BULLETPROOF
Education Services

EC-Council Certified Security Analyst (ECSA) v10.0

The ECSA pentest program takes the tools and techniques you learned in the Certified Ethical Hacker course (CEH) and enhances 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. It focuses on pentesting methodology with an emphasis on hands-on learning.

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

The ECSA penetration testing course provides students with a real world hands-on penetration testing experience and is a globally accepted hacking and penetration testing class available that covers the testing of modern infrastructures, operating systems and application environments while teaching students how to document and write a penetration testing report.

COURSE OUTLINE

1 - PENETRATION TESTING ESSENTIAL CONCEPTS (SELF-STUDY)
2 - INTRODUCTION TO PENETRATION TESTING AND METHODOLOGIES
3 - PENETRATION TESTING SCOPING AND ENGAGEMENT METHODOLOGY
4 - OPEN-SOURCE INTELLIGENCE (OSINT) METHODOLOGY
5 - SOCIAL ENGINEERING PENETRATION TESTING METHODOLOGY
6 - NETWORK PENETRATION TESTING METHODOLOGY - EXTERNAL
7 - NETWORK PENTETRATION TESTING METHODOLOGY - INTERNAL
8 - NETWORK PENETRATION TESTING METHODOLOGY - PERIMETER DEVICES
9 - WEB APPLICATION PENETRATION TESTING METHODOLOGY
10 - DATABASE PENETRATION TESTING METHODOLOGY
11 - WIRELESS PENETRATION TESTING METHODOLOGY
12 - CLOUD PENETRATION TESTING METHODOLOGY
13 - REPORT WRITING AND POST TESTING ACTIONS