061206T4CYB

CYBERSECURITY TECHNICIAN LEVEL 6

SEC/OS/CS/CR/10/6/A

CONDUCT CYBERSECURITY ASSESSMENT AND TESTING

Nov. / Dec. 2023

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

PRACTICAL ASSESSMENT

Time: 3 Hours

INSTRUCTIONS TO CANDIDATE

1. This assessment requires the candidate to demonstrate competence against unit of competency: **Conduct security assessment and testing**
2. In this assessment, you will be required to perform **three (3)** 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.
6. You are required to have Personal Protective Equipment for the practical assessment

This paper consists of TWO (2) 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 networked Computer laboratory having at least two computers installed with: -Kali Linux, Wireshark, Nmap, Metasploit, Nessus, OpenVAS, and any other vulnerability assessment software.
- Exam booklet.

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

TASK 1:

Using Nmap perform a network reconnaissance about your computer lab network. Take screenshot of every step.

1. Opening Nmap or terminal or command prompt. **(1 marks)**
2. Provide a list of IP addresses and hostnames of the live hosts discovered. **(2 marks)**
3. Conduct a port scan on the host you are using to identify open ports, services and version. **(5 marks)**
4. Determine the status of TCP port 80. **(2 marks)**
5. Use Nmap's operating system detection feature to identify the underlying OS of the host, its version and the mac address. **(5 marks)**
6. Draw a well labeled topology diagram based on the discovered hosts and their relationships. **(3 marks)**

TASK 2:

You are provided with the computer installed with windows 10 Operating System connected to a network. You are required to:

7. Assess the configuration of firewalls. **(2 marks)**
8. Scanned the windows using Nessus or OpenVAS. **(3 marks)**
9. Identified known vulnerabilities after scanning the windows using Nessus or OpenVAS. Note down the vulnerabilities on the provided booklet. **(4 marks)**
10. Analyze network traffic. **(3 marks)**
11. Identify potential security issues using Wireshark after analyzing the network. **(4marks)**
12. Perform penetration testing and exploitation of identified vulnerabilities using Metasploit. **(7 marks)**
13. Attempt to crack window’s login password or other passwords available using tools like John the Ripper or Hashcat. **(5 marks)**
14. Capture screenshots. **(2 marks)**

END