USN | | | | | | | | | | |

12SFC102/SFC12

First Semester M.Tech. Degree Examination, Dec. 2013/Jan. 2014
Pragmatics of Information Security

Time: 3 hrs. Max. Marks:100

Note: ***Answer any FIVE full questions.***

1 a. Propose a defense (an existing technology/ a method which can be used) to following attacks. Explain in 1-2 lines how will the defense detect and stop the attack.
   i) SYN attack DDOS attack.
   ii) A Malware with not known signature, which eats up a resource (Memory, CPU etc) on a Host
   iii) Bruteforce Password cracking attack
   iv) A Scanning attack (attacker probing a target network by sending different kinds of packets)
   v) Password capture for remote user authentication. **(10 Marks)**

   b. Briefly describe four types of Firewalls (what level, what do they filter, specific strengths, weakness etc). **(10 Marks)**

2 a. What mechanism do you use to verify a public key of a user? Describe the steps as how a certificate is generated and verified in brief (diagrammatically/ 7-8 lines). Which standard is most commonly in use to facilitate the same? Give example of 5 fields in certificate. **(10 Marks)**

   b. Explain Encryption and Decryption using Cipher Feedback Mode (CFB) form of processing (diagrammatically with few words). When do you use Cipher Feedback Mode form of processing? CFB mode is used to cover which security deficiency in ECB mode processing? **(10 Marks)**

3 a. How is a MAC different to a Hash Code? Describe the HMAC algorithm in brief. Bring out any 4 prima design objectives or advantages of HMAC algorithm? **(10 Marks)**

   b. Describe Fiestal Cipher structure (Diagrammatically with some explanation.). Bring out the five parameters which define a specific symmetric block Cipher. **(10 Marks)**

4 a. Describe in detail (what information is sent, why and use of information) for following communication in Kerberos
   i) User to Authentication Server (AS) and AS to User
   ii) User to Ticket Granting Server (TGS) and TGS to User. **(10 Marks)**

   b. Explain the 3 logical components of IDS in brief. (3-4 lines each) **(07 Marks)**

   c. What is the primary difference between IPS and IDS with an Example? **(03 Marks)**

5 a. Explain Role Based Access Control (RBAC) through Matrix representation (Matrix representation with minimal explanation to explain the matrix). **(06 Marks)**

   b. Describe three ways in which a message authentication can be achieved. Which method is most optimal according to you and why? Give an example scenario where you would recommend using each of the approach and why? **(08 Marks)**

   c. Why do we use salt value mechanism in Unix password scheme? Explain the scheme in brief. **(06 Marks)**

6 a. Explain in brief (1-2 line each) four functions supported by SMIME? What would be the steps followed to send a message in Signed and Enveloped data type? What is the difference between Signed and Clear signed data? **(10 Marks)**

b. What is a worm? How does a network worm propagate itself? Describe four possible countermeasure approaches to contain a worm attack (2-3 lines each). **(10 Marks)**

7 a. Describe what a stack frame would look like when a function P calls a function Q with some parameters and local variables. With this, explain how a stack buffer overflow attack is implemented? **(10 Marks)**

b. In IPSEC protocol what is a Security Association (SA)? What are the parameters which identify an SA uniquely? **(05 Marks)**

c. Bring out an 3 ways a virus tries to hide itself from an antivirus detection. **(05 Marks)**

8 a. Describe SSL protocol stack with brief description of each of the protocol. **(10 Marks)**

b. Describe 3 possible attacks on a packet filtering firewall. Explain how would you counteract these attacks? **(10 Marks)**