TechyEdz Solutions

Training | Consulting | Developement | Outsourcing

Ethical Hacker Certified (CEH)

9032803832

9032803832

contact@techyedz.com

www.techyedz.com

Certified Ethical Hacker (CEH)

Course Overview:

Certified Ethical Hacker (CEH) Certification is the most comprehensive course for network security professionals. This globally acceptable certification authenticates the applied knowledge of the network administrators, auditors and professionals from a security perspective. Since this course contents are vendor-neutral, it covers a wide range of network-security concepts. This training will help you to think from the malicious hackers viewpoint but try to penetrate the network, ethically and list out the loopholes and vulnerabilities.

The CEH Certification Course will teach the students about hacking from an entirely practical stand-point following the principle of 'Learning by Doing'. In this course you will be performing all the steps right from scanning and identifying vulnerable targets and gaining access to those systems and suggesting the remedies. The practical approach gives the student an in-depth knowledge about the hacking tools and techniques. The simulated lab environment will demonstrate how actual hackers penetrate through the multi-level defenses of the organization. This course additionally teaches you about the virus creation, DDoS attacks, Intrusion Detection techniques and Social Engineering, apart from the steps of hacking.

Course Outline:

1. Background

Network and Communication Technologies

- Networking technologies (e.g., hardware, infrastructure)
- Web technologies (e.g., web 2.0, skype)
- Systems technologies
- Communication protocols
- Telecommunication technologies
- Mobile technologies (e.g., smartphones)
- Wireless terminologies
- Cloud computing
- Cloud deployment models

Information Security Threats and Attack Vectors

- Malware (e.g., Trojan, virus, backdoor, worms)
- Malware operations
- Information security threats and attack vectors
- Attacks on a system (e.g., DoS, DDoS, session hijacking, webserver and web application attacks, SQL injection, wireless threats)
- Botnet
- Cloud computing threats and attacks
- Mobile platform attack vectors
- Cryptography attacks

Information Security Technologies

- Information security elements
- Information security management (e.g. IA, Defense-in-Depth, incident management)
- Security trends
- Hacking and ethical hacking
- Vulnerability assessment and penetration testing
- Cryptography
- Encryption algorithms
- Wireless encryption
- Bring Your Own Device (BYOD)
- Backups and archiving (e.g., local, network)
- IDS, firewalls, and honeypots

2. Analysis / Assessment

Information Security Assessment and Analysis

- Data analysis
- Systems analysis
- Risk assessments
- Vulnerability assessment and penetration testing
- Technical assessment methods
- Network sniffing
- Malware analysis

Information Security Assessment Process

- Footprinting
- Scanning (e.g., Port scanning, banner grabbing, vulnerability scanning, network discovery, proxy chaining, IP spoofing)
- Enumeration
- System hacking (e.g., password cracking, privilege escalation, executing applications, hiding files, covering tracks)

3. Security

Information Security Controls

- Systems security controls
- Application/file server
- IDS
- Firewalls
- Cryptography
- Disk Encryption
- Network security
- Physical security
- Threat modeling
- Biometrics
- Wireless access technology (e.g., networking, RFID, Bluetooth)
- Trusted networks
- Privacy/confidentiality (with regard to engagement)

Information Security Attack Detection

- Security policy implications
- Vulnerability detection
- IP Spoofing detection
- Verification procedures (e.g., false positive/negative validation)
- Social engineering (human factors manipulation)
- Vulnerability scanning
- Malware detection
- Sniffer detection
- DoS and DDoS detection

- Detect and block rogue AP
- Evading IDS (e.g., evasion, fragmentation)
- Evading Firewall (e.g., firewalking, tunneling)
- Honeypot detection
- Steganalysis

Information Security Attack Prevention

- Defend against webserver attacks
- Patch management
- Encoding schemes for web application
- Defend against web application attacks
- Defend against SQL injection attacks
- Defend against wireless and Bluetooth attacks
- Mobile platforms security
- Mobile Device Management (MDM)
- BYOD Security
- Cloud computing security

4. Tools / Systems / Programs

Information Security Systems

- Network/host based intrusion
- Boundary protection appliances
- Access control mechanisms (e.g., smart cards)
- Cryptography techniques (e.g., IPSec, SSL, PGP)
- Domain name system (DNS)
- Network topologies
- Subnetting
- Routers / modems / switches
- Security models
- Database structures

Information Security Programs

- Operating environments (e.g., Linux, Windows, Mac)
- Anti-malware systems and programs (e.g., anti-keylogger, anti-spyware, anti-

rootkit, anti-trojan, anti-virus)

- Wireless IPS deployment
- Programming languages (e.g. C++, Java, C#, C)
- Scripting languages (e.g., PHP, Javascript)

Information Security Tools

- Network/wireless sniffers (e.g., Wireshark, Airsnort)
- Port scanning tools (e.g., Nmap, Hping)
- Vulnerability scanner (e.g., Nessus, Qualys, Retina)
- Vulnerability management and protection systems (e.g., Founds tone, Ecora)
- Log analysis tools
- Exploitation tools
- Footprinting tools (e.g., Maltego, FOCA, Recon-ng)
- Network discovery tools (e.g., Network Topology Mapper)
- Enumeration tools (e.g., SuperScan, Hyena, NetScanTools Pro)
- Steganography detection tools
- Malware detection tools
- DoS/DDoS protection tools
- Patch management tool (e.g., MBSA)
- Webserver security tools
- Web application security tools (e.g., Acunetix WVS)
- Web application firewall (e.g., dotDefender)
- SQL injection detection tools (e.g., IBM Security AppScan)
- Wireless and Bluetooth security tools
- Android, iOS, Windows Phone OS, and BlackBerry device security tools
- MDM Solutions
- Mobile Protection Tools
- Intrusion Detection Tools (e.g., Snort)
- Hardware and software firewalls (e.g., Comodo Firewall)
- Honeypot tools (e.g., KFSenser)
- IDS/Firewall evasion tools (e.g., Traffic IQ Professional)
- Packet fragment generators
- Honeypot Detection Tools
- Cloud security tools (e.g., Core CloudInspect)
- Cryptography tools (e.g., Advanced Encryption Package)
- Cryptography toolkit (e.g., OpenSSL)
- Disk encryption tools
- Cryptanalysis tool (e.g., CrypTool)

5. Procedures / Methodology

Information Security Procedures

- Cryptography
- Public key infrastructure (PKI)
- Digital signature and Pretty Good Privacy (PGP)
- Security Architecture (SA)
- Service oriented architecture
- Information security incident
- N-tier application design
- TCP/IP networking (e.g., network routing)
- Security testing methodology

Information Security Assessment Methodologies

- Web server attack methodology
- Web application hacking methodology
- SQL injection methodology and evasion techniques
- SQL injection evasion techniques
- Wireless and Bluetooth hacking methodology
- Mobile platform (Android, iOS, Windows Phone OS, and BlackBerry) hacking methodology
- Mobile Rooting and Jailbreaking

6. Regulation / Policy

Information Security Policies/ Laws/Acts

- Security policies
- Compliance regulations (e.g., PCI-DSS, SOX)

Ethics of Information Security

- Professional code of conduct
- Appropriateness of hacking

- **Prerequisites:**

- Participants should have good knowledge and understanding of OS, TCP/IP and Network
- Networking Basics will be an additional advantage to understand the concepts easily

Who can attend:

- Information Security Analyst / Administrator
- Information Assurance (IA) Security Officer
- Information Security Manager / Specialist
- Information Systems Security Engineer / Manager
- Information Security Professionals / Officers
- Information Security / IT Auditors
- Risk / Threat/Vulnerability Analyst
- System Administrators
- Network Administrators and Engineers

Number of hours: 50hrs

Certification: CEH 312-50

Key Features:

- One to One Training
- Online Training
- Fastrack & Normal Track
- Resume Modification
- Mock Interviews
- Video Tutorials
- Materials
- Real Time Projects
- Virtual Live Experience
- Preparing for Certification