

CYBER SECURITY
(CSBS 4242)

Time Allotted : 2½ hrs

Full Marks : 60

Figures out of the right margin indicate full marks.

*Candidates are required to answer Group A and
any 4 (four) from Group B to E, taking one from each group.*

Candidates are required to give answer in their own words as far as practicable.

Group – A

1. Answer any twelve:

12 × 1 = 12

Choose the correct alternative for the following

- (i) Which Identity theft creates fake identity by combining personal information from multiple victims?
 - (a) Child ID theft
 - (b) Identity Cloning
 - (c) Synthetic Identity theft
 - (d) None of these
- (ii) What is the primary goal of a pharming attack?
 - (a) Redirect users to fraudulent websites
 - (b) Encrypt files for ransom
 - (c) Infect users' computers with ransomware
 - (d) Steal hardware devices
- (iii) What is the primary purpose of a phishing attack?
 - (a) Encrypt files for ransom
 - (b) Trick users into providing sensitive information
 - (c) Gain unauthorized access to a website
 - (d) Install antivirus software
- (iv) What is the purpose of an SQL injection attack?
 - (a) To encrypt files for ransom
 - (b) To disable antivirus software
 - (c) To overload a system with requests
 - (d) To inject malicious SQL code into a database
- (v) Which of the following is a Distributed Denial-of-Service (DDoS) attack technique?
 - (a) Man-in-the-Middle Attack
 - (b) Botnet-based flooding
 - (c) SQL Injection
 - (d) Social Engineering
- (vi) Which attack in DOS sends oversized ICMP packets?
 - (a) Flood attack
 - (b) Nuke attack
 - (c) SYN attack
 - (d) Ping of death attack

- (vii) What is the function of a keylogger?
 (a) Encrypt user data
 (b) Protect against phishing attacks
 (c) Delete system files
 (d) Record keystrokes to steal sensitive information
- (viii) _____ phishing is that type of phishing where the construction of a fake webpage is done for targeting definite keywords & waiting for the searcher to land on the fake webpage.
 (a) Voice (b) SMS (c) Search Engine (d) E-mail
- (ix) An attacker who eavesdrops on network communication to gather sensitive information is performing a/an
 (a) Active Attack (b) Passive Attack
 (c) Physical attack (d) Social Engineering Attack
- (x) Act of breaking into phone or other communication systems.
 (a) War dialer (b) Cracking
 (c) Phreaking (d) Hacking

Fill in the blanks with the correct word

- (xi) A _____ virus attaches itself to executable files and spreads when the file is executed.
- (xii) _____ consumes bandwidth, overloading infected systems and making them unreliable or unavailable.
- (xiii) _____ prevents users from accessing a system and the files it contains.
- (xiv) SQL injection is a cyber attack that exploits vulnerabilities in a website's _____.
- (xv) _____ is a means of bypassing an organization's existing security systems.

Group - B

2. (a) How to reduce the chances of becoming part of a Bot? [[C02](Remember/LOCQ)]
 (b) Explain the types of Stalkers. [[C02](Understand/LOCQ)]
 (c) What is reconnaissance? [[C02](Understand/LOCQ)]
6 + 3 + 3 = 12
3. (a) Differentiate among Green Hat Hacker, Blue Hat Hacker, Yellow Hat Hacker and Red Hat Hacker. [[C01](Analyze/IOCQ)]
 (b) Write short note on Phases of Cybercrime. [[C01/C02](Understand/LOCQ)]
 (c) Explain any four Passive attack tools used in Cybercrime. [[C02](Understand/LOCQ)]
4 + 4 + 4 = 12

Group - C

4. (a) How to prevent credit card frauds? [[C03](Understand/LOCQ)]

- (b) Explain Cryptographic Security for Mobile devices and LDAP security for Mobile devices. [[C03](Understand/LOCQ)]
6 + 6 = 12
5. (a) Explain the following term: Bluejacking, Bluesnarfing, Bluebugging, Car Whisperer. [[C03](Understand/LOCQ)]
- (b) Explain the working mechanism of Mishing with example. Discuss suitable countermeasures for Mishing. [[C03](Understand/LOCQ)]
6 + 6 = 12

Group - D

6. (a) Define keyloggers and spyware. How are they used in cyber espionage and financial fraud? [[C04](Understand/LOCQ)]
- (b) Explain the concept of phishing and credential stuffing in stealing user credentials. [[C04](Understand/LOCQ)]
(2 + 2 + 2 + 2) + 4 = 12
7. Discuss the different types of DoS attacks such as SYN flood, UDP flood, and HTTP flood. Explain their impact on system Performance. How can users protect against them? [[C05](Understand/LOCQ)]
(4 + 4 + 4) = 12

Group - E

8. (a) What are the different types of identity theft? Discuss the various techniques of identity theft. How do criminals steal personal data? [[C06](Understand/LOCQ)]
- (b) What are the different types of phishing scams? How do they affect users? [[C06](Understand/LOCQ)]
(2 + 4 + 2) + (2 + 2) = 12
9. (a) Define digital forensics and explain its importance in cybercrime investigation. [[C06](Understand/LOCQ)]
- (b) Differentiate between Dragnet and Gilnet. [[C06](Understand/LOCQ)]
- (c) Describe countermeasures against phishing attacks. [[C06](Understand/LOCQ)]
(2 + 4) + 4 + 2 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	95.83	4.16	0

