Sample Exam
Advanced Level Syllabus

Security Testing

Version GA – March 2016

International Software Testing Qualifications Board

Revision History

Version	Date	Remarks
1.0 – Beta	22 Sept 2015	Beta version of sample exam
1.0 - GA Candidate	04 March 2016	Updates after Exam WG review – question 18 and 29 changed to K3 level, typo in question 35 fixed, point allocations for #25 - #32 fixed.
1.0 – GA	15 March 2016	GA version with minor edits. LOs removed.

Question #1 (1 pt)

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

Question #2 (3 pts)

You are responsible for ensuring that new vendors brought on externally for the project are fully compliant with government mandated guidelines as part of your risk assessment. On which stakeholders should you primarily focus to ensure these outside vendors continue to comply?

a. Customers, users, and vendors to ensure there is good communication between them
b. Public users and vendors who will follow the law as it applies to the source of information
c. Federal and local agencies that communicate guidelines to follow
d. Both internal and external sources that will use the information for further analyzing the risk

Question #3 (1 pt)

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

Question #4 (3 pts)

Your role as the Security Administrator is to help your organization understand the effectiveness of security policies and procedures across the enterprise. You will report your effectiveness findings to Senior Management after your analysis has been completed. Which of the following is the optimum strategy to accomplish this?

a. Implement a static analysis evaluation independently for both policies and procedures
b. Analyze the results from a security test to validate effectiveness
c. Evaluate security test results that focus on current threats and attacks
d. Evaluate the static test results for new and emerging software threats

Question #5 (1 pt)

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

a. It can show that the organization has done due diligence to try to prevent such an incident
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. By tracing through the documented tests, the security testing team can discover how the breach was possible

Question #6 (1 pt)

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

Question #7 (2 pts)

You are working at a bank as part of the security testing team. During a recent security audit it was noted that the user's passwords were not strong enough. Since that time, a new set of requirements has been issued to ensure password strength. Given this information, what would be a reasonable set of security objectives for general password rule testing?

1. Verify that passwords meet the requirements for length
2. Verify that passwords meet the requirements for usage of characters, numbers, letters and capitalization
3. Verify that passwords can be retried three times
4. Verify that passwords cannot be re-used within a one year timeframe
5. Verify that passwords must be reset every three months
6. Verify that the user can request to have their password emailed to them
7. Verify that the system administrator can reset a locked password

a. 1, 2, 3, 4
b. 1, 2, 4, 5
c. 3, 4, 6, 7
d. 4, 5, 6, 7

Question #8 (2 pts)

Your company recently made headlines after a security breach resulted in confidential customer information being stolen. Management has reacted with an edict that the scope of the security testing objectives needs to be expanded immediately. While you agree that something needs to be done, you are worried that this approach may be too reactive and may not result in the testing that is needed.

According to the syllabus, what is a reasonable concern if these initiatives are implemented?

a. The testing will still miss issues because it will not be well-focused
b. The testing will be outsourced so that it can be done more efficiently
c. The testing scope may be too large and there may not be adequate resources to complete it
d. The testing objectives are not clearly defined and may miss the same issues as previously escaped to production

Question #9 (3 pts)

You have just accepted a job to create a security testing team for a company than handles sensitive medical information that is shared between doctors and hospitals. You have noticed that the security around this information is not sufficient to protect it from hackers or even accidental exposure. The person who had your job previously brought in a number of consultants to do testing, but the findings were not documented and no changes were implemented. In fact, you don't even know what the coverage was from the testing. You have presented your findings to the executive management team. While they have agreed in principle that they need security testing, they have not allocated the necessary budget or time to the project. It appears that while they think security is a good idea, they really have no understanding of what should be done or how it should be done. What should be your first step toward getting the executives aligned with the work that needs to be done?

a. Create a detailed list of all the possible security holes and present these to the executives
b. Provide a summary of the testing approach that you propose and give examples of how the testing will be conducted
c. Bring in the legal team to explain what a security breach could cost the organization
d. Create a security policy and security testing policy and demonstrate how that aligns with your proposed testing approach

Question #10 (2 pts)

You have just come from a meeting where there was much discussion regarding the security approach of the organization. One of the points of emphasis was the importance of testing to ensure that data is protected from fraudulent access, particularly credit card information. You have been asked to prepare a set of testing objectives that will help address this risk area. One of your tasks is to ensure that you are covering all the concerns of the stakeholders. Which stakeholder group is most likely to see the benefits from your efforts?

a. Executive management
b. Compliancy officers
c. Business customers
d. Regulatory officers

Question #11 (2 pts)

As a Security Administrator you are responsible for all aspects of the security process, including testing. For this particular process you are to use conceptual tests as a basis for manual tests and execute these from an external vendor's perspective. Which security testing process does this most parallel?

a. Security test creation of conditions and objectives
b. Security test implementation
c. Overall evaluating and reporting of security testing
d. Security test analysis and design

Question #12 (3 pts)

You have been developing a security test plan for a system that will store medical information for patients and will transfer that data to specialist doctors. You have covered the following areas in your plan:

- Scope (what's in scope and out of scope)
- Roles and assignments
- Responsibilities (vendors vs. internal)
- High level schedule
- Environment requirements and setup
- List of necessary authorizations and approvals

What information do you still need to supply in this test plan to meet the minimum requirements as noted in the syllabus?

a. A list of the necessary credentials and training for the personnel who will be conducting the testing
b. A schedule showing the time that will be required to design, run and evaluate the security tests
c. A copy of the regulatory standards that must be met by this system
d. A list of the individuals who will be doing the testing and their contact information in the event of a security breach

Question #13 (2 pts)

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.

Question #14 (1 pt)

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

Question #15 (1 pt)

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

Question #16 (3 pts)

You are reviewing a set of security test results run on a product that is going through final testing before release to production. This is an update of a version that is currently in production. The application just tested was your e-commerce site, and it has a defect that allows cross-site scripting. Which of the following is the proper set of steps you should take?

a. Report the problem to the developer, add it to the stakeholder report, and continue testing for other types of defects
b. Test if the problem exists in the current production version, document the defect in a secure system, notify the developer, continue testing for other XSS defects
c. Investigate the extent of the problem by conducting further tests on the planned release with particular concentration on other XSS isses, conduct static analysis on the code
d. Inform management, document the defect and include it in your weekly status report to stakeholders, continue testing for other security defects to determine the extent of the security issues

Question #17 (1 pt)

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

Question #18 (2 pts)

You have been asked by the business analyst to help with defining the requirements for the security aspects of a system. This is a safety-critical system that stores medical information for patients and supplies this information to health professionals at hospitals, doctors' offices and ambulances. At what point in the lifecycle should the security requirements be documented and at what level of detail?

a. They should not be documented formally because of the need to protect the security implementation within the code from outsiders
b. They should be documented in a detailed and unambiguous way in the requirements documents during the requirements phase
c. They should be documented during the design phase when the code approach is known rather than at the requirements phase when the approach is not known
d. They should be restricted to the functional access and availability requirements from the user's perspective and should be documented during the requirements phase

Question #19 (3 pts)

A deficiency has been discovered in production. If an unauthorized user copies a URL from a session of an authorized user, the unauthorized user can paste the URL into their session and continue to process with the authorized user's rights. In the case that was reported, the unauthorized user was able to use the authorized user's URL to change the system administration password. In order to close this gap, the developers will check the session ID and the user ID anytime a URL is used.

What is a realistic concern for this fix?

a. It will not fix the problem and session hijacking will still be possible
b. It will fix the problem, but the usability may be adversely affected
c. It will fix the problem, but performance may be adversely affected
d. It will not fix the problem and will expose a new vulnerability with session IDs

Question #20 (1 pt)

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

Question #21 (2 pts)

You have been testing a system that has 20 defined components. You have done extensive security testing on each of the components. The system is now ready to move into component integration security testing. How should you approach this testing?

a. Since component integration testing is concerned with the summation of the vulnerabilities of the individual components, conducting the same tests on the integrated components is the best approach.
b. The main risk is now in the integration of the components themselves, so testing should cover each interface and verify that there are no vulnerabilities in the interfaces and the components should also be retested.
c. It is likely that new vulnerabilities are present with the integrated components as well as with the larger system and infrastructure that is now testable, so testing should expand to include these new areas.
d. Since the components are now integrated, the security risks will be reduced because the possible interactions are now limited so only the integration points should be tested and no component re-testing is needed.

Question #22 (3 pts)

You are creating security test cases to check for SQL injection on an input field that allows up to 5 alphanumeric characters. You are planning to apply equivalence partitioning to reduce the number of test cases you will need to execute. Given this information, which of the following is the minimum set of inputs you would need to use to test this field?

a. bbbbb, 12345, ‘
b. %, ‘, @, ab123
c. ‘, ab123
d. ‘

Question #23 (2 pts)

You have been given the following requirement for security testing.

A user will be allowed to request their password. If they make this request, they must answer two of their three security questions correctly. If they answer correctly, a link will be sent to their email. The link will take them to a page where they can reset their password. Once reset, they can login with the new password. The link must be disabled 1 hour after it is sent. The user is allowed only two password requests without a reset, after which they will have to call the help desk. For any other errors, the user ID is locked and must be unlocked by the help desk.

Which of the following is the minimum list of test conditions to adequately test the functional security covered by this requirement?

a. Invalid user; valid user; 2 correct answers; 2 incorrect answers; good email; bad email; reset with good password; reset with bad password; link good; link expired; two requests without reset; three requests without reset
b. Valid user; 2 correct answers; good email; reset with good password; link good; two requests without reset
c. Invalid user; 2 incorrect answers; bad email; reset with bad password; link expired; three requests without reset
d. Buffer overflow on each input field; SQL injection on each input field; XXS on the login page and reset password page, invalid user; valid user; 2 correct answers; 2 incorrect answers; good email; bad email; reset with good password; reset with bad password; link good; link expired; two requests without reset; three requests without reset

Question #24 (2 pts)
A user will be allowed to request their password. If they make this request, they must answer two of their three security questions correctly. If they answer correctly, a link will be sent to their email address. The link will take them to a page where they can reset their password. Once reset, they can login with the new password. The link must be disabled one hour after it is sent. The user is allowed only two password requests without a reset, after which he will have to call the helpdesk. For any other errors, the user ID is locked and must be unlocked by the help desk.

Which of the following is a valid set of acceptance criteria for this requirement?

1. User can reset password if less than three requests have been made since last reset, and two security questions are answered correctly, and the link is used to reset and a valid password is entered at the reset prompt.
2. More than two requests results in user ID locked.
3. More than two requests without a reset results in user ID locked.
4. More than two security questions missed results in error.
5. More than two security questions missed, user ID is locked.
6. If email error is received by the system, user ID is locked.
7. If invalid password is entered on reset, the user is prompted with the proper rules.
8. Reset password can be used to log into the system.

a. 1, 2, 4, 6, 7, 8
b. 1, 2, 3, 4, 5, 6, 7, 8
c. 3, 5, 6, 7, 8
d. 1, 3, 5, 6, 8

Question #25 (2 pts)

You are implementing procedures for evaluating system hardening in an effort to test the system's security effectiveness. What procedure might you follow to ensure the hardening mechanisms put in place are working as expected?

a. Closely monitor various security performance reports and metrics to determine if the correct level of access and authentication is achieved
b. Frequently audit strong authentication to ensure a high level of intrusion protection is maintained at all times
c. Evaluate the hardware components that have been hardened and compare these to other hardened software components to ensure equilibrium is being achieved
d. Enlist a known hacker to conduct an independent assessment of the hardening effectiveness

Question #26 (1 pt)

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

Question #27 (2 pts)

Typical encryption mechanisms are vulnerable to threats which makes it important to understand their effectiveness at any given time. Identify which of the following you should implement to gain confidence in your encryption mechanisms?

a. Evaluate cryptographic keys to ensure they are at least 256 bits in size
b. Ensure you are applying random algorithms to generate random numbers where possible
c. Develop tests that ensure symmetric encryption is used in the right modes
d. Remove all WEP protocols to see how the system performs

Question #28 (1 pt)

Which is true of the relationship between a firewall and a network zone?

a. Both a network zone and firewall focus on the size of data that is being passed through
b. A network zone communicates through safe protocol options while a firewall ensures those protocols are safe
c. A sub-network can be considered a network zone and a firewall can be traffic monitoring software
d. A network zone blocks malicious traffic from an untrusted zone which the firewall does not filter

Question #29 (2 pts)

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

Question #30 (1 pt)

Which of the following is a main disadvantage to malware scanning tools?

a. They only detect certain levels of malware
b. They can only detect malware that is known to the tool
c. They tend to be overly complex to run
d. They do not provide updating and reporting capabilities

Question #31 (2 pt)

You need to remove personal identification numbers from a legacy system in order to reduce risk during testing. Part of your data obfuscation plan includes verifying how effectively the data is masked. Which of the following is the most effective approach to use?

a. Manually verify in the database that the data targeted for obfuscation is no longer understandable for logical human interpretation
b. Design a brute force attack on the obfuscated data
c. Substitute the sensitive data with random data of varying string lengths
d. Enlist the development teams to generate a program to stress the database for vulnerabilities

Question #32 (1 pt)

What is often considered the weakest link in software security?

a. The lack of a consistent and comprehensive security training plan
b. The effort necessary to maintain document and procedure updates in order to keep up with continuing security threats
c. The behavior of humans
d. The constant advancement in malicious techniques

Question #33 (1 pt)

Which of the following is a potential security risk?

a. Publishing an accounting department's organization chart on the company's web site
b. Posting birthday wishes for a co-worker on Facebook
c. Posting the company phone directory on the company Intranet
d. Posting professional experience in a Linked In profile

Question #34 (2 pts)

You are responsible for security testing your company's financial application. You have recently received email from a person who claims to have hacked into the system using Shodan and has discovered that you are running an out-of-date and vulnerable OS on one of your servers. You have checked and the hacker is correct. You have made sure the server has been updated. Your preliminary check has shown no trace of how the hacker got into your system. Should you be concerned?

a. No, this is a "white hat" hacker and means no harm to your company
b. No, you have fixed the vulnerability so the system is now safe
c. Yes, your security testing is not sufficient and you need to re-run your tests to see what was missed
d. Yes, since the hacker didn't admit how he got in the system, he can still access it and may decide to exploit the vulnerability next time

Question #35 (1 pt)

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 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

Question #36 (3 pts)

You are working in an organization where system administration access to the servers is highly restricted. Only three long-term and trusted employees know the root passwords. Recently though, there have been several odd occurrences. An unknown program, called "IKnowYourBirthday" was found to be running and was emailing birthday greetings to staff members. The birth dates were correct and the greetings were all signed "From your favorite server". This program was killed and no one could figure out where it came from. A second problem occurred when the corporate phone list was hacked and all the phone numbers were changed to 867-5309 (apparently taken from the song by the same name). The correct list was restored and again no one could figure out how it had been done, although the new file had been created by "root". You've just received a phone call from the lead system administrator telling you that the root password has been changed. It has been determined that the password was set to the lead system administrator's dog's name.

Further investigation has discovered that the problems started shortly after a series of virus–infected emails were detected. When the first one was found, safeguards were immediately put in place to stop any further spread of the virus, but now you are wondering if someone managed to get into the system via code that was introduced into the system by the virus.

What should you do now as your next step of investigation?

a. Look to see if the HR birthdate information was accessed from outside the system, and if so, trace the IP address
b. Verify if the lead system administrator's dog's name is posted somewhere in social media
c. Check the suspicious email that was sent and try to trace the IP address
d. Check the personnel files of the other two system administrators to see if there is an indication that they are unhappy

Question #37 (2 pts)

During testing of an upgrade, you have discovered that it is possible to create a man-in-the-middle attack that can change the amount charged to customers on your e-commerce web site. Your tester successfully changed the amount so that customers were all getting a 10% discount. What should you do first?

a. The tester should be discouraged from creating these types of attacks as they are not realistic in the production environment
b. Immediately inform management that the attack was created by the test team as part of testing, in case it is detected
c. Work with the developers to implement checks such as SSL-trip to ensure certificates are valid and not self-signed
d. Check production to see if the vulnerability is also in the production code

Question #38 (1 pt)

Why is it important to reassess security risk expectations on a frequent basis?

a. Stakeholders have to be educated on all security risks at all times
b. Stakeholders will make business decisions based on associated security risk levels
c. Users must develop a manual-based risk mitigation plan
d. Both user and stakeholder expectations regarding security should be kept from changing

Question #39 (1 pt)

Which of the following is an important aspect of security test results?

a. They are published for users and stakeholders to access in order to help them better understand risk
b. They should be shared with developers across the enterprise in order to mitigate risk for future development projects
c. The fewer people that know the better
d. Results should always be classified by criticality

Question #40 (3 pts)

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

Question #41 (1 pt)

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

Question #42 (3 pts)

You have been given the job of testing the organization's firewall. You have reviewed the implementation plan and steps, verified that the configuration has been set up as instructed by the firewall vendor and have conducted port scanning. Your organization is particularly concerned about denial of service (DOS) attacks, particularly since they had one when the old firewall was in place. What type of testing should you conduct to help detect unexpected behavior that could be exploited by a DOS attack?

a. Create tests that will send malformed network packets or fuzzed data and see if they are detected and rejected by the firewall
b. Implement automated tests to stress test the servers to test the failover capabilities
c. Test the encryption and decryption algorithms to determine if they are fast enough to deal with the load of a DOS attack
d. Conduct software component hardening to ensure the attack surface is reduced as much as possible

Question #43 (1 pt)

If you have acquired a tool that is used under the GNU General Public License, which of the following is an important consideration for tool maintenance?

a. Reliability of the vendor and ability to provide support
b. Frequency and availability of updates from the vendor
c. Technical capabilities of your team to support and customize the tool for your environment
d. License cost and support contract cost

Question #44 (1 pt)

Which of the following is a benefit of conforming to security testing standards?

a. They are consistent and easy to follow as they are separate and independent from project goals and objectives
b. They are the building blocks for future security testing, eliminating the need to start from scratch
c. They outline an effective offense to meet threats before they enter the system
d. They allow for latitude in security practices since threats are always changing dynamically

Question #45 (1 pt)
What are advantages to imposing security standards in contracts?

a. They provide each party a legal exit when an unforeseen security issue adversely affects the product
b. They provide a starting place for both parties to begin their negotiations
c. They are a convenient way to make public the agreement between parties
d. They can change as standards change, even when the contract is finalized