(ii) How many valid hosts are available in the subnet?

(iii) Find the network address.

(iv) Find the broadcast address.

(v) Find the range of valid host IP addresses.

7. Write short notes on **(any three)** : (5×3)

(i) Firewalls

(ii) PCI-DSS

(iii) PKI

(iv) DMZ

[This question paper contains 8 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 1850 **L**

Unique Paper Code : 2343012007

Name of the Paper : Network Security

Name of the Course : **B.Sc. (H) Computer Science**

Semester : IV

Duration : 3 Hours Maximum Marks : 90

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. The paper has **two** sections. **Section A** is compulsory.
3. Attempt any **four** questions from **Section B**.
4. Parts of a question must be answered together.

Section – A (Compulsory)

1. (a) The AES encryption consists of N rounds, what is the key length in bytes for (3)

(i) 10 rounds

(ii) 12 rounds

(iii) 14 rounds

(b) Identify the class of the following IP addresses:

(i) 10.25.14.8

(ii) 172.16.5.4

(iii) 192.168.1.10 (3)

(c) Encrypt the message "Cyber Security" using Caesar Cipher with key = 5. (3)

(d) How misuse-detection is different from anomaly-detection? (3)

(e) What is primary image and working image in forensics evidence collection? (3)

(f) A university stores student records, examination results, and fee details on its central server. One day, a hacker gains unauthorized access and changes the marks of several students. During investigation, the IT team also found that the website remained unavailable for two days because of a cyberattack. Identify three security breaches for event occurred. (3)

(iv) Software that is secretly or surreptitiously installed into an information system to gather information.

(v) Program that is installed on a system to launch attacks on other machines.

5. (a) Explain with the help of a diagram SSH Protocol Stack. (5)

(b) What do you mean by security policy? How system specific security policy is different from organization security policy? (5)

(c) What do you mean by Multifactor Authentication? Explain. (5)

6. (a) Explain Role Based Access Control Model. (5)

(b) Mobile devices need additional and specialized protection measures. Explain any five major security threats for mobile devices. (5)

(c) A company is assigned the IP address: (5)

192.168.10.0/26:

(i) Find the subnet mask.

4. (a) Using RSA algorithm, encrypt the message M = 7 using the following values: p = 3, q = 11, public key exponent e = 7. Find

(i) n

(ii) *Euler Totient Function,* $\phi(n)$

(iii) Public key

(iv) Private key

(v) Ciphertext C (5)

(b) During forensic investigation, the expert needs to collect volatile data. Identify five types of volatile data that can be contained /seized during evidence collection? (5)

(c) Identify the type of malware: (5)

(i) A computer program that can copy itself and infect a computer without permission or knowledge of the user.

(ii) A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

(iii) A set of tools used by an attacker after gaining root-level access.

(g) Define a VPN. What are the two protocols that a VPN use for (i) System authentication (ii) User Authentication? (3)

(h) How passive attacks are different from active attacks with reference to network security? Give examples. (3)

(i) Give port numbers for the following protocols :

(i) FTP

(ii) HTTP

(iii) HTTPS (3)

(j) Define the following terms:

(i) Honeypots

(ii) Honeynets

(iii) Honey-Clients (3)

Section B

2. (a) A cybercriminal targets users of an online banking portal. The bank stored password of users in hash form in a database. The attacker obtains usernames and hashed passwords from leaked databases and uses automated scripts to try

thousands of password combinations. Several user accounts are compromised as the attacker could identify passwords for many users. (5)

(i) Identify the type of password attack occurred in online banking portal

(ii) How this attack can be prevented?

(iii) Explain with the help of diagram Lamporte One Time Password.

(b) Define Patch Management. What is agent-based and agent-less approach of centralized patch management? (5)

(c) Identify the type of Intrusion Detection System for the following : (5)

(i) A company wants to monitor all incoming and outgoing network traffic for suspicious activities.

(ii) A bank needs to detect unauthorized file modifications on a single server.

(iii) A university wants to monitor login failures and malware activity on laboratory computers.

(iv) An e-commerce company installs monitoring software on individual employee systems to track suspicious processes.

(v) A cybersecurity team wants to detect Distributed Denial of Service (DDoS) attacks across the network.

3. (a) Define RFID Tag. Write any four uses of RFID tag. (5)

(b) Illustrate using a diagram and explain the five elements of Malware Defense. (5)

(c) A software company noticed unusual activity on its network. Several employee systems became slow, and important files were automatically encrypted with a ransom note demanding payment. The IT security team immediately disconnected infected systems from the network, restored data from backups, and started investigating the source of the attack.

What are the processes and steps that IT Security team will follow to manage the incident? (5)