Sample Exam - Answers
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 – point allocations for #25 - #32 fixed.
1.0 – GA	15 March 2016	GA version

Question #1 (1 pt)

B is correct as keeping the patch updates current on the system is one of the purposes of a security audit. The others are good practices, but not the purpose of the security audit.

Question #2 (3 pts)

C is correct as this is the source of the guidelines. The guidelines may change so it's important to keep the communications channels open with these folks. A, B and D all need to be informed, but the information needs to come from the federal and local agencies.

Question #3 (1 pt)

C is correct. When this policy is implemented, non-conforming devices will be removed until they conform. A is not correct as this would not be an expected results. B is not correct because these controls will be encouraged. D is not correct because access will be controlled, not severely limited.

Question #4 (3 pts)

B is correct. You should analyze the results of a security test to see if the policies and procedures have been followed and are effective. A is not correct because the static analysis should be over the code, if anything. C is not correct because the focus shouldn't just be on current threats and attacks, but also on configurations, etc. D is not correct because the focus is not just on the emerging threats.

Question #5 (1 pt)

A is correct per the syllabus. B is not correct because this information would probably not be helpful. C is not correct because the backup would likely be out of date and the information was not necessarily corrupted, but rather stolen or viewed. D is not correct because, although this may help point to areas where testing was not sufficient, it will not support the organization's defense of legal actions.

Question #6 (1 pt)

C is correct, security testing is a part of the larger area of information assurance.

Question #7 (2 pts)

B is correct because all of these are valid security objectives. A is not correct because 3 is functional rather than security-related (unless it locks them out, but we don't know that from this description). C is not correct because 6 and 7 are both functional rather than specific security requirements. D is not correct for the same reason as C.

Question #8 (2 pts)

C is correct per the syllabus as this is a common problem when the objectives are broadly defined. A and D are reasonable concerns, but you don't know when or how the test objectives will be defined, so

this may be controllable. B is always a possibility and may be the right thing to do in this case, but there has been no indication that outsourcing will occur at this time.

Question #9 (3 pts)

D is correct. At this point, the organization needs a high level policy and plan to move forward. Without this policy, the testing may continue to be sporadic and high level support and funding will be difficult. A and C are not correct at this point although they might be useful if you have trouble getting funding when you work to implement the policy. B is not right because you need an overall policy before you define the approach.

Question #10 (2 pts)

C is correct. The business customers will be most concerned with protection from fraudulent access as it is their data that is vulnerable. You would hope that A, B and D would also be involved, but this is not usually their primary benefit.

Question #11 (2 pts)

B is correct. The use of the conceptual tests to create the manual tests and perform the execution is part of the security test implementation. A and D are not correct because this has already been done with the creation of the conceptual tests. C will occur after the tests have been executed.

Question #12 (3 pts)

B is correct per the syllabus. A might be needed but that is not one of the minimum requirements and may already be understood in the roles and responsibilities section. C is not correct because the standards might be referenced but not included in the plan. D is not correct because this level of detail does not belong in the plan and the individual testers should not be contacted during a breach.

Question #13 (2 pts)

A is correct. B and C are not correct because of the word “several”. D is not correct because this would definitely not be a good security practice.

Question #14 (1 pt)

C is correct because the closer the test environment mimics production, the more valid the testing will be. This is particularly true when it comes to access rights and delegation settings. A is not correct because the system don’t need to be and probably shouldn’t be connected. B may be useful, but is not a main characteristic. D is not correct because it includes plug-ins that are not in production which could result in both false positives and false negatives from the testing.

Question #15 (1 pt)

A is correct. While some tools are quite good and effective for testing, they may be prohibited by some countries and some organizations. B is not correct because there is always a danger of deploying a

sub-optimal tool to deal with a crisis. A fast-track approval process makes sense, but a complete bypass is risky. C and D are not correct because there may be unknown risks from tools and it's better to do the due diligence in tool selection rather than deal with the consequences of a poorly selected tool.

Question #16 (3 pts)

B is correct. The first priority is to see if the problem exists in the production version. The defect should be documented only in a secure defect tracking system since the problem may exist in production. Since one XSS issue was found, there may be others so continued testing is warranted. A is not correct because the defect should not be publicized in the stakeholder report. C is not correct because while further testing is needed, notification is critical. D is not correct because of the stakeholder reporting.

Question #17 (1 pt)

A is correct. The checking should be done as soon as the code is written.

Question #18 (2 pts)

B is correct. A is not correct, although it is important that the documented requirements be protected from those who do not need to know. C is not correct because although they may be refined at the design level, they should be initially captured during the requirements definition phase. D is not correct because security requirements also need to include secure coding practices, etc.

Question #19 (3 pts)

C is correct. It is likely that this level of checking will slow down the system because it will have to check on each screen change. A and D are not correct because the fix should fix the problem. B is not correct because there should be no impact to usability (unless you are the hacker!).

Question #20 (1 pt)

B is correct. From a security testing standpoint, compiler warnings indicate potential issues that could lead to security gaps. A is not correct because warnings do not necessarily require a fix. C and D may be true, but are not related to security testing.

Question #21 (2 pts)

C is correct. New vulnerabilities may be present with the integrated components and new testing areas are likely to be available. A is not correct because component integration testing is not the sum of the individual components. B is not correct because the testing should not be limited to just the interfaces and the original components. D is not correct because security risks are likely to be increased, not decreased.

Question #22 (3 pts)

C is correct as this has one test for SQL injection and one for a valid input. This is the minimum number of tests. A and B have more than the minimum number and D doesn't have enough tests because it doesn't test the valid input. It would be advisable to do more testing on the various characters that can support SQL injection, but this question is asking to apply EP and get the minimum number of test cases.

Question #23 (2 pts)

A is correct as it covers the main scenarios for the functional security specified in the requirement. B tests only on the valid tests. C tests only the error conditions. D expands into attack testing as well as functional testing.

Question #24 (2 pts)

D is correct because it provides the acceptance criteria based on the requirement. 7 is tempting and would be logical, but it is not specified in the requirement. The others are not correct because they do not contain the proper criteria. 2 is incorrect where 3 is correct. 4 is incorrect where 5 is correct.

Question #25 (2 pts)

A is correct. There are security performance reports and metrics available that can be used to determine if you have achieved the right level of hardening. B is not correct because strong authentication is just one aspect of hardening. C is not correct because equilibrium is not needed. The more critical areas may warrant better hardening. D is not correct because there is the danger of the hacker not telling you what is found.

Question #26 (1 pt)

C is correct. It verifies that the user is legitimate and authorized. A is not correct because it is not looking at access rights. B is not correct because system resource utilization is not a consideration. D is not correct because common credential verification should not be used – each individual should have unique credentials.

Question #27 (2 pts)

C is correct per the syllabus. A is not correct because a minimum of 768 bits should be used. B is not correct because the random algorithm is easy to crack. D is not correct because WEP protocols should be left in place, not removed.

Question #28 (1 pt)

C is correct per the syllabus. A is incorrect because network zones do not focus on size of data. B is not correct. Network zones are parts of the configuration of the firewall and define the authorized flow of data between networks. D is not correct because the firewall blocks the traffic, not the network zone.

Question #29 (2 pts)

B is correct because these tests can be used to add new intrusive specifications which were formerly considered to be authorized traffic. A and C might be useful, but will not be as effective as B in making sure the tool will work for the future as well as the present. D is true for the usage, but not for the testing.

Question #30 (1 pt)

B is correct. The malware tool can only detect malware that it already knows about. B may be correct depending on the particular focus of the tool, but is not a main disadvantage. C is generally not true – the tools are normally easy to run. D is not correct because the tools provide the ability to update themselves with new findings and to produce reports.

Question #31 (2 pts)

B is correct per the syllabus. A brute force or dictionary attack can be used to see if personal information is still accessible. A is not correct because it is generally not feasible because of the amount of data and time it would take. C is not correct because this is more of an anonymizing exercise. Also, the field length might be limited so this may corrupt the data. D is not correct because we are not trying to stress test the database itself.

Question #32 (1 pt)

C is correct. It's the people and their behavior that is the weakest link. A, B and D are concerns, but C is the weakest link in the security chain.

Question #33 (1 pt)

A is correct. This information could be used to determine approval chains for invoice approvals which could then be used to create and approve fake invoices if the accounting system can be hacked. B is incorrect because the birth date should not be used in any employee information such as a password. C is incorrect because the company intranet should be behind the firewall with other protected information. D is not correct because this information is unlikely to be useful to a hacker.

Question #34 (2 pts)

D is correct and that is your biggest point of concern. A is not correct and could be a dangerous assumption. B is not correct because the hacker still has access to the system. C may be true, but re-running the same tests is not going to help with this issue.

Question #35 (1 pt)

C is correct. The biggest threat here is that the external protections are useless because the attacker is already inside the sytem. A and B are more likely to occur with an external attacker. D is not the most likely attack – generally internal users are after information they can sell or can use to embarass the company.

Question #36 (3 pts)

C is correct. It's the best place to start because it appears that this might have been where the problem originated. If C doesn't find anything, then A and D would be the next likely paths to pursue since it's possible this is an internal attack (D) or that the attacks are separate and the birthdate information might provide some information as to who has been near it. B might be pursued, but it would be easier to just ask the sys admin who would know the dog's name.

Question #37 (2 pts)

D is correct. The first priority is to see if the vulnerability is in the production code and get the problem fixed immediately. C should be the next step to ensure the developers are coding correctly and using all available tools to check for this type of issue. A is incorrect because this is exactly what security testers should be doing. B is incorrect because management permission should always be obtained prior to testing, not afterward.

Question #38 (1 pt)

B is correct. Stakeholders often have to make business decisions regarding the security risk level that is acceptable and any necessary mitigation plans. A is not correct because everyone doesn't need to know everything. C is not correct because a manual-based risk mitigation plan is not feasible and the users probably wouldn't be implementing this anyway. D is not correct because expectations should change.

Question #39 (1 pt)

C is correct. The results from security tests should be kept confidential and access to the results should be tightly controlled. This is because the outcome of the tests often identify weaknesses in the current system under test and often the same issues exist with the production system. A is not correct because of the need to tightly control access to the results. B is not correct because only limited parts of the report should be made available to the developers to improve their coding. Likewise, limited parts should be made available to infrastructure people to fix any infrastructure issues that may have been found. D is true, but is not the most important aspect.

Question #40 (3 pts)

C is correct. The risk impact should be described in the summary and detailed later in the report by discussing specific vulnerabilities. A is not correct because the details should not be in the summary. B is not correct because the information should not be recorded only at the end of the report. D is not correct because this is an important part of the report.

Question #41 (1 pt)

A is correct. B is incorrect because there are both dynamic and static analysis security tools. C is incorrect because memory leaks are detected by the general dynamic analysis tools, not the security specific ones. D is incorrect because this is true of all static analysis tools.

Question #42 (3 pts)

A is correct as both of these techniques are used to test firewalls. B and C are incorrect because the goal is to prevent the attack rather than let it get through the firewall. D is incorrect because software component hardening will help the individual software components, but not the firewall and its implementation.

Question #43 (1 pt)

C is correct. The GNU license is free and it is an open source community so there is no vendor. A and B are incorrect because there is no vendor. D is incorrect because the tool is free although you may have development costs in customizing the tool for your needs.

Question #44 (1 pt)

B is correct. A is not correct because security standards may be mentioned in the project goals and objectives. C is not correct because they are defensive in nature. D is not correct because they define certain standards that help define practices – the standards should be responsive to changes in the threats.

Question #45 (1 pt)

B is correct. By defining the security standards, each party can then determine what is required and further specify those requirements. A is not correct because it's too late then! C is not correct because the security agreements are likely to be kept private. D is not correct because contracts don't usually change in this way.