



Australian Government

ICTNWK609 Configure and manage intrusion prevention system on network sensors

Release: 1

ICTNWK609 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 1.0.

Application

This unit describes the skills and knowledge required to use appropriate 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
<i>Elements describe the essential outcomes.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element.</i>
1. Evaluate the ways IPS sensors are used to mitigate network attacks	1.1 Evaluate system requirements of the network according to industry standards for inline operations 1.2 Compare inline to promiscuous mode sensor operations and evaluate how IPS protects network devices from attacks 1.3 Evaluate the evasive techniques used by hackers and determine ways IPS can defeat those techniques in the network 1.4 Evaluate the considerations necessary for selection, placement, and deployment of a network IPS, including using features of IPS signature

ELEMENT	PERFORMANCE CRITERIA
2. Select and install IPS sensors and configure essential system parameters	2.1 Install and initialise the sensor for configuration of sensor interfaces, interface pairs, virtual local area network (VLAN) pairs and VLAN groups 2.2 Configure management access to the sensor appliance and create user accounts to comply with different user roles 2.3 Set up sensor communications with external management and monitoring systems 2.4 Manage and monitor sensor operation using built-in tools 2.5 Upgrade and maintain IPS sensor parameters and licensing requirements to maintain network integrity 2.6 Plan the mitigation of specific network vulnerabilities and exploits
3. Tune IPS sensor advanced system parameters to optimise attack mitigation performance	3.1 Tune sensor signatures to provide optimal protection of the network 3.2 Create custom signatures and a meta signature to meet mitigation performance configurations for given test scenarios while disabling alert production for the component signatures 3.3 Configure gateway for passive operating system (OS) fingerprinting 3.4 Configure the external product interface to receive and process information from external security and management products to automatically enhance the sensor configuration information 3.5 Configure a virtual sensor and anomaly detection 3.6 Monitor the IPS advanced features for optimal performance
4. Manage security and response of the IPS to network attacks	4.1 Monitor IPS events using network tools to determine appropriate response to network attacks 4.2 Use network management tools to assess and manage IPS effectiveness against security intrusion

Foundation Skills

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

Skill	Performance	Description
-------	-------------	-------------

	Criteria	
Reading	1.1-1.4	Recognises and interprets complex technical and regulatory information to determine and confirm job requirements
Writing	2.2, 2.5, 3.3-3.5	- Demonstrates sophisticated writing skills by selecting appropriate conventions and stylistic devices to express precise meaning - Writes and edits complex computer code and technical data, ensuring correct syntax and accuracy
Numeracy	2.2-2.4, 3.6, 4.1	Selects from, and flexibly applies, a wide range of highly developed mathematical and problem solving strategies and techniques in a broad range of contexts
Navigate the world of work	1.1, 2.5	Understands own legal rights and responsibilities, and considers implications of these when planning and undertaking work
Interact with others	2.2, 2.3, 3.4,	- Develops and implements communications strategies with internal and external persons - Shares knowledge, information and experience openly as an integral part of the working relationship
Get the work done	1.1-1.4, 2.1-2.6, 3.1-3.6, 4.1, 4.2	- Demonstrates a sophisticated understanding 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 - 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 - 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 - Recognises 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

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTNWK609 Configure and manage intrusion prevention system on network sensors	ICANWK609A Configure and manage intrusion prevention system on network sensors	Updated to meet Standards for Training Packages.	Equivalent unit

Links

Companion Volume implementation guides are found in VETNet -

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

Assessment Requirements for ICTNWK609 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 1.0.

Performance Evidence

Evidence of the ability to:

- evaluate intrusion prevention system (IPS) requirements and configure IPS sensors
- tune up IPS sensors to optimise attack mitigation
- use network tools and network management tools to monitor and manage security sensor events
- upgrade and maintain IPS sensors.

Note: If a specific volume or frequency is not stated, then evidence must be provided at least once.

Knowledge Evidence

To complete the unit requirements safely and effectively, the individual must:

- explain configuration, verification and troubleshooting procedures to undertake a switch and router operation and routing protocol
- outline deployment schemes
- summarise setting up and securing firewalls
- summarise internetwork operating system (IOS) and internet protocol (IP) networking models
- explain IP addressing and detailed understanding of the transmission control protocol (TCP) or IP stack
- outline IPS and intrusion detection system (IDS) strategies
- explain IPS sensor technologies and licensing requirements
- outline local area network or wide area network (LAN/WAN) implementations and design
- summarise network topologies, architectures and elements
- outline networking standards and protocols
- explain signatures and meta signatures
- explain threat mitigation strategies

- explain virtual local area network (VLAN) concepts and functionality
- outline virtual private network (VPN) technologies
- identify and describe legislation, regulations, standards and codes of practice relevant to network security.

Assessment Conditions

Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the networking industry, and include access to:

- a site or prototype where network installation may be conducted
- relevant hardware and software
- organisational guidelines
- live network
- an IPS system and its sensors.

Assessors must satisfy NVR/AQTF assessor requirements.

Links

Companion Volume implementation guides are found in VETNet -

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