# Lab – CTF Walkthrough for HA: Forensics Flag #2

## Overview

In this second lab, you will be tasked with capturing flag #2 for this CTF.

## Lab Requirements

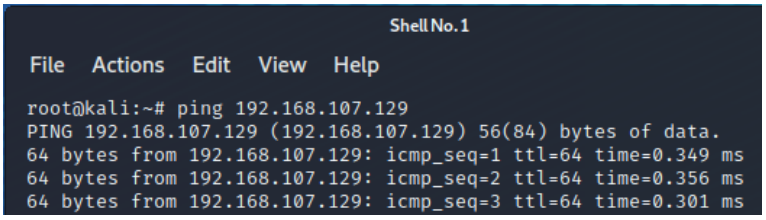
This lab requires the use of VMware Workstation Player. The forensic target was built using VMware, and though it is an OVA file, it will not acquire an IP address using DHCP when imported into VirtualBox.

- Install of **VMware Workstation Player**
- Once virtual install of **Kali Linux for VMWare**.
- The OVA image file for HA: Forensics Target downloaded from **Vulnhub**

## Begin the Lab!

Let us begin by ensuring we still have network connectivity with our target. I opened a terminal, and at the prompt, I type ping followed by my target machine's IP address.

```
ping 192.168.107.129
```



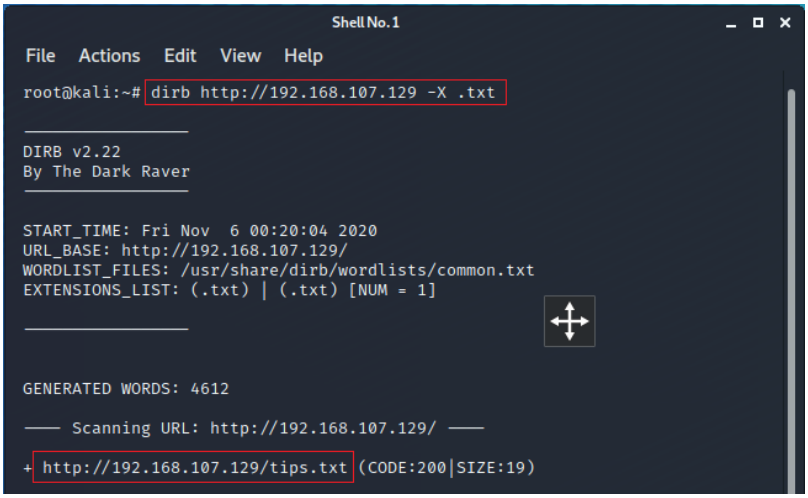

To stop the ping request, press the Ctrl+C key combination on your keyboard.

Clear your terminal.

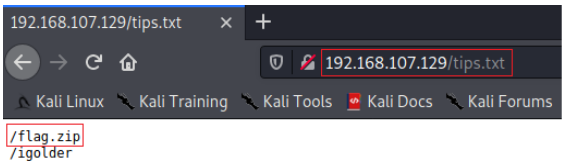
We will use **dirb** to search for any text files that might help point us in the right direction.

At the terminal, I have typed the following command. The -X is the extension filter, followed by what extension to look for.

```
dirb http://192.168.107.129 -X .txt
```

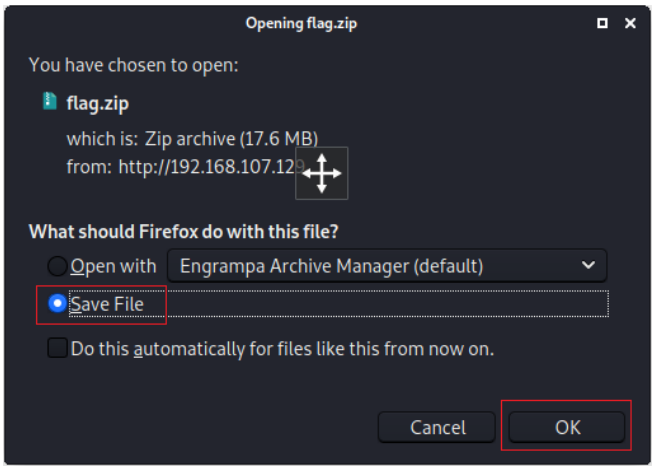



From where the file is located, it appears to be something like a robots.txt file. Let open a browser and browse to the file location. We have a flag.zip file.

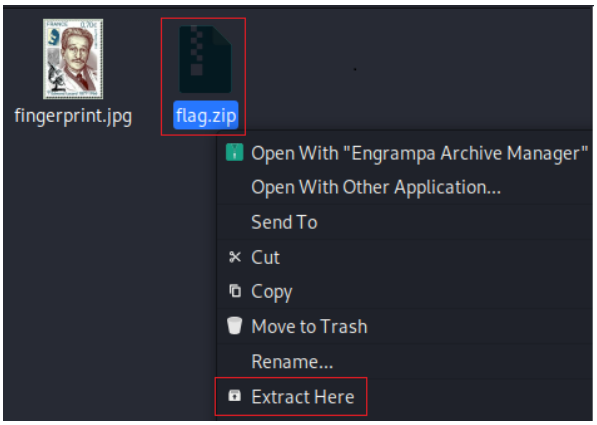


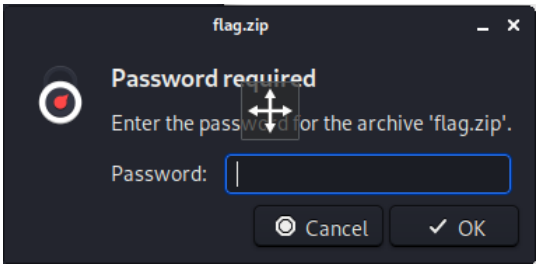

We need first to download the zip file. In the address bar, at the prompt, type in the IP address of your target, followed by the name of the file we want to download.
**http://192.168.107.129/flag.zip**

You are given the option to save the file. The file will be saved to your Download directory.

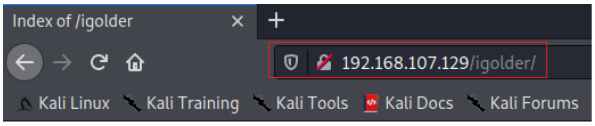



From your browser, open the download location, find the zip file, and attempt to extract the contents. We are prompted for a password.



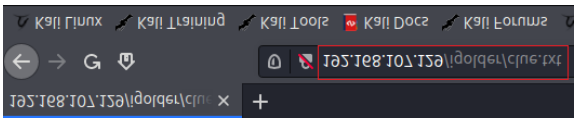

Return to your browser and attempt to open the folder labeled **`/igolder`**. Inside the directory, we find a clue.txt file. Open it.



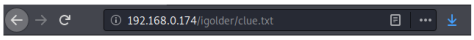

# Index of /igolder

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| clue.txt | 2020-09-24 07:42 | 2.4K | |

*Apache/2.4.29 (Ubuntu) Server at 192.168.107.129 Port 80*



The text file contains a PGP private key followed by an encrypted message.



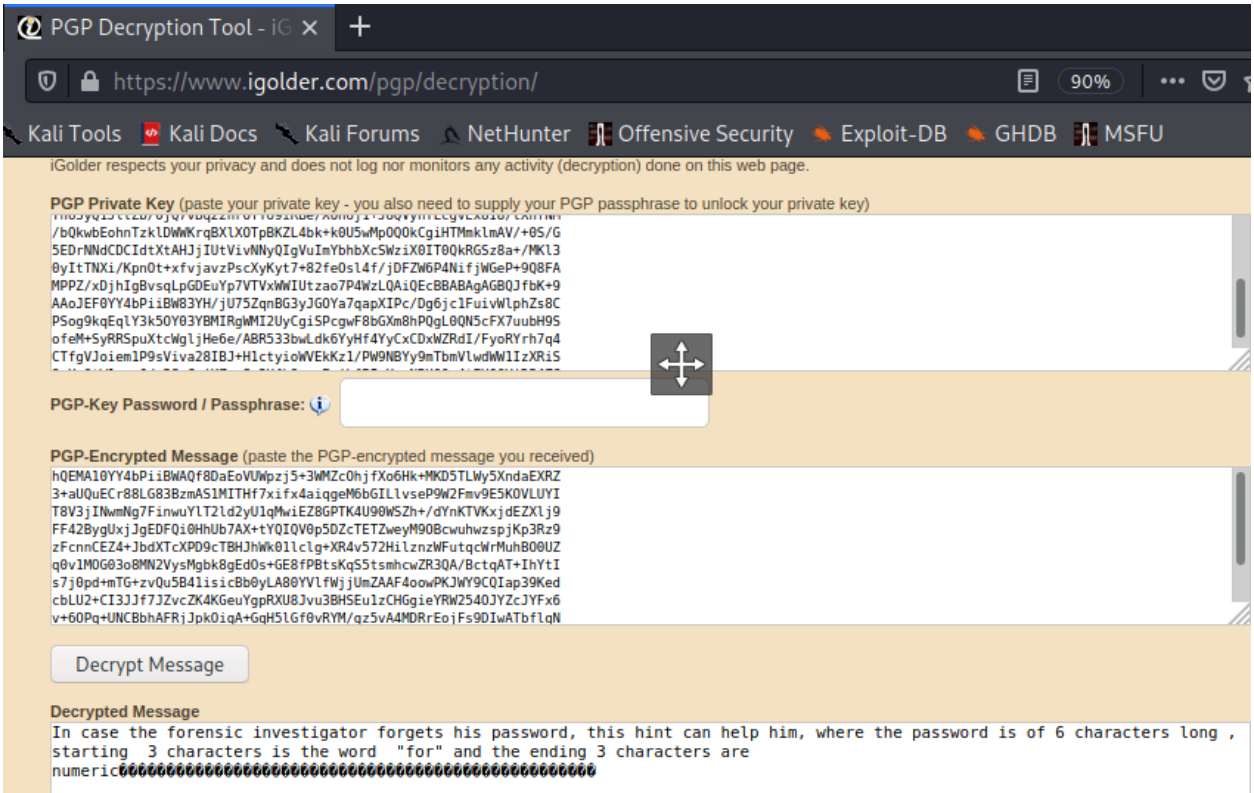


```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: BCPG C# v1.6.1.0

lQOsBF9sr70BCACvH5Vs2Lp9nyVIbVk4yraUmxDBxPJNitlU/IqcR2d+UDEORbDl
UClLXSqapjBFuu2Ap86SIcv/1VktRh79lnL5j4uKSAEuI/t6SJW4hlfovVBndUvT
X6Iw6TRJlLq5AsLOS38PWpIgL1ECIqliwNfCjjlvQd8xm/C9BV1lqM71JYtW34ST
XsKzxomVqGtWvrzs/tFege20z12JtqgPmqGApXzNjI4y7iH0vvVS8nCF58nwyjoH
wbx6EXk002hDe0/W7tsCGhp3gU5wzkUy4kfBfVrLp0/23kA/k4iJvlMPMAeQoJPx
AymXmXEKlp+igBrBicBw68SZgLAQhg8ZO2ybABEBAAH/AwMC/MDF76NvTu1gM8Y7
xjKap2L3OY8xeOoAeMQUueabuTPZrl7jB6YfsEcQj4xDjz05BXIQxP0PziHpXTk3
v5FlH5nhSWZI6OgN0HF6rdjByKT4CNlkt7IVIPEQc7IidQP5K1/YhbghysyYHyBH
3TRAEwJszcjj6TsAOM1mpLXlPweM1sC3ms8xoFVSipPcHviNcQq58zLpGcWvmmuc
ZfqrR8qfpU/wZEmEvcDW1FOCvq/BqoIpsPOXYfI+ul7C0ML0bmzi/u2p7EJLwf2E
tGBJ++wLdProHJHovp0WlQSHFamOWmM5p9SAq7lMegvIn3NHe0ZQS2agjBzNiMW5
LK/dZ01lIX1SSRNNOlLC+Tf/v6bS8gAD+WSGsYEITPcRP2OpCiCBoa4dTGsK7nyF
RHIngmJrp5g1agayG92ahUFRLqQ7KGa+hu3N8/pM+x/dNH1Uw/jhKHsacpgBBCPf
Zs/NZlcMbCI0TD6CFKe2QCEnOW6iLlOEgV2ptEPJLkinaFZ8BEf5HYHUhW1CqwTZ
otvsmzkijYDvaV77zylVqb9gMJelVNWLZG3fcw+eCGF1w0Bxno99xcxEgJpzdOeH
TnU3yQ1JlIZb/0jQ7vBqz2hrOTYo9iRBe/XOnUjl+J8QVynYLcgvExBIB/tXofNM
/bQKwbEohnTzklDWWKrqBXlXOTpBKZL4bk+k0U5wMpOQOkCgiHTMmklmAV/+05/G
5EDrNNdCDCIdtXtAHJjIUtVivNNyQIgVuImYbhbXcSWziX0IT0QkRGSz8a+/MKl3
0yItTNXi/KpnOt+xfvjavzPscXyKyt7+82feOsl4f/jDFZW6P4NifjWGeP+9Q8FA
MPPZ/xDjhIgBvsqLpGOEuYp7VTVxWWIUtzao7P4WzLQAiQEcBBABAgAGBQJfbK+9
AAoJEF0YY4bPiiBWB3YH/jU75ZqnBG3y3GOYa7qapXIPc/Dg6jc1FuivWlphZs8C
PSog9kqEqlY3k5OY03YBMIRgWMI2UyCgiSPcgwF8bGXm8hPQgL0QN5cFX7uubH9S
ofeM+SyRRSpuXtcWgljHe6e/ABR533bwLdk6YyHf4YyCxCDxWZRdI/FyoRYrh7q4
CTfgVJoiem1P9sViva28IBJ+H1ctyloWVEkKz1/PW9NBYy9mTbmVlwdWW1IzXRiS
OcXu0tW1rawJ/z55wCwjKZvvSm2Hfk9eguEojbfPIoXauNRH00u4tEHO6YjD54ZC
DxpZfSHSCsOWEfOAA5EO+uDGSY4+WB6ihKmCV+I6BJc=
=KoPg
-----END PGP PRIVATE KEY BLOCK-----
```

```
-----BEGIN PGP MESSAGE-----
Version: BCPG C# v1.6.1.0

hQEMA10YY4bPiiBWAQf8DaEoVUWpzj5+3WMZcOhjfXo6Hk+MKD5TLWy5XndaEXRZ
3+aUQuECr88LG83BzmAS1MITHf7xifx4aiqgeM6bGILlvseP9W2Fmv9E5KOVLUYI
T8V3jINwmNg7FinwuYlT2ld2yU1qMwiEZ8GPTK4U90WSZh+/dYnKTVKxjdEZXlj9
FF42BygUxjJgEDFQi0HhUb7AX+tYQIQV0p5DZcTETZweyM9OBcwuhwzspjKp3Rz9
zFcnnCEZ4+JbdXTcXPD9cTBHJhWk0llclg+XR4v572HilznzWFutqcWrMuhBO0UZ
q0v1MXG83o8MN2VysMqbk8gEdOs+G8fPBtsKqS5tsmhcwZR3QA/BctqAT+IhYtI
s7j0pd+mTG+zvQu5B4lisicBb0yLA80YVlfWjjUmZAAF4oowPKJWY9CQIap39Ked
cbLU2+CI3JJf7JZvcZK4KGeuYgpRXU8Jvu3BHSEu1zCHGgieYRW2540JYZcJYFx6
v+6OPq+UNCBbhAFRjJpkOigA+GgH5lGf0vRYM/gz5vA4MDRrEojFs9DIwATbflqN
QOs=
=Y9OD
-----END PGP MESSAGE-----
```

To decrypt the message, we need the passphrase. To do this, we visit the igolder.com PGP decryption page. **`https://www.igolder.com/pgp/decryption/`**

In the first box, we copy and paste the key. In the second box, we copy and paste the encrypted message. To view the decrypted message, we tell the program to decrypt the message.

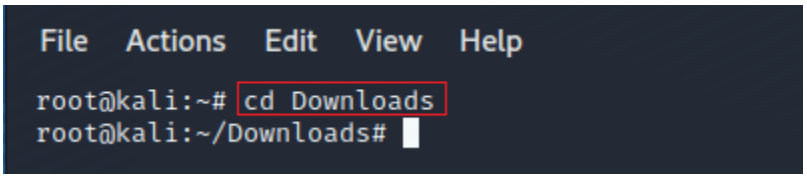



We are given a password hint. The first three characters of the password are the word ‘for,’ and the three remaining characters are numeric.

We next need to generate a dictionary file that will allow us to crack the password-protected zip file we downloaded earlier.

Open a terminal, and at the prompt, change location over to your Downloads directory.

**`cd Downloads`**




We can use crunch to create our dictionary file based on the information we learned from the password hint.

At the prompt, type the following command. **`crunch 6 6 -t for%%% -o dict.txt`**

Press enter.

```
File  Actions  Edit  View  Help

root@kali:~# cd Downloads
root@kali:~/Downloads# crunch 6 6 -t for%%% -o dict.txt
Crunch will now generate the following amount of data: 7000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1000

crunch: 100% completed generating output
root@kali:~/Downloads#
```

The dictionary.txt file was saved to the Downloads folder. We next need to use a zip file password cracking utility called fcrackzip.

If your install of Kali does not have fcrackzip, you can download it using the following command.

**apt-get install fcrackzip**

If you get a download error stating the package could not be found, ensure you have Internet access, and if that is not the issue, you will need to update your source.list with the correct address for the right repository.

Follow the directions using this information posted on this site.

**https://www.cyberpratibha.com/blog/add-kali-linux-repository/**

Once you have updated your scource.list, you need to perform a kali update and kali upgrade. Once both have been completed, you should now be able to download and install fcrackzip using the following command.

**apt-get install fcrackzip**

Welcome to open source!

Once we have fcrackzip installed, we can type in fcrackzip -h to view the help menu. This will help you decypher the command options used to crack the password for our glag.zip file.

```
Shell No.1
File  Actions  Edit  View  Help

crunch: 100% completed generating output
root@kali:~/Downloads# fcrackzip -h

fcrackzip version 1.0, a fast/free zip password cracker
written by Marc Lehmann <pcg@goof.com> You can find more info on
http://www.goof.com/pcg/marc/

USAGE: fcrackzip
          [-b|--brute-force]            use brute force algorithm
          [-D|--dictionary]             use a dictionary
          [-B|--benchmark]              execute a small benchmark
          [-c|--charset characterset]   use characters from charset
          [-h|--help]                   show this message
          [--version]                   show the version of this program
          [-V|--validate]               sanity-check the algorithm
          [-v|--verbose]                be more verbose
          [-p|--init-password string]   use string as initial password/file
          [-l|--length min-max]         check password with length min to m
ax
          [-u|--use-unzip]              use unzip to weed out wrong passwor
ds
          [-m|--method num]             use method number "num" (see below)
          [-2|--modulo r/m]             only calculate 1/m of the password
          file ...                    the zipfiles to crack

methods compiled in (* = default):
```

From our terminal prompt, type in the following command.

```
fcrackzip -u -D -p dict.txt flag.zip
```

We hit enter, and it immediately finds the password, which is for007.

```
File  Actions  Edit  View  Help

root@kali:~# cd Downloads
root@kali:~/Downloads# fcrackzip -u -D -p dict.txt flag.zip


PASSWORD FOUND!!!!: pw == for007
root@kali:~/Downloads#
```

Next, we need to extract the contents of the zip file. To do this at the prompt, type the following command.

**`unzip flag.zip`**

We are prompted for the password.

We are shown two files. One is the flag.pdf file, and the other is a DMP (dump) file we will come back to later.

```
File  Actions  Edit  View  Help

root@kali:~/Downloads# unzip flag.zip
Archive:  flag.zip
[flag.zip] flag.pdf password:
  inflating: flag.pdf
  inflating: lsass.DMP
root@kali:~/Downloads#
```

Use the shortcut on your desktop to visit the Downloads directory. Find the flag.pdf file, and x2 click it. This is your second flag for this CTF challenge.

End of the lab!

You are now ready to move on with capturing flag #3.