**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**

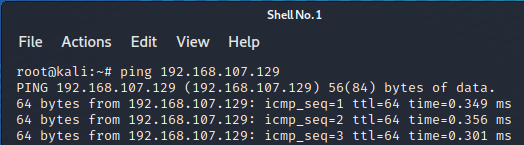
This lab requires the use of VMware Workstation Player. The forensic target was built using VMware, and though it is an OVA file, it will not acquire an IP address using DHCP when imported into VirtualBox.

* Install of [**VMware Workstation Player**](https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html)
* Once virtual install of [**Kali Linux for VMWare**](https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/).
* The OVA image file for HA: Forensics Target downloaded from [**Vulnhub**](https://download.vulnhub.com/ha/forensics.ova)

**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**

****

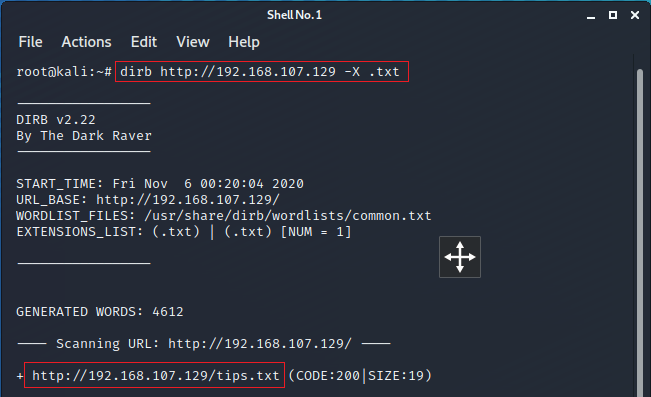
To stop the ping request, press the Ctrl+C key combination on your keyboard.

Clear your terminal.

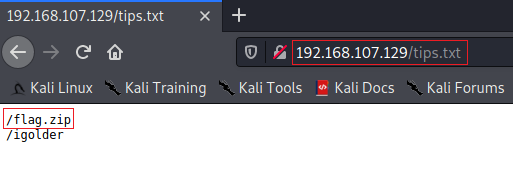
We will use **dirb** to search for any text files that might help point us in the right direction.

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**

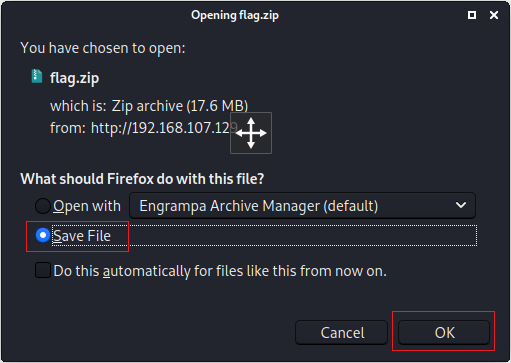
****

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.

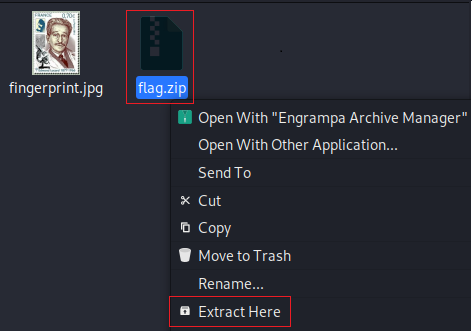
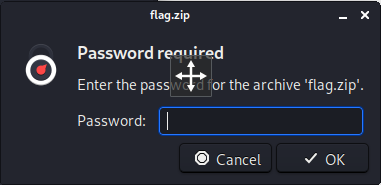


We need first to download the zip file. In the address bar, at the prompt, type in the IP address of your target, followed by the name of the file we want to download. [**http://192.168.107.129/flag.zip**](http://192.168.107.129/flag.zip)

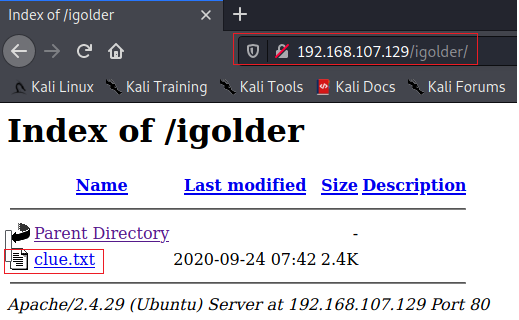
You are given the option to save the file. The file will be saved to your Download directory.

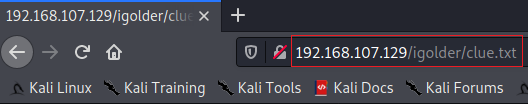


From your browser, open the download location, find the zip file, and attempt to extract the contents. We are prompted for a password.



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



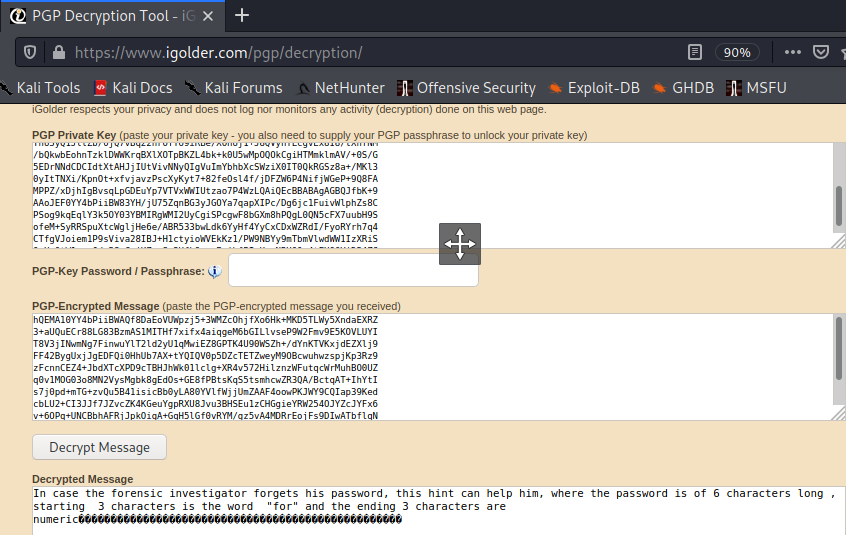


The text file contains a PGP private key followed by an encrypted message.



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.

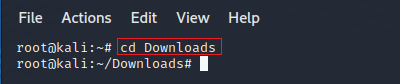


We are given a password hint. The first three characters of the password are the word ‘for,’ and the three remaining characters are numeric.

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.

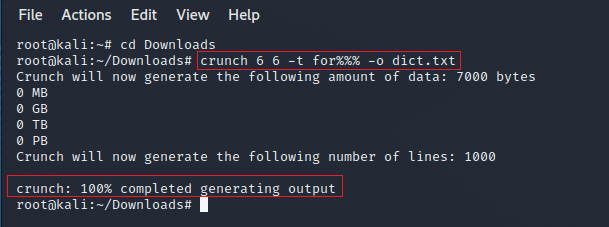
**cd Downloads**



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.



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.

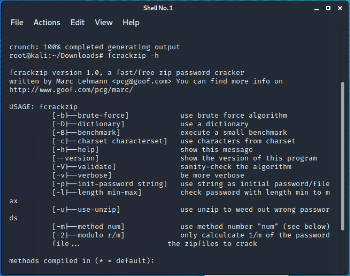
**https://www.cyberpratibha.com/blog/add-kali-linux-repository/**

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!

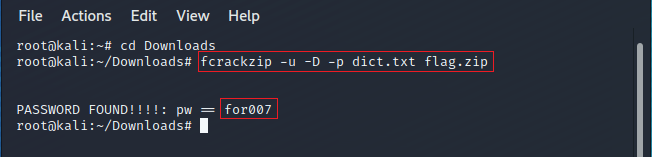
Once we have fcrackzip installed, we can type in fcrackzip -h to view the help menu. This will help you decypher the command options used to crack the password for our glag.zip file.



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.

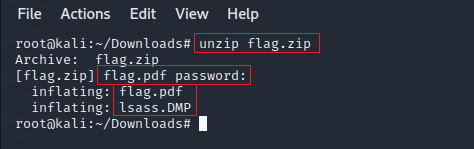


Next, we need to extract the contents of the zip file. To do this at the prompt, type the following command.

**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.



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.