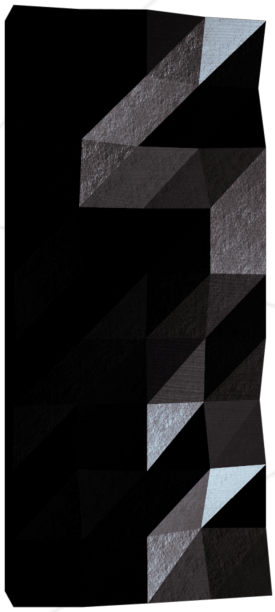


Snow Crash

A security project

42 Staff pedago@42.fr

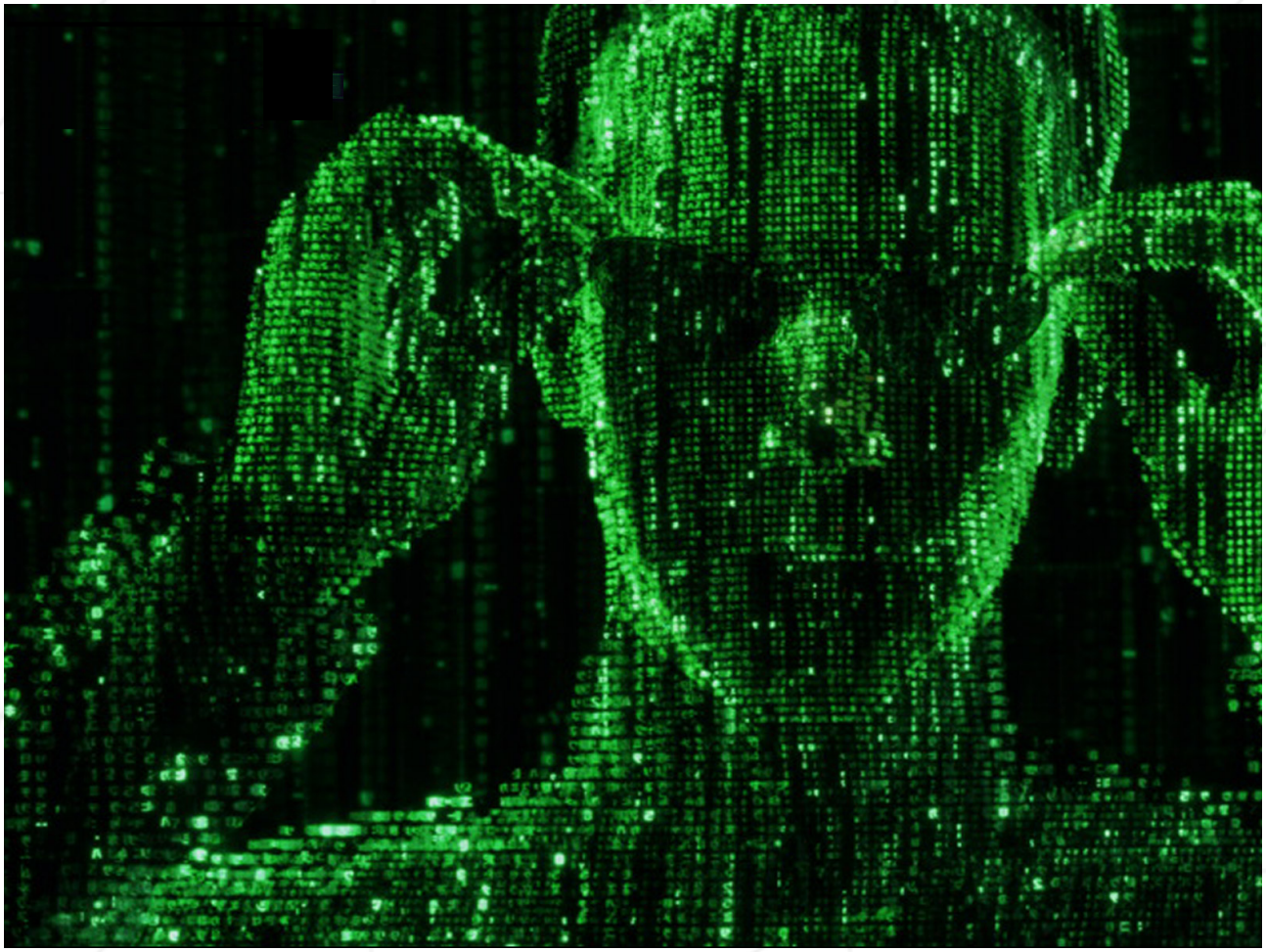
Summary: This project will be an introduction to cyber security.

Version: 3.2

Contents

Chapter I

Foreword



There is something wrong.

Chapter II

Introduction

As a developer, you may have to work on pieces of software that will be used by hundreds of people in your career.

If your software shows any weaknesses, it will expose the users.

It is your duty to understand the different techniques used to exploit these weaknesses in order to spot them and avoid them.

This project is a modest introduction to the wide world of cyber security. A world where you'll have no margin for errors.

Chapter III

Objectives

This project aims to make you discover, through several little challenges, cyber security in various fields.

You will use more or less complex methods that will give you a new perspective on IT in general.

You may reach dead ends during this project. You will have to surpass them yourself. You must be the one and only key to the locked doors you will face. This project aims to develop logical thinking you will retain and use in the future. Before asking for help, consider whether you have truly explored all the possibilities.

Chapter IV

General instructions

- This project will be evaluated by humans.
- You may need to demonstrate your results during your evaluation. Be ready to do so.
- To complete this project, you will need to use a 64-bit VM. Once you have started your machine with the ISO provided for this project, if your configuration is correct, you will see a simple prompt with an IP address:

```
  _____                  _____           _
 / ____|                / ____|         | |
| (___  _ __   _____   _| |     _ __ __ _ ___| |__
 \___ \| '_ \ / _ \ \ /\ / / |  | '__/ _` / __| '_ \
 ____) | | | | (_) \ V  V /| |____| | | (_| \__ \ | | |
|_____/|_| |_|\___/ \_/\_/ \_____|_|  \__,_|___/_| |_|

 Good luck & Have fun

    192.168.16.128

  SnowCrash login: _
```

If the IP address is not visible, you can retrieve it using the 'ifconfig' command once you are connected.

- Then, you will be able to register using the following couple of `login:password`: `level00:level00`.

  It is highly recommended to use the SSH connection available on port 4242:

```
$> ssh level00@192.168.16.128 -p 4242
```

- Once logged in, you will need to find the password that will allow you to log in to the "flagXX" account(XX = current level number).

Once logged into the "flagXX" account, execute the 'getflag' command. It will provide you with the password to access the next level. If you are unable to connect to a "flagXX" account, you will need to find an alternative method, such as a command injection on the program, depending on its permissions.

- Here is a session example:

```
level00@SnowCrash:~$ su flag00
Password:
Don't forget to launch getflag!
flag00@SnowCrash:~$ getflag
Check flag.Here is your token: ????????????????
flag00@SnowCrash:~$ su level01
Password:
level01@SnowCrash:~$ _
```

- To assist you with certain levels, you may need to use external software. It is advisable to learn how to use the `scp` command.

/tmp/ and /var/tmp/ folders have limited rights and will be reset from time to time. It is recommended not to work directly on the machine.

- Nothing is left to chance. If a problem arises, consider whether your code might be the cause.

- Of course, in the event of a genuine bug, please contact your local staff.

- You can post your questions on Slack, Discord, or any valid communication system on your campus.

Chapter V

Mandatory part

- Your repository must include everything that assisted you in solving each validated test.

- Your repository will look like this:

```
$> ls -al
[..]
drwxr-xr-x 2 root root 4096 Dec 3 XX:XX level00
drwxr-xr-x 2 root root 4096 Dec 3 XX:XX level01
drwxr-xr-x 2 root root 4096 Dec 3 XX:XX level02
drwxr-xr-x 2 root root 4096 Dec 3 XX:XX level03
[..]
$> ls -alR level00
level00:
total 16
drwxr-xr-x 3 root root 4096 Dec 3 15:22 .
drwxr-xr-x 6 root root 4096 Dec 3 15:20 ..
-rw-r--r-- 1 root root  5 Dec  3 15:22 flag
drwxr-xr-x 2 root root 4096 Dec 3 15:22 resources

level00/resources:
total 8
drwxr-xr-x 2 root root 4096 Dec 3 15:22 .
drwxr-xr-x 3 root root 4096 Dec 3 15:22 ..
-rw-r--r-- 1 root root  0 Dec  3 15:22 whatever.whatever
$> cat level00/flag | cat -e
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX$
$>
```

- You will keep everything you need to prove your results during the evaluation in the resource folder. The `flag` file may be empty; however, you may need to explain why.

WARNING: You must be able to clearly and precisely explain everything that is included in the folder. The folder must not include any binary files.

- If you need to use a specific file that is included on the project's ISO, you must download it during the evaluation. Under no circumstances should you include it

in your repository.

- If you plan to use a specific external software, you must set up a specific environment (VM, docker, Vagrant).
- You are encouraged to create scripts that will assist you, but you must be able to explain them during the evaluation.
- For the mandatory part, you must complete the following list of levels:
  - level00.
  - level01.
  - level02.
  - level03.
  - level04.
  - level05.
  - level06.
  - level07.
  - level08.
  - level09.

Please note that brute forcing the SSH flags is not permitted. This approach would be futile, as you will need to justify your solution during the evaluation.

Chapter VI

Bonus part

Bonus will be taken into account only if the mandatory part is PERFECT. PERFECT meaning it is completed, that its behavior cannot be faulted, even because of the slightest mistake, improper use, etc. Practically, it means that if the mandatory part is not validated, none of the bonus will be taken in consideration.

For the bonus part, you can complete the following list of levels:

- level10
- level11
- level12
- level13
- level14

Chapter VII

Submission and peer-evaluation

Submit your assignment to your `Git` repository as usual. Only the work inside your repository will be evaluated during the defense. Do not hesitate to double-check the names of your folders and files to ensure they are correct.