In this assignment, we'll look at password cracking and vulnerability exploitation with metasploit.

1 - Tools

Please install:

- `metasploit`
- `hashcat`

2 - Tasks

Submit your solution for the following tasks in **Moodle**. The solution should be a ZIP file with a brief report describing your findings and the files created during the execution of these tasks. The report must be in one of the following formats: txt, markdown, or PDF and should be submitted **until the next class date** - 23:59.
For 3 & 4 you can solve them directly tpas-desafios.

1. Perform a zone transfer attack against any of up.pt nameservers (including sub-domains if they exist)
2. Using **ONLY** nc or telnet check if any SMTP server from up.pt is vulnerable any of the misconfigurations (note: **do not use any other tool** than nc or telnet and don't perform automated queries) 💡Hint: some servers require you to initiate authorization first, e.g. `HELO someone`

3. Solve the `Crackstation` challenge on tpas-desafios with `hashcat`. More details are available in the challenge description. Useful links:
   https://hashcat.net/wiki/doku.php?id=mask_attack
   https://hashcat.net/wiki/doku.php?id=example_hashes
   Hint: the password has a reasonable length - less than 10 characters and at least 4

4. Solve the `MSF` challenge on tpas-desafios with `metasploit`.

   - Identify the software running behind Nginx and search for exploits on `msfconsole`.
   - After opening a shell session, run `cat /flag.txt`

5. Special task (optional):

   - Implement the exploit of the `msf` challenge (task 2) in a programming language of your choice (50 points)