

Roll No.

BCA-10 (Bachelor of Computer Application)

Sixth Semester, Examination-2014

BCA-604

Networking & System Security

Time Allowed : Three Hours

Maximum Marks : 60

Note : The paper is divided into three sections A, B and C. Notes for each section are given in the section itself.

Section - A

(Long answer type Questions)

**Note : Answer any 2 Questions. Each question carries 15 marks.
(2×15=30)**

1. (a) What are the key principles of the security? Explain with example.
(b) Distinguish between vulnerability and threat.
2. What is network security? Explain different types of attack in network.
3. (a) Describe different mechanisms for user authentication.
(b) Discuss Computer Intrusion with suitable examples.
4. Write short notes on following :
 - a. Kerbores
 - b. PKI
 - c. Intrusion Detection Systems (IDS)

Section - B

(Short answer type Questions)

**Note : Answer any 4 questions. Each question carries 5 marks.
(4×5=20)**

1. Explain digital signature in brief.
2. What is VPN? Discuss network applications of VPN.
3. Discuss Biometric based authentication.
4. Give a general structure of IPSec Authentication header.
5. What is risk assessment and mitigation?
6. Define following :
 - a. IPS products
 - b. Worms
7. Define virus and describe the virus spreading mechanism.
8. What is server security ?

Section - C

(Objective type Questions)

**Note : Answer all questions. Each question carries 1 Marks.
(10×1=10)**

1. Firewalls:
 - a. monitors traffic crossing network perimeters
 - b. imposes restrictions according to security policy
 - c. protect enterprise networks from unauthorized access
 - d. All of the above

2. AAA services stand for:
 - a. authentication, authorization, and accounting
 - b. audit, authorization, and accounting
 - c. authentication, automatic, and accounting
 - d. None of the above
3. QoS stands for:
 - a. Quality of Scale b. Quality of Service
 - c. Quality of Scale d. Quantitative Scope
4. VPN:
 - a. reduce cost. b. improve connectivity
 - c. maintain security d. All of the above
5. IPsec can be implemented in:
 - a. host-to-host transport mode
 - b. network tunneling mode
 - c. both a and b
 - d. none of the above
6. A public key infrastructure (PKI) is a set of _____ needed to create, manage, distribute, use, store, and revoke digital certificates
 - a. hardware
 - b. hardware, and software
 - c. hardware, software, and people
 - d. hardware, software, people, policies, and procedures

7. Which of the following is a good computer security practice?
- a. Authenticate Network Users
 - b. Back up Critical Information
 - c. Using firewall
 - d. All of the above
8. A strong password:
- a. does not contain your user name, real name, or company name.
 - b. can be your name.
 - c. a complete word and doesn't contain any other characters such as numbers and symbols.
 - d. never needs to change.
9. Boot sector viruse targets:
- a. boot sector/Master Boot Record (MBR)
 - b. Microsoft Word
 - c. RAM
 - d. None of the above
10. Common biometric schemes include:
- a. Voice recognition
 - b. Fingerprints
 - c. Face scanning and recognition
 - d. All of the above