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)

OBSERVATION CHECKLIST

INSTRUCTIONS TO THE ASSESSOR

1. You are required to mark the practical as the candidate performs the tasks.
2. You are required to take video clips at critical points.
3. Allocate the candidate **10 minutes** to carefully read through the instructions and to collect the tools/resources required for the tasks.
4. Allocate the candidate **3 Hours** to perform **three (3)** practical tasks.
5. The candidate should write his/her name, registration code, date and sign in the practical assessment attendance register.
6. Ensure the candidate has a name tag and registration code at the back and front.

This paper consists of FOUR (4) printed pages

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

OBSERVATION CHECKLIST

Candidate's Name & Registration No.			
Assessor's Name & Id code			
Unit(s) of Competency	**Conduct cyber security assessment and testing**		
Venue of Assessment			
Date of Assessment			
Assets to be evaluated:	**Marks allocated**	**Marks obtained**	**Comments**
TASK 1: Network Scanning			
a) Opened Nmap or terminal or command prompt. ***(Award 2 marks)***	**2**		
b) Identified the target computers' IP addresses. ***(Award 3 marks)***	**3**		
c) Conducted a Nmap scan on the host you to identify open ports, services and version. ***(Award 1 marks for each open port, port's service and version to maximum of 5 marks)***	**5**		
d) Documented open ports and services running on the host (target computer) ***(Award 3 marks)***	**3**		
e) Saved the scan results in a text file. ***(Award 2 marks)***	**2**		
f) Scan TCP port 80 and identify the services associated with it. ***(Award 2 marks)***	**2**		
g) Identified the underlying OS of the host, its version and the mac address. ***(Award 2 marks for OS its version, and 2 marks for the MAC Address)***	**4**		
h) Created a network map **(Award 2 marks for the discovered devices, 1**	**4**		

mark for their connections and 1mark for any relationship shown.			
TOTAL	**25**		
TASK 2: Vulnerability Assessment			
a) Assessed the configuration of windows Firewalls ***(Award 2 marks)***	**2**		
b) Scanned the windows using Nessus or OpenVAS ***(Award 3 marks)***	**3**		
c) Identified known vulnerabilities and prioritized them based on their severity and potential impact on the network's security ***(Award 2 marks for identification and 3marks for Prioritization)***	**5**		
d) Documented the vulnerabilities on the provided booklet. ***(Award 2 marks)***	**2**		
e) Analyzed the network traffic ***(Award 3 marks)***	**3**		
f) Identified potential security issues on the network ***(Award 5 marks)***	**5**		
TOTAL	**20**		
TASK 3: Developing PoC			
Developed an Exploitation Proof of Concept (PoC) in line with the standard operating procedure ***(Award 1 marks-Title, Author and Date)*** ***(Award 1 marks-Introduction)*** ***(Award 1 marks-Context)*** ***(Award 2 marks-Target System Information)*** ***(Award 3 marks-Vulnerability Description)*** ***(Award 1 marks- Prerequisites)*** ***(Award 5 -PoC Code/Step-by-step statements)*** ***(Award 2- Expected Outcomes)***	**20**		

(Award 2 -Mitigation Recommendations) ***(Award 2-Conclusion)***			
TOTAL	**20**		
Grand Total	**65**		

ASSESSMENT OUTCOME

The candidate was found to be:

Competent ☐ Not yet competent ☐

(Please tick as appropriate)

(The candidate is competent if s/he gets 50% or higher of the items of evaluation correct)

Feedback to candidate:

Feedback from candidate:

Candidate's Signature **Date**

---------- **----------**

Assessor's Signature **Date**

---------- **----------**