Cybersecurity Professional

www.us-council.com

This course is mapped to the popular Cybersecurity Professional Certification Exam.

Training can be taken from anywhere in the world through our Authorized Training Partners or through Online Training offering at the link below:

http://us-council.com/training.php

The cybersecurity professional certificate course is geared towards creating the absolute cybersecurity expert, equally at ease in providing security for futuristic networks and legacy systems.

The cybersecurity professional course provides comprehensive training in all aspects of cyber defense methodologies. This course covers the proactive defense mechanisms required of a cybersecurity professional including ethical hacking, firewalls, IPS, vulnerability assessment and cryptography. Vital cybersecurity reactive techniques are also discussed including SIEM, mobile and digital forensics, log analysis and patch management. This course consists of three modules viz

1. Security Risk Assessment (Ethical Hacking)

2. Proactive Defense and Countermeasures
3. Incident Response and Management

A thorough understanding of the underlying principles of networking and operating systems is a prerequisite to pursuing this advanced course. The student is expected to be knowledgeable in IP networks, TCP / IP stack, protocols like http, https, ICMP, ARP, services like DNS, DHCP, LDAP, telnet, ssh as well as routing protocols like RIP, EIGRP, BGP, etc. Expertise in Linux and Windows servers and related technologies is a must.

Key Topics:

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

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
    - o Logical Acquisition
    - o File System Acquisition
    - o Physical Acquisition
- Android Forensics
- Retrieving User Activity Information from Android Devices
- iOS (iPhone) Forensics
- Retrieving User Activity Information iOS Devices