

# MULTIPLE CHOICE QUESTIONS IN DATA COMMUNICATIONS AND NETWORKING

## A Complete Chapter Quiz

### Security in the Internet: IPSec, SSL/TLS, PGP, VPN, and Firewalls

Compilation of all the quizzes (MCQs) for each and every chapters in the book of Data Communications and Networking 4th Edition by Behrouz A. Forouzan.

1. \_\_\_\_\_ operates in the transport mode or the tunnel mode.

- A) **IPSec**
- B) SSL
- C) PGP
- D) none of the above

2. IKE creates SAs for \_\_\_\_\_.

- A) SSL
- B) PGP
- C) **IPSec**
- D) VP

3. \_\_\_\_\_ provides either authentication or encryption, or both, for packets at the IP level.

- A) AH
- B) **ESP**
- C) PGP
- D) SSL

4. One security protocol for the e-mail system is \_\_\_\_\_.

- A) IPSec
- B) SSL
- C) **PGP**
- D) none of the above

5. Typically, \_\_\_\_\_ can receive application data from any application layer protocol, but the protocol is normally HTTP.

- A) SSL
- B) TLS
- C) either (a) or (b)
- D) **both (a) and (b)**

6. IKE is a complex protocol based on \_\_\_\_\_ other protocols.

- A) two
- B) **three**
- C) four
- D) five

7. IPSec defines two protocols: \_\_\_\_\_ and \_\_\_\_\_.

- A) AH; SSL
- B) PGP; ESP
- C) **AH; ESP**
- D) all of the above

8. In the \_\_\_\_\_ mode, IPSec protects information delivered from the transport layer to the network layer.

- A) **transport**
- B) tunnel
- C) either (a) or (b)
- D) neither (a) nor (b)

9. \_\_\_\_\_ is the protocol designed to create security associations, both inbound and outbound.

- A) SA
- B) CA
- C) KDC
- D) **IKE**

10. A \_\_\_\_\_ network is used inside an organization.

- A) **private**
- B) public
- C) semi-private
- D) semi-public

11. SSL provides \_\_\_\_\_.

- A) message integrity
- B) confidentiality
- C) compression
- D) **all of the above**

12. The Internet authorities have reserved addresses for \_\_\_\_\_.

- A) intranets
- B) internets
- C) extranets
- D) **none of the above**

13. An \_\_\_\_\_ is a network that allows authorized access from outside users.

- A) intranet
- B) internet
- C) extranet
- D) none of the above

14. \_\_\_\_\_ is a collection of protocols designed by the IETF (Internet Engineering Task Force) to provide security for a packet at the network level.

- A) IPSec
- B) SSL
- C) PGP
- D) none of the above

15. IKE uses \_\_\_\_\_.

- A) Oakley
- B) SKEME
- C) ISAKMP
- D) all of the above

16. IPSec uses a set of SAs called the \_\_\_\_\_.

- A) SAD
- B) SAB
- C) SADB
- D) none of the above

17. An \_\_\_\_\_ is a private network that uses the Internet model.

- A) intranet
- B) internet
- C) extranet
- D) none of the above

18. \_\_\_\_\_ is actually an IETF version of \_\_\_\_\_.

- A) TLS; TSS
- B) SSL; TLS
- C) TLS; SSL
- D) SSL; SLT

19. In \_\_\_\_\_, there is a single path from the fully trusted authority to any certificate.

- A) X509
- B) PGP
- C) KDC
- D) none of the above

20. The combination of key exchange, hash, and encryption algorithms defines a \_\_\_\_\_ for each SSL session.

- A) list of protocols
- B) cipher suite
- C) list of keys
- D) none of the above

21. A \_\_\_\_\_ provides privacy for LANs that must communicate through the global Internet.

- A) VPP
- B) VNP
- C) VNN
- D) VPN

22. \_\_\_\_\_ uses the idea of certificate trust levels.

- A) X509
- B) PGP
- C) KDC
- D) none of the above

23. IPSec in the \_\_\_\_\_ mode does not protect the IP header.

- A) transport
- B) tunnel
- C) either (a) or (b)
- D) neither (a) nor (b)

24. \_\_\_\_\_ provides privacy, integrity, and authentication in e-mail.

- A) IPSec
- B) SSL
- C) PGP

- D) none of the above
25. In \_\_\_\_\_, there can be multiple paths from fully or partially trusted authorities.
- A) X509
- B) PGP**
- C) KDC
- D) none of the above
26. \_\_\_\_\_ provides authentication at the IP level.
- A) AH**
- B) ESP
- C) PGP
- D) SSL
27. In \_\_\_\_\_, the cryptographic algorithms and secrets are sent with the message.
- A) IPSec
- B) SSL
- C) TLS
- D) PGP**
28. \_\_\_\_\_ is designed to provide security and compression services to data generated from the application layer.
- A) SSL
- B) TLS
- C) either (a) or (b)
- D) both (a) and (b)**
29. \_\_\_\_\_ provide security at the transport layer.
- A) SSL
- B) TLS
- C) either (a) or (b)
- D) both (a) and (b)**
30. The \_\_\_\_\_ mode is normally used when we need host-to-host (end-to-end) protection of data.
- A) transport**

- B) tunnel
- C) either (a) or (b)
- D) neither (a) nor (b)
31. In the \_\_\_\_\_ mode, IPSec protects the whole IP packet, including the original IP header.
- A) transport
- B) tunnel**
- C) either (a) or (b)
- D) neither (a) nor (b)
32. \_\_\_\_\_ was invented by Phil Zimmerman.
- A) IPSec
- B) SSL
- C) PGP**
- D) none of the above
33. A \_\_\_\_\_ layer security protocol provides end-to-end security services for applications.
- A) data link
- B) network
- C) transport**
- D) none of the above
34. In PGP, to exchange e-mail messages, a user needs a ring of \_\_\_\_\_ keys.
- A) secret
- B) public**
- C) either (a) or (b)
- D) both (a) and (b)