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

INSTRUCTIONS TO CANDIDATE

This assessment requires the candidate to demonstrate competence against unit of competency: **Install Cyber Security System.**

1. Time allocated: **3 Hours.**
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 THREE (3) printed pages.

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

You have been provided with the following resources:

1. A Computer updated with the latest patches for windows 10/11 or Windows Server 2016/2019/2022. .
2. Snort for windows installation file.
3. Npcap (packet capture library) installation file.
4. Text editor (Notepad).
5. A web server running on the same machine or another machine within the network.
6. Administrator Privileges.
7. Internet.
8. Printer.
9. Printing papers.

INSTRUCTIONS:

As cyber security expert you have been contracted by Hifadhidata Ltd to manage their security systems. One of the first tasks assigned to yours to install an Intrusion Prevention System (IPS). In this assessment, you are required to complete the following tasks:

Task 1: Install Intrusion Prevention System (Snort).

i. Screen capture and save all steps in this task.
ii. Install Npcap.
iii. Extract Snort archive files.
iv. Set up Snort directories.
v. Configure files to their appropriate directories.
vi. Edit Snort.conf file.
vii. Set variables to define web server IP to be protected.
viii. Print out all the processes in **Task 1**.

Task 2: Create custom rules for monitoring web traffic.

i. Screen capture and save all steps in this task**.**
ii. Create a rule to detect SQL injection attempts.
iii. Create a rule to detect Cross-Site Scripts (XSS).
iv. Identify the web server IP to be protected.
v. Start Snort using command prompt.
vi. Monitor the IP address using Snort.
vii. Simulate a web attack using the curl tool.
viii. Review the Snort output for alerts.
ix. Modify test rules to improve detection.
x. Automate Snort execution.
xi. Print out all the processes in **Task 2.**

End.