Ec-Council- Certified Security Analyst ECSA

Certificate: Ec-Council- Certified Security Analyst ECSA	Accreditor: EC-Council
Duration: 5 Days	Language: English
Course Delivery: Classroom	

Course Overview

ECSA/LPT is a security class like no other! Providing real world hands on experience, it is the only in-depth Advanced Hacking and Penetration Testing class available that covers testing in all modern infrastructures, operating systems and application environments. EC-Council's Certified Security Analyst/LPT program is a highly interactive 5-day security class designed to teach Security Professionals the advanced uses of the LPT methodologies, tools and techniques required to perform comprehensive information security tests. Students will learn how to design, secure and test networks to protect your organization from the threats hackers and crackers pose. By teaching the tools and ground breaking techniques for Security and penetration testing this class will help you perform the intensive assessments required to effectively identify and mitigate risks to the security of your infrastructure. As students learn to identify security problems, they also learn how to avoid and eliminate them, with the class providing complete coverage of analysis and network security-testing topics.

Who Should Attend

Network server administrators, firewall administrators, Security Testers, system administrators, and risk assessment professionals

Exam Informaiton

The ECSA certification exam will be conducted on the last day of training. Students need to pass the online Prometric exam 412-79 to receive the ECSA certification. The Student also will be prepared for the LPT certification.

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.

Course Outline

ECSA V9 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.

Module 1: Need For Security Analysis

- Computer Security Concerns
- Information Security Measures
- Risk Analysis

- Hardening Security
- Security Policies
- Sample Policies
- Information Security Standards
- Information Security Acts and Laws

Module 2: TCP/IP Packet Analysis

- Introduction to TCP/IP
- TCP/IP Connection
- Introduction to IPv6
- TCP/IP Security
- Internet Control Message Protocol (ICMP)
- TCP/IP in Mobile Communications

Module 3: Penetration Testing Methodologies

- Introduction to Penetration Testing
- Types of Penetration Testing
- Phases of Penetration Testing
- Penetration Testing Consultants
- Ethics of a Licensed Penetration Tester
- Communication Skills of a Penetration Tester
- LPT Audited Logos

Module 4: Customers and Legal Agreements

- Why Do Organizations Need Pen Testing?
- Penetration Testing 'Rules of Behavior'
- Legal Issues in Penetration Testing
- Penetration Testing Contract
- How Much to Charge?

Module 5: Rules of Engagement

- Rules of Engagement (ROE)
- Clauses in ROE

Module 6: Penetration Testing Planning and Scheduling

- Test Plan and Its Purpose
- Content of a Test Plan
- Building a Penetration Test Plan
- Test Plan Identifier
- Test Deliverables
- Penetration Testing Planning Phase Define the Pen
- Staffing
- Kickoff Meeting
- Develop the Project Plan

Module 7: Pre- Penetration Testing Steps

- Pre-penetration Testing Steps

Module 8: Information Gathering

- What Is Information Gathering?
- Information Gathering Terminologies
- Information Gathering Steps

Module 9: Vulnerability Analysis

- What Is Vulnerability Assessment?
- Why Assessment
- Vulnerability Classification
- Types of Vulnerability Assessment
- How to Conduct a Vulnerability Assessment

- How to Obtain a High Quality Vulnerability Assessment
- Vulnerability Assessment Phases
- Vulnerability Analysis Stages
- Comparing Approaches to Vulnerability Assessment
- Characteristics of a Good Vulnerability Assessment Solution
- Vulnerability Assessment Considerations
- Vulnerability Assessment Reports
- Vulnerability Report Model
- Timeline
- Types of Vulnerability Assessment Tools
- Choosing a Vulnerability Assessment Tool
- Criteria for Choosing a Vulnerability Assessment Tool
- Best Practices for Vulnerability Assessment Tools
- Vulnerability Assessment Tools
- Reports
- Vulnerability Analysis Chart

Module 10: External Penetration Testing

- External Intrusion Test and Analysis
- Why Is It Done?
- Client Benefits
- External Penetration Testing
- Steps for Conducting External Penetration Testing
- Recommendations to Protect Your System from External Threats

Module 11: Internal Network Penetration Testing

- Internal Testing
- Steps for Internal Network Penetration Testing
- Recommendations for Internal Network Penetration Testing+

Module 12: Firewall Penetration Testing

- What Is a Firewall?
- What Does a Firewall Do?
- Packet Filtering
- What Can't a Firewall Do?
- How Does a Firewall Work?
- Firewall Logging Functionality
- Firewall Policy
- Periodic Review of Information Security Policies
- Firewall Implementation
- Build a Firewall Ruleset
- Maintenance and Management of Firewall
- Hardware Firewall
- Software Firewall
- Types of Firewalls
- Firewall Penetration Testing Tool: Firewall Test Agent
- Firewall Penetration Testing Tools
- Firewall Ruleset Mapping
- Best Practices for Firewall Configuration
- Steps for Conducting Firewall Penetration Testing
- Document Everything

Module 13: IDS Penetration Testing

- Introduction to IDS Application-based IDS
- Multi-Layer Intrusion Detection Systems
- Multi-Layer Intrusion Detection System Benefits
- Wireless Intrusion Detection Systems (WIDSs)

- Common Techniques Used to Evade IDS Systems
- IDS Penetration Testing Steps
- Recommendations for IDS Penetration Testing

Module 14: Password Cracking Penetration Testing

- Password - Terminology
- Importance of Passwords
- Password Types
- Common Password Vulnerabilities
- Password Cracking Techniques
- Types of Password Attacks
- How Are Passwords Stored in Windows?
- LM Authentication
- NTLM Authentication
- Kerberos Authentication
- LM, NTLMv1, and NTLMv2
- How Are Passwords Stored in Linux?
- Steps for Password Cracking Penetration Testing

Module 15: Social Engineering Penetration Testing

- What Is Social Engineering?
- Social Engineering Pen Testing
- Impact of Social Engineering on the Organization
- Common Targets of Social Engineering
- Requirements of Social Engineering
- Steps in Conducting Social Engineering

Module 16: Web Application Penetration Testing

- Introduction to Web Applications
- Web Application Components
- Web App Pen Testing Phases

Module 17: SQL Penetration Testing

- Introduction to SQL Injection
- How Do Web Applications Work?
- How Does SQL Injection Work?
- SQL Injection Attack Paths
- Impact of SQL Injection Attacks
- Types of SQL Injection Attacks
- SQL Injection Attack Characters
- SQL Injection Cheat Sheet
- SQL Injection Penetration Testing Steps
- Best Practices to Prevent SQL Injection

Module 18: Penetration Testing Reports and Post Testing Actions

- Penetration Testing Deliverables
- Writing Pen Testing Report
- Pen Testing Report Format
- Result Analysis
- Post Testing Actions
- Report Retention