AISECT LEARN
Better Education. Better Careers.

LIVE + SELF-PACED

CYBER SECURITY USING PYTHON

COURSE OVERVIEW

The Cybersecurity using Python (CUP) course is designed to equip participants with practical knowledge and skills in using Python programming for cybersecurity applications. This course aims to empower individuals to leverage Python's versatility and power to secure computer systems, networks, and applications effectively. Through hands-on coding exercises and real-world projects, students will learn to build robust security tools, automate routine cybersecurity tasks, and conduct penetration testing to identify and address vulnerabilities. By the end of this course, participants will be proficient in leveraging Python's libraries and modules to enhance their cybersecurity capabilities, making them valuable assets in defending against a wide range of cyber threats.

COURSE OBJECTIVE

Cybersecurity using Python (CUP) is an intensive course that equips learners with advanced programming skills in Python to strengthen cybersecurity practices. Participants will gain hands-on experience in developing security tools, automating security tasks, and analyzing vulnerabilities using Python scripts. By the end of the course, students will be proficient in leveraging Python to enhance cybersecurity measures and mitigate potential risks.

WHAT YOU WILL LEARN

The Cybersecurity using Python (CUP) course empowers participants to harness the power of Python programming language for solving cybersecurity challenges. Students will acquire a strong foundation in Python programming, regardless of their prior coding experience, and apply it to various cybersecurity domains.

Throughout the course, participants will explore network security using Python, developing tools and scripts to analyze network traffic, detect anomalies, and secure network communications. They will also delve into web application security, understanding how to perform vulnerability assessments and automate security testing using Python.

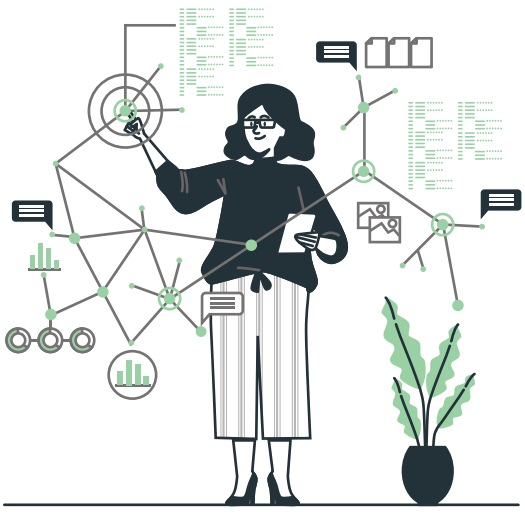
Participants will learn about malware analysis and threat hunting techniques, leveraging Python to extract and analyze malicious code and behavior. Additionally, they will explore log analysis, data visualization, and the use of Python libraries to gain insights into security events and trends.

By the end of the CUP course, participants will have a strong grasp of Python for cybersecurity purposes, equipped with the ability to develop custom cybersecurity tools and scripts, automate repetitive tasks, and enhance overall cybersecurity operations using the power of programming.

COURSE SKILL SET

• Understanding the importance of cybersecurity and its role in modern society.
• Familiarity with the CIA Triad (Confidentiality, Integrity, Availability) and its significance in cybersecurity.
• Knowledge of the hacking methodology and how cyber attacks are carried out.
• Understanding Social Engineering and its various tactics.
• Identification and understanding of different types of cyber attacks such as Brute Force Attacks, Phishing, DoS, DDoS, etc.
• Familiarity with the basics of Malicious Codes and Terminologies.
• Knowledge of cybersecurity breaches and the importance of penetration testing.
• Familiarity with various frameworks and standards used in cybersecurity.
• Understanding computer hardware and software elements, networking, OSI layers, and network protocols.
• Knowledge of IP addressing and subnet classes.
• Familiarity with various network devices and their functionalities.
• Ability to perform packet sniffing and packet spoofing using tools like Scapy.
• Understanding the concept of vulnerability and penetration testing.
• Knowledge of cybersecurity controls, policies, CVE, and CVSS.
• Awareness of different types of cyber threats and attacks, including architecture, design, implementation, and incident response.
• Knowledge of various cybersecurity defenses like Firewalls, Encryption, Biometrics, Anti-Virus, and Password Management.
• Understanding the concept of Cyber Kill Chain and its stages (Reconnaissance, Weaponization, Delivery, etc.).
• Proficiency in Python scripting, including variables, data types, flow controls, functions, classes, file handling, and important modules.
• Ability to create projects like a Port Scanner and Keylogger using Python.
• Knowledge of computer forensics investigation processes, data acquisition, and analysis using tools like Encase and Volatility.

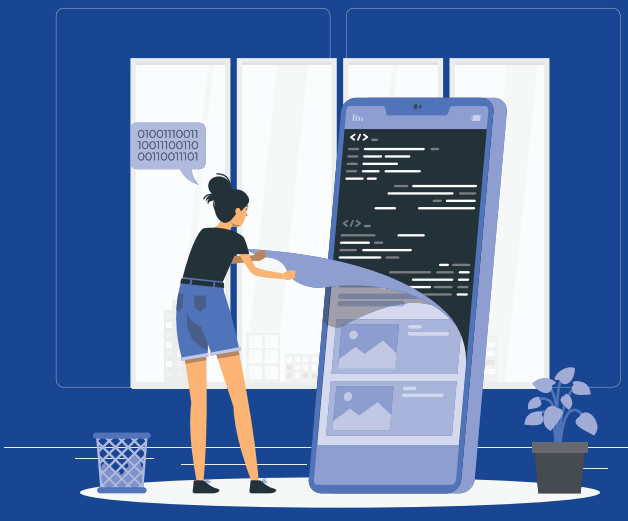
Instructor - **Ajay Gautam | Cyber Security Expert**
Instructor - **Aman Roy | Cyber Security Expert**
Duration - 1 Month
Eligibility - Any graduate with a Science stream
No. of Modules – 09 Modules
Language - English
Shareable certificate - Yes



PROGRAM SYLLABUS

Module 1 Introduction to Cybersecurity
Session 1.1 Introduction
Session 1.2 Why Cyber Security is Important?
Session 1.3 Role of cyber security enginner
Session 1.4 CIA Triad
Session 1.5 The Hacking Methodology
Session 1.6 The WhoIS Query
Session 1.7 Social Engineering
Session 1.8 Brute Force Attacks
Session 1.9 Phishing
Session 1.10 Bots and Botnets
Session 1.11 DoS and DDoS
Session 1.12 Pings
Session 1.13 Man in the Middle Attacks (MITM)

Module 2 Cyber Security Building blocks
Session 2.1 Malicious Codes and Terminologies
Session 2.2 Cybersecurity Breaches
Session 2.3 Penetration Testing and Methodologies
Session 2.4 Frameworks and Standards for Cybersecurity
Session 2.5 Hardware and Software Elements of Computer Systems
Session 2.6 Introduction to Networks and Reference Models
Session 2.7 OSI layers
Session 2.8 Network Protocol
Session 2.9 IP Address and Subnet Classes
Session 2.10 Network Devices
Session 2.11 Packet Sniffing
Session 2.12 Sniffing Using Scapy
Session 2.13 Packet Spoofing
Session 2.14 Packet Spoofing Using Scapy



Module 3 Basic concepts of Vulnerability
Session 3.1 Types of Hackers & Hacktivism
Session 3.2 Understanding Terminologies
Session 3.3 Vulnerability & Pentesting
Session 3.4 Cyber Security Controls

Session 3.5 Cyber Security Policies
Session 3.6 CVE & CVSS

Module 4 Security Basics
Session 4.1 Attacks & Threats
Session 4.2 Architecture & Design
Session 4.3 Implementation
Session 4.4 Operations & Incident Response
Session 4.5 Governance, Risk & Compliance
Session 4.6 Firewalls
Session 4.7 Encryption
Session 4.8 Biometrics
Session 4.9 Anti Virus
Session 4.10 Password Management
Session 4.11 What is Cyber Kill Chain?
Session 4.12 Reconnaissance
Session 4.13 Weaponization
Session 4.14 Delivery

Module 5 Python Scripting
Session 5.1 Introduction to Python
Session 5.2 Python execution and installation
Session 5.3 Identifiers, variables and Datatypes
Session 5.4 Operators
Session 5.5 Python-Flow Controls
Session 5.6 Functions
Session 5.7 Python Classes
Session 5.8 Inheritance,Files
Session 5.9 Python - File Handling, API programming.
Session 5.10 Python - important modules
Session 5.11 Project1 - Port Scanner
Session 5.12 Project2 - Keylogger

Module 6 Computer Forensics
Session 6.1 Computer Forensics investigation process
Session 6.2 Data Acquisition & Duplication
Session 6.3 Introduction to Windows Forensics
Session 6.4 Lab: Capturing Windows Memory
Session 6.5 Browser Forensics using Encase
Session 6.6 Lab: WebHistorian
Session 6.7 Memory Forensics

Module 7 Python Essentials
Session 7.1 Python Introduction
Session 7.2 Installation of Anaconda Navigator
Session 7.3 Jupyter Notebook Interface
Session 7.4 How to Open, Save and Rename a file
Session 7.5 Variables and Data Types
Session 7.6 Python Strings
Session 7.7 Loops (Conditional)
Session 7.8 Loops (iterative while)
Session 7.9 Loops (iterative For)
Session 7.10 Python Functions(Built in, Lambda, User defined functions)
Session 7.11 Lists
Session 7.12Tuples
Session 7.13Sets
Session 7.14 Dictionaries
Session 7.15 Numpy Arrays in Python
Session 7.16 Three Dimensional Arrays Indexing and slicing
Session 7.17 Matrices
Session 7.18 Pandas in Python
Session 7.19 Importing CSV, Excel Files
Session 7.20 Exporting CSV file

Module 8 Python data analysis
Session 8.1 Basic descriptive statistics with Numpy and Applying statistical functions on matrices
Session 8.2 Linear Algebra with NumPy
Session 8.3 Numpy Random Numbers
Session 8.4 Probability distributions using NumPy
Session 8.5 Normality test with SciPy

Module 9 Job roles
Session 9.1 Analyst
Session 9.2 Engineer Trainee