ECSA – Certified Security Analyst v10

EC-Council

Com certificação

- **Nível:** Avançado
- **Duração:** 40h

Sobre o curso

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

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.

A Security Credential Like No Other!

The ECSA penetration testing 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 pentest program takes the tools and techniques you learned in the Certified Ethical Hacker course (CEH) and enhances 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 focuses on pentesting methodology with an emphasis on hands-on learning

Destinatários

- Ethical Hackers

- Penetration Testers
- Network server administrators
- Firewall Administrators
- Security Testers
- System Administrators and Risk Assessment professionals

Metodologia

The ECSA course is a fully hands-on program with labs and exercises that cover real world scenarios. By practicing the skills that are provided to you in the ECSA class, we are able to bring you up to speed with the skills to uncover the security threats that organizations are vulnerable to.

This can be achieved effectively with the EC-Council iLabs Cyber Range. It allows you to dynamically access a host of Virtual Machines preconfigured with vulnerabilities, exploits, tools, and scripts from anywhere with an internet connection.

Our guided step-by-step labs include exercises with detailed tasks, supporting tools, and additional materials as well as our state-of-the-art “Open Environment” allowing you to launch a complete live range open for any form of hacking or testing.

Programa

- Penetration Testing Essential Concepts (Self-Study)
- 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