processexam
#1 Process Certification Guide

ISTQB CT-SEC

ISTQB CTFL - SECURITY TESTER CERTIFICATION QUESTIONS & ANSWERS

Exam Summary – Syllabus – Questions

CT-SEC

ISTQB Certified Tester Foundation Level - Security Tester

45 Questions Exam – 52/80 Cut Score – Duration of 120 minutes

www.ProcessExam.com

Table of Contents

Know Your CT-SEC Certification Well:

The CT-SEC is best suitable for candidates who want to gain knowledge in the ISTQB Specialist. Before you start your CT-SEC preparation you may struggle to get all the crucial Security Tester materials like CT-SEC syllabus, sample questions, study guide.

But don't worry the CT-SEC PDF is here to help you prepare in a stress free manner.

The PDF is a combination of all your queries like-

- What is in the CT-SEC syllabus?
- How many questions are there in the CT-SEC exam?
- Which Practice test would help me to pass the CT-SEC exam at the first attempt?

Passing the CT-SEC exam makes you ISTQB Certified Tester Foundation Level - Security Tester. Having the Security Tester certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

ISTQB CT-SEC Security Tester Certification Details:

Exam Name	ISTQB Certified Tester Security Tester
Exam Code	CT-SEC
Exam Fee	USD $265
Exam Duration	120 Minutes
Number of Questions	45
Passing Score	52/80
Format	Multiple Choice Questions
Schedule Exam	**Pearson VUE**
Sample Questions	**ISTQB CTFL - Security Tester Exam Sample Questions and Answers**
Practice Exam	**ISTQB Certified Tester Foundation Level - Security Tester (CT-SEC) Practice Test**

CT-SEC Syllabus:

Topic	Details
The Basis of Security Testing - 105 mins.	
Security Risks	- 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
Information Security Policies and Procedures	- 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
Security Auditing and Its Role in Security Testing	- Understand the purpose of a security audit
Security Testing Purposes, Goals and Strategies - 130 mins.	
Introduction	
The Purpose of Security Testing	- 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
The Organizational Context	- Understand how project realities, business constraints, software development lifecycle, and other considerations affect the mission of the security testing team
Security Testing Objectives	- 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
The Scope and Coverage of Security Testing Objectives	- 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
Security Testing Approaches	- Analyze a given situation and determine which security testing approaches are most likely to succeed - Analyze a situation in which a given security testing

Topic	Details
	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
Improving the Security Testing Practices	- Analyze KPIs (key performance indicators) to identify security testing practices needing improvement and elements not needing improvement
Security Testing Processes - 140 mins.	
Security Test Process Definition	- For a given project, demonstrate the ability to define the elements of an effective security test process
Security Test Planning	- Analyze a given security test plan, giving feedback on strengths and weaknesses of the plan
Security Test Design	- 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
Security Test Execution	- 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
Security Test Evaluation	- Analyze security test results to determine the following: • Nature of security vulnerability • Extent of security vulnerability • Potential impact of security vulnerability • Suggested remediation • Optimal test reporting methods
Security Test Maintenance	- Understand the importance of maintaining security testing processes given the evolving nature of technology and threats
Security Testing Throughout the Software Lifecycle - 225 mins.	
Role of Security Testing in a Software Lifecycle	- 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)
The Role of Security Testing in Requirements	- Analyze a given set of requirements from the security perspective to identify deficiencies

Topic	Details
The Role of Security Testing in Design	- Analyze a given design document from the security perspective to identify deficiencies
The Role of Security Testing in Implementation Activities	- 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
The Role of Security Testing in System and Acceptance Test Activities	- 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
The Role of Security Testing in Maintenance	- Implement an end-to-end security retest/regression test approach based on a given scenario
Testing Security Mechanisms - 240 mins.	
System Hardening	- Understand the concept of system hardening and its role in enhancing security - Demonstrate how to test the effectiveness of common system hardening mechanisms
Authentication and Authorization	- 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
Encryption	- Understand the concept of encryption and how it is applied in securing information systems - Demonstrate how to test the effectiveness of common encryption mechanisms
Firewalls and Network Zones	- 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
Intrusion Detection	- Understand the concept of intrusion detection tools and how they are applied in securing information systems

Topic	Details
	- Demonstrate how to test the effectiveness of existing intrusion detection tool implementations
Malware Scanning	- 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
Data Obfuscation	- 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
Training	- 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
Human Factors in Security Testing - 105 mins.	
Understanding the Attackers	- 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
Social Engineering	- Explain how security defenses can be compromised by social engineering
Security Awareness	- Understand the importance of security awareness throughout the organization - Given certain test outcomes, apply appropriate actions to increase security awareness
Security Test Evaluation and Reporting - 70 mins.	
Security Test Evaluation	- Understand the need to revise security expectations and acceptance criteria as the scope and goals of a project evolve
Security Test Reporting	- 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)

Topic	Details
	- Analyze a given interim security test status report to determine the level of accuracy, understandability, and stakeholder appropriateness
Security Testing Tools - 55 mins	
Types and Purposes of Security Testing Tools	- Explain the role of static and dynamic analysis tools in security testing
Tool Selection	- 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
Standards and Industry Trends - 40 mins.	
Understanding Security Testing Standards	- 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
Applying Security Standards	- Understand the difference between mandatory (normative) and optional (informative) clauses within any standard
Industry Trends	- Understand where to learn of industry trends in information security

ISTQB CT-SEC Sample Questions:

Question: 1

You are finalizing your security test status report for a project that is ready for deployment into production. There is a high degree of risk for this project due to the nature of the system. As a result, you want to place particular emphasis on risk.

Based on this, what is the best way to articulate risk on your report?

a) A descriptive risk assessment included in the summary
b) Overall risk included in the last section of the report
c) Risk impact described in the summary and later detailed in terms of specific vulnerabilities
d) Risk impact is not part of the summary of the report

Answer: c

Question: 2

In what way are dynamic security analysis tools different from general dynamic analysis tools?

a) The security tools probe the system rather than just the application under test
b) The security tools work the same in dynamic or static mode
c) The security tools are better suited to detect problems such as memory leaks
d) The security tools need to be tailored to the language in which the application is implemented

Answer: a

Question: 3

What are key attributes of security authentication of a medium complexity IT system?

a) It verifies that the user has the correct profile and corresponding rights to access limited parts of the system
b) It is key in identifying the amount of system resources the user can utilize
c) It verifies that user entering the system is legitimate
d) It uses common credentials among users to gain entry into the system

Answer: c

Question: 4

If an organization experiences a security breach and legal action results, how does it help the organization to have done security testing?

a) By tracing through the documented tests, the security testing team can discover how the breach was possible
b) The documentation from the security testing can be used to track down the perpetrator
c) Since any important information would have been backed up before security testing, this backup can be used to restore any compromised information
d) It can show that the organization has done due diligence to try to prevent such an incident

Answer: d

Question: 5

At what point in the SDLC should there be checking to ensure that proper secure coding practices have been followed?

a) Component testing
b) Integration testing
c) System testing
d) Security acceptance testing

Answer: a

Question: 6

What is a significant concern when seeking approval for the security testing tools?

a) Some countries prohibit the use of certain security testing tools
b) Ensure the approval process for security testing tools can be bypassed on an exception basis in cases where a malicious event is in progress
c) The risks of the tool are rarely known before it is procured and are better discovered when the tools is in use
d) Because security testing tool risks are usually known, there is no need for a mitigating strategy

Answer: a

Question: 7

Why is an attack from inside the organization particularly worrisome?

a) The attacker is likely driven by curiosity and will be unrelenting
b) The attacker is likely bored at work and will continue hacking the system for entertainment
c) The attacker is already inside the firewall and is an authorized system user
d) The attacker is likely to launch a DOS attack which will cripple the servers

Answer: c

Question: 8

Which of the following would you apply to most effectively test the abilities of an intrusion detection tool?

a) Develop a series of scenarios based on past experience
b) Use tests that generate malicious traffic to add new intrusive specifications
c) Apply it to situations of known malicious traffic
d) Use it in conjunction with other IDS products when possible

Answer: b

Question: 9

During component level testing, why should the security tester review compiler warnings?

a) Because these indicate security problems that must be fixed
b) Because these indicate potential issues that should be investigated
c) Because these indicate coding issues that will cause functional defects
d) Because these indicate poor programming practices that will increase maintainability

Answer: b

Question: 10

Which of the following are main characteristics of an effective security test environment?

a) Closely tied to production systems to enhance security at all points
b) Isolates different old versions of the operating systems for use in the environment
c) Includes all production environment plug-ins as well as other plug-ins not in the production environment in order to ensure the most comprehensive setup
d) Mimics the production environment in terms of access rights

Answer: d

Study Guide to Crack ISTQB Security Tester CT-SEC Exam:

- Getting details of the CT-SEC syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CT-SEC exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the ISTQB provided training for CT-SEC exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the CT-SEC sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on CT-SEC practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for CT-SEC Certification

Make ProcessExam.com your best friend during your ISTQB Certified Tester Security Tester exam preparation. We provide authentic practice tests for the CT-SEC exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual CT-SEC exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the CT-SEC exam.

Start Online Practice of CT-SEC Exam by Visiting URL

https://www.processexam.com/istqb/istqb-certified-tester-security-tester-ct-sec