

- Plan, perform, and evaluate security tests from a variety of perspectives
- Evaluate an existing security test suite and identify any additional security tests needed.
- 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.
- Understand the role of security standards (including security test standards), where to find them, and how to stay current with security developments worldwide.

With the prevalence of cyber security breaches, it is clear that more attention is needed in testing that security defenses are in place and working effectively. This course and certification covers much more than just penetration testing. Certainly, penetration testing is an important part of security testing, but there are many other threats and vulnerabilities that require other security testing approaches.

## Who Should Attend?

- Security testers
- Software testers who wish to develop a specialty in security testing
- Security administrators who wish to learn how to test new and existing defenses
- Developers who want to learn secure coding techniques
- Project managers who want to learn how security testing fits in the project lifecycle

## Pre-Qualification for the Advanced Certification Exam

This course follows the ISTQB Advanced Security Tester Syllabus. Exercises are performed for every K3 (apply) and K4 (analyze) learning objective. To sit for the ISTQB Advanced Security Tester exam, you must hold the ISTQB Certified Tester, Foundation Level (CTFL) designation and have 3+ years of software testing and related experience. After pre-qualification is completed, students receive an exam voucher good for one year.

## Prerequisites

Basic security and security testing concepts are assumed knowledge. If you wish to take the course without sitting for the exam, there are no additional prerequisites.

## Course Outline

---

## **The Basis of Security Testing**

- Security Risks
- Information Security Policies and Procedures
- Security Auditing and Its Role in Security Testing

## **Security Testing Purposes, Goals and Strategies**

- Introduction
- The Purpose of Security Testing
- The Organizational Context
- Security Testing Objectives
- The Scope and Coverage of Security Testing Objectives
- Security Testing Approaches
- Improving the Security Testing Practices

## **Security Testing Processes**

- Security Test Process Definition
- Security Test Planning
- Security Test Design
- Security Test Execution
- Security Test Evaluation
- Security Test Maintenance

## **Security Testing Throughout the Software Lifecycle**

- Role of Security Testing in a Software Lifecycle
- The Role of Security Testing in Requirements
- The Role of Security Testing in Design
- The Role of Security Testing in Implementation Activities
- The Role of Security Testing in System and Acceptance Test Activities
- The Role of Security Testing in Maintenance

## **Testing Security Mechanisms**

- System Hardening
- Authentication and Authorization
- Encryption
- Firewalls and Network Zones
- Intrusion Detection
- Malware Scanning
- Data Obfuscation
- Training

## **Human Factors in Security Testing**

- Understanding the Attackers
- Social Engineering
- Security Awareness

## **Security Test Evaluation and Reporting**

- Security Test Evaluation
- Security Test Reporting

## **Security Testing Tools**

- Types and Purposes of Security Testing Tools
- Tool Selection

## **Standards and Industry Trends**

- Understanding Security Testing Standards
- Applying Security Standards
- Industry Trends