

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)**

PRACTICE

OBSERVATION CHECKLIST

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

2. Created a New Virtual Machine in Virtual Box - <i>(Award 2 marks or zero)</i>	2		
3. Allocated Memory (RAM) - <i>(Award 2 marks or zero)</i>	2		
4. Created a Virtual Hard Disk - <i>(Award 2 marks or zero)</i>	2		
5. Configured the Virtual Machine - <i>(Award 2 marks or zero)</i>	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 - <i>(Award 1 mark or zero)</i>	1		
2. Booted the Kali Linux ISO from the VMware - <i>(Award 1 mark or zero)</i>			
3. Configured Network on the Kali Linux installation - <i>(Award 2 marks or zero)</i>			
4. Set Up Users and Password on the Kali Linux ISO installation - <i>(Award 2 marks or zero)</i>	2		
5. Partitioned Disk on the Kali Linux ISO installation - <i>(Award 2 marks or zero)</i>	2		
6. Completed the Kali Linux ISO installation by following the screen process - <i>(Award 2 marks or zero)</i>	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 (<i>Award 2 marks or zero</i>)	2		
2. Updated the Repository Index by running the following command <code>sudo apt update</code> - (<i>Award 2 marks or zero</i>)	2		
3. Upgrade the Installed Packages by <code>sudo apt upgrade -y</code> (<i>Award 2 marks or zero</i>)	2		
4. Run a full upgrade to update all the packages by <code>sudo apt full-upgrade -y</code> (<i>Award 2 marks or zero</i>)	2		
5. Reboot the system for updates to take effects by <code>sudo reboot</code> (<i>Award 2 marks or zero</i>)	2		
Sub-Total 3	0		
TASK 4: Scan institution website for vulnerabilities			
Scanned institution website for vulnerabilities			
1. Launch Metasploit Console. (<i>Award 2 marks or zero</i>)	2		
2. Gathered target Information by using ping then institution url provided to check if it's reachable and alive. E.g. <i>ping www.xxxxx.ac.ke</i> whereby xxxx is the url of the institute website (<i>Award 4 marks or zero</i>)	4		
3. Scanned for open Ports and Services with Nmap by typing <i>db_nmap -sS -Pn www.xxxxx.ac.ke</i> . (<i>Award 4 marks or zero</i>)	4		
4. Searched for Vulnerabilities in Identified Services, e.g <i>search apache</i> . (<i>Award 2 marks or zero</i>)	2		

5. Used auxiliary scanner module to scan for vulnerability e.g like scanning for HTTP Version Scanner. Issue the command: <i>use auxiliary/scanner/http/http_version</i> <i>set RHOSTS www.xxxxx.ac.ke run</i> (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	0		
GRAND T	0		
ASSES	OME		
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	
_____		_____	