

COMPUTER NETWORK SECURITY MONITORING

ISCED UNIT CODE: 0612 451 08A

TVET CDACC UNIT CODE: IT/CU/NSA/CR/06/5/MA

Relationship to Occupational Standards

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

Unit Duration: 220 Hours

UNIT DESCRIPTION

This unit covers the competencies required to monitor computer network security. It involves conducting computer network security assessment, monitoring computer network firewall activities and performing fundamental computer networking segmentation.

Summary of Learning Outcomes

LEARNING OUTCOMES	DURATION (HOURS)
1. Conduct computer network security assessment	50
2. Monitor Computer Network Firewall activities	90
3. Perform fundamental Computer Network segmentation	80
TOTAL	220

Learning Outcomes, Content and Suggested Assessment Methods

Elements	Performance Criteria
These describe the key outcomes which make up workplace functions	These are assessable statements which specify the required level of performance for each of the elements (Bold and italicized terms are elaborated in the range)

1. Conduct computer network security assessment	1.1 Network Security Threats & Vulnerabilities 1.1.1 Introduction to computer network security 1.1.2 Importance of computer network security 1.1.2.1 Preventing unauthorized access: 1.1.2.2 Protecting data integrity: 1.1.2.3 Ensuring business continuity: 1.1.3 Types of network security threats and vulnerabilities 1.1.3.1 Malware 1.1.3.2 Phishing 1.1.3.3 Man in the middle attack 1.1.3.4 Denial of service attack 1.1.3.5 SQL injection 1.1.3.6 Weak authentication and authorization 1.1.3.7 Physical security threats 1.2 Network Security Controls 1.2.1 Types of computer network security controls 1.2.1.1 Preventive controls 1.2.1.2 Detective controls 1.2.1.3 Corrective controls 1.2.2 Implementation of computer network security controls 1.2.2.1 Physical controls • Lock & Keys • Biometrics • Access Cards & Badges • CCTVs 1.2.2.2 Technical controls • Firewalls • Data Encryption • Network Segmentation • Network monitoring and logging 1.2.2.3 Administrative controls
--	---

	• Access controls • Employee training on security awareness. • Screening and verification • Authentication mechanism 1.3 Computer network risk assessment reports 1.3.1 computer network risk assessment 1.3.2 reasons for conducting computer network risk assessment 1.3.3 Key components of a computer network risk assessment 1.3.4 How to conduct a computer network risk assessment 1.3.5 Tools and technologies for computer network risk assessment 1.3.5.1 Planning and preparation: 1.3.5.2 Threat analysis 1.3.5.3 Vulnerability scanners: 1.3.5.4 Risk management software 1.3.6 Best practices for network risk assessment 1.3.7 Documentation of the risk assessment report
2. Monitor Computer Network Firewall activities	2.1 Computer Network Firewall 2.1.1 Introduction to computer network firewall 2.1.2 Importance of computer network firewall 2.1.3 Factors to consider in firewall monitoring 2.1.4 Types of firewall logs 2.1.4.1 Traffic 2.1.4.2 Event 2.1.4.3 System 2.1.4.4 Threat 2.1.5 Tools and techniques used in firewall monitoring 2.1.5.1 Packet filtering 2.1.5.2 Logging and reporting

	2.1.5.3 Bandwidth management 2.1.5.4 URL Filtering 2.1.5.5 SolarWinds Network Performance Monitor (NPM) 2.1.6 Best practices for firewall management 2.2 Firewall updates 2.2.1 Importance of regular firewall updates 2.2.2 procedure to updating firewall firmware and software 2.3 Computer network traffic. 2.3.1 Introduction to computer network traffic monitoring. 2.3.2 Benefits of computer network traffic monitoring 2.3.3 Monitoring of computer network traffic 2.3.4 Computer Network traffic monitoring tools 2.3.4.1 Wireshark 2.3.4.2 SolarWinds Network Performance Monitor (NPM) 2.3.4.3 Cisco Network Assistant (CNA)
3. Perform fundamental Computer Network segmentation	3.1 IP addressing scheme. 3.1.1 IP addressing and subnetting 3.1.2 IP address fundamentals 3.1.2.1 Physical address. MAC address. 3.1.2.2 Logical address. IP address. 3.1.2.3 Hostname. 3.1.2.4 IPv4 vs. IPv6 3.1.2.5 Classful addressing 3.1.2.6 Static vs. Dynamic IP Addressing 3.1.2.7 Public vs. Private IP Addresses 3.1.3 Steps in Designing an IP Addressing Scheme 3.2 Network segmentation 3.2.1 Introduction to network segmentation 3.2.1.1 Definition of network segmentation 3.2.1.2 Physical & logical segmentation

	3.2.1.3 Importance of network segmentation 3.2.2 Types of network segmentation 3.2.2.1 IP based 3.2.2.2 VLANs 3.2.2.3 Subnetting 3.2.2.4 Firewalls 3.2.2.5 Physical segmentation 3.2.3 Tools and techniques for network segmentation 3.2.3.1 Firewalls, Routers, and Access Control Lists (ACLs) 3.2.3.2 Network Access Control (NAC) 3.2.4 Monitoring and Managing Network Segments 3.3 Network privileges. 3.3.1 Introduction to network privilege management 3.3.1.1 Definition of Network Privileges. 3.3.1.2 Roles of network privileges. 3.3.2 Types of Network Privileges: 3.3.2.1 Read, Write, Execute 3.3.3 Roles of Privilege Management in Network Security 3.3.3.1 Administrator privileges 3.3.3.2 User privileges 3.3.3.3 Read-only access 3.3.3.4 Remote access privileges 3.3.4 implementation of network access control 3.3.5 Understand Network Access Requirements 3.3.6 Develop Access Control Policies 3.3.7 Select a Network Access Control Solution
--	---

RANGE

This section provides work environments and conditions to which the performance criteria apply. It allows for different work environments and situations that will affect performance.

VARIABLE	RANGE
1. Network security Threats & Vulnerabilities may include but not limited to:	● Malware ● Phishing ● Man in the middle attack ● Denial of service attack ● SQL injection ● Weak authentication and authorization ● Physical security threats
2. Network Security Controls may include but not limited to;	● Firewalls ● Network segmentation ● Network monitoring and logging ● Authentication mechanisms
3. Firewall activities may include but not limited to;	● Packet filtering ● Logging and reporting ● Bandwidth management ● URL Filtering
4. IP addressing scheme may include but not limited to;	● Classful addressing ● Private IP addressing ● Public IP addressing
5. Network segmentation may include but not limited to;	● VLANs ● Subnetting ● Firewalls ● Physical segmentation
6. Network privileges may include but not limited to;	● Administrator privileges ● User privileges ● Read-only access ● Remote access privileges

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			
14.	Textbooks		13 pcs	2:1
15.	Installation manuals			
16.	Flip Charts			
17.	PowerPoint presentations	For trainer's use		
B	Learning Facilities & infrastructure			
18.	Lecture/theory room		1	25:1
19.	Laboratory		1	25:1
C	Consumable materials			
20.	Printing papers		1 ream	1:20
21.	Toners/Cartridges		2 pcs	13:1
22.	Assorted colour of whiteboard markers			
D	Tools and Equipment			
23.	Computers		25 pcs	1:1
24.	Projector		1 pc	25:1
25.	Flash drives		25 pairs	1:1
26.	External CD/DVD drives		13 pcs	2:1