Python is the most popular scripting language among security researchers due to its broad user community and a large repository of libraries. 3rd party Python libraries allow you to do a lot of things ranging from target scan automation to solve captchas. The pentesters/auditors can use Python to automate their routine tasks, a Red teamer can use Python to craft purpose-built tools for a custom job or even extend the functionality of a Python tool. In other words, knowing Python empowers a security professional to innovate beyond the boundaries of current tools. Hence, knowing how to use Python in an offensive manner (i.e. attacker approach) is a valuable skill.

Prerequisites

- Basic knowledge of computers and networking
- Familiarity with Python or any programming language

What will you learn?

In this section, you will learn to use Python to automate scans/scraping, cracking passwords, analyzing file metadata, creating honeypots and automating interaction-based attacks.

Sub-sections/topics to be covered:

Password Cracking

Password cracking is an important activity of the Pentesting or Red teaming process that allows the pentester/attacker to recover the passwords for protected files that might be of interest. In this section, we have covered the challenges that deal with cracking passwords of encrypted ZIP and PDF files using different Python libraries.

File Metadata

File metadata refers to the information about a file e.g. author name, size, tags etc. This information can be very helpful for an attacker or pentester, especially when the file is corrupted or protected. The challenges in this section deal with extracting PDF metadata and analyzing the PE files.

PCAP Analysis

PCAP Analysis refers to traffic analysis using the stored/captured traffic (packets/frames) in a PCAP file. In this section, we will cover the exercises that deal with analyzing WiFi, HTTP, and VoIP traffic using the scapy and pyshark Python libraries.

Server Attacks

Python libraries developed to interact with remote servers running different services like FTP, HTTP, SSH can be used to launch and automate attacks. In this section, we will cover different types of live servers and interact and attack those servers using Python.

Debugging

Debugging refers to analyzing a running program or binary in order to find and remove bugs.
In this section, we will learn to analyze/debug a binary using the Pygdbmi Python library.

Client Emulation

The python libraries written by people to enable interaction with different services can be used to emulate a client. Such emulated clients can be used for information gathering, monitoring, and even attacking. In this section, we will learn how to use Python libraries to emulate a client.

Server Emulation

A python program with help of respective Python libraries can behave/respond like a server. This kind of code can be modified and deployed as a custom honeypot to lure the attackers. In this section, the labs cover the emulation of SSH, HTTP, and FTP servers. In each lab the user is provided with skeleton code in IDE and terminal access to a Kali machine, the user can run the code to deploy the server and then interact with it using the Kali attacker machine.