Exam Name – Certified Software Security Tester (CSST)™

Exam Code – CSST-001

Sample Exam

(Question): Which of the following is a purpose of a security audit?

(A): To prevent users from using simple passwords
(B): To reveal insufficient patch updates provided by the vendor
(C): To halt unauthorized intruders from accessing the system
(D): To require users to change their password after a predetermined set of days

(Correct): B

(Question): Which of the following is a consequence of a policy that minimizes access to a system or device to acceptable levels?

(A): More devices are added to mitigate the impact
(B): Proper controls of self-provisioning devices such as routers are prohibited
(C): Devices that do not conform are removed from the wireless network
(D): Access to the VPN is severely restricted

(Correct): C

(Question): Which of the following would be revealed during an audit of security practices:

(A): Misconfiguration of a firewall zone
(B): Inadequate application of security updates from a software vendor
(C): Levels of risk for digital and physical assets
(D): Stakeholder responsibilities in information security practices

(Correct): B

(Question): Which of the following is a correct statement?

(A): Information assurance is a part of security testing
(B): Information assurance and security testing are two terms for the same thing
(C): Security testing is a part of information assurance
(D): The two terms refer to different areas of security

(Correct): C

(Question): Which of the following test cases would best test a system's security procedure?

(A): Three unsuccessful login attempts will generate a lock-out message. Contact your manager or the System Administrator so they can give you a temporary password over the phone. You must then change the temporary password upon logging in. You log out then log back in using your newly created password.
(B): You receive a lock-out message after several attempts to log in. You call IT support to obtain a new password. You log in with the temporary password, log back out, then log in again and enter a new password.
(C): After several attempts you are locked out of the system. You use a password that worked previously. However, it no longer works. You attempt to create a new

password but you are now locked out. A complete reboot of the machine is the next step to take you to the prompt to re-enter the password.
(D): After the first attempt to use an invalid password you immediately pull up a list of passwords on your notepad on your PC to ensure you are using the correct one. You try another password from the list and it works.

(Correct): A

(Question): 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): Mimics the production environment in terms of access rights
(D): 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

(Correct): C

(Question): 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

(Correct): A