Code : 061814

B.Tech 8th Semester Exam., 2020

NETWORK SECURITY

Time : 3 hours *Full Marks* : 70

Instructions :

(i) The marks are indicated in the right-hand margin.

*(ii) There are **NINE** questions in this paper.*

*(iii) Attempt **FIVE** questions in all.*

*(iv) Question No. **1** is compulsory.*

1. Choose the correct answer of any *seven* of the following : 2×7=14

(a) _____ is concerned with preventing the unauthorized disclosure of sensitive information.

(i) Confidentiality

(ii) Integrity

(iii) Availability

(iv) None of the above

(b) S1—The KDC knows the secret keys of all clients and servers on the network.

S2—The KDC initially exchanges information with the client and server by using these secret keys.

S3—Kerberos authenticates a client to a requested service on a server through the TGS and by issuing temporary symmetric session keys for the communications between the client and the KDC, the server and the KDC, and the client and the server.

S4—Communication then takes place between the client and the server by using those temporary session keys.

In the given statements (S1, S2, S3, S4) which statement is true for Kerberos principle?

(i) Only S1

(ii) S1 and S2

(iii) S1, S2 and S3

(iv) All statements are true

(c) PAP (Password Authentication Protocol) is vulnerable to

(i) ID and password guessing

(ii) Replay attack

(iii) Both *(i)* and *(ii)*

(iv) None of the above

(d) is a file transfer client program, which enables file transfer between the Windows workstation and an FTP server.

(i) PGP

(ii) sFTP

(iii) True for both PGP and sFTP

(iv) None of the above

(e) Which of the following is the type of software that has self-replicating software that causes damage to files and sytem?

(i) Viruses

(ii) Trojan horses

(iii) Bots

(iv) Worms

(f) DoS attacks exist for which part of the OSI protocol stack?

(i) Application and Presentation

(ii) Session and Transport

(iii) Network and Data Link

(iv) All of the above

(g) Which protocol is used to provide secure connections across the Internet?

(i) ARP

(ii) HTTPS

(iii) NTP

(iv) POP3

(h) TELNET is a general-purpose

(i) client/server application program

(ii) database-server application program

(iii) client-end application program

(iv) server-end application program

(i) Which of the following explains cookies nature?

(i) Non-volatile

(ii) Volatile

(iii) Intransient

(iv) Transient

(j) Which of the following protocols can be used to manage WLAN infrastructure devices?

(i) SSH

(ii) SNMP

(iii) Telnet

(iv) All of the above

2. (a) What are the security mechanisms provided by OSI security architecture? Discuss in detail. 7

(b) Define formal process. What are the entities involved in the Defense-in-Depth protection methodology? 7

3. How business continuity and disaster planning mechanism handle effects of major system and network failures? Illustrate with an example scenario. 14

4. What are the security requirements for remote access? How is authentication different from authorization? Illustrate with an example. 14

5. What are the attacks associated with Windows operating system? Discuss in detail. 14

6. Explain the working procedure of Web browser. Ilustrate the three popular attacks on Web browser. Also, suggest the appropriate security mechanism for those popular attacks. 14

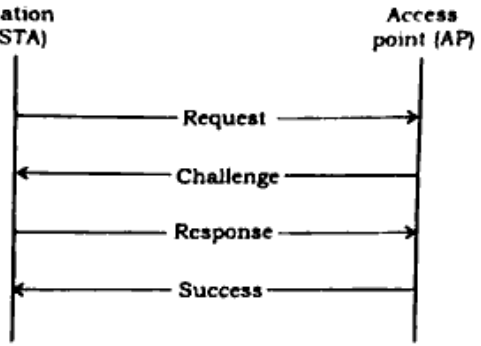
7. What is the role of domain name system (DNS) in network communication? How can cache poisoning attack be launched against DNS server? Discuss the DNS design strategies for securing DNS server. 14

8. Prior to the introduction of IEEE 802·11i, the security scheme for IEEE 802·11 was wired equivalent privacy (WEP). WEP assumed all devices in the network share a secret key. The purpose of the authentication scenario is for the STA to prove that it possesses the secret key. Authentication proceeds as shown in given figure (Page–7). The STA sends a message to the AP requesting authentication. The AP issues a challenge, which is sequence of 128 random bytes sent as plaintext. The STA encrypts the challenge with the shared key and returns it to the AP. The AP decrypts the incoming value and compares it to the challenge that it sent. If there is a match, the AP confirms that authentication has succeeded.

(a) What are the benefits of this authentication scheme?

(b) This authentication scheme is incomplete. What is missing and why is this important?

(c) What is a cryptographic weakness of this scheme?



14

9. List the characteristic of good firewall implementation. How is a circuit gateway different from an application gateway? 14

★ ★ ★