Solutions Security Strategies

RC:1270765

SEC-CONCEPTS NETWORKS®

It's Possible

Consultancy | Solutions | Security | Strategies

EC-COUNCIL

CERTIFICATIONS

- CERTIFIED SECURE COMPUTER USER (CSCU)
- CERTIFIED NETWORK DEFENDER (CND)
- CERTIFIED ETHICAL HACKING (CEHV9)
- COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI)
- EC-COUNCIL CERTIFIED SECURITY ANALYST (ECSA)

PROGRAMME GUIDE

EC-COUNCIL CERTIFICATIONS PROGRAMME GUIDE

OVERVIEW

EC-Council certifications validate skills and expertise in the field of IT security. As computer crimes continue to escalate in scale and complexity, organizations are hiring record numbers of trained and certified IT security specialists to combat hackers, malicious attacks and security threats. EC-Council certifications prove your real-world skills and qualifications in today's most demanded computer security domains, including, ethical hacking, computer forensics, network security and penetration testing, helping to move you to the top of the list for a wide range of private and public sector positions in information security.

"To beat a hacker, you need to think like one!" is is the motto of EC-Council's flagship certification - Certified Ethical Hacker (CEH) - and the epitome of its stance on IT security training and certification. EC-Council certification training first teaches you how to "be" a cyber-criminal, because understanding the motivations, tricks and techniques of attackers is the first step in making you the ultimate weapon against attack. EC-Council certifications measure your skills in the latest information security tools, technologies, prevention methods and countermeasures. EC-Council credentials are used by a variety of government organizations - including the National Security Agency and the Department of Defense - to clear government personnel and contractors for privileged access to sensitive data, and recognized worldwide as a trusted indicator of advanced skills and qualifications in the IT security field.

EC-COUNCIL CERTIFICATIONS SALARIES

Average salaries for EC-Council certified professionals:
• ENSA: Network Security Administrator salary: $85,000
• CEH: Certified Ethical Hacker salary: $89,000
• ECSA: Certified Security Analyst salary: $90,000
• LPT: Licensed Penetration Tester salary: $92,000
• CHFI: Computer Hacking Forensic Investigator salary: $96,000
Salary by EC-Council Certificate (USA)
Source: Payscale.com

WHY CHOOSE EC-COUNCIL CERTIFICATIONS?

• EC-Council is a globally accepted information security organization.
• EC-Council provides Completely Vendor Neutral tactical security programs.
• EC-Council certified members earn top salaries by employing the most advanced capabilities.
• To beat a hacker, you must think like one, this is the premise of our flagship certification, the Certified Ethical Hacker, which teaches the tools and techniques of the world's most notorious underground hackers.
• Stay in tune with this rapid changing industry, EC-Council invests millions into R&D across hundreds of experts in each program, equipping global thought leaders and security practitioners with the tools and knowledge to defend what matters.
• EC-Council's cutting edge programs are defining the world of ethical hacking. Recognized by the US Department of Defense, CEH is a premier certification option for US Cyber Defenders. Recognized by the National Security Agency Committee on National Security Standards at every level.
• EC-Council programs cover everything from Novice Computer Security to techniques used in defending critical infrastructure and top secret government networks in the Enclave.
• Certified candidates will be equipped with a plethora of tools through EC-Council's many industry contributions.
• Certified candidates will possess the ability to apply acquired knowledge to secure real assets. Weekly and

Monthly Security Seminars are held at no charge to our members providing continuing education from global thought leaders and best of breed organizations.

• EC-Council provides News Communities through our Hacker Journals Project, Code Red Center provides latest threats and alerts ensuring you are always up on current issues.

• EC-Council even has a private University, Licensed by the NM Department of Higher Education providing a Master's Program in Security Science taking your knowledge and certifications to a globally superior level in a field that requires nothing less to stay secure.

• Learn what over 70,608 other security practitioners and leaders already have, join our base of Certified Members and reap the benefits.

CERTIFIED SECURE COMPUTER USER (CSCU) CERTIFICATION

Course Description

CSCU provides individuals with the necessary knowledge and skills to protect their information assets. This course covers fundamentals of various computer and network security threats such as identity theft, credit card fraud, phishing, virus and backdoors, emails hoaxes, loss of confidential information, hacking attacks, and social engineering.

Exam Information

- Exam name: CSCU (112-12) exam
- Number of questions: 50
- Passing score: 70%
- Test duration: 2 Hours
- Test format: Multiple choice
- Test delivery: EC-Council exam portal

Key Outcomes

- Fundamentals of various computer and network security threats
- Understanding of identity theft, phishing scams, malware, social engineering, and financial frauds
- Learn to safeguard mobile, media and protect data
- Protecting computers, accounts, and social networking profiles as a user
- Understand security incidents and reporting

Course Outline

- Introduction to security
- Securing operating systems
- Malware and antivirus
- Internet security
- Security on social networking sites
- Securing email communications
- Securing mobile devices
- Securing the cloud
- Securing network connections
- Data backup and disaster recovery

CERTIFIED NETWORK DEFENDER (CND) CERTIFICATION

Course Description

CND is the world's most advanced network defense course that covers 14 of the most current network security domains any individuals will ever want to know when they are planning to protect, detect, and respond to the network attacks. The course contains hands-on labs, based on major network security tools and to provide network administrators real world expertise on current network security technologies and operations.

Exam Information

- Exam title: CND
- Exam code: 312-38
- Number of questions: 100
- Duration: 4 hours
- Availability: ECC exam
- Test format: Interactive multiple choice questions

Key Outcomes

- Knowledge on how to protect, detect, and respond to network attacks
- Network defense fundamentals
- Application of network security controls, protocols, perimeter appliances, secure IDS, VPN, and firewall configuration
- Intricacies of network traffic signature, analysis, and vulnerability scanning

Course Outline

- Computer network and defense fundamentals
- Network security threats, vulnerabilities, and attacks
- Network security controls, protocols, and devices
- Network security policy design and implementation
- Physical security
- Host security
- Secure firewall configuration and management
- Secure IDS configuration and management
- Secure VPN configuration and management
- Wireless network defense
- Network traffic monitoring and analysis
- Network risk and vulnerability management
- Data backup and recovery
- Network incident response and management

CERTIFIED ETHICAL HACKER (CEH) CERTIFICATION

Course Description

CEH is the world's most advanced certified ethical hacking course that covers 18 of the most current security domains any individual will ever want to know when they are planning to beef-up the information security posture of their organization. The accredited course provides the advanced hacking tools and techniques used by hackers and information security professionals.

Exam Information

- Number of questions: 125
- Test duration: 4 Hours
- Test format: Multiple choice
- Test delivery: ECC exam, VUE
- Exam prefix: 312-50 (ECC exam), 312-50 (VUE)

Key Outcomes

- Thorough introduction to ethical hacking
- Exposure to threat vectors and counter measures
- Addresses emerging areas of cloud and mobile hacking
- Prepares you to combat Trojans, malware, backdoors and more
- Enables you to hack using mobile

Course Outline

- Introduction to ethical hacking
- Foot printing and reconnaissance
- Scanning networks
- Enumeration
- Sniffing
- System hacking
- Malware threats
- Social engineering
- Denial of service
- Session hijacking
- Hacking web applications
- SQL injection
- Hacking wireless networks
- Hacking web servers
- Hacking mobile platforms
- Evading IDS, Firewalls, and Honeypot
- Cloud computing
- Cryptography

EC-COUNCIL CERTIFIED SECURITY ANALYST (ECSA) CERTIFICATION

Course Description

ECSA is a globally accepted hacking and penetration testing program that covers the testing of modern infrastructures, operating systems, and application environments while teaching the students how to document and write a penetration testing report. This program takes the tools and techniques covered in CEH to next level by utilizing EC-Council's published penetration testing methodology.

Exam Information

Exam:

- Test format: Multiple choice
- Number of Questions: 150
- Passing Score: 70%
- Test Duration: 4 Hours

Penetration testing:

- Complete ECSA Practical Cyber Range Challenges in thirty Days
- Submit report within thirty Days completion of challenges
- Passing Criteria: 70 / 100 (Max)

Key Outcomes

- Introduce to security analysis and penetration testing methodologies
- In-depth vulnerability analysis, network penetration testing from external and internal evading firewalls and ids
- Learn to own web applications and databases, and take over cloud services
- Analyze security of mobile devices and wireless networks
- Present findings in a structured actionable report

Course Outline

- Security analysis and penetration testing methodologies
- TCP IP packet analysis
- Pre-penetration testing steps
- Information gathering methodology
- Vulnerability analysis
- External network penetration testing methodology
- Internal network penetration testing methodology
- Firewall penetration testing methodology
- IDS penetration testing methodology
- Web application penetration testing methodology
- SQL penetration testing methodology
- Database penetration testing methodology
- Wireless network penetration testing methodology
- Mobile devices penetration testing methodology
- Cloud penetration testing methodology
- Report writing and post-test actions

COMPUTER HACKING AND FORENSIC INVESTIGATOR (CHFI) CERTIFICATION

Course Description

CHFI is a comprehensive course covering major forensic investigation scenarios, enabling students to acquire hands-on experience. The program provides a strong baseline knowledge of key concepts and practices in the digital forensic domains relevant to today's organizations. Moreover, CHFI provides firm grasp on the domains of digital forensics.

Exam Information

- Number of Questions: 150
- Passing Score: 70%
- Test Duration: 4 hours
- Test Format: Multiple choice
- Test Delivery: ECC exam portal

Key Outcomes

- Comprehensive forensics investigation process
- Forensics of file systems, operating systems, network and database, websites, and email systems
- Techniques for investigating on cloud, malware, and mobile
- Data acquisition and analysis as well as anti-forensic techniques
- Thorough understanding of chain of custody, forensic report, and presentation

Course Outline

- Computer forensics in today's world
- Computer forensics investigation process
- Understanding hard disks and file systems
- Defeating anti-forensics techniques
- Operating system forensics
- Network forensics
- Investigating web attacks
- Database forensics
- Cloud forensics
- Malware forensics
- Investigating email crimes
- Mobile forensics
- Forensics report writing and presentation
- Data Acquisition and Duplication

EC-COUNCIL LICENSED PENETRATION TESTER (LPT) MASTER CERTIFICATION

Course Description

The LPT (Master) credential is the World's first Online, Remotely Proctored Penetration Testing exam developed in close collaboration with SMEs and practitioners around the world after a thorough job role, job task, and skills-gap analysis.

The LPT (Master) practical exam is the capstone to EC-Council's entire information security track, right from the CEH to the ECSA Program. The LPT (Master) exam covers the entire Penetration Testing process and lifecycle with keen focus on report writing, required to be a true professional Penetration Tester.

Exam Information

- Exam duration: 18 hours (Three progressive level exams for six hour duration each)
- Passing Criteria: Achieve a minimum of 5 out of 9 challenges across 3 progressive levels
- Exam Format: Completely Hands-On
- Exam delivery: EC-Council remote proctoring service

Key Outcomes

LPT (Master) demonstrates:

Mastery of Penetration Testing skills

- A consistent, repeatable and measurable approach to Penetration Testing
- Commitment to code of ethics
- Ability to present analyzed results through professional reports