

Roll No.

BCA-E501(DE1)

B. C. A. (Fifth Semester) EXAMINATION, 2023-24

CYBER SECURITY

Time : 2 $\frac{1}{2}$ Hours

Maximum Marks : 60

Note : Attempt all questions.

Section—A

1. Multiple choice type questions : 1 each
 - (i) A can be a hardware device or a software program that filters all the packets of data that comes through a network, the internet, etc. (CO3, BL-1)
 - (a) Firewall
 - (b) Antivirus
 - (c) Malware
 - (d) Cookies

P. T. O.

(ii) Which of the following malware types does not clone or replicate itself through infection ?

(CO3, BL-1)

- (a) Viruses
- (b) Worms
- (c) Trojans
- (d) Rootkits

(iii) Which of these methods is used to check the validity of a message ?

(CO2, BL-1)

- (a) Digital signature
- (b) Protocol
- (c) Message Digest
- (d) Decryption algorithm

(iv) The most important step in system hacking is :

(CO2, BL-2)

- (a) Cracking passwords
- (b) Covering tracks
- (c) Information gathering
- (d) None of the above

(v) Pick one of the following methods for hiding information inside a picture :

(CO2, BL-2)

- (a) Image Rendering
- (b) Steganography
- (c) Rootkits
- (d) Bitmapping

(vi) Which of the following statements is true for the firewall ? (CO3, BL-2)

- (a) It is a barrier created to stop files from hurting the company.
- (b) It is a tool put in place at a business's perimeter to stop uninvited physical entrance.
- (c) It is a device placed at an organisation's perimeter to prevent unwanted access.
- (d) All of the above

(vii) What is used for encrypting data at the network level ? (CO2, BL-3)

- (a) IPSec
- (b) S/MIME
- (c) SMTP
- (d) HTTPS

(viii) Cyber security is..... (CO1, BL-1)

- (a) Cyber Security provides security against malware
- (b) Cyber Security protects a system from cyber attacks
- (c) Cyber Security provides security against cyber-terrorists
- (d) All of the Above

(ix) An attempt to steal, spy, damage or destroy computer systems, networks, or their associated information : (CO1, BL-1)

- (a) Cryptography
- (b) Digital hacking
- (c) Cyber-attack
- (d) Computer security

(x) is a code injecting method used for attacking the database of a system/website.

(CO2, BL-1)

- (a) XML Injection
- (b) HTML injection
- (c) SQL Injection
- (d) Malicious code injection

(xi) Lack of access control policy is a/an

(CO1, BL-2)

- (a) Bug
- (b) Attack
- (c) Threat
- (d) Vulnerability

- (xii) is a violent act done using the Internet, which either threatens any technology user or leads to loss of life or otherwise harms anyone in order to accomplish political gain. (CO1, BL-2)
- (a) Cyber-attack
 - (b) Cyber-warfare
 - (c) Cyber-terrorism
 - (d) Cyber campaign
2. Attempt any *four* of the following : 3 each
- (a) Enlist various challenges and constraints associated with internet governance of cyber security. (CO1, BL-2)
 - (b) Describe the purpose of Denial of Service (DoS) filters. (CO2, BL-2)
 - (c) Emphasize the distinctions between SOAP and REST in web services. (CO3, BL-4)
 - (d) Identify and explain common vulnerabilities associated with SSL/TLS protocols. (CO2, BL-4)
 - (e) Describe key exchange mechanisms involved in the SSL/TLS handshake to ensure secure communication ? (CO3, BL-3)

Section—B

3. Attempt any *two* of the following : 6 each

- (a) Explore the impact of cybercrime on individuals, businesses, and governments, taking into consideration financial losses, privacy breaches, and legal ramifications. (CO1, BL-3)
- (b) Explain the steps involved in encryption and decryption of Pretty Good Privacy (PGP) secure email communication. (CO2, BL-3)
- (c) Uttaranchal technical university is looking to enhance the security of its network infrastructure. The organization has decided to implement packet filtering as part of its overall security strategy. The network includes internal servers, client workstations, and a connection to the internet.

As a cyber-security expert suggest the filtering criteria and packet filtering configuration techniques. (CO3, BL-5)

4. Attempt any *two* of the following : 6 each

- (a) Discuss the reasons behind the need for an international convention on cyberspace, emphasizing the global nature of cyber threats

and analyse specific incidents or trends illustrating the limitations of a purely national approach to cyber security. (CO1, BL-4)

- (b) Describe the weak authentication and its implications for cyber security and what strategies can be employed to strengthen authentication mechanisms and prevent unauthorized access ? (CO2, BL-4)
 - (c) Discuss the role of digital certificates in S/MIME for identity verification and which information is included in S/MIME digital certificate.
- (CO3, BL-4)

5. Attempt any *two* of the following : 6 each

- (a) Explain the role of network-based intrusion detection systems in identifying potential threats in various scenarios as well as discuss the advantages and challenges of network-based intrusion detection. (CO2, BL-2)
- (b) A company wants to establish a secure communication channel between its servers using the RSA algorithm. The company selects two prime numbers as 61 and 53. The public key is

generated with $e = 17$. Compute the corresponding private key and perform the encryption and decryption for the message “42”.

(CO3, BL-6)

- (c) Distinguishing between hardware and software-based key loggers, and list the software based key-logger modes of operation (kernel-level and user-level). (CO1, BL-4)