061206T4CYB

CYBERSECURITY TECHNICIAN LEVEL 6

SEC/OS/CS/CR/10/6/A

CONDUCT CYBERSECURITY ASSESSMENT AND TESTING

Nov. / Dec. 2023

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

PRACTICAL ASSESSMENT

ASSESSOR'S GUIDE

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 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

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: Using Nmap			
i. Wore Personal Protective Equipment ✓ Safety boots ✓ Dust coat or any other PPE observed ***(Award 1 mark each)***	**2**		
1. Opening Nmap or terminal or command prompt. ***(Award 1 mark)***	**1**		
2. Provided a list of IP addresses and hostnames of the live hosts discovered ***(Award 2 marks)***	**2**		
3. Identified open ports, services and version ***(Award 1 marks for each open port, port's service and version to maximum of 5 marks)***	**5**		
4. Determined the status of TCP port 80. ***(Award 2 marks)***	**2**		
5. Identified the underlying OS of the host, its version and the mac address. ***(Award 2 marks for OS detected, 1 mark for the version and 2 marks for the MAC Address)***	**5**		
6. Drawn a topology diagram **(Award 2 marks for the diagram, 1 mark for correct labeling)**	**3**		

Task 2:			
7. Assessed the configuration of ***Firewalls*** ***(Award 2 marks)***	**2**		
8. Scanned the windows using Nessus or OpenVAS ***(Award 3 marks)***	**3**		
9. Identified the vulnerabilities and noted on the booklet. ***(Award 4 marks)***	**4**		
10. Analyzed the network traffic ***(Award 3 marks)***	**3**		
11. Identified potential security issues on the network ***(Award 4 marks)***	**4**		
12. Performed penetration testing and exploitation of identified vulnerabilities using Metasploit. ***(Award 7 marks)***	**7**		
13. Attempted to crack windows login password or other available passwords. ***(Award 5 marks)***	**5**		
14. Candidate took screenshots ***(Award 2 marks)***	**2**		
Grand Total	**50**		

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
----------	----------