061006T4ICT

ICT TECHNICIAN LEVEL 6

IT/OS/ICT/CR/3/6

CONTROL ICT SECURITY THREATS

NOV/DEC 2023

TVET CURRICULUM DEVELOPMENT, ASSESSMENT AND CERTIFICATION

COUNCIL (TVET CDACC)

WRITTEN ASSESSMENT

TIME: 3 Hours

INSTRUCTIONS TO CANDIDATE

1. This paper has TWO sections A and B. Attempt questions in each section
   as per instructions given in the section.
2. You are provided with a separate answer booklet.
3. Marks for each question are indicated in the brackets.
4. Do not write on the question paper

SECTION A: 40 MARKS

Answer ALL questions in this section.

1. Define the following terms as used in cyber security: (8 Marks)

   i.   asset;

   ii.   threat;

   iii.   logic bomb;

   iv.   Vulnerability.

2. Define the term ethical penetration as used in testing.   (2 Marks)

3. State THREE ways in which one can prevent brute force attack.   (3 Marks)

4. Differentiate between the following :   (4 Marks)

   i.   *Vulnerability Assessment* and *Penetration Testing.*

   ii.   *Update* and *Overhaul* of security systems.

5. Mention any THREE ways attackers may use to identify an individual password.

                                                                             (3 Marks)

6. Outline FOUR symptoms of malware infection in a computer system.   (4 Marks)

7. Explain the term SQL injection.   (2 Marks)

8. Explain the term Secure Socket Layer (SSL).   (2 Marks)

9. Discuss THREE common categories of ICT security threats.   (6 Marks)

10. Explain THREE categories of computer hackers.   (6 Marks)

SECTION B: 60 MARKS

Answer THREE questions in this section.

11.
   a) Explain the SIX steps of setting up a firewall. (12 Marks)

   b) Information security is important to every organisation connected to network. Explain FOUR functions of information security. (8 Marks)

12. The government of Kenya thwarted an attempted attack on the government services. You are appointed to give advisory on measures to protect the services from being attacked again. Explain TEN measures you would recommend. (20 Marks)

13.
   a) Explain THREE goals of ICT security. (6 Marks)

   b) Discuss SEVEN elements of an Information security policy. (14 Marks)

14.
   a) Explain **FIVE** steps followed when coming up with system testing plan. (10 Marks)

   b) Discuss **FIVE** types of logical security control measures which can be implemented in computer organisation. (10 Marks)

THIS IS THE LAST PRINTED PAGE.