EC-Council Certified Security Analyst-Licensed Penetration Tester

Duration: 5 Days Course Code: ECSA-LPT Version: 9.0

Overview:

The ECSA course provides you with a real world hands-on penetration testing experience and is a globally accepted hacking and penetration testing class available 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.
The ECSA program takes the tools and techniques you learned in the Certied Ethical Hacker course (CEH) and elevates your ability into full exploitation by teaching you how to apply the skills learned in the CEH by utilizing EC-Council's published penetration testing methodology.
It is a highly interactive, comprehensive, standards-based and methodology intensive training program 5-day security class which teaches information security professionals to conduct real life penetration tests.
As the ECSA course is a fully hands-on program, the exercises cover real world scenario. By practicing the skills that are provided to you in the ECSA class, we are able to bring you up to speed with the latest threats that organizations may be vulnerable to.
This course is the part of the Information Security Track of EC-Council. This is a "Professional" level course, with the Certified Ethical Hacker course being the "Core" and the Licensed Penetration Tester being the "Master" level certication.

Target Audience:

Ethical Hackers, Penetration Testers Network server administrators, Firewall Administrators, Security Testers, System Administrators and Risk Assessment professionals.

Objectives:

- The ECSAV9 penetration testing course is designed to enhance the skills based competency of a penetration tester. This course is intensively hands-on and a tremendous amount of emphasis is placed on the practical competency of the student.
- To become eligible, a student must conduct a detailed penetration test through the EC-Council Cyber Range iLabs environment and submit a written report via EC-Council's ASPEN system.
- Only candidates that successfully complete the penetration test in the Cyber Range iLabs environment are allowed to challenge the ECSA exam.
- You will conduct a penetration test on a company that has various departments, subnets and servers, and multiple operating systems with defense mechanisms architecture that has both militarized and non-militarized zones.
- The design of the course is such that the instructor in the class will actually take you through the core concepts of conducting a penetration test based on EC-Council's published penetration testing methdology and guide you through the report writing process for this organization.

Prerequisites:

Testing and Certification

The ECSA exam aims to test a candidate's knowledge and application of critical penetration testing methodologies.The exam requires a candidate to perform real-world penetration testing over EC-Council's secure cyber-range and to produce a penetration testing report which clearly document the vulnerabilities found. This report will be graded by our professionals. Candidates that successfully submit an acceptable report will proceed on to a multiple choice exam that tests a candidates knowledge. Candidates that successfully submit an acceptable report and the pass the multiple choice exam will be awarded the ECSA credential.

The ECSAv9 exam includes 2 required stages.

1. Report writing stage requires candidates to perform various penetration testing exercises on EC-Council's iLabs before submitting a pentest report to EC-Council for assessment. Candidates that submit reports to the required standards will be provided with exam

vouchers for the multiple choice exam.

2. Multiple choice exams are proctored online through the EC-Council Exam portal or VUE:

- Credit Towards Certication: ECSA v9
- Number of Questions: 150
- Passing Score: 70%
- Test Duration: 4 hours

Content:

Core Modules

- 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

Self-Study Modules

- Password Cracking Penetration Testing
- Router and Switches Penetration Testing
- Denial-of-Service Penetration Testing
- Stolen Laptop, PDAs and Cell Phones Penetration Testing
- Source Code Penetration Testing
- Physical Security Penetration Testing
- Surveillance Camera Penetration Testing
- VoIP Penetration Testing
- VPN Penetration Testing
- Virtual Machine Penetration Testing
- War Dialing
- Virus and Trojan Detection
- Log Management Penetration Testing
- File Integrity Checking
- Telecommunication and Broadband Communication Penetration Testing
- Email Security Penetration Testing
- Security Patches Penetration Testing
- Data Leakage Penetration Testing
- SAP Penetration Testing
- Standards and Compliance
- Information System Security Principles
- Information System Incident Handling and Response
- Information System Auditing and Certication

Note: Self-study modules are available in ASPEN portal

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.be