061206T4CYB

CYBER SECURITY TECHNICIAN LEVEL 6

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

CONDUCT SECURITY ASSESSMENT AND TESTING

Nov/Dec 2024

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

PRACTICAL ASSESSMENT

Time: 3 Hours

INSTRUCTIONS TO CANDIDATE

This assessment requires the candidate to demonstrate competence against unit of competency:

Conduct Security Assessment and Testing

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 1 printed pages

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

Task 1

Perform a basic Cyber Security Assessment and Testing on a simulated network or system, identifying vulnerabilities, understanding potential risks, generate reports and suggest remedy(s).

1. Setup a Testing Environment - virtual lab environment or a sandbox in Kali Linux
2. Update the Operating System
3. Step 1: Reconnaissance Phase
   a) Install and Setup Nmap, Masscan, ZMap or any other relevant tool
   b) Scan the network to discover open ports on then gather information about services running on open ports
4. Step 2: Scanning and Enumeration Phase
   a) Install and Set up OpenVAS, Nessus or any other relevant tool
   b) Conduct a new scan targeting on for known vulnerabilities using the download tool
   c) Review the scan results to identify vulnerabilities.
5. Step 3: Exploitation Phase
   a) Install and Setup Metasploit or any other relevant tool
   b) Simulate the exploitation of vulnerabilities.
   c) Review the scan results to identify vulnerabilities.
   d) Verify if the exploits are successful and assess the impact.
6. Step 4: Post-Exploitation and Documentation phase
   a) Evaluate the level of access gained and the impact on the system.
   b) Document your findings, including vulnerabilities discovered, exploits used, and the impact.
7. Step 5: Re-assess
   a) Re-scan the system after applying remediation to ensure vulnerabilities are fixed.