EC-Council Certified Security Analyst (ECSA) v9.0

Students will conduct a penetration test on a company that has various departments, subnets and servers, and multiple operating systems with defense mechanisms architecture that has both militarized and non-militarized zones.

Length Days: 5 | Length Hours: 40

TARGET AUDIENCE

Ethical Hackers, Penetration Testers, Network Server Administrators, Firewall Administrators, Security Testers, System Administrators and Risk Assessment Professionals.

COURSE OBJECTIVES

To be eligible to attempt the exam, candidates are required to perform real-world penetration testing over EC-Council's secure cyber range and to produce a penetration test report that clearly documents the vulnerabilities found. This report will be graded by EC-Council. Candidates that successfully submit an acceptable report will proceed on to a multiple-choice exam that tests a candidate's knowledge. Candidates that successfully pass the multiple-choice exam will be awarded the ECSA credential.

COURSE OUTLINE

- 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
- DS 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