Roll No. | | | | | | | | | | | | |

Total No. of Pages : 02

Total No. of Questions : 08

M.Tech.(IT)(2015 & Onwards)/(CSE Engg.) (2015 to 2017) (Sem.–1)

INFORMATION SECURITY

Subject Code : MTCS-103

Paper ID : [72631]

Time : 3 Hrs. Max. Marks : 100

INSTRUCTION TO CANDIDATES :

1. **Attempt any FIVE questions out of EIGHT questions.**
2. **Each question carries TWENTY marks.**

1. a. Explain the relationship between Policies, Guidelines, and Procedures. What are the goals of each, who is responsible for each?

   b. Explain how you can perform OS fingerprinting? How is it useful for performing intrusive attacks?

2. Answer briefly :

   a. What is the major limitation of traditional substitution ciphers? How do the modern block ciphers address it?

   b. What is the major limitation of the traditional one-time pad? How do the modern stream ciphers address it?

   c. Is AES a Feistel cipher? Why/Why not?

3. Alice and Bob are very good friends and don't mind sharing the same RSA modulus n. Of course, to have their own different private keys, they use different public exponents, $e1$, $e2$. Moreover $e1$ and $e2$ are relatively prime. A common friend Charlie sends a message x to both, encrypting it with their respective RSA keys, $y1 = xe1 \bmod n$, $y2 = xe2 \bmod n$. Show how Eve, who knows the public keys of Alice and Bob and observes the ciphertexts $y1$ and $y2$, can find out the message x.

4. a. What are the generic steps involved in anomaly detection? Explain what are the main issues.

   b. Define and compare packet filtering and application level firewalls. What are their pros and cons?

5. To design a secure network of an organization, I recommend use of following network devices :

   a. Routers

   b. Network IDS

   c. HIDS

   d. VPN

   e. Deploying DMZ architecture

   State where will it be best to deploy the device and how will it contribute to secure network design.

6. a. State 03 technical methods using which interception can be done in a network?

   b. What solutions would you like to propose to prevent DOS attack in a network of 500 machines primarily due to Flooding?

   c. How is a DOS attack different from a DDOS attack?

7. State of the following argument is True or False and justify your response dearly :

   a. An advantage of behavioural-based techniques for detection is that they are well-suited for preventing attempted attacks from succeeding.

   b. It is fundamentally harder to create a detector with a low rate of false positives than a low rate of false negatives.

   c. Signature-based techniques have the appealing property that it's easy to share the signatures between different parties.

8. If a worm uses random scanning of IP addresses to probe for new victims, then the time required for it to infect a target population increases linearly with the size of the population.