B.TECH/IT/7TH SEM/INFO 4142/2018
CYBER LAW & 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 any 5 (five) from Group B to E, taking at least one 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) .....hat hacker discloses information about security holes in public.
(a)White (b) Black (c) Grey (d) Brown.

(ii) Method in which phisher identifies prospective victims in advance and conveys false information to entice them for disclosing personal and financial data is known as
(a) rod and reel (b) lobsterpot
(c) gillnet (d) dragnet.

(iii) Three Ps of cybercrime are
(a) phishing, pharming and privacy
(b) phishing, pharming and phreaking
(c) phishing, pharming and phoraging
(d) none of these.

(iv) In.....identity theft victim's life is compromised.
(a) synthetic (b) business (c) child (d) identity cloning.

(v) ..... is used for Bluetooth hacking
(a) blue Scanner (b) blue Sniff (c) bluesnarfer (d) all of these.

(vi) ..... is a example of cybercrime against property.
(a) Logic bomb (b) Cyberterrorism
(c) Password sniffing (d) Internet time theft.

(vii) ..... is a program that automatically dials phone numbers with a motive of hacking.
(a) War dialer (b) Cracking
(c) Phreaking (d) Hacking.

(viii) ..... is the oldest type of DoS attack that uses invalid ICMP packets.
(a) Ping of death attack (b) Nuke
(c) Teardrop attack (d) Flood attack.

(ix) Tools used to launch DoS attack are
(a) Trinoo (b) Targa (c) Crazy Pinger (d) Both b and c.

(x) What is the name of the virus that changes its viral signature whenever it spreads through the system?
(a) Cracker (b) Polymorphic virus
(c)Trojan horses (d) Stealth virus

Group – B

2. (a) Differentiate between black hat hacker, white hat hacker, brown hat hacker and grey hat hacker.
(b) Explain any six passive attack tools used in cybercrime.
6 + 6 = 12

3. (a) State the phases involved in planning cybercrime.
(b) How does cyberstalking work? (Explain all steps in detail)
(c) State different types of cybercriminals with examples.
3 + 4 + 5 = 12

Group – C

4.(a) What is Keylogger? Differentiate between software and hardware Keylogger.
(b) What is Smishing? Suggest some suitable tips to protect from Smishing attack.
(2 + 4) + (2 + 4) = 12

5.(a) Discuss about different types of attacks on mobile phones.
(b) What is Vishing attack? How does it work? Suggest some techniques to prevent Vishing attack.
6 + (2 + 2 + 2) = 12

Group – D

6.(a) What is SQL injection? Explain the steps in SQL injection attack.
(b) Differentiate between strong, weak and random passwords.
(c) What is buffer overflow attack?
(d) Differentiate between Trojan Horse and Backdoor.
(1 + 4) + 3 + 2 + 2=12

7.(a) What is Permanent Denial of Service (PDoS) attack? State any four of the preventive measures for DDoS attack.
(b) Discuss the functions of Backdoor.
(c) What is anonymizer? State the purposes of proxy server.
(2 + 4) +3 +(1 + 2) = 12

Group – E

8.(a) Differentiate between Phishing and Spambots. Explain the methods of Phishing.

(b) State and discuss the steps of digital forensic investigation.

(2 + 4) + 6 = 12

9.(a) Explain the different types of identity theft in detail.

(b) State the risks associated with geotagging and preventive measures for geotagging. Explain any five tools for digital forensic analysis.

4 + 3 + 5 = 12