ISTQB

CT-SEC
ISTQB Certified Tester Security Tester (CT-SEC)

For More Information – Visit link below:
https://www.examsempire.com/
Product Version
1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.

https://examsempire.com/

Latest Version: 6.0

Question: 1

Why is an attack from inside the organization particularly worrisome?
Response:

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: 2

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

A. Component testing
B. Integration testing
C. System testing
D. Security acceptance testing

Answer: A

Question: 3

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

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: 4

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

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: 5

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

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: 6

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

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

Question: 7

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

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: 8

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

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: 9

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

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: 10

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?
Response:

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

Thank You for Trying Our Product

Discount Coupon Code is: 20OFF2022

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/