EC-Council Certified Security Analyst | ECSA (Practical)

Introduction

EC-Council Certified Security Analyst (Practical) is a 12-hour, rigorous practical exam built to test the candidate's penetration testing skills. The candidates are required to demonstrate the applications of the penetration testing methodology that is taught in the ECSA program. Moreover, the candidate is also required to perform a comprehensive security audit of an organization, just like in the real world. Starting with challenges requiring to perform advanced network scans beyond perimeter defenses, leading to automated and manual vulnerability analysis, exploit selection, customization, launch, and post-exploitation maneuvers.

Key Outcomes

This course teaches you about core aspects such as:

- Threat and exploit research, understand exploits in the wild and customize payloads.
- Creating a professional pen testing report with essential elements

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

Prerequisites

No formal prerequisites are there but it is strongly recommended that the candidate attempt the ECSA (Practical) exam only if he/she has attended the ECSA course/equivalent training.

Target Audience

This certification program is intended for;

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

Duration

24 hours training course