

COMPUTER NETWORK SECURITY CONFIGURATION

ISCED UNIT CODE: 0612 451 06A

TVET CDACC UNIT CODE: IT/CU/NSA/CR/04/5/MA

Relationship to Occupational Standards

This unit addresses the Unit of Competency: Configure Computer Network Security

Unit Duration: 210 Hours

Unit Description

This unit covers the competencies required to configure computer network security. It involves conducting computer network risk assessment, performing computer network segmentation, configuring computer network firewall and conducting computer network security user training.

Summary of Learning Outcomes

LEARNING OUTCOMES	DURATION (HOURS)
1. Conduct Computer Network Risk Assessment	50
2. Perform Computer Network Segmentation	60
3. Configure Computer Network Firewall	60
4. Conduct Computer Network Security User Training	40
TOTAL	210

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Conduct computer network risk assessment	1.1 Inventory of computer network 1.1.1 Introduction of computer network inventory. 1.1.2 Types of computer network inventory. 1.1.2.1 Hardware inventory 1.1.2.2 Software inventory	● Practical test ● Project ● Portfolio of evidence ● Oral questioning

	1.1.2.3 IP address inventory 1.1.2.4 Device configuration inventory 1.2 Identify and prioritize security threats and vulnerabilities 1.2.1 Introduction to computer network, security threats and vulnerabilities. 1.2.2 Categories of computer network, security threats 1.2.2.1 Internal (Outdated or unpatched software Misconfigured firewalls / operating systems, Denial of service, Man in the middle attack etc) 1.2.2.2 External (Malware attacks, Social engineering attacks, Phishing etc) 1.2.3 Types of computer network vulnerabilities. 1.3 Develop security Controls 1.3.1 Introduction to computer network security controls. 1.3.2 Types of computer network security controls. 1.3.2.1 Preventive 1.3.2.2 Detective controls 1.3.2.3 Corrective controls 1.3.2.4 Deterrent controls 1.3.2.5 Compensating controls 1.3.2.6 Administrative control 1.3.2.7 Logical/technical control 1.3.2.8 Physical controls 1.3.2.9 Technological controls 1.4 Risk assessment documentation 1.4.1 Meaning of computer network Risk Assessment Report	● Interviews ● Third party report ● Written tests ● Case study
--	---	---

	1.4.2 Types of computer network Risk Assessment Report. 1.4.2.1 Qualitative Risk Assessment Report 1.4.2.2 Quantitative Risk Assessment Report 1.4.2.3 Operation Risk Assessment Report	
2. Perform computer network segmentation	2.1 IP addressing scheme. 2.1.1 IP addressing and subnetting 2.1.2 IP address fundamentals 2.1.2.1 Physical address. MAC address. 2.1.2.2 Logical address. IP address. 2.1.2.3 Hostname. 2.1.2.4 IPv4 vs. IPv6 2.1.2.5 Classful addressing 2.1.2.6 Static vs. Dynamic IP Addressing 2.1.2.7 Public vs. Private IP Addresses 2.1.3 Steps in Designing an IP Addressing Scheme 2.2 Network segmentation 2.2.1 Introduction to network segmentation 2.2.1.1 Definition of network segmentation 2.2.1.2 Physical & logical segmentation 2.2.1.3 Importance of network segmentation 2.2.2 Types of network segmentation 2.2.2.1 IP based 2.2.2.2 VLANs 2.2.2.3 Subnetting 2.2.2.4 Firewalls 2.2.2.5 Physical segmentation 2.2.3 Tools and techniques for network segmentation	● Practical test ● Project ● Portfolio of evidence ● Oral questioning ● Interviews ● Third party report ● Written tests ● Case study

	2.2.3.1 Firewalls, Routers, and Access Control Lists (ACLs) 2.2.3.2 Network Access Control (NAC) 2.2.4 Monitoring and Managing Network Segments 2.3 Network privileges. 2.3.1 Introduction to network privilege management 2.3.1.1 Definition of Network Privileges. 2.3.1.2 Roles of network privileges. 2.3.2 Types of Network Privileges: 2.3.2.1 Read, Write, Execute 2.3.3 Roles of Privilege Management in Network Security 2.3.3.1 Administrator privileges 2.3.3.2 User privileges 2.3.3.3 Read-only access 2.3.3.4 Remote access privileges 2.3.4 implementation of network access control 2.3.5 Understand Network Access Requirements 2.3.6 Develop Access Control Policies 2.3.7 Select a Network Access Control Solution	
3. Configure network firewall	3.1 Firewall security 3.1.1 Introduction to firewall security 3.1.2 Types of firewall security 3.1.2.1 Hardware firewall 3.1.2.2 Software firewall 3.1.2.3 Cloud firewall 3.1.2.4 Open-source firewall 3.1.3 Firewall architecture and components	● Practical test ● Project ● Portfolio of evidence ● Oral questioning ● Interviews ● Third party

	3.2 Firewall Zone and IP address 3.2.1 Types of firewall zones 3.2.2 IP address structure 3.2.2.1 Network ID 3.2.2.2 Hosting ID 3.3 Access Control list 3.3.1 Network Access Control List (ACL) Concepts 3.3.1.1 Purpose of ACLs 3.3.1.2 Wildcard mask in ACLs 3.3.1.3 Types of IPv4 ACLs 3.4 Login and Firewall services 3.4.1 Firewall login and configuration concepts 3.4.2 Types of firewall services 3.4.2.1 Packet filtering 3.4.2.2 Stateful inspection 3.4.2.3 Application-level gateway 3.4.2.4 Virtualization 3.5 Firewall Configuration 3.5.1 Concepts of Firewall configuration 3.5.2 Steps of Firewall configuration 3.5.3 Best practices for firewall configuration 3.5.4 Objectives of firewall testing 3.5.5 Steps of Firewall testing 3.5.6 Tools for Firewall testing 3.5.7 Best practices for firewall testing 3.6 Firewall management 3.6.1 Concepts of firewall management 3.6.1.1 Firewall maintenance 3.6.1.2 Firewall monitoring 3.6.1.3 Compliance and auditing	report • Written tests • Case study • Written tests • Case study
--	---	--

	3.6.1.4 Firewall documentation	
4. Conduct Computer Network security user training	4.1 Security Awareness 4.1.1 Introduction to computer network security awareness 4.1.2 User and customer training methods 4.2 Network security implementation 4.2.1 User training on implementation of Network security practices 4.2.1.1 Network security policies 4.2.1.2 Network security best practices 4.2.1.3 Network segmentation user training 4.2.1.4 Firewall implementation 4.3 Incidence Responses 4.3.1 User training on computer network incident response. 4.3.2 Types of computer network incident response 4.3.3 Components of incident response training for users 4.3.4 Incident response team functions and responsibilities 4.4 Regular updates 4.4.1 User training on computer networks regular updates. 4.4.2 Patch management 4.5 Network Compliance training 4.5.1 Concepts of computer networks Compliance training. 4.5.2 Legal and regulatory requirement. 4.5.3 Compliance policies and procedures 4.5.4 Compliance monitoring and auditing	● Practical test ● Project ● Portfolio of evidence ● Oral questioning ● Interviews ● Third party report ● Written tests ● Case study

	4.5.5 Emerging trends in computer network compliance 4.6 Network testing and simulation 4.6.1 Introduction to network testing and simulation. 4.6.2 Components of network testing and simulation. 4.6.2.1 Network performance testing 4.6.2.2 Network security testing 4.6.2.3 Network simulation techniques	
--	--	--

Suggested Methods of delivery

- Role playing
- Viewing of related videos
- Group discussions.
- Instructor led facilitation using active learning strategies.
- Projects.
- Demonstrations.
- Site visits.

Recommended Resources for 25 Trainees

S/No.	Category/Item	Description/Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	Learning Materials			
1.	Textbooks		13 pcs	2:1
2.	Installation manuals			
3.	Flip Charts			
4.	PowerPoint presentations	For trainer's use		
B	Learning Facilities & infrastructure			
5.	Lecture/theory room		1	25:1
6.	Laboratory		1	25:1
C	Consumable materials			
7.	Printing papers		1 ream	1:20

8.	Toners/Cartridges		2 pcs	13:1
9.	Assorted colour of whiteboard markers			
D	Tools and Equipment			
10.	Computers		25 pcs	1:1
11.	Projector		1 pc	25:1
12.	Flash drives		25 pairs	1:1
13.	External CD/DVD drives		13 pcs	2:1