

TE (IT) Sem VI  
Information & Network Security  
11/5/2013

ws-Con-2013-1

Con. 7257-13.

GS-9810

(3 Hours)

[Total Marks : 100]

- N.B 1) Question No.1 is Compulsory.  
2) Attempt any **Four** out of remaining

- Q.1. (a) Consider online examination system, where students can login and answer questions online. For this system identify vulnerability, threat and attacks (05)  
(b) Describe and explain the Denial of Service (DOS) attack in a network. What controls are required to avoid it. (05)  
(c) Describe any two malicious program flaws (05)  
(d) Explain covert channels and why they are a security threat. (05)
- Q.2. (a) Explain "Buffer Overflow" and "Incomplete Mediation" flaws in a program and how they can be used to attack the system. (10)  
(b) Describe in detail how Antivirus programs work. (10)
- Q.3. (a) What are the measures provided by an Operating System for security (10)  
(b) List and describe the flaws present in the TCP protocol that can lead to security breaks. (10)
- Q.4. (a) Describe the working of the RSA algorithm. Illustrate the working using the values of  $p = 5$  and  $q = 7$ . (10)  
(b) Explain the concept of a Digital Signature". Describe a public key method to create and check digital signatures. (10)
- Q.5. (a) How are hash functions useful for information Security. Explain any one Hash Security algorithm. (10)  
(b) Explain the role of a firewall in securing a network. Describe different types of firewalls (10)
- Q.6 (a) Explain the working of Kerberos in detail (10)  
(b) Describe different types of Intrusion Detection Systems (IDS) (10)
- Q.7. Write a detailed note on the following topics ;  
1. Secure Sockets Layer (SSL) (10)  
2. DES Algorithm (10)
-