

## Training Program Information

---

### Course Outline

**Note:** EC-Council's fundamental courses are conducted by selected academic partners such as colleges and universities around the world.

- **Module I: Security Basics**
  - Importance of Information Technology
  - Why Security?
  - The Security, functionality and ease of use Triangle
  - Elements of Security
  - Essential Terminology
  - Can Hacking be Ethical?
  - Computer Crimes and Implications
  - Legal Perspective (US Federal Law)
- **Module II: Addressing Threats**
  - Module Objectives
  - What is a Threat?
  - Internal Threat
  - Sniffing
  - External Threat
  - Social engineering
  - Methods of Attack
  - Denial of service (DoS) attack
  - Virus
  - Worms
  - Trojans
  - Organizational Threat
  - Accidental Security breach
  - Automated Computer Attack
- **Module III Backdoors, Virus and Worms**
  - Virus History
  - Life Cycle of a Virus
  - Terminologies
  - What is a Trojan?
  - Indications of a Virus Attack
  - Anti-Virus Software
  - Popular Anti-Virus Packages
- **Module IV: Linux**
  - Why Linux?
  - Linux – Basics

- Why is Linux Hacked?
- How to apply patches to vulnerable programs
- Linux Rootkits
- Ramen

- **Module V: Password Cracking**

- Authentication - Definition
- What is a Password Cracker?
- Modus Operandi of an attacker using a password cracker
- How does a Password Cracker work? (a)
- How does a Password Cracker work? (b)
- Attacks – Classification
- Password Guessing
- LOphtCrack
- Brutus
- Password Generators

- **Module VI: Cryptography**

- Basics of Cryptography
- Public-key Cryptography
- How Encryption works
- Digital Signature
- What is SSH?
- RSA (Rivest, Shamir, and Adleman)
- RSA Attacks
- RSA Challenge
- MD5
- SHA (Secure Hash Algorithm)
- Disk Encryption

- **Module VII: Web Servers and Web Applications**

- How Web Servers Work?
- IIS Components
- Popular Web Servers and Common Security Threats
- Apache Vulnerability
- Attacks against IIS
- Increasing Web Server Security
- The Web Application set up
- Web Application Threats

- **Module VIII: Wireless Network**

- Introduction to Wireless Networking
- Business and Wireless Attacks
- Basics
- Components of a wireless network
- Types of Wireless Network
- Setting up a WLAN
- Detecting a Wireless Network
- How to access a WLAN?

- Advantages
- Antennas
- SSIDs
- Access Point Positioning
- Rogue Access Points
- NetStumbler

- **Module IX: Intrusion Detection System**

- Introduction
- Intrusion Detection System (IDS)
- Intrusion Detection System (IDS)
- Types of IDS
- Ways to Detect an Intrusion
- System Integrity Verifiers (SIV)
- Snort 2.1.0
- LogIDS 1.0:
- IDS Software Vendors

- **Module X: Firewalls and Honeypots**

- Introduction
- Terminology
- What is a Firewall?
- Firewall Identification
- Banner Grabbing
- Common Tools
- Honeypot
- The HoneyNet Project
- Types of Honeypots
- Advantages of Honeypots
- Honeypot – KFSensor
- Honeypot-Specter

- **Module XI: Hacking Cycle**

- Why Security?
- What does a Malicious Hacker do?
- Gaining Access
- Maintaining Access
- Covering Tracks

- **Module XII: Introduction to Ethical Hacking**

- Hacker Classes
- Hacktivism
- Can Hacking be Ethical?
- What do Ethical Hackers do?
- Skill Profile of an Ethical Hacker
- How do they go about it?
- Modes of Ethical Hacking
- Security Testing

- **Module XIII: Networking Revisited**

- Network Layers

- Application Layer
  - Transport Layer
  - Internet Layer
  - Network Interface Layer
  - Physical layer
  - Differentiating Protocols & Services (b)
  - Mapping Internet Protocol to OSI
  - OSI Layers and Device Mapping:
  - Network Security
  - Essentials of Network Security
  - Network Security Policies
  - Defining good security policy
  - Types of Network Security Policies
- **Module XIV: Secure Network Protocols**
    - Secure Network Protocols
    - Web security applications - SSL
    - Web Security applications – SSH
    - E-Mail security applications – S/MIME
    - E-mail security applications – PGP
    - VPN Security applications - IPSec
    - VPN security applications - PPTP
    - Wireless security applications – WEP
    - Public Key Infrastructure
    - ACL – Access Control Lists
    - AAA (Authentication, Authorization, and Accounting)
    - RADIUS
    - TACACS+
    - Kerberos
    - IKE
- **Module XV: Authentication**
    - Authentication
    - Authentication? Authorization? Identification
    - Types of authentication
    - Steps for performing Authentication
    - Examples of Authentication
    - Authentication over HTTP
    - Authentication Service Model
    - Basic authentication scheme
    - Form based Authentication
    - Digital Certificates
    - Attacks on Authentication
- **Module XVI: Network Attacks**
    - Denial of Service
    - Countermeasures
    - Scanning
    - Countermeasures
    - Sniffing
    - Countermeasures
    - IP spoofing
    - ARP Spoofing
    - Countermeasures
    - Session Hijacking
    - Protecting against Session Hijacking
    - Spamming

- Eavesdropping
- Countermeasures
- **Module XVI: Bastion Hosts and DMZ**
- Bastion Host
- Kinds of bastion hosts
- Need for a bastion host
- Basic principles for building a bastion host
- Requirement to setup a Bastion Host
- Hardware requirements
- Selecting an OS for bastion host
- Positioning a Bastion Host
- Network location
- Selecting a Secure Location
- Auditing the Bastion Host
- Connecting the Bastion Host
- Different ways to create a DMZ
- Where to place Bastion host in the DMZ
- Benefits of DMZ
  
- **Module XVII: Proxy Servers**
  - What are Proxy Servers?
  - Benefits of a Proxy server
  - Other benefits of Proxy Server
  - Functioning of a proxy server
  - Proxy Servers, Fire walling and filtering
  - Communication via a Proxy Server
  - Connecting proxy servers
  - Proxy server vs. Packet filters
  - Networking protocols and proxy servers
  - S-HTTP
  - SOCKS
  - Types of Proxy Servers
  - Proxy Server based Firewalls
  - Microsoft Internet Security & Acceleration Server (ISA)
  - Wingate
  - Symantec Enterprise firewall
  - Limitations of a Proxy server
  
- **Module XVIII: Virtual Private Network**
  - What is a VPN?
  - VPN Deployment
  - Tunneling described
  - Types of Tunneling
  - Popular VPN tunneling protocols
  - VPN Security
  - VPN via SSH and PPP
  - VPN via SSL and PPP
  - VPN via concentrator
  - Other methods
  - VPN Registration and Passwords
  - Introduction to IPSec
  - IPSec services
  - Combining VPN and Firewalls
  
- **Module XIX: Wireless Network Security**
  - Introduction to Wireless Networking
  - Basics

- Types of Wireless Network
- Wireless Local Area Network (WLAN)
- Wireless Personal Area Network (WPAN)
- Wireless Metropolitan Area Network (WMAN)
- Wireless Wide Area Network (WWAN)
- Antennas
- SSIDs
- Rogue Access Points
- NetStumbler
- What is Wired Equivalent Privacy (WEP)?
- AirSnort
- 802.11 Wireless LAN Security
- Wireless Transport Layer Security (WTLS)
- Extensible Authentication Protocol (EAP) Methods
- 802.11i
- Wi-Fi Protected Access (WPA)
- TKIP
- Eavesdropping
- Wireless Intrusion Detection System (WIDS)
- Securing Wireless Networks
- Maximum Security
- Part C – Computer Forensics
  
- **Module XX: Computer Forensics fundamentals**
  - Definition of Forensic Science
  - Need for Computer forensics
  - Cyber Crime
  - Examples of cyber crime
  - Cyber Crime Investigation Process
  - Challenges in Cyber Crime Investigation
  - Federal Bureau of Investigation
  - National Infrastructure Protection Center
  - Reporting security breaches to law enforcement
  - What is cyber law?
  - Basic approaches for formulation of cyber laws
  - Cyber laws
  - Federal statutes
  
- **Module XXI: Trademark, copyright and patents**
  - Trademarks
  - Trademark eligibility and benefits of registering it
  - Trademark infringement
  - Trademark Search
  - Copyright and copyright notice
  - Investigating copyright status of a particular work
  - How long does a copyright last?
  - Doctrine of “fair use”
  - How are copyrights enforced?
  - SCO vs. IBM
  - Plagiarism
  - Turnitin
  
- **Module XXII: Network and Router Forensics Fundamentals**
  - Internal Threat
  - External Threat
  - Automated Computer Attack
  - Sources of evidence on a network

- Ethereal
- What is a router?
- Functions of a Router
- Types of Router Attacks
- Denial of service (DoS) attack
- Packet Mistreating Attacks
- Routing Table Poisoning
- Router Forensics vs. Traditional Forensics
- Incident Response
- Investigating Routers
- Accessing the Router
  
- **Module XXIII: Incident response and forensics**
  - Analysis on incident reports
  - Incident
  - How to identify the incident
  - Reporting an incident
  - More about incident reports
  - Incident handling procedure
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Follow Up
  - CSIRT Overview
  - Need for CSIRT
  
- **Module XXIV**
  - Introduction to digital evidence
  - Rules of evidence
  - Evidence life cycle
  - Digital Evidence Investigation process
  - Securing digital evidence
  - Documenting Digital evidence
  - Handling Digital Evidence in a Forensics lab
  - Obtaining digital signatures
  - Processing digital evidence
  - Processing digital evidence
  - Storing Digital Evidence
  - Evidence retention and media storage needs
  - Hex2Text
  - File Date Time Extractor
  
- **Module XV: Understanding Windows, DOS, Linux and Macintosh**
  - Understanding File Systems
  - Types of file systems
  - Exploring Microsoft File Structure
  - Exploring Microsoft File Structure (Contd.)
  - Exploring Microsoft File Structures
  - Gathering Evidence on Windows systems
  - Gathering Volatile evidence
  - Forensic Tool: pslist
  - Forensic Tool: fport
  - Checking Registry
  - Resplendent Registrar 3.30

- How to create a system state backup?
- UNIX overview
- Linux overview
- Exploring Unix/Linux data structures
- Understanding Unix/Linux boot process
- Understanding Linux loader
- Exploring Macintosh boot tasks
  
- **Module XXVI: Steganography**
  - Differences between Steganography and Cryptography
  - Image Steganography
  - Types of Steganography
  - Real World Applications of Steganography
  - Practical Applications of Steganography
  - Unethical use of Steganography
  - The Steganography Tree
  - Hiding Information in text Files
  - Hiding Information In DNA
  - Fort Knox
  
- **Module XXVII: Analyzing logs**
  - Importance of Logs in Forensics
  - Audit incidents
  - Application logs
  - Examining intrusion and security events
  - Logging in Unix/ Linux-Syslog
  - Remote logging
  - Windows logging
  - Remote logging in windows
  - ntsyslog
  - Significance of synchronized time
  - Event gathering
  - EventCombMT
  - Writing scripts
  - Event gathering tools
  - Forensic tool: fwanalog
  
- **Module XXVIII: E-mail crime and Computer Forensics**
  - Understanding Internet protocols
  - Exploring the roles of the client and server in e-mail
  - Identifying e-mail crimes and violation
  - Identifying e-mail crimes and violations
  - Investigating e-mail crime and violation
  - Viewing e-mail headers
  - Examining an E-mail Header
  - Tracing an E-mail Message
  - Using Network Logs related to e-mail
  - Using specialized e-mail forensic tools
  - FINALeMAIL
  - Tracing back
  - Tracing back web based mails
  - Searching e-mail addresses
  - eMailTrackerPro
  
- **XXIX: Reporting**
  - Significance of an investigative report

- Report specifications
  - Report classification (a)
  - Report classification (b)
  - What to include in an Investigative Report?
  - Layout of an investigative report
  - Writing report
  - Investigative report format
  - Report and expert opinion
  - Use of supporting material
  - Importance of consistency
  - Salient features of a good report
- 
- **Module XXX: Computer Forensics as a Profession**
    - Developing Computer Forensics Resources
    - Preparing for Computing Investigations
    - Understanding Enforcement Agency Investigations
    - Understanding Corporate Investigations
    - Maintaining professional conduct
    - Part A - Information Security – Exercises
    - Part B - Network Security – Exercises
    - Part C - Computer Forensics – Exercises