CYBERSECURITY WITH PYTHON- CRASH COURSE

Course Overview

This course provides a comprehensive introduction to malware analysis, focusing on using Python to dissect, understand, and mitigate malicious software. By the end of the course, participants will have a solid understanding of malware characteristics and behaviors and will be equipped with practical skills to perform basic to advanced malware analysis using Python.

Module 1: Introduction to Malware Analysis

Lesson 1.1: What is Malware?

Definition and Types of Malware

History and Evolution of Malware

Lesson 1.2: Goals of Malware Analysis

Understanding Intent and Impact

Identifying Indicators of Compromise (IOCs)

Lesson 1.3: Setting Up a Safe Analysis Environment

Virtual Machines and Sandboxing

Essential Tools and Software

Module 2: Basics of Python for Malware Analysis

Lesson 2.1: Python Basics

Syntax and Structure

Data Types and Control Structures

Lesson 2.2: File Handling in Python

Reading and Writing Files

Working with Binary Data

Lesson 2.3: Networking with Python

Sockets and Network Connections

HTTP Requests and Responses

Module 3: Static Analysis

Lesson 3.1: Understanding Static Analysis

What is Static Analysis?

Benefits and Limitations

Lesson 3.2: Analyzing Malware Files

Identifying File Types and Characteristics

Extracting Metadata and Strings

Lesson 3.3: Disassembly and Decompilation

Using Disassembly Tools

Introduction to Decompilation with Python Libraries

Module 4: Dynamic Analysis

Lesson 4.1: Understanding Dynamic Analysis

What is Dynamic Analysis?

Setting Up a Dynamic Analysis Environment

Lesson 4.2: Monitoring Malware Behavior

Using Python for Process Monitoring

Network Traffic Analysis with Python

Lesson 4.3: API Hooking and Tracing

Introduction to API Hooking

Implementing API Hooks in Python

Module 5: Advanced Malware Analysis Techniques

Lesson 5.1: Unpacking and Decrypting Malware

Techniques for Unpacking Malware

Using Python for Decryption

Lesson 5.2: Analyzing Obfuscated Code

Identifying Obfuscation Techniques

Deobfuscation with Python

Lesson 5.3: Malware Evasion Techniques

Understanding Evasion Techniques

Detecting and Mitigating Evasion with Python

Module 6: Case Studies and Practical Exercises

Lesson 6.1: Analyzing Real-World Malware Samples

Step-by-Step Analysis of Malware Samples

Documenting and Reporting Findings

Lesson 6.2: Hands-On Projects

Building a Malware Analysis Toolkit with Python

Developing Custom Python Scripts for Analysis

Lesson 6.3: Final Project

Comprehensive Malware Analysis Project

Presentation and Peer Review

Module 7: Best Practices and Ethical Considerations

Lesson 7.1: Best Practices for Malware Analysis

Maintaining Security and Privacy

Staying Updated with Latest Trends and Tools

Lesson 7.2: Ethical and Legal Considerations

Understanding Legal Implications

Ethical Responsibilities in Malware Analysis

This courseware covers both theoretical and practical aspects of malware analysis, ensuring that participants gain a thorough understanding of the subject and hands-on experience with Python-based analysis techniques