E|CSA™
CERTIFIED SECURITY ANALYST

EC-Council

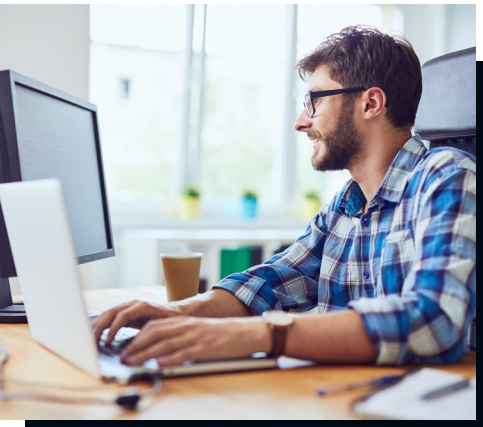
RSA®

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 pentesting 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 pentesting program and not just pentesting 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 pentesting 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 pass 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.

WHO'S IT FOR?

- Ethical Hackers
- Penetration Testers
- Network Server Administrators
- Firewall Administrators
- Security Testers
- System Administrators and Risk Assessment professionals

COURSE OUTLINE

- Module 00: Penetration Testing Essential Concepts (Self-Study)
- Module 01: Introduction to Penetration Testing and Methodologies
- Module 02: Penetration Testing Scoping and Engagement Methodology
- Module 03: Open-Source Intelligence (OSINT) Methodology
- Module 04: Social Engineering Penetration Testing Methodology
- Module 05: Network Penetration Testing Methodology – External
- Module 06: Network Penetration Testing Methodology – Internal
- Module 07: Network Penetration Testing Methodology – Perimeter Devices
- Module 08: Web Application Penetration Testing Methodology
- Module 09: Database Penetration Testing Methodology
- Module 10: Wireless Penetration Testing Methodology
- Module 11: Cloud Penetration Testing Methodology
- Module 12: Report Writing and Post Testing Actions

EXAM INFORMATION

CREDIT TOWARDS CERTIFICATION: ECSA
NUMBER OF QUESTIONS: 150

DURATION: 4 hours

TEST FORMAT: Multiple Choice

TEST DELIVERY: ECC Exam Portal

Contact us at:
RSAU@rsa.com