ĐỀ THI KẾT THÚC HỌC PHẦN

MÔN: CƠ SỞ AN TOÀN THÔNG TIN

Thời gian làm bài: 60 phút

Mã đề thi: 03

14/10

LƯU Ý: - *Không viết vẽ vào đề thi, không sử dụng tài liệu;*

(Một câu hỏi có thể có một hoặc nhiều câu trả lời, mỗi câu hỏi 0,25 điểm)

Câu 1 **Những phát biểu nào sau đây là SAI?**

A. Lỗ hổng an toàn của một hệ thống thông tin là những khiếm khuyết trong cơ chế bảo vệ của hệ thống đó mà có thể bị khai thác để phá vỡ một hoặc một số tính chất an toàn thông tin của hệ thống.

(B) Bất kỳ một khiếm khuyết nào trong một hệ thống thông tin mà có thể bị tin tặc hay thậm chí người dùng hợp lệ của hệ thống khai thác để gây mất an toàn thông tin cho hệ thống thì đều là lỗ hổng an toàn thông tin của hệ thống đó.

C. Mã định danh CVE được gắn cho các lỗ hổng an toàn để đảm bảo tính thống nhất trong cộng đồng khi đề cập đến các lỗ hổng.

(D) Nếu trong hệ thống có tồn tại khiếm khuyết thì sớm hay muộn sẽ bị khai thác để làm tổn hại tới tính an toàn của hệ thống; khi đó khiếm khuyến đó sẽ trở thành lỗ hổng.

Câu 2 **Trình tự truy cập nào sau đây là ĐÚNG?**

A. Xác thực → Định danh → Cấp quyền

B. Định danh → Cấp quyền → Xác thực

(C) Định danh → Xác thực → Cấp quyền

D. Cấp quyền → Xác thực → Định danh

Câu 3 **Đâu là các hệ mật khóa bí mật**

(A) DES

B. RSA

(C) RC4

(D) AES

Câu 4 **Tấn công XSS có thể được sử dụng với mục đích nào sau đây:**

(A) Đánh cắp tài khoản

(B) Đánh cắp cơ sở dữ liệu

C. Từ chối dịch vụ

(D) Đánh cắp cookie (SessionID)

E. Thực hiện Click Hijacking

F. Vét cạn mật khẩu

Câu 5 **Một đoạn mã độc sử dụng các cuộc tấn công từ điển vào máy tính để có quyền truy cập vào tài khoản quản trị. Đoạn mã này sau đó liên kết các máy tính bị xâm nhập với nhau nhằm mục đích nhận các lệnh từ xa. Thuật ngữ nào mô tả ĐÚNG NHẤT loại mã độc này?**

A. Exploit

(B) Botnet

C. Logic bomb

D. Backdoor

Câu 6 **Lỗ hổng nào sau đây là lỗ hổng web**

(A) SQL Injection

(B) Cross-Site Scripting (XSS)

(C) Cross-Site Request Forgery (CSRF)

D. Buffer overflow

E. Format string

(F) Xác thực yếu

Câu 7 **Cho bảng cơ sở dữ liệu SINHVIEN như sau:**

Với truy vấn SELECT * FROM SINHVIEN, kết quả trả về cho người dùng có mức bảo mật C là kết quả nào dưới đây?

A.

B.

C.

D.

Câu 8 **Để dễ dàng cấp quyền truy cập vào tài nguyên mạng cho nhân viên, bạn quyết định phải có một cách dễ dàng hơn là cấp cho người dùng quyền truy cập cá nhân vào tệp, máy in, máy tính và ứng dụng. Mô hình bảo mật nào bạn nên xem xét sử dụng?**

A. Kiểm soát truy cập bắt buộc

B. Kiểm soát truy cập tùy ý
C. Kiểm soát truy cập dựa trên vai trò
D. Kiểm soát truy cập thời gian trong ngày

Câu 9 **Trong mật mã khóa bí mật, số lượng khóa trong hệ thống 10 người dùng là**
A. 54
B. 45
C. 10
D. 20
E. 50

Câu 10 **Trong mã hóa dữ liệu sử dụng mật mã khóa công khai, phát biểu nào sau đây là ĐÚNG:**
A. Dữ liệu được mã hóa bằng khóa công khai, giải mã bằng khóa bí mật
B. Tốc độ thực thi nhanh
C. Mọi người đều có thể giải mã
D. Từ khóa công khai không thể tìm ra khóa bí mật
E. Dữ liệu mã hóa bằng khóa bí mật, giải mã bằng khóa công khai

Câu 11 **Xác thực nào dưới đây KHÔNG phải là xác thực đa nhân tố**
A. Thẻ từ + Mã PIN
B. Mật khẩu một lần (OTP – One Time Passowrd)
C. Mật khẩu + vị trí địa lý
D. Token
E. Smartcard + Mã PIN

Câu 12 **Mục đích của Chữ ký số:**
A. Đảm bảo tính xác thực
B. Đảm bảo tính bí mật
C. Đảm bảo tính toàn vẹn
D. Đảm bảo tính chống chối bỏ

Câu 13 **Những phát biểu nào sau đây là ĐÚNG?**
A. Tính toàn vẹn của thông tin là tính chất đảm bảo thông tin không bị sửa đổi khi truyền từ điểm nguồn tới điểm đích.
B. Thông tin lưu trữ cũng cần được đảm bảo tính toàn vẹn.
C. Nhiệm vụ đảm bảo tính toàn vẹn của thông tin là phát hiện sự sửa đổi thông tin nếu có sự sửa đổi đó.
D. Nhiệm vụ đảm bảo tính toàn vẹn của thông tin là tạo một bản sao của thông tin để thay thế bản gốc khi phát hiện sự sửa đổi.
E. Việc tạo và lưu giữ một hay nhiều bản sao của thông tin có thể giúp kiểm tra tính toàn vẹn của thông tin.

Câu 14 **Tấn công Stuxnet được phát hiện vào tháng 6 năm 2010. Chức năng chính của nó là che giấu sự hiện diện của nó trong khi lập trình lại các hệ thống máy tính công nghiệp (gọi là PLC), cụ thể là máy ly tâm hạt nhân trong nhà máy điện hạt nhân Iran. Phần mềm độc hại đã được phát tán thông qua các ổ đĩa flash USB, trong đó nó truyền các bản sao của chính nó đến các máy chủ khác. Điều nào sau đây áp dụng cho Stuxnet?**
A. Rootkit
B. Spam
C. Worm
D. Adware

Câu 15 **Đâu là những ví dụ về rò rỉ thông tin?**
A. Nhân viên bán hàng đọc được thông tin mật của công ty thương mại.
B. Từ ngoài vùng khiếm soát có thể nghe được nội dung cuộc họp của công ty, trong đó có thông tin mật, do hệ thống loa hoạt động với công suất lớn.
C. Thông tin mật của công ty bị đối thủ biết được do họ mua chuộc người trong nội bộ công ty đặt thiết bị nghe lén.
D. Thông tin mật của công ty bị đối thủ biết được do nhân viên gửi nhầm file chứa thông tin mật trong quá trình làm việc.

Câu 16 **Đâu là mục tiêu của mã độc khi tấn công người dùng**
A. Thu thập dữ liệu trên máy tính
B. Ăn cắp thông tin như mật khẩu, mã bảo mật thẻ tín dụng.
C. Sử dụng tài nguyên trên máy nạn nhân (để "đào" Bitcoin).
D. Mã hóa dữ liệu và đòi tiền chuộc.
E. Phá hủy dữ liệu trên máy nạn nhân.
F. Vét cạn mật khẩu

Câu 17 **Những phát biểu nào sau đây là đúng?**
A. An toàn thông tin là bảo vệ thông tin và hệ thống thông tin trước tấn công của tin tặc, bao

Commented [HNNQ1]: 9/ Công thức mật mã đối xứng (N*(n-1))/2
11/ 1 cái

ĐÁNH DẤU 12
MÀU ĐỎ: ĐÚNG
MÀU XANH: CÓ VẺ ĐÚNG
MÀU TÍM: HÊN XUI =))

An toàn thông tin bao gồm việc đảm bảo hoạt động ổn định của hệ thống thông tin trước khả năng xảy ra sự cố vật lý.
C. Một trong những nhiệm vụ của an toàn thông tin là ngăn chặn sự phát tán tin giả trên mạng để không gây tác động tiêu cực lên nhận thức của cộng đồng.

u 18 **Mô hình dưới đây thuộc mô hình nào**
A. Access Control List (ACM)
B. Access Capability (Profile)
C. RBAC
D. MAC

u 19 **Đâu KHÔNG phải là tính chất an toàn của thông tin?**
A. Tính bí mật
B. Tính cấp thiết
C. Tính chính xác
D. Tính sẵn sàng
E. Tính kịp thời

u 20 **Cho hàm băm H, từ H(x) không thể tìm được x là tính chất nào của hàm băm**
A. Nén
B. Kháng tiền ảnh
C. Kháng tiền ảnh thứ 2
D. Kháng va chạm

u 21 **Độ an toàn của mật khẩu nào dưới đây là lớn nhất (biết rằng mật khẩu có thể gồm chữ số, chữ cái hoa và thường)**
A. 12345678
B. 12a4567
C. A2a34567
D. 2a13456
E. 123456789012
F. 1a2345678

22 **Những phát biểu nào sau đây là SAI?**
A. Hiểm họa an toàn thông tin là bất kỳ sự tác động nào mà có thể dẫn đến sự phá vỡ một hoặc một số tính chất an toàn của thông tin.
B. Hiểm họa an toàn thông tin là những dự định của tin tặc tác động lên một hệ thống thông tin nhằm phá vỡ một hoặc một số tính chất an toàn của thông tin.
C. Hiểm họa an toàn thông tin là khả năng tiềm tàng trong tương lai về việc một hoặc một số tính chất an toàn của thông tin bị phá vỡ bởi tin tặc, hoặc thậm chí là bởi những người dùng hợp lệ trong hệ thống.
D. Mọi hành động dù là vô tình hay cố ý của người dùng hợp lệ trong hệ thống nếu có thể phá vỡ một hay một số tính chất an toàn của thông tin thì đều được coi là hiểm họa an toàn thông tin đối với hệ thống đó.

23 **Loại lỗ hổng nào dẫn đến việc ghi dữ liệu vượt ra ngoài ranh giới bộ nhớ dự kiến?**
A. Pointer dereferences
B. Integer overflow
C. Buffer overflow
D. Rò rỉ bộ nhớ
E. Stack overflow
F. Heap overflow

24 **Phát biểu nào sau đây ĐÚNG?**
A. Worms ghi lại tất cả các ký tự đã gõ vào một tệp văn bản.
B. Worms tự phát tán sang các hệ thống khác.
C. Worms có thể mang virus.
D. Worms lây nhiễm vào đĩa cứng MBR.

25 **Tính chất sao trong mô hình kiểm soát truy cập bắt buộc MAC nhằm**
A. Không đọc lên
B. Không đọc xuống
C. Không ghi lên
D. Không ghi xuống

26 **Ma trận kiểm soát truy cập (Acess Control Matrix) thuộc mô hình kiểm soát truy cập nào**
A. Kiểm soát truy cập bắt buộc (MAC)
B. Kiểm soát truy cập tùy chọn (DAC)
C. Kiểm soát truy cập dựa trên vai trò (RBAC)
D. Kiểm soát truy cập dựa trên thuộc tính (ABAC)

E. Kiểm soát truy cập dựa trên chính sách (PBAC)

Câu 27 **Biểu thức thể hiện tính trội nào dưới đây là ĐÚNG?**

A. (3, Kinh doanh) ≤ (2, (Hành chính, Lập trình viên))

B. (3, Kinh doanh, Hành chính) ≤ (2, (Kinh doanh, Lập trình viên))

C. (2, Kinh doanh) ≤ (3, (Kinh doanh, Lập trình viên))

D. (2, (Kinh doanh, Lập trình viên)) ≤ (3, Kinh doanh)

Câu 28 **Những phát biểu nào sau đây là ĐÚNG?**

A. ISO 27001 là một tiêu chuẩn về an toàn thông tin

B. ISO 27001 là một bộ các tiêu chuẩn quốc tế về quản lý an toàn thông tin

C. ISO 27001 là một tiêu chuẩn xác định các yêu cầu đối với hệ thống quản lý an toàn thông tin.

D. ISO 27001 là một tiêu chuẩn xác định các yêu cầu đối với hệ thống bảo vệ thông tin.

Câu 29 **Mô hình bảo mật nào sử dụng phân loại dữ liệu và phân quyền người dùng dựa trên phân loại dữ liệu**

A. RBAC

B. DAC

C. PKI

D. MAC

Câu 30 **Tại sao cần sử dụng hàm băm trong chữ ký số**

A. Giảm kích thước chữ ký

B. Tăng độ an toàn

C. Bảo đảm khả năng tính toán hiện nay

D. Không thể thiếu được trong sơ đồ chữ ký số

Câu 31 **Những phát biểu nào sau đây là ĐÚNG?**

A. Một tổ chức chỉ có thể được chứng nhận đạt chuẩn ISO 27001 khi đáp ứng tất cả các yêu cầu của ISO 27001

B. Một tổ chức được chứng nhận đạt chuẩn ISO 27001 có nghĩa là hệ thống thông tin của tổ chức đó được đảm bảo an toàn.

C. Một tổ chức được chứng nhận đạt chuẩn ISO 27001 có nghĩa là tổ chức đó đã triển khai việc bảo vệ thông tin một cách đúng đắn.

Câu 32 **Đâu là công cụ đóng băng ổ đĩa**

A. Deep Freeze (Faronics Corporation)

B. Shadow Defender

C. Returnil Virtual System

D. VMWare

E. VPN

F. Bitlocker

Câu 33 **Kiểm soát truy cập nào thực hiện việc gán nhãn an toàn tới các thực thể và đối tượng?**

A. MAC

B. DAC

C. RBAC

D. RuBAC

Câu 34 **Những phát biểu nào sau đây là đúng?**

A. Tính bí mật là một trong những tính chất an toàn của thông tin.

B. Tính bí mật của thông tin phải bao hàm tính chính xác của thông tin.

C. Thông tin được đảm bảo bí mật thì cũng đảm bảo tính toàn vẹn.

D. Để đảm bảo tính bí mật thì thông tin cần được mã hóa.

E. Để đảm bảo tính bí mật thì cần nghiêm cấm việc tạo bản sao của thông tin.

F. Để đảm bảo tính bí mật thì chỉ cung cấp thông tin cho người có thẩm quyền tiếp cận.

Câu 35 **Người quản lý của bạn đã đọc về các cuộc tấn công SQL Injecttion và đang tự hỏi có thể làm gì để bảo vệ chống lại chúng đối với các ứng dụng được phát triển nội bộ. Bạn muốn giới thiệu điều gì cho quản lý của mình?**

A. Kiểm thử và vá lỗi mã nguồn web

B. Sử dụng phần mềm Antivirus

C. Xác thực đầu vào

D. Tường lửa

E. Sử dụng mật mã

F. Sử dụng DLP

Câu 36 **Chức năng User Account Control (UAC) trong Windows 8 cho phép người dùng có thể thay đổi các cài đặt của Windows nhưng trước khi thay đổi sẽ hiển thị lời nhắc để xác nhận lại sự thay đổi này cho người dùng. Điều này giúp chống lại tấn công nào?**

C. Spyware
D. Worms

Câu 37 **Mã độc nào sau đây có khả năng tự nhân bản**
(A) Virus
B. Trojan
(C) Worm
D. Logic Bomb
E. Ransomware

Câu 38 **Bạn theo dõi và kiểm tra lưu lượng mạng hàng tuần để đảm bảo rằng mạng đang được sử dụng đúng cách. Khi làm như vậy, bạn nhận thấy lưu lượng truy cập đến cổng TCP 53 trên máy chủ của mình từ một địa chỉ IP không xác định. Sau khi xem lại nhật ký máy chủ của bạn, bạn nhận thấy nhiều lần thất bại trong việc thực hiện chuyển vùng đến máy chủ của mình. Đây là dấu hiệu của kiểu tấn công nào?**
A. ARP poisoning
B. Cross-site scripting
(C) DNS poisoning
D. MAC flooding

Câu 39 **Không thể tìm được cặp (x,y) sao cho H(x) = H(y) là tính chất nào của hàm băm**
A. Kháng tiền ảnh
B. Nén
(C) Kháng va chạm
D. Kháng tiền ảnh thứ 2

Câu 40 **Được phát hiện vào năm 1991, virus Michelangelo được cho là đã được kích hoạt để ghi đè lên 100 sector đĩa cứng đầu tiên với dữ liệu null mỗi năm vào ngày 6 tháng 3, đúng vào ngày sinh nhật của nghệ sĩ người Ý. Michelangelo thuộc loại virus nào?**
A. Zero day
B. Worm
C. Trojan
(D) Logic bomb

Câu 41 **Một hacker ngồi trong quán cà phê có điểm truy cập Internet và tiến hành thực hiện ARP poisoning mọi người kết nối với mạng không dây để tất cả lưu lượng truy cập qua máy tính xách tay hacker trước khi cô định tuyến lưu lượng truy cập vào Internet. Đây là loại tấn công nào?**
A. Rainbow tables
(B) Man in the middle
C. DNS poison
D. Spoofing

Câu 42 **Biện pháp đối phó nào sau đây được thiết kế để bảo vệ chống lại cuộc tấn công vét cạn vào mật khẩu?**
A. Cập nhật bản vá
(B) Tạm khóa, khóa tài khoản
C. Nâng cao độ phức tạp của mật khẩu
D. Sử dụng mật khẩu mạnh

Câu 43 **Khi truy cập vào các tài liệu trong một thư mục trên máy tính của bạn, bạn nhận thấy tất cả các tệp đã bị đổi tên thành các tên tệp ngẫu nhiên. Ngoài ra, bạn thấy một tài liệu chứa các hướng dẫn thanh toán để giải mã các tệp tin. Trong trường hợp này bạn đã nhiễm mã độc nào?**
A. Encryptionware
B. Virus
C. Criminalware
(D) Ransomware
E. Worm

Câu 44 **Mã xác thực thông điệp (MAC – Message Authentication Code) nhằm:**
(A) Đảm bảo tính xác thực
B. Đảm bảo tính bí mật
C. Đảm bảo tính toàn vẹn
D. Đảm bảo tính chống chối bỏ

Câu 45 **Loại phần mềm nào giúp lọc bỏ các email rác không mong muốn?**
A. Anti-spam
B. Antivirus