Http Basic Auth [Let's Defend – Write-up]

We receive a log indicating a possible attack, can you gather information from the .pcap file?

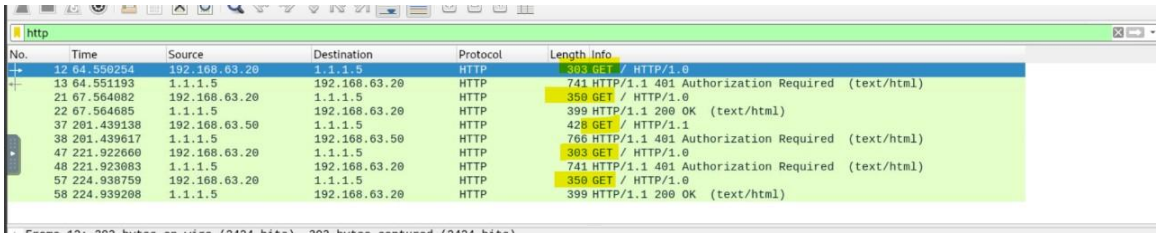
Log file: /root/Desktop/ChallengeFile/webserver.em0.pcap

Note: pcap file found public resources.

| Start Investigation

Q1: How many HTTP GET requests are in pcap?

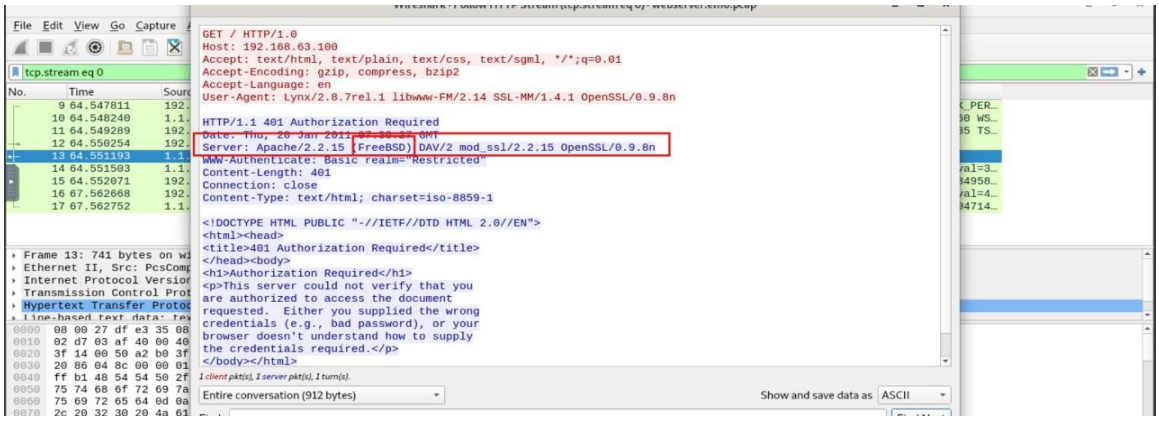
After I opened the pcap file, I searched for http to get the GET method.



Answer: 5

Q2: What is the server operating system?

After that, I checked one of the packets in question 1 and then searched for a server.



Answer: freebsd

Q3: What is the name and version of the web server software?

Also, the answer in the same packet

```
HTTP/1.1 401 Authorization Required
Date: Thu, 20 Jan 2011 07:36:27 GMT
Server: Apache/2.2.15 (FreeBSD) DAV/2 mod_ssl/2.2.15 OpenSSL/0.9.8n
WWW-Authenticate: Basic realm="Restricted"
Content-Length: 401
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
```

Answer: apache/2.2.15

Q4: What is the version of OpenSSL running on the server?

Also, the answer in the same packet

```
HTTP/1.1 401 Authorization Required
Date: Thu, 20 Jan 2011 07:36:27 GMT
Server: Apache/2.2.15 (FreeBSD) DAV/2 mod_ssl/2.2.15 OpenSSL/0.9.8n
WWW-Authenticate: Basic realm="Restricted"
Content-Length: 401
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Authorization Required</title>
</head><body>
<h1>Authorization Required</h1>
<p>This server could not verify that you
are authorized to access the document
```

Answer: openssl/0.9.8n

Q5: What is the client's user-agent information?

Also, the answer in the same packet

```
GET / HTTP/1.0
Host: 192.168.63.100
Accept: text/html, text/plain, text/css, text/sgml, */*;q=0.01
Accept-Encoding: gzip, compress, bzip2
Accept-Language: en
User-Agent: Lynx/2.8.7rel.1 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.8n

HTTP/1.1 401 Authorization Required
```

Answer: lynx/2.8.7rel.1 libwww-fm/2.14 ssl-mm/1.4.1 openssl/0.9.8n

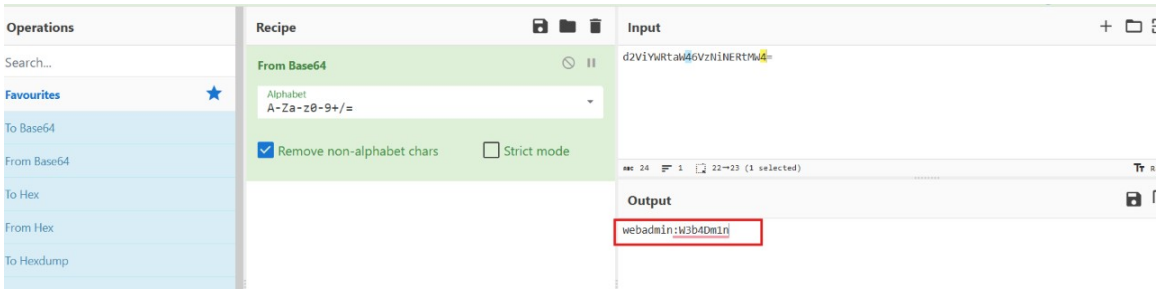
Q6: What is the username used for Basic Authentication?

I checked one of the packets and got the username and password for base64

```
GET / HTTP/1.0
Host: 192.168.63.100
Accept: text/html, text/plain, text/css, text/sgml, */*;q=0.01
Accept-Encoding: gzip, compress, bzip2
Accept-Language: en
User-Agent: Lynx/2.8.7rel.1 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.8n
Authorization: Basic d2ViYWRtaW46VzNiNERtMW4=

HTTP/1.1 200 OK
Date: Thu, 20 Jan 2011 07:39:08 GMT
Server: Apache/2.2.15 (FreeBSD) DAV/2 mod_ssl/2.2.15 OpenSSL/0.9.8n
Last-Modified: Mon, 27 Dec 2010 13:11:28 GMT
ETag: "3f44b-2c-4986412e52000"
Accept-Ranges: bytes
Content-Length: 44
Connection: close
Content-Type: text/html

<html><body><h1>It works!</h1></body></html>
```



So I cracked it using cyberchef and got the username and password, this answer for questions 6 and 7.

Answer: webadmin

Q7: What is the user password used for Basic Authentication?

Answer: w3b4dm1n

Summary

This investigation into HTTP Basic Authentication was an eye-opening experience that significantly improved my network forensics and packet analysis skills.

Through this lab, I learned how to move beyond basic traffic monitoring to performing deep packet inspection (DPI) using Wireshark. It was fascinating to see how a server's entire "fingerprint"—including its OS (FreeBSD), web server version (Apache/2.2.15), and even the OpenSSL version—is clearly visible within HTTP response headers.

The most valuable lesson, however, was the hands-on demonstration of why Basic Authentication is a major security risk. Seeing the Authorization header in the packet and realizing it was just a simple Base64 string that I could easily decode with CyberChef to reveal the username (webadmin) and password (w3b4dm1n) made the concept of "clear-text credentials" very real to me. This investigation perfectly bridged the gap between theoretical security risks and actual, exploitable vulnerabilities.