QUICKSTART
Over 35 Years Of Technology Training

Document Generated: 06/30/2024

Learning Style: On Demand

Provider: EC-Council

Difficulty: Intermediate

Course Duration: 32 Hours

Certified Security Analyst (ECSA)

What's Included:

- *Official EC Council Training Videos*
- *Official EC Council Courseware included*
- *Official EC Council ilabs subscription (6 months)*
- *EC Council Exam Voucher with Remote Proctoring Service included*

About this Course:

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.

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.

Course Objectives:

- Identify security issues in network design and implementation
- Detect security issues in web applications that exists due to insecure design and development practices
- Identify employees that do not properly authenticate, follow, validate, handle, the processes and technology
- Identify misconfigurations in organization’s wireless infrastructure including WLAN, Mobile,
- Determine security issues in organization’s cloud infrastructure
- Identify security issues in the configuration of database server and their instances

Audience:

- 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

Credly Badge:

Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges