Offensive Python

Duration**: 40 hours**

Overview

The world of information security consists of a multitude of complex issues and techniques on how to deal with the many environments that can be vulnerable to global cyber-attacks. The groups that get stronger are not only the hackers who try to hurt you but also the defense groups in the organizations, the more known the attacks, the more definite their defense. The course offers participants advanced levels of attack to evade the many defense mechanisms available in the market today with the help of independent tools and Python programming capabilities.

במסגרת הקורס יתבצע תרגול ע"י סימולטור ייעודי להכשרה.

Target Audience

- Ethical hackers and penetration testers
- Students preparing for OSCP, OSCE, GPEN, GXPN, CEH
- Information security professionals and cybersecurity consultants
- System and network security administrators
- Programmers who want to get their hands dirty

Pre-requisites

ידע ב-LINUX ברמה בסיסית

Objectives

- Understanding the cyber threat landscapes
- Acquiring knowledge and tools
- Identifying attacks when accruing on the network
- Testing networks and systems for vulnerabilities and create an attack mechanism
- Reinforce Metasploit framework using Python
- Becoming familiar with a variety of available tools for performing security-related tasks

Module 1: Offensive Networking with Python .א

This module will teach the students how to use python programming language during any penetration testing or ethical hacking operation and how to use Python to automate your network analysis scripts on various information security fields.

Offensive Networking

- Raw Sockets Basics
- Socket Libraries and Functionality
- Programming Servers and Clients
- Writing Packet Sniffers
- PCAP File Parsing and Analysis
- Automating Network Attacks with Python

Utilizing Scapy

- Crafting packets with Scapy
- Routing using Scapy
- Creating Automation with Scapy
- Offensive Scapy Techniques
- DDoS Attack
- Port Scanning and Version Detection
- Automate the Process of PCAP Parsing
- Using Scapy to Create a Custom Wireless Data leakage tool

Module 2: Ethical Hacking with Python .ב

This module will teach students to handle common and various ethical hacking techniques to write automation processes to that procedure.

Ethical Hacking

- Privesc Enumeration Scripts
- Python I/O Handling

Password Cracking

- Wordlist Generation Tool
- Building Password Guessing Tool
- Password Cracking with Python
- Automating Brute-force Attacks
- Automate Banner Grabbing

Advanced Scanning with Python

Shodan CLI Integration
Automated Nmap Script
Advanced Shodan Search with Python

Web Application pen-testing automation process
Fuzzing
Requests and Response
Examine Directories and Files
Parsing HTML Files
URL Fetching and Parsing
Customizing SQL Injection Queries
Parsing Tweets

Module 3: Replicate Metasploit features .ג

Metasploit framework is written in Ruby and does not support scripts written in Python, so it requires some additional tuning to automate the actions of the attacker using Metasploit and Python together. In this module, students will learn how to automate Metasploit script using Python and other useful techniques for ethical hacking.

Creating Offensive Tool
Interact Python with Metasploit
Create Metasploit Scripts
Build a Port Scanner
Process Monitoring with Python
Cracking Tools
Reverse Shells
Extracting Images from TCP Streams

Mimicking Metasploit Framework
Auxiliary in Python
Understanding Reverse and Bind Shells
Working with Anonymity
Enumerating Services
Post Exploitation Procedures
Introduction to Buffer Overflow attacks
Pymetasploit3 – Metasploit Automation Library