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) Ping flood is associated with
(a) Ping of death attack (b) Nuke
(c) Teardrop attack (d) Flood attack

(ii) An example of Cybercrime against Individual
(a) Logic bomb (b) Cyber terrorism
(c) Password sniffing (d) Internet time theft

(iii) Which hacker discloses information about security holes in public?
(a) White Hat (b) Black Hat
(c) Grey Hat (d) Brown Hat.

(iv) What is the name of the viruses that fool a user into downloading and/or executing them by pretending to be useful applications?
(a) Cracker (b) Worm
(c) Trojan horses (d) Keylogger.

(v) Device that makes untraceable activity on the Internet
(a) Proxy server (b) Malwares
(c) Keyloggers (d) Anonymizer.

(vi) Method in which Phisher identify prospective victims in advance and convey false information toentice them for disclosing personal and financial data.
(a) Rod and Reel (b) Lobsterpot
(c) Gillnet (d) Dragnet

(vii) Three P's of Cybercrime.
(a) Phishing, Pharming and Privacy (b) Phishing, Pharming and Phreaking
(c) Phishing, Pharming and Phoraging (d) None of these.

(viii) What is the self-replicating program called?
(a) Keylogger (b) Cracker
(c) Worm (d) All of these.

(ix) Pharming is used for
(a) Data hiding (b) Data alteration
(c) Host file poisoning (d) All of these

(x) Which of the following helps in Bluetooth hacking?
(a) Blue Scanner (b) Blue Sniff
(c) Bluesnarfer (d) All of these.

Fill in the blanks with the correct word

(xi) The written Cyber Defamation is called _____.

(xii) _____ prevents users from accessing a system and the files it contains.

(xiii) Boot Sector Virus also known as _____.

(xiv) _____attempts to bypass detection by antivirus scanner by installing itself in the interrupt handler chain.

(xv) _____ consumes bandwidth, overloading infected systems and making them unreliable or unavailable.

Group - B

2. (a) Differentiate between Cyberspace, Cybersquatting and Cyberterrorism. *[(CO1)(Analyze/IOCQ)]*

(b) Differentiate among Salami attack, Logic Bomb and Software Piracy. *[(CO1)(Analyze/IOCQ)]*

6 + 6 = 12

3. (a) Differentiate among Green Hat Hacker, Blue Hat Hacker, Yellow Hat Hacker and Red Hat Hacker. *[(CO2)(Analyze/IOCQ)]*

(b) Explain any four Passive attack tools used in Cybercrime. *[(CO2)(Understand/LOCQ)]*

(c) Explain the working of Cyberstalking in detail. *[(CO2)(Understand/LOCQ)]*

4 + 4 + 4 = 12

Group - C

4. (a) Explain the security challenges posed by mobile device. *[(CO3)(Understand/LOCQ)]*

(b) Explain any six guidelines for implementing Mobile device security. *[(CO3)(Understand/LOCQ)]*

6 + 6 = 12

5. (a) Define Credit card fraud. Explain different techniques of Credit card fraud. *[(CO3)(Understand/LOCQ)]*

(b) Explain the countermeasures to be practiced to prevent attacks on mobile/cell phones. *[(CO3)(Understand/LOCQ)]*

(2 + 6) + 4 = 12

Group - D

6. (a) Defend the statement "Keylogger attack make system vulnerable". *[(CO4)(Analyze/IOCQ)]*
   (b) How polymorphic virus infects the system-Explain. *[(CO4)(Understand/LOCQ)]*
   (c) Differentiate among Software Keylogger, Hardware Keylogger and Anti Keylogger. *[(CO4)(Analyze/IOCQ)]*

4 + 3 + 5 = 12

7. (a) Differentiate between Smurf attack and Teardrop attack. *[(CO5)(Analyze/IOCQ)]*
   (b) Explain DoS, DDoS and PDoS attack with a suitable example. *[(CO5)(Understand/LOCQ)]*
   (c) Differentiate between Trojan Horse and Backdoor. *[(CO5)(Analyze/IOCQ)]*

4 + 4 + 4 = 12

Group - E

8. (a) Differentiate between Phishing and Spambots. Differentiate between Lobsterpot, Dragnet and Gillnet. *[(CO6)(Analyze/IOCQ]*
   (b) Explain different types of Human based Techniques of Identity Theft. *[(CO6)(Understand/LOCQ)]*

(2 + 4) + 6 = 12

9. (a) Explain any six types of Phishing Scams. *[(CO6)(Understand/LOCQ)]*
   (b) Define Homograph attack. Explain Geotagging in detail. *[(CO6)(Understand/LOCQ)]*
   (c) Explain any three tools for Digital Forensic Analysis. *[(CO6)(Understand/LOCQ)]*

6 + 3 + 3 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	59.4	40.6	0

Course Outcome (CO):

1. Define the concept of Cybercrime and Cybercriminals.
2. Discuss the different tools for Active attack and Passive attack.
3. Compare the attacks on mobile/Cell phones.
4. Explain types of Virus and Worms, Trojan Horse and Backdoor.
5. Explain Denial of Service (DOS) attacks, DDOS attack and SQL injection.
6. Explain Phishing and Identity theft and Digital Forensic Analysis.

**LOCQ: Lower Order Cognitive Question; IOCQ: Intermediate Order Cognitive Question; HOCQ: Higher Order Cognitive Question.*