Advanced Security Tester
Course Outline

General Description

This course provides test engineers with advanced skills in security test analysis, design, and execution. In a hands-on, interactive fashion, you'll learn how to plan, perform, and evaluate security tests based on organizational security policies, security risks and standards, and common vulnerabilities, within the context of the project lifecycle. Using a running case study, you'll work through ways to analyze current and future security threats, the coverage of existing security tests against these threats, and the adequacy of security policies, procedures, and mechanisms. You'll determine what security tests are most important. You'll evaluate a particular security testing approach will succeed and suggest enhancements where needed.

You'll learn ways to help your organization become more aware of security awareness, and practice thinking like a hacker so you can anticipate the bad guys' moves with smart security tests. You'll explore options for reporting security test results that don't leak important information to those without a need to know, and also options for using tools to support your security test efforts.

By the end of this course, an attendee should be able to:

- Plan, perform and evaluate security tests from a variety of perspectives – policy-based, risk-based, standards-based, requirements-based and vulnerability-based.
- Align security test activities with project lifecycle activities.
- Analyze the effective use of risk assessment techniques in a given situation to identify current and future security threats and assess their severity levels.
- Evaluate the existing security test suite and identify any additional security tests.
- Analyze a given set of security policies and procedures, along with security test results, to determine effectiveness.
- For a given project scenario, identify security test objectives based on functionality, technology attributes and known vulnerabilities.

- Analyze a given situation and determine which security testing approaches are most likely to succeed in that situation.
- Identify areas where additional or enhanced security testing may be needed.
- Evaluate effectiveness of security mechanisms.
- Help the organization build information security awareness.
- Demonstrate the attacker mentality by discovering key information about a target, performing actions on a test application in a protected environment that a malicious person would perform, and understand how evidence of the attack could be deleted.
- Analyze a given interim security test status report to determine the level of accuracy, understandability, and stakeholder appropriateness.
- Analyze and document security test needs to be addressed by one or more tools.
- Analyze and select candidate security test tools for a given tool search based on specified needs.
- Understand the benefits of using security testing standards and where to find them.

Created by Rex Black, President of RBCS, Inc. (www.rbcs-us.com), past President of the International Software Testing Qualifications Board (www.istqb.org), past President of the American Software Testing Qualifications Board (www.astqb.org), and co-author of the International Software Testing Qualifications Board Advanced Syllabus, this course is also ideal for testers and test teams preparing for certification. It covers the International Software Testing Qualifications Board Advanced Level Syllabus Security Tester 2016, and has been accredited by an ISTQB-recognized National Board.

Learning Objectives

Through presentation, discussion, and hands-on exercises, attendees will learn to:

- Understand the role of risk assessment in supplying information for security test planning and design and aligning security testing with business needs
- Identify the significant assets to be protected, the value of each asset and the data required to assess the level of security needed for each asset
- Analyze the effective use of risk assessment techniques in a given situation to identify current and future security threats
- Understand the concept of security policies and procedures and how they are applied in information systems

- Analyze a given set of security policies and procedures along with security test results to determine effectiveness
- Understand the purpose of a security audit
- Understand why security testing is needed in an organization, including benefits to the organization such as risk reduction and higher levels of confidence and trust
- Understand how project realities, business constraints, software development lifecycle, and other considerations affect the mission of the security testing team
- Explain why security testing goals and objectives must align with the organization's security policy and other test objectives in the organization
- For a given project scenario, demonstrate the ability to identify security test objectives based on functionality, technology attributes and known vulnerabilities
- Understand the relationship between information assurance and security testing
- For a given project, demonstrate the ability to define the relationship between security test objectives and the need for strength of integrity of sensitive digital and physical assets
- Analyze a given situation and determine which security testing approaches are most likely to succeed
- Analyze a situation in which a given security testing approach failed, identifying the likely causes of failure
- For a given scenario, demonstrate the ability to identify the various stakeholders and illustrate the benefits of security testing for each stakeholder group
- Analyze KPIs (key performance indicators) to identify security testing practices needing improvement and elements not needing improvement
- For a given project, demonstrate the ability to define the elements of an effective security test process
- Analyze a given security test plan, giving feedback on strengths and weaknesses of the plan
- For a given project, implement conceptual (abstract) security tests, based on a given security test approach, along with identified functional and structural security risks
- Implement test cases to validate security policies and procedures

- Understand the key elements and characteristics of an effective security test environment
- Understand the importance of planning and obtaining approvals before performing any security test
- Analyze security test results to determine the following: Nature of security vulnerability; Extent of security vulnerability; Potential impact of security vulnerability; Suggested remediation; and, Optimal test reporting methods
- Understand the importance of maintaining security testing processes given the evolving nature of technology and threats
- Explain why security is best achieved within a lifecycle process
- Implement the appropriate security-related activities for a given software lifecycle (e.g., iterative, sequential)
- Analyze a given set of requirements from the security perspective to identify deficiencies
- Analyze a given design document from the security perspective to identify deficiencies
- Understand the role of security testing during component testing
- Implement component level security tests (abstract) given a defined coding specification
- Analyze the results from a given component level test to determine the adequacy of code from the security perspective
- Understand the role of security testing during component integration testing
- Implement component integration security tests (abstract) given a defined system specification
- Implement an end-to-end test scenario for security testing which verifies one or more given security requirements and tests a described functional process
- Demonstrate the ability to define a set of acceptance criteria for the security aspects of a given acceptance test
- Implement an end-to-end security retest/regression test approach based on a given scenario
- Understand the concept of system hardening and its role in enhancing security

- Demonstrate how to test the effectiveness of common system hardening mechanisms
- Understand the relationship between authentication and authorization and how they are applied in securing information systems
- Demonstrate how to test the effectiveness of common authentication and authorization mechanisms
- Understand the concept of encryption and how it is applied in securing information systems
- Demonstrate how to test the effectiveness of common encryption mechanisms
- Understand the concept of firewalls and the use of network zones and how they are applied in securing information systems
- Demonstrate how to test the effectiveness of existing firewall implementations and network zones
- Understand the concept of intrusion detection tools and how they are applied in securing information systems
- Demonstrate how to test the effectiveness of existing intrusion detection tool implementations
- Understand the concept of malware scanning tools and how they are applied in securing information systems
- Demonstrate how to test the effectiveness of existing malware scanning tool implementations
- Understand the concept of data obfuscation tools and how they are applied in securing information systems
- Demonstrate how to test the effectiveness of data obfuscation approaches
- Understand the concept of security training as a software lifecycle activity and why it is needed in securing information systems
- Demonstrate how to test the effectiveness of security training
- Explain how human behavior can lead to security risks and how it impacts the effectiveness of security testing
- For a given scenario, demonstrate the ability to identify ways in which an attacker could discover key information about a target and apply measures to protect the environment
- Explain the common motivations and sources for performing computer system attacks

- Analyze an attack scenario (attack performed and discovered) and identify possible sources and motivation for the attack
- Explain how security defenses can be compromised by social engineering
- Understand the importance of security awareness throughout the organization
- Given certain test outcomes, apply appropriate actions to increase security awareness
- Understand the need to revise security expectations and acceptance criteria as the scope and goals of a project evolve
- Understand the importance of keeping security test results confidential and secure
- Understand the need to create proper controls and data-gathering mechanisms to provide the source data for the security test status reports in a timely, accurate, and precise fashion (e.g., a security test dashboard)
- Analyze a given interim security test status report to determine the level of accuracy, understandability, and stakeholder appropriateness
- Explain the role of static and dynamic analysis tools in security testing
- Analyze and document security testing needs to be addressed by one or more tools
- Understand the issues with open source tools
- Understand the need to evaluate the vendor's capabilities to update tools on a frequent basis to stay current with security threats
- Understand the benefits of using security testing standards and where to find them
- Understand the difference in applicability of standards in regulatory versus contractual situations
- Understand the difference between mandatory (normative) and optional (informative) clauses within any standard
- Understand where to learn of industry trends in information security

Course Materials

This course includes the following materials:

Name	*Description*
Course Outline	A general description of the course along with learning objectives, course materials and an outline of the course topics, including approximate timings for each section.
Noteset	A set of approximately 300 PowerPoint slides covering the topics to be addressed.
Foundation Sample Exam Questions	A set of approximately 150 pages of review materials for the Foundation level covering every learning objective in the ISTQB Foundation Syllabus.
Foundation Mock Exam	A practice exam containing 40 questions and answers to provide a review of the ISTQB Foundation exam.
Advanced Security Tester Sample Exam Questions	A complete set of questions for every learning objective in the Test Analyst module of the ISTQB Advanced Syllabus.
Exercises	A set of exercises for the course, based on a realistic case study.
Advanced Security Tester Mock Exam	A practice exam containing questions and answers to assess your readiness for the ISTQB Advanced exam.
Project Source Documents for Course Exercises	Specifications and documents used in the realistic case study used in exercises for the course.
Bibliography and resources	A set of further readings, Web sites, tools and other resources to help implement the concepts.

The printed course materials are provided in a binder in a way which makes it convenient for course attendees to remove portions as needed for reference; e.g., during exercises.

Session Plan

The course runs for three days, with attendees encouraged to take the ISTQB Advanced Security Tester exam on the following day. Each day is about 360 minutes of class time, from 9:00 to 5:30. For accredited course offerings, material is covered as described. For custom courses, material may be deleted, added, or expanded upon as needed.

Please note that timings are approximate, depending on attendee interest and discussion. All of the lectures include exercises and/or knowledge-check questions except as noted.

The following shows this session plan in relationship to the chapters and sections of the ISTQB Advanced Syllabus Security Tester.

Introduction and Review (60 minutes)

1. The Basis of Security Testing - 105 minutes

1.1 Security Risks

1.2 Information Security Policies and Procedures

1.3 Security Auditing and Its Role in Security Testing

Exercise

2. Security Testing Purposes, Goals and Strategies - 130 minutes

2.1 Introduction

2.2 The Purpose of Security Testing

2.3 The Organizational Context

2.4 Security Testing Objectives

2.5 The Scope and Coverage of Security Testing Objectives

2.6 Security Testing Approaches

2.7 Improving the Security Testing Practices

Exercise

3. Security Testing Processes - 140 minutes

3.1 Security Test Process Definition

3.2 Security Test Planning

3.3 Security Test Design

3.4 Security Test Execution

3.5 Security Test Evaluation

3.6 Security Test Maintenance

Exercise

4. Security Testing Throughout the Software Lifecycle - 225 minutes

4.1 Role of Security Testing in a Software Lifecycle

4.2 The Role of Security Testing in Requirements

4.3 The Role of Security Testing in Design

4.4 The Role of Security Testing in Implementation Activities
4.5 The Role of Security Testing in System and Acceptance Test Activities
4.6 The Role of Security Testing in Maintenance
Exercise

5. Testing Security Mechanisms - 240 minutes

5.1 System Hardening
5.2 Authentication and Authorization
5.3 Encryption
5.4 Firewalls and Network Zones
5.5 Intrusion Detection
5.6 Malware Scanning
5.7 Data Obfuscation
5.8 Training
Exercise

6. Human Factors in Security Testing - 105 minutes

6.1 Understanding the Attackers
6.2 Social Engineering
6.3 Security Awareness
Exercise

7. Security Test Evaluation and Reporting - 70 minutes

7.1 Security Test Evaluation
7.2 Security Test Reporting
Exercise

8. Security Testing Tools - 55 minutes

8.1 Types and Purposes of Security Testing Tools
8.2 Tool Selection
Exercise

9. Standards and Industry Trends - 40 minutes

9.1 Understanding Security Testing Standards
9.2 Applying Security Standards
9.3 Industry Trends

Recommended Readings

The class materials include a bibliography of books related to software testing, software security, quality, and other topics of interest to the security test professional.