061206T4CYB

CYBER SECURITY TECHNICIAN LEVEL 6

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

CONDUCT SECURITY ASSESSMENT AND TESTING

Nov. / Dec. 2023

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

WRITTEN ASSESSMENT

Time: 3 hours

INSTRUCTIONS TO CANDIDATES

1. This paper has two sections **A** and **B.**
2. You are provided with a separate answer booklet.
3. Marks for each question are as indicated.
4. Do not write on the question paper.

This paper consists of 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

SECTION A: (40 MARKS)

Attempt all questions in this section.

1. Explain THREE ways in which an organization's operation platform, in line with industry best practices, contributes to a successful security assessment and testing. **(6 marks)**
2. Describe ONE major role that search engines play in information gathering during a security assessment and testing. **(2 marks)**
3. Outline FOUR steps involved in conducting information gathering in line with the industry best practice. **(4 marks)**
4. Explain TWO benefits of establishing a network topology based on industry best practices. **(4 marks)**
5. Describe ONE major role of rainbow tables in security assessment and testing. **(2 marks)**
6. List FOUR steps involved in preparing and deploying payloads in line with the environment and industry best practices and ethics. **(4 marks)**
7. Discuss TWO methods of manipulating human emotions in social engineering. **(4 marks)**
8. Describe THREE best practices for maintaining access to remote hosts. **(6 marks)**
9. Discuss TWO importance's of analyzing the results of vulnerability scans. **(4 marks)**
10. Explain TWO ways on how consideration of the nature of the target influences the assessment process. **(4 marks)**

SECTION B: (60 MARKS)

Attempt any three questions in this section.

11. A cybersecurity consulting firm has been hired to conduct a comprehensive security assessment and testing for a large financial institution. They need to ensure that the types of information required are established according to industry best practices and that the nature of the target is determined in line with the information required.
    a) Discuss FIVE ways the consulting firm may use to assess risks. **(10 marks)**
    b) Explain FIVE specific types of information that the firm may require in order conduct to security assessment and testing. **(10 marks)**
12. Wananchi Company was concerned about the security of its network. They wanted to ensure that they were aware of all of the vulnerabilities in their systems so that they could address them before they were exploited by attackers.
    a) Describe FIVE approaches the company may use to identify vulnerable points. **(10 marks)**
    b) Describe FIVE ways to mitigate the identified vulnerabilities. **(10 marks)**
13. A security team is performing a host identification and services enumeration exercise for a network. They want to ensure that live hosts are identified according to the standard operating procedure and that services running on the live hosts are identified in line with industry best practices.
    a) Discuss FIVE importance of following the standard operating procedure for live host identification during a security assessment and testing. **(10 marks)**
    b) Explain FIVE industrial practices for validating the identified live hosts and services during a security assessment and testing. **(10 marks)**
14. The statement "Exploitation proof of concept was generated in line with the standard operating procedure" means that the proof of concept (PoC) exploit was created in accordance with the organization's established procedures for developing and testing exploits.

    a). Describe the FIVE steps of the standard operating procedure (SOP) for generating PoC exploits. **(10 marks)**

    b). An organization has implemented a set of policies and procedures for managing authorization credentials. These policies and procedures are designed to ensure that authorization credentials are created, stored, and used in a secure manner.

i. Define the term authorization as used in cybersecurity. **(2 marks)**

ii. Discuss FOUR requirements for authorization credentials as defined by organization's ICT policy. **(8 marks)**

END