



Home > My courses > [Reg] Jaringan Komputer (A,B,C) Gasal 2021-2022 > Chapter 7. Security in Computer Networks > Kuis Chapter 7 - Semua Kelas

**Started on** Wednesday, 15 December 2021, 1:06 PM

**State** Finished

**Completed on** Wednesday, 15 December 2021, 1:56 PM

**Time taken** 50 mins 1 sec

**Marks** 19.00/20.00

**Grade** 95.00 out of 100.00

### Question 1

Correct

Mark 1.00 out of 1.00

Fungsi hash menghasilkan output dengan panjang byte yang fix.

Select one:

- ☒ True ✓
- ☐ False

The correct answer is 'True'.

**Question 2**

Correct

Mark 1.00 out of 1.00

Istilah apa yang digunakan untuk menyatakan kegagalan IDS dalam mendeteksi suatu serangan atau traffic yang ilegal?

Select one:

- ☐ a. False positive
- ☐ b. True positive
- ☐ c. True negative
- ☒ d. False negative ✓

The correct answer is: False negative

**Question 3**

Correct

Mark 1.00 out of 1.00

Jenis serangan apa yang coba dilindungi oleh HMAC?

Select one:

- ☐ a. DDoS
- ☐ b. DoS
- ☒ c. Man-in-the-middle ✓
- ☐ d. Brute force

The correct answer is: Man-in-the-middle

**Question 4**

Correct

Mark 1.00 out of 1.00

Pernyataan mana yang merupakan fitur dari HMAC?

Select one:

- ☐ a. HMAC menggunakan *secret key* yang hanya diketahui pengirim dan dapat mencegah *man-in-the-middle attacks*.
- ☐ b. HMAC didasari oleh fungsi hash RSA.
- ☐ c. HMAC menggunakan protokol seperti SSL atau TLS untuk memberikan *confidentiality* pada layer session.
- ☒ d. HMAC menggunakan secret key untuk verifikasi otentisitas dan integritas pesan, yang kemudian keduanya menjadi input dari fungsi hash. ✓

The correct answer is: HMAC menggunakan secret key untuk verifikasi otentisitas dan integritas pesan, yang kemudian keduanya menjadi input dari fungsi hash.

**Question 5**

Correct

Mark 1.00 out of 1.00

Seorang hacker mengambil alih sesi yang Anda sedang lakukan dengan remote server sehingga Anda tidak memiliki akses ke server tersebut. Jenis serangan apakah ini?

Select one:

- ☒ a. Hijacking ✓
- ☐ b. DDoS
- ☐ c. Spoofing
- ☐ d. Sniffing

The correct answer is: Hijacking

**Question 6**

Incorrect

Mark 0.00 out of 1.00

Algoritma cryptography apa yang digunakan untuk menjamin kerahasiaan data maupun integritas data (dengan mekanisme yang berbeda)?

Select one:

- ☒ a. HMAC ❌
- ☐ b. SHA-1
- ☐ c. RSA
- ☐ d. AES

The correct answer is: RSA

**Question 7**

Correct

Mark 1.00 out of 1.00

Sebuah penjual online membutuhkan suatu layanan *non-repudiation* dari sebuah transaksi. Komponen apa yang digunakan untuk layanan tersebut?

Select one:

- ☐ a. private key si penjual online
- ☐ b. public key si penjual
- ☒ c. digital signature ✔️
- ☐ d. shared secret unik yang hanya diketahui oleh si penjual dan pelanggannya

The correct answer is: digital signature

**Question 8**

Correct

Mark 1.00 out of 1.00

Apa yang menjadi tugas IDS?

Select one:

- ☐ a. untuk menjalankan kebijakan access control berdsarkan isi/konten dari packet.
- ☒ b. mendeteksi pola traffic jahat berdasarkan signature tertentu yang sudah disimpan. ✓
- ☐ c. menyaring traffic berdasarkan informasi di layer aplikasi.
- ☐ d. menyaring traffic berdasarkan rules yang sudah ditentukan dan konteki dari koneksi.

The correct answer is: mendeteksi pola traffic jahat berdasarkan signature tertentu yang sudah disimpan.

**Question 9**

Correct

Mark 1.00 out of 1.00

Kunci apa yang digunakan penerima untuk dekripsi ciphertext jika algoritma asymmetric key digunakan untuk enkripsi data?

Select one:

- ☒ a. private key penerima ✓
- ☐ b. public key penerima
- ☐ c. private key pengirim
- ☐ d. public key pengirim

The correct answer is: private key penerima

**Question 10**

Correct

Mark 1.00 out of 1.00

Intrusion Detection System (IDS) digunakan untuk memblokir sebuah packet yang berisi malware atau yang merupakan bagian dari active attack.

Select one:

- ☐ True
- ☒ False ✓

IDS can only detects intrusion, but it's not able to block or filter the malicious packet

The correct answer is 'False'.

## Question 11

Correct

Mark 7.00 out of 7.00

Tentukan istilah/terminologi paling tepat pada setiap statement berikut:

Mengambil alih kendali dari sebuah komunikasi yang berlangsung sehingga target (baik sender atau receiver) digantikan oleh attacker.

Hijacking



Saat mengirim packet, attacker mengganti source IP atau MAC address pada packet yang dikirim menjadi IP atau MAC address milik target.

Spoofing



Memastikan bahwa hanya pihak yang berwenang dalam komunikasi saja yang dapat membaca atau memahami message.

Confidentiality



Memastikan bahwa informasi atau service dapat diakses oleh user legitimate kapanpun dibutuhkan.

Availability



Cara untuk membuktikan identitas pihak yang ingin terlibat dalam komunikasi.

Authentication



Memastikan bahwa message tidak diubah tanpa terdeteksi, baik message tersebut dalam state *in transit* (dikirim) atau *at rest* (disimpan)

Integrity



Serangan yang dilakukan oleh **banyak** agents yang bertujuan untuk menghabiskan resource yang tersedia pada target (Bandwidth, CPU, RAM, etc).

Distributed Denial of Service



Your answer is correct.

The correct answer is: Mengambil alih kendali dari sebuah komunikasi yang berlangsung sehingga target (baik sender atau receiver) digantikan oleh attacker. → Hijacking, Saat mengirim packet, attacker mengganti source IP atau MAC address pada packet yang dikirim menjadi IP atau MAC address milik target. → Spoofing, Memastikan bahwa hanya pihak yang berwenang dalam komunikasi saja yang dapat membaca atau memahami message. → Confidentiality, Memastikan bahwa informasi atau service dapat diakses oleh user legitimate kapanpun dibutuhkan. → Availability, Cara untuk membuktikan identitas pihak yang ingin terlibat dalam komunikasi. → Authentication, Memastikan bahwa message tidak diubah tanpa terdeteksi, baik message tersebut dalam state *in transit* (dikirim) atau *at rest* (disimpan) → Integrity, Serangan yang dilakukan oleh **banyak** agents yang bertujuan untuk menghabiskan resource yang tersedia pada target (Bandwidth, CPU, RAM, etc). → Distributed Denial of Service

**Question 12**

Correct

Mark 1.00 out of 1.00

Teknologi apa yang memerlukan *trusted third-party* untuk mengeluarkan credential yang berisi informasi identitas pihak tertentu serta public key yang valid?

Select one:

- ☒ a. digital certificates ✓
- ☐ b. hashing algorithms
- ☐ c. symmetric keys
- ☐ d. digital signatures

The correct answer is: digital certificates

**Question 13**

Correct

Mark 1.00 out of 1.00

Seorang admin web server mengatur konfigurasi sehingga komunikasi dengan web server terenkripsi. Aspek information security apakah yang ditangani melalui konfigurasi ini?

Select one:

- ☐ a. availability
- ☐ b. integrity
- ☒ c. confidentiality ✓
- ☐ d. scalability

The correct answer is: confidentiality



**Question 14**

Correct

Mark 1.00 out of 1.00

Apa tujuan dari *reconnaissance attack* pada jaringan komputer?

Select one:

- ☐ a. agar user tidak dapat mengakses sumber daya jaringan
- ☒ b. untuk mengumpulkan informasi terkait jaringan dan sistem yang menjadi target ✓
- ☐ c. untuk mencuri data pada server di jaringan
- ☐ d. untuk mengalihkan traffic data

The correct answer is: untuk mengumpulkan informasi terkait jaringan dan sistem yang menjadi target