

# Shiba Insider

## Contents

Scenario.....	2
Pre-requisites .....	2
Initial thoughts from scenario .....	2
Challenge Questions .....	2
What is the response message obtained from the PCAP file? .....	2
What is the password of the ZIP file? .....	4
Will more passwords be required? .....	4
What is the name of a widely-used tool that can be used to obtain file information? .....	5
What is the name & value of the interesting information obtained from the image file metadata? ..	5
Based on the answer from the previous question, what tool needs to be used to retrieve the information hidden in the file? .....	6
Enter the ID retrieved. ....	6
What is the profile name of the attacker? .....	6

## Scenario

Can you uncover the insider?

## Pre-requisites

- Load kali
- Run `sudo apt update && sudo apt -y upgrade > reboot`
- Change network to host only instead of NAT – to restrict network so malware inside the pcap is contained within the VM
- Extract inner zip and pcap from the challenge zip
  - Load Wireshark and open the pcap file

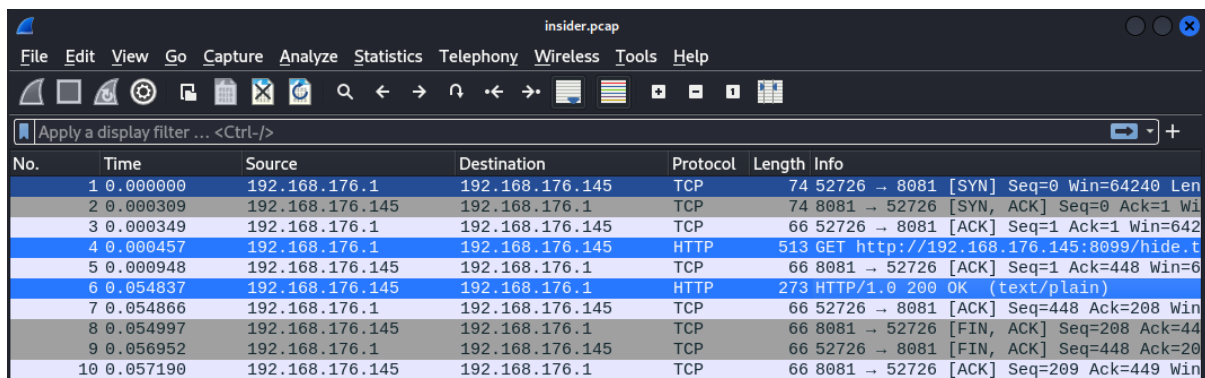
## Initial thoughts from scenario

- Inner zip is password protected, so likely have to find the password in the pcap
  - Given I need credentials, maybe it's a pcap using a cleartext protocol such as FTP/HTTP? Could also be found in payload of TCP packet?

## Challenge Questions

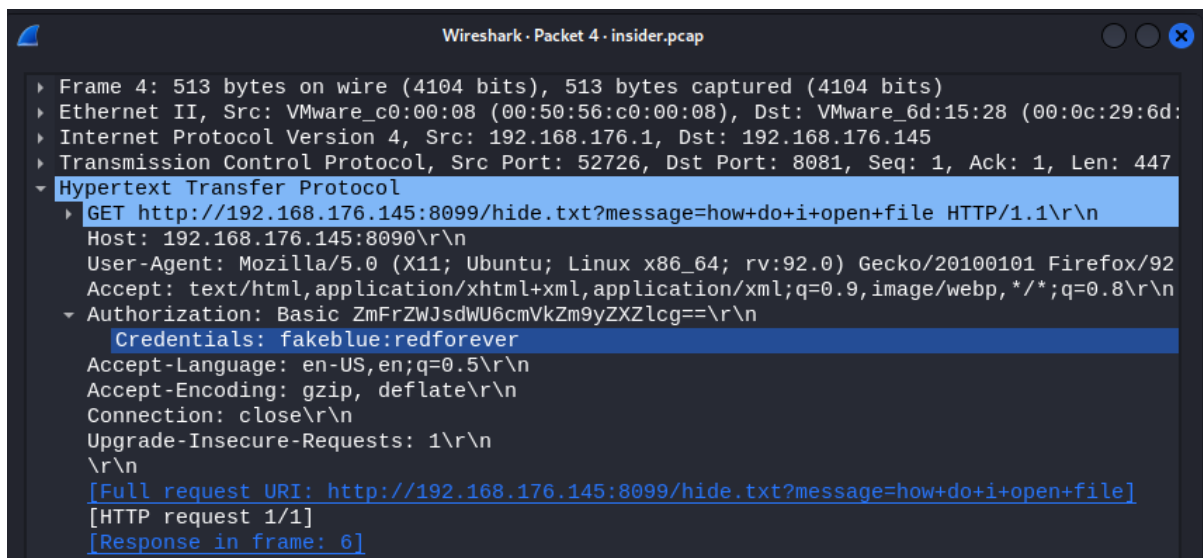
What is the response message obtained from the PCAP file?

- **Answer: use your own password**

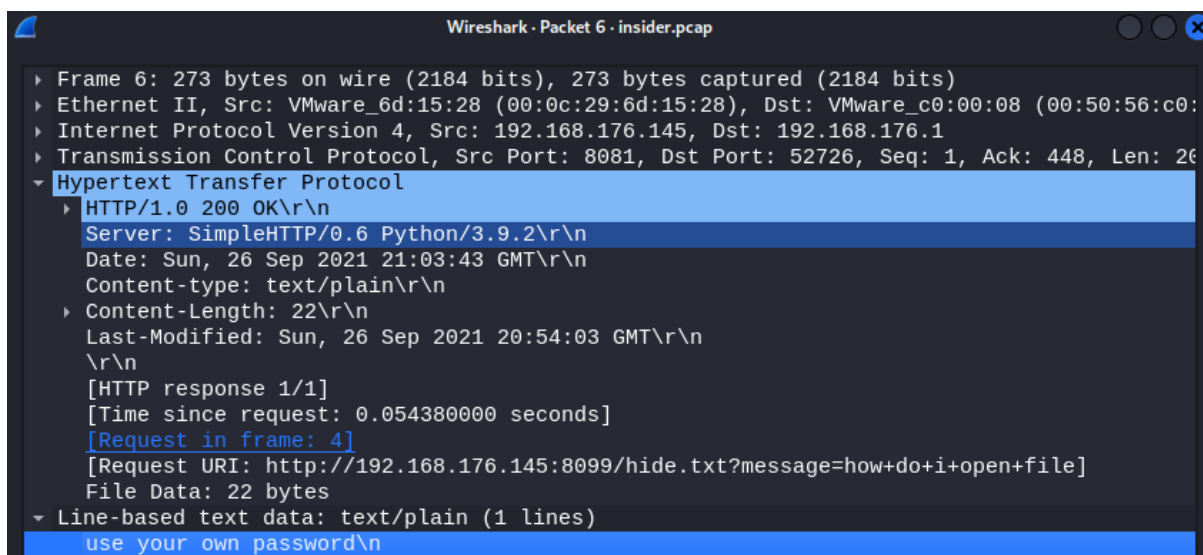


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.176.1	192.168.176.145	TCP	74	52726 → 8081 [SYN] Seq=0 Win=64240 Len=0
2	0.000309	192.168.176.145	192.168.176.1	TCP	74	8081 → 52726 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
3	0.000349	192.168.176.1	192.168.176.145	TCP	66	52726 → 8081 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.000457	192.168.176.1	192.168.176.145	HTTP	513	GET http://192.168.176.145:8081/hidden.txt
5	0.000948	192.168.176.145	192.168.176.1	TCP	66	8081 → 52726 [ACK] Seq=1 Ack=448 Win=64240 Len=0
6	0.054837	192.168.176.145	192.168.176.1	HTTP	273	HTTP/1.0 200 OK (text/plain)
7	0.054866	192.168.176.1	192.168.176.145	TCP	66	52726 → 8081 [ACK] Seq=448 Ack=208 Win=64240 Len=0
8	0.054997	192.168.176.145	192.168.176.1	TCP	66	8081 → 52726 [FIN, ACK] Seq=208 Ack=448 Win=0 Len=0
9	0.056952	192.168.176.1	192.168.176.145	TCP	66	52726 → 8081 [FIN, ACK] Seq=448 Ack=208 Win=0 Len=0
10	0.057190	192.168.176.145	192.168.176.1	TCP	66	8081 → 52726 [ACK] Seq=209 Ack=449 Win=0 Len=0

- As theorised in the “Initial Thoughts” section above, the pcap contains HTTP/TCP traffic.
- Frames 4 and 6 immediately stand out due to HTTP traffic being a cleartext protocol, reviewing them each in detail reveals:

A screenshot of the Wireshark interface showing packet 4. The packet list on the left shows 'Frame 4: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits)'. The packet details pane on the right shows the following structure: Ethernet II (Src: VMware\_c0:00:08, Dst: VMware\_6d:15:28), Internet Protocol Version 4 (Src: 192.168.176.1, Dst: 192.168.176.145), Transmission Control Protocol (Src Port: 52726, Dst Port: 8081, Seq: 1, Ack: 1, Len: 447), and Hypertext Transfer Protocol. The HTTP details show a GET request for 'http://192.168.176.145:8099/hide.txt?message=how+do+i+open+file' with various headers including Host, User-Agent (Mozilla/5.0), Accept, Authorization (Basic ZmFrZWJsdWU6cmVkJm9yZXZlcg==), Accept-Language, Accept-Encoding, Connection, and Upgrade-Insecure-Requests. The status bar at the bottom indicates '[Full request URI: http://192.168.176.145:8099/hide.txt?message=how+do+i+open+file]', '[HTTP request 1/1]', and '[Response in frame: 6]'.

```
Wireshark - Packet 4 - insider.pcap
Frame 4: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits)
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_6d:15:28 (00:0c:29:6d:15:28)
Internet Protocol Version 4, Src: 192.168.176.1, Dst: 192.168.176.145
Transmission Control Protocol, Src Port: 52726, Dst Port: 8081, Seq: 1, Ack: 1, Len: 447
Hypertext Transfer Protocol
  GET http://192.168.176.145:8099/hide.txt?message=how+do+i+open+file HTTP/1.1\r\n
  Host: 192.168.176.145:8099\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefox/92.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  Authorization: Basic ZmFrZWJsdWU6cmVkJm9yZXZlcg==\r\n
  Credentials: fakeblue:redforever\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: close\r\n
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Full request URI: http://192.168.176.145:8099/hide.txt?message=how+do+i+open+file]
  [HTTP request 1/1]
  [Response in frame: 6]
```

A screenshot of the Wireshark interface showing packet 6. The packet list on the left shows 'Frame 6: 273 bytes on wire (2184 bits), 273 bytes captured (2184 bits)'. The packet details pane on the right shows the following structure: Ethernet II (Src: VMware\_6d:15:28, Dst: VMware\_c0:00:08), Internet Protocol Version 4 (Src: 192.168.176.145, Dst: 192.168.176.1), Transmission Control Protocol (Src Port: 8081, Dst Port: 52726, Seq: 1, Ack: 448, Len: 26), and Hypertext Transfer Protocol. The HTTP details show a '200 OK' response with headers: Server (SimpleHTTP/0.6 Python/3.9.2), Date (Sun, 26 Sep 2021 21:03:43 GMT), Content-type (text/plain), Content-Length (22), and Last-Modified (Sun, 26 Sep 2021 20:54:03 GMT). The status bar at the bottom indicates '[HTTP response 1/1]', '[Time since request: 0.054380000 seconds]', '[Request in frame: 4]', '[Request URI: http://192.168.176.145:8099/hide.txt?message=how+do+i+open+file]', and 'File Data: 22 bytes'. The packet bytes pane at the bottom shows the text 'use your own password'.

```
Wireshark - Packet 6 - insider.pcap
Frame 6: 273 bytes on wire (2184 bits), 273 bytes captured (2184 bits)
Ethernet II, Src: VMware_6d:15:28 (00:0c:29:6d:15:28), Dst: VMware_c0:00:08 (00:50:56:c0:00:08)
Internet Protocol Version 4, Src: 192.168.176.145, Dst: 192.168.176.1
Transmission Control Protocol, Src Port: 8081, Dst Port: 52726, Seq: 1, Ack: 448, Len: 26
Hypertext Transfer Protocol
  HTTP/1.0 200 OK\r\n
  Server: SimpleHTTP/0.6 Python/3.9.2\r\n
  Date: Sun, 26 Sep 2021 21:03:43 GMT\r\n
  Content-type: text/plain\r\n
  Content-Length: 22\r\n
  Last-Modified: Sun, 26 Sep 2021 20:54:03 GMT\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.054380000 seconds]
  [Request in frame: 4]
  [Request URI: http://192.168.176.145:8099/hide.txt?message=how+do+i+open+file]
  File Data: 22 bytes
  Line-based text data: text/plain (1 lines)
  use your own password
```

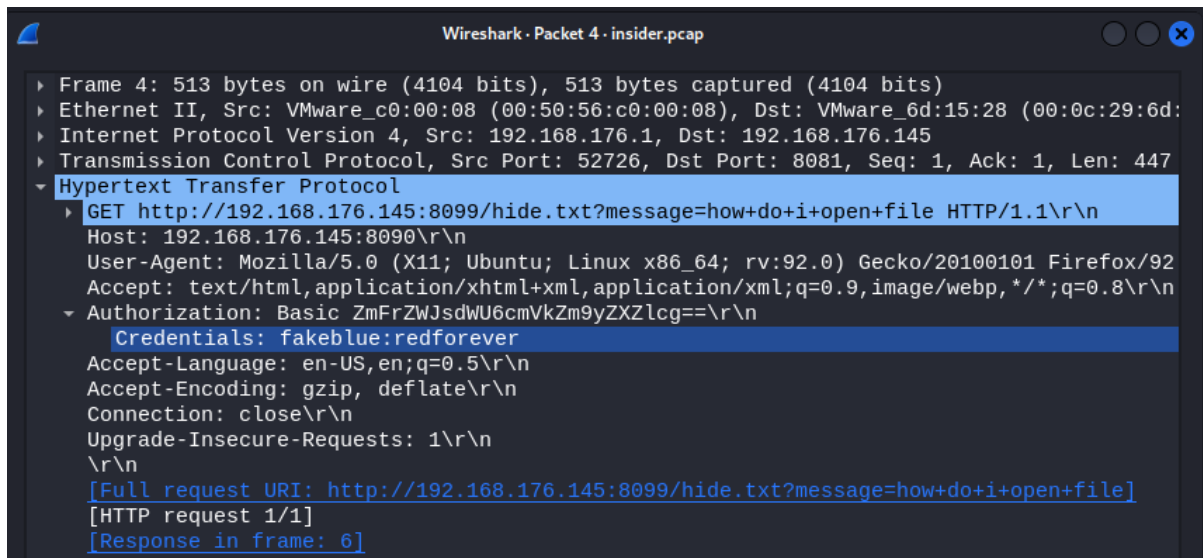
- Frame 4:
  - Src\_ip = 192.168.176.1, src\_port = 8099
  - Dst-IP = 192.168.176.145, dst\_port = 8081
  - Requesting a file called hide.txt passing it a “message” parameter with value “how do I open file”
  - Authorisation credentials are fakeblue:redforever
    - In the format user:pass
- Frame 6:
  - Src\_ip = 192.168.176.145, src\_port = 8081
  - Dst\_ip = 192.168.176.1, dst\_port = 52576
  - Server responding is SimpleHTTP v0.6 using Python3.9.2
  - Text/data returned is “use your own password”

After analysing the communications, we can see that the server response contains the answer which is “use your own password”.

## What is the password of the ZIP file?

- Answer: redforever

Due to our analysis for the previous question, we've already analysed the conversation that contains the answer. As seen in frame 4:



Authorisation credentials submitted are fakeblue:redforever, in the format user:pass

## Will more passwords be required?

- Answer: No

Using the password “redforever”, we can unzip “file.zip”:

```
(kali㉿kali)-[~/Documents/BTLO/Challenges/Shiba_Insider]
$ ls -l
total 72
-rw-r--r-- 1 kali kali 66759 Oct  8  2021 file.zip
-rw-r--r-- 1 kali kali  1514 Oct  8  2021 insider.pcap

(kali㉿kali)-[~/Documents/BTLO/Challenges/Shiba_Insider]
$ unzip file.zip
Archive:  file.zip
[file.zip] ssdog1.jpeg password:
  inflating: ssdog1.jpeg
  inflating: README.txt

(kali㉿kali)-[~/Documents/BTLO/Challenges/Shiba_Insider]
$ ls -l
total 160
-rw-r--r-- 1 kali kali 66759 Oct  8  2021 file.zip
-rw-r--r-- 1 kali kali  1514 Oct  8  2021 insider.pcap
-rw-rw-r-- 1 kali kali    86 Sep 26  2021 README.txt
-rw-rw-r-- 1 kali kali 84417 Sep 26  2021 ssdog1.jpeg

(kali㉿kali)-[~/Documents/BTLO/Challenges/Shiba_Insider]
$ |
```

By using cat on the README.txt, we find out that no more passwords are required:

```
(kali㉿kali)-[~/Documents/BTLO/Challenges/Shiba_Insider]
$ cat README.txt
Shiba Dog has everything you need and decided that no more passwords will be needed

(kali㉿kali)-[~/Documents/BTLO/Challenges/Shiba_Insider]
$ |
```

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

- Answer: Exiftool

No analysis needed, when analysing files or metadata exiftool is often a go to.

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

- Answer: Technique:Steganography

Running Exiftool on the JPG reveals the following:

```
(kali㉿kali)-[~/Documents/BTLO/Challenges/Shiba_Insider]
$ exiftool ssdog1.jpeg
ExifTool Version Number      : 12.67
File Name                    : ssdog1.jpeg
Directory                    : .
File Size                     : 84 kB
File Modification Date/Time   : 2021:09:26 21:07:52+01:00
File Access Date/Time        : 2021:09:26 21:07:57+01:00
File Inode Change Date/Time   : 2023:12:06 14:29:05+00:00
File Permissions              : -rw-rw-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
```

After reviewing, there are two line that standout which are “Technique” and “Technique Command”. Steganography involves hiding data within digital files such as images, audio, video, or text documents. It typically utilises small, imperceptible changes to the least significant bits (LSBs) of the cover media to embed the secret data.

Therefore, as this is suspicious, we can confirm the answer.

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

- Answer: Steghide

No analysis needed, Steghide is a popular tool to analyse files that utilise Steganography techniques.

Enter the ID retrieved.

- Answer: 0726ba878ea47de571777a

Install steghide if not already installed:

```
(kali@kali)-[~/Documents/BTLO/Challenges/Shiba_Insider]
$ sudo apt install steghide
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
steghide is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

(kali@kali)-[~/Documents/BTLO/Challenges/Shiba_Insider]
$ steghide extract -sf ssdog1.jpeg
Enter passphrase:
wrote extracted data to "idInsider.txt".

(kali@kali)-[~/Documents/BTLO/Challenges/Shiba_Insider]
$ cat idInsider.txt
0726ba878ea47de571777a
```

Command above is as follows:

- Steghdie – the name of the tool
- Extract – tells steghide we want to extract information
- -sf – tells steghide we want to extract information from a file
- Ssdog1.jpeg – the name of the file to extract information from

At the password prompt, I first tried “redforever” with no luck, and after double checking to see if I had missed another password (which I hadn’t), I tried no password and bingo:

- ID – 0726ba878ea47de571777a

What is the profile name of the attacker?

- Answer: bluetiger

Append the id extracted previously to [blueteamlabs.online/home/user/\[idHere\]](https://blueteamlabs.online/home/user/[idHere]), giving us our answer as seen on the following page:

BTLO


https://blueteamlabs.online/home/user/0726ba878ea47de571777a

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Blue Team Labs Online v.420.99

Home Investigations PRO FREE Challenges FREE Leaderboard BECOME PRO!

Collectibles



**bluetiger**  
Rank: Initiate

1679965	10	0	1
Global Position	Country Position	Points	Investigations Challenges