



An toàn thông tin_ Nhóm 04CLC

[Nhà của tôi](#) / [Các khoá học của tôi](#) / [INSE330380_22_1_04CLC](#) / [Test 2. Begin 19h, 4/12/2022](#) / [Test 2_Review_all](#)

Câu hỏi 41

Chưa trả lời

Đạt điểm 1,00

Frank rất quan tâm đến các cuộc tấn công vào máy chủ thương mại điện tử của công ty. Ông đặc biệt lo lắng về tấn công SQL Injection. Điều nào sau đây sẽ bảo vệ tốt nhất trước cuộc tấn công cụ thể này?

- ☒ a. Lưu lượng truy cập web được mã hóa
- ☐ b. Firewall
- ☐ c. IDS
- ☐ d. Lọc dữ liệu người dùng nhập vào

[Clear my choice](#)

Câu hỏi 42

Câu trả lời đã được lưu

Đạt điểm 1,00

Giả sử thuật toán RSA đã tạo ra cặp khóa public $(7, 187)$ và private $(23, 187)$. Muốn tạo chữ kí cho message $M=3$ sẽ được tính là?

- ☒ a. 181
- ☐ b. 23
- ☐ c. 137
- ☐ d. 121

$$\begin{aligned} & \text{en} \quad \text{d} \quad \text{n} \\ & 3^{23} \bmod 187 \\ & M^d \bmod n \end{aligned}$$

[Clear my choice](#)

Thời gian còn lại 0:01:49

Câu hỏi 43

Câu trả lời đã được lưu

Đạt điểm 1,00

Tấn công một máy tính bằng cách gửi các gói TCP handshake không đúng thứ tự đến đích (wrong order) xảy ra ở tầng nào?

- ☐ a. Network Interface layer
- ☒ b. Transport layer
- ☐ c. Internet layer
- ☐ d. Application layer

Clear my choice**Câu hỏi 44**

Câu trả lời đã được lưu

Đạt điểm 1,00

Tấn công nào sau đây là tấn công chủ động (active)

- ☒ a. Sniffing
- ☐ b. Scan port
- ☒ c. DoS
- ☐ d. ping

Clear my choice**Câu hỏi 45**

Chưa trả lời

Đạt điểm 1,00

Assume RSA has the public key $(7, 187)$ and private key $(23, 187)$. The ciphertext $C = 3$ will be decrypted to

tạo chỉ ký + decrypt -> private key

- ☐ a. 171
- ☒ b. 181
- ☒ c. 133
- ☐ d. 121

$$3^d \bmod n$$

Clear my choice

Câu hỏi 46

Câu trả lời đã được lưu

Đạt điểm 1,00



Which is the operation in DES function?

- ☒ a. Straight P-box
- ☐ b. Shiftleft
- ☐ c. Mixcolumn
- ☐ d. Compression P-box

Clear my choice**Câu hỏi 47**

Câu trả lời đã được lưu

Đạt điểm 1,00

John muốn thêm luật (rule) vào ACL cho tệp script00.sh để cấp cho student04 quyền đọc và ghi đối với tệp đó. Lệnh nào sau đây được thực hiện?

- ☐ a. getfacl -m u:student04:rw- script00.sh
- ☐ b. setfacl -x u:student04:rw- script00.sh
- ☒ c. setfacl -m u:student04:rw- script00.sh
- ☐ d. getfacl -x u:student04:rw- script00.sh

Clear my choice**Câu hỏi 48**

Câu trả lời đã được lưu

Đạt điểm 1,00

Câu nào sau đây KHÔNG phải là một cơ chế điều khiển truy cập?

- ☐ a. Discretionary Access Control (DAC)
- ☐ b. Attribute Based Access Control (ABAC)
- ☒ c. Subjective Access Control (SAC)
- ☐ d. Mandatory Access Control (MAC)
- ☐ e. Role Based Access Control (RBAC)

Clear my choice

Câu hỏi 49

Câu trả lời đã được lưu

Đạt điểm 1,00

Điều nào sau đây mô tả tốt nhất cơ chế kiểm soát truy cập trong đó các quyết định kiểm soát truy cập dựa trên trách nhiệm của người dùng trong một tổ chức?

- ☒ a. Discretionary Access Control (DAC)
- ☐ b. Subjective Access Control (SAC)
- ☐ c. Mandatory Access Control (MAC)
- ☐ d. Attribute Based Access Control (ABAC)
- ☐ e. Role Based Access Control (RBAC)

[Clear my choice](#)

Câu hỏi 50

Câu trả lời đã được lưu

Đạt điểm 1,00

Given below table for encryption and decryption. Which is the plaintext of cypher = 010?

3 bits
↓

	00	01	10	11
0	011	101	111	100
1	000	010	001	110

Table used for
encryption

3 bits
↓

3 bits
↓

	00	01	10	11
0	100	110	101	000
1	011	001	111	010

Table used for
decryption

3 bits
↓

- ☐ a. 011
- ☐ b. 001
- ☒ c. 101
- ☐ d. 110

cắt - hàng

[Clear my choice](#)

◀ Chapter 12 - Hash - MAC - HMAC - Digital Signature

[Chuyển tới...](#)

[Review - Chapter 1,3,4,5,6 ▶](#)