TECIS60441

Carry out information security testing activities

Overview

Information security testing is the activity of assessing a system for the presence of security weaknesses or vulnerabilities. Network or infrastructure security testing, involves assessing network devices, servers, and other network infrastructure services such as Domain Name Service (DNS) for security vulnerabilities. Application security testing generally refers to testing custom or commercial software applications for security vulnerabilities. Web application security testing is specifically focused on testing web applications and mobile application security testing is specifically focused on testing mobile applications.

There are a few common types of security testing used. A vulnerability assessment typically involves scanning for security issues using some combination of automated tools and manual assessment techniques to confirm the presence of a vulnerability without actually exploiting it. Penetration testing identifies and exploits vulnerabilities. The goal is to emulate a real attacker who can break into a system and steal or modify data or impact the systems availability. Runtime testing involves assessing the system for security issues from the perspective of an end user. Code review involves assessing an application by reviewing its source code. Not performing a code review leaves a system open to greater risk from malicious insider threats.

This standard covers the competencies required to conduct security testing in order to contribute to the determination of the level of resilience of an information system to information security threats and vulnerabilities. It includes selecting and applying testing methods, including penetration testing.

Performance criteria

You must be able to:

1. scope and plan the information security testing approach, to proactively target the most significant threats and vulnerabilities
2. use a range of appropriate methods, tools and techniques to conduct information security testing for the identification of vulnerabilities across multiple information systems
3. undertake information security tests, under controlled conditions, to assess compliance against relevant internal and/or external standards
4. design and implement tests plans for testing networks and application based information systems in line with organisational standards
5. interpret information assurance requirements to produce information security test acceptance criteria
6. design and develop accurate tests to ensure that information assurance requirements are tested against relevant internal and/or external standards
7. plan and execute attack based penetration testing to exploit vulnerabilities and identify specific security issues
8. critically review the results of information security testing, prioritising outcomes and recommending actions
9. communicate the results of information security testing to a range of audiences justifying and evidencing any recommendations on security issues and non compliance

Knowledge and understanding

You need to know and understand:

1. the specific threats that may be of particular importance to any particular information system
2. how to scope and plan an information security testing approach following standard procedures
3. the differences between vulnerability testing and penetration testing
4. how to develop and apply information security tests for both networks and applications
5. how to undertake vulnerability testing
6. how to undertake penetration testing
7. the range of tools and techniques that can be applied for information security testing, including vulnerability and penetration testing and how to apply them
8. relevant UK legislation and its impact on information security testing
9. how to interpret the results from information security testing
10. the importance of ensuring that information security testing is designed to ensure testing of all aspects of information systems across the core principles including: confidentiality, integrity, availability, authorisation, authentication and non-repudiation
11. the potential impact of the vulnerabilities identified on any information system and on the organisation
12. where to find the latest information on vulnerabilities or exploits and can design tests to identify them

Carry out information security testing activities

Developed by	e-skills
Version Number	1
Date Approved	March 2016
Indicative Review Date	April 2019
Validity	Current
Status	Original
Originating Organisation	The Tech Partnership
Original URN	TECIS60441
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, information security testing, penetration testing