No. of Printed Pages : **2**

Sl. No.

B5.3 - R4 : NETWORK MANAGEMENT AND INFORMATION SECURITY

NOTE :

1. **Answer question 1 and any FOUR questions from 2 to 7.**
2. **Parts of the same question should be answered together and in the same sequence.**

Time : 3 Hours **Total Marks : 100**

1. (a) Explain why an organization would want to use all of the following information security controls: firewalls, intrusion prevention systems, intrusion detection systems and a CIRT.

(b) What is the difference between authentication and authorization ?

(c) Differentiate between Dynamic analysis, black box security testing and static analysis & code review in mobile application security testing.

(d) Discuss various types of firewalls with example.

(e) Discuss the important uses of cryptography.

(f) Describe how to perform risk assessment and explain security controls, state 3 types of Functional Security Controls.

(g) List and explain 5 ways to harden your Network security.

(7x4)

2. (a) Explain OSI model.

(b) How Address Resolution Protocol (ARP) works ? Discuss important terms of ARP.

(c) What is ping ? How to get the ping value of any site corresponding to your server.

(6+6+6)

3. Explain how the following items individually and collectively affect the overall level of security provided by using a password as an authentication credential.

(a) Length and Complexity requirements (which types of characters are required to be used: numbers, alphabetic, case-sensitivity of alphabetic, special symbols like $ or !)

(b) Maximum password age (how often password must be changed) and Minimum password age (how long a password must be used before it can be changed)

(c) Maintenance of password history (how many prior passwords does system remember to prevent reselection of the same password when required to change passwords) and Time frame during which account lockout threshold is applied (i.e., if lockout threshold is five failed login attempts, time frame is whether those 5 failures must occur within 15 minutes, 1 hour, 1 day, etc.) **(6+6+6)**

4. Discuss each of these three attacks and explain in detail how each attack actually works. Also, describe suggested controls for reducing the risks if these attacks will be successful.

(a) Buffer overflows

(b) SQL injection

(c) Cross-site scripting

(6+6+6)

5. Answer the following.

(a) The concept of computational complexity has superseded the notion of covertime as a measure of the security of a cryptosystem. Explain how computational complexity theory provides the theoretical basis for the design of modern scalable cryptosystems.

(b) Describe how a one-way hash function may be used for message authentication.

(c) Explain briefly the concepts: one-way function, one-way hash function, trapdoor one-way function.

(6+6+6)

6. Answer the following.

(a) What are three methods that could have been used to infect a laptop with malware ?

(b) How could phishing take place at an organization ?

(c) What is meant by the term 'brute force attack' ?

(6+6+6)

7. Answer the following.

(a) In an RSA cryptosystem, a participant 'A' uses two prime numbers p = 13 and q =17 to generate her public and private keys. If the public key of A is 35. Then the private key of A is :

(b) Briefly explain Elliptic curve cryptography with its point addition and doubling computational steps.

(9+9)

- o 0 o -