

Labs: Red Team

Pablo Fraile Alonso

Binary Exploitation

TODO: Add the source code, add dockerfile to run? With GDB but custom with good theme, etc.

Reverse Engineering

- 1) TODO: Put my custom binary for reverse-engineering.
- 2) [Get all the code from the hlogedu search package](#): A clue for this, read about [pyinstaller](#)

Machine pwning

TODO: Add machine pwning.

Website audit

- Find as many vulnerabilities as you can of the [owasp juice shop](#). You've the [security report here](#).

Anonymity Online

- 1) Create and configure a Tor hidden service (onion service).
- 2) Configure an onion service to provide SSH access to your device.
- 3) Use **torsocks** to route an application's traffic through the Tor network (via ssh, telnet, etc.), for example when connecting to a friend's laptop.

Wireless

- 1) Use hashcat for breaking this TP-Link wireless network password: TODO

Extra Exercices:

- 1) [Binary Exploitation \(stack\) \(PicoCTF\) \(- Solution\)](#)
- 2) [Binary Exploitation \(heap\) \(PicoCTF\) \(- Solution\)](#)