CLS | Learning Solutions

Why Learn Offensive Cyber Security And CTF?

Offensive Security is a proactive and adversarial approach to protecting computer systems, networks and individuals from attacks, pen testing is an authorized simulated attack performed on a computer system to evaluate its security.

Audience Profile :

- Any one interest in Learning offensive cyber security from scratch and build a career in today's top wanted Information technology field.
- This course is great for those who are already in IT and are looking to expand their horizons to learn how the back end of an offensive security operation works. Whether you're a software developer, system administrator, this course is for you!

Prerequisites:

- CCNA .
- Linux Administration .
- Windows server Administration.

Course Overview:

- This learning path will teach you all you need about It and Operating systems and Cyber Security threats.
- It will prepeare you for the role of SOC analyst in an Operation Security Center.
- In this track, students will learn the fundamentals of Networks and Systems Administration.
- Then you will learn Offensive Security & Pen Testing and identify the concepts with practices.
- Cyber Security is becoming increasingly prevalent, with a larger number of businesses becoming affected by cyber attacks each year.

Offensive Cyber Security And CTF Outline:

- Offensive Cyber Security Introduction
- Active and Passive Reconnaissance
- Network Discovery
- Major System and Network Protocols
- Vulnerabilities
- Operating System Hacking
- Malware
- Layer 2 Attacks – Layer 3 Attacks
- Social Engineering
- Session Hijack
- Denial of Service
- Defensive devices and systems
- Web Attacks
- SQL Injection
- Wireless Attacks – Mobile Attack – IOT Attack
- Encryption methods
- Cloud Risks
- Countermeasures
- Risk Management
- Security Assessment
- Security Operations
- Security Design