SDA.ACADEMY
Cybersecurity training

THINKCYBER

Syllabus

Offensive Python

CYBERIUM ARENA

-SIMULATOR-

Description

The world of information security consists of many complex issues and techniques for dealing with the many environments that can be vulnerable to global cyber-attacks. 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.

The course helps prepare for the certification exam GPYC (SANS).

Target Audience

The course targets participants with a strong foundation of computer networking knowledge and Linux interested in upgrading their current cyber knowledge and capabilities.

Pre-requisites

Linux

Networking

Objectives

- Acquiring Python knowledge and building tools
- Building defense tools
- Building network-based tools
- Becoming familiar with a variety of libraries for security-related tasks

Module 1: Working with Python

This module will teach the students how to use the Python programming language and how to use Python to automate their network analysis scripts on various information security fields.

Python Networking

- Introduction to Sockets
- Connecting with TCP and UDP
- Banner Grabbing
- Port Scanner

Useful Libraries for Security

- Cymruwhois
- Faker

Password Cracking

- Brute Force Attacks
- Brute Force Zip Attacks
- FTP Cracker

Module 2: Packet Crafting with Python

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

Scapy

- Sniffing with Scapy
- Researching Pcap Files
- Crafting Packets
- Sending Packets
- Automation with Scapy
- Port Scanners
- MiTM Attack
- Creating Security Tools

Module 3: Scanners

In this module, students will learn to generate custom scans and use automation to achieve cyber procedures.

Scanning with Python

- Nmap
- Shodan

Automation with Python

- Paramiko
- Pexpect

Module 4: WebApp Security with Python

The web application security module is an important part of the training. Students will learn how to use their knowledge on the web, extract sensitive data, and create web servers for red-team tasks.

HTTP Programming

- Simple Web Server
- Urllib

BeautifulSoup Requests

- Web Application Security
- Setting the User Agent
- Setting Cookies
- Using Web Proxy
- Spidering

Module 5: Replicate Metasploit features

In this module, students will learn how to automate Metasploit script using Python and other useful techniques for ethical hacking.

Working with Payloads

- MSFVenom
- The Python Payload
- TCP Reverse Shell Explained
- HTTP Reverse Shell Explained
- Persistence Explained
- Upgrading your Shell
- DDNS Reverse Shell

Local Attacks

- DNS Poison
- Extracting Passwords from Chrome
- Keylogger