

Blue Team Labs Online: Shuba Insider

The following writeup is for [Shiba Insider](#) on Blue Team Labs Online, it's an easy lab that involves analysing a PCAP file using Wireshark, and then using tools like steghide and exiftool to analyse a given jpg file. If you enjoy simply challenges, I recommend this room. If however, you enjoy difficult and more realistic challenges I would not recommend this one.

What is the response message obtained from the PCAP file?

If you open the PCAP, there are only 10 captured packets:

No.	Time	Source	Destination	Destination Port	Protocol	Info
1	2021-09-26 21:03:43	192.168.176.1	192.168.176.145	8081	TCP	52726 → 8081 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2677...
2	2021-09-26 21:03:43	192.168.176.145	192.168.176.1	52726	TCP	8081 → 52726 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM...
3	2021-09-26 21:03:43	192.168.176.1	192.168.176.145	8081	TCP	52726 → 8081 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2677149058 TSecr=...
4	2021-09-26 21:03:43	192.168.176.1	192.168.176.145	8081	HTTP	GET http://192.168.176.145:8099/hidden.txt?message=how+do+i+open+file HT...
5	2021-09-26 21:03:43	192.168.176.145	192.168.176.1	52726	TCP	8081 → 52726 [ACK] Seq=1 Ack=448 Win=64768 Len=0 TSval=1924421063 TSecr=...
6	2021-09-26 21:03:43	192.168.176.145	192.168.176.1	52726	HTTP	HTTP/1.0 200 OK (text/plain)
7	2021-09-26 21:03:43	192.168.176.1	192.168.176.145	8081	TCP	52726 → 8081 [ACK] Seq=448 Ack=208 Win=64128 Len=0 TSval=2677149112 TS...
8	2021-09-26 21:03:43	192.168.176.145	192.168.176.1	52726	TCP	8081 → 52726 [FIN, ACK] Seq=208 Ack=448 Win=64768 Len=0 TSval=19244211...
9	2021-09-26 21:03:43	192.168.176.1	192.168.176.145	8081	TCP	52726 → 8081 [FIN, ACK] Seq=448 Ack=209 Win=64128 Len=0 TSval=26771491...
10	2021-09-26 21:03:43	192.168.176.145	192.168.176.1	52726	TCP	8081 → 52726 [ACK] Seq=209 Ack=449 Win=64768 Len=0 TSval=1924421119 TS...

If you follow the TCP stream for the first HTTP GET request, we can see the following:

```
GET http://192.168.176.145:8099/hidden.txt?message=how+do+i+open+file HTTP/1.1
Host: 192.168.176.145:8099
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Authorization: Basic ZmFrZWJsdWU6cmVkZm9yZXZlcg==
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.9.2
Date: Sun, 26 Sep 2021 21:03:43 GMT
Content-type: text/plain
Content-Length: 22
Last-Modified: Sun, 26 Sep 2021 20:54:03 GMT

use your own password
```

The response message is simply “use your own password”.

What is the password of the ZIP file?

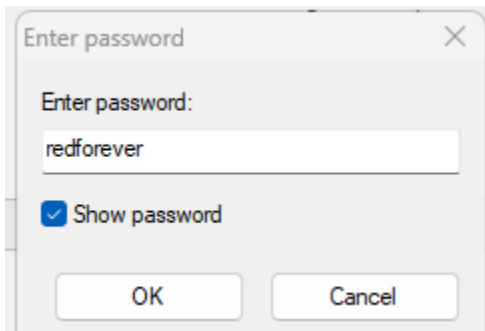
In the GET Request, you can see that HTTP basic auth was used. If you decode the Base64 encoded string, you can find a set of credentials:

Input
ZmFrZWJsdWU6cmVkJm9yZXZlcg==
REC 28 1
Output
fakeblue:redforever

The password is redforever, We can use this password to unzip the zip file:

D

Will more passwords be required?



What is the name of a widely-used tool that can be used to obtain file information?

Exiftool is the name of a widely-used tool that can be used to obtain file metadata.

What is the name and value of the interesting information obtained from the image file metadata?

```

(kali@kali)-[~/Downloads]
$ exiftool ssdog1.jpeg
ExifTool Version Number      : 12.76
File Name                    : ssdog1.jpeg
Directory                   : .
File Size                    : 84 kB
File Modification Date/Time  : 2025:02:06 23:46:51-05:00
File Access Date/Time       : 2025:02:06 23:46:51-05:00
File Inode Change Date/Time  : 2025:02:06 23:46:51-05:00
File Permissions             : -rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : None
X Resolution                 : 1
Y Resolution                 : 1
XMP Toolkit                  : Image::ExifTool 11.88
Technique                    : Steganography
Technique Command            : steghide
Image Width                  : 1080
Image Height                 : 1018
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:4:4 (1 1)
Image Size                   : 1080x1018
Megapixels                   : 1.1

```

The answer is technique:steganography

Based on the answer from the previous question, what tool needs to be used to retrieve the information hidden in the file?

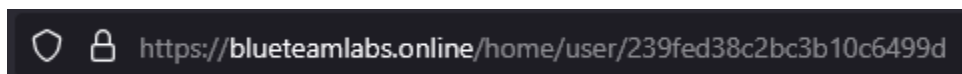
Steghide.

Enter the ID retrieved.

After using steghide or a tool like Aperisolve, you can see that it extracts a file named "idInsider.txt" containing the following ID: 0726ba878ea47de571777a.

What is the profile name of the attacker?

If you check out your profile on BTLO, you can see there is a user ID string in the URL:



The screenshot shows a web browser address bar with a lock icon on the left and a URL: <https://blueteamlabs.online/home/user/239fed38c2bc3b10c6499d>

Let's replace this string with the ID retrieved previously:



bluetiger



Rank: **Initiate**