What you will learn:

- Vulnerability Analysis
    - Learn how to perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems. This module covers the vulnerability management life cycle, and various approaches and tools used to perform the vulnerability assessment.
- Hacking Challenges at the End of Each Module
    - Challenges at the end of each modules ensures you can practice what you have learnt. They help student understand how knowledge can be transformed as skills and can be used to solve real-life issues.
- Coverage of latest Malware
    - The course is updated to include the latest ransomware, banking and financial malware, IoT botnets, Android malwares and more!
- Hands-on Program
    - More than 60 percent of class time is dedicated to the learning of practical skills and this is achieved through labs.

Course Outline

- **Fundamentals**
  - OS
    - Types of OS
    - Windows
    - Linux
    - Unix
    - GNU
  - Command Line
    - Windows
      - Powershell
      - Batch
      - Scripting in PS and Batch
    - Linux
      - Bash
      - Scripting
  - Programming
    - Python
      - Fundamentals
- Networking
    - Basic
    - IPv4
    - IPv6
    - DNS
    - Protocols

- Introduction to Ethical Hacking

- Footprinting and Reconnaissance

- Scanning Networks

- Enumeration

- Vulnerability Analysis

- **System Hacking**
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- **Hacking Web Applications**
    - OWASP TOP 10
- Hacking Wireless Networks
- Hacking Mobile Platforms
- **Cloud Computing**
- Cryptography