QUIZIZZ

NAME : _____

CLASS : _____

CSATTT-C1+C2
44 Questions

DATE : _____

1. An toàn hệ thống thông tin là:

A. Việc đảm bảo thông tin trong hệ thống không bị đánh cắp

B. Việc đảm bảo cho hệ thống thông tin hoạt động trơn tru, ổn định

C. Việc đảm bảo cho hệ thống thông tin không bị tấn công

D. Việc đảm bảo các thuộc tính an ninh, an toàn của hệ thống thông tin

2. An toàn thông tin (Information Security) là gì?

A. Là việc phòng chống đánh cắp thông tin

B. Là việc phòng chống tấn công mạng

C. Là việc bảo vệ chống sử dụng, tiết lộ, sửa đổi, vận chuyển hoặc phá hủy thông tin một cách trái phép

D. Là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép

3. An toàn thông tin gồm hai lĩnh vực chính là:

A. An toàn máy tính và An toàn Internet

B. An ninh mạng và An toàn hệ thống

C. An toàn máy tính và An ninh mạng

D. An toàn công nghệ thông tin và Đảm bảo thông tin

4. Biện pháp nào không thể phòng chống hiệu quả tấn công khai thác lỗi tràn bộ đệm?

A. Sử dụng các thư viện an toàn hoặc ngôn ngữ lập trình không gây tràn

B. Kiểm tra mã nguồn để tìm điểm có khả năng gây tràn và khắc phục

C. Sử dụng công cụ gỡ rối để ngăn chặn tràn trong thời gian vận hành

D. Đặt cơ chế không cho phép thực hiện mã trong dữ liệu (DEP)

5. Các kỹ thuật và công cụ thường được sử dụng trong an ninh mạng bao gồm:

A VPN, SSL/TLS, PGP

B Điều khiển truy nhập, tường lửa, proxy và các giao thức bảo mật, ứng dụng dựa trên mật mã

C Điều khiển truy nhập

D Tường lửa, proxy

6. Các lỗ hổng an ninh trong hệ điều hành máy chủ là mối đe dọa thuộc vùng nào trong 7 vùng cơ sở hạ tầng CNTT?

A Vùng mạng LAN-to-WAN

B Vùng máy trạm

C Vùng mạng LAN

D Vùng mạng WAN

7. Các lỗ hổng bảo mật thường tồn tại nhiều nhất trong thành phần nào của hệ thống:

A Các thành phần phần cứng

B Hệ điều hành

C Các ứng dụng

D Các dịch vụ mạng

8. Các thành phần chính của hệ thống máy tính gồm:

A CPU, Bộ nhớ, HDD và Hệ thống bus truyền dẫn

B CPU, hệ điều hành và các ứng dụng

C CPU, Bộ nhớ, HDD, hệ điều hành và các ứng dụng

D Hệ thống phần cứng và Hệ thống phần mềm

9. Các thành phần của an toàn thông tin gồm:

A An toàn máy tính, An ninh mạng, Quản lý ATTT và Chính sách ATTT

B An toàn máy tính, An toàn dữ liệu, An ninh mạng, Quản lý ATTT

C An toàn máy tính, An ninh mạng, Quản lý rủi ro ATTT và Chính sách ATTT

D An toàn máy tính và dữ liệu, An ninh mạng, Quản lý ATTT và Chính sách ATTT

10. Các vùng bộ nhớ thường bị tràn gồm:

A Ngăn xếp (Stack) và Bộ nhớ đệm (Cache)

B Hàng đợi (Queue) và Vùng nhớ cấp phát động (Heap)

C Hàng đợi (Queue) và Ngăn xếp (Stack)

D Ngăn xếp (Stack) và Vùng nhớ cấp phát động (Heap)

11. Các yêu cầu cơ bản trong đảm bảo an toàn thông tin và an toàn hệ thống thông tin gồm:

A Bí mật, Toàn vẹn và Không chối bỏ
B Bí mật, Toàn vẹn và Sẵn dùng
C Bảo mật, Toàn vẹn và Khả dụng
D Bảo mật, Toàn vẹn và Sẵn dùng

12. Đảm bảo thông tin (Information assurance) thường được thực hiện bằng cách:

A Sử dụng kỹ thuật tạo dự phòng cục bộ
B Sử dụng kỹ thuật tạo dự phòng ra băng từ
C Sử dụng kỹ thuật tạo dự phòng ngoại vi
D Sử dụng kỹ thuật tạo dự phòng ra đĩa cứng

13. Dạng tấn công chèn mã được tin tặc thực hiện phổ biến trên các trang web nhắm đến các cơ sở dữ liệu là:

A Tấn công chèn mã XSS
B Tấn công chèn mã HTML
C Tấn công chèn mã SQL
D Tấn công chèn mã CSRF

14. Đâu là dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng?

A Lỗi thiết kế
B Lỗi quản trị
C Lỗi tràn bộ đệm
D Lỗi cấu hình

15. Đâu là một trong các biện pháp phòng chống tấn công khai thác lỗi tràn bộ đệm?

A Sử dụng các kỹ thuật mật mã
B Sử dụng cơ chế cấm thực hiện mã trong dữ liệu
C Sử dụng công nghệ xác thực mạnh
D Sử dụng tường lửa

16. Để đảm bảo an toàn cho hệ thống điều khiển truy cập, một trong các biện pháp phòng chống hiệu quả là:

A Không mở các email của người lạ hoặc email quảng cáo
B Không cài đặt và chạy các chương trình tải từ các nguồn không tin cậy
C Không cho phép chạy các chương trình điều khiển từ xa
D Không dùng tài khoản có quyền quản trị để chạy các chương trình ứng dụng

17. Hệ thống thông tin là:

A. Một hệ thống gồm các thành phần phần mềm nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin, tri thức và các sản phẩm số

B. Một hệ thống gồm các thành phần phần cứng nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin, tri thức và các sản phẩm số

C. Một hệ thống gồm các thành phần phần cứng và phần mềm nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin

D. Một hệ thống tích hợp các thành phần nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin, tri thức và các sản phẩm số

18. Khi khai thác lỗi tràn bộ đệm, tin tặc thường chèn mã độc, gây tràn và ghi đè để sửa đổi thành phần nào sau đây của bộ nhớ Ngăn xếp để chuyển hướng nhằm thực hiện mã độc của mình:

A. Các biến đầu vào của hàm

B. Bộ đệm hoặc biến cục bộ của hàm

C. Con trỏ khung ngăn xếp (sfp)

D. Địa chỉ trở về của hàm

19. Lỗ hổng bảo mật (Security vulnerability) là một điểm yếu tồn tại trong một hệ thống cho phép tin tặc:

A. Khai thác nhằm chiếm quyền điều khiển hệ thống

B. Khai thác, tấn công phá hoại và gây tê liệt hệ thống

C. Khai thác nhằm đánh cắp các thông tin trong hệ thống

D. Khai thác gây tổn hại đến các thuộc tính an ninh của hệ thống đó

20. Lỗi tràn bộ đệm là lỗi trong khâu:

A. Quản trị phần mềm

B. Lập trình phần mềm

C. Thiết kế phần mềm

D. Kiểm thử phần mềm

21. Mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin thường gồm các lớp:

A. An ninh tổ chức, An ninh mạng và An toàn hệ điều hành và ứng dụng

B. An ninh tổ chức, Tường lửa và Điều khiển truy cập

C. An ninh tổ chức, An ninh mạng và Điều khiển truy cập

D. An ninh tổ chức, An ninh mạng và An ninh hệ thống

22. Một điểm yếu điển hình trong hệ thống điều khiển truy cập là việc sử dụng mật khẩu dễ đoán hoặc mật khẩu được lưu ở dạng rõ. Đây là điểm yếu thuộc khâu:

A Trao quyền
B Xác thực
C Quản trị
D Xác thực và Trao quyền

23. Một thông điệp có nội dung nhạy cảm truyền trên mạng bị sửa đổi. Các thuộc tính an toàn thông tin nào bị vi phạm?

A Toàn vẹn
B Bí mật, Toàn vẹn và Sẵn dùng
C Bí mật và Toàn vẹn
D Bí mật

24. Một trong các biện pháp cụ thể cho quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống là:

A Định kỳ nâng cấp hệ thống phần mềm
B Định kỳ nâng cấp hệ thống phần cứng
C Định kỳ cập nhật các bản vá và nâng cấp hệ điều hành
D Định kỳ cập nhật thông tin về các lỗ hổng từ các trang web chính thức

25. Một trong các nội dung rất quan trọng của quản lý an toàn thông tin là:

A Quản lý hệ điều hành
B Quản lý hệ thống
C Quản lý rủi ro
D Quản lý các ứng dụng

26. Người sử dụng hệ thống thông tin quản lý trong mô hình 4 loại hệ thống thông tin là:

A Nhân viên
B Quản lý bộ phận
C Quản lý cao cấp
D Giám đốc điều hành

27. Nguy cơ bị tấn công từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS) thường gặp ở vùng nào trong 7 vùng cơ sở hạ tầng CNTT?

A Vùng mạng WAN
B Vùng máy trạm
C Vùng mạng LAN-to-WAN
D Vùng mạng LAN

28. Nguyên nhân của sự tồn tại các điểm yếu trong hệ thống có thể do:

A Lỗi cấu hình hoạt động

B Lỗi quản trị

C Tất cả các khâu trong quá trình phát triển và vận hành

D Lỗi thiết kế, lỗi cài đặt và lập trình

29. Nguyên tắc cơ bản cho đảm bảo an toàn thông tin, hệ thống và mạng là:

A Cần mua sắm và lắp đặt nhiều thiết bị an ninh chuyên dụng

B Phòng vệ nhiều lớp có chiều sâu

C Cân bằng giữa tính hữu dụng, chi phí và tính năng

D Cần đầu tư trang thiết bị và chuyên gia đảm bảo an toàn

30. Quản lý các bản vá và cập nhật phần mềm là phần việc thuộc lớp bảo vệ nào trong mô hình tổng thể đảm bảo an toàn hệ thống thông tin?

A Lớp an ninh hệ điều hành và phần mềm

B Lớp an ninh hệ thống

C Lớp an ninh mạng

D Lớp an ninh cơ quan/tổ chức

31. Tại sao cần phải đảm bảo an toàn cho thông tin?

A Do có quá nhiều nguy cơ tấn công mạng

B Do có quá nhiều phần mềm độc hại

C Do có nhiều thiết bị kết nối mạng Internet

D Do có nhiều thiết bị kết nối mạng Internet với nhiều nguy cơ và đe dọa

32. Tìm phát biểu đúng trong các phát biểu sau:

A Điểm yếu hệ thống chỉ xuất hiện trong các mô đun phần cứng

B Điểm yếu chỉ xuất hiện khi hệ thống bị tấn công

C Điểm yếu hệ thống chỉ xuất hiện trong các mô đun phần mềm

D Điểm yếu hệ thống có thể xuất hiện trong cả các mô đun phần cứng và phần mềm

33. Tính bí mật của thông tin có thể được đảm bảo bằng:

A Các kỹ thuật mã hóa

B Bảo vệ vật lý

C Sử dụng VPN

D Bảo vệ vật lý, VPN, hoặc mã hóa

34. Trong 7 vùng của cơ sở hạ tầng CNTT, vùng nào có nhiều mối đe dọa và nguy cơ nhất?

A Vùng truy nhập từ xa
B Vùng mạng LAN
C Vùng người dùng
D Vùng mạng WAN/Internet

35. Trong tấn công khai thác lỗi tràn bộ đệm, tin tặc thường sử dụng một số lệnh NOP (No Operation) ở phần đầu của mã tấn công. Mục đích của việc này là để:

A Tăng khả năng mã tấn công được thực hiện
B Tăng khả năng phá hoại của mã tấn công
C Tăng khả năng gây lỗi chương trình
D Tăng khả năng gây tràn bộ đệm

36. Trong tấn công khai thác lỗi tràn bộ đệm, tin tặc thường sử dụng shellcode. Shellcode đó là dạng:

A Mã Java
B Mã Hợp ngữ
C Mã máy
D Mã C/C++

37. Việc quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống cần được thực hiện theo nguyên tắc chung là:

A Cân bằng giữa An toàn, Tin cậy và Rẻ tiền
B Cân bằng giữa An toàn, Rẻ tiền và Chất lượng
C Cân bằng giữa An toàn, Hữu dụng và Rẻ tiền
D Cân bằng giữa An toàn, Hữu dụng và Tin cậy

38. Việc thực thi quản lý ATTT cần được thực hiện theo chu trình lặp lại là do

A Trình độ cao của tin tặc và công cụ tấn công ngày càng phổ biến
B Số lượng và khả năng phá hoại của các phần mềm độc hại ngày càng tăng
C Máy tính, hệ điều hành và các phần mềm được nâng cấp nhanh chóng
D Các điều kiện bên trong và bên ngoài hệ thống thay đổi theo thời gian

39. Sâu SQL Slammer được phát hiện vào năm nào?

A 2002
B 1997
C 2007
D 2003

40. Trong các vùng hạ tầng CNTT, vùng nào dễ bị tấn công DoS, DDoS nhất?

A Vùng người dùng
B Vùng mạng LAN
C Vùng mạng WAN
D Vùng mạng LAN-to-WAN

41. Trong các vùng hạ tầng CNTT, vùng nào có các lỗ hổng trong các phần mềm ứng dụng của máy chủ?

A Vùng máy trạm
B Vùng mạng LAN-to-WAN
C Vùng truy nhập từ xa
D Vùng mạng LAN

42. Trong các vùng hạ tầng CNTT, vùng nào có các lỗ hổng trong quản lý phần mềm ứng dụng của máy chủ?

A Vùng máy trạm
B Vùng mạng LAN-to-WAN
C Vùng truy nhập từ xa
D Vùng hệ thống và ứng dụng

43. Tìm phát biểu đúng trong các phát biểu sau:

A Mối đe dọa là bất kỳ một hành động tấn công nào vào hệ thống mạng
B Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống
C Mối đe dọa là bất kỳ một hành động tấn công nào vào hệ thống máy tính
D Mối đe dọa là bất kỳ một hành động tấn công nào vào hệ thống máy tính và mạng

44. Sâu SQL Slammer tấn công khai thác lỗi tràn bộ đệm trong hệ quản trị cơ sở dữ liệu:

A SQL Server 2012
B SQL Server 2000
C SQL Server 2008
D SQL Server 2003

Answer Key

1. d	2. d	3. d	4. c
5. b	6. c	7. c	8. d
9. d	10. d	11. b	12. c
13. c	14. c	15. b	16. d
17. d	18. d	19. d	20. b
21. d	22. b	23. c	24. c
25. c	26. b	27. a	28. d
29. b	30. b	31. d	32. d
33. d	34. c	35. a	36. c
37. c	38. d	39. d	40. c
41. d	42. d	43. b	44. b