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

1 - Tools

Please install:

- `metasploit`

```
$ curl
  https://raw.githubusercontent.com/rapid7/metasploit-omnibus/maste
  r/config/templates/metasploit-framework-wrappers/msfupdate.erb >
  msfinstall && chmod 755 msfinstall && ./msfinstall
```

- `hashcat`

```
$ sudo apt-get install hashcat
```

2 - Tasks

There's no need to send solutions for this assignment, flags should be submitted directly on tpas-desafios, except for the **optional task** for extra points. You can submit the extra task in Moodle:

1. 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

2. 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`

3. Special task (optional):

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