CIBERSEGURANÇA
CAPTURE THE FLAG CHALLENGE

Since this is a Cyber Security class you probably want to start exercising your recently acquired knowledge. This alternative work allows you to show off your skills. Just select a CTF challenge from bellow, exercise yourself on a number of challenges, select 10 of the most challenging ones you found and write an essay detailing your approach to solve it.

Since this work should be about network security, at least five of the selected challenges should be on networking (forensics for example), and you must obtain more than 1000 points on picoCTF or 150 in HackTheBox.

This work is evaluated by the written report that you should deliver on *moodle*, and a discussion that **you should schedule with the teacher by email** for the first week after the end of classes and where the teacher will assess your report by selecting a random challenge and asking you how did you solve it.

Available CTF running challenges are:

- picoCTF
    - classroom code: CJccEz3dK
      https://play.picoctf.org/classrooms/1012

Network security challenges on picoCTF are for example:

    - Wireshark doo dooo do doo...
    - Wireshark twoo twooo two twoo...
    - shark on wire 1
    - shark on wire 2
    - WPA-ing Out
    - scrambled-bytes
    - Very very very Hidden
    - WebNet0
    - WebNet1
    - Nice netcat...

- Hack The Box
    - Join ISEL university after registering your own user:
      https://app.hackthebox.com/universities/overview/262

Network security challenges on HackTheBox are for example:

    - MarketDump

- Window's Infinity Edge
- Obscure

Useful links:

https://www.kali.org

http://docs.pwntools.com/en/stable/

https://www.hopperapp.com/tutorial.html

https://www.megabeets.net/a-journey-into-radare-2-part-1/

https://urlscan.io/

https://secsy.net/

https://hashcat.net/wiki/doku.php?id=example_hashes

https://gchq.github.io/CyberChef/

https://exifdata.com/

https://md5decrypt.net/en/HashFinder/

https://www.shodan.io/

https://www.exploit-db.com/

WHAT TO INCLUDE ON THE REPORT?

- Detail every process in order to get the flag;
- Screenshots on the process;
- Don't include the easiest ones (unzipping for example);