Australian Government

Department of Education, Employment and Workplace Relations

ICANWK609A Configure and manage intrusion prevention system on network sensors

Release: 1

ICANWK609A Configure and manage intrusion prevention system on network sensors

Modification History

Release	Comments
Release 1	This Unit first released with *ICA11 Information and Communications Technology Training Package version 1.0*

Unit Descriptor

This unit describes the performance outcomes, 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.

Application of the Unit

This unit applies to the use of IPS and signatures of IPS sensors, installation and configuration of advanced features, analysis of IPS sensor events as well as the upgrade and maintenance of IPS systems. Relevant job roles include certified IPS specialist, network security specialist and network security manager.

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
Elements describe the essential outcomes of a unit of competency.	*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.*

Elements and Performance Criteria

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
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

Required Skills and Knowledge

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

Required skills

- communication skills to liaise with internal and external personnel on technical, operational and business-related matters
- literacy skills to:
  - interpret technical documentation
  - write reports as required
- numeracy skills to:
  - interpret results and evaluate performance and interoperability of network
  - take test measurements
- planning and organisational skills to:
  - coordinate the process in liaison with others
  - plan, prioritise and monitor own work
- problem-solving and contingency-management skills to:
  - adapt configuration procedures to requirements of network
  - reconfigure depending on differing operational contingencies, risk situations and environments
  - debug networking entities configuration issues
  - troubleshoot
- research skills to investigate appropriate hardware to meet requirements
- technical skills to:
  - assess and implement security requirements
  - select and configure networking devices
  - use calling line identification (CLI) and the web interface in configuration of network entities
  - use networking and network management tools.

Required knowledge

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

- signatures and meta signatures
- threat mitigation strategies
- VLAN concepts and functionality
- VPN technologies.

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: • evaluate 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.
Context of and specific resources for assessment	Assessment must ensure access to: • site or prototype where network installation may be conducted • relevant hardware and software • organisational guidelines • live network • IPS system and its sensors • 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: • direct observation of the candidate installing, configuring and testing a new or updated network • evaluation of documentation prepared by the candidate outlining testing procedures, test results, recommendation to network changes and completion records • verbal or written questioning of required knowledge.
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.

System requirements may refer to:	• application • business • network • people in the organisation • system.
Network may include:	• data • firewall • IDS • internet • IPS • large and small LAN • protocol • WAN • wireless LAN (WLAN).
Industry standards may include:	• Australian Standards (AS) • International Electrotechnical Commission (IEC) • International Organization for Standardization (IOS) • security policy and procedures.
Configuration of sensor interfaces may include:	• allowed hosts • assignment of virtual sensors • creation of pairs • enabling • software bypass.
User may include:	• external • internal • remote access • temporary.

Sensor parameters and licensing requirements may include:	• application of software images and upgrades
	• configuration of files:
	  • file transfer protocol (FTP)
	  • hypertext transfer protocol (HTTP)
	  • hypertext transfer protocol secure (HTTPS)
	  • service control point (SCP)

	• installation of sensor licence • installation of signature update of file names • performing sensor password recovery.
Mitigation-performance configurations may include:	• event action filters • event variables • general settings for event action rules • response actions based on risk taking • target value ratings.

Test scenarios may include:	• exploiting the network:
	  • denial of service (DOS) and OS exploitation and countermeasures
	  • eavesdropping and interception attacks and countermeasures
	  • infrastructure flooding attacks and countermeasures
	• simple network reconnaissance:
	  • dynamic host configuration protocol (DHCP) response sniffing and spoofing and countermeasures
	  • hacking devices and hacking countermeasures
	  • port scanning and port scanning countermeasures
	  • sniffing and sniffing countermeasures.

Network tools may include:	• command line interface (CLI) • IPS device manager • IPS event viewer.
Network management tools may include:	• intrusion attacks • network security management • sniffer trace.

Unit Sector(s)

Networking