CEH - Certified Ethical Hacker v12 Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

The EC-Council's Certified Ethical Hacker (CEH v12) Training program will enhance your knowledge of essential security fundamentals. Certified Ethical Hacker (CEH V12) certification course is one of the most sought-after security qualifications in the world. This internationally recognized security course validates your ability to discover weaknesses in the organization's network infrastructure and aids in the effective combat of cyber-attacks.

The C|EH v12 program is a specialized, one-of-a-kind training program to teach everything about ethical hacking with hands-on training, labs, assessment, a mock engagement (practice), and a global hacking competition.

This certification is a DoD Approved 8570 Baseline Certification and meets**DoD 8140/8570 training requirements.**

Since the threat in the cyber world is increasing continuously, the industry needs cyber security professionals who prevent threats and attacks in organizations worldwide. The Certified Ethical Hacker (C|EH v12) program is one of the most respected certifications in the cybersecurity field.

The EC-Council has introduced new updated technologies in C|EH v12 program, including the MITRE ATT&CK Framework, Diamond Model of Intrusion Analysis, Techniques for Establishing Persistence, Evading NAC and Endpoint Security, Fog Computing, Edge Computing, and Grid Computing. These updated technologies will prepare you to think like a hacker, so you have the skills to protect your infrastructure.

Bilginç IT Academy is an **Official Accredited Training Partner of EC-Council**, delivering EC-Council-authorized cybersecurity trainings and certification programs globally.

Prerequisites

Basic understanding of network essentials and core concepts, including server and network components.

Target Audience:

- Ethical Hackers
- System Administrators
- Network Administrators
- Engineers
- Web Managers
- Auditors
- Security Professionals

CEH - Certified Ethical Hacker v12 Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

After completing the C|EH v12 certification program, you will have a thorough understanding of:

- Ethical hacking fundamentals, cyber kill chain concepts, an overview of information security, security measures, and numerous information security laws and regulations.
- Footprinting concepts and methodologies, as well as using footprinting tools and countermeasures.
- Enumeration techniques include NFS enumeration and related tools, DNS cache snooping, and DNSSEC Zone walking along with the countermeasures.
- Concepts of vulnerability assessment, its categories and strategies, and first-hand exposure to the technologies used in industry.
- Phases of system hacking, attacking techniques to obtain, escalate, and maintain access on the victim and covering tracks.
- Malware threats, analysis of various viruses, worms, and trojans like Emotet and battling them to prevent data. APT and Fileless Malware concepts have been introduced to this domain.
- Packet sniffing concepts, techniques, and protection against the same.
- Social engineering concepts and related terminologies like identity theft, impersonation, insider threats, social engineering techniques, and countermeasures.
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, use cases, and attack and defense tools.
- Security solutions like firewall, IPS, honeypots, evasion, and protection.
- Operational Technology (OT) essentials, threats, attack methodologies, and attack prevention. The concept of OT is a new addition.
- Recognizing the vulnerabilities in IoT and ensuring the safety of IoT devices.
- Encryption algorithms, Public Key Infrastructure (PKI), cryptographic attacks, and cryptanalysis.
- Cloud computing, threats and security, essentials of container technology, and serverless computing.

Outline

C|EH v12 program is divided into 20 modules:

Module 1: Introduction to Ethical Hacking

Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Key topics covered:

- Elements of Information Security
- Cyber Kill Chain Methodology

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

- MITRE ATT&CK Framework
- Hacker Classes
- Ethical Hacking
- Information Assurance (IA)
- Risk Management
- Incident Management
- PCI DSS
- HIPPA
- SOX
- GDPR

Module 2: Foot Printing and Reconnaissance

Learn how to use the latest techniques and tools to perform foot printing and reconnaissance, a critical pre-attack phase of the ethical hacking process.

Hands-On Lab Exercises:

Over 30 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform foot printing on the target network using search engines, web services, and social networking sites
- Perform website, email, whois, DNS, and network foot printing on the target network

Module 3: Scanning Networks

Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Hands-On Lab Exercises:

Over 10 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform host, port, service, and OS discovery on the target network
- Perform scanning on the target network beyond IDS and firewall

Module 4: Enumeration

Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, plus associated countermeasures.

Hands-On Lab Exercises:

Over 20 hands-on exercises with real-life simulated targets to build skills on how to:

Perform NetBIOS, SNMP, LDAP, NFS, DNS, SMTP, RPC, SMB, and FTP Enumeration

BILGINC IT Academy

info@bilginc.com

bilginc.com

Module 5: Vulnerability Analysis

Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems.

Hands-On Lab Exercises:

Over 5 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform vulnerability research using vulnerability scoring systems and databases
- Perform vulnerability assessment using various vulnerability assessment tools

Module 6: System Hacking

Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks.

Hands-On Lab Exercises:

Over 25 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform an active online attack to crack the system's password
- Escalate privileges using privilege escalationtools
- Escalate privileges in Linux machine
- Hide data using steganography
- Clear Windows and Linux machine logs using various utilities
- Hiding artifacts in Windows and Linux machines

Module 7: Malware Threats

Get an introduction to the different types of malware, such as Trojans, viruses, and worms, as well as system auditing for malware attacks, malware analysis, and countermeasures.

Hands-On Lab Exercises:

Over 20 hands-on exercises with real-life simulated targets to build skills on how to:

- Gain control over a victim machine using malware
- Infect the target system using a virus
- Perform static and dynamic malware analysis

Key topics covered:

- Malware, Components of Malware
- APT
- Trojan
- Types of Trojans
- Exploit Kits
- Virus
- Virus Lifecycle

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Types of Viruses
- Ransomware
- Computer Worms
- Fileless Malware
- Malware Analysis
- Static Malware Analysis
- Dynamic Malware Analysis
- Virus Detection Methods
- Trojan Analysis
- Virus Analysis
- Fileless Malware Analysis
- Anti-Trojan Software
- Antivirus Software
- Fileless Malware Detection Tools

Module 8: Sniffing

Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

Hands-On Lab Exercises:

Over 10 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform MAC flooding, ARP poisoning, MITM and DHCP starvation attack
- Spoof a MAC address of Linux machine
- Perform network sniffing using various sniffing tools
- Detect ARP poisoning in a switch-based network

Key topics covered:

- Network Sniffing
- Wiretapping
- MAC Flooding
- DHCP Starvation Attack
- ARP Spoofing Attack
- ARP Poisoning
- ARP Poisoning Tools
- MAC Spoofing
- STP Attack
- DNS Poisoning
- DNS Poisoning Tools
- Sniffing Tools
- Sniffer Detection Techniques
- Promiscuous Detection Tools

Module 9: Social Engineering

Learn social engineering concepts and techniques, including how to identify theft attempts, audit

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

human-level vulnerabilities, and suggest social engineering countermeasures.

Hands-On Lab Exercises:

Over 4 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform social engineering using Various Techniques
- Spoof a MAC address of a Linux machine
- Detect a phishing attack
- Audit an organization's security for phishing attacks

Key topics covered:

- Social Engineering
- Types of Social Engineering
- Phishing
- Phishing Tools
- Insider Threats/Insider Attacks
- Identity Theft

Module 10: Denial-of-Service

Learn about different Denial-of-Service (DoS) and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

Hands-On Lab Exercises:

Over 5 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform a DoS and DDoS attack on a target host
- Detect and protect against DoS and DDoS attacks

Key topics covered:

- DoS Attack, DDoS Attack
- Botnets
- DoS/DDoS Attack Techniques
- DoS/DDoS Attack Tools
- DoS/DDoS Attack Detection Techniques
- DoS/DDoS Protection Tools

Module 11: Session Hijacking

Understand the various session hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

Hands-On Lab Exercises:

Over 4 hands-on exercises with real-life simulated targets to build skills on how to:

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Perform session hijacking using various tools
- Detect session hijacking

Key topics covered:

- Session Hijacking
- Types of Session Hijacking
- Spoofing
- Application-Level Session Hijacking
- Man-in-the-Browser Attack
- Client-side Attacks
- Session Replay Attacks
- Session Fixation Attack
- CRIME Attack
- Network Level Session Hijacking
- TCP/IP Hijacking
- Session Hijacking Tools
- Session Hijacking Detection Methods
- Session Hijacking Prevention Tools

Module 12: Evading IDS, Firewalls, and Honeypots

Get introduced to firewall, intrusion detection system, and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.

Hands-On Lab Exercises:

Over 7 hands-on exercises with real-life simulated targets to build skills on how to:

- Bypass Windows Firewall
- Bypass firewall rules using tunneling
- Bypass antivirus

Module 13: Hacking Web Servers

Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

Hands-On Lab Exercises:

Over 8 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform web server reconnaissance using various tools
- Enumerate web server information
- Crack FTP credentials using a dictionary attack

Key topics covered:

- Web Server Operations
- Web Server Attacks

- DNS Server Hijacking
- Website Defacement
- Web Cache Poisoning Attack
- Web Server Attack Methodology
- Web Server Attack Tools
- Web Server Security Tools
- Patch Management
- Patch Management Tools

Module 14: Hacking Web Applications

Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.

Hands-On Lab Exercises:

Over 15 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform web application reconnaissance using various tools
- Perform web spidering
- Perform web application vulnerability scanning
- Perform a brute-force attack
- Perform Cross-Site Request Forgery (CSRF) Attack
- Identify XSS vulnerabilities in web applications
- Detect web application vulnerabilities using various web application security tools

Key topics covered:

- Web Application Architecture
- Web Application Threats
- OWASP Top 10 Application Security Risks – 2021
- Web Application Hacking Methodology
- Web API
- Webhooks and Web Shell
- Web API Hacking Methodology
- Web Application Security

Module 15: SQL Injections

Learn about SQL injection attack techniques, injection detection tools, and countermeasures to detect and defend against SQL injection attempts.

Hands-On Lab Exercises:

Over 4 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform an SQL injection attack to extract database information
- Detect SQL injection vulnerabilities using various SQL injection detection tools

Key topics covered:

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- SQL Injection
- Types of SQL injection
- Blind SQL Injection
- SQL Injection Methodology
- SQL Injection Tools
- Signature Evasion Techniques
- SQL Injection Detection Tools

Module 16: Hacking Wireless Networks

Learn about wireless encryption, wireless hacking methodologies and tools, and Wi-Fi security tools

Hands-On Lab Exercises:

Over 3 hands-on exercises with real-life simulated targets to build skills on how to:

- Foot Print a wireless network
- Perform wireless traffic analysis
- Crack WEP, WPA, and WPA2 networks
- Create a rogue access point to capture data packets

Key topics covered:

- Wireless Terminology
- Wireless Networks
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology
- Wi-Fi Encryption Cracking
- WEP/WPA/WPA2 Cracking Tools
- Bluetooth Hacking
- Bluetooth Threats
- Wi-Fi Security Auditing Tools
- Bluetooth Security Tools

Module 17: Hacking Mobile Platforms

Learn about mobile platform attack vectors, Android vulnerability exploits, and mobile security guidelines and tools.

Hands-On Lab Exercises:

Over 5 hands-on exercises with real-life simulated targets to build skills on how to:

- Hack an Android device by creating binary payloads
- Exploit the Android platform through ADB
- Hack an Android device by creating APK file
- Secure Android devices using various Android security tools

Key topics covered:

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Mobile Platform Attack Vectors
- OWASP Top 10 Mobile Risks
- App Sandboxing
- SMS Phishing Attack (SMiShing)
- Android Rooting
- Hacking Android Devices
- Android Security Tools
- Jailbreaking iOS
- Hacking iOS Devices
- iOS Device Security Tools
- Mobile Device Management (MDM)
- OWASP Top 10 Mobile Controls
- Mobile Security Tools

Module 18: IoT Hacking & OT Hacking

Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

Hands-On Lab Exercises:

Over 2 hands-on exercises with real-life simulated targets to build skills on how to:

- Gather information using Online foot printing tools
- Capture and analyze IoT device traffic

Key topics covered:

- IoT Architecture
- IoT Communication Models
- OWASP Top 10 IoT Threats
- IoT Vulnerabilities
- IoT Hacking Methodology
- IoT Hacking Tools
- IoT Security Tools
- IT/OT Convergence (IIOT)
- ICS/SCADA
- OT Vulnerabilities
- OT Attacks
- OT Hacking Methodology
- OT Hacking Tools
- OT Security Tools

Module 19: Cloud Computing

Learn different cloud computing concepts, such as container technologies and server less computing, various cloud-based threats and attacks, and cloud security techniques and tools.

Hands-On Lab Exercises:

Over 5 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform S3 Bucket enumeration using various S3 bucket enumeration tools
- Exploit open S3 buckets
- Escalate IAM user privileges by exploiting misconfigured user policy

Key topics covered:

- Cloud Computing
- Types of Cloud Computing Services
- Cloud Deployment Models
- Fog and Edge Computing
- Cloud Service Providers
- Container
- Docker
- Kubernetes
- Serverless Computing
- OWASP Top 10 Cloud Security Risks
- Container and Kubernetes Vulnerabilities
- Cloud Attacks
- Cloud Hacking
- Cloud Network Security
- Cloud Security Controls
- Cloud Security Tools

Module 20: Cryptography

In the final module, learn about cryptography and ciphers, public-key infrastructure, cryptography attacks, and cryptanalysis tools.

Hands-On Lab Exercises:

Over 10 hands-on exercises with real-life simulated targets to build skills on how to:

- Calculate MD5 hashes
- Perform file and text message encryption
- Create and use self-signed certificates
- Perform email and disk encryption
- Perform cryptanalysis using various cryptanalysis tools

Key topics covered:

- Cryptography
- Encryption Algorithms
- MD5 and MD6 Hash Calculators
- Cryptography Tools
- Public Key Infrastructure (PKI)
- Email Encryption
- Disk Encryption
- Cryptanalysis
- Cryptography Attacks
- Key Stretching

CEH - Certified Ethical Hacker v12 Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com