Quizizz bảng tính

Tên

ATBMHTTT_PTIT_Chương 1 &2 (Tổng quan & Các dạng tấn công)

Lớp học

Tổng số câu hỏi: 44

Thời gian làm bài: 16phút

Ngày

Tên người hướng dẫn: Ngọ Văn Trọng

☑ Nhiều lựa chọn

1. An toàn hệ thống thông tin là:

a) Việc đảm bảo cho hệ thống thông tin hoạt động trơn tru, ổn định

b) Việc đảm bảo thông tin trong hệ thống không bị đánh cắp

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

☑ Nhiều lựa chọn

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

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

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

c) Là việc phòng chống đánh cắp thông tin

d) Là việc phòng chống tấn công mạng

☑ Nhiều lựa chọn

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

a) An toàn máy tính và An toàn Internet

b) An toàn máy tính và An ninh mạng

c) An ninh mạng và An toàn hệ thống

d) An toàn công nghệ thông tin và Đảm bảo thông tin

☑ Nhiều lựa chọn

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) Sử dụng công cụ gỡ rối để ngăn chặn tràn trong thời gian vận hành
c) Kiểm tra mã nguồn để tìm điểm có khả năng gây tràn và khắc phục
d) Đặt cơ chế không cho phép thực hiện mã trong dữ liệu (DEP)

☑ Nhiều lựa chọn

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

a) Điều khiển truy nhập, tường lửa, proxy và các giao thức bảo mật, ứng dụng dựa trên mật mã
b) VPN, SSL/TLS, PGP
c) Tường lửa, proxy
d) Điều khiển truy nhập

☑ Nhiều lựa chọn

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 mạng WAN
c) Vùng mạng LAN
d) Vùng máy trạm

☑ Nhiều lựa chọn

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

a) Các dịch vụ mạng
b) Các thành phần phần cứng
c) Hệ điều hành
d) Các ứng dụng

☑ Nhiều lựa chọn

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

a) CPU, Bộ nhớ, HDD và Hệ thống bus truyền dẫn
b) Hệ thống phần cứng và Hệ thống phần mềm
c) CPU, hệ điều hành và các ứng dụng
d) CPU, Bộ nhớ, HDD, hệ điều hành và các ứng dụng

☑ Nhiều lựa chọn

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 và dữ liệu, An ninh mạng, Quản lý ATTT và Chính sách ATTT

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

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

☑ Nhiều lựa chọn

10. Các vùng bộ nhớ thường bị tràn gồm:

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

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

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

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

☑ Nhiều lựa chọn

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

a) Bảo mật, Toàn vẹn và Sẵn dùng

b) Bảo mật, Toàn vẹn và Khả dụng

c) Bí mật, Toàn vẹn và Không chối bỏ

d) Bí mật, Toàn vẹn và Sẵn dùng

☑ Nhiều lựa chọn

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 ngoại vi

c) Sử dụng kỹ thuật tạo dự phòng ra đĩa cứng

d) Sử dụng kỹ thuật tạo dự phòng ra băng từ

☑ Nhiều lựa chọn

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 HTML

b) Tấn công chèn mã XSS

c) Tấn công chèn mã SQL

d) Tấn công chèn mã CSRF

☑ Nhiều lựa chọn

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

a) Lỗi tràn bộ đệm
b) Lỗi quản trị
c) Lỗi cấu hình
d) Lỗi thiết kế

☑ Nhiều lựa chọn

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

a) Sử dụng tường lửa
b) Sử dụng cơ chế cấm thực hiện mã trong dữ liệu
c) Sử dụng công nghệ xác thực mạnh
d) Sử dụng các kỹ thuật mật mã

☑ Nhiều lựa chọn

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 cài đặt và chạy các chương trình tải từ các nguồn không tin cậy
b) Không mở các email của người lạ hoặc email quảng cáo
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

☑ Nhiều lựa chọn

17. Hệ thống thông tin là:

a) 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
b) 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
c) 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
d) 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

☑ Nhiều lựa chọn

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) Con trỏ khung ngăn xếp (sfp)
b) Bộ đệm hoặc biến cục bộ của hàm
c) Địa chỉ trở về của hàm
d) Các biến đầu vào của hàm

☑ Nhiều lựa chọn

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

a) Khai thác, tấn công phá hoại và gây tê liệt hệ thống
b) Khai thác nhằm đánh cắp các thông tin trong hệ thống
c) Khai thác nhằm chiếm quyền điều khiển hệ thống
d) Khai thác gây tổn hại đến các thuộc tính an ninh của hệ thống đó

☑ Nhiều lựa chọn

20. Lỗi tràn bộ đệm là lỗi trong khâu:

a) Kiểm thử phần mềm
b) Quản trị phần mềm
c) Thiết kế phần mềm
d) Lập trình phần mềm

☑ Nhiều lựa chọn

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, Tưởng lửa và Điều khiển truy cập
b) An ninh tổ chức, An ninh mạng và An ninh hệ thống
c) An ninh tổ chức, An ninh mạng và An toàn hệ điều hành và ứng dụng
d) An ninh tổ chức, An ninh mạng và Điều khiển truy cập

☑ Nhiều lựa chọn

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) Xác thực
b) Xác thực và Trao quyền
c) Trao quyền
d) Quản trị

☑ Nhiều lựa chọn

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) Bí mật và Toàn vẹn
b) Bí mật
c) Toàn vẹn
d) Bí mật, Toàn vẹn và Sẵn dùng

☑ Nhiều lựa chọn

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 cập nhật các bản vá và nâng cấp hệ điều hành
b) Định kỳ cập nhật thông tin về các lỗ hổng từ các trang web chính thức
c) Định kỳ nâng cấp hệ thống phần mềm
d) Định kỳ nâng cấp hệ thống phần cứng

☑ Nhiều lựa chọn

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

a) Quản lý rủi ro
b) Quản lý hệ thống
c) Quản lý hệ điều hành
d) Quản lý các ứng dụng

☑ Nhiều lựa chọn

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

a) Nhân viên
b) Giám đốc điều hành
c) Quản lý bộ phận
d) Quản lý cao cấp

☑ Nhiều lựa chọn

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 LAN
b) Vùng mạng WAN
c) Vùng máy trạm
d) Vùng mạng LAN-to-WAN

☑ Nhiều lựa chọn

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

a) Lỗi cấu hình hoạt động
b) Lỗi thiết kế, lỗi cài đặt và lập trình
c) Lỗi quản trị
d) Tất cả các khâu trong quá trình phát triển và vận hành

☑ Nhiều lựa chọn

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

a) Cần đầu tư trang thiết bị và chuyên gia đảm bảo an toàn
b) Phòng vệ nhiều lớp có chiều sâu
c) Cân bằng giữa tính hữu dụng, chi phí và tính năng
d) Cần mua sắm và lắp đặt nhiều thiết bị an ninh chuyên dụng

☑ Nhiều lựa chọn

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 cơ quan/tổ chức
b) Lớp an ninh hệ điều hành và phần mềm
c) Lớp an ninh hệ thống
d) Lớp an ninh mạng

☑ Nhiều lựa chọn

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

a) Do có nhiều thiết bị kết nối mạng Internet
b) Do có quá nhiều nguy cơ tấn công mạng
c) Do có nhiều thiết bị kết nối mạng Internet với nhiều nguy cơ và đe dọa
d) Do có quá nhiều phần mềm độc hại

☑ Nhiều lựa chọn

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 hệ thống có thể xuất hiện trong cả các mô đun phần cứng và phần mềm
c) Điểm yếu hệ thống chỉ xuất hiện trong các mô đun phần mềm
d) Điểm yếu chỉ xuất hiện khi hệ thống bị tấn công

☑ Nhiều lựa chọn

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

a) Bảo vệ vật lý, VPN, hoặc mã hóa
b) Sử dụng VPN
c) Các kỹ thuật mã hóa
d) Bảo vệ vật lý

☑ Nhiều lựa chọn

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 người dùng
c) Vùng mạng LAN
d) Vùng mạng WAN/Internet

☑ Nhiều lựa chọn

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 gây tràn bộ đệm
b) Tăng khả năng phá hoại của mã tấn công
c) Tăng khả năng gây lỗi chương trình
d) Tăng khả năng mã tấn công được thực hiện

☑ Nhiều lựa chọn

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

a) Mã Hợp ngữ
b) Mã Java
c) Mã C/C++
d) Mã máy

☑ Nhiều lựa chọn

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 Tin cậy
d) Cân bằng giữa An toàn, Hữu dụng và Rẻ tiền

☑ Nhiều lựa chọn

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

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

☑ Nhiều lựa chọn

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

a) 1997
b) 2003
c) 2002
d) 2007

☑ Nhiều lựa chọn

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

a) Vùng mạng LAN
b) Vùng mạng WAN
c) Vùng người dùng
d) Vùng mạng LAN-to-WAN

☑ Nhiều lựa chọn

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

a) Vùng truy nhập từ xa
b) Vùng máy trạm
c) Vùng mạng LAN
d) Vùng mạng LAN-to-WAN

☑ Nhiều lựa chọn

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 mạng LAN-to-WAN
b) Vùng hệ thống và ứng dụng
c) Vùng truy nhập từ xa
d) Vùng máy trạm

☑ Nhiều lựa chọn

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 máy tính

b) Mối đe dọa là bất kỳ một hành động tấn công nào vào hệ thống máy tính và mạng

c) Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống

d) Mối đe dọa là bất kỳ một hành động tấn công nào vào hệ thống mạng

☑ Nhiều lựa chọn

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

a) SQL Server 2003

b) SQL Server 2000

c) SQL Server 2008

d) SQL Server 2012

Phím trả lời

1. d) Việc đảm bảo các thuộc tính an ninh, an toàn của hệ thống thông tin
2. a) Là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép
3. d) An toàn công nghệ thông tin và Đảm bảo thông tin
4. b) Sử dụng công cụ gỡ rối để ngăn chặn tràn trong thời gian vận hành
5. a) Điều khiển truy nhập, tường lửa, proxy và các giao thức bảo mật, ứng dụng dựa trên mật mã
6. c) Vùng mạng LAN
7. d) Các ứng dụng
8. b) Hệ thống phần cứng và Hệ thống phần mềm
9. b) An toàn máy tính và dữ liệu, An ninh mạng, Quản lý ATTT và Chính sách ATTT
10. a) Ngăn xếp (Stack) và Vùng nhớ cấp phát động (Heap)
11. d) Bí mật, Toàn vẹn và Sẵn dùng
12. b) Sử dụng kỹ thuật tạo dự phòng ngoại vi
13. c) Tấn công chèn mã SQL
14. a) Lỗi tràn bộ đệm
15. b) Sử dụng cơ chế cấm thực hiện mã trong dữ liệu
16. d) Không dùng tài khoản có quyền quản trị để chạy các chương trình ứng dụng
17. b) 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. c) Địa chỉ trở về của hàm
19. d) Khai thác gây tổn hại đến các thuộc tính an ninh của hệ thống đó
20. d) Lập trình phần mềm
21. b) An ninh tổ chức, An ninh mạng và An ninh hệ thống
22. a) Xác thực
23. a) Bí mật và Toàn vẹn
24. a) Định kỳ cập nhật các bản vá và nâng cấp hệ điều hành
25. a) Quản lý rủi ro
26. c) Quản lý bộ phận
27. b) Vùng mạng WAN

28. b) Lỗi thiết kế, lỗi cài đặt và lập trình

29. b) Phòng vệ nhiều lớp có chiều sâu

30. c) Lớp an ninh hệ thống

31. c) Do có nhiều thiết bị kết nối mạng Internet với nhiều nguy cơ và đe dọa

32. b) Điểm yếu hệ thống có thể xuất hiện trong cả các mô đun phần cứng và phần mềm

33. a) Bảo vệ vật lý, VPN, hoặc mã hóa

34. b) Vùng người dùng

35. d) Tăng khả năng mã tấn công được thực hiện

36. d) Mã máy

37. d) Cân bằng giữa An toàn, Hữu dụng và Rẻ tiền

38. c) Các điều kiện bên trong và bên ngoài hệ thống thay đổi theo thời gian

39. b) 2003

40. b) Vùng mạng WAN

41. c) Vùng mạng LAN

42. b) Vùng hệ thống và ứng dụng

43. c) Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống

44. b) SQL Server 2000