.89.123	192.168.64.2	TCP	66	80 → 57672 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=13
4	0.052262329	192.168.64.2	45.79.89.123	TCP	54	57672 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
5	0.052205678	45.79.89.123	192.168.64.2	TCP	66	80 → 57686 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=13
6	0.052228314	192.168.64.2	45.79.89.123	TCP	54	57686 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0

After the ports were opened, my browser requested the page at the URL,

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	192.168.64.2	45.79.89.123	TCP	74	57672 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
2	0.000066981	192.168.64.2	45.79.89.123	TCP	74	57686 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
3	0.052205387	45.79.89.123	192.168.64.2	TCP	66	80 → 57672 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=13
4	0.052226329	192.168.64.2	45.79.89.123	TCP	54	57672 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
5	0.052205678	45.79.89.123	192.168.64.2	TCP	66	80 → 57686 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=13
6	0.0522283114	192.168.64.2	45.79.89.123	TCP	54	57686 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
7	0.052721654	192.168.64.2	45.79.89.123	HTTP	409	GET /basicauth/ HTTP/1.1
8	0.107171681	45.79.89.123	192.168.64.2	TCP	54	80 → 57686 [ACK] Seq=1 Ack=356 Win=64128 Len=0
9	0.107171889	45.79.89.123	192.168.64.2	HTTP	457	HTTP/1.1 401 Unauthorized (text/html)
10	0.107222457	192.168.64.2	45.79.89.123	TCP	54	57686 → 80 [ACK] Seq=356 Ack=404 Win=64128 Len=0
11	5.053171379	192.168.64.2	45.79.89.123	TCP	54	57672 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64256 Len=0
12	5.108720587	45.79.89.123	192.168.64.2	TCP	54	80 → 57672 [FIN, ACK] Seq=1 Ack=2 Win=64256 Len=0

```

> Transmission Control Protocol, Src Port: 57686, Dst Port: 80, Seq: 1, Ack: 0000 3e a6 f6 05 ba 64 8a 19 13 ec b0 35 08 00 45 00 >...
-> Hypertext Transfer Protocol
  > GET /basicauth/ HTTP/1.1\r\n
    Host: cs338.jeffondich.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 F... 0010 01 8b 7e 12 40 90 40 06 33 e6 c0 a8 40 02 2d 4f ...@...
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif 0020 59 7b e1 56 00 50 1e dd 34 e0 87 0e a4 6d 50 18 Y{.V...
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Full request URI: http://cs338.jeffondich.com/basicauth/]
  [HTTP request 1/3]
  
```

and the server denied access, claiming it was a protected area and offering the credential input pop-up.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	192.168.64.2	45.79.89.123	TCP	74	57672 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
2	0.000066981	192.168.64.2	45.79.89.123	TCP	74	57686 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
3	0.052205387	45.79.89.123	192.168.64.2	TCP	66	80 → 57672 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=13
4	0.052226329	192.168.64.2	45.79.89.123	TCP	54	57672 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
5	0.052205678	45.79.89.123	192.168.64.2	TCP	66	80 → 57686 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=13
6	0.0522283114	192.168.64.2	45.79.89.123	TCP	54	57686 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
7	0.052721654	192.168.64.2	45.79.89.123	HTTP	409	GET /basicauth/ HTTP/1.1
8	0.107171681	45.79.89.123	192.168.64.2	TCP	54	80 → 57686 [ACK] Seq=1 Ack=356 Win=64128 Len=0
9	0.107171889	45.79.89.123	192.168.64.2	HTTP	457	HTTP/1.1 401 Unauthorized (text/html)
10	0.107222457	192.168.64.2	45.79.89.123	TCP	54	57686 → 80 [ACK] Seq=356 Ack=404 Win=64128 Len=0
11	5.053171379	192.168.64.2	45.79.89.123	TCP	54	57672 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64256 Len=0
12	5.108720587	45.79.89.123	192.168.64.2	TCP	54	80 → 57672 [FIN, ACK] Seq=1 Ack=2 Win=64256 Len=0

```

> Transmission Control Protocol, Src Port: 80, Dst Port: 57686, Seq: 1, Ack: 0000 8a 19 13 ec b0 35 3e a6 f6 05 ba 64 08 00 45 00 ...
-> Hypertext Transfer Protocol
  > HTTP/1.1 401 Unauthorized\r\n
    Server: nginx/1.18.0 (Ubuntu)\r\n
    Date: Wed, 20 Sep 2023 20:46:51 GMT\r\n
    Content-Type: text/html\r\n
    > Content-Length: 188\r\n
    Connection: keep-alive\r\n
    WWW-Authenticate: Basic realm="Protected Area"\r\n
  \r\n
  [HTTP response 1/3]
  [Time since request: 0.054450235 seconds]
  [Request in frame: 7]
  
```

Between the time the client received the denial HTTP and I sent the credentials back, my client asked to shut down one port, 57672, and the server agreed. The client requested, however, that the connection on port 57686 persist and the server also agreed.

No.	Time	Source	Destination	Protocol	Length	Info
11	5.053171379	192.168.64.2	45.79.89.123	TCP	54	57672 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64256 Len=0
12	5.108720587	45.79.89.123	192.168.64.2	TCP	54	80 → 57672 [FIN, ACK] Seq=1 Ack=2 Win=64256 Len=0
13	5.108763118	192.168.64.2	45.79.89.123	TCP	54	57672 → 80 [ACK] Seq=2 Ack=2 Win=64256 Len=0
14	10.189359811	192.168.64.2	45.79.89.123	TCP	54	[TCP Keep-Alive] 57686 → 80 [ACK] Seq=355 Ack=404 Win=64...
15	10.242026325	45.79.89.123	192.168.64.2	TCP	54	[TCP Keep-Alive ACK] 80 → 57686 [ACK] Seq=404 Ack=356 Wi...

Once I had input the credentials, the client sent another HTTP packet, this time including the username and password in base64.

No.	Time	Source	Destination	Protocol	Length	Info
11	5.053171379	192.168.64.2	45.79.89.123	TCP	54	57672 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64256 Len=0
12	5.108726587	45.79.89.123	192.168.64.2	TCP	54	80 → 57672 [FIN, ACK] Seq=1 Ack=2 Win=64256 Len=0
13	5.108763118	192.168.64.2	45.79.89.123	TCP	54	57672 → 80 [ACK] Seq=2 Ack=2 Win=64256 Len=0
14	10.189359811	192.168.64.2	45.79.89.123	TCP	54	[TCP Keep-Alive] 57686 → 80 [ACK] Seq=355 Ack=404 Win=64
15	10.242026325	45.79.89.123	192.168.64.2	TCP	54	[TCP Keep-Alive ACK] 80 → 57686 [ACK] Seq=404 Ack=356 Wi
16	15.980037269	192.168.64.2	45.79.89.123	HTTP	452	GET /basicauth/ HTTP/1.1
17	16.033377861	45.79.89.123	192.168.64.2	TCP	54	80 → 57686 [ACK] Seq=404 Ack=754 Win=64128 Len=0
18	16.035123607	45.79.89.123	192.168.64.2	HTTP	458	HTTP/1.1 200 OK (text/html)
19	16.035140853	192.168.64.2	45.79.89.123	TCP	54	57686 → 80 [ACK] Seq=754 Ack=808 Win=64128 Len=0
20	16.086554654	192.168.64.2	45.79.89.123	HTTP	369	GET /favicon.ico HTTP/1.1
21	16.210461974	45.79.89.123	192.168.64.2	TCP	54	80 → 57686 [ACK] Seq=808 Ack=1069 Win=64128 Len=0
22	16.210462224	45.79.89.123	192.168.64.2	HTTP	383	HTTP/1.1 404 Not Found (text/html)

```

Hypertext Transfer Protocol
  GET /basicauth/ HTTP/1.1\r\n
Host: cs338.jeffondich.com\r\n
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 F
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
  Authorization: Basic Y3MzMzg6cGFzc3dvcml0eQ=\r\n
    Credentials: cs338:password
\r\n
[Full request URI: http://cs338.jeffondich.com/basicauth/]

```

The server accepted the credentials, and sent back the HTTP for the actual page.

No.	Time	Source	Destination	Protocol	Length	Info
11	5.053171379	192.168.64.2	45.79.89.123	TCP	54	57672 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64256 Len=0
12	5.108726587	45.79.89.123	192.168.64.2	TCP	54	80 → 57672 [FIN, ACK] Seq=1 Ack=2 Win=64256 Len=0
13	5.108763118	192.168.64.2	45.79.89.123	TCP	54	57672 → 80 [ACK] Seq=2 Ack=2 Win=64256 Len=0
14	10.189359811	192.168.64.2	45.79.89.123	TCP	54	[TCP Keep-Alive] 57686 → 80 [ACK] Seq=355 Ack=404 Win=64
15	10.242026325	45.79.89.123	192.168.64.2	TCP	54	[TCP Keep-Alive ACK] 80 → 57686 [ACK] Seq=404 Ack=356 Wi
16	15.980037269	192.168.64.2	45.79.89.123	HTTP	452	GET /basicauth/ HTTP/1.1
17	16.033377861	45.79.89.123	192.168.64.2	TCP	54	80 → 57686 [ACK] Seq=404 Ack=754 Win=64128 Len=0
18	16.035123607	45.79.89.123	192.168.64.2	HTTP	458	HTTP/1.1 200 OK (text/html)
19	16.035140853	192.168.64.2	45.79.89.123	TCP	54	57686 → 80 [ACK] Seq=754 Ack=808 Win=64128 Len=0
20	16.086554654	192.168.64.2	45.79.89.123	HTTP	369	GET /favicon.ico HTTP/1.1
21	16.210461974	45.79.89.123	192.168.64.2	TCP	54	80 → 57686 [ACK] Seq=808 Ack=1069 Win=64128 Len=0
22	16.210462224	45.79.89.123	192.168.64.2	HTTP	383	HTTP/1.1 404 Not Found (text/html)

```

Transmission Control Protocol, Src Port: 80, Dst Port: 57686, Seq: 404, A
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
Server: nginx/1.18.0 (Ubuntu)\r\n
Date: Wed, 20 Sep 2023 20:47:07 GMT\r\n
Content-Type: text/html\r\n
Transfer-Encoding: chunked\r\n
Connection: keep-alive\r\n
Content-Encoding: gzip\r\n
\r\n
[HTTP response 2/3]
[Time since request: 0.055086338 seconds]
[Prev request in frame: 7]

```

Frame (458 bytes) De-chunked entity body (205 bytes) Uncompressed ent... ▾