

Department of Computer Engineering

Academic Year: 2021-22(EVEN)

<u>QUESTION BANK</u>	
Subject : Cryptography and System Security	Semester: VI

1. State one vulnerability in TCP/IP and ICMP protocol. Explain how the vulnerability may be exploited leading to an attack?
2. What kind of reconnaissance information is obtained during port scanning process?
3. What is IDS? How it differs from firewall?
4. How cross site scripting attack occurs? Explain with suitable example.
5. Compare between worm and virus
6. What are the different ways in which an attacker can mount a DOS attack on a system?
7. Explain ARP spoofing and DNS spoofing with neat diagram.
8. What are different types of firewall?
9. Why would you use IPSec instead of SSL? How are they different?
10. List various types of software vulnerabilities. How these vulnerabilities are exploited to launch buffer overflow attack.
11. Explain handshake protocol in SSL.
12. In PGP, Explain how Alice and Bob exchange secret Key for encrypting the message
13. How is security achieved in Transport and Tunnel modes of IPSEC?
14. Explain the role of AH and ESP.
15. How does PGP achieve confidentiality and authentication in emails?
16. What are the different components of Intrusion Detection System?
17. Compare signature based IDS to anomaly based IDS.
18. What is Denial of Service attack?
19. What are the different ways in which an attacker can mount a DOS attack on a system?
20. Explain SQL injection Attack with example ?
21. Explain Buffer overflow Attack with example?
22. Explain how IP spoofing attacks works .
23. Explain Types of DoS attacks
24. What is Nonce?what is significance of Nonce in entity authentication