



Australian Government

ICTCYS603 Undertake penetration testing for organisations

Release: 1

ICTCYS603 Undertake penetration testing for organisations

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 6.0.

Application

This unit describes the skills and knowledge required to use a range of methodologies to simulate an attack on an organisation's information and security systems and report the results back to the organisation.

It applies to those who work as network security specialists or administrators and conduct a simulated attack on an organisation's cyber assets to determine the effectiveness of the organisation's cyber security measures.

No licensing, legislative or certification requirements apply to this unit at the time of publication.

Unit Sector

Cyber security

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
<i>Elements describe the essential outcomes.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element.</i>
1. Prepare for penetration testing	1.1 Analyse organisation's existing cyber security environment, systems and network requirements 1.2 Identify individual data types and level of security requirements 1.3 Establish and outline goal and objectives of performing penetration testing 1.4 Evaluate scanning tools and select according to vulnerability assessment requirements 1.5 Establish and document testing regime and schedule, and requirements according to organisational procedures
2. Conduct penetration	2.1 Perform penetration test according to testing plan and

tests	procedures 2.2 Identify and document vulnerabilities arising from vulnerability assessment 2.3 Identify and document potential threats arising from penetration test according to organisational and testing procedures
3. Conduct follow up activities	3.1 Remediate identified vulnerabilities according to testing procedures 3.2 Determine and document improvement plan 3.3 Evaluate penetration testing effectiveness against testing plan and procedures 3.4 Escalate unresolved vulnerabilities to required personnel 3.5 Submit documentation to required personnel and seek and respond to feedback

Foundation Skills

This section describes those language, literacy, numeracy and employment skills that are essential to performance but not explicit in the performance criteria.

SKILL	DESCRIPTION
Numeracy	Uses mathematical formulae to determine requirements for penetration testing
Reading	Identifies information from technical, manufacturer and organisational documentation to determine and confirm job requirements
Writing	Prepares complex workplace documentation findings, threats and work performed using required structure, layout and required language
Planning and organising	Operates from a broad conceptual plan, developing the operational detail in stages, regularly reviewing priorities and performance during implementation, and identifying and addressing issues
Problem solving	Identifies context to recognise anomalies and subtle deviations to normal expectations, focusing attention and remedying problems as they arise
Self-management	Takes full responsibility for identifying and considering organisational protocols and requirements
Technology	Identifies principles, concepts, language and practices associated with the digital and cyber world

Unit Mapping Information

No equivalent unit. New unit.

Links

Companion Volume Implementation Guide is found on VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>

Assessment Requirements for ICTCYS603 Undertake penetration testing for organisations

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 6.0.

Performance Evidence

The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to:

- plan and implement penetration testing and resolve queries and vulnerabilities on at least three vulnerabilities.
- In the course of the above, the candidate must:
- identify weaknesses as part of penetration testing process.

Knowledge Evidence

The candidate must be able to demonstrate knowledge to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including knowledge of:

- security risks and vulnerabilities in software systems
- tools used in testing a network for vulnerabilities including scanning tools
- advanced level penetration testing of a system
- methods and tools used to protect data in an organisation
- risk mitigation strategies
- organisational procedures applicable to undertaking penetration testing, including:
- establishing goals and objectives of penetration testing
- defining scope of testing and establishment of testing regime
- documenting established requirements
- establishing penetration testing procedures
- documenting findings, threats and work performed
- key organisational environments, systems and networks required to undertake penetration testing for organisations.

Assessment Conditions

Skills in this unit must be demonstrated in a workplace or simulated environment where the conditions are typical of those in a working environment in this industry.

This includes access to:

- hardware, software and digital devices required to undertake penetration testing
- analytic platform and applicable user instructions
- data recognition software
- single security device and an organisation device
- legislative requirements and organisational policies and procedures applicable to undertaking penetrations testing.

Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

Links

Companion Volume Implementation Guide is found on VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>