TECIS60431

Contribute to 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 sets out the skills needed to identify and characterise threats, vulnerabilities and attacks on information systems. It also includes how to undertake information security testing.

Performance criteria

You must be able to:

1. identify threats, vulnerabilities and attacks that can occur in information systems in line with organisational standards
2. determine the different attack processes and methodologies that can be used to undertake an information security attack
3. assess the current threats to the organisation, analysing trends and highlighting information security issues relevant to the organisation
4. test for public domain vulnerabilities and the potential for exploitation, where appropriate by conducting exploits and reports potential issues and mitigation options
5. evaluate and classify threats in line with threat intelligence frameworks, organisational and external standards
6. accurately record and report on any vulnerabilities and threats identified during security testing

Knowledge and understanding

You need to know and understand:

1. the difference between threat, risk, attack and vulnerability
2. that threats exploit vulnerabilities to become attacks
3. where to find information about threats, vulnerabilities and attacks
4. what are the typical threats, attacks and exploits and the motivations behind them
5. how specific attacks work including denial of service, phishing and buffer overflow
6. the range of techniques for determining attack methods including reconnaissance, scanning, creation, test, attack/gain access, exfiltration & exiting/kill chain etc.
7. how users are targeted in an attack
8. why security testing cannot guarantee security
9. what is meant by vulnerability and penetration testing
10. the range of threats and vulnerabilities that need to be considered during penetration testing design and development activities
11. what the legal requirements for penetration testing are
12. the accepted penetration testing techniques, the range of methods and tools that are available and how to apply them
13. when and how to schedule information security testing
14. the importance of conducting information security tests routinely on existing services within the organisation
15. the importance of accurately recording and communicating the results of penetration tests

TECIS60431

Contribute to 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	TECIS60431
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