UNIT-IV : Transport-level Security

1. Web security is particularly important because the web is widely used for:
a) Only entertainment purposes
b) Commerce, banking, and exchange of sensitive personal information over an inherently insecure network
c) Hardware diagnostics
d) Offline data storage
Answer: b

2. Which of the following is a key web security consideration?
a) Protecting the server, the client, and the data in transit between them
b) Improving page loading speed only
c) Reducing the number of web pages
d) Increasing bandwidth usage
Answer: a

3. SSL (Secure Sockets Layer) operates at which layer of the network architecture?
a) Between the application layer and the transport layer
b) At the physical layer
c) At the data link layer
d) At the network layer only
Answer: a

4. TLS (Transport Layer Security) is essentially:
a) A completely unrelated protocol to SSL
b) The successor/standardized version of SSL with improved security
c) A hardware-based encryption chip
d) A replacement for HTTP entirely
Answer: b

5. The SSL/TLS protocol primarily provides which security services for client-server communication?
a) Confidentiality, integrity, and authentication b) Only compression
c) Only routing d) Only error correction
Answer: a

6. The SSL/TLS handshake protocol is mainly used to:
a) Compress the data being sent
b) Negotiate cipher suites, authenticate parties, and establish a shared session key
c) Permanently store session data
d) Route packets to the correct destination
Answer: b

7. In the SSL/TLS handshake, the server typically authenticates itself to the client using a:

a) Symmetric session key

b) Digital certificate (containing its public key), signed by a trusted CA

c) Plain text password

d) Hash of the client's IP address

Answer: b

8. After the SSL/TLS handshake is complete, actual application data is protected using: a) Only asymmetric encryption for all data

b) A symmetric session key derived during the handshake, for fast bulk encryption

c) No encryption at all

d) Steganography

Answer: b

9. The SSL/TLS Record Protocol is responsible for:

a) Negotiating the cipher suite only

b) Fragmenting, compressing, and applying MAC/encryption to application data

c) Generating the server's certificate

d) Resolving domain names

Answer: b

10. HTTPS is essentially:

a) HTTP combined with SSL/TLS to provide a secure communication channel

b) A completely separate protocol unrelated to HTTP

c) HTTP without any encryption

d) A file transfer protocol only

Answer: a

11. HTTPS typically uses which default port?

a) 80 b) 21 c) 443 d) 25

Answer: c

12. One of the main reasons HTTPS is preferred over HTTP for sensitive transactions is that it:

a) Loads pages faster regardless of encryption

b) Encrypts data in transit, preventing eavesdropping and tampering

c) Removes the need for a web server

d) Eliminates the need for a domain name

Answer: b

13. Secure Shell (SSH) is primarily used for:

a) Secure remote login and command execution over an insecure network

b) Sending unencrypted emails

c) Browsing static web pages

d) Compressing video files

Answer: a

14. SSH provides which of the following security features?

a) Encryption, integrity, and strong authentication of the remote session

b) Only file compression

c) Only IP address masking

d) Only DNS resolution

Answer: a

15. The SSH protocol architecture typically consists of which of the following layered components?

a) Transport layer protocol, user authentication protocol, and connection protocol

b) Only a single monolithic protocol

c) HTTP and FTP combined

d) Only a compression layer

Answer: a

16. The SSH Transport Layer Protocol is mainly responsible for:

a) User password verification only

b) Server authentication, key exchange, encryption, and integrity protection of the session

c) File transfer only

d) Domain name resolution

Answer: b

17. SSH can also be used to securely tunnel/forward other protocols, a feature commonly known as:

a) Port forwarding (tunneling) b) Domain forwarding

c) Packet sniffing d) Traffic shaping

Answer: a

Unit 8: Wireless Network Security

18. Wireless networks are generally considered more vulnerable to security threats than wired networks mainly because:

a) Data travels over open radio frequencies, making interception easier

b) Wireless signals cannot be encrypted

c) Wireless networks don't use any protocols

d) Wireless devices have unlimited range

Answer: a

19. Which of the following is a unique security threat associated specifically with wireless networks?

a) SQL injection

b) Rogue access points and eavesdropping on radio signals

c) Buffer overflow in desktop applications

d) Cross-site scripting

Answer: b

20. Mobile device security is particularly challenging because mobile devices:

a) Never connect to any network

b) Are easily lost or stolen, and often connect to untrusted networks

c) Cannot store sensitive data

d) Always have unlimited processing power

Answer: b

21. Which of the following is a common mobile device security measure?

a) Disabling all security software

b) Device encryption, screen locks/biometrics, and remote wipe capability

c) Removing all installed applications

d) Permanently disabling updates

Answer: b

22. IEEE 802.11 is the standard primarily associated with:

a) Wired Ethernet networks

b) Wireless Local Area Networks (WLANs)

c) Cellular mobile networks

d) Fiber optic communication

Answer: b

23. In an IEEE 802.11 wireless LAN, the device that connects wireless clients to a wired network is called the:

a) Router only

b) Access Point (AP)

c) Switch

d) Modem

Answer: b

24. The original security protocol defined for IEEE 802.11 (now considered weak/broken) was:

a) WPA2

b) WEP (Wired Equivalent Privacy)

c) 802.11i
d) AES-GCM
Answer: b

25. WEP's security weaknesses were primarily due to:
a) Use of a strong, unbreakable cipher
b) Weak key management, short/static keys, and flaws in its use of the RC4 stream cipher
c) Excessive encryption overhead d) Use of asymmetric cryptography only
Answer: b
26. IEEE 802.11i was developed specifically to:
a) Increase wireless network speed only
b) Address the security weaknesses of WEP and define robust security for wireless LANs
c) Replace Ethernet cabling standards d) Define new physical layer modulation only
Answer: b
27. The security framework introduced by IEEE 802.11i is commonly implemented in products as:
a) WEP b) WPA2 (Wi-Fi Protected Access 2) c) HTTP d) SSH
Answer: b
28. IEEE 802.11i mandates the use of which encryption algorithm for robust security (CCMP)?
a) RC4 b) DES c) AES d) Blowfish
Answer: c
29. In IEEE 802.11i, the four-way handshake is primarily used to:
a) Establish and confirm fresh session keys (pairwise transient keys) between the client and access point
b) Transfer files between devices c) Resolve IP address conflicts
d) Compress wireless signals
Answer: a
30. CCMP, used in IEEE 802.11i, stands for:
a) Cipher Block Chaining Message Authentication Code Protocol
b) Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
c) Certificate Chain Management Protocol
d) Common Cryptographic Message Protocol
Answer: b
31. IEEE 802.11i defines two main phases of operation: discovery and:
a) Compression b) Authentication and key management
c) Routing d) Modulation
Answer: b
32. In the IEEE 802.11i architecture, the entity that often acts as the authentication server is based on the:
a) RC4 algorithm

b) IEEE 802.1X framework, often using a RADIUS server

c) Diffie-Hellman exchange only

d) X.509 certificate revocation list

Answer: b