ECSA™
EC-Council Certified Security Analyst

# EC-Council Certified Security Analyst (ECSA)

## Course Description

ECSA is a globally accepted hacking and penetration testing program that covers the testing of modern infrastructures, operating systems, and application environments while teaching the students how to document and write a penetration testing report.

This program takes the tools and techniques covered in CEH to next level by utilizing EC-Council's published penetration testing methodology.

## Key Outcomes

- Introduce 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 security of mobile devices and wireless networks
- Present findings in a structured actionable report

## Exam Information

**Exam:**

- Test format: Multiple choice
- Number of Questions: 150
- Passing Score: 70%
- Test Duration: 4 Hours

**Penetration testing:**

- Complete ECSA Practical Cyber Range Challenges in thirty Days
- Submit report within thirty Days completion of challenges
- Passing Criteria: 70 / 100 (Max)

## 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
- 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