

# Course Description



Intermediate cyber security course intended for students seeking to enhance their PT and Python abilities.

This course is offer as the next level course for our unique CHCSS program graduates.

Topics include working with Python, learning to use basic object-oriented programing, working with Python projects, using threads and learning coding conventions.

The second part of the course include topics of gathering cyber intelligence, learn to do penetration testing for both application and infrastructure level, using various exploitation tools and making payloads for attacks. Learn to use tools for various cyber-attacks like Wi-Fi hacking, MITM XSS, SQL Injections ,Phishing, session hijacking, etc.

The course also gives tools for evaluate vulnerability in web sites. All of those topics are being practice by the students in our Hands-On labs that were develop specifically for the purpose of this course. The students also using our unique cyber simulator for practical knowledge on how to mitigate the various attacks. The course also contains homework for the students as additional hands-on material.

## Target Audience

This course is intended for intermediate security personnel wishing to learn how to use the various tools for successful PT.

## Prerequisites

- Good understanding of basic cyber-attacks and tools.
- Good understanding of networking protocols and TCP/IP
- Using Kali and basic Linux commands - Recommended