Lab 01 - Introduction

Objectives

- Simple CTF tasks
- Introduction to basic security-related tools
- Simple program compiling tools
- Basics of networking related monitoring tools

Preparation

You may use the UPB's OpenStack cloud to instantiate a Virtual Machine [https://cloud.grid.pub.ro] to be used for this lab! Read these instructions if you wanna know how!.

CTF local tasks

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

01. [10p]B64 encoding

- The flag is in b64.txt. It should look something like this: **FLAG{...}**.
    - **Hint:** python3, base64

02. [10p]EXIF

- The flag is hidden somewhere within this image. Remember its format.
    - **Hint:** it's not steganography; don't look at the pixels

03. [10p]From Manchester with love

- Remember RL? Remember Manchester [https://en.wikipedia.org/wiki/Manchester_code#Encoding]?

04. [10p]Corrupted file

- The header seems to be damaged…

Up for more?

- CTFlearn [https://ctflearn.com]
- OverTheWire [https://overthewire.org/wargames/]
- Cryptopals Challenges [https://cryptopals.com/]
- PicoCTF [https://picoctf.com/]

OS Management

05. [10p]Web server & console browser

- Install and configure **apache2** and **links**. Use the latter to connect to http://localhost [http://localhost]
    - **Hint:** use the distro specific package manager.

06. [10p]Disk space & usage

- Display the disk space usage for each individual directory (. and .. excluded) in the first two hierarchical levels of */usr/include/* in a human readable format
    - **Hint:** find, du
- Sort the list in ascending order, by size

Program compilation tools

07. [10p]Program compilation

- Download the following program [https://curl.haxx.se/libcurl/c/simple.html] and compile it using **gcc**.
- What is the program intended for?
- Modify the program such that it connects to “http://localhost [http://localhost]” (i.e. your local apache server) and prints the response (apache's default HTML test page) to stdout, just like standard curl.
    - **Hint:** you need to install libcurl's development libraries.
    - **Hint:** you need some flags for the compiler to know where libcurl is installed (see library's documentation [https://curl.haxx.se/libcurl/c/libcurl-tutorial.html])

08. [10p]Static compilation

- Statically compile the program (but keep a copy of the old, shared executable).
    - **Hint:** curl-config --static-libs
    - **Hint:** Note that you'll need even more development libraries: libidn11-dev librtmp-dev libssl-dev libcrypto++-dev libkrb5-dev libldap2-dev libnghttp2-dev libpsl-dev libssh-dev libzstd-dev libbrotli-dev
    - **Hint:** Getting a pthread-related linker error? Try *-lpthread* at the end of the gcc command!
- Check the size difference. What does it mean?
    - **Hint:** ldd
- Uninstall libcurl and see which of the executables successfully run now!
- Reinstall curl again if you need it ;)

Networking related tools

09. [10p]Traffic sniffing

- Use the tcpdump suite to save all the traffic from interface ens3/eth0 to a file.
    - **Hint:** Tcpdump may complain that it has no privileges to write the log file. Use ”-Z student” (man!) to reacquire them.

Feedback

11. [10p]Feedback

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