Writing exploits in Python

What is an exploit?

An **exploit** is a code that takes advantage of some software vulnerabilities or bugs in order to do something not intended by its programmer

Usually it interacts with the target software through the same interface as normal users

3 main scenarios:

- **CLI interface**
- **HTTP API**
- **In-browser interaction**

Interacting: CLI interface

Target software can be executed either locally on the attacker machine or remotely and it uses **stdin** and **stdout** to interact with users

If locally executed we simply use the standard linux terminal simulator, **nc** can be used for remote connections

PROS → Good for initial tests

CONS→ Quite difficult to automate in a script

Interacting: CLI interface

pwntools
python package with lots of utilities to write exploits

Supports both local and remote programs, using the same functions

Makes writing exploits easy, from simple in/out interactions to complex binary exploitation techniques

pip3 install pwntools

GitHub: https://github.com/Gallopsled/pwntools
Docs: https://docs.pwntools.com/en/latest/

Using pwntools

```
1   from pwn import *
2
3   conn = process('./local.exe')
4   conn = remote('chall.it', 3000)
```

process and **remote** open a connection respectively with a local or a remote process and return similar class objects, with the same input and output function utilities

Let's write an exploit to solve a challenge!

nc software-17.challs.olicyber.it 13000