**Professional Course Examination, May 2023**

( 6th Semester )

**BACHELOR OF COMPUTER APPLICATIONS**

( Computer Networking–II )

*Full Marks* : 75

*Time* : 3 hours

*The figures in the margin indicate full marks for the questions*

( PART : A—OBJECTIVE )

( *Marks* : 25 )

SECTION—I

( *Marks* : 15 )

**A.** Tick (✓) the correct answer in the brackets provided :                    1×10=10

1. A ـــــــ is an extension of an enterprise's private intranet across a public network such as the internet, creating a secure private connection.

   *(a)* VNP          (     )

   *(b)* VPN          (     )

   *(c)* VSN          (     )

   *(d)* VSPN          (     )

2. Which of the following is the type of firewall?

   (a) Packet filtering firewall     (   )

   (b) Dual homed gateway firewall     (   )

   (c) Screen host firewall     (   )

   (d) All of the above     (   )

3. _____ is to protect data and passwords.

   (a) Encryption     (   )

   (b) Authentication     (   )

   (c) Authorization     (   )

   (d) Non-repudiation     (   )

4. Which of the following is not the external security threats?

   (a) Front-door threats     (   )

   (b) Back-door threats     (   )

   (c) Underground threats     (   )

   (d) Denial of service (DoS)     (   )

5. Phishing is a form of

   (a) spamming     (   )

   (b) identity theft     (   )

   (c) impersonation     (   )

   (d) scanning     (   )

6. Sniffing is used to perform _____ fingerprinting.

   (a) passive stack        (   )

   (b) active stack         (   )

   (c) passive banner grabbing        (   )

   (d) scanned        (   )

7. What is the most important activity in computer network system hacking?

   (a) Information gathering        (   )

   (b) Cracking passwords        (   )

   (c) Escalating privileges        (   )

   (d) Covering tracks        (   )

8. How is IP address spoofing detected?

   (a) Installing and configuring an IDS that can read the IP header        (   )

   (b) Comparing the TTL values of the actual and spoofed addresses        (   )

   (c) Implementing a firewall to the network        (   )

   (d) Identify all TCP sessions that are initiated but does not complete successfully        (   )

9. What is the purpose of a denial of service attack?

   (a) Exploit a weakness in the TCP/IP stack        (   )

   (b) To execute a Trojan on a system        (   )

   (c) To overload a system so it is no longer operational        (   )

   (d) To shutdown services by turning them off        (   )

10. What type of symmetric key algorithm using a streaming cipher is used to encrypt information?

    *(a)* DES      ( )

    *(b)* RC4      ( )

    *(c)* SHA      ( )

    *(d)* MD5      ( )

**B.** State whether the following statements are *True (T)* or *False (F)* by putting a Tick (✓) mark :              1×5=5

1. Traditional cipher is symmetric key cryptography.

    (    *T*    /    *F*    )

2. Active threats involve attempts by an attacker to obtain information relating to communication.

    (    *T*    /    *F*    )

3. A denial of service attack takes place when the availability to a resource is intentionally blocked or degraded by an attacker.

    (    *T*    /    *F*    )

4. Software firewall is also sometimes called personal firewall.

    (    *T*    /    *F*    )

5. Message authentication does not ensure that the message has been sent by a genuine identity.

    (    *T*    /    *F*    )

SECTION—II

( *Marks* : 10 )

**C.** Answer any *five* of the following questions :                2×5=10

1. What is worm and how can it be prevented?

2. Differentiate between plain text and cipher text.

3. What is the role played by authentication in cryptography?

4. Distinguish between packet-filter firewall and proxy firewall.

5. What are IKE and VPN?

6. What are firewall analysis tools?

7. Mention any wireless security tools

## ( PART : B—DESCRIPTIVE )

( *Marks* : 50 )

**1.** *(a)* Explain the following network security attacks. Mention how to take preventive measurement :                10

*(i)* Trojan horses

*(ii)* Brute force

*(iii)* Man-in-the-middle

*(iv)* Mail bombing

**OR**

*(b)* Explain with suitable demonstration how cybercriminal stole information using phishing and social engineering.

**2.** *(a)* Describe RSA algorithm and estimate the encryption and decryption values for the RSA algorithm parameters.     10

<div align="center"><b>OR</b></div>

*(b)* Write short notes on symmetric-key cryptography and asymetric-key cryptography.

**3.** *(a)* What are the types of attack addressed by message authentication? Explain the two levels of functionality that comprise a message authentication.     10

<div align="center"><b>OR</b></div>

*(b)* Write short notes on the following internet security :

    *(i)* Network layer security

    *(ii)* Application layer security

**4.** *(a)* Explain IP security protocols (SSL/TLS) in detail.     10

<div align="center"><b>OR</b></div>

*(b)* How does PGP provide authentication and confidentiality for email services and for file transfer applications? Draw the block diagram and explain the components.

**5.** *(a)* Explain intrusion detection prevention system (IDPS). What are port scanners and firewall analysis tools in IDPS?     10

<div align="center"><b>OR</b></div>

*(b)* Define the following security threats and mention how to prevent network system from their attacks :

    *(i)* Packet sniffers

    *(ii)* Malicious virus

<div align="center">★ ★ ★</div>