
Authorized Training Center

CISCO

ORACLE APPROVED EDUCATION CENTER

Microsoft GOLD CERTIFIED Partner

# Ec-council Certified Security Analyst ECSA - Version 8 Course
# 36 Contact Hours

## Course Overview:

The EC–Council Security Analyst (ECSA) program is a comprehensive, standards-based, methodology intensive training program which teaches information security professionals to conduct real life penetration tests by utilizing EC-Council's published penetration testing methodology.

The ECSA Program is a 5-day complete hands-on training program. This Penetration Testing training course uses real-time scenarios to train students in penetration testing methodologies.

EC-Council's Certified Security Analyst (ECSA) course will help you master a documented penetration testing methodology that is repeatable and that can be used in a penetration testing engagement, globally.

## Who Should Attend:

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

## Exam Informaiton:

Credit Towards Certification: ECSA
Number of Questions: 150
Passing Score: 70%
Test Duration: 4 hours
Test Format: Multiple Choice
Test Delivery: Prometric Online Web site

Legal Agreement
Ethical Hacking or ECSA and Countermeasures course mission is to educate, introduce and demonstrate hacking tools for penetration testing purposes only. Prior to attending this course, you will be asked to sign an agreement stating that you will not use the newly acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to compromise any computer system, and to indemnify EC-Council with respect to the use or misuse of these tools, regardless of intent.

Not anyone can be a student — the Accredited Training Centers (ATC) will make sure the applicants work for legitimate companies.


Authorized Training Center

CISCO

ORACLE APPROVED EDUCATION CENTER

Microsoft GOLD CERTIFIED Partner

## Course Outline:

ECSA V8 Curriculum consists of instructor led training and self-study. The Instructor will provide the details of self-study modules to the students beginning of the class.

**Core Modules**

1. Need for Security Analysis
2. TCP IP Packet Analysis
3. Penetration Testing Methodologies
4. Customers and Legal Agreements
5. Rules of Engagement
6. Penetration Testing Planning and Scheduling
7. Pre-penetration Testing Steps
8. Information Gathering
9. Vulnerability Analysis
10. External Penetration Testing
11. Internal Network Penetration Testing
12. Firewall Penetration Testing
13. IDS Penetration Testing
14. Password Cracking Penetration Testing
15. Social Engineering Penetration Testing
16. Web Application Penetration Testing
17. SQL Penetration Testing
18. Penetration Testing Reports and Post Testing Actions

**Self-Study Modules**

19. Router and Switches Penetration Testing
20. Wireless Network Penetration Testing
21. Denial-of-Service Penetration Testing
22. Stolen Laptop, PDAs and Cell Phones Penetration Testing
23. Source Code Penetration Testing
24. Physical Security Penetration Testing
25. Surveillance Camera Penetration Testing
26. Database Penetration Testing
27. VoIP Penetration Testing
28. VPN Penetration Testing
29. Cloud Penetration Testing
30. Virtual Machine Penetration Testing
31. War Dialing
32. Virus and Trojan Detection
33. Log Management Penetration Testing
34. File Integrity Checking




35. Mobile Devices Penetration Testing
36. Telecommunication and Broadband Communication

**Penetration Testing**

37. Email Security Penetration Testing
38. Security Patches Penetration Testing
39. Data Leakage Penetration Testing
40. SAP Penetration Testing
41. Standards and Compliance
42. Information System Security Principles
43. Information System Incident Handling and Response
44. Information System Auditing and Certification