PyPen
Python Penetration Testing Library

Google Summer of Code

Developer

- **Liosis Konstantinos Christos**

Mentors

- **Andreatos Antonios**
- **Karampelas Panagiotis**
- **Pavlatos Christos**

GitHub repository: https://github.com/eellak/gsoc2018-pypen

GSoC link: https://summerofcode.withgoogle.com/projects/#5583642407993344

Google Summer of Code - PyPen

Project objective:

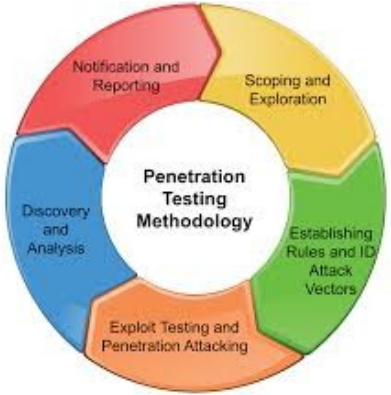
- A basic, easy to use library for tasks such as:
  - user information gathering
  - system information gathering
  - a variety of attack tools.

Python ensures **portability** and **ease of use**, and makes the module capable of either **standalone use** or **easy integration with existing implementations**.

Google Summer of Code - PyPen

Project structure:

- User Reconnaissance
- Target System Reconnaissance
- Attack PenTest Tools



Disclaimer: The purpose of this library is educational, for Penetration Testing and Ethical Hacking purposes and under no circumstances should be used for malicious actions.

Google Summer of Code - PyPen

User Reconnaissance

- Exploitation of possible public user information on Facebook
- Creation of an ad-hoc dictionary that can:
  - Significantly speed up targeted dictionary attack with JohnTheRipper.
- **Possible use case**: Detection of weak employee passwords in a company/ organization.

Google Summer of Code - PyPen

Target System Reconnaissance

Gathering various system information about a possible target can give the pentester plenty of insight on it's vulnerabilities. Information regarding:

- open ports/sockets & pipes
- the Operating System and it's version
- Running processes, etc.

To put our information gathering modules to use, we created a simple client-server model to operate as a "backchannel".

Attack PenTest Tools

In this third and final subsection we try to combine the information retrieved previously with the attack procedure. We can:

- Bruteforce an FTP connection or use a previously created dictionary for password cracking
- Make use of information regarding valuable files and run a ransomware for these
- Use an open port to run a DoS attack by flooding

Google Summer of Code - PyPen

Timeline

The project has been dissected into 3 sections, as mentioned beforehand

- User Reconnaissance has been completed by June 5th;
- Target System Reconnaissance is almost done (at least the core part);
- The rest of our time will be dedicated to implementing the Attack PenTest tools, possible extra features and, of course, testing (on different machines & dedicated server). Individual testing for each completed module has already taken place.

Google Summer of Code - PyPen

Thank you for your time
Good luck to all the participants :D