Australian Government

ICTNWK622 Configure and manage intrusion prevention system on network sensors

Release: 1

ICTNWK622 Configure and manage intrusion prevention system on network sensors

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 required tools, equipment and software to implement an intrusion prevention system (IPS) on IPS sensors to mitigate network attacks.

It applies to individuals with advanced Information and Communications Technology (ICT) skills who are working as certified IPS specialists, network security specialists and network security managers.

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. Evaluate ways IPS sensors are used to mitigate network attacks	1.1 Evaluate inline operations network system requirements according to industry standards and organisational requirements 1.2 Evaluate inline to promiscuous mode sensor operations and IPS devices network protection capability 1.3 Evaluate and determine ways IPS can defeat evasive network hacking methods 1.4 Evaluate selection considerations, placement and deployment of network IPS and IPS signature
2. Select, install and configure	2.1 Install, initialise and configure sensor interfaces,

ELEMENT	PERFORMANCE CRITERIA
IPS sensors	interface pairs, virtual local area network (VLAN) pairs and VLAN groups 2.2 Configure management access to sensor appliance and create required user accounts 2.3 Set up, manage and monitor sensor communications with external management and monitoring systems and use built-in tools 2.4 Upgrade IPS sensor parameters and licensing requirements and maintain network integrity 2.5 Plan mitigation of specific network vulnerabilities and exploits according to organisational requirements
3. Tune IPS sensor advanced system parameters	3.1 Tune sensor signatures and provide optimal protection of network 3.2 Create custom and meta signatures and align to mitigation performance requirements 3.3 Configure passive operating system (OS) fingerprinting gateway 3.4 Configure external product interface to receive and process information from external security and management products 3.5 Configure a virtual sensor and anomaly detection
4. Manage IPS security and network response attacks	4.1 Monitor IPS events and determine network attack response 4.2 Assess IPS effectiveness against security intrusion 4.2 Report on security and response attacks according to organisational requirements

Foundation Skills

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

SKILL	DESCRIPTION
Learning	• Demonstrates a sophisticated knowledge of principles, concepts, language and practices associated with the digital world and uses these to troubleshoot and understand the uses and potential of new technology • Demonstrates knowledge that identified ‘problems’ can be surface indicators of deeper issues and routinely reframes problem definitions as part of the process of identifying a root cause

SKILL	DESCRIPTION
Numeracy	• Selects from and flexibly applies, a wide range of highly developed mathematical and problem-solving strategies and techniques in a broad range of contexts
Reading	• Recognises and interprets complex technical and regulatory information to determine and confirm job requirements
Writing	• Demonstrates sophisticated writing skills by selecting required conventions and stylistic devices to express precise meaning • Writes and edits complex computer code and technical data, ensuring correct syntax and accuracy
Teamwork	• Develops and implements communications strategies with internal and external persons • Shares knowledge, information and experience openly as an integral part of the working relationship
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	• 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 • Uses a mix of intuitive and formal processes to identify key information and issues, evaluate alternative strategies, anticipate consequences and consider implementation issues and contingencies
Self-management	• Understands own legal rights and responsibilities and considers implications of these when planning and undertaking work • Demonstrates an acute awareness of the importance of knowledge, monitoring and controlling access to digitally stored and transmitted information

Unit Mapping Information

Supersedes and is equivalent to ICTNWK609 Configure and manage intrusion prevention system on network sensors.

Links

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