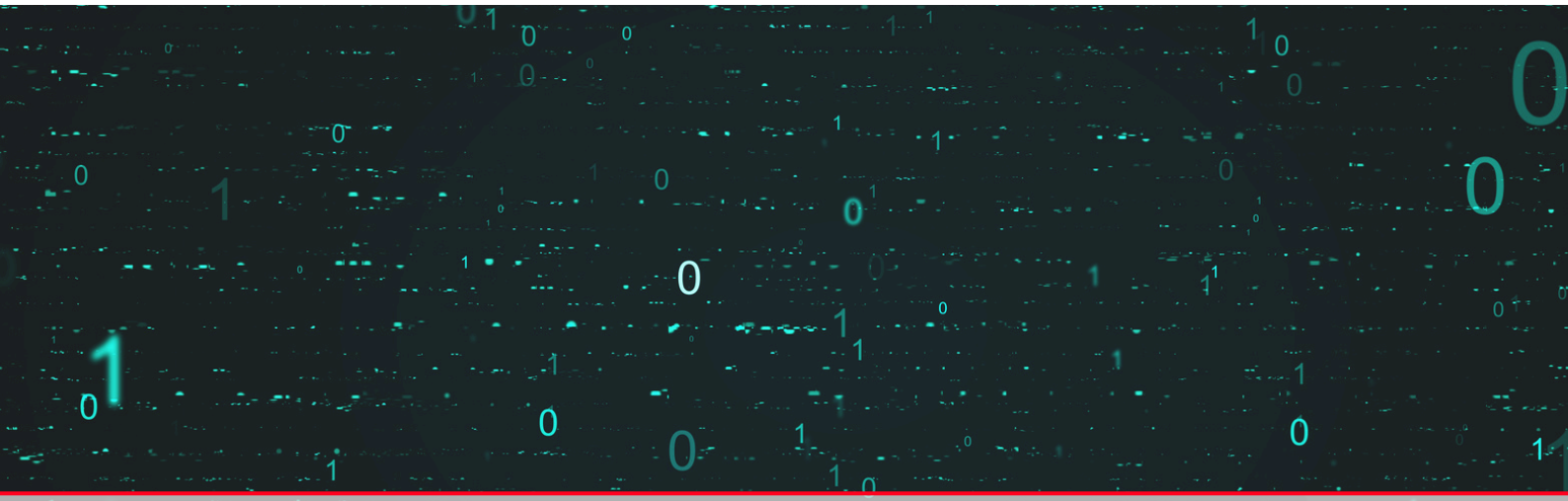
ZOOM TECHNOLOGIES

CYBEREYE™ The Science of Security
BY US-COUNCIL
www.us-council.com



Ethical Hacking & Prevention

The Ethical Hacking & Prevention certificate course is geared towards creating awareness on various types of cyber-attacks and security countermeasures to mitigate the attacks.

The Ethical Hacking & Prevention course provides comprehensive training on all aspects of Vulnerability Assessment, Penetration Testing, Cryptography, Darkweb, IoT attacks, and Password Cracking methodologies. This course consists of Security Risk Assessment (Ethical Hacking) module.

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:

- Vulnerability Assessment
- Penetration Testing
- Cryptography
- DarkWeb
- Password Cracking
- Dos and DDos Attacks
- Attack Mitigation Techniques

Ethical Hacking & Prevention

CYBEREYE The Science of Security BY US-COUNCIL

Module 1: Security Risk Assessment

- Introduction to Ethical Hacking
  - What is Hacking
  - Skills of a hacker
  - Types of Hackers
  - Network Security Challenges
  - What is Ethical Hacking
- Information Security
- Information Assurance
- Elements of Information Assurance
- Stages of Hacking

Module 2: Vulnerability Based Hacking

- Footprinting
  - What is Footprinting
  - Footprinting Techniques
- Scanning
  - What is Scanning
  - What is Enumeration
  - Scanning methodology
  - Continuous Automated Red Teaming (CART)
  - AI Fuzzing
  - Vulnerability Assessment
  - Penetration Testing

Module 3: Hacking Web Applications

- What is a Web Application
- Web Application Attacks
  - Code Injection
  - Web site defacement
  - SQL Injetion
  - XSS

Module 4: Cryptography

- What is Cryptography
- Types of Cryptography
- Cryptographic Hash

Module 5: Password Hacking Attacks

- Password guessing
- Shoulder Surfing
- Social Engineering
- System hacking
- Bruteforce attack
- Dictionary attack
- Rainbow tables

Module 6: Sniffers

- What is a sniffer
- How does a sniffer function
- Sniffing techniques

Module 7: Phishing

- What is Phishing
- Phishing techniques
  - Spear Phishing
  - Whaling
  - Pharming
  - Vishing

Module 8: Wireless Hacking

- What is a Wireless Network
- Types of Wireless Networks
- Different WiFi standards
- WiFi attacks

Module 9: Malware

- What is Malware
- Types of Malware
- Privilege Escalation
- Unauthorized Application Execution

Module 10: IoT Attacks

- What is IoT
- IoT communication methods
- IoT communication protocols

+91 7893399822 priya@zoomgroup.com www.zoomgroup.com

- IoT Operating Systems
- Security Challenges in IoT
- IoT Attacks

Module 11: Cloud Computing

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

Module 12: Blockchain Attacks

- What is Blockchain
- Blockchain Attacks
- Denial of Service (DoS)
  - What is DoS
  - What is DDoS
  - Botnets
  - DoS/ DDoS attack techniques

Module 13: Anonymizers

- What is an anonymizer
- Why are anonymizers used
- Types of anonymizers
  - Proxy
  - VPN Proxy
  - TOR Browser

Module 14: DarkWeb

- What is DarkWeb
- Different DarkWeb technologies
- Freenet
- I2P
- TOR

Module 15: Covering Tracks

- How hackers cover their tracks

Module 16: Securing the Network

- Hardware encryption
- Software encryption
- PKI

Module 17:

- Cyber Kill Chain
- Introduction to MITRE ATT&CK Framework
- Introduction to Security Compliance Standards
- Cyber Resilience
- Cyber Fusion Center