061206T4CYB

CYBER SECURITY TECHNICIAN LEVEL 6

SEC/OS/CS/CR/08/6/A

Install Cyber Security System

Nov/Dec 2024

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

PRACTICAL ASSESSMENT GUIDE

INSTRUCTIONS TO THE ASSESSOR

Assess the candidate as the practical progresses observing the critical areas

You are required to mark the practical as the candidate perform the tasks

You are required to take the video clips at critical points

Ensure the candidate has a name tag and registration code at the back and front

This paper consists of FOUR (4) printed pages.

Assessor should check the tool to ascertain that all the pages are printed as indicated and that no questions are missing

OBSERVATION CHECKLIST

Candidate's name & Registration No.			
Assessor's name & Reg. code			
Unit(s) of Competency	**Install Cyber Security System**		
Venue of Assessment			
Date of assessment			
(Award mark(s) appropriately as guided for in the items for evaluation indicated. Give a brief comment where necessary)			
Items to be evaluated:	**Marks Available**	**Marks Obtained**	**Comments**
Task 1: Snort intrusion prevention system installed.			
i. Npcap installed ***– Award 1mark or 0***	**1**		
ii. Snort archive extracted to C:\snort. ***– Award 1mark or 0***	**1**		
iii. Snort directories created. ***-Award 4 marks or 0*** ***NB. award 1 mark each (Log, rules, preproc_rules, etc directories)***	**4**		
iv. Configuration files copied to their appropriate directories. ***- Award 4 marks or 0*** **NB. – *award 1 mark each for copying files to their directories.***	**4**		
v. `Snort.Conf` file edited using a text editor. ***- Award 1 marks***	**1**		
vi. Network variables set to define the network to be protected. (Web server IP). ***- Award 1 marks***	**1**		
All the steps above are documented and printed. ***-Award 5 marks or 0*** ***NB-1 mark for every step documented***	**5**		
Task 2: Custom rules created for monitoring web traffic.			
i. A rule created to detect SQL injection attempts. ***Award 1 marks or 0***	**1**		
ii. A rule created to detect cross-site scripting. ***Award 1 mark or 0***	**1**		

iii.	Network interface identified. ***Award 1 mark or 0***	**1**		
iv.	Snort started as administrator in command prompt. ***Award 1 mark or 0***	**1**		
v.	IP address monitored using snort. ***Award 1 mark or 0***	**1**		
vi.	Web attacks simulated (Curl tool for simulation**) Award** ***1 marks or 0***	**1**		
vii.	Snort output reviewed for alerts triggered by the attacks. ***Award 1 mark or 0***	**1**		
viii.	Snort logs generated analyzed. ***Award 1 mark or 0***	**1**		
ix.	Test rules modified to improve detection. ***Award 1 mark or 0***	**1**		
x.	Snort execution automated. ***Award 1 mark or 0***	**1**		
xi.	All the steps above are documented and printed. ***Award 9 marks or 0*** ***NB-1 mark for every step documented***	**9**		
		36		

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**

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

End.