**Chapter 17:** **Transport-Level Security**

**TRUE OR FALSE**

T F 1. ISSl/TLS includes protocol mechanisms to enable two TCP users to

determine the security mechanisms and services they will use.

T F 2. Unlike traditional publishing environments, the Internet is three-

way and vulnerable to attacks on the Web servers.

T F 3. Sessions are used to avoid the expensive negotiation of new

security parameters for each connection that shares security

parameters.

T F 4. Microsoft Explorer originated SSL.

T F 5. The World Wide Web is fundamentally a client/server application

running over the Internet and TCP/IP intranets.

T F 6. One way to classify Web security threats is in terms of the location

of the threat: Web server, Web browser, and network traffic

between browser and server.

T F 7. The encryption of the compressed message plus the MAC must

increase the content length by more than 1024 bytes.

T F 8. The Change Cipher Spec Protocol is one of the three SSL-specific

protocols that use the SSL Record Protocol.

T F 9. The SSL Record Protocol is used before any application data is

transmitted.

T F 10. The first element of the CipherSuite parameter is the key exchange

method.

T F 11. The certificate message is required for any agreed on key

exchange method except fixed Diffie-Hellman.

T F 12. Phase 3 completes the setting up of a secure connection of the

Handshake Protocol.

T F 13. The shared master secret is a one-time 48-byte value generated

for a session by means of secure key exchange.

T F 14. The TLS Record Format is the same as that of the SSL Record

Format.

T F 15. Server authentication occurs at the transport layer, based on the

server possessing a public/private key pair.

**MULTIPLE CHOICE**

1. The The SSL Internet standard version is called \_\_\_\_\_\_\_\_\_ .

A)  SSH   B)  HTTP

C)  SLP   D)  TLS

2. The most complex part of SSL is the \_\_\_\_\_\_\_\_\_\_ .

A)  SSL Record Protocol   B)  Handshake Protocol

C)  Change Cipher Spec Protocol   D)  Alert Protocol

3. \_\_\_\_\_\_\_\_\_ attacks include impersonating another user, altering messages in transit

between client and server and altering information on a Web site.

A)  Active   B)  Passive

C)  Shell   D)  Psuedo

4. The symmetric encryption key for data encrypted by the client and decrypted by

the server is a \_\_\_\_\_\_\_\_\_ .

A)  server write key   B)  client write key

C)  sequence key   D)  master key

5. \_\_\_\_\_\_\_\_\_ provides secure, remote logon and other secure client/server facilities.

A)  SLP   B)  HTTPS

C)  TLS   D)  SSH

6. An SSL session is an association between a client and a server and is created by

the \_\_\_\_\_\_\_\_\_\_\_ .

A)  Handshake Protocol   B)  user

C)  Spec Protocol   D)  administrator

7. An arbitrary byte sequence chosen by the server to identify an active or

resumable session state is a \_\_\_\_\_\_\_\_\_ .

A)  peer certificate   B)  session identifier

C)  compression   D)  cipher spec

8. The \_\_\_\_\_\_\_\_\_ is used to convey SSL-related alerts to the peer entity.

A)  Change Cipher Spec Protocol   B)  Alert Protocol

C)  SSL Record Protocol   D)  Handshake Protocol

9. With each element of the list defining both a key exchange algorithm and a

CipherSpec, the list that contains the combination of cryptographic algorithms

supported by the client in decreasing order of preference is the \_\_\_\_\_\_\_\_\_\_ .

A)  CipherSuite   B)  Random

C)  Session ID   D)  Version

10. Phase \_\_\_\_\_\_\_\_\_ of the Handshake Protocol establishes security capabilities.

A)  4   B)  1

C)  2   D)  3

11. The \_\_\_\_\_\_\_\_\_\_ approach is vulnerable to man-in-the-middle attacks.

A)  Anonymous Diffie-Hellman   B)  Fixed Diffie-Hellman

C)  Fortezza   D)  Ephemeral Diffie-Hellman

12. The final message in phase 2, and one that is always required, is the \_\_\_\_\_\_\_\_\_\_\_

message, which is sent by the server to indicate the end of the server hello and

associated messages.

A)  server\_done   B)  no\_certificate

C)  goodbye   D)  finished

13. Defined as a Proposed Internet Standard in RFC 2246, \_\_\_\_\_\_\_\_\_ is an IETF

standardization initiative whose goal is to produce an Internet standard version

of SSL.

A)  SSH   B)  CCSP

C)  TLS   D)  SHA-1

14. A Pseudorandom Function takes as input:

A)  a secret value   B)  an identifying label

C)  a seed value   D)  all of the above

15.  \_\_\_\_\_\_\_\_\_ is organized as three protocols that typically run on top of TCP for

secure network communications and are designed to be relatively simple and

inexpensive to implement.

A)  SSL   B)  SSH

C)  TLS   D)  SSI

**SHORT ANSWER**

1. \_\_\_\_\_\_\_\_\_\_ provides security services between Transport Layer Protocol and

applications that use TCP.

1. The \_\_\_\_\_\_\_\_\_ Protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm along with cryptographic keys to be used to protect data sent in an SSL Record.
2. \_\_\_\_\_\_\_\_\_ attacks include eavesdropping on network traffic between browser and server and gaining access to information on a Web site that is supposed to be restricted.
3. \_\_\_\_\_\_\_\_\_\_ provides confidentiality using symmetric encryption and message integrity using a message authentication code.
4. The \_\_\_\_\_\_\_\_\_ takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment.
5. \_\_\_\_\_\_\_\_\_\_ refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server.
6. Two important SSL concepts are the SSL session and the SSL \_\_\_\_\_\_\_\_\_ .
7. Three standardized schemes that are becoming increasingly important as part of Web commerce and that focus on security at the transport layer are: SSL/TLS, HTTPS, and \_\_\_\_\_\_\_\_\_.
8. Three higher-layer protocols defined as part of SSL and used in the management of SSL exchanges are: The Handshake Protocol, The Change Cipher Spec Protocol, and the \_\_\_\_\_\_\_\_\_\_ .
9. \_\_\_\_\_\_\_\_\_ would appear to be the most secure of the three Diffie-Hellman options because it results in a temporary, authenticated key.
10. A signature is created by taking the hash of a message and encrypting it with the sender's \_\_\_\_\_\_\_\_\_ .
11. The handshake is complete and the client and server may begin to exchange application layer data after the server sends its finished message in phase \_\_\_\_\_\_\_\_\_ of the Handshake Protocol.
12. \_\_\_\_\_\_\_\_\_ require a client write MAC secret, a server write MAC secret, a client write key, a server write key, a client write IV, and a server write IV, which are generated from the master secret in that order.
13. TLS makes use of a pseudorandom function referred to as \_\_\_\_\_\_\_\_\_\_ to expand secrets into blocks of data for purposes of key generation or validation.
14. \_\_\_\_\_\_\_\_\_\_ allows the client to set up a "hijacker" process that will intercept selected application-level traffic and redirect it from an unsecured TCP connection to a secure SSH tunnel.