CYBERIUM ARENA

Description

Embark on a comprehensive journey into Python-based cybersecurity. Delve into Python networking, covering sockets, banner grabbing, and advanced tools like Nmap and Shodan. Focus on packet crafting, teaching the intricacies of Scapy, packet sniffing, and creating security tools. Introduce WebApp Security, exploring HTTP programming, web application security measures, and techniques like spidering. Finally, unveil the powerful features of Metasploit, from working with payloads and reverse shells to local attacks and keylogging.

OFFENSIVE PYTHON

Module 1: Python Networking

Dive into the foundational aspects of networking with an introduction to sockets and connections via TCP and UDP. Explore security tools and techniques, from banner grabbing and port scanning to leveraging libraries like Cymruwhois and Faker. Master password cracking methods, utilizing tools such as Nmap, Shodan, and specialized brute force attacks.

Introduction to Sockets

Connecting with TCP and UDP
Banner Grabbing
Port Scanner

Useful Libraries for Security

Cymruwhois
Faker
Brute Force Attacks
Brute Force Zip Attacks
FTP Cracker

Scanners

Nmap
Shodan

Module 2: Packet Crafting

Delve into the world of Scapy, a powerful tool for packet manipulation and network analysis. Master the art of sniffing, researching pcap files, and automating tasks with Scapy. Enhance your security toolkit by crafting and sending packets, deploying port scanners, executing MiTM attacks, and designing bespoke security tools.

Scapy

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

Module 3: WebApp Security

HTTP programming, exploring the creation of simple web servers and harnessing libraries like Urllib, BeautifulSoup, and Requests. Dive deeper into web application security, mastering techniques such as setting user agents, managing cookies, utilizing web proxies, and the art of spidering.

HTTP Programming

Simple Web Server
Urllib
BeautifulSoup
Requests

Web Application Security

Setting the User Agent
Setting Cookies
Using Web Proxy
Spidering

Module 4: Metasploit Features

Navigate the intricate world of payloads, from mastering MSFVenom to understanding Python-specific payloads. Delve into the mechanics of reverse shells, including TCP and HTTP variants, and grasp the importance of persistence in cyber operations. Enhance your skillset with techniques like upgrading shells, executing local attacks, DNS poisoning, extracting passwords from Chrome, and deploying keyloggers.

Working with Payloads

MSFVenom
The Python Payload
TCP Reverse Shell Explained
HTTP Reverse Shell Explained
Persistence Explained
DDNS Reverse Shell
DNS Poison
Extracting Passwords from Chrome
Keylogger

ZX Offense | LEVEL: 5 | DURATION: 40h