©2023 TVET CDACC

061205T4CYB

CYBER SECURITY LEVEL 5

SEC/OS/CS/CR/07/5/A

CONDUCT CYBER SECURITY ASSESSMENT AND TESTING

Nov. / Dec. 2023

TVET CURRICULUM DEVELOPMENT, ASSESSMENT AND CERTIFICATION COUNCIL (TVET CDACC)

PRACTICAL ASSESSMENT

Time: 3 Hours

INSTRUCTIONS TO CANDIDATE

1. This assessment requires the candidate to demonstrate competence against unit of competency: **Conduct security assessment and testing**
2. In this assessment, you will be required to perform **three (3)** practical tasks.
3. Write your name, registration code, date and sign in the practical assessment attendance register.
4. You have **10 minutes** to carefully read through the instructions and to collect the tools/resources required for the tasks.
5. The assessor will record your performance at critical points using audio-visual means.
6. You are required to have Personal Protective Equipment for the practical assessment

This paper consists of THREE (3) printed pages

Candidates should check the question paper to ascertain that all pages are printed as indicated and that no questions are missing

The following resources will be provided to the candidate:

- ♦ A networked Computer installed with windows 10 and window-based network monitoring and scanning tools such as wireshark, Nmap, Metasploit, Nessus, OpenVAS, Nikto or any other vulnerability assessment software.
- ♦ Exam booklet.

In this assessment, you are required to complete the following tasks:

TASK 1 - Network Scanning (25 marks)

1. You've been tasked with scanning and mapping your computer lab network to identify all active devices and services. Using Nmap perform a network investigation about your computer lab network. Take screenshot of every step.

a) Open Nmap or terminal or command prompt.

b) Identify the target computers' IP addresses.

c) Conduct a Nmap scan on the host you are using to identify open ports, services and version.

d) Document open ports and services running on the host (target computer)

e) Save the scan results in a text file.

f) Scan TCP port 80 and identify the services associated with it.

g) Identify the underlying OS of the host, its version and the mac address using Nmap's operating system detection feature.

h) Create a network map to visually represent the discovered devices, their connections and the relationships between them.

TASK 2 - Vulnerability Assessment (20marks)

2. You are provided with the computer installed with windows 10 Operating System connected to a network. You are required to;

a) Assess the configuration of window firewalls.

b) Using Nessus or OpenVAS scan the windows.

c) Identify known vulnerabilities and prioritize them based on their severity and potential impact on the network's security.

d) Document the vulnerabilities on the provided booklet.

e) Using wire shark tool analyze network traffic.

f) Identify and document potential security issues after analyzing the network using wire shark tool.

TASK 3 - Develop Exploitation Proof of Concept (PoC) (20marks)

3. Based on vulnerabilities identified in **task 2**, develop an Exploitation Proof of Concept (PoC) in line with the standard operating procedure that will help organizations in assessing the risk associated with a particular vulnerability.