061206T4CYB

CYBERSECURITY TECHNICIAN LEVEL 6

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

INSTALL CYBER SECURITY SYSTEM

Nov. / Dec. 2023

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

PRACTICAL ASSESSMENT

Time : 3 hours

INSTRUCTIONS TO CANDIDATES

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

This paper consists of 3 printed pages

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

The following resources will be provided to the candidate:

- A Computer with an operating system installed (Windows 10 preferred).
- Microsoft Defender Antivirus installed in the computer
- Reliable internet connection

TASK 1: Configuring Microsoft Defender Antivirus (30 Marks)

You have been asked to configure and test Microsoft Defender Antivirus on the provided computer. You need to configure protection settings to enable controlled folder access and ensure that Microsoft Defender can detect vulnerabilities. You have decided to simulate a virus using a test file, sample.txt, located at C:\Files, to validate successful threat detection. You will also test out exclusions to see how adding an exclusion changes the behaviour of the virus scanning process.

Perform the following tasks

1. Configure Microsoft Defender Antivirus. **(5 marks)**
2. Perform a scan. **(2 marks)**
3. Introduce suspicious software. **(10 marks)**
4. View the quarantined file. **(3 marks)**
5. Configure exclusions. **(5 marks)**
6. Validate the excluded folder. **(5 marks)**

TASK 2: Configuring Windows Security Settings **(20 Marks)**

You will configure Windows Local Security Policy. Windows Local Security Policy is used to configure a variety of security requirements for stand-alone computers that are not part of an Active Directory domain. You will modify password requirements, enable auditing, configure some user rights, and set some security options. You will then use Event Manager to view logged information.

Perform the following tasks

7. Review the security requirements. **(5 marks)**
8. Open the Windows Local Security Policy tool. **(4 marks)**
9. Configure the Password Policy security settings. **(8 marks)**

- Accessed password policy security settings
- Enforce password history to **3**
- Maximum password age to **30 days**
- Minimum password age to **1 character**
- Minimum password length audit to **8 characters**
- Password must meet complexity requirement- **"Enabled"**
- Relax minimum password length limits**-"Enabled"**
- Store password using reversible encryption –**"Enabled"**

10. Configure the Account Lockout threshold to 2 **(3 marks)**

END