# Cybersecurity Professional

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.

This course is meant for those professionals who are looking for comprehensive and total knowledge in the network security domain. This is the only course which teaches both hacking and countermeasure techniques. And in keeping with Zoom's standards, this course is entirely hands on and real time oriented. And need we say, the instructors are network security and intrusion specialists with several years of experience. This course consists of three modules viz

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

## Course Outline

- Security Risk Assessment
- Dos and DDos Attacks
- Attack Mitigation Techniques
- Firewalls, IDS, IPS
- Cryptography
- Incident Response and Management
- Log Analysis
- Forensics

# COURSE CURRICULUM

**Module 1: Security Risk Assessment (Ethical Hacking)**

Introduction to Ethical Hacking
- What is Hacking
- What is Ethical Hacking
- What is Penetration Testing
- What is Vulnerability Auditing

Footprinting
- What is FootPrinting
- Footprinting Techniques
- Footprinting Website & Tools

Scanning
- What is Network scanning
- Types of Scanners
- Vulnerability Scanner Tools

Proxy
- What is a proxy server
- Types of proxies
- What is a Darkweb
- Why hackers prefer to use Darkweb

Hacking Web Servers & Web Applications
- What is a web server
- Types of web attacks

Session Hijacking
- What is session hijacking
- Session hijacking Techniques
- Session hijacking Tools

Denial of Service
- What is a DoS and DDoS attack
- DoS attack techniques
- DoS attack Tools

System Hacking
- What is System Hacking
- What is Password Cracking
- Password Cracking techniques
- Password Cracking Website & Tools

Sniffers
- What is a sniffer
- Sniffing Techniques
- Sniffing Tools

Phishing
- What is Phishing
- Phishing Techniques
- Phishing Tools

Malware
- What is malware
- Types of malware
- Malware creation Tools
- USB password stealers

Wireless Hacking
- Types of wireless networks
- Wireless Hacking Techniques
- Wireless Hacking Tools

Kali Linux
- What is Kali Linux
- Kali Linux Tools

**Module 2: Proactive Defence and Countermeasures**

Introduction to Security
- What is security?
- Layer 1 Security
- Layer 2 Security
- Layer 3 security

Firewalls
- What is a Firewall?
- Types of firewalls
- Designing Security with Firewalls
- NAT
- Security Policy
- Logs Management
- Application Security
- Content / Web Security
- Authentication

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

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

High Availability
Virtual / Cloud Devices Security
Host Security
- OS Hardening
- Patch management
- Antivirus
- Endpoint Security

**Module 3: Incident Response and Management**

SIEM
- Introduction to SIEM
- SIEM Architecture
- Events and Logs
- Event Correlation and Event Collection
- Correlation Rules
- Forensic Data
- SIEM Deployment

Incident Response
- Introduction Incident Response
- Incident Response Policy
- Incident Handling
- Forensics of Incident response
- Inside Threat
- Incident Recovery
- Malware Analysis

Mobile Forensics
- Forensic Acquisition of Smartphones
    1. Logical Acquisition
    2. File System Acquisition
    3. Physical Acquisition
- Android Forensics
- Retrieving User Activity Information from Android Devices
- iOS (iPhone) Forensics
- Retrieving User Activity Information iOS Devices