

Started on	Monday, 1 January 2024, 6:41 PM
State	Finished
Completed on	Monday, 1 January 2024, 6:41 PM
Time taken	10 secs
Marks	0.00/50.00
Grade	0.00 out of 10.00 (0%)
For CBM, the grade above is shown relative to the maximum for all correct at C=1. ?	
Results for the whole quiz (50 questions)	
Average CBM mark	0.00
Accuracy	0.0%
CBM bonus	0.0%
Accuracy + Bonus	0.0%
Break-down by certainty	
C=3	No responses
C=2	No responses
C=1	No responses

Question 1
Not answered
Weight 1.00

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

- ☐ a. Y giả mạo địa chỉ MAC của X
- ☐ b. X giả mạo địa chỉ IP của Y
- ☐ c. Y giả mạo địa chỉ IP của X
- ☐ d. X giả mạo địa chỉ MAC của Y

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.
The correct answer is:
X giả mạo địa chỉ MAC của Y



Question 2

Not answered

Weight 1.00

Ma trận điều khiển truy cập (Access control matrix) thể hiện mối quan hệ giữa các thành phần nào sau đây?

- ☐ a. Rights/Permissions
- ☐ b. Users
- ☐ c. Object
- ☐ d. Security policy
- ☐ e. Subject
- ☐ f. Database

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answers are:

Subject,

Object,

Rights/Permissions

Question 3

Not answered

Weight 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. True negative
- ☐ b. False negative
- ☐ c. True positive
- ☐ d. False positive

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

False negative

Question 4

Not answered

Weight 1.00

1Cho mô tả sau:

User Nam có quyền đọc và ghi trên file bt1. Nam cũng có quyền đọc trên file bt2 và có quyền thực thi trên file bt3.

User Ha có quyền đọc trên file bt1. Hà có quyền đọc và ghi trên file bt2. Hà không có quyền truy cập trên file bt3.

Xác định ACL (Access control list) đối với file bt2?

- ☐ a. $ACL(bt2) = Nam: \{read\}, Ha: \{read\}$
- ☐ b. $ACL(bt2) = Nam: \{read, write\}, Ha: \{read\}$
- ☐ c. $ACL(bt2) = Nam: \{read\}, Ha: \{read, write\}$
- ☐ d. $ACL(bt2) = Nam: \{read, write\}, Ha: \{read, write\}$
- ☐ e. $ACL(bt2) = Nam: \{read, execute\}, Ha: \{read, write\}$

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

$ACL(bt2) = Nam: \{read\}, Ha: \{read, write\}$

Question 5

Not answered

Weight 1.00

Diffie - Hellman là thuật toán dùng để

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

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Trao đổi khóa

Question 6

Not answered

Weight 1.00

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

- ☐ a. Kiểm tra giá trị Return Address có bị sửa đổi hay không
- ☐ b. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu
- ☐ c. 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
- ☐ 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

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

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

Question 7

Not answered

Weight 1.00

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

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

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Backdoor


Question 8

Not answered

Weight 1.00

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

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

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Electronic codebook mode - ECB


Question 9

Not answered

Weight 1.00

Tấn công Buffer Overflow có hai loại là?

- ☐ a. SQL injection và XSS
- ☐ b. Stack và memory
- ☐ c. Stack và SQL injection
- ☐ d. Heap và network overflow
- ☐ e. Heap và stack

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Heap và stack


Question **10**

Not answered

Weight 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. Các dấu hiệu bất thường
- ☐ c. Nội dung website
- ☐ d. Các dấu hiệu bình thường

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Các dấu hiệu tấn công


Question **11**

Not answered

Weight 1.00

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

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

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Là lỗ hổng phá hoại hệ thống trong vòng một ngày


Question 12

Not answered

Weight 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. 802.3
- ☐ b. 802.11X
- ☐ c. Radius
- ☐ d. 802.3D

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Radius


Question 13

Not answered

Weight 1.00

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

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

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answers are:

ShiftRows,

SubBytes,

MixRows

Question 14

Not answered

Weight 1.00

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

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

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Nó có thể cho phép mã độc được chèn vào

Question 15

Not answered

Weight 1.00

Mục đích chính của chương trình nâng cao nhận thức bảo mật là?

- ☐ a. Đảm bảo rằng mọi người đều hiểu chính sách và thủ tục của tổ chức
- ☐ b. Cảnh báo tất cả người dùng truy cập vào tất cả các hệ thống sẽ được theo dõi hàng ngày
- ☐ c. Thông báo cho người dùng để tuân thủ các quy định liên quan đến bảo vệ dữ liệu và thông tin
- ☐ d. Thông báo cho mọi người rằng quyền truy cập vào thông tin sẽ được cấp khi người sử dụng có yêu cầu

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Đảm bảo rằng mọi người đều hiểu chính sách và thủ tục của tổ chức


Question 16

Not answered

Weight 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 Private của Bob
- ☐ b. Khóa Public của Alice
- ☐ c. Khóa Public của Bob
- ☐ d. Khóa Private của Alice

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Khóa Private của Bob


Question 17

Not answered

Weight 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 đặt 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. 80, 20, 21, 25, 443
- ☐ c. 434, 21, 80, 25, 20
- ☐ d. 110, 443, 21, 59, 25

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

80, 20, 21, 25, 443

Question 18

Not answered

Weight 1.00

Trong tổ chức bộ nhớ của chương trình C, phần Data-Segment lưu các thông tin gì của chương trình?

- ☐ a. Lưu các biến static/global chưa được khởi tạo trong chương trình
- ☐ b. Lưu các biến static/global đã được khởi tạo trong chương trình
- ☐ c. Lưu mã nguồn thực thi
- ☐ d. Lưu các biến cục bộ trong chương trình
- ☐ e. Lưu các đối số của một hàm

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Lưu các biến static/global đã được khởi tạo trong chương trình

Question 19

Not answered

Weight 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?

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

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answers are:

Con người,

Quy trình,

Công nghệ


Question **20**

Not answered

Weight 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 Public của Bob
- ☐ b. Khóa Private của Alice
- ☐ c. Khóa Private của Bob
- ☐ d. Khóa Public của Alice

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Khóa Public của Bob


Question **21**

Not answered

Weight 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. DES
- ☐ b. Diffie-Hellman
- ☐ c. ECC
- ☐ d. RSA

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

RSA


Question **22**

Not answered

Weight 1.00

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

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

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Hardening


Question **23**

Not answered

Weight 1.00

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

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

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Biết các hoạt động bình thường của hệ thống là như thế nào


Question **24**

Not answered

Weight 1.00

Công cụ nào dùng để quét cổng của máy tính

- ☐ a. telnet
- ☐ b. nmap
- ☐ c. nslookup
- ☐ d. ping
- ☐ e. tracer

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

nmap


Question **25**

Not answered

Weight 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 có được kết nối truy cập từ xa
- ☐ d. Để ẩn hoạt động của chúng trên mạng

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Để ẩn hoạt động của chúng trên mạng


Question **26**

Not answered

Weight 1.00

Trong HĐH Linux, để tắt chức năng phát sinh địa chỉ bộ nhớ ngẫu nhiên, sử dụng lệnh nào sau đây?

- ☐ a. `$sudo sysctl -w kernel.randomize_store_space=0`
- ☐ b. `$sudo sysctl -w kernel.randomize_va_space=0`
- ☐ c. `$sudo sysctl -w kernel.randomize_ram_space=0`
- ☐ d. `$sudo sysctl -w kernel.randomize_sa_space=0`
- ☐ e. `$sudo sysctl -w kernel.randomize_as_space=0`

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

`$sudo sysctl -w kernel.randomize_va_space=0`


Question **27**

Not answered

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

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Least Privilege


Question 28

Not answered

Weight 1.00

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

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

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Đào tạo nâng cao nhận thức người dùng


Question 29

Not answered

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

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Transport layer


Question **30**

Not answered

Weight 1.00

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

- ☐ a. VPN
- ☐ b. IPSec
- ☐ c. SSL/TLS
- ☐ d. HTTP
- ☐ e. SMTP

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

SSL/TLS

Question **31**

Not answered

Weight 1.00


Cho mô tả sau:

User Nam có quyền đọc và ghi trên file bt1. Nam cũng có quyền đọc trên file bt2 và có quyền thực thi trên file bt3.

User Ha có quyền đọc trên file bt1. Hà có quyền đọc và ghi trên file bt2. Hà không có quyền truy cập trên file bt3.

Xác định CList (Capability list) đối với user Ha?

- ☐ a. CList(Ha) = bt1: {read, write}, bt2: {write}, bt3: {read}
- ☐ b. CList(Ha) = bt1: {}, bt2: {write}, bt3: {}
- ☐ c. CList(Ha) = bt1: {read}, bt2: {read, write}, bt3: {read, write}
- ☐ d. CList(Ha) = bt1: {read, write}, bt2: {read, write}, bt3: {}
- ☐ e. CList(Ha) = bt1: {read}, bt2: {read, write}, bt3: {}

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

CList(Ha) = bt1: {read}, bt2: {read, write}, bt3: {}


Question **32**

Not answered

Weight 1.00

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

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

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Subjective Access Control


Question **33**

Not answered

Weight 1.00

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

- ☐ a. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu
- ☐ b. 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
- ☐ c. Kiểm tra giá trị Return Address có bị sửa đổi hay không
- ☐ 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

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

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


Question **34**

Not answered

Weight 1.00

Chuẩn nào sau đây liên quan đến [an toàn thông tin](#)?

- ☐ a. ISO 2015
- ☐ b. ISO 21997
- ☐ c. ISO 27001
- ☐ d. ISO 9001
- ☐ e. ISO 2600

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

ISO 27001


Question **35**

Not answered

Weight 1.00

Access control liên quan đến 2 chức năng chính là?

- ☐ a. Authorization
- ☐ b. Least privilege principle
- ☐ c. Rule Based Access Control
- ☐ d. Role Based Access Control
- ☐ e. Authentication

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answers are:

Authentication,

Authorization

Question 36

Not answered

Weight 1.00

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

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

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Rootkit

Question 37

Not answered

Weight 1.00

Mục tiêu chính của [an toàn thông tin](#) là đảm bảo các tính chất theo mô hình C-I-A là?

- ☐ a. Tính dễ mở rộng
- ☐ b. Tính bí mật
- ☐ c. Tính sẵn sàng
- ☐ d. Tính chống chối bỏ
- ☐ e. Tính toàn vẹn
- ☐ f. Tính xác thực

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answers are:

Tính bí mật,

Tính toàn vẹn,

Tính sẵn sàng


Question **38**

Not answered

Weight 1.00

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

AES	<input type="text" value="Choose..."/>
3DES	<input type="text" value="Choose..."/>
DES	<input type="text" value="Choose..."/>
SHA-512	<input type="text" value="Choose..."/>
MD5	<input type="text" value="Choose..."/>

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

AES → 128bits,

3DES → 64bits,

DES → 64bits,

SHA-512 → 512bits,

MD5 → 128bits


Question **39**

Not answered

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

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Discretionary Access Control (DAC)

Question **40**

Not answered

Weight 1.00

Từ ma trận điều khiển truy cập, ta có thể suy ra các thông tin nào sau đây?

- ☐ a. Objects orientation list
- ☐ b. Capability lists
- ☐ c. Access control lists
- ☐ d. Subjects orientation lists
- ☐ e. Group policy objects

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answers are:

Access control lists,

Capability lists

Question **41**

Not answered

Weight 1.00

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

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

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Lọc dữ liệu người dùng nhập vào

Question **42**

Not answered

Weight 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 cần giá trị của hàm băm để có thể kích hoạt được phần mềm mới
- ☐ d. Khách hàng có thể khẳng định tính xác thực của Site mà họ download gói cập nhật về

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Khách hàng có thể xác thực tính toàn vẹn và gói cập nhật cho phần mềm sau khi download về

Question **43**

Not answered

Weight 1.00

Mô hình AAA liên quan đến các chứng năng nào sau đây?

- ☐ a. Accessing
- ☐ b. Accounting
- ☐ c. Authentication
- ☐ d. Automation
- ☐ e. Authenticity
- ☐ f. Authorization

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answers are:

Authentication,

Authorization,

Accounting


Question **44**

Not answered

Weight 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. RBAC (Role Based Access Control)
- ☐ b. Attribute Based Access Control
- ☐ c. DAC (Discretionary Access Control)
- ☐ d. Rule Based Access Control
- ☐ e. MAC (Mandatory Access Control)

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

RBAC (Role Based Access Control)


Question **45**

Not answered

Weight 1.00

Tấn công DoS/DDoS làm ảnh hưởng đến tiêu chuẩn nào của [an toàn thông tin](#)?

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

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Tính sẵn sàng

Question **46**

Not answered

Weight 1.00

Hai dạng mã độc nào sau đây sống độc lập?

- ☐ a. Rootkit
- ☐ b. Trojan
- ☐ c. Zombie
- ☐ d. Logic boom
- ☐ e. Worm

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answers are:

Zombie,

Worm

Question **47**

Not answered

Weight 1.00

Mục đích chính của các kỹ thuật điều khiển truy cập là?

- ☐ a. Giới hạn các quyền truy cập và các hành động cho người dùng hợp pháp được sử dụng
- ☐ b. Cung cấp tất cả các quyền truy cập cho người dùng
- ☐ c. Bảo vệ máy tính khỏi virus
- ☐ d. Ngăn chặn người dùng trái phép truy cập vào tài nguyên hệ thống

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Giới hạn các quyền truy cập và các hành động cho người dùng hợp pháp được sử dụng

Question 48

Not answered

Weight 1.00

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 vị trí của các tường lửa trên mạng
- ☐ c. Để xác định các host đang hoạt động trên mạng
- ☐ d. Để xác định vị trí của các host đang hoạt động trên mạng

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Để xác định các host đang hoạt động trên mạng

Question 49

Not answered

Weight 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. Cross-site scripting
- ☐ c. SQL Injection
- ☐ d. Social Engineering

Certainty ? : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Social Engineering


Question **50**

Not answered

Weight 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 1	Choose...
Layer 2	Choose...
Layer 5	Choose...
Layer 4	Choose...
Layer 7	Choose...
Layer 6	Choose...
Layer 3	Choose...

Certainty  : ☐ C=1 (Unsure: <67%) ☐ C=2 (Mid: >67%) ☐ C=3 (Quite sure: >80%)

Your answer is incorrect.

The correct answer is:

Layer 1 → Data security,

Layer 2 → Application security,

Layer 5 → Perimeter security,

Layer 4 → LAN security,

Layer 7 → Policies, procedures, awareness,

Layer 6 → Physical security,

Layer 3 → Host security

[◀ test attt](#)

Jump to...

[An toàn thông tin ►](#)