Course Outline

Certified Security Analyst

Duration: 5 day (30 hours)

Introduction

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

Target Audience:

Network server administrators, firewall administrators, information security analysts, system administrators, and risk assessment professionals all benefit from the ECSA program.

Topics Covered:

- Security Analysis and Penetration Testing Methodologies
- TCP IP Packet Analysis
- Pre-penetration Testing Steps
- Information Gathering Methodology
- Vulnerability Analysis
- External Network Penetration Testing Methodology
- Internal Network Penetration Testing Methodology
- Firewall Penetration Testing Methodology
- IDS Penetration Testing Methodology
- Web Application Penetration Testing Methodology
- SQL Penetration Testing Methodology
- Database Penetration Testing Methodology
- Wireless Network Penetration Testing Methodology
- Mobile Devices Penetration Testing Methodology
- Cloud Penetration Testing Methodology
- Report Writing and Post Test Actions