Australian Government

ICTNWK618 Design and implement a security system

Release: 1

ICTNWK618 Design and implement a security system

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 software tools, equipment and protocols to implement a security system.

It applies to individuals who work in ICT roles that involve the planning and implementing of networks, including budgeting, and determining and resolving network security threats.

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

Unit Sector

Networking

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
Elements describe the essential outcomes.	*Performance criteria describe the performance needed to demonstrate achievement of the element.*
1. Assess network infrastructure threats	1.1 Identify major industry standard network attacks and malware 1.2 Evaluate mitigation methods for required network attacks and malware according to organisational network architecture 1.3 Determine and document options for defending network architecture
2. Secure edge devices (routers)	2.1 Secure required network routers according to technical requirements 2.2 Secure required administration access to routers using the router operating system (OS) 2.3 Secure required router OS and its configuration file(s)

ELEMENT	PERFORMANCE CRITERIA
3. Implement authentication, authorisation and accounting (AAA) and secure access control system (ACS)	3.1 Determine and implement required authentication and authorisation 3.2 Configure router and use AAA according to technical requirements 3.3 Analyse and compare Terminal Access Controller Access-Control System Plus (TACACS+) and Remote Authentication Dial In User Service (RADIUS) AAA protocols for securing the network
4. Mitigate threats to routers and networks using access control lists (ACLs)	4.1 Assess and document access control list functionality and requirements 4.2 Configure and verify IP ACLs to mitigate threats and prevent internet protocol (IP) address spoofing 4.3 Test IP ACLs functionality against organisational and technical requirements
5. Implement secure network management and reporting	5.1 Configure secure shell (SSH) on routers and enable secure management 5.2 Configure routers to send log messages to a log server with tools 5.3 Document layer two attack prevention methods and confirm basic switch security features 5.4 Configure layer two attack prevention switch
6. Implement intrusion detection and prevention system (IDPS) feature set in the router OS using secure device manager (SDM)	6.1 Evaluate and compare network based and host based IDPS and identify malicious activity, log information, attempt to stop activity and document reported activity 6.2 Determine IDPS technologies, attack responses and monitoring options 6.3 Configure router OS IDPS operations according to organisational and technical requirements 6.4 Finalise reports and documentation and submit to required personnel

Foundation Skills

This section describes language, literacy, numeracy and employment skills incorporated in the performance criteria that are required for competent performance.

SKILL	DESCRIPTION
Numeracy	• Interprets numerical data when taking test measurements,

SKILL	DESCRIPTION
	interpreting results and evaluating performance and interoperability of the network
Oral communication	• Establishes and maintains complex and effective spoken communication to convey and clarify a range of complex information
Reading	• Recognises and interprets technical documentation to determine and confirm job requirements
Writing	• Develops a broad range of materials, such as reports, for a specific audience using clear and detailed language to convey explicit information
Teamwork	• Actively identifies the requirements of important communication exchanges, selecting required channels, format, tone and content to suit purpose and audience and monitors impact • Actively identifies, creates and utilises linkages to enhance knowledge sharing, idea creation, individual and collective engagement and work outcomes
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	• Responds intuitively to problems requiring immediate resolution, using knowledge of context to recognise anomalies and deviations from normal expectation in a network environment
Self-management	• Uses a broad range of strategies to store, access and organise virtual information, recognising that design choices will influence what information is retrieved and how it may be interpreted and used • Demonstrates an acute awareness of the importance of knowledge, monitoring and controlling access to digitally stored and transmitted information • Monitors outcomes of decisions, considering results from a range of perspectives and identifying key concepts and principles that may be adaptable to future situations
Technology	• Considers the strategic and operational potential of digital trends to achieve work goals, enhance work processes, create opportunities and enhance or reduce risks

Unit Mapping Information

Supersedes and is equivalent to ICTNWK601 Design and implement a security system.

Links

Companion Volume Implementation Guide is found on VETNet - https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2