EC-Council Security Analyst (ECSA)
Course certification training

Course Agenda

Index

Course Curriculum

Lesson 0 - Penetration Testing Essential Concepts
- Computer Network Fundamentals
- Network Security Controls and Devices
- Windows and Linux Security
- Web Application and Web Server Architecture and Operations
- Web Application Security Mechanisms
- Information Security Attacks
- Information Security Standards

Lesson 1- Introduction to Penetration Testing Methodologies
- Penetration Testing Process and Methodologies & Benefits
- Types, Areas and Selection of Pentesting

Lesson 2- Penetration Testing Scoping and Engagement Methodology
- Penetration Testing Scoping and Rules and Engagement
- Penetration Testing Engagement Contract and Preparation

Lesson 3- Open-Source Intelligence (OSINT) Methodology

- OSINT Through World Wide Web (WWW), Website Analysis, DNS Interrogation
- Automating your OSINT Effort Using Tools/Frameworks/Scripts

Lesson 4 - Social Engineering Penetration Testing Methodology
- Social Engineering Penetration Testing Techniques & Steps
- Social Engineering Penetration testing using E

Lesson 5 - Network Penetration Testing Methodology – External
- External Network Information & Reconnaissance
- Scanning, and Exploitation

Lesson 6 - Penetration Testing Methodology – Internal
- Internal Network Information Reconnaissance and Scanning
- Internal Network Enumeration and Vulnerability Scanning
- Local and Remote System Exploitation

Lesson 7 - Network Penetration Testing Methodology - Perimeter Devices
- Firewall Security Assessment Techniques
- iDs Security Assessment Techniques
- Router and Switch Security Assessment Techniques

Lesson 8 - Web Application Penetration Testing Methodology
- Web Application Content Discovery and Vulnerability Scanning
- SQL Injection Vulnerability Penetration Testing
- XSS, Parameter Tampering, Weak Cryptography, Security Misconfiguration and Client side scripting, vulnerabilities penetration techniques
- Authentication, Authorization, session, Web Server Vulnerabilities Penetration Testing

Lesson 9 - Database Penetration Testing Methodology

- Database Penetration Testing Techniques & Information Reconnaissance
- Database Enumeration & Exploitation

Lesson 10 - Wireless Penetration Testing Methodology
- WLAN Penetration Testing Techniques
- RFID and NFC Penetration Testing Techniques
- Mobile Device Penetration Testing Techniques
- loT Penetration Testing Techniques

Lesson 11 - Cloud Penetration Testing Methodology
- Cloud Specific Penetration Testing Techniques and Recommendations
- Cloud Specific Penetration Testing Methods

Lesson 12 - Report Writing and Post Testing Actions
- Penetration Testing Report Writing Process
- Penetration Testing Reporting Formats