061205T4CYB

CYBER SECURITY LEVEL 5

SEC/OS/CS/CR/07/5/A

CONDUCT CYBER SECURITY ASSESSMENT AND TESTING

Nov. / Dec. 2023

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

WRITTEN ASSESSMENT

Time: 3 Hours

INSTRUCTIONS TO CANDIDATES

Maximum marks for each question are indicated in brackets ().

*This paper consists of **THREE** sections: A, B and C.*

Answer questions as per instructions in each section.

You are provided with a separate answer booklet.

Answer the questions in English

This paper consists of SEVEN (7) 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: (20 Marks)

Answer ALL the questions in this section.

1. Which of the following best describes the primary source for determining the types of information required in line with industry best practices?
   A. Company's financial statements
   B. Industry standards and regulations
   C. Internal employee preferences
   D. Social media trends
2. When establishing an organization's operation platform in line with industry best practices, which of the following is a key consideration?
   A. The organization's preferred color scheme for branding.
   B. Adherence to industry-specific standards and best practices.
   C. The CEO's personal hobbies and interests.
   D. The availability of the latest mobile devices for employees.
3. Which of the following protocols is commonly used in service and protocol enumeration to identify open ports and services?
   A. TCP/IP
   B. HTTP
   C. SNMP
   D. Nmap
4. Why is information gathering and reconnaissance an essential phase in cybersecurity assessments?
   A. To directly exploit vulnerabilities.
   B. To determine the scope of the assessment.
   C. To install security patches.
   D. To encrypt sensitive data.
5. What is the primary purpose of service enumeration in a cyber-security assessment?
   A. To identify potential vulnerabilities and weaknesses in network services.
   B. To map out the physical locations of devices on a network.
   C. To determine the compliance of the network with industry standards.
   D. To assess user satisfaction with network services.

6. What is the purpose of multi-factor authentication (MFA) in user identification?
   A. To collect more user information.
   B. To simplify the login process.
   C. To add an extra layer of security by requiring multiple forms of verification.
   D. To identify users based on their IP addresses.
7. Which of the following methods is an example of passive reconnaissance in information gathering?
   A. Port scanning.
   B. Social engineering.
   C. Observing an organization's website and social media.
   D. Launching a DDoS attack.
8. Which of the following is NOT considered a strong and secure password practice?
   A. Using a combination of upper- and lower-case letters, numbers, and special characters.
   B. Using easily guessable information like "password" or "123456."
   C. Creating long and unique passwords for different accounts.
   D. Changing passwords regularly.
9. Which of the following practices can help mitigate vulnerabilities on a host?
   A. Regularly updating software and applying security patches
   B. Disabling firewalls and antivirus software
   C. Sharing administrator credentials with multiple users
   D. Ignoring security alerts and notifications
10. What is a vulnerable point on a host in the context of cyber security?
   A. The physical location of the host
   B. Software or hardware weaknesses that can be exploited
   C. The IP address assigned to the host
   D. The host's network connectivity status

11. During the initial stages of a cyber-security assessment, which of the following activities typically falls under information gathering and reconnaissance?
    A. Installing intrusion detection systems (IDS).
    B. Scanning for vulnerabilities.
    C. Conducting social engineering attacks.
    D. Collecting publicly available data about the target
12. Why is it essential for an organization to align its operation platform with industry-specific standards and best practices?
    A. To cater to the personal preferences of top management.
    B. To save money on operational expenses.
    C. To enhance efficiency, compliance, and competitiveness.
    D. To prioritize employee leisure activities.
13. Which of the following is a crucial element in user identification and authentication?
    A. The user's favorite color.
    B. A strong and unique password.
    C. The user's email address.
    D. The user's physical location.
14. Which of the following is NOT a typical source of information during reconnaissance for a cybersecurity assessment?
    A. Social media profiles.
    B. Network traffic logs.
    C. Domain registration data.
    D. Network scans.
15. During the initial stages of a cyber-security assessment, which of the following activities typically falls under information gathering and reconnaissance?
    A. Installing intrusion detection systems (IDS).
    B. Scanning for vulnerabilities.
    C. Conducting social engineering attacks.
    D. Collecting publicly available data about the target.

16. Which of the following best describes an "open-box" vulnerability assessment?
    A. Assessors have no prior knowledge of the target system.
    B. Assessors have partial knowledge of the target system.
    C. Assessors have full access and knowledge of the target system.
    D. Assessors focus solely on physical security.
17. What does payload deployment refer to in the context of cyber security?
    A. The act of delivering security updates to network devices.
    B. The process of encoding and packaging malicious code.
    C. Executing or delivering the malicious payload on a target system.
    D. Setting up firewalls and intrusion detection systems.
18. Which of the following is an example of a "something you are" factor in multi-factor authentication?
    A. Fingerprint scan.
    B. A PIN code.
    C. A username.
    D. A passphrase.
19. What is the primary purpose of payload preparation in cyber security?
    A. To deliver security patches to target systems.
    B. To design attractive user interfaces for applications.
    C. To encode and package malicious code for delivery to a target system.
    D. To establish secure communication between network devices.
20. Which of the following is a common technique used in payload preparation to make malicious payloads harder to detect by security tools?
    A. Digital signatures.
    B. Encryption and obfuscation.
    C. Clear text.
    D. Anti-virus scanning.

Section B: (40 Marks)

Answer ALL the questions in this section.

21. Outline FOUR reasons of probing and scanning in a cyber security assessment **(4marks)**
22. Explain TWO reasons why determining the nature of the target is a critical step in the information gathering process. **(4marks)**
23. Discuss THREE benefits that organization may accrue after aligning its operation platform with industry best practice. **(6marks)**
24. Payloads in the context of ethical hacking are prepared and deployed to assess and test the vulnerabilities and weaknesses in a system. Identify FOUR ethical considerations that should be taken into account when engaging in payload preparation and deployment for security testing purposes.

    (4marks)
25. Using a relevant example, identify FOUR ways in which exploitation proof of concept can help security experts in testing and validating security controls. **(4marks)**
26. Explain what social engineering is in the context of user and system manipulation, and provide an example of a social engineering technique. **(3marks)**
27. State FIVE key elements typically included in a network topology diagram.

    (5marks)
28. Distinguish between difference between a vulnerability assessment and a penetration test.

    (4marks)
29. Explain TWO ways in which probing and scanning help in identifying vulnerabilities.

    (4marks)
30. List TWO types of information collected during a cyber-security assessment and testing process. **(2marks).**

Section C :(40 MARKS)

Attempt any two questions in this section.

31. Smart Firm company is in the process of establishing a local area network to facilitate sharing of resources such information and printers. The company has office set up consisting of three computers (Comp A, Comp B, and Comp C) connected to a central switch (Switch D). The switch is then connected to a router (Router E) for internet connectivity.
    a) As a network expert, draw a network topology diagram for the company using relevant symbols. Ensure that the diagram clearly represents the network connections and the flow of data within the network.
    (6marks)
    b) Identify FOUR scanning techniques you would utilize during the network scan **(4marks)**
    c) Discuss FOUR network management best practices you should follow to ensure efficient operations.
    (10marks)
32. Top mark is a manufacturing company that produces drinks of different flavors. To reach their customer, it has established a website and social media accounts. The company handle sensitive information about the customers. As a cyber-security expert, you have been contracted to assess the cyber security status of the company.
    a) Describe FIVE possible sources of information that you can use to collect information about Company and its systems.
    (10marks)
    b) Discuss FIVE techniques that you could utilize to gather information about Top mark Company **(10marks)**
33. As the cyber security technician of Top mark company, one of your responsibilities is testing and exploiting known vulnerabilities within the company's systems.
    a) Describe FIVE vulnerabilities you could exploit. **(10marks)**
    b) After testing and exploiting know vulnerabilities, you are supposed to generate an exploitation proof of concept (PoC). Discuss FIVE benefits of generating PoC in line with the standard operating procedures. **(10marks)**