This question paper consists of TWO (2) sections. Answer ALL questions in the answer booklet provided. [100 MARKS]

SECTION A **(60 Marks)**

There are THIRTY (30) questions in this section. Answer ALL questions in the answer booklet provided.

1. What type of security focuses on preventing malicious threats from viruses such as Malware by employing measures like anti-virus software and user education?

   A. Data security
   B. Application security
   C. Endpoint security
   D. Cloud security

2. Which security type emphasizes protecting digital data storage and requires users to be cautious in managing their accounts to avoid data theft?

   A. Mobile security
   B. Network security
   C. Database and Infrastructure security
   D. Cloud security

3. Which security aspect involves designing a plan to recover data loss and ensure business continuity in the event of unexpected incidents?

   A. Application security
   B. Endpoint security
   C. Business continuity and disaster recovery
   D. Database and Infrastructure security

4. What are examples of sensitive information mentioned in the text that must be protected?

   A. Intellectual property
   B. Non-public personal information (NPI)
   C. Non-public corporate information
   D. All of the above

5. Which regulatory framework is cited as an example in the text that has been established to address cyber security concerns?

   A. General Data Protection Regulation (GDPR)
   B. Anti-virus regulations
   C. Data Leaking Prevention Act
   D. Cyber Security Protection Law

6. What is a cybersecurity framework?

   A. specialized form of virus
   B. Malicious logic that activates under specified conditions
   C. A system of standards, guidelines, and best practices
   D. A hidden computer flaw known to an intruder

7. Which of the following frameworks is mentioned as being designed to improve cybersecurity for providers of U.S. critical infrastructure?

   A. SANS
   B. NIST CSF
   C. Logic bomb
   D. Trojans horse

8. How is a cyber-attack different from a security breach?

   A. A cyber-attack is a successful event, while a security breach is an attempt.
   B. A security breach is an attempt, while a cyber-attack is a successful event.
   C. Both are synonymous terms.
   D. A cyber-attack and a security breach have no distinction.

9. What are the four main phases of the NIST incident response lifecycle?

   A. Preparation; Detection and Analysis; Containment, Eradication, and Recovery; and Post-Event Activity.
   B. SANS; NIST; Logic bomb; and Worm.
   C. Virus; Trojan horse; Bacterium; and Trapdoor.
   D. Incident; Response; Security; and Compromise.

10. Which of the following is described as a computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms?

   A. Virus
   B. Worm
   C. Trojan horse
   D. Logic bomb

11. What is the primary goal of identity thieves?

    A. Secretly gaining access to a computer system
    B. Committing crimes such as fraud or theft
    C. Creating and spreading malicious software
    D. Tricking individuals into clicking links

12. How do hackers gain access to a computer system?

    A. By creating and spreading malicious software
    B. By tricking individuals into clicking links
    C. By secretly obtaining unauthorized access
    D. By causing damage to computer files

13. What is the definition of phishing?

    A. Creating and spreading malicious software
    B. Secretly obtaining unauthorized access to personal information
    C. Stealing personal information by tricking individuals
    D. Causing damage to computer files through unauthorized access

14. What are potential consequences of phishing attacks?

    A. Loss of access to campus computing network
    B. Compromised personal data
    C. Lawsuits and prosecution
    D. All of the above

15. What is the general term for any program or file that is harmful to a computer user, including computer viruses, worms, Trojans, and spyware?

    A. Identity thieves
    B. Malware
    C. Phishing
    D. Hackers

16. What is a recommended practice to verify the legitimacy of a website before clicking a link?

    A. Hover over or long tap the link to display the true URL
    B. Open attachments from unknown sources
    C. Provide personal information over the phone
    D. Click on advertisements to download software

17. What is the purpose of ransomware?

    A. Records actions and keystrokes to steal passwords
    B. Prevents or limits users from accessing their system unless a ransom is paid
    C. Slows down the computer and tracks visited sites
    D. Removes viruses and repairs infected files

18. How does adware impact a computer system?

    A. In Encrypts user files
    B. Prevents access to the system
    C. Records actions and keystrokes
    D. Slows down the computer and tracks visited sites

19. What does antivirus software do?

    A. Encrypts user files
    B. Prevents access to the system
    C. Removes viruses and repairs infected files
    D. Records actions and keystrokes

20. What is a recommended method to reduce the risk of losing important files to ransomware, a virus, or other disasters?

    A. Open attachments from unknown sources
    B. Save copies of important files to a flash drive, external hard drive, or online backup service
    C. Test backup files periodically to ensure they are readable
    D. Provide personal information over the phone

21. Which type of scanning involves sending a SYN packet to each remote port and relies on open ports responding with SYN/ACK packets?

    A. TCP FIN scanning
    B. Fragmentation scanning
    C. Relay/bounce scanning
    D. TCP SYN scanning

22. What is the purpose of using a port scanning tool like NMAP?

    A. To send spoofed packets to hide the real scan
    B. To identify the operating system and log listening ports
    C. To perform relay/bounce scanning through another system
    D. To break up the scan into smaller packets for firewall evasion

23. What is a common component for vulnerability scanners?

    A. Data vulnerability
    B. Decoy scanning
    C. Fragmentation scanning
    D. TCP FIN scanning

24. Which information can be obtained through IP Spoofing?

    A. The version of an application running
    B. What services are available/listening
    C. Information about specific vulnerabilities
    D. Acquiring information using another computer's IP address

25. What is an example of non-technical spoofing?

    A. IP Spoofing
    B. Reverse social engineering
    C. TCP SYN
    D. Fragmentation scanning

26. What is a characteristic of Hit-list scanning?

    A. Uses information contained on the victim machine to find new targets
    B. Acts behind a firewall
    C. Involves infecting machines with a list of potentially vulnerable targets
    D. Creates large amounts of traffic

27. Which scanning technique involves looking for targets in its own local network and acts behind a firewall?

    A. Topological scanning
    B. DRDoS Attacks
    C. Local subnet scanning
    D. Honeypots

28. What is a characteristic of DRDoS Attacks?

    A. Floods victims with packets
    B. Uses spoofed IP addresses
    C. Requires the attacker to have access to the victim's LAN
    D. Involves sending HTTP headers to crash Apache Web server

29. What is a characteristic of low-interaction honeypots?

    A. In Acts as a network created to be attacked
    B. Emulates services and operating systems
    C. Allows attackers to interact with the basic operating system
    D. Records every activity and traps attackers

30. Which is a difficulty in defending against DDoS attacks?

    A. Attack packets usually have spoofed IP addresses
    B. Filtering incoming flow may reject legitimate traffic
    C. Local subnet scanning creates large amounts of traffic
    D. DRDoS Attacks require the attacker to have access to the victim's LAN

SECTION B

(40 Marks)

There are TWO (2) questions in this section. Choose and answer ONE (1) question only.

Question 1

Explain the various methods and ethical considerations involved in password cracking and phishing attacks. Discuss their advantages, disadvantages, and the importance of ethical use of password cracker tools.

Question 2

Discuss the significance of Metasploit in penetration testing and cybersecurity. Explore its evolution, functionalities, and the impact it has had on the field of exploit development. Additionally, elaborate the different types of Metasploit payloads and their roles in carrying out cyber-attacks.

***** END OF QUESTION PAPER *****