

CYBER SECURITY
(CBS3233)

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 type of attack involves directly modifying data on a system without the user's knowledge?
(a) Active Attack (b) Passive Attack
(c) DOS (d) Phishing
- (ii) _____ refers to phishing performed over smart-phone by calling.
(a) Vishing (b) Algo-based phishing
(c) Email-based phishing (d) Mishing
- (iii) Which of the following is not an example or type of phishing?
(a) Spear phishing (b) Deceptive phishing
(c) Whaling (d) Monkey in the Middle
- (iv) How does a Trojan Horse differ from a virus?
(a) A Trojan spreads automatically
(b) A Trojan does not require execution
(c) A Trojan appears to be legitimate software while containing malicious code
(d) A Trojan infects the boot sector
- (v) Which of the following anonymization tools is commonly used to access the dark web?
(a) Google Chrome (b) Mozilla Firefox
(c) Tor Browser (d) Internet Explorer
- (vi) What is the primary purpose of a proxy server in cybercrime?
(a) Enhancing website speed (b) Hiding the attacker's real IP address
(c) Blocking phishing emails (d) Encrypting files for ransom
- (vii) Which of the following is a type of Trojan that allows remote control of an infected system?
(a) Rootkit (b) Remote Access Trojan (RAT)
(c) Ransomware (d) Boot Sector Virus

- (viii) Which hashing algorithm is widely used in digital forensics to verify data integrity?
 (a) AES-128 (b) SHA-256
 (c) RSA (d) DES
- (ix) Which of the following forensic techniques is used to recover deleted files?
 (a) Phishing attack (b) Live analysis
 (c) Data carving (d) Social engineering
- (x) What is the main challenge in cloud forensics?
 (a) Easy access to logs (b) Limited data encryption
 (c) Data stored in multiple locations (d) Lack of legal issues

Fill in the blanks with the correct word

- (xi) A common tool used in digital forensic analysis to recover deleted files and analyze hard drives is _____.
- (xii) _____ is the process of embedding location data into photos and videos, which can be exploited for tracking individuals.
- (xiii) A brute force attack systematically tries every possible _____ until the correct one is found.
- (xiv) Stealing someone's personal information to commit fraud, open accounts, or make transactions is known as _____.
- (xv) A phishing attack that uses fake customer service emails to steal credentials is known as _____ phishing.

Group - B

2. (a) Explain the phases involved in planning Cybercrime. [[C01](Understand/IOCQ)]
 (b) Differentiate between Google Earth and Internet Archive. [[C01](Analyze/IOCQ)]
 (c) Explain the working of Cyberstalking in detail. [[C02](Understand/LOCQ)]
4 + 4 + 4 = 12
3. (a) Write short note on Botnet Menace. [[C01/C02](Understand/LOCQ)]
 (b) Explain the term patriot hacking. [[C01](Understand/LOCQ)]
 (c) Explain the following tools: Website Watcher, Arphound, Hping. [[C02](Remember/LOCQ)]
4 + 2 + 6 = 12

Group - C

4. (a) What is mobile virus? How to prevent from Mobile Malwares Attack? [[C03](Understand/LOCQ)]
 (b) Explain financial fraud. [[C03](Understand/LOCQ)]
 (c) What do you mean by the term Triangulation? [[C03](Understand/LOCQ)]
6 + 3 + 3 = 12

5. (a) Explain the Registry setting process for Mobile devices. *[[C03](Understand/LOCQ)]*
 (b) Explain the term phishing. *[[C03](Understand/LOCQ)]*
 (c) Define Credit card fraud. Explain different techniques of Credit card fraud. *[[C03](Understand/LOCQ)]*
3 + 3 + 6 = 12

Group - D

6. (a) What is password cracking attacks? *[[C04](Understand/LOCQ)]*
 (b) Explain the working mechanism of spyware. *[[C04](Understand/LOCQ)]*
 (c) Discuss the advantages of Anti keylogger. *[[C04](Understand/LOCQ)]*
 (d) Classify different types of computer viruses and explain their impact on system security. *[[C04](Understand/LOCQ)]*
2 + 3 + 3 + 4 = 12
7. (a) Define PDoS attack. Differentiate between PDos and Dos attack. *[[C05](Understand/LOCQ)]*
 (b) Explain SQL Injection with examples. *[[C05](Understand/LOCQ)]*
 (c) Differentiate between Hybrid password attack and Spyware. *[[C04](Analyze/IOCQ)]*
5 + 3 + 4 = 12

Group - E

8. (a) How can multi-factor authentication (MFA) and encryption help prevent identity theft? *[[C06](Understand/LOCQ)]*
 (b) Describe online financial fraud as a form of identity theft. How does it impact victims? *[[C06](Understand/LOCQ)]*
(3 + 3) + (3 + 3) = 12
9. (a) Compare and contrast computer forensics, mobile forensics, and network forensics. *[[C06](Understand/LOCQ)]*
 (b) Explain the role of volatile and non-volatile data in digital forensics. *[[C06](Understand/LOCQ)]*
(3 × 3) + 3 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	87.5	12.5	0

