TECIS60532

Contribute to information security vulnerability assessments

Overview

Vulnerabilities provide potential entry points through which a network or application, (typically a web site) can have its functionality or data damaged, downloaded, or manipulated. A typical Web site may have many potential vulnerabilities. Malware (malicious software or code) can be installed by hackers by exploiting security weaknesses to gain access to website and install malicious code.

Vulnerability analysis, also known as vulnerability assessment, is a process that defines, identifies, and classifies the security holes (vulnerabilities) in network or communications infrastructure and in information systems applications. In addition, vulnerability analysis can forecast the effectiveness of proposed information security countermeasures and evaluate their actual effectiveness after they are put into use. Vulnerability assessment seeks to identify both instances of malware on systems as well as system and network-level vulnerabilities.

This standard defines the competencies required to assist conducting vulnerability assessments under supervision. This includes following processes for planning and undertaking vulnerability assessments under supervision.

Performance criteria

You must be able to:

1. contribute to vulnerability assessments in line with organisational standards
2. collate information on the outputs from vulnerability assessments and identify vulnerabilities in networks and information systems that need investigating
3. communicate the outcomes of vulnerability assessments to relevant stakeholders on newly identified vulnerabilities
4. identify and report any instances of malware identified during vulnerability assessments
5. identify when and how to seek advice and guidance from other individuals during vulnerability assessment activities
6. assist in documenting the outcomes of vulnerability assessments in line with organisational standards

Knowledge and understanding

You need to know and understand:

1. the range of information assets on which vulnerability assessments need to be conducted
2. the processes, procedures, methods, tools and techniques relating to vulnerability assessment activities and how to apply them
3. how to conduct malware scanning and vulnerability assessments
4. the range of malware scanning and vulnerability assessment activities that can be used to identify malware and vulnerabilities in an organisation's information systems and assets
5. the range of known vulnerabilities that may compromise an organisation's infrastructure and information assets
6. the purpose of vulnerability assessments in maintaining information security
7. how to source up to date vulnerability information
8. the processes and procedures that need to be followed when undertaking vulnerability assessments and malware scanning
9. the importance of clearly communicating the outputs of vulnerability assessments and malware scanning

TECIS60532

Contribute to information security vulnerability assessments

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	TECIS60532
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, vulnerability assessment