061205T4CYB

CYBER SECURITY LEVEL 5

SEC/OS/CS/CR/04/5/A

Secure Software Application

Nov/Dec 2024

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

PRACTICAL ASSESSMENT

OBSERVATION CHECKLIST

Candidate's Name & Registration Code			
Assessors Name & Registration Code			
Venue of Assessment			
Date of Assessment			
Items to be Evaluated: *Please award marks as appropriate. Give a brief comment on your observation.*	**Marks Available**	**Marks Obtained**	**Comments**
TASK 1: Install the Virtual Box/VMware			
1. Ran the installer for VirtualBox/VMware - *(Award 2 marks or zero)*	**2**		

2. Created a New Virtual Machine in Virtual Box - *(Award 2 marks or zero)*	**2**		
3. Allocated Memory (RAM) -*(Award 2 marks or zero)*	**2**		
4. Created a Virtual Hard Disk -*(Award 2 marks or zero)*	**2**		
5. Configured the Virtual Machine - *(Award 2 marks or zero)*	**2**		
Sub – Total 1	**10**		
TASK 2: Install Kali Linux on the VirtualBox/VMware installed in task 1			
1. Launched Virtual machine Workstation Player from the desktop - *(Award 1 mark or zero)*	**1**		
2. Booted the Kali Linux ISO from the VMware - *(Award 1 mark or zero)*	**1**		
3. Configured Network on the Kali Linux ISO installation - *(Award 2 marks or zero)*	**2**		
4. Set Up Users and Password on the Kali Linux ISO installation - *(Award 2 marks or zero)*	**2**		
5. Partitioned Disk on the Kali Linux ISO installation - *(Award 2 marks or zero)*	**2**		
6. Completed the Kali Linux ISO installation by following the screen process - *(Award 2 marks or zero)*	**2**		
Sub – Total 2	**10**		
TASK 3: Update Kali Linux			
Updated and upgraded Kali Linux operating system.			

1. Opened the terminal by clicking the terminal icon or pressing Ctrl + Alt + T *(Award 2 marks or zero)*	**2**		
2. Updated the Repository Index by running the following command sudo apt update - *(Award 2 marks or zero)*	**2**		
3. Upgrade the Installed Packages by sudo apt upgrade –y *(Award 2 marks or zero)*	**2**		
4. Run a full upgrade to update all the packages by sudo apt full-upgrade –y *(Award 2 marks or zero)*	**2**		
5. Reboot the system for updates to take effects by sudo reboot *(Award 2 marks or zero)*	**2**		
Sub-Total 3	**10**		
TASK 4: Scan institution website for vulnerabilities			
Scanned institution website for vulnerabilities 1. Launch Metasploit Console. *(Award 2 marks or zero)*	**2**		
2. Gathered target Information by using ping then institution url provided to check if it's reachable and alive. E.g. ***ping www.xxxxx.ac.ke*** whereby xxxx is the url of the institute website *(Award 4 marks or zero)*	**4**		
3. Scanned for open Ports and Services with Nmap by typing ***db_nmap -sS -Pn www.xxxxx.ac.ke.*** *(Award 4 marks or zero)*	**4**		
4. Searched for Vulnerabilities in Identified Services, e.g ***search apache.*** *(Award 2 marks or zero)*	**2**		

5. Used auxiliary scanner module to scan for vulnerability e.g like scanning for HTTP Version Scanner. Issue the command: ***use auxiliary/scanner/http/http_version*** ***set RHOSTS www.xxxxx.ac.ke run*** *(Award 4 marks or zero)*	**4**		
6. Identified Vulnerabilities – checked and identified vulnerabilities if any *(Award 2 marks or zero)*	**2**		
7. Screenshot the identified vulnerabilities and saved *(Award 2 marks or zero)*	**2**		
Sub-Total 4	**20**		
GRAND TOTAL	**50**		

ASSESSMENT OUTCOME

The candidate was found to be:

Competent ☐ Not yet Competent ☐

(Please tick as appropriate)

(The candidate is competent if the candidate obtains at least 50%)

Feedback from the Candidate:

Feedback to the Candidate:

Candidate Signature **Date:**

_____ _____

Assessor's Signature **Date**

_____ _____