EC-COUNCIL CERTIFIED SECURITY ANALYST V.10

sanisoft
information technologies

**Well Trained People,
Better Served Customers.**

COURSE OVERVIEW

EC-Council Certified Security Analyst V.10 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-bystep 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 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.

DURATION: 40 HOURS | EXAM CODE: ECSA

COURSE OBJECTIVE

The ECSA pentest program takes the tools and techniques you learned in the Certified 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

- Focuses on pentesting methodology with an emphasis on hands-on learning
- The exam will now have a prerequisite of submitting a pentesting report
- The goal of these changes is to make passing ECSA more difficult; therefore making it a more respected certification

COURSE PREREQUISITES

- While the Certified Security Analyst Training v10 certification is not a prerequisite for the ECSA course, we strongly advise candidates to take the Certified Ethical Hacker v10 course to attain the CEH prior to the commencement of the ECSA course.

COURSE OUTLINE

- Introduction to Penetration Testing and Methodologies
- Penetration Testing Scoping and Engagement Methodology
- Open Source Intelligence (OSINT) Methodology
- Social Engineering Penetration Testing Methodology
- Network Penetration Testing Methodology – External
- Network Penetration Testing Methodology – Internal
- Network Penetration Testing Methodology – Perimeter Devices
- Web Application Penetration Testing Methodology
- Database Penetration Testing Methodology
- Wireless Penetration Testing Methodology
- Cloud Penetration Testing Methodology
- Report Writing and Post Testing Actions
- Self-Study Modules

TARGET AUDIENCE

- Network Administrators
- Network security Administrators
- Network Security Engineer
- Network Defense Technicians
- CND Analyst
- Security Analyst
- Security Operator
- Anyone who involves in network operations

SaniSoft
information technologies

410, AL-DANA CENTER, AL MAKTOUM ROAD DEIRA, DUBAI, UAE

+971 55 3575426 +971 4 2238786 training@sanisoft-it.com