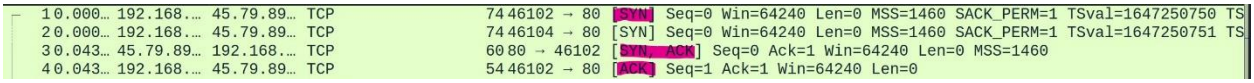
AUTHOR - KAI JOHNSON

STORY

Chapter 1: the handshake

Firstly, the client and server engage in a tcp 3-way handshake.

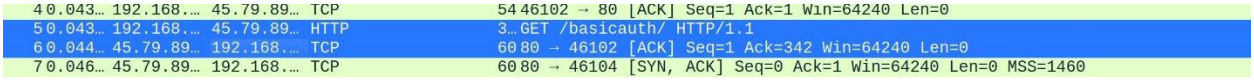
1. the client (192.168.58.128, the vmware software) sends [SYN] (a synchronization request),
2. the server (45.79.89.123, cs231.jeffondich.com) returns [SYN, ACK] (an acknowledgement and its own synchronization request),
3. the client returns [ACK] (an acknowledgement of the server's message).



Chapter 2: the HTML request

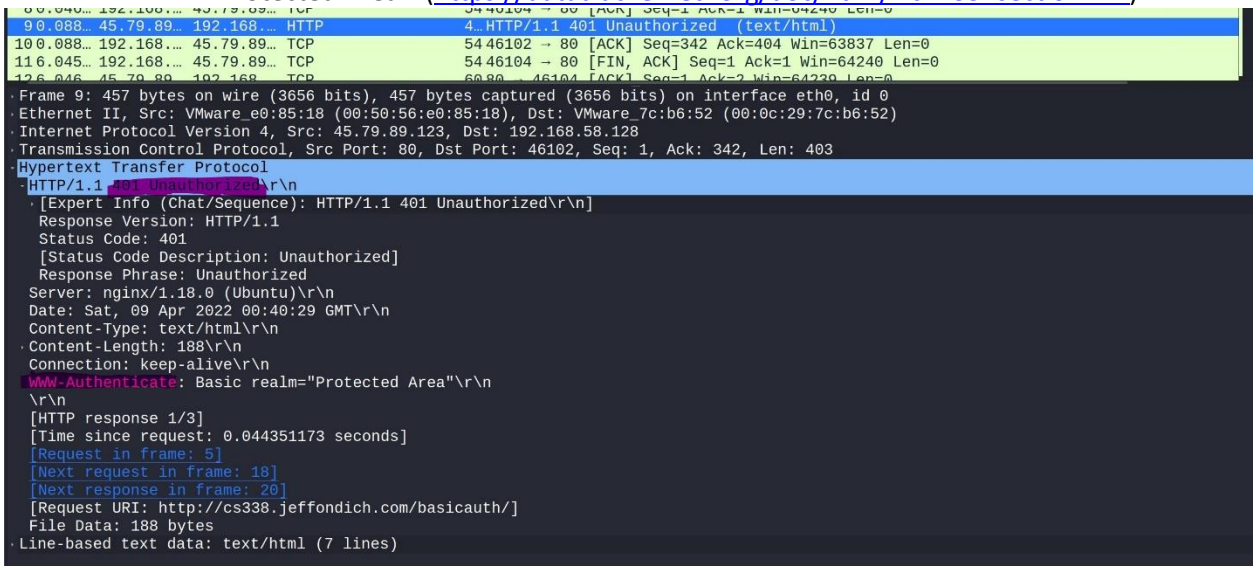
Now that a connection is set up between the client and server, the client makes its' request: it wants access to the page: http://cs338.jeffondich.com/basicauth/

4. the client sends an HTTP GET request for the above page
5. the server acknowledges the request

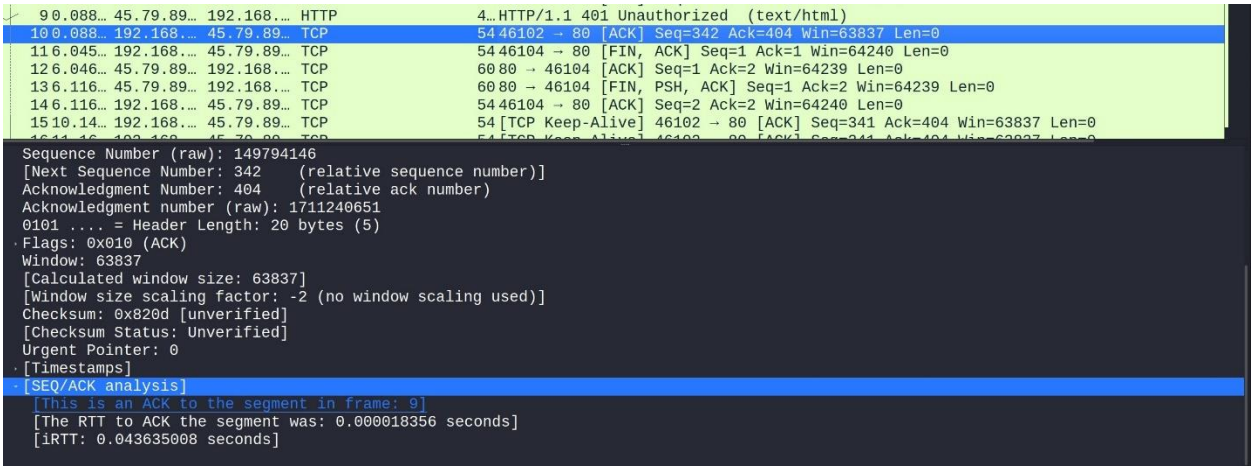


Chapter 3: the initial server rejection

6. the server sends back an HTTP "Unauthorized" packet, with status code 401, telling the client that authorization is required to visit the webpage that they requested,
    a. issuing a "WWW-Authenticate" challenge for the Basic scheme with a realm value of "Protected Area" (https://datatracker.ietf.org/doc/html/rfc7235#section-4.2)

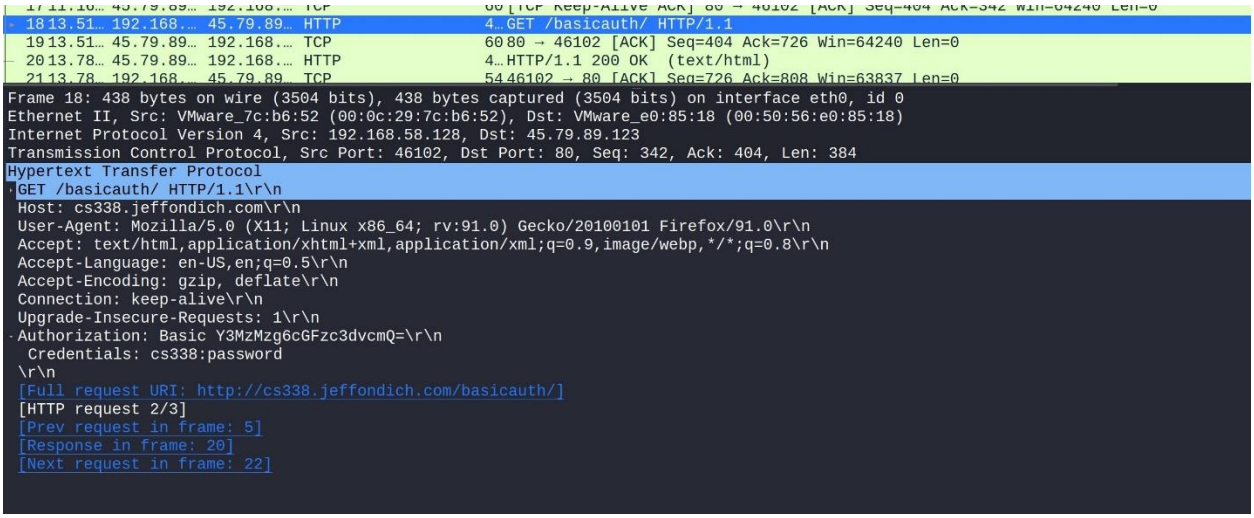


7. the client acknowledges the HTTP response from the server



Chapter 4: the extremely secure credential communication

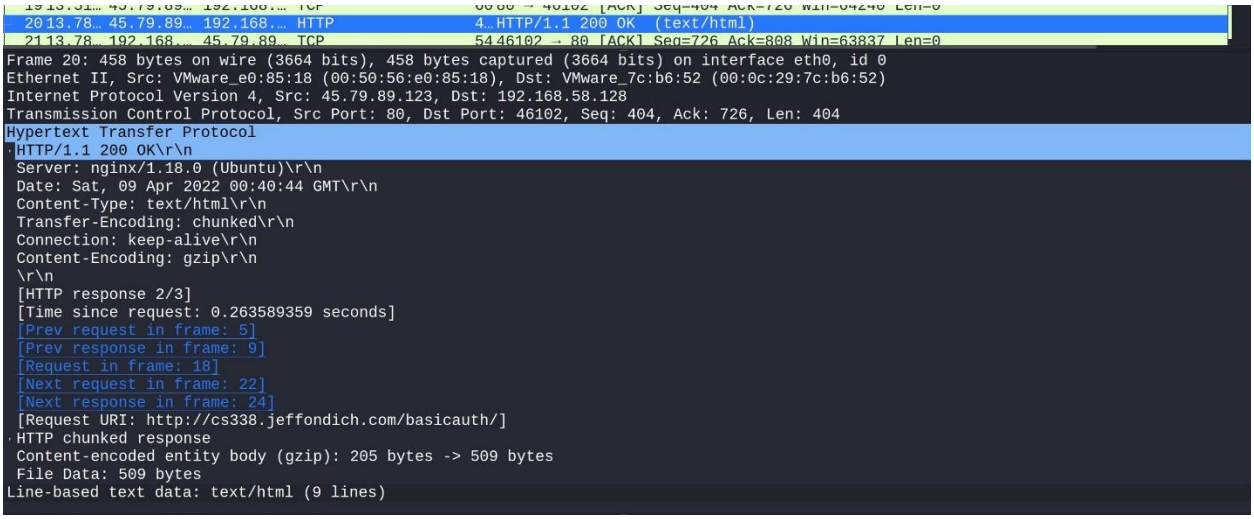
8. once the user (that is, the human trying to access http://cs338.jeffondich.com/basicauth/ through the firefox browser installed on their virtual machine) submits the credential pair, the client sends another HTTP GET request, with an Authorization header.
    a. The authorization header indicates the authorization scheme and the credentials.
        i. As communicated by the server (discussed in 6), the authorization scheme is “Basic.” Consequently, the first portion of the authorization header indicates this authorization scheme: it reads “`Authorization: Basic`”
        ii. the next portion are the credentials. The userID and the password are combined to form the user-pass (userID + “:” + password). Thus, a username of “cs338” and password of “password” form the user-pass “cs338:password”. This user-pass is then encoded to an octet sequence, which is encoded by base64. The user-pass of “cs338:password” is encoded as “`Y3MzMzg6cGFzc3dvcmQ=`”.
            1. encoding from user-pass to octet does not have specific implementation specified in original definition of authentication scheme
            2. for more discussion of base64 encoding scheme, see https://datatracker.ietf.org/doc/html/rfc4648#section-4
            3. notably, the credentials are NOT ENCRYPTED; if a program can decode base64 encoding (eg, the wireshark GUI) it can print the sent credentials
        iii. Thus, the authorization header reads
        `Authorization: Basic Y3MzMzg6cGFzc3dvcmQ=`
        containing the authorization scheme and the credentials.
        iv. for more on the Basic authorization scheme, see: https://datatracker.ietf.org/doc/html/rfc7617



9. the server returns a TCP acknowledgement

Chapter 5: the access

10. the server accepts the credential pair and returns an “OK” package containing the html for the webpage



11. the client returns a TCP acknowledgement

Chapter 6: wait, what about that logo?

12. the client also sends an HTTP GET request for http://cs338.jeffondich.com/favicon.ico
13. the server acknowledges the request, and returns an HTTP 404 not found response
14. the client acknowledges the HTTP not found message