CYBERSECURITY
(IOT2104)

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 malware is designed to replicate itself and spread to other computers?
(a) Trojan (b) Virus
(c) Worm (d) Spyware

(ii) The Cyber Kill Chain model is used to
(a) Identify and classify various types of malware
(b) Outline the stages of a cyber-attack from initial compromise to data exfiltration
(c) Encrypt sensitive data for secure transmission
(d) Develop cybersecurity policies and compliance measures

(iii) Which cybersecurity principle is concerned with ensuring that data is accurate and trustworthy?
(a) Confidentiality (b) Integrity
(c) Availability (d) Non-repudiation

(iv) Which component of the CIA triad is most impacted by a ransomware attack?
(a) Confidentiality (b) Integrity
(c) Availability (d) Authentication

(v) Which of the following is an example of multi-factor authentication?
(a) Username and password (b) Password and security question
(c) Password and biometric factor (d) Password and PIN

(vi) What is the primary difference between reconnaissance and surveillance?
(a) Reconnaissance involves ongoing monitoring, while surveillance is a one-time check.
(b) Reconnaissance is often a preemptive activity, while surveillance is continuous.
(c) Surveillance is typically done by human agents, while reconnaissance uses technology.
(d) There is no significant difference; the terms are interchangeable.

(vii) Which tool would you use to resolve a domain name into its corresponding IP address?
(a) whois (b) Harvester
(c) Host (d) Netcraft

(viii) What is footprinting in the context of reconnaissance?
(a) The process of removing malware from a system
(b) The initial stage of gathering information to map out a target's network
(c) The final stage of a penetration test where a report is generated
(d) The process of exploiting a vulnerability in a system

(ix) Which type of proxy server is used to provide anonymity by hiding the client's IP address?
(a) Forward Proxy (b) Reverse Proxy
(c) Transparent Proxy (d) Anonymous Proxy

(x) After monitoring a security incident response process, what step is taken in the optimization phase?
(a) Training employees on new security protocols
(b) Rewriting the incident response plan
(c) Implementing a new security control
(d) Developing the plan for the first time

Fill in the blanks with the correct word

(xi) In the context of cyber warfare, the technique used to disrupt or damage an opponent's information systems is _____

(xii) Hash functions and checksums help ensure _____

(xiii) _____ is a scan that avoids detection by not completing the TCP handshake

(xiv) An attack where an attacker manipulates people into divulging confidential information is called _____

(xv) A _____ model is used to identify, assess, and prioritize potential threats to a system

Group - B

2. (a) Discuss the major types of cyber-attacks. *[(CO1)(Understand/LOCQ)]*
(b) Define Section 43 and Section 65 under the Information Technology Act of India. *[(CO2)(Remember/LOCQ)]*
(c) Differentiate between cyber threats and threat actors. *[(CO3)(Analyse/IOCQ)]*
6 + 4 + 2 = 12

3. (a) Explain the term 'social engineering'. How can it affect cyber security? *[(CO1/CO3)(Understand/HOCQ)]*
(b) Identifies the role of the Information Technology Act in cyber security. *[(CO2)(Remember/LOCQ)]*
(c) Why does a debate exist among cyber security experts as to what kind of activity constitutes cyber warfare? *[(CO3)(Understand/IOCQ)]*
(3 + 2) + 5 + 2 = 12

Group - C

4. (a) 'The incident response lifecycle is crucial for cyber security' – Explain. *[(CO5)(Understand/HOCQ)]*
   (b) Discuss a lifecycle which is a systematic process that organizations use to manage and respond to cybersecurity incidents. *[(CO5)(Understand/LOCQ)]*
   (c) Differentiate between DoS and Man-in-the-Middle attacks. *[(CO3)(Analyse/LOCQ)]*

4 + 6 + 2 = 12

5. (a) Discuss the role of authentication, authorization, and accounting (AAA) in access control provide examples. *[(CO5)(Understand/LOCQ)]*
   (b) What are the major components of a cybersecurity governance model? How do they influence policy-making and risk management? *[(CO2)(Understand/LOCQ)]*

6 + 6 = 12

Group - D

6. (a) Describe key components and techniques involved in passive information gathering. *[(CO4)(Understand/LOCQ)]*
   (b) How can reconnaissance lead to threat and risk in an organisation? *[(CO1/CO4)(Understand/IOCQ)]*
   (c) How can active and passive reconnaissance be differentiated with respect to timing and visibility? *[(CO4)(Analyse/HOCQ)]*

6 + 4 + 2 = 12

7. (a) Why are ping sweeps used in cyber security? *[(CO4)(Understand/LOCQ)]*
   (b) Describe some important flags of nmap command. *[(CO4)(Remember/LOCQ)]*
   (c) How can OS fingerprinting techniques lead to a cyber-threat? *[(CO3/CO4)(Analyse/HOCQ)]*

4 + 6 + 2 = 12

Group - E

8. (a) Discuss the benefits of Virtual Private Network. *[(CO6)(Remember/LOCQ)]*
   (b) Describe the basics of internet security. *[(CO1/CO6)(Understand/LOCQ)]*
   (c) Explain two access control models. *[(CO5)(Understand/IOCQ)]*

4 + 6 + 2 = 12

9. (a) What is Business Process Management (BPM)? How does it relate to cybersecurity and risk management in an organization? *[(CO6)(Understand/LOCQ)]*
   (b) Describe the Information Technology Infrastructure Library (ITIL). Highlight its key processes and explain its relevance to cybersecurity. *[(CO6)(Understand/LOCQ)]*

6 + 6 = 12

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	76.04	10.42	13.54