Cybersecurity Professional

Welcome to the Cybersecurity course. This course is mapped to the popular Cybersecurity Professional course from the US-Council (www.us-council.com). Zoom Technologies are the official training partners of US-Council.

In today's increasingly interconnected world, protecting your organization's critical information and systems from cyber threats is more important than ever. This course is designed to give you a comprehensive understanding of cybersecurity concepts and practices, equipping you with the skills and knowledge necessary to defend against cyber attacks. You will learn about various types of threats, including malware, phishing, and social engineering, as well as the strategies and technologies used to detect, prevent, and respond to them right from risk management, to ethical hacking and penetration testing. Whether you are a network administrator or security professional, or simply interested in learning about cybersecurity, this course will provide you with the skills you need to help keep your systems and data secure.

Our USP: Our cybersecurity expert instructors are experts in every sense of the word - they have a formidable reputation in the industry as real time cybersecurity gurus with decades of experience. All our classes are conducted **LIVE with 100% Student Interaction**. Our world class instructors, courseware and labs ensure that the students gain hands on **Practical Knowledge** and are not limited to theory alone. Come, **ZOOM** with us into a cybersecurity career!

Course Outline

This Course Consists of Three Modules:

1. Security Risk Assessment (Ethical Hacking)
2. Proactive Defense and Countermeasures
3. SIEM & Incident Response

A Few Topics:

- Vulnerability Auditing
- Penetration Testing
- Wi-Fi Hacking
- IoT Device Hacking
- Phishing
- Whaling
- Darkweb

Course Curriculum

Module 1: Security Risk Assessment (Ethical Hacking)

Introduction to Hacking
- What is Hacking
- What is Ethical Hacking
- What is Information Security
- What is Information Assurance
- CIA Triad
- Stages of Hacking

Vulnerability Based Hacking
Footprinting
- What is Footprinting
- Footprinting Objectives
- Footprinting Techniques

Scanning
- What is Scanning
- What is Enumeration
- Scanning Methodology
- What is Vulnerability Auditing
- What is Penetration Testing
- Continuous Automated Red Teaming (CART)
- AI Fuzzing

Hacking Web Applications
- Directory Traversal
- Website Defacement
- Code Injection
- SQL Injection
- XSS

Cryptography
- Common Terminology
- Symmetric Key Encryption
- Asymmetric Key Encryption

Password Hacking Attacks
Password Cracking Attacks
- Bruteforce attack
- Dictionary attack
- Rainbow table attack

Sniffers
- What is a sniffer
- Sniffing techniques
- ARP Poisoning
- Session Hijacking

Phishing
- What is Phishing
- Spear Phishing
- Deepfake Phishing
- Whaling
- Pharming

Wireless Hacking
- What is a wireless network
- Types of wireless networks
- Wireless network attacks

Malware
- What is a Malware
- Types of Malwares

IoT Attacks
- What is IoT
- IoT communication methods
- IoT Operating Systems
- IoT Attacks

Cloud Computing
- What is Cloud Computing
- Types of Cloud Computing
- Types of Cloud Computing Services
- Cloud Computing Attacks

Blockchain Attacks
- What is Blockchain
- Blockchain Attacks

Covering Tracks
DoS
- What is DoS
- DoS attack techniques

Anonymizers
- What is an anonymizer
- Proxy server
- VPN server
- TOR Browser

DarkWeb
- What is DarkWeb
- Different DarkWeb technologies

Cyber Kill Chain
Securing the network
MITRE ATT&CK Framework
Security Compliance Standards

Module 2: Proactive Defence and Countermeasures

Introduction to Security
- Network Security Challenges
- Elements of Information Security
- Security, Functionality and Usability Triangle
- Zero Trust approach
- Castle Moat approach

Firewall
- What is a Firewall
- Types of Firewall
- Designing network security with Firewall
- Secure Access Service Edge (SASE)
- NAT
- Security Policy
- Logs Management
- Application Security
- Content / Web Security
- Authentication

Virtual Private Networks
- What is VPN
- Type of VPNs
- GRE
- IPSEC
- SSL

Intrusion Prevention Systems
- What is an Intrusion Detection System
- What is an Intrusion Prevention System

Unified Threat Management
- What is UTM
- How UTM is different from Firewall
- Advantages of UTM

High Availability
Virtual / Cloud Devices
Cisco ASA
Stormshield UTM

Module 3: SIEM & Incident Response

SIEM
- What is SIEM
- Functions of SIEM
- SIEM architecture

Incident Management
- Incident response policy
- Incident Handling