Assignment 5

Deadline : first day after Leave

1. Define authentication system. Illustrate the need of mutual authentication over one-way authentication with an example.
2. Define SSL protocol. Mention the services provided by PGP.
3. We say that SSL/TLS is not really a single protocol, but a stack of protocols. Explain. What are the different protocols in the SSL/TLS stack?
4. There are two aspects to a secure communication link: authentication and confidentiality. How do you understand these two words? Does the Kerberos protocol give us both?
5. What is Needam Schroder protocol? How it works? What is its drawback?
6. Explain about working Mechanism of Kerberos(with steps and figure). How it resolves the problem of Needam Schroder protocol?
7. Define malware. Classify and explain them.
8. Explain types of trojans.
9. Explain types of virus.
10. Differentiate between worm and Virus.
11. What is PGP? Explain five services of PGP.
12. What is PEP? explain. Compare PEP and PGP.
13. What is the difference between a connection and a session in SSL/TLS? Can a session include multiple connections? Explain the notions “connection state” and “session sate” in SSL/TLS. What security features apply to each?
14. What is a certificate and why are certificates needed in public key cryptography?
15. Explain the structure of X.509 certificate.
16. Describe the concept behind public key infrastructure. Explain components of PKI with appropriate diagram.
17. What are the possible phases that a virus can go through, during its life cycle?
18. How rabbits and bacterium can be malicious to a secure system?
19. Define authentication system. How hardware-based challenge response systems can be used as authentication approach.
20. How many layers are in the TCP/IP protocol suite for internet communications? Name the layers. Name some of the protocols in each layer.
21. How Trojan horse differs from viruses? Discuss about possible types of Trojan horses.
22. What is a certificate and why are certificates needed in public key cryptography.
23. Describe the concept behind public key infrastructure
24. What are the possible phases that a virus can go through, during its life cycle?
25. In which situation using Kerberos system seem to be good? Describe what the major components of Kerberos system are.
26. What is the role of the SSL Record Protocol in SSL/TLS? Explain.
27. Define PKI Trust Model.
28. What are the services provided by IPSec?
29. What is meant by intrusion detection system? Differentiate IPS and IDS.
30. What is meant by intruder? Explain its types.
31. Write the four SSL Protocols. How do they work? Explain with Diagram.