061006T4ICT

ICT TECHNICIAN LEVEL 6

ICT/OS/IT/CR/3/6

CONTROL ICT SECURITY THREATS

July/August 2024

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

WRITTEN ASSESSMENT

TIME: 3 HOURS

INSTRUCTIONS TO CANDIDATE

1. This paper consists of two sections; **A** and **B**
2. Answer **ALL** the question as guided in each section
3. Marks for each question are as indicated in the brackets
4. You are provided with a separate answer booklet to answer the questions
5. Do not write in this question paper

This paper consists of FOUR (4) printed pages

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

SECTION A (40 Marks)

Answer ALL the questions in this section

1. Olive has been invited for an interview as an IT technician, List FOUR commonly recognized IT security threats in an organization that he is likely to asked. (4 Marks)
2. ICT security threats can be mitigated well if identified early, Outline FOUR methods commonly used to identify ICT security risks. (4 Marks)
3. Organizations suffer from security attacks because they are not aware of security threats, state any FOUR reasons why organizations need to be clearly aware of ICT security threats. (4 Marks)
4. IT security controls are measures put in place to help mitigate security threats, state FOUR reasons why IT security controls need to be in place. (4 Marks)
5. During an interview, you have been asked to define the following terminologies as used in control ICT security threats (4 Marks)
   i. Encryption
   ii. Patch Management
   iii. Vulnerability Assessment
   iv. Penetration Testing
6. Three experts from silicon electronics had a heated debate on how to improve IT ventures. Outline any FOUR best hones for coordination of security measures into the improvement and arrangement pipelines of IT ventures. (4 Marks)
7. State how organizations adjust the requirement for exacting security measures with the prerequisite for consistent client encounter in IT frameworks (4 Marks)
8. A client brought their laptop to Ember electronics seeking for assistance with firewall configurations. Enumerate any four network firewalls utilized to enhance logical security. (4 Marks)
9. Quickfix ventures a company domiciled in Penetration testing hired you to perform penetration testing for one of their clients. State any FOUR reporting process for findings and recommendations from penetration tests (4 Marks)
10. ICT security policy address confidentiality and integrity concerns during penetration testing. (4 Marks)

SECTION B (60 Marks)

*Answer **any THREE** questions in this section*

11.

a. Organizations develop security checking frameworks to help maintain the security controls. Discus any SIX challenges organizations may confront when actualizing and keeping up a security checking framework in IT. (6 Marks)

b. Upendo school experienced a security attack recently, outline FOUR indicators that the attack was a potential DDoS (Distributed Denial of Service) attack (4 Marks)

c. Ngao IT security agency recommended the following access control mechanisms to a client. Discuss how they work and their importance in computer security (6marks)

   i. Access control lists
   ii. Capability lists
   iii. Access control matrices

d. Data is becoming a vital resource in any organization. Users must authenticate themselves to the system to ensure data remains secure. As a system administrator of an IT firm, discuss any FOUR ways you would use for authenticating users to the server (4marks)

12.

a. Most security attacks come in form of malicious software, explain the following types of malicious software (6marks)

   i. Worms
   ii. Trojans
   iii. Logical bombs

b. Hackers do indeed post a big threat in the internet community. In order to detect and investigate hacker's attacks, the IT administrators need to acquire a few skills. Describe THREE skills that are needed to investigate hacker's attacks (6marks)

c. An IT specialist should take several steps to identify and attempt to retrieve possible evidence that may exist on a subject's computer system. Describe these six steps (6marks)

d. Most organizations fall prey to security attacks, state two precaution measures to take if you are under attack (2 marks)

13.

a. Several techniques are employed to compromise internet security. Briefly illustrate using diagrams where applicable the following techniques and for each technique, give TWO counter measures.
    i. Man-in-the-middle Attacks (5 marks)
    ii. Traffic analysis (5 marks)

b. You have been invited to talk about cybercrime during cyber security awareness campaign. Explain five actions that are categorized as computer crime according to the computer misuse and cybercrimes act of 2018. (10 marks)

14.

a. Distinguish between these following in relation to Systems security.
    i. Threat and attack (4marks)
    ii. Vulnerability and exploit (4marks)

b. As system/network administrators you are supposed to maintain system/network security, define the term password and list FOUR rules to help secure your network and computers (6 marks)

c. Explain three effective security strategies to secure computer integrity (6 marks)