2504N442

Candidate's Seat No :_____

Integ. MSc (CSF) Semester-4 Examination

ICSF - 207

Cyber Security Fundamentals-II

Time : 2-30 Hours] **April-2024** **[Max. Marks : 70**

Instructions: Illustrate your answers with neat diagrams wherever necessary.

Que 1 Write the following

(i) Discuss the concept of access control mechanisms in cybersecurity. Compare and contrast discretionary access control (DAC) and mandatory access control (MAC) systems, highlighting their key features, advantages, and limitations. (7 Marks)

(ii) Explain the concept of malicious code in cybersecurity, detailing its characteristics, types, and potential impacts on computer systems (7 Marks)

OR

(i) Explain the process of brute force attacks, including the automated nature of the attack. (7 Marks)

(ii) Explain the concept of a timing attack in cybersecurity. Describe how timing attacks exploit variations in system response times to gain unauthorized access to sensitive information or compromise security measures. (7 Marks)

Que 2 Write the following

(i) Define what XSS is and how it can be exploited by attackers. Describe the types of XSS attacks. (7 Marks)

(ii) Explain SQL injection as a vulnerability in web applications. Describe how SQL injection attacks work, including their objectives and potential consequences. Discuss common mitigation techniques to prevent SQL injection attacks in web development. (7 Marks)

OR

(i) Explain the differences between computer worms and Trojans, providing examples of each type of malware. Discuss their methods of propagation, potential impacts on computer systems, and strategies for mitigating their risks. (7 Marks)

(ii) Explain the concept of topological worms in the context of computer security. Discuss how these worms propagate through a network topology and the potential risks they pose to network infrastructure. (7 Marks)

Que 3 Write the following

(i) Describe the architecture of the Linux operating system in detail (7 Marks)

(ii) Explain the usage and functionality of the grep command in Linux (7 Marks)

OR

(i) Explain the hierarchical structure of the Linux file system. Discuss the significance of directories such as /bin, /etc, /usr, and /home in the Linux file system hierarchy. (7 Marks)

(ii) Explain what shell scripting is and how it is used in the context of operating systems. (7 Marks)

P.T.O.

MMG-2

Que 4 Write the following

(i) Difference between Symmetric key Cryptography and Asymmetric key cryptography. (7 Marks)

(ii) In an RSA cryptosystem, a participant uses two prime numbers p = 3 and q = 11 to generate his public and private keys. If the private key is 7, then how will the text "**Cybersecurity**" be encrypted using the public key? (7 Marks)

OR

(i) What is SET? Explain who we can implement in Cryptography. (7 Marks)

(ii) Explain the concepts of digital certificates and digital signatures in the context of cybersecurity. Discuss their roles in ensuring authenticity, integrity, and confidentiality of digital communications. (7 Marks)

Que 5 Attempt any seven out of twelve (14 Marks)

(i) Trojans are named after the _____ horse of Greek mythology, as they masquerade as legitimate software or files to deceive users into executing them.

(ii) Examples of malicious code include: ____

(iii) The use of _____ can help mitigate the risk of sniffing attacks by encrypting network traffic.

(iv) Another approach to mitigate SQL injection vulnerabilities is by implementing proper _____ validation and sanitization techniques.

(v) Cross-Site Scripting (XSS) is a type of _____ attack where attackers inject malicious scripts into web pages viewed by other users.

(vi) Cross-Site Scripting (XSS) is a serious security vulnerability that allows attackers to execute malicious scripts in the context of a user's _____.

(vii) Phishing is a type of _____ attack that involves tricking individuals into providing sensitive information such as usernames, passwords, and credit card details.

(viii) To make a shell script executable, you need to give execute permissions using the _____ command.

(ix) A cryptographic algorithm that uses the same key for both encryption and decryption is called _____.

(x) A hash function takes an input (or 'message') and returns a fixed-size string of bytes, which is typically a _____.

(xi) A cryptographic protocol that provides secure communication over a computer network is called _____.

(xii) The process of attempting to reverse-engineer a hash value to obtain the original input is called _____.