

061206T4CYB

CYBER SECURITY TECHNICIAN LEVEL 6

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

Secure Software Application

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:

Secure Software Application.

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 3 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

You are tasked with assessing the security of a web server running under your institution IP address or other as provided. Use Nmap to perform a detailed port scan of this server, following the steps below:

1. Download and install Nmap
2. Perform a basic scan to identify which ports are open on the server and version detection for the open ports.
3. Use Nmap to detect the operating system running on the server.
4. Conduct a scan of all 65535 TCP ports on the server.
5. Perform a stealth scan (SYN scan) to identify open ports without establishing a full connection.
6. Attempt to evade potential firewalls or Intrusion Detection Systems (IDS) by using packet fragmentation.
7. Based on your scans, summarize the potential security risks associated with the open ports and services identified on the server.

TASK 2

You are tasked to perform a vulnerability assessment of a web application using Burp Suite, focusing on identifying and exploiting web vulnerabilities, and providing remediation recommendations.

1. Download and install Burp suite and set up your browser to use Burp Suite as a proxy.
2. Deploy or access a web application that will serve as your target.
3. Use Burp Suite's proxy to capture and analyze all HTTP/S traffic between the browser and the web application.
4. Use Burp Suite's Spider tool to automatically discover the web application's content and functionality.
5. Perform automated scans using Burp Suite's Scanner or manually investigate using the Intruder and Repeater tools.
6. For each vulnerability identified, use Burp Suite's Repeater or Intruder tools to manually test and exploit the vulnerability.
7. Generate a detailed report that includes all identified vulnerabilities
8. suggest fixes or directly apply them to the web application.

THIS IS THE LAST PRINTED PAGE.