B.TECH/IT/7TH SEM/INFO 4142/2019

CYBER LAW AND SECURITY POLICY
(INFO 4142)

Time Allotted : 3 hrs **Full Marks : 70**

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and <u>any 5 (five)</u> from Group B to E, taking <u>at least one</u> from each group.

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

Group – A
(Multiple Choice Type Questions)

1. Choose the correct alternative for the following: **10 × 1 = 10**

(i) __________ is a technique used to find passwords or encryption key.
(a) War dialer (b) Cracking
(c) Phreaking (d) Brute force hacking

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

(iii) Tool used for testing Bluetooth penetration is
(a) Bluesnarfer (b) BlueBugger
(c) BlueDiving (d) none of these.

(iv) Website forgery is a __________ technique.
(a) Identity Theft (b) Vishing
(c) Phishing (d) none of these

(v) _________ is an invisible pop-ups.
(a) In-session phishing (b) Web Trojans
(c) Pharming (d) Synthetic Trojans

(vi) ____________ are malicious programs that redirects user traffic to fake websites.
(a) Cracker (b) Worm
(c) Trojan horses (d) Redirectors

(vii) ____________ Tool launches various attacks such as ICMP flood, SYN flood, UDP flood and Smurf attack.
(a) Tribe flood network (b) Targa
(c) MStream (d) None of the mentioned

(viii) Three Ps of Cybercrime are
(a) Phishing, Pharming and Privacy
(b) Phishing, Pharming and Phreaking
(c) Phishing, Pharming and Phoraging
(d) none of these.

(ix) __________ targets top management executives in private organizations.
(a) Spear Phishing (b) Whaling
(c) Worm (d) All of the mentioned

(x) Which tool is used to protect online identity?
(a) Targa (b) Anti Tracks
(c) Trinoo (d) None of the above.

Group – B

2. (a) State different types of Cybercriminals with examples. Differentiate between Salami attack and Software Piracy.

(b) Explain any four Passive attack tools used in Cybercrime.

(c) Differentiate between Data Diddling and Web Jacking.

(4 + 2) + 4 + 2 =12

3. (a) What is Cyberstalking? How does Cyberstalking work? (Explain all steps in detail)

(b) Explain any four Active attack tools used in Cybercrime.

(c) What is Patriot hacking?

(2 + 4) + 4 + 2 = 12

Group – C

4. (a) What are the operating guidelines for implementing mobile device security in organizations?

(b) Discuss different techniques of credit card fraud.

(c) Differentiate between software and hardware Keylogger.

6 + 4 + 2 = 12

5. (a) Compare the following security services in context to mobile device:
(i) Cryptographic security
(ii) LDAP security
(iii) RAS security
(iv) Media player control security.

(b) Discuss different types of worm**.**

(c) Suggest some measures to prevent Vishing attack.

4 + 4 + 4 = 12

Group – D

6. (a) What are the steps to prevent DDoS attack? Differentiate between Strong, Weak and Random Passwords.

   (b) What is Permanent Denial of Service (PDoS) attack? State the preventive measures of DoS attack.

(4 + 2) + (2 + 4) = 12

7. (a) What is Blind SQL Injection attack? Differentiate between Trojan Horse and Backdoor. State the preventive measures from Trojan Horse and Backdoor.

   (b) State any three guidelines applicable to password policies to be implemented in organization.

   (c) What is Buffer Overflow attack? Can you suggest mechanism to prevent it?

(2 + 2 + 2) + 3 + (1 + 2) = 12

Group – E

8. (a) Explain different techniques of Phishing.

   (b) Discuss different types of Human based Techniques of Identity Theft.

6 + 6 =12

9. (a) State the preventive measures from being a victim of Phishing.

   (b) Discuss any four tools to protect online identity.

   (c) Explain any four tools for Digital Forensic Analysis.

4 + 4 + 4 = 12