Australian Government

ICTNWK601 Design and implement a security system

Release: 1

ICTNWK601 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 1.0.

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 plan and implement networks, are involved in business budgeting, and determine and resolve 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 the security threats facing network Infrastructure	1.1 Evaluate mitigation methods for network attacks and different types of malware 1.2 Propose a methodical concept of defending network architecture
2. Secure edge devices (routers)	2.1 Secure network routers using software tools 2.2 Secure administration access to routers using the router operating system (OS) 2.3 Secure router OS and its configuration file(s)
3. Implement authentication, authorisation and	3.1 Evaluate and implement the functions and importance of authentication, authorisation and accounting

ELEMENT	PERFORMANCE CRITERIA
accounting (AAA) and secure access control system (ACS)	3.2 Configure the router using AAA 3.3 Analyse and compare the features of 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 the functionality of access control lists and document the caveats to be considered when building them 4.2 Configure and verify IP ACLs to mitigate threats and to prevent internet protocol (IP) address spoofing using tools
5. Implement secure network management and reporting	5.1 Configure secure shell (SSH) on routers to enable secure management 5.2 Configure routers to send log messages to a log server with tools
6. Mitigate common layer 2 attacks	6.1 Document how to prevent layer 2 attacks by configuring basic switch security and features 6.2 Configure switch to prevent layer 2 attacks
7. Implement the router OS firewall-feature set	7.1 Evaluate and compare the operational strategies and weaknesses of the different firewall technologies 7.2 Implement zone-based firewall to strategically secure group of interfaces
8. Implement the intrusion detection and prevention system (IDPS) feature set in the router OS using secure device manager (SDM)	8.1 Evaluate and compare network based versus host based IDPS to identify malicious activity, log information, attempt to block/stop activity, and report activity 8.2 Determine IDPS technologies, attack responses and monitoring options 8.3 Configure the router OS IDPS operations using secure device manager to monitor network and system activities for malicious activity
9. Implement site-to-site virtual private networks (VPNs) using SDM	9.1 Assess the different methods used in cryptography 9.2 Evaluate internet key exchange (IKE) protocol functionality and phases to support authentication and define the binding blocks of IPSec and the security functions it provides 9.3 Configure and verify an IPSec site-to-site VPN with pre-shared key (PSK) authentication to provide a secure channel between the two parties

Foundation Skills

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

Skill	Performance Criteria	Description
Reading	1.1	• Recognises and interprets technical documentation to determine and confirm job requirements
Writing	1.2, 4.1, 6.1, 8.1, 8.2,	• Develops a broad range of materials, such as reports, for a specific audience using clear and detailed language to convey explicit information
Oral Communication	8.2	• Establishes and maintains complex and effective spoken communication to convey and clarify a range of complex information
Numeracy	9.2	• Interprets numerical data when taking test measurements, interpreting results and evaluating performance and interoperability of the network
Interact with others	1.2, 8.1	• Actively identifies the requirements of important communication exchanges, selecting appropriate channels, format, tone and content to suit purpose and audience, and monitors impact
Get the work done	1.1, 2.1-2.3, 3.1-3.3, 4.1, 4.2, 5.1, 5.2, 6.2, 7.1, 7.2, 8.1, 8.3, 9.1-9.3	• Considers the strategic and operational potential of digital trends to achieve work goals, enhance work processes, create opportunities and enhance or reduce risks • Actively identifies, creates and utilises linkages to enhance knowledge sharing, idea creation, individual and collective engagement and work outcomes • 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 • Is acutely aware of the importance of understanding, monitoring and controlling access to digitally stored and transmitted information • May operate from a broad conceptual plan, developing the operational detail in stages,

		regularly reviewing priorities and performance during implementation, and identifying and addressing issues • Monitors outcomes of decisions, considering results from a range of perspectives and identifying key concepts and principles that may be adaptable to future situations • Responds intuitively to problems requiring immediate resolution, using understanding of context to recognise anomalies and deviations from normal expectation in a network environment

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTNWK601 Design and implement a security system	ICANWK601A Design and implement a security system	Updated to meet Standards for Training Packages	Equivalent unit

Links

Companion Volume implementation guides are found in VETNet - https://vetnet.education.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2