Australian Government

Department of Education, Employment and Workplace Relations

ICANWK602A Plan, configure and test advanced server based security

Release: 1

ICANWK602A Plan, configure and test advanced server based security

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 implement advanced server security using secure authentication and network services on a network server.

Application of the Unit

This unit applies to planning, designing, implementing, maintaining, monitoring and troubleshooting advanced security on network servers.

Relevant job roles include information and communications technology (ICT) network specialist, ICT network engineer, network security specialist, network security planner and network security designer.

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. Plan advanced network-server security according to business needs	1.1 Consult with ***client*** and key ***stakeholders*** to identify security requirements in an advanced ***network server*** environment 1.2 Analyse and review existing ***client security documentation*** and predict network service vulnerabilities 1.3 Research ***network authentication*** and ***network service*** configuration options and implications to produce network security solutions 1.4 Ensure features and capabilities of network service security options meet the business needs 1.5 Produce or update server security design documentation to include new solutions 1.6 Obtain sign-off for the security design from the ***appropriate person***
2. Prepare for network-server security implementation	2.1 Prepare for work in line with site-specific safety requirements and enterprise OHS processes and procedures 2.2 Identify safety hazards and implement risk control measures in consultation with appropriate personnel 2.3 Consult appropriate person to ensure the task is coordinated effectively with others involved at the worksite 2.4 Back up server before implementing configuration changes
3. Configure the advanced network-server security according to design	3.1 Configure ***update services*** to provide automatic updates to ensure maximum security and reliability 3.2 Configure network authentication, authorisation and accounting services to log and prevent unauthorised access to the server 3.3 Configure ***basic service security*** and access control lists to limit access to authorised users, groups or networks 3.4 Implement ***encryption*** as required by the design 3.5 Configure advanced network service ***security options for services*** and ***remote access*** 3.6 Configure the ***operating system*** or ***third-party firewall*** to filter traffic in line with security requirements 3.7 Ensure security of server logs and log servers are appropriately implemented for system integrity 3.8 Implement ***backup and recovery*** methods to enable restoration capability in the event of a disaster
4. Monitor and test	4.1 Test server to assess the effectiveness of network service

network-server security	security according to agreed design plan 4.2 Monitor server logs, network traffic and open ports to detect possible intrusions 4.3 Monitor important files to detect unauthorised modifications 4.4 Investigate and verify alleged violations of server or data security and privacy breaches 4.5 Recover from, report and document security breaches according to security policies and procedures 4.6 Evaluate monitored results and reports to implement and test improvement actions required to maintain the required level of network service security

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 security-related matters
- literacy skills to:
  - interpret technical documentation
  - write reports in required formats
  - read and interpret enterprise security procedures, policies and specifications
  - review vendor sites, bulletins and notifications for security information
- planning and organisational skills to:
  - plan control methods for network service security and authentication
  - plan, prioritise and monitor own work
- problem-solving and contingency-management skills to:
  - adapt configuration procedures to requirements of network service security and reconfigure depending on differing operational contingencies, risk situations and environments
  - detect, investigate and recover from security breaches
- safety-awareness skills to:
  - apply precautions and required action to minimise, control or eliminate hazards that may exist during work activities
  - follow enterprise OHS procedures
  - work systematically with required attention to detail without injury to self or others, or damage to goods or equipment
- research skills to interrogate vendor databases and websites to implement different configuration requirements to meet security levels
- technical skills to:
  - design network service and authentication security
  - identify the technical requirements, constraints and manageability issues for given customer server-security requirements
  - implement security strategies
  - install network service and authentication security design
  - monitor log files for security information
  - select and use server and network diagnostics
  - test server security.

Required knowledge

- auditing and penetration testing techniques
- best practice procedures for implementing backup and restore
- cryptographic techniques
- procedures for error and event logging and reporting

- intrusion detection and recovery procedures
- network service configuration, including DNS, DHCP, web, mail, FTP, SMB, NTP and proxy
- network service security features, options and limitations
- network service vulnerabilities
- operating system help and support utilities
- planning, configuration, monitoring and troubleshooting techniques
- security protection mechanisms
- security threats and risks
- server firewall configuration
- server monitoring and troubleshooting tools and techniques, including network monitoring and diagnostic utilities
- user authentication and directory services.

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: • identify network service security vulnerabilities and appropriate controls • plan, design and configure a secure network authentication service • secure a wide range of network services to ensure server and data security including: DNS, web and proxy, mail, FTP and firewall • implement cryptographic techniques • monitor the server for security breaches.

Context of and specific resources for assessment	Assessment must ensure access to:
	• site where server installation may be conducted
	• relevant server specifications:
	  • cabling
	  • networked (LAN) computers
	  • server diagnostic software
	  • switch
	  • client requirements
	  • WAN service point of presence
	  • workstations
	• relevant regulatory documentation that impacts on installation activities
	• 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: • evaluation of security design report for a server with complex network service security requirements • direct observation of the candidate configuring complex security requirements • verbal or written questioning of required skills and knowledge • evaluation of prepared report outlining intrusion detection,

	recovery, reporting and documentation procedures • evaluation of system design and implementation in terms of network service security and suitability for business needs.
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.

Client may include:	• external organisations • ICT company • individuals • internal departments • internal employees • service industry.
Stakeholders may include:	• development team • IT manager or representative • project team • sponsor • user.
Network server may include:	• applications server • communications server • content and media server • multiple servers • physical server • virtual server.
Client security documentation may include:	• risk assessment reports • security incident reports and server logs • security plans • security policies • security procedures.
Network authentication may include:	• biometrics • enterprise single sign-on • Hesiod • Kerberos • lightweight directory access protocol (LDAP) • Novell Directory Services (NDS) • network information service (NIS) • pluggable authentication modules (PAM) • public key authentication (PKA) • public key infrastructure (PKI) and digital certificates • Red Hat Directory Services (RHDS) • security tokens and smart cards

	• SMB or Samba software • two-factor and multifactor authentication • Windows Active Directory Services (WADS).

Network service may include:	• dynamic host configuration protocol (DHCP)
	• dynamic name system (DNS)
	• firewall
	• file transfer protocol (FTP)
	• hypertext transfer protocol (HTTP) or secure (HTTPS)
	• internet message access protocol (IMAP)
	• network authentication:
	  • remote procedure call (RPC)
	  • NIS
	  • Kerberos
	• network file system (NFS)
	• network time protocol (NTP)
	• open source secure shell software suite (open SSH)
	• post-office protocol (POP)
	• print services
	• proxy
	• server messages block (SMB)
	• simple mail transfer protocol (SMTP)
	• simple network management protocol (SNMP)
	• structured query language server (SQL)
	• transmission control protocol or internet protocol (TCP/IP).

Appropriate person may include:	• authorised business representative • client • representative from the IT department • supervisor • security manager.
Update services may include:	• Potentially Unwanted Program Remover (PUP) • Red Hat Network • Windows Server Update Services • Yellow Dog Update Manager (YUM).
Basic service security may include:	• host-based access control • network service access control lists (ACL) • network service authentication • network share permissions • security-enhanced Linux (SE Linux) • TCP wrappers • Windows group policy • eXtended interNET Daemon (xinetd) and service limits.

Encryption may include:	• asymmetric encryption • certificate authority configuration • digital signatures and signature verification • email encryption • encrypted file systems • encrypted network traffic • GNU Privacy Guard (GnuPG or GPG) • public key infrastructure (PKI) • secure sockets layer (SSL) certificates • symmetric encryption.

Security options for services may include:	• network file services security options, such as:
	  • disk quotas
	  • distributed file system security
	  • encrypted file systems
	  • NFS security
	  • shares and their permissions
	  • SMB or Samba security options
	• name resolution services, such as:
	  • bogus servers and blackholes
	  • DNS topologies
	  • dynamic DNS security
	  • restrictive zone transfers and recursive queries
	  • transaction signatures
	  • transaction signature (TSIG)
	  • views
	• web and proxy services, such as:
	  • authentication
	  • common gateway interface (CGI) security
	  • server-side includes
	  • SSL certificates
	  • suEXEC
	• mail services, such as:
	  • email encryption
	  • mail filtering including spam filtering
	  • mail topology design
	  • secure sockets layer and transport layer security protocols (SSL/TLS)
	  • start transport layer security (STARTTLS)
	  • virus scanning
	• FTP services, such as:

	• anonymous FTP • FTP authentication • secure access to home directories.
Remote access security options may include:	• dial-up • internet connection sharing (ICS) • inbound and outbound filters • network address translation (NAT) • open SSH • port forwarding • remote authentication dial-in user service (RADIUS) • RADIUS proxy • remote access policy • routing and remote access services (RRAS) • secure remote access protocols • secure wireless • terminal services • virtual private network (VPN).
Operating system may include:	• Linux • Unix • Windows server.
Third-party firewall may include:	• incoming and outgoing traffic filtering • iptables • internet security and acceleration (ISA) server • kernel level firewalls • Microsoft Windows Firewall • netfilter • SmoothWall • traffic filtering by ports and protocols.
Backup and recovery may include:	• automated backups using operating system backup and job scheduling tools • backup and recovery of mail systems • backup and recovery of network directory service objects • backups using third party software • database backup and recovery • volume shadow copies.

Unit Sector(s)

Networking