PREVIEW QUESTION BANK

Module Name : nou24-cs04 Introduction to Cyber Security-ENG
Exam Date : 18-May-2024 Batch : 09:00-12:00

Sr. No.	Client Question ID	Question Body and Alternatives	Marks	Negative Marks
Objective Question				
1	11721001	Which of the following is NOT considered a primary goal of cybersecurity? 1. Confidentiality 2. Integrity 3. Accessibility 4. Availability A1 : 1 A2 : 2 A3 : 3 A4 : 4		
Objective Question				
2	11721002	Given below are two statements, one is labelled as Assertion (A) and other one labelled as Reason (R). Assertion (A): Social engineering attacks rely on manipulating individuals to divulge confidential information. Reason (R): Social engineering attacks do not exploit human psychology and trust to deceive victims into performing actions or revealing sensitive information. In light of the above statements, choose the *correct* answer from the options given below. 1. Both (A) and (R) are true and (R) is the correct explanation of (A). 2. Both (A) and (R) are true but (R) is NOT the correct explanation of (A). 3. (A) is true but (R) is false. 4. (A) is false but (R) is true. A1 : 1 A2 : 2 A3 : 3 A4 : 4		
Objective Question				
3	11721003			

Match **List-I** with **List-II**

List-I	**List-II**
(A). Remote Wipe	(I). Small pieces of data stored on a user's device by websites to track and authenticate users.
(B). Spam Filter	(II). A feature that allows users to remotely erase data from their lost or stolen smartphones to prevent unauthorized access.
(C). Cross-Site Scripting (XSS)	(III). An email security measure that detects and blocks unsolicited or unwanted emails.
(D). Cookies	(IV). A security vulnerability where attackers inject malicious scripts into web pages viewed by other users.

Choose the **correct** answer from the options given below:

1. (A) - (II), (B) - (III), (C) - (IV), (D) - (I)
2. (A) - (I), (B) - (II), (C) - (III), (D) - (IV)
3. (A) - (I), (B) - (II), (C) - (IV), (D) - (III)
4. (A) - (III), (B) - (IV), (C) - (I), (D) - (II)

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

4 11721004

Which type of attack involves tricking individuals into revealing sensitive information?

1. DDoS attack
2. Phishing attack
3. Brute force attack
4. SQL injection attack

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

5 11721005

Given below are two statements:

Statement (I): Encryption is the process of converting data into a format that cannot be easily understood by unauthorized users.

Statement (II): Decryption is the process of converting encrypted data back into its original form.

In light of the above statements,choose the *most appropriate* answer from the options given below.

1. Both Statement (I) and Statement (II) are true.
2. Both Statement (I) and Statement (II) are false.
3. Statement (I) is true but Statement (II) is false.
4. Statement (I) is false but Statement (II) is true.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

6 11721006

Which of the following is a recommended practice to enhance smartphone security?

1. Disabling automatic updates
2. Downloading apps from third-party app stores
3. Enabling biometric authentication
4. Sharing your passcode with friends

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

7 11721007

Given below are two statements, one is labelled as Assertion (A) and other one labelled as Reason (R).

Assertion (A): Encryption is an essential technique in cybersecurity to protect data from unauthorized access.

Reason (R): Encryption converts plaintext into ciphertext using algorithms and keys, making it unreadable without proper decryption.

In light of the above statements, choose the *correct* answer from the options given below.

1. Both (A) and (R) are true and (R) is the correct explanation of (A).
2. Both (A) and (R) are true but (R) is NOT the correct explanation of (A).
3. (A) is true but (R) is false.
4. (A) is false but (R) is true.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

8 11721008

Match **List-I** with **List-II**

List-I	**List-II**
(A). Cybersecurity Policy	(I). Establishes guidelines for protecting information assets
(B). Risk Assessment	(II). Identifies potential threats and vulnerabilities
(C). Penetration Testing	(III). Evaluates the effectiveness of security controls
(D). Incident Response Plan	(IV). Outlines procedures for responding to security incidents

Choose the **correct** answer from the options given below:

1. (A) - (I), (B) - (II), (C) - (III), (D) - (IV)
2. (A) - (I), (B) - (IV), (C) - (III), (D) - (II)
3. (A) - (I), (B) - (II), (C) - (IV), (D) - (III)
4. (A) - (III), (B) - (IV), (C) - (I), (D) - (II)

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

9 11721009

Given below are two statements, one is labelled as Assertion (A) and other one labelled as Reason (R).

Assertion (A): Firewalls are an essential component of network security.

Reason (R): Firewalls monitor and control incoming and outgoing network traffic based on predetermined security rules.

In light of the above statements, choose the *correct* answer from the options given below.

1. Both (A) and (R) are true and (R) is the correct explanation of (A).
2. Both (A) and (R) are true but (R) is NOT the correct explanation of (A).
3. (A) is true but (R) is false.
4. (A) is false but (R) is true.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

10 11721010

Given below are two statements:

Statement (I): Phishing is a cyber attack method that involves tricking individuals into providing sensitive information such as passwords or credit card details.

Statement (II): Malware refers to software designed to disrupt, damage, or gain unauthorized access to computer systems.

In light of the above statements,choose the *most appropriate* answer from the options given below.

1. Both Statement (I) and Statement (II) are true.
2. Both Statement (I) and Statement (II) are false.
3. Statement (I) is true but Statement (II) is false.
4. Statement (I) is false but Statement (II) is true.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

11 11721011

Which of the following are examples of network security measures?

(A). Intrusion Detection Systems (IDS)

(B). Public key cryptography

(C). Social engineering

(D). Secure Sockets Layer (SSL) certificates

Choose the ***correct*** answer from the options given below:

1. (A), (B) and (D) only.
2. (B) and (D) only.
3. (A), (B), (C) and (D).
4. (B), (C) and (D) only.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

12 11721012

Given below are two statements, one is labelled as Assertion (A) and other one labelled as Reason (R).

Assertion (A): Using public Wi-Fi networks without proper security measures can pose significant risks to personal data.

Reason (R): Public Wi-Fi networks are often unsecured, making it easier for cybercriminals to intercept data transmitted over these networks.

In light of the above statements, choose the *correct* answer from the options given below.

1. Both (A) and (R) are true and (R) is the correct explanation of (A).
2. Both (A) and (R) are true but (R) is NOT the correct explanation of (A).
3. (A) is true but (R) is false.
4. (A) is false but (R) is true.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

13 11721013

Match **List-I** with **List-II**

List-I	**List-II**
(A). Phishing	(I). Disguised as a legitimate program
(B). Ransomware	(II). Fraudulent solicitation in email or on a web site
(C). Denial of Service (DoS)	(III). Inaccessible to its intended users
(D). Trojan Horse	(IV). Encrypts Files

Choose the **correct** answer from the options given below:

1. (A) - (I), (B) - (II), (C) - (III), (D) - (IV)
2. (A) - (II), (B) - (IV), (C) - (III), (D) - (I)
3. (A) - (I), (B) - (II), (C) - (IV), (D) - (III)
4. (A) - (III), (B) - (IV), (C) - (I), (D) - (II)

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

14 11721014

What is the purpose of encryption in cybersecurity?

1. To monitor network traffic
2. To prevent unauthorized access
3. To detect malware
4. To optimize system performance

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

15 11721015

Given below are two statements:

Statement (I): Firewall is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Statement (II): Antivirus software is used to encrypt sensitive data to protect it from unauthorized access.

In light of the above statements, choose the *most appropriate* answer from the options given below.

1. Both Statement (I) and Statement (II) are correct.
2. Both Statement (I) and Statement (II) are incorrect.
3. Statement (I) is correct but Statement (II) is incorrect.
4. Statement (I) is incorrect but Statement (II) is correct.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

16 11721016

Which of the following is an example of a social engineering attack?

1. Installing antivirus software
2. Using strong passwords
3. Sending fraudulent emails to trick recipients into revealing personal information
4. Enabling two-factor authentication

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

17 11721017

What is the primary role of a firewall in network security?

1. To encrypt data transmission
2. To monitor network traffic for suspicious activities
3. To authenticate users
4. To manage software updates

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

18 11721018

Which term refers to the practice of discovering and exploiting vulnerabilities in computer systems?

1. Encryption
2. Penetration testing
3. Social engineering
4. Network monitoring

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

19 11721019

Given below are two statements, one is labelled as Assertion (A) and other one labelled as Reason (R).

Assertion (A): Data encryption ensures confidentiality by converting plaintext into unreadable ciphertext.

Reason (R): Data encryption alone is sufficient to protect data integrity and availability.

In light of the above statements, choose the *correct* answer from the options given below.

1. Both (A) and (R) are true and (R) is the correct explanation of (A).
2. Both (A) and (R) are true but (R) is NOT the correct explanation of (A).
3. (A) is true but (R) is false.
4. (A) is false but (R) is true.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

20 11721020

Given below are two statements:

Statement I: Two-factor authentication (2FA) requires users to provide two different authentication factors to verify their identity.

Statement II: Data encryption is a preventive security measure used to detect and respond to security breaches in real-time.

In light of the above statements,choose the *most appropriate* answer from the options given below.

1. Both Statement (I) and Statement (II) are true.
2. Both Statement (I) and Statement (II) are false.
3. Statement (I) is true but Statement (II) is false.
4. Statement (I) is false but Statement (II) is true.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

21 11721021

What are typical examples of physical security measures?

(A). CCTVs

(B). Biometric access controls

(C). Security Lighting

(D). Security Alarm

Choose the ***correct*** answer from the options given below:

1. (A), (B) and (D) only.
2. (A) and (D) only.
3. (A), (B), (C) and (D).
4. (B), (C) and (D) only.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

22 11721022

What does the acronym "DDoS" stand for in the context of cybersecurity?

1. Data Distribution over Systems
2. Digital Defense of Systems
3. Direct Detection of Security breaches
4. Distributed Denial of Service

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

23 11721023

Given below are two statements, one is labelled as Assertion (A) and other one labelled as Reason (R).

Assertion (A): Biometrics is the most suitable means of identifying and authenticating individuals in a reliable and fast way through unique biological characteristics.

Reason (R): Biometric authentication methods are immune to spoofing attacks and cannot be compromised.

In light of the above statements, choose the *correct* answer from the options given below.

1. Both (A) and (R) are true and (R) is the correct explanation of (A).
2. Both (A) and (R) are true but (R) is NOT the correct explanation of (A).
3. (A) is true but (R) is false.
4. (A) is false but (R) is true.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

24 11721024

Which of the following is NOT a common type of social engineering attack?

1. Phishing
2. Spoofing
3. Trojan Horse
4. SQL Injection

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

25 11721025

Given below are two statements:

Statement I: Denial of Service (DoS) attacks aim to gain unauthorized access to a system by exploiting vulnerabilities in the software.

Statement II: Social engineering involves manipulating individuals to disclose confidential information or perform certain actions.

In light of the above statements,choose the *most appropriate* answer from the options given below.

1. Both Statement (I) and Statement (II) are true.
2. Both Statement (I) and Statement (II) are false.
3. Statement (I) is true but Statement (II) is false.
4. Statement (I) is false but Statement (II) is true.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

26 11721026

What are characteristics of a secure web browser?

(A). Built-in pop-up blockers

(B). Cookie Blocking

(C). Automatic Updates

(D). Storing passwords in plain text

Choose the ***correct*** answer from the options given below:

1. (A), (B) and (D) only.
2. (A), (B) and (C) only.
3. (A), (B), (C) and (D).
4. (B), (C) and (D) only.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

27 11721027

Given below are two statements, one is labelled as Assertion (A) and other one labelled as Reason (R).

Assertion (A): Regular software updates are crucial for maintaining cybersecurity.

Reason (R): Software updates often include patches for security vulnerabilities discovered in previous versions.

In light of the above statements, choose the *correct* answer from the options given below.

1. Both (A) and (R) are true and (R) is the correct explanation of (A).
2. Both (A) and (R) are true but (R) is NOT the correct explanation of (A).
3. (A) is true but (R) is false.
4. (A) is false but (R) is true.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

28 11721028

What term describes the process of converting plaintext into ciphertext?

1. Encryption
2. Decryption
3. Authentication
4. Authorization

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

29 11721029

Which of the following is NOT a common category of malware?

1. Virus
2. Spyware
3. Router
4. Ransomware

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

30 11721030

Given below are two statements:

Statement I: A VPN (Virtual Private Network) provides a secure connection over the internet by encrypting data transmitted between a user's device and a remote server.

Statement II: Phishing attacks typically involve attackers attempting to gain access to a system by exploiting vulnerabilities in software.

In light of the above statements, choose the *most appropriate* answer from the options given below.

1. Both Statement (I) and Statement (II) are correct.
2. Both Statement (I) and Statement (II) are incorrect.
3. Statement (I) is correct but Statement (II) is incorrect.
4. Statement (I) is incorrect but Statement (II) is correct.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

31 11721031

Which of the following are examples of network security devices?

(A). Intrusion Detection System (IDS)

(B). Printers

(C). Intrusion Prevention System (IPS)

(D). Firewalls

Choose the ***correct*** answer from the options given below:

1. (A), (B) and (D) only.
2. (A), (B) and (C) only.
3. (A), (B), (C) and (D).
4. (A), (C) and (D) only.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

32 11721032

Which protocol is commonly used to secure email communication?

1. HTTP
2. SMTP
3. FTP
4. Telnet

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

33 11721033

Match **List-I** with **List-II**

List-I	**List-II**
(A). Authentication	(I). Digital Certificate
(B). Public Key Infrastructure	(II). Username and Password
(C). Two-Factor Authentication	(III). Symmetric Encryption
(D). Encryption	(IV). Requires two forms of identification

Choose the **correct** answer from the options given below:

1. (A) - (I), (B) - (II), (C) - (III), (D) - (IV)
2. (A) - (I), (B) - (III), (C) - (II), (D) - (IV)
3. (A) - (I), (B) - (II), (C) - (IV), (D) - (III)
4. (A) - (II), (B) - (I), (C) - (IV), (D) - (III)

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

34 11721034

What is the term for a security vulnerability that has been discovered but not yet patched by the software vendor?

1. Brute force attack
2. Zero-day exploit
3. Buffer overflow
4. Cross-site scripting

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

35 11721035

Given below are two statements:

Statement I: Using a secure HTTPS connection ensures encrypted communication between the browser and the website, enhancing data confidentiality.

Statement II: Web browser extensions and plugins can introduce security vulnerabilities and should be carefully reviewed and updated regularly.

In light of the above statements, choose the *most appropriate* answer from the options given below.

1. Both Statement (I) and Statement (II) are correct.
2. Both Statement (I) and Statement (II) are incorrect.
3. Statement (I) is correct but Statement (II) is incorrect.
4. Statement (I) is incorrect but Statement (II) is correct.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

36 11721036

What are examples of cybersecurity best practices for employees?

(A). Using weak passwords

(B). Sharing sensitive information with unauthorized personnel

(C). Reporting suspicious emails or activities

(D). Encrypt Data

Choose the ***correct*** answer from the options given below:

1. (A), (B) and (D) only.
2. (A), (B) and (C) only.
3. (A), (B), (C) and (D).
4. (C) and (D) only.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

37 11721037

What is the primary purpose of security awareness training for employees?

1. To install antivirus software on employee devices
2. To educate employees about cybersecurity risks and best practices
3. To block access to unauthorized websites
4. To perform regular backups of sensitive data

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

38 11721038

Given below are two statements, one is labelled as Assertion (A) and other one labelled as Reason (R).

Assertion (A): Avoiding oversharing personal information on social media platforms helps mitigate the risk of identity theft and privacy breaches.

Reason (R): Cybercriminals may use information shared on social media, such as birthdates, addresses, or vacation plans, to perpetrate identity theft or target individuals for phishing attacks.

In light of the above statements, choose the *correct* answer from the options given below.

1. Both (A) and (R) are true and (R) is the correct explanation of (A).
2. Both (A) and (R) are true but (R) is NOT the correct explanation of (A).
3. (A) is true but (R) is false.
4. (A) is false but (R) is true.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

39 11721039

What does the term "vulnerability" refer to in cybersecurity?

1. An unauthorized person gaining access to a network
2. A weakness in a system that could be exploited by a threat
3. Encrypting data to protect it from unauthorized access
4. A type of malware that spreads through email attachments

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

40 11721040

Given below are two statements:

Statement I: A strong password should be complex, consisting of a combination of uppercase and lowercase letters, numbers, and special characters.

Statement II: Salami Attack is a type of malware that encrypts files or systems and demands payment from the victim to restore access.

In light of the above statements, choose the *most appropriate* answer from the options given below.

1. Both Statement (I) and Statement (II) are correct.
2. Both Statement (I) and Statement (II) are incorrect.
3. Statement (I) is correct but Statement (II) is incorrect.
4. Statement (I) is incorrect but Statement (II) is correct.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

41 11721041

What are examples of common cybersecurity threats?

(A). Phishing attacks

(B). Software updates

(C). Insider Threats

(D). Denial-of-Service (DoS) Attacks

Choose the ***correct*** answer from the options given below:

1. (A), (C) and (D) only.
2. (A), (B) and (D) only.
3. (A), (B), (C) and (D).
4. (B), (C) and (D) only.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

42 11721042

What does HTTPS stand for in the context of web browsing?

1. Hypertext Transfer Protocol Secure
2. High-Efficiency Transport Protocol System
3. Hypertext Transfer Protocol Service
4. Hosted Encryption and Protection System

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

43 11721043

Given below are two statements, one is labelled as Assertion (A) and other one labelled as Reason (R).

Assertion (A): Denial of Service (DoS) attacks does not disrupt the availability of network resources.

Reason (R): DoS attacks exploit vulnerabilities in software to gain unauthorized access to a system.

In light of the above statements, choose the *correct* answer from the options given below.

1. Both (A) and (R) are true and (R) is the correct explanation of (A).
2. Both (A) and (R) are true but (R) is NOT the correct explanation of (A).
3. (A) is true but (R) is false.
4. (A) is false but (R) is true.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

44 11721044

What is the purpose of a browser cookie?

1. To track user activity and personalize website experiences
2. To prevent unauthorized access to websites
3. To encrypt data transmission between the browser and web servers
4. To block access to certain websites

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

45 11721045

Given below are two statements:

Statement I: A keylogger is a hardware device used to monitor network traffic and detect suspicious activities.

Statement II: Network segmentation involves dividing a computer network into smaller subnetworks to enhance security and performance.

In light of the above statements, choose the *most appropriate* answer from the options given below.

1. Both Statement (I) and Statement (II) are correct.
2. Both Statement (I) and Statement (II) are incorrect.
3. Statement (I) is correct but Statement (II) is incorrect.
4. Statement (I) is incorrect but Statement (II) is correct.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

46 11721046

What is the purpose of a Virtual Private Network (VPN) in cybersecurity?

(A). To adds security and anonymity to users when they connect to web-based services and sites.

(B). To block all incoming network traffic

(C). To disable encryption on network communication

(D). To provides a secure, encrypted connection between two points.

Choose the ***correct*** answer from the options given below:

1. (A), (B) and (D) only.
2. (A), (B) and (C) only.
3. (A) and (D) only.
4. (B), (C) and (D) only.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

47 11721047

Given below are two statements, one is labelled as Assertion (A) and other one labelled as Reason (R).

Assertion (A): Phishing is a common cyber attack method used to deceive individuals into revealing sensitive information.

Reason (R): Phishing emails often mimic legitimate messages from trusted sources to trick recipients into clicking on malicious links or providing personal data.

In light of the above statements, choose the *correct* answer from the options given below.

1. Both (A) and (R) are true and (R) is the correct explanation of (A).
2. Both (A) and (R) are true but (R) is NOT the correct explanation of (A).
3. (A) is true but (R) is false.
4. (A) is false but (R) is true.

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

48 11721048

Which of the following is a recommended practice to enhance smartphone security?

1. Disabling automatic software updates
2. Using public Wi-Fi networks without encryption
3. Installing apps only from official app stores
4. Sharing passwords with friends and family

A1 : 1

A2 : 2

A3 : 3

A4 : 4

Objective Question

49 11721049

Given below are two statements, one is labelled as Assertion (A) and other one labelled as Reason (R).

Assertion (A): Enabling app permissions selectively enhances smartphone security.

Reason (R): Allowing all permissions requested by apps ensures smooth functionality and better security.

In light of the above statements, choose the *correct* answer from the options given below.

1. Both (A) and (R) are true and (R) is the correct explanation of (A).
2. Both (A) and (R) are true but (R) is NOT the correct explanation of (A).
3. (A) is true but (R) is false.
4. (A) is false but (R) is true.

		A1 : 1 A2 : 2 A3 : 3 A4 : 4
Objective Question		
50	11721050	Given below are two statements: Statement I: Security patches are software updates designed to fix vulnerabilities and improve the security of a system. Statement II: VPN (Virtual Private Network) are used to prevent unauthorized access to a network by monitoring and analyzing network traffic. In light of the above statements, choose the *most appropriate* answer from the options given below. 1. Both Statement (I) and Statement (II) are correct. 2. Both Statement (I) and Statement (II) are incorrect. 3. Statement (I) is correct but Statement (II) is incorrect. 4. Statement (I) is incorrect but Statement (II) is correct. A1 : 1 A2 : 2 A3 : 3 A4 : 4