061206T4CYB

CYBER SECURITY TECHNICIAN LEVEL 6

SECURE SOFTWARE APPLICATION

SEC/OS/CS/CR/06/6/A

Nov. / Dec. 2023

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

PRACTICAL ASSESSMENT

INSTRUCTIONS TO CANDIDATE

1. This assessment requires the candidate to demonstrate competence against unit of competency: **Secure Software Application.**
2. Time allocated: **3 Hours.**
3. In this assessment, you will be required to perform **two (2)** practical tasks.
4. Write your name, registration code, date and sign in the practical assessment attendance register.
5. You have **10 minutes** to carefully read through the instructions and to collect the tools/resources required for the tasks.
6. The assessor will record your performance at critical points using audio-visual means.

This paper consists of 2 printed pages.

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

The following resources will be provided to the candidate:

- A Computer with Kali linux (open-source) installed and an operating system installed (preferably windows 10).
- Reliable internet connection.

Instructions:

In this assessment, you are required to complete the following tasks:

Task A: Software hardening. (20 marks)

1. Install a free antivirus, update it and activate Microsoft defender firewall applying the necessary settings to specifying who can install/uninstall software.

Task B: Perform application security assessment and application hardening. (30 marks)

Kali Linux contains tools for application software assessment. In this task you are expected to:

1. Run Kali Linux and conduct a vulnerability assessment to identify vulnerabilities in the Windows operating system. Perform screen capture to document the vulnerabilities identified.
2. Apply patches to address the identified vulnerabilities in the Windows Operating System, configure network settings to enhance security and enable disk encryption.
3. Conduct vulnerability scanning to verify the effectiveness of the implemented security measures using Kali Linux. Perform screen capture to document the result after addressing the vulnerabilities.