TECIS60451

Manage 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 defines the competencies concerning with managing security testing activities in order to contribute to the determination of the level of resilience of an information system to information security threats and vulnerabilities. This includes managing resources activities and deliverables. This includes planning, conducting and reporting on comprehensive penetration testing approaches, as well as designing and implementing organisational policies, standards and processes.

Performance criteria

You must be able to:

1. lead and manage an information security testing team, allocating resources effectively and implementing training and development in line with organisational requirements
2. design, implement and maintain the information security testing standards processes, procedures, methods, tools and techniques to reflect the changing nature of security threats and risks to the organisation
3. research, identify and incorporate up to date methods to test and identify vulnerabilities to network and information systems
4. select and specify the most appropriate tools to be used during information security testing activities
5. clearly define the scope of information security testing assignments in alignment with test scenarios and organisational requirements
6. design and execute controlled attacks on networks and information systems as part of a comprehensive penetration testing approach in line with organisational standards
7. review the vulnerabilities identified as a result of information security testing and identify the potential impact on the organisation's information systems and assets
8. critically review the results of information security testing, identifying security issues and determining priorities for action and/or escalation where appropriate
9. communicate the results of information security testing to a range of audiences, justifying and evidencing security issues and making recommendations on their remediation

Knowledge and understanding

You need to know and understand:

1. the purpose, limitations and utility of information security testing
2. how to use the range of tools and techniques that can be applied for information security testing
3. the role and importance of proactive information security testing activities, such as vulnerability and penetration testing to identify security issues within the organisation's network and information systems infrastructure and assets
4. the results and outcomes of information security testing activities in identifying security issues and informing and directing remediation activities
5. the importance in ensuring that information security testing is conducted proactively and routinely/regularly through the lifecycle and lifetime of network and information systems
6. the range of scanning and testing activities that can be used to identify vulnerabilities in an organisation's network and information system
7. the range of current, identified vulnerabilities that exist and need to be tested for
8. the importance of maintaining up to date reference information for new threats and vulnerabilities
9. the external standards, best practice frameworks and codes of conduct that an organisation's information systems infrastructure assets should comply with
10. how to design, develop and implement metrics for monitoring the security status of information, applications, systems and networks through information security testing
11. how to maintain lists of authorised or banned applications or devices for use on protective information security monitoring systems

TECIS60451

Manage 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	TECIS60451
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