11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Started on** Thursday, 16 November 2023, 9:07 AM

**State** Finished

**Completed on** Thursday, 16 November 2023, 9:09 AM

**Time taken** 1 min 59 secs

**Marks** 0.00/55.00

**Grade 0.00** out of 10.00 (**0**%)

**Question 1**

Not answered

Marked out of 1.00

**v1 (latest)**

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

1. Là lỗ hổng nhà sản xuất chưa kịp vá
2. Là lỗ hổng phá hoại hệ thống trong vòng một ngày
3. Là lỗ hổng nguy hiểm khi tấn công vào hệ thống chưa có giải pháp bảo vệ
4. Là lỗ hổng hacker chưa công bố rộng rãi

Câu trả lời của bạn sai. The correct answer is:



Là lỗ hổng phá hoại hệ thống trong vòng một ngày

**Question 2**

Not answered

Marked out of 1.00

**v1 (latest)**

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

1. Subjects orientation lists
2. Capability lists
3. Group policy objects
4. Access control lists
5. Objects orientation list

Your answer is incorrect.

The correct answers are: Access control lists,

Capability lists

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 3**

Not answered

Marked out of 1.00

**v1 (latest)**

Access control liên quan đến 2 chức năng chính là?

1. Rule Based Access Control
2. Least privilege principle
3. Authorization
4. Role Based Access Control
5. Authentication

Your answer is incorrect. The correct answers are:

Authentication, Authorization



**Question 4**

Not answered

Marked out of 1.00

**v1 (latest)**

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

1. $sudo sysctl –w kernel.randomize\_sa\_space=0
2. $sudo sysctl –w kernel.randomize\_ram\_space=0
3. $sudo sysctl –w kernel.randomize\_store\_space=0
4. $sudo sysctl –w kernel.randomize\_as\_space=0
5. $sudo sysctl –w kernel.randomize\_va\_space=0

Your answer is incorrect. The correct answer is:

$sudo sysctl –w kernel.randomize\_va\_space=0

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 5**

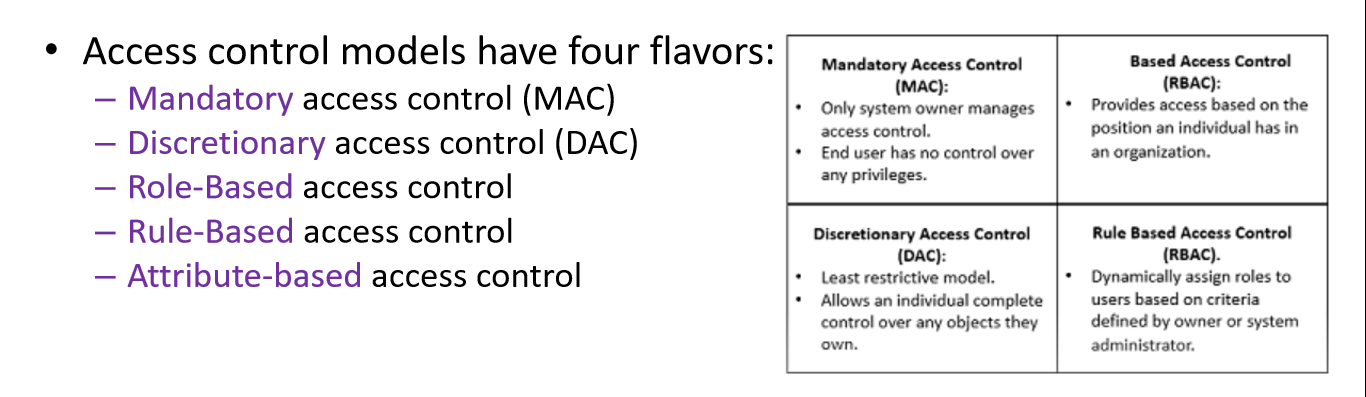
Not answered

Marked out of 1.00

**v1 (latest)**

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

1. Mandatory Access Control (MAC)
2. Attribute Based Access Control (ABAC)
3. Role Based Access Control (RBAC)
4. List Based Access Control (LBAC)
5. Discretionary Access Control (DAC)



Your answer is incorrect. The correct answer is:

Discretionary Access Control (DAC)



**Question 6**

Not answered

Marked out of 1.00

**v1 (latest)**

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

1. Lưu các biến static/global đã được khởi tạo trong chương trình
2. Lưu mã nguồn thực thi
3. Lưu các biến cục bộ trong chương trình
4. Lưu các biến static/global chưa được khởi tạo trong chương trình
5. Lưu các đối số của một hàm

Your answer is incorrect. The correct answer is:

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

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 7**

Not answered

Marked out of 1.00

**v1 (latest)**

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

1. Hashing
2. Hardening
3. Nonrepudiation
4. Auditing
5. Cleaning

Your answer is incorrect. The correct answer is:

Hardening



**Question 8**

Not answered

Marked out of 1.00

**v1 (latest)**

Tại sao hacker hay sử dụng máy chủ proxy?

1. Để ẩn hoạt động của chúng trên mạng
2. Để có được kết nối truy cập từ xa
3. Để tạo một máy chủ ma trên mạng
4. Để tạo kết nối mạnh mẽ hơn với mục tiêu

Your answer is incorrect. The correct answer is:

Để ẩn hoạt động của chúng trên mạng

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 9**

Not answered

Marked out of 1.00

**v1 (latest)**

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

1. 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
2. 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
3. Kiểm tra giá trị Return Address có bị sửa đổi hay không
4. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu

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 10**

Not answered

Marked out of 1.00

**v1 (latest)**

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

1. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu
2. 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
3. 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
4. Kiểm tra giá trị Return Address có bị sửa đổi hay không

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

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 11**

Not answered

Marked out of 1.00

**v1 (latest)**

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

1. Ngăn chặn người dùng trái phép truy cập vào tài nguyên hệ thống
2. Bảo vệ máy tính khỏi virus
3. Giới hạn các quyền truy cập và các hành động cho người dùng hợp pháp được sử dụng
4. Cung cấp tất cả các quyền truy cập cho người dùng

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 12**

Not answered

Marked out of 1.00

**v1 (latest)**

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?

1. Discretionary Access Control
2. Least Privilege
3. Mandatory Access Control
4. Separation of Duties

Your answer is incorrect.

The correct answer is: Least Privilege

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 13**

Not answered

Marked out of 1.00

**v1 (latest)**

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?

1. Quy trình
2. Đào tạo nâng cao nhận thức
3. Đội ngũ chuyên gia bảo mật
4. Con người
5. Tăng chi phí đầu tư cho bảo mật
6. Công nghệ

Your answer is incorrect. The correct answers are:

Con người, Quy trình, Công nghệ



**Question 14**

Not answered

Marked out of 1.00

**v1 (latest)**

Chuẩn nào sau đây liên quan đến an toàn thông tin?

1. ISO 2015
2. ISO 21997
3. ISO 27001
4. ISO 2600
5. ISO 9001

Your answer is incorrect.

The correct answer is: ISO 27001

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 15**

Not answered

Marked out of 1.00

**v1 (latest)**

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?

1. CList(Ha) = bt1: {read}, bt2: {read, write}, bt3: {}
2. CList(Ha) = bt1: {read, write}, bt2: {read, write}, bt3: {}
3. CList(Ha) = bt1: {}, bt2: {write}, bt3: {}
4. CList(Ha) = bt1: {read, write}, bt2: {write}, bt3: {read}
5. CList(Ha) = bt1: {read}, bt2: {read, write}, bt3: {read, write}

Your answer is incorrect. The correct answer is:

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



**Question 16**

Not answered

Marked out of 1.00

**v1 (latest)**

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?

1. Khóa Private của Alice
2. Khóa Public của Bob
3. Khóa Public của Alice
4. Khóa Private của Bob

Your answer is incorrect.

The correct answer is: Khóa Private của Bob

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 17**

Not answered

Marked out of 1.00

**v1 (latest)**

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?

1. ACL(bt2) = Nam: {read, write}, Ha: {read, write}
2. ACL(bt2) = Nam: {read}, Ha: {read, write}
3. ACL(bt2) = Nam: {read, write}, Ha: {read}
4. ACL(bt2) = Nam: {read, execute}, Ha: {read, write}
5. ACL(bt2) = Nam: {read}, Ha: {read}

Your answer is incorrect. The correct answer is:

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



**Question 18**

Not answered

Marked out of 1.00

**v1 (latest)**

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

1. Authenticity
2. Authorization
3. Accounting
4. Authentication
5. Accessing
6. Automation

Your answer is incorrect.

The correct answers are: Authentication,

Authorization, Accounting

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 19**

Not answered

Marked out of 1.00

**v1 (latest)**

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

1. Xác thực 2 yếu tố
2. Quét lỗ hổng cho hệ thống định kỳ
3. Đào tạo nâng cao nhận thức người dùng
4. Phần mềm chống lừa đảo

Your answer is incorrect. The correct answer is:

Đào tạo nâng cao nhận thức người dùng

**Question 20**

Not answered

Marked out of 1.00

**v1 (latest)**

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



1. Là lỗ hổng phá hoại hệ thống trong vòng một ngày
2. Là lỗ hổng nguy hiểm khi tấn công vào hệ thống chưa có giải pháp bảo vệ
3. Là lỗ hổng nhà sản xuất chưa kịp vá
4. Là lỗ hổng hacker chưa công bố rộng rãi

Your answer is incorrect. The correct answer is:

Là lỗ hổng phá hoại hệ thống trong vòng một ngày

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 21**

Not answered

Marked out of 1.00

**v1 (latest)**

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

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

Your answer is incorrect. The correct answer is:

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

**Question 22**

Not answered

Marked out of 1.00

**v1 (latest)**

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



1. ping
2. Sniffing
3. Scan port
4. DoS

Câu trả lời của bạn sai.

The correct answer is: DoS

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 23**

Not answered

Marked out of 1.00

**v1 (latest)**

Thành phần nào KHÔNG phải là của virus?

1. Cơ chế lây nhiễm
2. Password
3. Trigger - sự kiện làm cho payload được kích hoạt
4. Payload - những gì nó làm, độc hại hay lành tính

Câu trả lời của bạn sai. The correct answer is:

Password

**Question 24**

Not answered

Marked out of 1.00

**v1 (latest)**

**Hai** dạng mã độc nào sau đây sống độc lập?



1. Rootkit
2. Worm
3. Zombie
4. Logic boom
5. Trojan

Câu trả lời của bạn sai.

The correct answers are: Worm, Zombie

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 25**

Not answered

Marked out of 1.00

**v1 (latest)**

Mã độc nào KHÔNG lây nhiễm?

1. Virus
2. Zombie
3. Trojan
4. Worm

Câu trả lời của bạn sai. The correct answer is:

Trojan

**Question 26**

Not answered

Marked out of 1.00

**v1 (latest)**

Metamorphic virus có đặc điểm gì?



1. Lẩn tránh phát hiện thông qua nén kích thước
2. Lẩn tránh phát hiện nhờ mã hóa
3. Lẩn tránh phát hiện nhờ thông minh
4. Lẩn tránh phát hiện thông qua việc ghi đè lên chính nó

Câu trả lời của bạn sai. The correct answer is:

Lẩn tránh phát hiện thông qua việc ghi đè lên chính nó

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 27**

Not answered

Marked out of 1.00

**v1 (latest)**

Firewall lọc gói dữ liệu dựa vào những yếu tố nào?

1. Vị trí đặt server
2. Đường link
3. IP nguồn, IP đích
4. Hệ điều hành của server

Câu trả lời của bạn sai. The correct answer is:

IP nguồn, IP đích

**Question 28**

Not answered

Marked out of 1.00

**v1 (latest)**

Một hệ thống xác thực sinh trắc học xác định một người dùng hợp pháp là trái phép khi vào hệ thống là hiện tượng gì sau?



1. False negative
2. False positive
3. True negative
4. True positive

Câu trả lời của bạn sai.

The correct answer is: False positive

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 29**

Not answered

Marked out of 1.00

**v1 (latest)**

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?

1. False positive
2. True negative
3. True positive
4. False negative

Câu trả lời của bạn sai.

The correct answer is: False negative

**Question 30**

Not answered

Marked out of 1.00

**v1 (latest)**

Ví dụ nào sau đây là ví dụ về xác thực hai yếu tố?



1. L2TP và IpSec
2. Thumbprint và card
3. Username và password
4. Client và server

Câu trả lời của bạn sai.

The correct answer is: Thumbprint và card

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 31**

Not answered

Marked out of 1.00

**v1 (latest)**

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

1. Các dấu hiệu bất thường
2. Nội dung website
3. Các dấu hiệu bình thường
4. Các dấu hiệu tấn công

Câu trả lời của bạn sai. The correct answer is:

Các dấu hiệu tấn công

**Question 32**

Not answered

Marked out of 1.00

**v1 (latest)**

Hệ thống phát hiện xâm nhập dựa vào bất thường (Anomaly-based IDS) hoạt động dựa vào yếu tố nào?



1. Các tấn công
2. Nội dung website xấu
3. Các hành vi bất thường
4. Các hành vi bình thường

Câu trả lời của bạn sai.

The correct answer is: Các hành vi bình thường

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 33**

Not answered

Marked out of 1.00

**v1 (latest)**

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

1. Cipher feedback mode - CFB
2. Cipher block chaining mode - CBC
3. Electronic codebook mode - ECB
4. Output feedback mode – OFB

Câu trả lời của bạn sai.

The correct answer is: Electronic codebook mode - ECB

**Question 34**

Not answered

Marked out of 1.00

**v1 (latest)**

Chuẩn nào sau đây liên quan đến an toàn thông tin?



1. ISO 9001
2. ISO 2015
3. ISO 27001
4. ISO 2600

Câu trả lời của bạn sai.

The correct answer is: ISO 27001

11/16/23, 3:09 PM Kiem tra cuoi ki 2: Attempt review (page 1 of 20) | MMS

**Question 35**

Not answered

Marked out of 1.00

**v1 (latest)**

Nam làm hỏng máy tính của Lan, tính chất nào sau đây bị vi phạm? (chọn 2)

1. Tính bí mật
2. Tính xác thực
3. Tính chống chối bỏ
4. Tính toàn vẹn
5. Tính sẵn sàng

Câu trả lời của bạn sai. The correct answers are:

Tính sẵn sàng, Tính toàn vẹn



**Question 36**

Not answered

Marked out of 1.00

**v1 (latest)**

Mô hình Bell La Padula (BLP) qui định cách truy xuất thông tin là gì

1. No read up, no write down
2. No read down, no write up
3. No read down, no write down
4. No read up, no write up

Câu trả lời của bạn sai. The correct answer is:

No read up, no write down

Các giải pháp mã hóa KHÔNG đảm bảo được tính chất nào sau đây

Question 37Answer

a.

Tính toàn vẹn

b.

Tính xác thực

c.

Tính sẵn sàng

d.

Tính bí mật

Đảm bảo dữ liệu không bị sửa đổi trong quá trình lưu trữ hay trong quá trình truyền qua mạng bởi những người dùng không hợp pháp gọi là?

Question 38Answer

a.

Availability

b.

Integrity

c.

Non-repudiation

d.

Confidentiality

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

Question 39Answer

a.

Ransomeware

b.

Code Red

c.

Logic boom

d.

Rootkit

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

Question 40Answer

a.

Xác thực 2 yếu tố

b.

Quét lỗ hổng cho hệ thống định kỳ

c.

Đào tạo nâng cao nhận thức người dùng

d.

Phần mềm chống lừa đảo

Rủi ro chính từ việc sử dụng phần mềm lỗi thời (outdated software) là gì

Question 41Answer

a.

Nó có thể không còn được hỗ trợ bởi các nhà cung cấp

b.

Nó có thể không có tất cả các tính năng bạn cần

c.

Có thể dễ dàng xâm nhập hơn phần mềm mới hơn

d.

Nó có thể không có các tính năng bảo mật hiện đại nhất

Nếu bạn chia sẻ quá nhiều thông tin trên phương tiện truyền thông xã hội, bạn có thể gặp rủi ro gì?

Question 42Answer

a.

Ransomware

b.

Mã độc (malware)

c.

Tấn công giả mạo (Phishing)

d.

Đánh cắp tiền

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?

Question 43Answer

a.

Lưu lượng truy cập web được mã hóa

b.

Lọc dữ liệu người dùng nhập vào

c.

Firewall

d.

IDS

Điều nào sau đây đúng khi nói về tấn công làm tràn bộ đệm (buffer Overflow)

Question 44Answer

a.

Ghi đè các giá trị lên các biến của chương trình nhằm thay đổi hành vi của chương trình theo mục đích của kẻ tấn công

b.

Xóa dữ liệu người dùng

c.

Xảy ra do kiểm tra dữ liệu đầu vào không đầy đủ hoặc bị bỏ qua

d.

Kẻ tấn công gửi các chuỗi dữ liệu lớn làm tràn bộ đệm đã được thiết kế cho chương trình

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

Question 45Answer

a.

Role Based Access Control (RBAC)

b.

Discretionary Access Control (DAC)

c.

Subjective Access Control (SAC)

d.

Mandatory Access Control (MAC)

e.

Attribute Based Access Control (ABAC)

Điều nào sau đây xảy ra khi một chuỗi dữ liệu được gửi đến bộ đệm lớn hơn bộ đệm được thiết kế để xử lý?

Question 46Answer

a.

Spoofing attack

b.

SYN flood

c.

Blue Screen of Death

d.

Buffer overflow

e.

Man in the middle attack

f.

Brute Force attack

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?

Question 47Answer

a.

Mandatory Access Control (MAC)

b.

Role Based Access Control (RBAC)

c.

Discretionary Access Control (DAC)

d.

Attribute Based Access Control (ABAC)

e.

Subjective Access Control (SAC)

Điều nào sau đây mô tả đúng nhất cơ chế kiểm soát truy cập cho phép chủ sở hữu dữ liệu tạo và quản lý kiểm soát truy cập?

Question 48Answer

a.

Discretionary Access Control (DAC)

b.

Attribute Based Access Control (ABAC)

c.

List Based Access Control (LBAC)

d.

Mandatory Access Control (MAC)

e.

Role Based Access Control (RBAC)

Hình sau đây mô tả đúng nhất cơ chế kiểm soát truy cập nào

Question 49Answer

a.

Discretionary Access Control (DAC)

b.

Mandatory Access Control (MAC)

c.

List Based Access Control (LBAC)

d.

Role Based Access Control (RBAC)

e.

Attribute Based Access Control (ABAC)

Ma trận điều khiển truy cập (Access control matrix) thể hiện mối quan hệ giữa các thành phần nào sau đây? (chọn 3)

Question 50Answer

a.

Database

b.

Users

c.

Security policy

d.

Subject

e.

Object

f.

Rights/Permissions

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

Question 51Answer

a.

Subjects orientation lists

b.

Capability lists

c.

Group policy objects

d.

Objects orientation list

e.

Access control lists

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 **ACL** (Access control list) đối với file **bt2**

Question 54Answer

a.

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

b.

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

c.

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

d.

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

e.

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

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

You can preview this quiz, but if this were a real attempt, you would be blocked because: This quiz is currently not available.

**Question 1**

Not yet answered

**v1 (latest)**

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?

1. Con người
2. Công nghệ
3. Đào tạo nâng cao nhận thức
4. Đội ngũ chuyên gia bảo mật
5. Quy trình
6. Tăng chi phí đầu tư cho bảo mật



**Question 2**

Not yet answered

**v1 (latest)**

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?

1. DES
2. RSA
3. Diffie-Hellman
4. ECC

Clear my choice

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 3**

Not yet answered

**v1 (latest)**

Công cụ nào dùng để quét cổng của máy tính

1. telnet
2. nmap
3. nslookup
4. ping
5. tracert Clear my choice

**Question 4**

Not yet answered

**v1 (latest)**

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

1. Tính sẵn sàng
2. Tính dễ mở rộng



1. Tính chống chối bỏ
2. Tính bí mật
3. Tính toàn vẹn
4. Tính xác thực

**Question 5**

Not yet answered

**v1 (latest)**

Diffie - Hellman là thuật toán dùng để

1. Hash khóa
2. Mã hóa khóa
3. Giải mã khóa
4. Tạo khoá
5. Trao đổi khóa Clear my choice

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 6**

Not yet answered

**v1 (latest)**

**Hai** dạng mã độc nào sau đây sống độc lập?

1. Worm
2. Logic boom
3. Zombie
4. Trojan
5. Rootkit

**Question 7**

Not yet answered

**v1 (latest)**

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?

1. Separation of Duties
2. Least Privilege



1. Mandatory Access Control
2. Discretionary Access Control Clear my choice

**Question 8**

Not yet answered

**v1 (latest)**

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

1. Cleaning
2. Hashing
3. Nonrepudiation
4. Hardening
5. Auditing Clear my choice

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 9**

Not yet answered

**v1 (latest)**

Access control liên quan đến 2 chức năng chính là?

1. Role Based Access Control
2. Least privilege principle
3. Authentication
4. Authorization
5. Rule Based Access Control

**Question 10**

Not yet answered

**v1 (latest)**

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

1. X giả mạo địa chỉ IP của Y
2. Y giả mạo địa chỉ IP của X
3. Y giả mạo địa chỉ MAC của X



1. X giả mạo địa chỉ MAC của Y Clear my choice

**Question 11**

Not yet answered

**v1 (latest)**

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?

1. 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
2. Khách hàng có thể xác thực tính toàn vẹn và gói cập nhật cho phần mềm sau khi download về
3. Khách hàng có thể khẳng định tính xác thực của Site mà họ download gói cập nhật về
4. Khách hàng cần giá trị của hàm băm để có thể kích hoạt được phần mềm mới Clear my choice

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 12** Not yet answered **v1 (latest)**

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

1. Để xác định vị trí của các host đang hoạt động trên mạng
2. Để xác định vị trí của các tường lửa trên mạng
3. Để xác định các host đang hoạt động trên mạng
4. Để xác định các cổng đang mở trên mạng Clear my choice

**Question 13** Not yet answered **v1 (latest)**

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

1. $sudo sysctl –w kernel.randomize\_store\_space=0
2. $sudo sysctl –w kernel.randomize\_sa\_space=0
3. $sudo sysctl –w kernel.randomize\_va\_space=0



1. $sudo sysctl –w kernel.randomize\_as\_space=0
2. $sudo sysctl –w kernel.randomize\_ram\_space=0 Clear my choice

**Question 14**

Not yet answered

**v1 (latest)**

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

1. Đào tạo nâng cao nhận thức người dùng
2. Quét lỗ hổng cho hệ thống định kỳ
3. Xác thực 2 yếu tố
4. Phần mềm chống lừa đảo Clear my choice

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 15** Not yet answered **v1 (latest)**

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. 434, 21, 80, 25, 20

 c. 110, 443, 21, 59, 25

 d. 80, 20, 21, 25, 443

Clear my choice

**Question 16**

Not yet answered

**v1 (latest)**

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

1. HTTP
2. SSL/TLS



1. IPSec
2. SMTP
3. VPN

Clear my choice

**Question 17** Not yet answered **v1 (latest)**

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

1. Kiểm tra giá trị Return Address có bị sửa đổi hay không
2. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu
3. 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
4. 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

Clear my choice

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 18** Not yet answered **v1 (latest)**

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?

1. CList(Ha) = bt1: {read, write}, bt2: {write}, bt3: {read}
2. CList(Ha) = bt1: {read, write}, bt2: {read, write}, bt3: {}
3. CList(Ha) = bt1: {read}, bt2: {read, write}, bt3: {read, write}
4. CList(Ha) = bt1: {read}, bt2: {read, write}, bt3: {}
5. CList(Ha) = bt1: {}, bt2: {write}, bt3: {} Clear my choice

**Question 19**

Not yet answered

**v1 (latest)**

Tại sao hacker hay sử dụng máy chủ proxy?



1. Để có được kết nối truy cập từ xa
2. Để tạo kết nối mạnh mẽ hơn với mục tiêu
3. Để tạo một máy chủ ma trên mạng
4. Để ẩn hoạt động của chúng trên mạng Clear my choice

**Question 20**

Not yet answered

**v1 (latest)**

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

1. Object
2. Database
3. Subject
4. Rights/Permissions
5. Security policy
6. Users

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 21** Not yet answered **v1 (latest)**

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?

1. Network Interface layer
2. Application layer
3. Network layer
4. Internet layer
5. Transport layer Clear my choice

**Question 22**

Not yet answered

**v1 (latest)**

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

1. Cross Site Request Forgery



1. Cross-site scripting
2. Social Engineering
3. SQL Injection Clear my choice

**Question 23** Not yet answered **v1 (latest)**

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

1. Lưu lượng truy cập web được mã hóa
2. Lọc dữ liệu người dùng nhập vào
3. IDS
4. Firewall Clear my choice

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 24** Not yet answered **v1 (latest)**

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

1. Nghiên cứu dấu hiệu hoạt động của các loại tấn công chính
2. Cấu hình IDS để phát hiện và báo cáo tất cả các lưu lượng bất thường
3. Biết các hoạt động bình thường của hệ thống là như thế nào
4. Nhận biết các cuộc tấn công mới Clear my choice

**Question 25** Not yet answered **v1 (latest)**

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

1. Attribute Based Access Control (ABAC)
2. Role Based Access Control (RBAC)
3. List Based Access Control (LBAC)



1. Discretionary Access Control (DAC)
2. Mandatory Access Control (MAC) Clear my choice

**Question 26**

Not yet answered

**v1 (latest)**

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

1. Nó có thể phục vụ cho việc tạo ra các đoạn mã phức tạp không cần thiết
2. Nó có thể tạo ra việc loại bỏ các ứng dụng không cần thiết
3. Nó có thể không thực hiện việc phân chia xử lý các tác vụ
4. Nó có thể cho phép mã độc được chèn vào Clear my choice

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 27** Not yet answered **v1 (latest)**

Tấn công Buffer Overflow có hai loại là?

1. Heap và network overflow
2. Stack và memory
3. Stack và SQL injection
4. Heap và stack
5. SQL injection và XSS Clear my choice

**Question 28**

Not yet answered

**v1 (latest)**

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

1. Access control lists
2. Group policy objects



1. Capability lists
2. Objects orientation list
3. Subjects orientation lists

**Question 29** Not yet answered **v1 (latest)**

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

Một quản trị mạng mới thay thế hub bằng switch. Khi sử dụng phần mềm Sniffer bắt các gói tin trên mạng, người quản trị thấy được dữ liệu trao đổi giữa máy tính của anh ta và máy chủ, nhưng không thấy được các trao đổi giữa những máy khác trong mạng với máy chủ. Coi như switch hoạt động tốt, điều gì đã tạo ra hiện tượng trên?

a. Switch được cấu hình VLAN

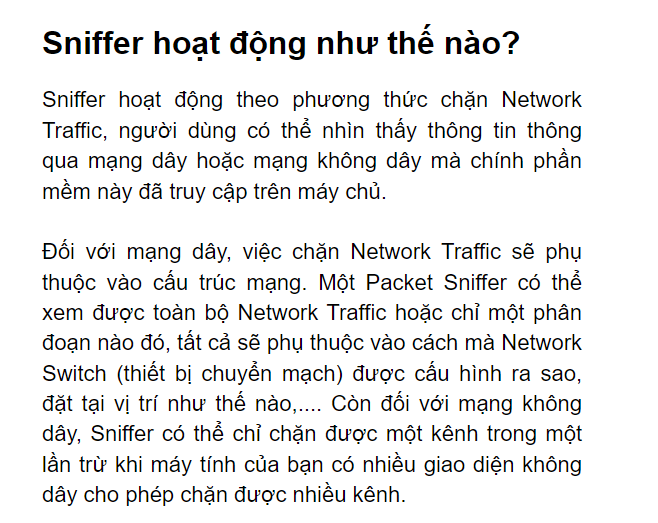
b. Trừ thông tin broadcast và unknown unicast, switch không gửi thông tin ra tất cả các cổng

c. Phần mềm Sniffer không bắt được thông tin qua cổng Ethernet

d. Phần mềm Sniffer cấu hình sai

=> B

=> a



Đảm bảo dữ liệu không bị sửa đổi trong quá trình lưu trữ hay trong quá trình truyền qua mạng bởi những người dùng không hợp pháp gọi là?

a. Nonrepudiation

b. Integrity

c. Confidentiality

d. Availability

=> B

-> **check với file đáp án của test cuối kỳ rùi**

Mặc dù báo cáo quét lỗ hổng cho thấy không có lỗ hổng nào được phát hiện, nhưng một cuộc kiểm tra thâm nhập tiếp theo cho thấy có các lỗ hổng trên mạng. Thuật ngữ nào sau đây mô tả cho trường hợp này?

a. Passive scan

b. False negative

c. Active scan

d. False positive

**=> B**

Email Server nên được đặt ở vùng mạng nào?

a. DZM

b. INSIDE

c. DMZ

d. OUTSIDE

**=> C**

Email Server thường nên được đặt ở vùng mạng DMZ (Demilitarized Zone). Vùng mạng DMZ là một khu vực mạng nằm giữa mạng nội bộ (inside network) và mạng ngoại vi (outside network). Đặt Email Server ở vùng DMZ giúp tăng cường bảo mật, vì nó tạo ra một lớp bảo vệ giữa mạng nội bộ và mạng Internet. Điều này giúp giảm rủi ro từ các tấn công mạng mục tiêu vào Email Server và cung cấp một lớp an ninh bổ sung cho hệ thống.

Đâu là mục tiêu chủ yếu của kiểu tấn công Social Engineering?

a. Peer to Peer Network

b. Email

c. Con người

d. Local Area Network

**=> C**

Quản trị viên bảo mật thiết lập một AP mới nhưng nhận ra quá nhiều người bên ngoài có thể kết nối với AP đó và truy cập trái phép. Các cách nào sau đây sẽ là cách TỐT NHẤT để giảm thiểu vấn đề này?

a. Tất cổng kết nối có dây

b. Disable SSID broadcast

c. MAC filtering

d. Sử dụng kênh 1, 4, 7 trong cấu hình AP

e. Sử dụng 802.11ax

=> B, C, E

**=> b, c**

Access control liên quan đến 2 chức năng chính là?

a. Role Based Access Control

b. Authentication

c. Least privilege principle

d. Authorization

e. Rule Based Access Control

=> b, d

=> check với file đáp án của test cuối kỳ rùi

Khái niệm bảo mật nào khuyến khích quản trị viên cài đặt tường lửa, chương trình quét phần mềm độc hại (malware scanner) và IDS trên các host?

a. Endpoint security

b. Network access control (NAC)

C. SAFE

d. VLAN

e. RADIUS

**=> b**

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

a. Tính chống chối bỏ

b. Tính sẵn sàng

c. Tính toàn vẹn

d. Tính dễ mở rộng

e. Tính xác thực

f. Tính bí mật

=> b, c, f

=> check với file đáp án của test cuối kỳ rùi

Hệ thống IDS/IPS phát hiện xâm nhập dựa vào các kỹ thuật nào sau đây?

a. Role-based detection

b. Anomaly-based detection

c. Classify-based detection

d. Attribute-based detection

e. Signature-based detection

**=> b, e**

Giải pháp StackGuard 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 chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu

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.

=> a

=> check với file đáp án của test cuối kỳ rùi

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

a. Cross Site Request Forgery

b. SQL Injection

c. Cross-site scripting

d. Social Engineering

**=> d**

Theo bạn giải pháp nào cần được áp dụng với các tài khoản người dùng trong hệ thống của một nhân viên nghỉ việc?

a. Vô hiệu hóa các tài khoản của nhân viên đó và xóa ngay lập tức các dữ liệu được lưu trữ

b. Duy trì các tài khoản người dùng và giữ lại các dữ liệu được lưu trữ trong một thời gian

C. Vô hiệu hóa các tài khoản của nhân viên đó và giữ lại các dữ liệu được lưu trữ trong một thời gian

d. Không sử dụng các lựa chọn nào ở đây

**=> C**

Bạn là người tư vấn giải pháp an toàn thông tin, một khách hàng của bạn quan tâm đến việc chống lại giả mạo và nhiễm độc ARP trong mạng của họ. Giải pháp nào dưới đây **KHÔNG** áp dụng cho mục đích này?

a. Sử dụng firewall giữa các phân vùng trong LAN

b. Sử dụng công cụ giám sát ARP trong mạng

C. Sử dụng port security trên các switch

d. Nếu trong một mạng nhỏ thì sử dụng ARP tỉnh

**=> C**

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

a. Authentication

b. Automation

c. Authenticity

d. Authorization

e. Accounting

f. Accessing

=> a, d, e

=> check với file đáp án của test cuối kỳ rùi

Kiểu tấn công nào sau đây không phải kiểu tấn công từ chối dịch vụ?

a. Sử dụng Botnet

b. Ping of Death

c. Main-In-The-Middle (MITM)

d. ICMP Flood

e. Teardrop

* **C**

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 ACL (Access control list) đối với **file bt2?**

a. ACL(bt2) = Nam: {read), Ha: {read}

b. ACL(bt2) Nam: (read, write), Ha: {read, write}

c. ACL(bt2) = Nam: {read}, Ha: {read, write}

d. ACL(bt2)= Nam: (read, write), Ha: (read)

e. ACL(bt2) = Nam: (read, execute), Ha: (read, write}

=> C

=> check với file đáp án của test cuối kỳ rùi

Phát biểu nào sau đây không check với file đáp án của test cuối kỳ rùi về vùng DMZ?

a. Để nâng cao sự bảo mật cho hệ thống

b. Thường chứa email server hoặc web server

c. Chứa các server chỉ phục vụ cho người dùng bên trong

d. Là nơi đặt các public server

**=> c**

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

a. Subjects orientation lists

b. Access control lists

c. Objects orientation list

d. Group policy objects

e. Capability lists

=> b, e

=> check với file đáp án của test cuối kỳ rùi

Việc tắt các port không sử dụng trên switch hay gỡ bỏ các dịch vụ, giao thức, phần mềm không cần thiết gọi là gì?

a. Hashing

b. Hardening

c. Unused-removing

d. Auditing

e. Non-repudiation

**=> b**

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

a. Subjects

b. Objects

c. Rights/Permissions

d. Data

e. Security policies

=> a, b, c

=> check với file đáp án của test cuối kỳ rùi

Muốn thay thế telnet với một giao thức an toàn hơn để quản lý các thiết bị mạng, ta cần sử dụng giao thức nào sau đây?

a. SMTP

b. SSH

d. SFTP

e. SNMP

C. HTTP

**=> B**

Điều nào sau đây xảy ra khi một chuỗi dữ liệu được gửi đến bộ đệm lớn hơn bộ đệm được thiết kế để xử lý?

a. Man in the middle attack

b. SYN flood

c. Brute Force attack

d. Buffer overflow

e. Spoofing attack

=> d

=> check với file đáp án của test cuối kỳ rùi

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 của 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

**=> b**

Điều nào sau đây mô tả check với file đáp án của test cuối kỳ rùi nhất cơ chế kiểm soát truy cập cho phép chủ sở hữu dữ liệu tạo và quản lý kiểm soát truy cập?

a. MACS (Mandatory Access Control)

b. Rule Based Access Control

c. RBACS (Role Based Access Control)

d. LBACS (List Based Access Control)

e. DACs (Discretionary Access Control)

=> e

=> check với file đáp án của test cuối kỳ rùi

Một kiểu tấn công DoS sử dụng cơ chế bắt tay ba bước (three-way handshake) của TCP là?

a. SYN Flood

b. Buffer Overflow

c. Ping of Death

d. SQL Injection

e. Brute force

* **A**

Điều nào sau đây không check với file đáp án của test cuối kỳ rùi khi nói về lỗ hồng 0-day?

a. Là lỗ hồng phá hoại hệ thống trong vòng một ngày

b. Là lỗ hồng nguy hiểm khi tấn công vào hệ thống chưa có giải pháp bảo vệ

O C. Là lỗ hồng hacker chưa công bố rộng rãi

O d Là lỗ hồng nhà sản xuất chưa kịp và

**=> a**

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

a. Lưu các đối số của một hàm

b. Lưu các biến static/global chưa được khởi tạo trong chương trình

C. Lưu các biến cục bộ trong chương trình

d. Lưu mã nguồn thực thi

e. Lưu các biến static/giobal **đã** được khởi tạo trong chương trình

=> e

=> check với file đáp án của test cuối kỳ rùi

Chuẩn nào sau đây liên quan đến an toàn thông tin?

O a. ISO 2600

O b. ISO 9001

O c. ISO 2015

Od. ISO 27001

Oe. ISO 21997

* D
* Check với file đáp án của test cuối kỳ rùi

Tấn công Buffer Overflow có hai loại là?

a. SQL injection và XSS

O b. Stack và memory

c. Heap và stack

O d. Heap và network overflow

O e. Stack và SQL injection

* C
* Check với file đáp án của test cuối kỳ rùi

Câu hỏi 48: Công cụ nào dùng sau đây để quét cổng của máy tính?

a. ping

b. nslookup

c. telnet

d. nmap

O e. tracert

Mã độc Rootkit thường trú ẩn ở đâu?

Oa. Text file

O b. RAM

O c. Boot Sector

d. Operation system

=> d

=> check với file đáp án của test cuối kỳ rùi

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

O a. Cipher feedback mode - CFB

O b. Output feedback mode - OFB

c. Cipher block chaining mode - CBC

d. Electronic codebook mode – ECB

=> d

=> check với file đáp án của test cuối kỳ rùi

Giả sử thuật toán RSA đã tạo ra cặp khóa pubic (7,187) và private (23,187). Message M= 12 sẽ được mã hóa thành gì?

a. 133

O b. 17

O c. 121

O d. 177

* D
* check với file đáp án của test cuối kỳ rùi

Trong mật mã khóa công khai, nếu A muốn gửi thông điệp đến B

O a. Thông điệp được mã hóa bằng khóa riêng của A

O b. Thông điệp được mã hóa bằng khóa công khai của A

O c. Thông điệp được mã hóa bằng khóa riêng của B

d. Thông điệp được mã hóa bằng khóa công khai của B

=> d

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?

O a. Diffie-Hellman

O b. DES

O c. ECC

0 O d. ZUC

e. RSA

=> e

Tại sao hacker hay sử dụng máy chủ proxy?

O a. Để có được kết nối truy cập từ xa

O b. Để tạo một máy chủ ma trên mạng

O c. Để tạo kết nối mạnh mẽ hơn với mục tiêu

d. Để ẩn hoạt động của chúng trên mạng

=> d

Thuật toán nào dưới đây không phải là thuật toán mã hóa khối?

a. AES

O b. 3DES

O C. DES

d. RC4

**=> d**

Câu nào sau đây không phải là một mô hình điều khiển truy cập?

a. Role Based Access Control

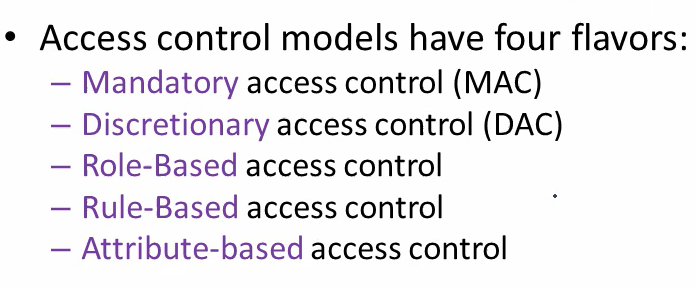
O b. Attribute Based Access Control

O c. Discretionary Access Control (DAC)

d. Subjective Access Control

e. Mandatory Access Control (MAC)

**=> d**



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

O a. Worm

b. Rootkit

O c. Trojan

O d. Adware

* **b**

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?

O a. Lưu lượng truy cập web được mã hóa

b. Lọc dữ liệu người dùng nhập vào

c. Firewall

d. IDS

* b
* check với file đáp án của test cuối kỳ rùi

Trong mật mã khóa công khai (PKI), để xác nhận mình là người gửi thông tin, người gửi sẽ sử dụng khóa nào?

a. Session key

b. Secret key

c. Public key

d. Private key

=> d

C. (chưa chắc)

Nếu bạn chia sẻ quá nhiều thông tin trên phương tiện truyền thông xã hội, bạn có thể gặp rủi ro gì?

O a. Tấn công giả mạo (Phishing)

O b. Mã độc (malware)

C. Ransomware

© d. Đánh cấp danh tính (Identity theft)

* a
* check với file đáp án của test cuối kỳ rùi

Giao thức nào sau đây thuộc mã khóa công khai ?

O a. AES

O b. 3DES

O c. DES

d. RSA

**=> d**

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

a. Nó có thể cho phép mã độc được chèn vào

O b. Nó có thể tạo ra việc loại bỏ các ứng dụng không cần thiết

O c. Nó có thể không thực hiện việc phân chia xử lý các tác vụ

O d. Nó có thể phục vụ cho việc tạo ra các đoạn mã phức tạp không cần thiết

* **a**

Công cụ nào dưới đây có thể dùng để xác định các kết nối mạng đang có trên máy tính?

a. Netstat

O b. Tracert

O c. Ipconfig

O d. Ping

* **a**

Rủi ro chính từ việc sử dụng phần mềm lỗi thời (outdated software) là gì?

O a. Nó có thể không còn được hỗ trợ bởi các nhà cung cấp

O b. Nó có thể không có tất cả các tính năng bạn cần

© c. Nó có thể không có các tính năng bảo mật hiện đại nhất

O d. Có thể dễ dàng xâm nhập hơn phần mềm mới hơn

* a
* check với file đáp án của test cuối kỳ rùi

Máy chủ web của một công ty được cấu hình những dịch vụ sau HTTP, SSL, FTP, SMTP Máy chủ này được đặt trong vùng DMZ. Đấu là những cổng cần phải mở trên tường lửa để cho phép các máy trạm có thể sử dụng dịch vụ trên máy này?

a. 434, 21, 80, 25, 20

O b. 119, 23, 21, 80, 23

c. 80, 20, 21, 25, 443

d. 110, 443, 21, 59,25

**=> c**

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

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

b. Thông báo cho người dùng để tuân thủ các quy định liên quan đến bảo vệ dữ liệu và thông tin

C. Thông báo cho mọi người rằng quyền truy cập vào thông tin sẽ được cấp khi người sử dụng có yêu cầu

O d. Cảnh báo tất cả người dùng truy cập vào tất cả các hệ thống sẽ được theo dõi hàng ngày

* **a**

1. RBAC (Role Based Access Control)
2. DAC (Discretionary Access Control)
3. MAC (Mandatory Access Control)
4. Attribute Based Access Control
5. Rule Based Access Control Clear my choice

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 30** Not yet answered **v1 (latest)**

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?

1. True positive
2. True negative
3. False positive
4. False negative Clear my choice

**Question 31** Not yet answered **v1 (latest)**

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

1. Là lỗ hổng nguy hiểm khi tấn công vào hệ thống chưa có giải pháp bảo vệ
2. Là lỗ hổng phá hoại hệ thống trong vòng một ngày
3. Là lỗ hổng hacker chưa công bố rộng rãi



1. Là lỗ hổng nhà sản xuất chưa kịp vá Clear my choice

**Question 32**

Not yet answered

**v1 (latest)**

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

1. Cung cấp tất cả các quyền truy cập cho người dùng
2. Giới hạn các quyền truy cập và các hành động cho người dùng hợp pháp được sử dụng
3. Bảo vệ máy tính khỏi virus
4. Ngăn chặn người dùng trái phép truy cập vào tài nguyên hệ thống Clear my choice

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 33** Not yet answered **v1 (latest)**

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

1. Kiểm tra giá trị Return Address có bị sửa đổi hay không
2. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu
3. 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
4. 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

Clear my choice

**Question 34**

Not yet answered

**v1 (latest)**

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

1. Authorization
2. Automation



1. Accounting
2. Authenticity
3. Accessing
4. Authentication

**Question 35**

Not yet answered

**v1 (latest)**

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

1. Lưu mã nguồn thực thi
2. Lưu các đối số của một hàm
3. Lưu các biến cục bộ trong chương trình
4. Lưu các biến static/global đã được khởi tạo trong chương trình
5. Lưu các biến static/global chưa được khởi tạo trong chương trình Clear my choice

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 36** Not yet answered **v1 (latest)**

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

1. Mandatory Access Control (MAC)
2. Subjective Access Control
3. Role Based Access Control
4. Attribute Based Access Control
5. Discretionary Access Control (DAC) Clear my choice

**Question 37**

Not yet answered

**v1 (latest)**

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

1. Các dấu hiệu bình thường
2. Các dấu hiệu bất thường



1. Nội dung website
2. Các dấu hiệu tấn công Clear my choice

**Question 38**

Not yet answered

**v1 (latest)**

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

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

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 39** Not yet answered **v1 (latest)**

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

1. Electronic codebook mode - ECB
2. Cipher feedback mode - CFB
3. Cipher block chaining mode - CBC
4. Output feedback mode – OFB Clear my choice

**Question 40** Not yet answered **v1 (latest)**

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

DES 3DES MD5 SHA-512

128bits 64bits 64bits 128bits

512bits



**Question 41** Not yet answered **v1 (latest)**

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?

1. Khóa Public của Alice
2. Khóa Public của Bob
3. Khóa Private của Bob
4. Khóa Private của Alice Clear my choice

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 42** Not yet answered **v1 (latest)**

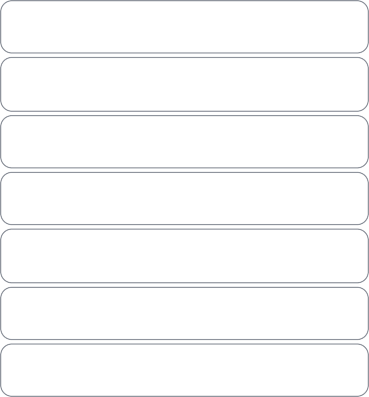
Tấn công nào có thể bỏ qua hệ thống xác thực để truy cập vào máy tính?

1. Brute Force
2. Backdoor
3. DoS
4. Front door Clear my choice

**Question 43** Not yet answered **v1 (latest)**

Mô hình bảo mật theo chiều sâu (defense in depth) gồm các lớp bảo mật theo thứ tự từ trong ra ngoài là? Layer 5

Layer 1



Perimeter security Data security

Policies, procedures, awareness Physical security

LAN security Host security

Application security



Layer 7

Layer 6

Layer 4

Layer 3

Layer 2

**Question 44**

Not yet answered

**v1 (latest)**

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

1. Tính toàn vẹn
2. Tính chống thoái thác
3. Tính bí mật
4. Tính xác thực
5. Tính sẵn sàng Clear my choice

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 45** Not yet answered **v1 (latest)**

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

1. MixRows
2. ShiftRows
3. Compression P-box
4. Straight P-box
5. Shif left
6. SubBytes

**Question 46**

Not yet answered

**v1 (latest)**

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?

1. Khóa Public của Bob



1. Khóa Private của Bob
2. Khóa Public của Alice
3. Khóa Private của Alice Clear my choice

**Question 47**

Not yet answered

**v1 (latest)**

Chuẩn nào sau đây liên quan đến an toàn thông tin?

1. ISO 9001
2. ISO 27001
3. ISO 2600
4. ISO 21997
5. ISO 2015

Clear my choice

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS

**Question 48** Not yet answered **v1 (latest)**

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. 802.3D

 c. 802.11X

d. Radius Clear my choice

**Question 49** Not yet answered **v1 (latest)**

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?



1. ACL(bt2) = Nam: {read}, Ha: {read, write}
2. ACL(bt2) = Nam: {read, execute}, Ha: {read, write}
3. ACL(bt2) = Nam: {read, write}, Ha: {read}
4. ACL(bt2) = Nam: {read, write}, Ha: {read, write}
5. ACL(bt2) = Nam: {read}, Ha: {read} Clear my choice

**Question 50**

Not yet answered

**v1 (latest)**

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

1. Adware
2. Trojan
3. Rootkit
4. Worm Clear my choice

11/15/23, 10:23 PM Đề thi cuối kỳ | MMS