301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

View Full Course Details including Latest Schedule Online

EC-COUNCIL

ECSA Certification Training

Course Overview

Our 5-day instructor-led EC-Council ECSA (EC-Council Certified Security Analyst) training and certification boot camp in Washington, DC Metro, Tysons Corner, VA, Columbia, MD or Live Online is designed to provide students with hands-on penetration testing experience. The ECSA v10 penetration training course enhances the skills of a penetration tester. The instructor will take students through the core concepts of conducting a penetration test based on EC-Council's published penetration testing methodology and guide you through the report writing process for the organization.

Course Outline

Penetration Testing Essential Concepts

- Computer network fundamentals
- TCP/IP protocol suite
- IP addressing and port numbers
- Network terminology
- Network security controls
- Network security devices
- Network File System (NFS)
- Windows security
- Unix/Linux security
- Virtualization
- Web server
- Web application
- Web markup and programming languages
- Application development frameworks and their vulnerabilities
- Web API's
- Web sub components
- Web application security mechanisms
- Working of most common information security attacks
- Information security standards, laws and acts

PhoenixTS

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Introduction to Penetration Testing and Methodologies

- What is penetration testing?
- Benefits of conducting a penetration test
- ROI for penetration testing
- How penetration testing differs from ethical hacking?
- Comparing security audit, vulnerability assessment, and penetration testing
- Types of penetration testing
- Penetration testing: cost and comprehensiveness
- Selecting an appropriate testing type
- Different ways of penetration testing
- Selecting the appropriate way of penetration testing
- Common areas of penetration testing
- Penetration testing process
- Penetration testing phases
- Penetration testing methodologies
- Need for a methodology
- LPT penetration testing methodology
- Penetration testing essentials

Penetration Testing Scoping and Engagement Methodology

- Penetration testing: pre-engagement activities
- Pre-engagement activities
- Request for Proposal (RFP)
- Preparing response requirements for proposal submission
- Setting the Rules of Engagement (ROE)
- Establishing communication lines: identify the details of the key contact
- Timeline
- Time/location
- Frequency of meetings
- Time of day
- Identify who can help you?
- ROE document
- Handling the legal issues in penetration testing engagement
- Penetration testing contract
- Preparing for test
- Handling scope creeping during pen test

Open-Source Intelligence (OSINT) Methodology

- OSINT gathering steps
- OSINT through the world wide web
- OSINT through website analysis
- OSINT through DNS interrogation
- Automating your OSINT effort using tools/frameworks/scripts

Social Engineering Penetration Testing Methodology

- Social engineering penetration testing
- Skills required to perform social engineering pen test
- Common targets of social engineering pen test
- Do remember: before social engineering pen test
- Black box or white box?
- Social engineering penetration testing steps
- Social engineering penetration testing using e-mail attack vector
- Social engineering penetration testing using telephone attack vector
- Social engineering penetration testing using physical attack vector

Network Penetration Testing Methodology – External

- Network penetration testing
- External vs internal penetration testing
- External network penetration testing
- Internal network penetration testing
- Network penetration testing process
- White, black, or grey-box network penetration testing?
- External network penetration testing steps
- Port scanning
- OS and service fingerprinting
- Vulnerability research
- Exploit verification

Network Penetration Testing Methodology – Internal

- Internal network penetration testing
- Why internal network penetration testing?
- Internal network penetration testing steps

- Footprinting
- Network scanning
- OS and service fingerprinting
- Enumeration
- Vulnerability assessment
- Windows exploitation
- Unix/Linux exploitation
- Other internal network exploitation techniques
- Automating internal network penetration test effort
- Post exploitation

Network Penetration Testing Methodology – Perimeter Devices

- Steps for firewall penetration testing
- Steps for IDS penetration testing
- Steps for router penetration testing
- Steps for switch penetration testing
- Assessing firewall security implementation
- Assessing IDS security implementation
- Assessing security of routers
- Assessing security of switches

Web Application Penetration Testing Methodology

- White box or black box?
- Web application penetration testing
- Web application security frame
- Security frame vs vulnerabilities vs attacks
- Web application penetration testing steps
- Discover web application default content
- Discover web application hidden content
- Conduct web vulnerability scanning
- Identify the attack surface area
- Tests for SQL injection vulnerabilities
- Tests for XSS vulnerabilities
- Tests for parameter tampering
- Tests for weak cryptography vulnerabilities
- Tests for security misconfiguration vulnerabilities
- Tests for client-side scripting attack
- Tests for broken authentication and authorization vulnerabilities
- Tests for broken session management vulnerabilities
- Test for web services security

- Tests for business logic flaws
- Tests for web server vulnerabilities
- Tests for thick clients vulnerabilities

Database Penetration Testing Methodology

- Database penetration testing steps
- Information reconnaissance
- Database enumeration: Oracle
- Database enumeration: MS SQL Server
- Database enumeration: MySQL
- Vulnerability and exploit research
- Database exploitation: Oracle
- Database exploitation: MS SQL Server
- Database exploitation: MySQL

Wireless Penetration Testing Methodology

- Wireless penetration testing
- WLAN penetration testing steps
- RFID penetration testing steps
- NFC penetration testing steps
- Mobile device penetration testing steps
- IoT penetration testing steps
- Wireless Local Area Network (WLAN) penetration testing
- RFID penetration testing
- NFC penetration testing
- Mobile device penetration testing
- IoT penetration testing

Cloud Penetration Testing Methodology

- Distribution of public cloud services: AWS, Azure, Google Clouds are on TOP among others
- Cloud computing security and concerns
- Security risks involved in cloud computing
- Role of penetration testing in cloud computing
- Do remember: cloud penetration testing
- Scope of cloud pen testing
- Cloud penetration limitations
- Cloud specific penetration testing
- Cloud reconnaissance

- Identify the type of cloud to be tested
- Identify what to be tested in the cloud environment
- Identify the tools for penetration test
- Identify what allowed to be tested in cloud environment
- Identify which tests are prohibited
- AWS's provision for penetration testing
- Azure's provision for penetration testing
- Google Cloud's provision for penetration testing
- Identify date and time for penetration test
- Cloud specific penetration testing
- Recommendations for cloud testing

Report Writing and Post Testing Actions

- Penetration testing deliverables
- Goal of the penetration testing report
- Types of pen test reports
- Characteristics of a good pen testing report
- Writing the final report
- Document properties/version history
- Table of contents/final report
- Summary of execution
- Scope of the project
- Evaluation purpose/system description
- Assumptions/timeline
- Summary of evaluation, findings, and recommendations
- Methodologies
- Planning
- Exploitation
- Reporting
- Comprehensive technical report
- Result analysis
- Recommendations
- Appendices
- Sample appendix
- Penetration testing report analysis
- Report on penetration testing
- Pen test team meeting
- Research analysis
- Pen test findings
- Rating findings
- Analyze
- Prioritize recommendations

- Delivering penetration testing report
- Cleanup and restoration
- Report retention
- Sign-off document template
- Post-testing actions for organizations

EC-Council ECSA v10 Certification Exams

ECSA v10 Knowledge Exam Details

- Number of Questions – 150
- Passing Score – 70%
- Duration – 4 hours
- Format – multiple choice
- Delivery – Prometric and Pearson Vue

ECSA v10 Practical Exam Details

- Exam name – EC-Council Certified Security Analyst (Practical)
- Number of Challenges – 8
- Duration- 12 hours
- Format – iLabs cyber range
- Passing Score – 5 out of 8 challenges and the submission of an acceptable penetration testing report

**The ECSA v10 Practical exam requires a $100 non-refundable if you do not hold one of the following certifications in good standing: CEH, ECSA, or CHFI*

ECSA v10 Certification Training FAQs

What is the recommended experience for the ECSA v10 certification training course?

It is recommended that candidates for the ECSA v10 certification should have at least one of the following:
– a EC-Council Certified Ethical Hacker certification in good standing
– At least two years of experience working in the information security industry
– Another relevant industry certification, such as Offensive Security Certified Professional (OSCP) or GIAC Penetration Tester (GPEN)

Who is the ECSA v10 Certification designed for?

The certification is designed for individuals with the following job role/title:
– Ethical Hackers
– Penetration Testers
– Security Analysts
– Security Engineers
– Network Server Administrators
– Firewall Administrators
– Security Testers
– System Administrators
– Risk Assessment Professionals

When was the ECSA Certification last updated?

EC-Council regularly updates their certifications to keep up with industry trends. The ECSA certification was updated to version 10 in 2018. You can read more about the latest version of the ECSA certification in this blog post : ECSA v10 vs v9: What's New on the Certification Exam

Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

Included in this **ECSA Certification Training** course

- 5-Day Training with an ECSA Certified Instructor
- Official EC-Council ECSA courseware
- Pre and Post Assessments
- Complete the ECSA Practical Packet During Class
- Onsite ECSA Exam Scheduling
- Certificate of Completion for up to 40 CEUs/CPEs to be used toward renewing relevant certifications

- ECSA Course Retake Guarantee
- EC-Council Training Center of the Year
- EC-Council Authorized Training Course
- Notepad, pen and highlighter
- Variety of bagels, fruits, doughnuts and cereal available at the start of class*
- Tea, coffee and soda available throughout the day*
- Freshly baked cookies every afternoon*

**denotes this benefit is only available at participating locations*