Test-2 a - Ôn tập an toàn thông tin

An toàn thông tin (Trường Đại học Sư phạm Kỹ Thuật Thành phố Hồ Chí Minh)

An toan thong tin_ Nhom 04CLC

Câu hỏi 1

Câu trả lời đã được lưu

Đạt điểm 1,00

What are components of modern block cipher? (chose 2)

- [ ] a. Feedback function
- [ ] b. Shift register
- [x] c. Exclusive-Or
- [x] d. Straight P-box

Câu hỏi 2

Câu trả lời đã được lưu

Đạt điểm 1,00

Điều gì xảy ra khi máy X sử dụng kỹ thuật ARP spoofing để nghe lén thông tin từ máy Y?

- ( ) a. X giả mạo địa chỉ IP của Y
- ( ) b. Y giả mạo địa chỉ IP của X
- ( ) c. Y giả mạo địa chỉ MAC của X
- (•) d. X giả mạo địa chỉ MAC của Y

Clear my choice

Câu hỏi 3

Câu trả lời đã được lưu

Đạt điểm 1,00

Phương pháp nào sau đây là TỐT NHẤT để giảm hiệu quả của các cuộc tấn công lừa đảo trên mạng?

- a. Quét lỗ hổng cho hệ thống định kỳ
- b. Xác thực 2 yếu tố
- c. Đào tạo nâng cao nhận thức người dùng
- d. Phần mềm chống lừa đảo

Clear my choice

Câu hỏi 4

Câu trả lời đã được lưu

Đạt điểm 1,00

Trong các giao thức dưới đây, giao thức nào cho phép xác thực user khi user gắn thiết bị vào port layer 2?

- a. Radius
- b. 802.3D
- c. 802.3
- d. 802.11X

Clear my choice

Câu hỏi 5

Câu trả lời đã được lưu

Đạt điểm 1,00

Avalanche Effect property proves DES has been to be strong, means:.....

- a. a small change in the ciphertext should create a significant change in the plaintext
- b. a small change in the ciphertext or key should create a significant change in the plaintext
- c. a small change in the plaintext should create a significant change in the ciphertext and key
- d. a small change in the plaintext or key should create a significant change in the ciphertext

Clear my choice

Câu hỏi 6

Câu trả lời đã được lưu

Đạt điểm 1,00

Tấn công DoS/DDoS làm ảnh hưởng đến tiêu chuẩn nào của an toàn thông tin?

- a. Tính bí mật
- b. Tính toàn vẹn
- c. Tính sẵn sàng
- d. Tính xác thực
- e. Tính chống thoái thác

Clear my choice

Câu hỏi 7

Câu trả lời đã được lưu

Đạt điểm 1,00

Tại sao các nhà phát triển phần mềm đính kèm theo các giá trị băm bằng hàm MD5 của các gói cập nhật cho phần mềm cùng với các gói đó để các khách hàng của họ có thể download từ Internet?

- a. Khách hàng có thể yêu cầu các bản cập nhật mới cho phần mềm trong tương lai bằng cách sử dụng giá trị hàm băm đính kèm theo
- b. Khách hàng có thể xác thực tính toàn vẹn và gói cập nhật cho phần mềm sau khi download về
- c. Khách hàng có thể khẳng định tính xác thực của Site mà họ download gói cập nhật về
- d. Khách hàng cần giá trị của hàm băm để có thể kích hoạt được phần mềm mới

Clear my choice

Câu hỏi 8

Câu trả lời đã được lưu

Đạt điểm 1,00

Thời gian còn lại 0:17:17

Trong an toàn thông tin, Ping Sweep được sử dụng để làm gì?

- a. Để xác định các cổng đang mở trên mạng
- b. Để xác định các host đang hoạt động trên mạng
- c. Để xác định vị trí của các host đang hoạt động trên mạng
- d. Để xác định vị trí của các tường lửa trên mạng

Clear my choice

Câu hỏi 9

Câu trả lời đã được lưu

Đạt điểm 1,00

Diffie - Hellman là thuật toán dùng để

- a. Mã hóa khóa
- b. Hash khóa
- c. Tạo khoá
- d. Trao đổi khóa
- e. Giải mã khóa

Clear my choice

Câu hỏi 10

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. Transport layer
- b. Network Interface layer
- c. Network layer
- d. Application layer
- e. Internet layer

Clear my choice

Câu hỏi 11

Câu trả lời đã được lưu

Đạt điểm 1,00

In asymmetric key cryptography (also known as public encryption). Alice needs to decrypt the text Bob sent, what key does Alice need to use?

- a. Bob's Public Key
- b. Bob's Private Key
- c. Alice's Private Key
- d. Alice's Public Key

Clear my choice

Câu hỏi 12

Câu trả lời đã được lưu

Đạt điểm 1,00

Mô hình bảo mật theo chiều sâu (defense in depth) gồm các lớp bảo mật theo thứ tự từ trong ra ngoài là?

Layer 4	LAN security
Layer 7	Policies, procedures, awareness
Layer 1	Data security
Layer 3	Host security
Layer 2	Application security
Layer 5	Perimeter security
Layer 6	Physical security

Câu hỏi 13

Câu trả lời đã được lưu

Đạt điểm 1,00

Which are server involved in the Kerberos protocol? (choose 2)

- [ ] a. Access control server
- [ ] b. Authorization Server
- [x] c. Authentication server
- [x] d. Ticket-granting server

Câu hỏi 14

Câu trả lời đã được lưu

Đạt điểm 1,00

Sắp xếp các thông tin cho đúng về độ dài đầu ra của các thuật toán mã hóa sau

SHA-512	512bits
AES	128bits
DES	64bits
MD5	128bits
3DES	64bits

Câu hỏi 15

Câu trả lời đã được lưu

Đạt điểm 1,00

Một máy chủ Web của một công ty được cấu hình các dịch vụ sau: HTTP, HTTPS, FTP, SMTP. Máy chủ này được đạt trong vùng DMZ. Những cổng nào cần phải mở trên Firewall để cho phép máy người dùng có thể sử dụng dịch vụ trên máy này?

- a. 119, 23, 21, 80, 23
- b. 110, 443, 21, 59, 25
- c. 434, 21, 80, 25, 20
- d. 80, 20, 21, 25, 443

Clear my choice

Câu hỏi 16

Câu trả lời đã được lưu

Đạt điểm 1,00

Assume the RSA has the pubic key (7,187) and the private key (23,187). Which is the signature of message M= 3 ?

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

Clear my choice

Câu hỏi 17

Câu trả lời đã được lưu

Đạt điểm 1,00

Công cụ nào dùng để quét cổng của máy tính

- a. telnet
- b. ping
- c. nmap
- d. nslookup
- e. tracert

Clear my choice

Câu hỏi 18

Câu trả lời đã được lưu

Đạt điểm 1,00

Để nâng cao việc phát triển các giải pháp an toàn cho một hệ thống CNTT, người ta tập trung đầu tư vào 3 vấn đề chính là?

- [x] a. Con người
- [x] b. Công nghệ
- [ ] c. Đội ngũ chuyên gia bảo mật
- [ ] d. Đào tạo nâng cao nhận thức
- [x] e. Quy trình
- [ ] f. Tăng chi phí đầu tư cho bảo mật

Câu hỏi 19

Câu trả lời đã được lưu

Đạt điểm 1,00

Hai dạng mã độc nào sau đây sống độc lập?

- [ ] a. Rootkit
- [x] b. Worm
- [ ] c. Trojan
- [x] d. Zombie
- [ ] e. Logic boom

Câu hỏi 20

Câu trả lời đã được lưu

Đạt điểm 1,00

Trong mã hóa bất đối xứng (còn gọi là mã hóa hóa công khai). Alice cần **mã hóa** văn bản để gửi cho Bob thì Alice cần dùng khóa gì?

- ( ) a. Khóa Private của Alice
- ( ) b. Khóa Public của Alice
- ( ) c. Khóa Private của Bob
- (•) d. Khóa Public của Bob

Clear my choice

Câu hỏi 21

Câu trả lời đã được lưu

Đạt điểm 1,00

Given 2 primes: p=13, q=19, which of the values is a valid of "e" in RSA?

- a. 21
- b. 47
- c. 39
- d. 27

Clear my choice

Câu hỏi 22

Câu trả lời đã được lưu

Đạt điểm 1,00

Which is the objective of hash function?

- a. Availability
- b. Confidentiality
- c. Integrity
- d. Authentication

Clear my choice

Câu hỏi 23

Câu trả lời đã được lưu

Đạt điểm 1,00

Kiểu tấn công nào sau đây **không** phải khai thác các lỗ hổng của ứng dụng Web?

- a. Cross Site Request Forgery
- b. Social Engineering
- c. SQL Injection
- d. Cross-site scripting

Clear my choice

Câu hỏi 24

Câu trả lời đã được lưu

Đạt điểm 1,00

Các khối xử lý nào được dùng trong mã hóa đối xứng AES? (chọn 3)

- [x] a. ShiftRows
- [ ] b. Shif left
- [ ] c. Straight P-box
- [x] d. MixRows
- [x] e. SubBytes
- [ ] f. Compression P-box

Câu hỏi 25

Câu trả lời đã được lưu

Đạt điểm 1,00

Giao thức nào sau đây được dùng để mã hóa dữ liệu trao đổi giữa Web Browser và Web server?

- ( ) a. SMTP
- ( ) b. IPSec
- ( ) c. HTTP
- ( ) d. VPN
- (•) e. SSL/TLS

Clear my choice

Câu hỏi 26

Câu trả lời đã được lưu

Đạt điểm 1,00

Hệ thống phát hiện xâm nhập dựa vào dấu hiệu (Signature-based IDS) hoạt động dựa vào yếu tố nào?

- (•) a. Các dấu hiệu tấn công
- ( ) b. Nội dung website
- ( ) c. Các dấu hiệu bất thường
- ( ) d. Các dấu hiệu bình thường

Clear my choice

Câu hỏi 27

Câu trả lời đã được lưu

Đạt điểm 1,00

Điều nào sau đây KHÔNG đúng khi nói về lỗ hổng 0-day?

- a. Là lỗ hổng phá hoại hệ thống trong vòng một ngày
- b. Là lỗ hổng nhà sản xuất chưa kịp vá
- c. Là lỗ hổng nguy hiểm khi tấn công vào hệ thống chưa có giải pháp bảo vệ
- d. Là lỗ hổng hacker chưa công bố rộng rãi

Clear my choice

Câu hỏi 28

Câu trả lời đã được lưu

Đạt điểm 1,00

Cơ chế kiểm soát truy cập nào cho phép chủ sở hữu dữ liệu tạo và quản lý kiểm soát truy cập?

- a. Attribute Based Access Control (ABAC)
- b. List Based Access Control (LBAC)
- c. Discretionary Access Control (DAC)
- d. Mandatory Access Control (MAC)
- e. Role Based Access Control (RBAC)

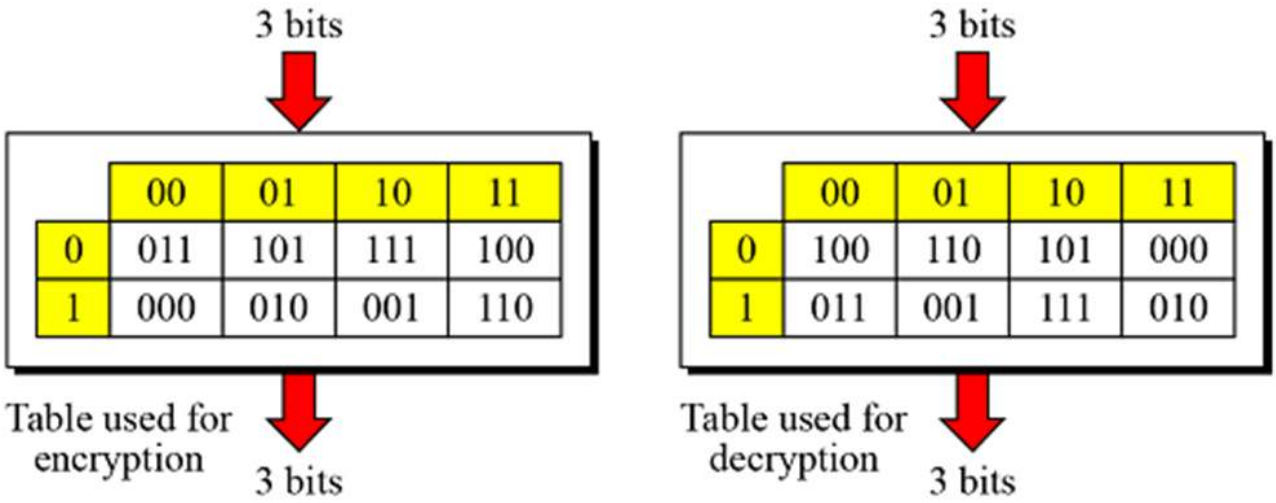
Clear my choice

Câu hỏi 29

Câu trả lời đã được lưu

Đạt điểm 1,00

Given below table for encryption and decryption. Which is the cypher of plaintext = 110?



- a. 001
- b. 101
- c. 011
- d. 100

Clear my choice

Câu hỏi 30

Câu trả lời đã được lưu

Đạt điểm 1,00

Giải pháp Stackshield giúp phòng chống tấn công tràn bộ đệm trên stack thực hiện như sau:

- a. Sử dụng một vùng nhớ đệm an toàn giữa Return Address và Buffer. Sử dụng vùng nhớ đệm an toàn này để kiểm tra xem Return Address có bị sửa đổi hay không
- b. Kiểm tra giá trị Return Address có bị sửa đổi hay không
- c. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu
- d. Lưu trữ giá trị Return Address ở một nơi khác và sử dụng nó để kiểm tra xem giá trị ở Return Address có bị sửa đổi hay không

Clear my choice

Câu hỏi 31

Câu trả lời đã được lưu

Đạt điểm 1,00

Trong mã hóa bất đối xứng (còn gọi là mã hóa hóa công khai). Bob muốn **tạo chữ ký** cho văn bản M để gửi cho Alice. Bob cần dùng khóa gì?

- a. Khóa Public của Bob
- b. Khóa Private của Bob
- c. Khóa Public của Alice
- d. Khóa Private của Alice

Clear my choice

Câu hỏi 32

Câu trả lời đã được lưu

Đạt điểm 1,00

Thuật toán mật mã nào sau đây dựa trên độ khó của bài toán phân tích các số lớn thành tích của hai thừa số nguyên tố ban đầu?

- a. RSA
- b. Diffie-Hellman
- c. ECC
- d. DES

Clear my choice

Câu hỏi 33

Câu trả lời đã được lưu

Đạt điểm 1,00

Chế độ hoạt động nào sau đây mã hóa các khối một cách riêng biệt?

- a. Output feedback mode – OFB
- b. Electronic codebook mode - ECB
- c. Cipher feedback mode - CFB
- d. Cipher block chaining mode - CBC

Clear my choice

Câu hỏi 34

Câu trả lời đã được lưu

Đạt điểm 1,00

Điều nào sau đây sẽ bảo vệ tốt nhất trước cuộc tấn công cụ SQL Injection?

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

Clear my choice

Câu hỏi 35

Câu trả lời đã được lưu

Đạt điểm 1,00

Việc gỡ bỏ những dịch vụ và giao thức không cần thiết gọi là?

- a. Hardening
- b. Nonrepudiation
- c. Hashing
- d. Cleaning
- e. Auditing

Clear my choice

Câu hỏi 36

Câu trả lời đã được lưu

Đạt điểm 1,00

Ưu điểm của hệ thống phát hiện xâm nhập dựa vào dấu hiệu là gì?

- a. Kẻ tấn công không thể giả mạo được hành vi khác dấu hiệu tấn công
- b. Phát hiện chính xác các tấn công
- c. Phát hiện nhanh các tấn công Zero-day
- d. Phát hiện được các tấn công mới

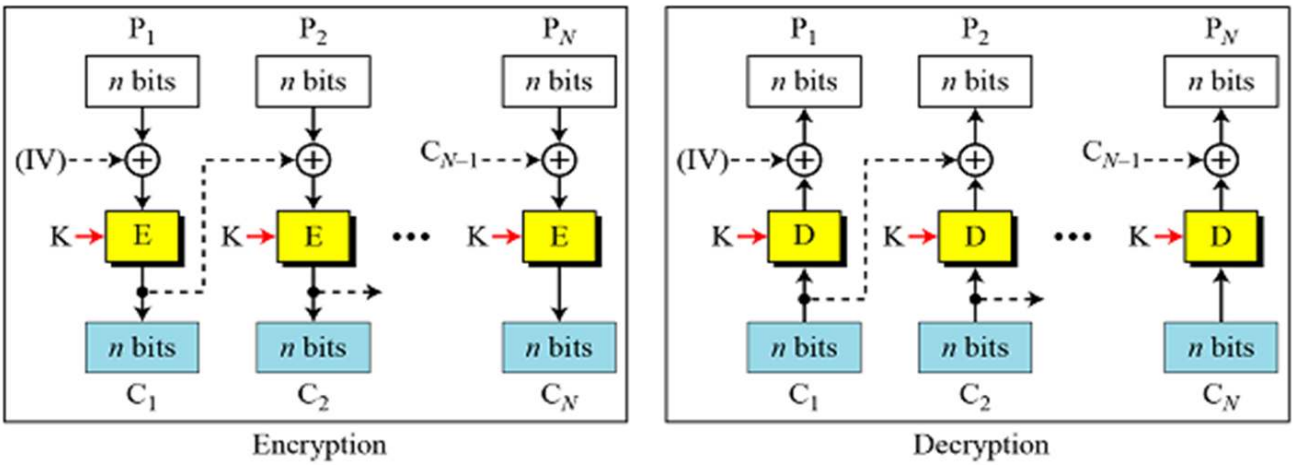
Clear my choice

Câu hỏi 37

Câu trả lời đã được lưu

Đạt điểm 1,00

Given below figure, which mode?



- a. cipher block chaining mode - CBC
- b. output feedback mode – OFB
- c. electronic codebook mode - ECB
- d. cipher feedback mode - CFB

Clear my choice

Câu hỏi 38

Câu trả lời đã được lưu

Đạt điểm 1,00

Một hệ thống xác thực sinh trắc học cho phép một người giả mạo hình thức nhân viên công ty khi vào hệ thống là hiện tượng gì sau?

- a. False positive
- b. True positive
- c. False negative
- d. True negative

Clear my choice

Câu hỏi 39

Câu trả lời đã được lưu

Đạt điểm 1,00

Điều nào sau đây là rủi ro tiềm ẩn khi chương trình chạy ở chế độ đặc quyền?

- a. Nó có thể không thực hiện việc phân chia xử lý các tác vụ
- b. Nó có thể tạo ra việc loại bỏ các ứng dụng không cần thiết
- c. Nó có thể cho phép mã độc được chèn vào
- d. Nó có thể phục vụ cho việc tạo ra các đoạn mã phức tạp không cần thiết

Clear my choice

Câu hỏi 40

Câu trả lời đã được lưu

Đạt điểm 1,00

Cách tốt nhất để nhận ra hành vi bất thường và đánh ngờ trên hệ thống của bạn là gì?

- a. Biết các hoạt động bình thường của hệ thống là như thế nào
- b. Nhận biết các cuộc tấn công mới
- c. Nghiên cứu dấu hiệu hoạt động của các loại tấn công chính
- d. Cấu hình IDS để phát hiện và báo cáo tất cả các lưu lượng bất thường

Clear my choice

Câu hỏi 41

Câu trả lời đã được lưu

Đạt điểm 1,00

Loại malware nào sau đây có thể ẩn các tiến trình và các tập tin trên hệ thống?

- a. Adware
- b. Trojan
- c. Rootkit
- d. Worm

Clear my choice

Câu hỏi 42

Câu trả lời đã được lưu

Đạt điểm 1,00

Một hệ thống kiểm soát truy cập chỉ cấp cho người dùng những quyền cần thiết để họ thực hiện công việc đang hoạt động theo nguyên tắc bảo mật nào?

- a. Least Privilege
- b. Separation of Duties
- c. Discretionary Access Control
- d. Mandatory Access Control

Clear my choice

Câu hỏi 43

Câu trả lời đã được lưu

Đạt điểm 1,00

Which are operations in Key generation of DES? (choose 2)

- a. Compression P-box
- b. S-box
- c. Shift left
- d. Mixcolumn

Câu hỏi 44

Câu trả lời đã được lưu

Đạt điểm 1,00

Tấn công nào có thể bỏ qua hệ thống xác thực để truy cập vào máy tính?

- a. Brute Force
- b. Front door
- c. DoS
- d. Backdoor

Clear my choice

Câu hỏi 45

Câu trả lời đã được lưu

Đạt điểm 1,00

What is the **confusion** property of Product ciphers

- a. hide the relationship between the ciphertext & the key
- b. hide the relationship between the ciphertext & the plaintext
- c. hide the relationship between the round keys
- d. hide the relationship between the key & the plaintext

Clear my choice

Câu hỏi 46

Câu trả lời đã được lưu

Đạt điểm 1,00

Which of the following does a database security solution **not** monitor?

Select one:

- a. Database changes
- b. Database complexity
- c. Sensitive data access
- d. Security events

Clear my choice

Câu hỏi 47

Câu trả lời đã được lưu

Đạt điểm 1,00

What type of firewall analyzes the status of traffic

Select one:

- a. Packet
- b. Stateful inspection
- c. Circuit level
- d. Network-based IDS

Clear my choice

Câu hỏi 48

Câu trả lời đã được lưu

Đạt điểm 1,00

DES - Data Encryption Standard algorithm has block size....., key size.....

- a. Block 56bits, key 64bits
- b. Block 64bits, key 58bits
- c. Block 64bits, key 64bits
- d. Block 64bits, key 56bits

Clear my choice

Câu hỏi 49

Câu trả lời đã được lưu

Đạt điểm 1,00

Tại sao hacker hay sử dụng máy chủ proxy?

- a. Để tạo kết nối mạnh mẽ hơn với mục tiêu
- b. Để tạo một máy chủ ma trên mạng
- c. Để ẩn hoạt động của chúng trên mạng
- d. Để có được kết nối truy cập từ xa

Clear my choice

Câu hỏi 50

Câu trả lời đã được lưu

Đạt điểm 1,00

Which is the operation in DES function?

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

Clear my choice

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

Chuyển tới...

Review - Chapter 1,3,4,5,6: Security concepts; Software & OS Security; Authentication & Access Control ►