EC-Council Certified Security Analyst (ECSA)

Introduction

The EC-Council Certified Security Analyst Certification is an advanced security certification that complements the Certified Ethical Hacker (CEH) certification by validating the analytical phase of ethical hacking. An ECSA is a step ahead of a CEH by being able to analyze the outcome of hacking tools and technologies.

Key Outcomes

- Introduction to security analysis and penetration testing methodologies
- In-depth vulnerability analysis, network penetration testing from external and internal evading firewalls and IDS
- Learn to own web applications and databases, and take over cloud services
- Analyze the security of mobile devices and wireless networks
- Present findings in a structured actionable report

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

Prerequisites

Knowledge of Certified Ethical Hacker (CEH)

Target Audience

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

Duration

24 hours training course