EC-COUNCIL CERTIFIED SECURITY ANALYST V.10

DURATION: 5 DAYS

COURSE OVERVIEW

The ECSA program offers a seamless learning progress continuing where the CEH program left off.

The new ECSAv10 includes updated curricula and an industry recognized comprehensive step-by step penetration testing methodology. This allows a learner to elevate their ability in applying new skills learned through intensive practical labs and challenges.

Unlike most other pen testing programs that only follow a generic kill chain methodology; the ECSA presents a set of distinguishable comprehensive methodologies that are able to cover different pen testing requirements across different verticals.

It is a highly interactive, comprehensive, standards based, intensive 5-days training program that teaches information security professionals how professional real-life penetration testing are conducted.

Building on the knowledge, skills and abilities covered in the new CEH v10 program, we have simultaneously re-engineered the ECSA program as a progression from the former.

Organizations today demand a professional level pen testing program and not just pen testing programs that provide training on how to hack through applications and networks.

Such professional level programs can only be achieved when the core of the curricula maps with and is compliant to government and/or industry published pen testing frameworks

This course is a part of the VAPT Track of EC-Council. This is a “Professional” level course, with the Certified Ethical Hacker being the “Core” and the Licensed Penetration Tester being the “Master” level certification.

In the new ECSAv10 course, students that passes the knowledge exam are given an option to pursue a fully practical exam that provides an avenue for them to test their skills, earning them the ECSA (Practical) credential. This new credential allows employers to validate easily the skills of the student.

TARGET AUDIENCE

Ethical Hackers, Penetration Testers, Security Analysts, Security Engineers, Network Server Administrators, Firewall Administrators, Security Testers, System Administrators, and Risk Assessment Professionals.

COURSE CONTENT

1. Introduction to Penetration Testing and Methodologies
2. Penetration Testing Scoping and Engagement Methodology
3. Open Source Intelligence (OSINT) Methodology
4. Social Engineering Penetration Testing Methodology
5. Network Penetration Testing Methodology - External
6. Network Penetration Testing Methodology - Internal
7. Network Penetration Testing Methodology - Perimeter Devices
8. Web Application Penetration Testing Methodology
9. Database Penetration Testing Methodology
10. Wireless Penetration Testing Methodology
11. Cloud Penetration Testing Methodology
12. Report Writing and Post Testing Actions
13. Self-Study Modules

Professional penetration testers are required to continue learning throughout their career, keeping closely engaged to the fast changing cybersecurity industry. To enable continuous learning, the ECSA course comes packed with tons to self-study resources.

1. Penetration Testing Essential Concepts This is an Essential Prerequisite as it helps you to prepare you the ECSA courseware. Serves as a base to build Advanced Pen Testing Concepts
2. Password Cracking Penetration Testing
3. Denial-of-Service Penetration Testing
4. Stolen Laptop, PDAs and Cell Phones Penetration Testing
5. Source Code Penetration Testing 6. Physical Security Penetration Testing
6. Surveillance Camera Penetration Testing
7. VoIP Penetration Testing
8. VPN Penetration Testing
9. Virtual Machine Penetration Testing

10. War Dialing
11. Virus and Trojan Detection
12. Log Management Penetration Testing
13. File Integrity Checking
14. Telecommunication and Broadband Communication Penetration Testing
15. Email Security Penetration Testing
16. Security Patches Penetration Testing
17. Data Leakage Penetration Testing
18. SAP Penetration Testing
19. Standards and Compliance
20. Information System Security Principles
21. Information System Incident Handling and Response
22. Information System Auditing and Certification

TEST CERTIFICATION

The ECSA exam aims to test a candidate's knowledge and application of critical penetration testing methodologies.

Candidates that successfully pass the multiple-choice exam will be awarded the ECSA credential.

As a powerful addition to the ECSA exam, the new ECSA (Practical) exam is now available adding even more value to the ECSA certification.