1. Pada operasional SSL Record Protocol, terdapat beberapa tahap yang harus diperlakukan terhadap application data. Berikut ini adalah tahap-tahap tersebut, kecuali …

Select one:

a. MAC addressing

b. fragmentation

c. compression

d. encryption

1. Sistem eCommerce tentunya berjalan di atas platform yang harus dikelola keamanannya, salah satu cara dalam menjaga platform security tersebut adalah ..

Select one:

a. Menerapkan otentikasi dan otorisasi

b. Memberlakukan expired password

c. Menghapus database default dari platform database

d. Memastikan password dibaca dari data yang terenkripsi

1. Di bawah ini yang bukan merupakan penanggulangan resiko dari keamanan dalam jejaring media sosial adalah …

Select one:

a. memperhatikan unggahan di media sosial yang dapat mendeskripsikan diri lebih akurat

b. membatasi user lain yang dapat melihat informasi personal

c. memperhatikan fitur koneksi nirkabel yang digunakan media sosial

d. memperhatikan fitur geo-tagging yang digunakan media social

1. Berikut ini yang bukan merupakan komponen kerentanan dalam sebuah sistem eCommerce adalah …

Select one:

a. Network Protocol Risks

b. Client-Server Risks

c. Database Security

d. Platform Security

1. Dua metode yang digunakan untuk mengenkripsi email adalah ..

Select one:

a. L2TP dan PGP

b. S/MIME dan PGP

c. SSH dan PGP

d. PPTP dan PGP

6. Dalam steganografi, media penyembunyian sebelum disisipkannya pesan rahasia disebut …

Select one:

a. stego-media

b. plain-text

c. secret-media

d. cover-object

7. Berikut ini adalah tiga protokol lapisan yang lebih tinggi sebagai bagian dari TLS, kecuali …

Select one:

a. SSL Change Cipher Spec Protocol

b. SSL Warning Protocol

c. SSL Alert Protocol

d. SSL Handshake Protocol

8. Arsitektur dari TLS tersusun atas beberapa “stack”. Di bawah ini yang bukan merupakan “stack” tersebut adalah …

Select one:

a. SSL Alert Protocol

b. SSL Warning Protocol

c. SSL Handshake Protocol

d. SSL Record Protocol

9. Dua metodologi dasar dalam Social Engineering Attack adalah …

Select one:

a. impeachment dan seduction

b. imperceptible dan seduction

c. impersonation dan seduction

d. imperialism dan seduction

10. TLS Connection, sebagai salah satu konsep penting dalam TLS, didefinisikan dalam spesifikasi hubungan … yang bersifat sementara dan setiap koneksi hanya dikaitkan dalam satu sesi.

Select one:

a. client-server

b. decentralized

c. peer-to-peer

11. Bahwa informasi yang dikomunikasikan dan disimpan secara aman dan hanya dapat diakses oleh yang berhak saja adalah merupakan aspek keamanan …

Select one:

a. Integrity

b. Authenticity

c. Confidentiality

d. Availability

12. Kepastian informasi dikirimkan secara menyeluruh, lengkap dan dalam keadaan tidak berubah, dan tidak bisa diubah tanpa seijin pemiliknya termasuk dalam aspek keamanan …

Select one:

a. Integrity

b. Confidentiality

c. Availability

d. Authenticity

13. Aspek keamanan … memastikan bahwa pihak, obyek, dan informasi yang berkomunikasi adalah riil dan tidak palsu.

Select one:

a. Confidentiality

b. Availability

c. Authenticity

d. Integrity

14. Berikut ini adalah dua prinsip utama dalam keamanan database adalah …

Select one:

a. access-control dan availability

b. authorization dan availability

c. authentication dan authorization

d. authentication dan availability

15. Salah satu algoritma yang menerapkan steganografi pada domain spasial adalah …

Select one:

a. DCT

b. DFT

c. LSB

d. DWT

16. SSL Record Protocol menyediakan layanan confidentiality dalam aspek keamanan untuk SSL Connection, dimana SSL Record Protocol tersebut mendefinisikan shared secret key untuk digunakan dalam …

Select one:

a. membentuk Message Authentication Code (gaby)

b. membentuk Media Authentication Code

c. symmetric encryption (shinta)

d. asymmetric encryption

17. Metode fundamental dalam encryption adalah …

Select one:

a. substitution dan transportition

b. subscription dan transposition

c. substitution dan transposition

d. subscription dan transportation

18. Pada jaringan internet, electronic mail (email) bergantung pada tiga protokol utama berikut ini, kecuali …

Select one:

a. Simple Mail Transfer Protocol

b. Mail Transmission Protocol

c. Internet Message Access Protocol

d. Post Office Protocol

19. Salah satu layanan keamanan yang paling banyak digunakan, dan layanan keamanan ini diimplementasikan sebagai sekumpulan protokol yang mengandalkan TCP kemudian selanjutnya menjadi standar Internet RFC4346 adalah …

Select one:

a. Transport Layer Security

b. Transportation Layer Security

c. Transmission Layer Security

d. Transfer Layer Security

20. Perbedaan antara enkripsi simetris dan asimetris terletak pada …

Select one:

a. plain-text

b. receiver

c. key

d. cipher-text

21. Berikut ini adalah jenis atau tipe algoritma dalam cryptography, kecuali …

Select one:

a. Symmetric

b. Huffman

c. Asymmetric

d. Hashing

22. Koneksi HTTP menggunakan port 80 atau 8080 secara default, Sedangkan jika menggunakan koneksi HTTPS, maka digunakan port … yang memanggil SSL.

Select one:

a. 442

b. 21

c. 22

d. 443

23. “Denial of Service attack” (DoS attack), dimana server dikirimkan request palsu yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain, merupakan suatu serangan yang dapat mengganggu aspek keamanan …

Select one:

a. Integrity

b. Availability

c. Confidentiality

d. Authenticity

24. SHA dan Message Digest (MD) termasuk pada tipe algoritma cryptography …

Select one:

a. Huffman

b. Hash­

c. Asymmetric

d. Symmetric

25. Dalam implementasinya, TLS/SSL adalah merupakan protokol keamanan pada Transport Layer. Sedangkan IPSec adalah merupakan protokol keamanan pada …

Select one:

a. Application Layer

b. Network Layer

c. Transmission Layer

d. Physical Layer

26. Algoritma kriptografi yang termasuk dalam Asymmetric Encryption antara lain …

Select one:

a. ECC dan CAST

b. Diffie-Hellman (DH) dan RSA

c. Blowfish dan Twofish

d. DES dan 3DES

27. Tipe atau jenis algoritma cryptography yang merupakan cikal bakal dari digital signature adalah …

Select one:

a. Symmetric

b. Huffman

c. Asymmetric

d. Hash

28. Perbedaan metode Pretty Good Privacy dalam mengenkripsi email dengan metode lainnya adalah pada …

Select one:

a. komunikasi harus memanfaatkan server untuk key management

b. tidak harus menjaga keterbaruan perangkat lunak

c. key management yang dilakukan secara local (yuni)

d. tidak memberikan keamanan yang baik terhadap serangan brute-force

29. HTTPS merupakan kombinasi antara HTTP dengan SSL dalam penerapan komunikasi yang aman antara web browser dengan web server. Saat HTTPS digunakan, salah satu elemen yang mengalami encryption adalah …

Select one:

a. Footer HTTP

b. Session

c. Variable

d. Cookie

30. Terdapat beberapa istilah teknis dalam cara kerja atau metode pengiriman email, yang diantaranya adalah …

Select one:

a. mail user agent, mail transfer agent, mail receiver agent

b. mail user agent, mail transmission agent, mail delivery agent

c. mail user agent, mail transfer agent, mail delivery agent

d. mail sender agent, mail transfer agent, mail delivery agent