0110N637

Candidate's Seat No :_____

B.Sc Sem.-6 (Rep) Examination

SE 311

Computer Science (B) Cyber Security

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

Q1(A)	Explain the concept of risk management in cybersecurity. How does it help organizations protect their assets?	(7)
Q1(B)	Discuss the differences between symmetric and asymmetric encryption. Provide examples of when each type might be used.	(7)
	OR	
Q1(A)	Describe the various types of malware and how they can affect a system. Provide examples of each type.	(7)
Q1(B)	Explain the role of firewalls in network security. What are the differences between packet filtering firewalls and stateful inspection firewalls?	(7)
Q2(A)	Discuss the principles of access control and the importance of implementing effective access control mechanisms in an organization.	(7)
Q2(B)	What is a Distributed Denial of Service (DDoS) attack? Describe methods to prevent or mitigate such attacks.	(7)
	OR	
Q2(A)	Explain the concept of multi-factor authentication (MFA) and its importance in enhancing security. What are some common MFA methods?	(7)
Q2(B)	Discuss the principles and practices of secure software development. How can developers ensure their applications are secure?	(7)
Q3(A)	Describe the steps involved in a typical incident response process. Why is each step important for effective incident management?	(7)
Q3(B)	What is social engineering? Provide examples of common social engineering attacks and strategies to protect against them.	(7)
	OR	
Q3(A)	Explain the concept of cryptographic hashing and its uses in cybersecurity. How does hashing differ from encryption?	(7)
Q3(B)	Discuss the role of intrusion detection systems (IDS) and intrusion prevention systems (IPS) in network security. How do they differ?	(7)
Q4(A)	What is a zero-day vulnerability? Why are they particularly dangerous, and what strategies can organizations use to protect against them?	(7)
Q4(B)	Describe the importance of patch management in maintaining cybersecurity. What challenges are associated with patch management?	(7)
	OR	
Q4(A)	Explain the concept of security policies and procedures. How can they be used to enhance an organization's security posture?	(7)
Q4(B)	Discuss the differences between ethical hacking and malicious hacking. What are the key ethical considerations for ethical hackers?	(7)
Q5	**MCQ Attempt any seven out of twelve.(2 Marks each)**	**(14)**

N637-2

1) Which of the following best describes a "phishing" attack?
   A) An attack that exploits vulnerabilities in software.
   B) An attempt to acquire sensitive information by pretending to be a trustworthy entity.
   C) A type of denial-of-service attack.
   D) An attack that physically damages hardware.
2) What is the primary goal of a "man-in-the-middle" (MitM) attack?
   A) To interrupt the normal operation of a network.
   B) To intercept and potentially alter communication between two parties.
   C) To overwhelm a server with requests.
   D) To exploit a software vulnerability.
3) Which protocol is used to secure email communication?
   A) HTTP
   B) FTP
   C) SSL/TLS
   D) SMTP
4) Which of the following is an example of a "zero-day" vulnerability?
   A) A vulnerability that is publicly known but not yet patched.
   B) A software bug that has been fixed in a recent update.
   C) A vulnerability that is exploited before the vendor releases a fix.
   D) A known vulnerability that has been mitigated by security software.
5) Which type of malware is designed to disguise itself as legitimate software?
   A) Worm
   B) Trojan horse
   C) Ransomware
   D) Adware
6) In cybersecurity, what does the acronym "CIA" stand for?
   A) Central Intelligence Agency
   B) Confidentiality, Integrity, Availability
   C) Computer Information Access
   D) Cyber Intelligence Assessment
7) Which of the following is the best method to prevent SQL injection attacks?
   A) Regularly updating antivirus software
   B) Using prepared statements with parameterized queries
   C) Encrypting all data in the database
   D) Disabling JavaScript in the browser
8) What is a "Denial of Service" (DoS) attack designed to do?
   A) Steal sensitive information from a user.
   B) Prevent legitimate users from accessing a service or resource.
   C) Install malware on a target system.
   D) Intercept communications between two parties.
9) Which security measure helps protect against "brute force" attacks?
   A) Regular software updates
   B) Strong, complex passwords and account lockout mechanisms
   C) Using antivirus software
   D) Encryption of data in transit
10) What does the term "social engineering" refer to in cybersecurity?
   A) The manipulation of individuals to gain unauthorized access to information or systems.
   B) The design of secure software and hardware systems.
   C) The physical security of network infrastructure.
   D) The use of cryptographic techniques to secure communications.

N637-3

11) What is the purpose of "network segmentation" in cybersecurity?
A) To enhance network speed and performance.
B) To isolate different parts of a network to limit the spread of an attack.
C) To simplify network management.
D) To create redundant network paths.

12) What does the term "ransomware" refer to?
A) A type of malware that encrypts data and demands payment for the decryption key.
B) A software that tracks user behavior for marketing purposes.
C) A vulnerability scanner used to detect potential security weaknesses.
D) A method of gaining unauthorized access to a network by exploiting a flaw.

BEST OF LUCK