COMPUTER NETWORK SECURITY

ASSIGNMENT

Answer ALL Questions

Question One (30 marks)

a. Define the following terminologies:
   i. Security attack. (1 mark)
   ii. Security service. (1 mark)
   iii. Security attack. (1 mark)
b. Differentiate between white hat hackers, grey hat hackers, and black hat hackers by describing them. (3 marks)
c. List three basic rules to follow when shaping policy. (3 marks)
d. Briefly describe the three degrees of freedom provided by IPSec. (3 marks)
e. Describe two common reasons for applying a digital signature to communications. (4 marks)
f. Describe three recommended courses of action to undertake should you discover your system is under attack. (3 marks)
g. List three pros of a reasonably effective intrusion detection system. (3 marks)
h. List three critical functions provided by Virtual Private Networks. (3 marks)
i. Describe three limitations of firewalls. (3 marks)
j. Briefly explain rule-based ethics. (2 marks)

Question Two (20 marks)

a. List and describe the roles of the supporting organizations of computer security. (8 marks)
b. Describe the major controls of computer security, citing an example in each instance. (12 marks)

Question Three (20 marks)

a. Define the following terminologies:
   i. Policy (1 mark)
   ii. Standard (1 mark)
   iii. Practices, procedures and guidelines (1 mark)
b. Hence, using a diagram and appropriate explanations describe how the above terminologies relate to each other. (5 marks)
c. Describe how the following systems work, paying attention to the dimensions of security each provides and any special features/capabilities of each:
   i. Pretty Good Privacy (PGP). (4 marks)
   ii. IPSec. (4 marks)
   iii. Secure Shell. (4 marks)

Question Four (20 marks)

a. Describe three types of cryptography. (12 marks)
b. Describe two types of firewalls. (8 marks)