



Australian Government

Department of Education, Employment and Workplace Relations

ICASAS517A Use network tools

Release: 1

ICASAS517A Use network tools

Modification History

Release	Comments
Release 1	This Unit first released with <i>ICA11 Information and Communications Technology Training Package version 1.0</i>

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to use tools to assist in managing a network effectively.

Application of the Unit

This unit applies to system administrators and network administrators who monitor security and resolve issues for the network.

Licensing/Regulatory Information

No licensing, legislative, regulatory or certification requirements apply to this unit at the time of endorsement but users should confirm requirements with the relevant federal, state or territory authority.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Element	Performance Criteria
<i>Elements describe the essential outcomes of a unit of competency.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element. Where bold italicised text is used, further information is detailed in the required skills and knowledge section and the range statement. Assessment of performance is to be consistent with the evidence guide.</i>

Elements and Performance Criteria

1. Use command line tools	1.1 Outline command-line environment 1.2 Differentiate command-line and graphical user interface (GUI) systems 1.3 List <i>command-line tools</i> 1.4 Apply command-line tools in <i>GUI environment</i>
2. Use hardware tools	2.1 Identify appropriate <i>hardware tools</i> and their function 2.2 Review OHS requirements for tool use 2.3 Manage network using hardware tools 2.4 Analyse test results
3. Use software tools	3.1 Identify appropriate <i>software tools</i> for network security 3.2 Recognise <i>areas of vulnerability</i> 3.3 Classify function of each tool 3.4 Manage network using software tools 3.5 Analyse test results

Required Skills and Knowledge

This section describes the skills and knowledge required for this unit.

Required skills

- analytical skills to:
 - anticipate and respond to a range of attacks
 - evaluate performance
 - identify and interrogate complex and varied areas of attack
 - interpret results of tests
- technical skills to:
 - develop and refine security of the network
 - resolve network vulnerabilities
 - test network functions and security.

Required knowledge

- available network tools
- processes and techniques related to using network tools
- range of attacks that affect network security
- problems and challenges relating to network security.

Evidence Guide

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Overview of assessment	
Critical aspects for assessment and evidence required to demonstrate competency in this unit	Evidence of the ability to: • identify and use appropriate tools for: • monitoring network performance • identifying network threats • isolating security breaches.
Context of and specific resources for assessment	Assessment must ensure access to: • maintenance procedures • network system • availability of hardware and software tools • security diagnostic software • appropriate learning and assessment support when required • modified equipment for people with special needs.
Method of assessment	A range of assessment methods should be used to assess practical skills and knowledge. The following examples are appropriate for this unit: • verbal or written questioning to assess candidate's knowledge of network tools • direct observation of candidate demonstrating use of appropriate network tools • evaluation of prepared report, outlining: • selection of appropriate tool • interpretation of output • recommendation of solution • evaluation of candidate's secured system.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, where appropriate. Assessment processes and techniques must be culturally appropriate, and suitable to the communication skill level, language, literacy and numeracy capacity of the candidate and the work being performed. Indigenous people and other people from a non-English speaking background may need additional support. In cases where practical assessment is used it should be combined

	with targeted questioning to assess required knowledge.
--	---

Range Statement

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

Command line tools may include:	• arp • arping • dig • hostname • ifconfig • ipconfig • mtr • nbtstat • netstat • nslookup • Ping • route • traceroute.
GUI environment may include:	• Linux platforms • Mac platforms • Windows platforms.
Hardware tools may include:	• butt set • cable stripper • cable testers • multimeter • optical time-domain reflectometer (OTDR) • protocol analyser • punch down tool • snips • temperature monitor • time-domain reflectometer (TDR) • toner probe • voltage event recorder.
Software tools may include:	• intrusion detection software • intrusion prevention software • packet sniffers or network analysers • port scanners • protocol analysers.

<i>Areas of vulnerability</i> may include:	• exploits • unsecured ports • wide-scale attacks • worms.
--	--

Unit Sector(s)

Systems administration and support