AMRITSAR GROUP OF COLLEGES NAAC Grade "A" 3rd Cycle | Autonomous College under Autonomous Category | (Since 2014) Conferred by UGC	B.Tech (6th Sem) – 3 ASSIGNMENT-2 Information Security AGCS-21604A	DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Question Sets

Set 1: Question Number 1, 2, 11, 13, 21, 23, 32, 37,43
Set 2: Question Number 5, 6, 14, 17, 24, 26, 33, 39, 46
Set 3: Question Number 8, 9, 19,20, 28, 29, 36, 42, 48

Allocation of Question Sets to students

Set	Uni. Roll No.
1	2233709,2233719,2233721,2233727,2233730,2233731,2233732,2233734,2233735,2233737, 2233738,2233740,2233741,2233742,2233745,2239631,2333486,2333487, 2131902
2	2233708,2233711, 2233714,2233718,2233720,2233723,2233724,2233725,2233733,2233744, 2234225,
3	2233712,2233713,2233716,2233722,2233728,2233729,2233736,2233739,2233743,2233746,223 3748,2234221,2239633

Section – A (2 Marks each)

Q.No.	Question	CO
1.	Describe the basic components of the Kerberos system.	CO-4
2.	What are the potential weaknesses or vulnerabilities of Kerberos?	
3.	Explain the role of the Key Distribution Center (KDC) in Kerberos authentication.	
4.	What is an X.509 certificate, and what is its primary use in computer security?	
5.	What is IPsec, and what problem does it address in computer networking?	
6.	Explain the purpose and role of the public key within an X.509 certificate. How is it used in practice?	
7.	Discuss the security features of Kerberos.	
8.	What are some advantages and limitations of IPsec in terms of network security and performance?	
9.	What is the Encapsulating Security Payload (ESP) protocol in IPsec, and how does it provide confidentiality and integrity?	
10.	Differentiate Transport and Tunnel mode in IPSEC.	
11.	Describe cross-site scripting.	CO-5
12.	List various types of common web security threats.	
13.	Differentiate between authentication and authorization in web security?	
14.	What is session management and why is it important for web security applications?	
15.	In which layer does SSL works?	
16.	Briefly define the purpose of transport layer security.	
17.	Discuss the requirements in Secure electronic transaction.	
18.	Why security association is required to transmit the data between server and client	
19.	Discuss the handshaking with respect to SSL.	
20.	What is the purpose of web security?	
21.	What is intruder ?List the 3 classes of intruder	
22.	Define virus. Specify the types of viruses.	

23.	What is application level gateway?	CO-6
24.	List the design goals of firewalls	
25.	What is worm,zombie and Honey pot?	
26.	What is trusted software?	
27.	Define: Malicious software	
28.	What is firewall and list its characteristics?Write four general techniques of firewall	
29.	State the difference between threats and attack.	
30.	What do you mean by Trojan horse?	

Section – B (4 Marks each)

Q.No.	Question	CO
31.	Discuss the concept of a Certification Authority (CA) in the context of X.509 certificates. What role does a CA play in certificate issuance and validation?	CO-4
32.	Describe the structure of an X.509 certificate. What information does it contain?	
33.	Explain the concept of Security Associations (SAs) in IPsec. Why are SAs important for secure communication?	
34.	Explain the process of how Kerberos authentication works.	
35.	Explain the two main modes of operation in IPsec. How do they differ?	
36.	Describe the purpose and function of the Authentication Header (AH) protocol in IPsec.	
37.	Describe in detail web security requirements.	CO-5
38.	Explain the change cipher Spec protocol.	
39.	What is SSL/TLS certificate? How does TLS works.	
40.	What is Secure electronic transaction protocol? Explain its components.	
41.	Explain the process of Secure electronic transaction with an example?	
42.	Differentiate between TLS and SSL.	
43.	Explain the technical details of firewall and describe any three types of firewall with neat diagram.	CO-6
44.	Describe signature based intrusion detection system.	
45.	Describe Rule based intrusion detection system.	
46.	Explain briefly about trusted systems.	
47.	Enumerate counter measure for viruses and worms.	
48.	Justify Intrusion provides early warning of an intrusion so that action can be taken to prevent or minimize damage?	