# Lab 01 - Introduction

## Objectives

- Simple CTF tasks
- Introduction to Python scripting
- Introduction to basic security-related tools

## Useful Tools

- man
- find
- base64
- hexedit
- Binwalk
- john, zip2john
- xxd
- gzip, bzip2, tar

## Preparation

You may use the UPB's OpenStack cloud to spawn a Virtual Machine to be used for this lab! Read this guide.

Download the task archive for this section. Each exercise will have a corresponding folder.

## Python Warmup

### 01. Decode 'til You Drop

- One of your friends gave you this string which looks encoded… Figure out what encoding was used and decode it. Be patient, it may take a couple of decoding rounds :)

### 02. Zip it good

- The archive contains the flag. What is the password?
    - **Hint:** the password is in the wordlist

## CTF tasks

### 03. Find the impostor

- The flag for this exercise is found in a file under the inhere directory. The file has the following properties:
    - human-readable
    - 987 bytes in size
    - not executable

### 04. Unknown File Type

- We've found this file on a confiscated machine, but we can't figure what it is. Can you help us?

## 05. Corrupted File

- During a transmission, one of our files got corrupted. Take a look and see if you can do something about it.

Maybe there is something wrong with the header.

- **Hint:** use a hex editor to check the file's header

## 06. Hidden File

- There is something wrong with the size of this image. Is there anything else there?
  - **Hint:** use Binwalk. ”-e” option is buggy sometimes.

## 07. Waiting for eternity

- We stared at this gif for the last hour but nothing is happening. Would you like to join us and stare at it for the next hour?

## 08. The great file squeeze

- You are being given a file which is a hexdump of the flag that has been repeatedly compressed. Reverse the process and get the flag :)
  - **Hint:** hexdump, man

## 09 [bonus]. Web Fuzzer

- Start this task by opening a specific docker container on your VM:

```
docker run -d -p 8080:80 ghcr.io/cs-pub-ro/isc-lab-intro-web
```

- You can now access a webserver on local port 8080 (try it with `curl localhost:8080`). Your task is to retrieve the hidden flag by trying all web paths inside the given wordlist (write your own fuzzer in Python, check the lab archive for resources!).
  - *Hint*: use the Python requests [https://requests.readthedocs.io/en/latest/] library to issue web requests! Check their HTTP status code to know when you successfully found an existing web file ;)

# Feedback

Please take a minute to fill in the feedback form [https://forms.gle/BugCwG6GNkdq5DTg7] for this lab.

isc/labs/01.txt · Last modified: 2024/10/07 08:29 (external edit)