QUIZIZZ bảng tính

ATBMHTTT_PTIT_Tổng hợp
Tổng số câu hỏi: 271
Thời gian làm bài: 2 giờ 16 phút
Tên người hướng dẫn: Ngọ Văn Trọng

Tên
Lớp học
Ngày

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

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

a) An toàn công nghệ thông tin và Đảm bảo thông tin
b) An toàn máy tính và An toàn Internet
c) An ninh mạng và An toàn hệ thống
d) An toàn máy tính và An ninh mạng

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

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

4. An toàn hệ thống thông tin là:

a) Việc đảm bảo cho hệ thống thông tin không bị tấn công
b) Việc đảm bảo cho hệ thống thông tin hoạt động trơn tru, ổn định
c) Việc đảm bảo thông tin trong hệ thống không bị đánh cắp
d) Việc đảm bảo các thuộc tính an ninh, an toàn của hệ thống thông tin

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

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

6. 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

7. 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

8. 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
b) Toàn vẹn
c) Bí mật và Toàn vẹn
d) Bí mật, Toàn vẹn và sẵn dùng

9. 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 mạng LAN-to-WAN
d) Vùng máy trạm

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

a) Là việc phòng chống tấn công mạng
b) Là việc phòng chống đánh cắp thông tin
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

11. 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 thông tin về các lỗ hổng từ các trang web chính thức
d) Định kỳ cập nhật các bản vá và nâng cấp hệ điều hành

12. Các mật khẩu nào sau đây là khó phá nhất đối với một hacker ?

a) LaT3r
b) password83
c) reception
d) !$aLtNb83

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

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

a) Điểm yếu chỉ xuất hiện khi hệ thống bị tấn công
b) Điểm yếu hệ thống chỉ xuất hiện trong các mô đun phần cứng
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

15. Người sử dụng hệ thống trợ giúp ra quyết định trong mô hình 4 loại hệ thống thông tin là:

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

16. 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

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

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

18. Trên thực tế, có thể giảm khả năng bị tấn công nếu có thể...

a) Triệt tiêu được hết các mối đe dọa
b) Kiểm soát chặt chẽ người dùng
c) Triệt tiêu được hết các nguy cơ
d) Giảm thiểu các lỗ hổng bảo mật

19. 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 2012
d) SQL Server 2008

20. Trong suốt quá trình kiểm định một bản ghi hệ thống máy chủ, các mục nào sau đây có thể được xem như là một khả năng đe dọa bảo mật ?

a) Ba tập tin mới được lưu trong tài khoản thư mục bởi người sử dụng là “finance”
b) Hai lần login thành công với tài khoản Administrator
c) Năm trăm ngàn công việc in được gởi đến một máy in
d) Năm lần nổ lực login thất bại trên tài khoản “jsmith”

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

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

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

a) An toàn máy tính, An ninh mạng, Quản lý rủi ro ATTT và Chính sách ATTT
b) An toàn máy tính, An ninh mạng, Quản lý ATTT và Chính sách ATTT
c) An toàn máy tính, An toàn dữ liệu, An ninh mạng, Quản lý ATTT
d) An toàn máy tính và dữ liệu, An ninh mạng, Quản lý ATTT và Chính sách ATTT

23. 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 Khả dụng
b) Bí mật, Toàn vẹn và không chối bỏ
c) Bí mật, Toàn vẹn và Sẵn dùng
d) Bảo mật, Toàn vẹn và Sẵn dùng

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

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

25. 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

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

a) Các kỹ thuật mã hóa

b) Bảo vệ vật lý

c) Bảo vệ vật lý, VPN, hoặc mã hóa

d) Sử dụng VPN

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

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

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 cục bộ

28. Lỗi tràn bộ đệm là lỗi trong khâu:

a) Thiết kế phần mềm

b) Quản trị phần mềm

c) Lập trình phần mềm

d) Kiểm thử phần mềm

29. 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 cấu hình

c) Lỗi quản trị

d) Lỗi thiết kế

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 mạng

c) Lớp an ninh hệ thống

d) Lớp an ninh hệ điều hành và phần mềm

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

32. Một trong các mối đe dọa an toàn thông tin thường gặp là:

a) Phần mềm quảng cáo
b) Phần mềm phá mã
c) Phần mềm độc hại
d) Phần mềm nghe lén

33. Trong các vùng hạ tầng CNTT, vùng nào có nhiều mối đe dọa nguy cơ nhất?

a) vùng mạng LAN
b) vùng người dùng
c) vùng máy trạm
d) vùng mạng LAN-to-WAN

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

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

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

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

36. 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, Hữu dụng và Tin cậy
c) Cân bằng giữa An toàn, Rẻ tiền và Chất lượng
d) Cân bằng giữa An toàn, Hữu dụng và Rẻ tiền

37. Các mối nguy cơ đe dọa thường trực là:

a) Mất thông tin và các phầm mềm nghe lén.
b) Tin tặc và các phần mềm độc hại
c) Phần cứng và phần mềm độc hại.
d) Các phần mềm độc hại.

38. Người sử dụng hệ thống thông tin điều hành trong mô hình 4 loại hệ thống thông tin là:

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

39. Các phần của hệ thống thông tin dựa trên máy tính là:

a) Phần cứng (Hardware), phần mềm (Software), dữ liệu (Data), bảo vệ (Security), hệ thống mạng (Networks), tập các lệnh kết hợp (Procedures).
b) Phần cứng (Hardware), phần mềm (Software), cơ sở dữ liệu (Databases), mạng riêng ảo (VPN), tập các lệnh kết hợp (Procedures).
c) Phần cứng (Hardware), phần mềm (Software), người dùng (Actor), hệ thống mạng (Networks), tập các lệnh kết hợp (Procedures).
d) Phần cứng (Hardware), phần mềm (Software), cơ sở dữ liệu (Databases), hệ thống mạng (Networks), tập các lệnh kết hợp (Procedures).

40. Công thức tính tỉ lệ tính sẵn dùng:

a) A = (Uptime)/(Uptime + Downtime).
b) A = (Uptime)/(Loadtime + Downtime).
c) A = (Uptime)/(Uptime + Loadtime).
d) A = (Uptime)/(Uptime + Downtime + Loadtime).

41. Các bước thực thi quản lí ATTT:

a) Lập kế hoạch (Plan), Thực thi kế hoạch (Do), Thực hiện kiểm tra (Check), Thực hiện các kiểm soát (Control).
b) Lập kế hoạch (Plan), Thực thi kế hoạch (Do), Giám sát kết quả thực hiện (Monitor), Thực hiện kiểm tra (Check).
c) Lập kế hoạch (Plan), Thực thi kế hoạch (Do), Thực hiện kiểm tra (Check), Hành động (Act).
d) Lập kế hoạch (Plan), Thực thi kế hoạch (Do), Giám sát kết quả thực hiện (Monitor), Thực hiện các kiểm soát (Control).

42. Chính sách an toàn thông tin không bao gồm:

a) Chính sách an toàn ở mức tổ chức (Organizational security policy)
b) Chính sách an toàn ở mức logic (Logical security policy)
c) Chính sách an toàn ở mức người dùng (User security policy).
d) Chính sách an toàn ở mức vật lý (Physical security policy)

43. Tính toàn vẹn liên quan đến ... và ... của dữ liệu.

a) tính hợp lệ (validity) ... sự chính xác (accuracy).

b) tính hợp lệ (validity) ... sự chính xác (rigorous).

c) sự hợp pháp (legalization) ... sự chính xác (rigorous).

d) sự hợp pháp (legalization) ... sự chính xác (accuracy).

44. Các lớp phòng vệ điển hình để đảm bảo ATTT và an toàn HTTT:

a) Lớp bảo vệ vật lý (Physical Security), Lớp an ninh mạng (Network Security), Lớp an ninh hệ thống (System Integrity).

b) Lớp an ninh cơ quan/tổ chức (Plant Security), Lớp an ninh mạng (Network Security), Lớp an ninh hệ thống (System Security).

c) Lớp an ninh cơ quan/tổ chức (Plant Security), Lớp mạng riêng ảo (Virtual Private Network), Lớp an ninh hệ thống (System Integrity).

d) Lớp an ninh cơ quan/tổ chức (Plant Security), Lớp an ninh mạng (Network Security), Lớp an ninh hệ thống (System Integrity).

45. Các đe dọa với tầng người dùng bao gồm:

a) Coi nhẹ hoặc vi phạm các chính sách an ninh an toàn; thăm dò và rà quét trái phép các cổng dịch vụ; thiếu ý thức về vấn đề an ninh an toàn.

b) Đưa CD/DVD/USB với các files cá nhân vào hệ thống; người dùng tải ảnh, âm nhạc, video; nguy cơ từ người dùng giả mạo trong mạng WLAN.

c) Coi nhẹ hoặc vi phạm các chính sách an ninh an toàn; đưa CD/DVD/USB với các files cá nhân vào hệ thống; thiếu ý thức về vấn đề an ninh an toàn.

d) Đưa CD/DVD/USB với các files cá nhân vào hệ thống; người dùng tải ảnh, âm nhạc, video; truy nhập trái phép vào máy trạm.

46. Trong các vùng hạ tầng CNTT, vùng nào dễ bị tấn công kiểu vét cạn (brute force) nhất?

a) vùng mạng LAN-to-WAN.

b) vùng người dùng

c) vùng truy cập từ xa

d) vùng hệ thống/ứng dụng

47. Các đe dọa với vùng máy trạm bao gồm:

a) Coi nhẹ hoặc vi phạm các chính sách an ninh an toàn; đưa CD/DVD/USB với các files cá nhân vào hệ thống; thiếu ý thức về vấn đề an ninh an toàn.

b) Đưa CD/DVD/USB với các files cá nhân vào hệ thống; người dùng tải ảnh, âm nhạc, video; truy nhập trái phép vào máy trạm.

c) Đưa CD/DVD/USB với các files cá nhân vào hệ thống; người dùng tải ảnh, âm nhạc, video; nguy cơ từ người dùng giả mạo trong mạng WLAN.

d) Coi nhẹ hoặc vi phạm các chính sách an ninh an toàn; thăm dò và rà quét trái phép các cổng dịch vụ; thiếu ý thức về vấn đề an ninh an toàn.

48. Người sử dụng Hệ thống xử lý giao dịch trong mô hình 4 loại hệ thống thông tin là:

a) Quản lý cao cấp

b) Nhân viên

c) Quản lý bộ phận

d) Giám đốc điều hành

49. Đâu là 1 lớp phòng vệ an ninh mạng:

a) Lớp quản trị tài khoản và phân quyền người dùng.

b) Tường lửa, mạng riêng ảo (VPN).

c) Lớp chính sách & thủ tục đảm bảo ATTT.

d) Lớp phát hiện và ngăn chặn phần mềm độc hại.

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

a) Sử dụng cơ chế cấm thực hiện mã trong dữ liệu

b) Sử dụng các kỹ thuật mật mã

c) Sử dụng tường lửa

d) Sử dụng công nghệ xác thực mạnh

51. 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

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

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

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 cứng

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

53. 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)

54. Lỗ hổng an ninh trong một hệ thống là:

a) Bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại
b) Tất cả điểm yếu hoặc khiếm khuyết trong hệ thống
c) Các điểm yếu trong các phần mềm ứng dụng
d) Các điểm yếu trong hệ điều hành

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

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

56. Trên thực tế, có thể giảm khả năng bị tấn công nếu có thể...

a) Triệt tiêu được hết các nguy cơ
b) Triệt tiêu được hết các mối đe dọa
c) Kiểm soát chặt chẽ người dùng
d) Giảm thiểu các lỗ hổng bảo mật

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

a) SQL Server 2008
b) SQL Server 2003
c) SQL Server 2012
d) SQL Server 2000

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

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

59. 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++

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

a) Khai thác gây tổn hại đến các thuộc tính an ninh của hệ thống đó
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 nhằm chiếm quyền điều khiển hệ thống

61. Lỗi tràn bộ đệm là lỗi trong khâu:

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

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

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

63. Loại tấn công nào sau đây chiếm quyền truy nhập đến tài nguyên lợi dụng cơ chế điều khiển truy nhập DAC?

a) Phishing
b) Spoofing
c) Trojan horse
d) Man in the middle

64. Đâu là tên viết đúng của Hệ thống phát hiện đột nhập/xâm nhập?

a) Intrusion Detection System
b) Intrusion Detector System
c) Intrusion Detecting System
d) Instruction Detection System

65. Mức độ nghiêm trọng chia Microsoft là

a) Cao, Quan trọng, Trung bình, Không quan trọng
b) Nguy hiểm, Cao, Trung bình, Thấp
c) Cao, Trung bình, Thấp, Yếu
d) Nguy hiểm, Quan trọng, Trung bình, Thấp

66. Tác hại của lỗi tràn bộ đệm là:

a) Có thể khiến cho ứng dụng ngừng hoạt động, gây mất dữ liệu hoặc thậm chí giúp kẻ tấn công kiểm soát hệ thống
b) Gây mất dữ liệu của người dùng
c) Chiếm quyền kiểm soát và phá hỏng hệ thống
d) Khiến chương trình ngừng hoạt động

67. Đâu không phải là một trong các biện pháp phòng chống lỗi không kiểm tra đầu vào

a) Kiểm tra tất cả các dữ liệu đầu vào, đặc biệt dữ liệu nhập từ người dùng và từ các nguồn không tin cậy
b) Không dùng user quản trị (root hoặc admin) để chạy các chương trình ứng dụng
c) Kiểm tra sự hợp lý của nội dung dữ liệu
d) Tạo các bộ lọc để lọc bỏ các ký tự đặc biệt và các từ khóa của các ngôn ngữ trong các trường hợp cần thiết mà kẻ tấn công có thể sử dụng

68. Các dạng dữ liệu cần kiểm tra là

a) Các file âm thanh, hình ảnh, hoặc đồ họa do người dùng hoặc các tiến trình khác cung cấp
b) Các trường dữ liệu text
c) Các dữ liệu từ mạng hoặc các nguồn không tin cậy
d) Các dữ liệu được đưa ra bởi hệ thống

69. Kẻ tấn công có thể kiểm tra tất cả các ... đầu vào và thử tất cả các ... có thể khai thác được

a) Bước / Phương thức
b) Dữ liệu / Khả năng
c) Bước / Khả năng
d) Dữ liệu / Phương thức

70. Khi kiểm soát truy cập bị lỗi, một người dùng bình có thể ... của người quản trị và có toàn quyền truy nhập vào hệ thống

a) Đưa quyền
b) Xin quyền
c) Mượn quyền
d) Đoạt quyền

71. Đâu không phải là phương pháp phòng chống lỗ hổng điều khiển truy cập

a) Không dùng user quản trị (root hoặc admin) để chạy các chương trình ứng dụng
b) Sử dụng các công cụ phân tích mã tự động tìm các điểm có khả năng xảy ra lỗi
c) Kiểm soát chặt chẽ người dùng, xóa bỏ hoặc cấm truy nhập với những người dùng ngầm định kiểu everyone
d) Luôn chạy các chương trình ứng dụng với quyền tối thiểu – vừa đủ để thực thi các tác vụ

72. Đâu không phải là 1 vấn đề xảy với cơ chế xác thực

a) Sử dụng cơ chế xác thực không đủ mạnh
b) Sử dụng mật khẩu đơn giản, dễ đoán, hoặc dùng mật khẩu trong thời gian dài
c) Chọn mật khẩu đủ mạnh để sử dụng
d) Mật khẩu được lưu dưới dạng rõ (plain text)

73. Đâu là một thao tác an toàn đối với file

a) Không kiểm tra chính xác loại file, định danh thiết bị, các links hoặc các thuộc tính khác của file trước khi sử dụng
b) Thực hiện đọc/ghi file lưu ở những nơi mà các người dùng khác cũng có thể ghi file đó
c) Không kiểm tra mã trả về sau mỗi thao tác với file
d) Sử dụng mật khẩu và quyền phù hợp để truy cập

74. Đâu không phải là 1 biện pháp khắc phục và tăng cường khả năng để kháng cho hệ thống

a) Sử dụng các biện pháp phòng vệ ở lớp ngoài như tường lửa, proxies
b) Cần có chính sách quản trị người dùng, mật khẩu và quyền truy nhập chặt chẽ ở mức hệ điều hành và mức ứng dụng
c) Thường xuyên cập nhật thông tin về các điểm yếu, lỗ hổng bảo mật từ các trang web chính thức
d) Người dùng được quyền truy nhập vào mọi tác vụ của hệ thống

75. Một điều kiện đua tranh tồn tại khi có sự thay đổi ... của 2 hay một số sự kiện gây ra sự thay đổi ... của hệ thống

a) Trật tự / Hành vi
b) Vị trí / Quá trình
c) Trật tự / Quá trình
d) Vị trí / Hành vi

76. Các loại điểm yếu của hệ thống là

a) Có điểm yếu đã biết và chưa được khắc phục
b) Có điểm yếu đã biết và đã được khắc phục
c) Có điểm yếu chưa biết/chưa được phát hiện
d) Tất cả các đáp

77. Một trong các dạng lỗ hổng thường gặp trong hệ điều hành và các phần mềm ứng dụng là

a) DDos
b) SYN floods
c) Buffer Overflows
d) Worms

78. Trong điểm yếu bảo mật do các điều kiện tranh đua, Kẻ tấn công có thể lợi dụng ... giữa 2 sự kiện để ..., đổi tên file hoặc can thiệp vào quá trình hoạt động bình thường của hệ thống

a) Khoảng cách / Thay đổi biến
b) Khoảng thời gian / Thay đổi biến
c) Khoảng thời gian / Chèn mã độc
d) Khoảng cách / Chèn mã độc

79. Các lỗ hổng bảo mật trên hệ thống là do

a) Dịch vụ cung cấp
b) Con người tạo ra
c) Bản thân hệ điều hành
d) Tất cả đều đúng

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

a) Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống.
b) Mối đe dọa là bất kỳ một hành động tấn công nào vào hệ thống máy tính.
c) Mối đe dọa là bất kỳ một hành động tấn công nào vào hệ thống mạng.
d) Mối đe dọa là bất kỳ một hành động tấn công nào vào hệ thống máy tính và mạng.

81. Khác biệt cơ bản của vi rút và sâu là:

a) Sâu Có khả năng phá hoại lớn lơn
b) Vi rút có khả năng tự lây lan mà không cần tương tác của người dùng
c) Sâu có khả năng tự lây lan mà không cần tương tác của người dùng
d) Vi rút có khả năng phá hoại lớn lớn

82. Dạng tấn công gây ngắt quãng dịch vụ hoặc kênh truyền thông cho người dùng bình thường là:

a) Fabrications
b) Interruptions
c) Modifications
d) Interceptions

83. Tấn công nghe lén là kiểu tấn công:

a) Thụ động
b) Chiếm quyền điều khiển
c) Chủ động và bị động
d) Chủ động

84. Dạng tấn công chặn bắt thông tin truyền trên mạng để sửa đổi hoặc lạm dụng là:

a) Fabrications
b) Interruptions
c) Modifications
d) Interceptions

85. Có thể phòng chống tấn công Smurf bằng cách cấu hình các máy và router không trả lời...

a) Các yêu cầu TCP hoặc các yêu cầu phát quảng bá
b) Các yêu cầu ICMP hoặc các yêu cầu phát quảng bá
c) Các yêu cầu UPD hoặc các yêu cầu phát quảng bá
d) Các yêu cầu HTTP hoặc các yêu cầu phát quảng bá

86. Đâu là một kỹ thuật tấn công Dos?

a) Smurf
b) DNS spoofing
c) DNS Cache Poisoning
d) UDP Ping

87. Dạng tấn công giả mạo thông tin thường để đánh lừa người dùng thông thường là:

a) Fabrications
b) Modifications
c) Interceptions
d) Interruptions

88. Kỹ thuật tấn công Smurf sử dụng giao thức ICMP và Cơ chế gửi...

a) Broadcast
b) Multicast
c) Unicast
d) Anycast

89. Pharming là kiểu tấn công vào...

a) Máy chủ cơ sở dữ liệu của trang web
b) Máy chủ web
c) Máy khách/trình duyệt web
d) Máy chủ và máy khách web

90. Đây là một công cụ kiểm tra lỗ hổng tấn công chèn mã SQL trên các website:

a) SQL Server
b) SQLite
c) SQLCheck
d) SQLmap

91. Khác biệt cơ bản giữa tấn công DoS và DDoS là:

a) Phạm vi tấn công
b) Kỹ thuật tấn công
c) Mức độ gây hại
d) Tần suất tấn công

92. Các máy tính ma/máy tính bị chiếm quyền điều khiển thường được tin tặc sử dụng để...

a) Đánh cắp dữ liệu từ máy chủ cơ sở dữ liệu
b) Thực hiện tấn công tràn bộ đệm.
c) Gửi thư rác, thư quảng cáo
d) Gửi các yêu cầu tấn công chèn mã

93. Trong dạng tấn công vào mật khẩu dựa trên từ điển, tin tặc đánh cắp mật khẩu của người dùng bằng cách:

a) Vét cận các mật khẩu có thể có
b) Lắng nghe trên đường truyền để đánh cắp mật khẩu
c) Thử các từ có tần suất sử dụng cao làm mật khẩu trong từ điển
d) Tìm mật khẩu trong từ điển các mật khẩu

94. Một trong các phương thức lây lan thường gặp của sâu mạng là:

a) Lây lan thông qua sao chép các file
b) Lây lan thông qua khả năng thực thi từ xa
c) Lây lan thông qua dịch vụ POP
d) Lây lan thông qua Microsoft Office

95. Đây là một kỹ thuật tấn công Dos?

a) DNS spoofing
b) Ping of death
c) SYN requests
d) IP spoofing

96. Tấn công từ chối dịch vụ (Dos - Denial of Service Attacks) là dạng tấn công có khả năng...

a) Cản trở người dùng hợp pháp truy nhập các file dữ liệu của hệ thống
b) Gây hư hỏng phần cứng máy chủ
c) Cản trở người dùng hợp pháp truy nhập các tài nguyên hệ thống
d) Đánh cắp dữ liệu trong hệ thống

97. Mật khẩu an toàn trong thời điểm hiện tại là mật khẩu có:

a) Chứa các ký tự từ nhiều dạng ký tự
b) Khả năng chống tấn công phát lại và chứa các ký tự từ nhiều dạng ký tự
c) Độ dài từ 8 ký tự trở lên, gồm chữ cái hoa, thường, chữ số và ký tự đặc biệt
d) Độ dài lớn hơn hoặc bằng 8 ký tự

98. Nguy cơ cao nhất mà một cuộc tấn công chèn mã SQL có thể gây ra cho một hệ thống là:

a) Đánh cắp các thông tin trong cơ sở dữ liệu
b) Chèn, xóa hoặc sửa đổi dữ liệu
c) Vượt qua các khâu xác thực người dùng
d) Chiếm quyền điều khiển hệ thống

99. Một trong các biện pháp có thể sử dụng để phòng chống tấn công kiểu người đứng giữa là:

a) Sử dụng chứng chỉ số để xác thực thông tin nhận dạng các bên
b) Sử dụng tường lửa để ngăn chặn
c) Sử dụng các hệ thống IPS/IDS
d) Sử dụng mã hóa để đảm bảo tính bí mật các thông điệp truyền

100. Macro viruses là loại viruses thường lây nhiễm vào...

a) Các file tài liệu của bộ phần mềm Microsoft Office
b) Các file tài liệu của bộ phần mềm Microsoft Exchange
c) Các file tài liệu của bộ phần mềm Microsoft SQL
d) Các file tài liệu của bộ phần mềm Open Office

101. Tấn công kiểu Social Engineering là dạng tấn công khai thác yếu tố nào sau đây trong hệ thống?

a) Người dùng
b) Máy trạm
c) Máy chủ
d) Hệ điều hành & ứng dụng

102. Câu lệnh SQL nào tin tặc thường sử dụng trong tấn công chèn mã SQL để đánh cắp các thông tin trong cơ sở dữ liệu?

a) INSERT SELECT
b) UNION SELECT
c) UNION INSERT
d) SELECT UNION

103. Phishing là một dạng của loại tấn công sử dụng...

a) Kỹ thuật chèn mã
b) Kỹ thuật xã hội
c) Kỹ thuật giả mạo địa chỉ IP
d) Kỹ thuật gây tràn bộ đệm

104. Các dạng phần mềm độc hại (malware) có khả năng tự nhân bản gồm:

a) Virus, worm, zombie
b) Virus, worm, trojan
c) Virus, trojan, zombie
d) Virus, zombie, spyware

105. Một trong các cách virus thường sử dụng để lây nhiễm vào các chương trình khác là:

a) Xáo trộn mã của virus
b) Thay thế các chương trình
c) Ẩn mã của virus
d) Sửa đổi các chương trình

106. Trong tấn công DDoS phản chiếu hay gián tiếp, có sự tham gia của một số lượng lớn máy chủ trên mạng Internet không bị tin tặc chiếm quyền điều khiển. Các máy chủ này được gọi là...

a) Requesters
b) Injectors
c) Forwarders
d) Reflectors

107. Mục đích chính của tấn công giả mạo địa chỉ IP là:

a) Để vượt qua các hàng rào kiểm soát an ninh
b) Để vượt qua các hệ thống IPS và IDS
c) Để đánh cắp các dữ liệu nhạy cảm trên máy trạm
d) Để đánh cắp các dữ liệu nhạy cảm trên máy chủ

108. Trojan horses là dạng phần mềm độc hại thường giành quyền truy nhập vào các file của người dùng khai thác cơ chế điều khiển truy nhập...

a) Rule-Based
b) Role-Based
c) MAC
d) DAC

109. Một trong các biện pháp hiệu quả để phòng chống Macro virus :

a) Cấm tự động thực hiện macro trong Microsoft Office
b) Sử dụng tường lửa
c) Cấm tự động thực hiện macro trong Microsoft Exchange
d) Sử dụng IPS/IDS

110. Đâu là một biện pháp phòng chống SYN Floods:

a) SYN Proxy
b) SYN Firewalls
c) SYN IDS
d) SYN Cache

111. Các zombie thường được tin tặc sử dụng để:

a) Thực hiện tấn công DoS
b) Thực hiện tấn công DDoS
c) Thực hiện tấn công tràn bộ đệm
d) Đánh cắp dữ liệu từ máy chủ CSDL

112. Tấn công kiểu Social Engineering có thể cho phép tin tặc:

a) Đánh cắp thông tin nhạy cảm của người dùng
b) Đánh cắp thông tin nhạy cảm trong cơ sở dữ liệu máy chủ
c) Phá hỏng máy chủ
d) Đánh cắp toàn bộ dữ liệu trên máy chủ

113. Tấn công bằng mã độc có thể gồm:

a) SQLi, XSS, CSRF và Buffer overflow
b) Chèn mã XSS, CSRF
c) Tràn bộ đệm
d) Chèn mã SQL

114. Tại sao việc sử dụng thủ tục cơ sở dữ liệu (Stored procedure) là một trong các biện pháp hiệu quả để ngăn chặn triệt để tấn công chèn mã SQL ?

a) Thủ tục cơ sở dữ liệu cho phép tách mã lệnh SQL khỏi dữ liệu người dùng
b) Thủ tục cơ sở dữ liệu độc lập với các ứng dụng
c) Thủ tục cơ sở dữ liệu có khả năng cẩm chèn mã
d) Thủ tục cơ sở dữ liệu lưu trong cơ sở dữ liệu và chạy nhanh hơn câu lệnh trực tiếp

115. Dạng tấn công chèn mã được tin tặc sử dụng 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

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

a) Sử dụng công nghệ xác thực mạnh
b) Sử dụng các thư viện lập trình an toàn //or sử dụng cơ chế cấm thực hiện mã trong dữ liệu (DEP)
c) Sử dụng tường lửa
d) Sử dụng các kỹ thuật mật mã

117. Để thực hiện tấn công Smurf, tin tặc phải giả mạo địa chỉ gói tin ICMP trong yêu cầu tấn công. Tin tặc sử dụng...

a) Địa chỉ router làm địa chỉ nguồn của gói tin
b) Địa chỉ máy nạn nhân làm địa đích của gói tin
c) Địa chỉ máy nạn nhân làm địa chỉ nguồn của gói tin
d) Địa chỉ router làm địa đích của gói tin

118. Để thực hiện tấn công DDOS, tin tặc trước hết cần chiếm quyền điều khiển của một lượng lớn máy tính. Các máy tính bị chiếm quyền điều khiển thường được gọi là:

a) Trojans
b) Zombies
c) Worms
d) Viruses

119. Điểm yếu là

a) Là 1 khiếm khuyết của phần mềm
b) Một lỗi khi xây dựng phần cứng máy tính
c) Một lỗi hoặc một khiếm khuyết tồn tại trong hệ thống
d) Một lỗi hoặc một khiếm khuyết tồn tại trong kết nối mạng

120. Tìm phát biểu đúng

a) Lỗ hổng là bất kỳ điểm yếu nào trong hệ thống cho phép hacker có thể gây tác hại
b) Lỗ hổng là bất kỳ điều gì trong hệ thống cho phép mối đe dọa có thể gây tác hại
c) Lỗ hổng là bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại
d) Lỗ hổng là bất kỳ điểm yếu nào trong mạng cho phép mối đe dọa có thể gây tác hại

121. Đâu không phải là mối quan hệ giữa mối đe dọa và lỗ hổng

a) Không thể triệt tiêu được hết các lỗ hỏng, nhưng có thể giảm thiểu các mối đe dọa, qua đó giảm thiểu khả năng bị tận dụng để tấn công

b) Nếu tồn tại một lỗ hổng trong hệ thống, sẽ có khả năng một mối đe dọa trở thành hiện thực

c) Không thể triệt tiêu được hết các mối đe dọa, nhưng có thể giảm thiểu các lỗ hổng, qua đó giảm thiểu khả năng bị tận dụng để tấn công

d) Các mối đe dọa thường khai thác một hoặc một số lỗ hổng đã biết để thực hiện các cuộc tấn công phá hoại

122. Dạng tấn công liên quan đến việc nghe trộm trên đường truyền và chuyển hướng thông tin để sử dụng trái phép là

a) Interruptions

b) Modifications

c) Interceptions

d) Fabrications

123. Đâu không phải là 1 kiểu tấn công thụ động

a) Sửa đổi dữ liệu trong file

b) Không gây ra thay đổi trên hệ thống

c) Nghe lén

d) Giám sát lưu lượng tren đường truyền

124. Đâu không phải là 1 dạng tấn công

a) Tràn bộ đệm

b) Tấn công từ chối dịch vụ

c) Tấn công giả mạo địa chỉ

d) Tấn công kiểu Social Engineering

125. Đâu là một nguyên nhân dẫn đến bị tấn công bằng mã độc

a) Dữ liệu đầu vào từ người dùng hoặc từ các nguồn khác không được kiểm tra hoặc kiểm tra không kỹ lưỡng

b) Để mật khẩu ở dạng bản rõ

c) Sử dụng thủ tục bắt tay ba bước

d) Xâm phạm vào bộ nhớ riêng của ứng dụng

126. Đâu không phải là một biện pháp phòng chống dựa trên thiết lập quyền truy nhập người dùng phù hợp

a) Chia nhóm người dùng, chỉ cấp quyền vừa đủ để truy cập các bảng biểu, thực hiện câu truy vấn và chạy các thủ tục

b) Người dùng được quyền truy nhập vào mọi tác vụ của hệ thống

c) Tốt nhất, không cấp quyền thực hiện các câu truy vấn, cập nhật, sửa, xóa trực tiếp dữ liệu; Thủ tục hóa tất cả các câu lệnh và chỉ cấp quyền thực hiện thủ tục

d) Không sử dụng người dùng có quyền system admin hoặc database owner làm người dùng truy cập dữ liệu

127. Trong tấn công DoS, việc gửi một lượng lớn yêu cầu gây cạn kiệt tài nguyên hệ thống hoặc băng thông đường truyền là loại tấn công nào

a) Flooding attacks

b) Sniffing

c) Logic attacks

d) SYN cache

128. SYN floods là kỹ thuật gây ... các gói tin mở kết nối TCP

a) Giả mạo

b) Hỏng hóc

c) Dừng

d) Ngập lụt

129. Đâu không phải là cách phòng chống SYN floods

a) Sử dụng mật khẩu mạnh

b) Sử dụng kỹ thuật lọc

c) Giảm thời gian chờ

d) Sử dụng Firewall và proxy

130. Điểm khác biệt của Reflective DDoS so với DDoS là gì

a) Một lượng lớn yêu cầu giả mạo với địa chỉ nguồn là địa chỉ máy nạn nhân đến một số lớn các máy khác được gửi đi

b) Các máy tính do kẻ tấn công điều khiển (Slaves/Zombies) trực tiếp tấn công máy nạn nhân

c) Tạo một lượng lớn yêu cầu kết nối giả mạo

d) Phạm vi tấn công lớn

131. Đâu không phải là 1 các tấn công kiểu Social Engineering

a) Kẻ tấn công có thể giả danh làm người có vị trí cao hơn so với nạn nhân để có được sự tin tưởng

b) Kẻ tấn công bắt buộc người dùng truy cập vào đường dẫn giả mạo

c) Kẻ tấn công có thể lập trang web giả để đánh lừa người dùng cung cấp các thông tin cá nhân và thông tin tài khoản, thẻ tín dụng, ...

d) Kẻ tấn công có thể mạo nhận là người được ủy quyền của người có thẩm quyền để yêu cầu các nhân viên tiết lộ thông tin về cá nhân/tổ chức

132. Tìm phương án sai, Tấn công bằng bomb thư có thể thực hiện bằng

a) Hoặc khai thác lỗi trong hệ thống gửi nhận email SMTP

b) Có thể thực hiện được bằng kỹ thuật Social Engineering

c) Kẻ tấn công có thể lợi dụng các máy chủ email không được cấu hình tốt để gửi email cho chúng

d) Sử dụng phương pháp truyền tin TCP

133. Chọn phát biểu đúng về logic bomb

a) Thường được "nhúng" vào các chương trình đặt trưng và thường tự động "phát nổ" trong một số điều kiện cụ thể

b) Thường được "nhúng" vào các chương trình bình thường

c) Thường được "nhúng" vào các chương trình bình thường và thường hẹn giờ để "phát nổ" trong một số điều kiện cụ thể

d) Thường "có sẵn" trong các chương trình bình thường và thường tự động "phát nổ" trong một số điều kiện cụ thể

134. Trojan horse là chương trình chứa ..., thường giả danh những chương trình ..., nhằm lừa người dùng kích hoạt chúng

a) Mã máy / Thông dụng

b) Mã độc / Thông dụng

c) Mã độc / Có ích

d) Mã máy / Có ích

135. Trojan horse thường được sử dụng để

a) Thực thi gián tiếp các tác vụ, mà tác giả của chúng không thể thực hiện trực tiếp do không có quyền truy nhập

b) Thực thi trực tiếp các tác vụ

c) Thực thi trực tiếp các tác vụ, mà tác giả của chúng không thể thực hiện gián tiếp dù đã được cấp quyền truy nhập

d) Thực thi gián tiếp các tác vụ, mà tác giả của chúng không thể thực hiện được do không thể truy nhập

136. Zombie là một chương trình được thiết kế để giành quyền ... một máy tính có kết nối Internet, và sử dụng máy tính bị kiểm soát để ... các hệ thống khác

a) Kiểm soát / Tấn công
b) Kiểm soát / Nghe lén
c) Xâm nhập / Tấn công
d) Xâm nhập / Nghe lén

137. Tìm phát biểu sai trong các phát biểu sau về vòng đời của virus

a) Giai đoạn "nằm im": Virus trong giai đoạn không được kích hoạt và có thể được kích hoạt nhờ một sự kiện nào đó
b) Giai đoạn kích hoạt: virus được kích hoạt để thực thi các tác vụ đã thiết được định sẵn. Virus cũng thường được kích hoạt dựa trên một sự kiện nào đó
c) Giai đoạn thực hiện: thực thi các tác vụ. Một số virus có thể vô hại, nhưng một số khác có thể xoá dữ liệu, chương trình...
d) Giai đoạn phát tán: Virus kiểm soát những chương trình mà nó đã tiếp xúc

138. Đâu không phải một phương pháp lây lan của Worms

a) Lây lan qua thư điện tử: sử dụng email để gửi bản copy của sâu đến các máy khác
b) Lây lan thông qua khả năng log-in (đăng nhập) từ xa
c) Lây lan thông qua khả năng thực thi từ xa
d) Cần sự đồng ý từ người dùng để lây lan từ máy này sang máy khá

139. Loại mã nguồn độc hại nào có thể được cài đặt song không gây tác hại cho đến khi một hoạt động nào đó được kích hoạt?

a) Sâu
b) Logic bomb
c) Stealth virus
d) Trojan horse

140. PGP đảm bảo tính bí mật thông điệp bằng cách sử dụng:

a) Mã hóa khóa đối xứng sử dụng khóa công khai
b) Mã hóa khóa bất đối xứng sử dụng khóa phiên
c) Mã hóa khóa bất đối xứng sử dụng khóa công khai
d) Mã hóa khóa đối xứng sử dụng khóa phiên

141. Số lượng thao tác trong mỗi vòng xử lý của hàm băm MD5 là:

a) 16
b) 12
c) 14
d) 18

142. Trong các cặp khoá sau đây của hệ mật RSA với p=5 ; q=7 , cặp khóa nào có khả năng đúng nhất :

a) (e = 4 , d =11)
b) (e = 7 , d =23)
c) (e = 3 , d =18)
d) (e = 12 , d =11)

143. Thuật giải SHA-1 dùng để :

a) Tạo chữ ký số
b) Tạo một giá trị băm có độ dài cố định 160 bit
c) Tạo khoá đối xứng
d) Tạo một giá trị băm có độ dài cố định 256 bit

144. Một hệ mã hóa (cryptosystem) được cấu thành từ hai thành phần chính gồm:

a) Giải thuật mã hóa và ký số
b) Phương pháp mã hóa và chia khối
c) Giải thuật mã hóa và giải mã
d) Phương pháp mã hóa và không gian khóa

145. Giải thuật mã hóa và giải mã

a) NOT
b) OR
c) XOR
d) AND

146. Kích thước khối dữ liệu xử lý của giải thuật mã hóa AES là:

a) 160 bit
b) 128 bit
c) 192 bit
d) 64 bit

147. Điểm khác nhau chính giữa hai loại hàm băm MDC và MAC là:

a) MDC an toàn hơn MAC
b) MDC là loại hàm băm không khóa, còn MAC là loại hàm băm có khóa
c) MDC có khả năng chống đụng độ cao hơn MAC
d) MAC an toàn hơn MDC

148. Một trong các điểm yếu của các hệ mã hóa khóa công khai là:

a) Độ an toàn thấp
b) Khó cài đặt trên thực tế
c) Khó khăn trong quản lý và phân phối khóa
d) Tốc độ chậm

149. Hai thuộc tính cơ bản quan trọng nhất của một hàm băm là:

a) Dễ tính toán và có đầu ra cố định
b) Nén và dễ tính toán
c) Một chiều và đầu ra cố định
d) Nén và một chiều

150. Độ an toàn của hệ mật mã RSA dựa trên...

a) Khóa có kích thước lớn
b) Chi phí tính toán lớn
c) Độ phức tạp cao của giải thuật RSA
d) Tính khó của việc phân tích số nguyên rất lớn

151. Khi sinh cặp khóa RSA, các số nguyên tố p và q nên được chọn với kích thước...

a) p càng lớn càng tốt
b) Bằng khoảng một nửa kích thước của modulo n
c) q càng lớn càng tốt
d) Không có yêu cầu về kích thước của p và q

152. Tìm phát biểu đúng về mã hóa khóa bất đối xứng (Asymmetric key cryptography):

a) Sử dụng một khóa chung cho cả quá trình mã hóa và giải mã
b) Chỉ sử dụng kỹ thuật mã hóa khối
c) An toàn hơn mã hóa khóa bí mật
d) Sử dụng một khóa quá trình mã hóa và một khóa khác cho giải mã

153. Tìm phát biểu đúng về mã hóa khóa đối xứng (Symmetric key cryptography):

a) Sử dụng một khóa quá trình mã hóa và một khóa khác cho giải mã
b) An toàn hơn mã hóa khóa công khai
c) Chỉ sử dụng kỹ thuật mã hóa khối
d) Sử dụng một khóa chung cho cả quá trình mã hóa và giải mã

154. Số lượng vòng lặp chính thực hiện xáo trộn dữ liệu theo hàm Feistel (F) trong giải thuật DES là:

a) 20
b) 16
c) 18
d) 14

155. Các hộp thay thế s-box trong giải thuật DES có số bít đầu vào và đầu ra tương ứng là:

a) Vào 4 bít và ra 4 bít
b) Vào 6 bít và ra 4 bít
c) Vào 6 bít và ra 6 bít
d) Vào 8 bít và ra 6 bít

156. Một trong các ứng dụng phổ biến của các hàm băm là để tạo chuỗi...

a) CheckNum
b) CheckTotal
c) Checksum
d) CheckError

157. Trong quá trình xử lý thông điệp đầu vào tạo chuỗi băm, số lượng vòng xử lý của hàm băm SHA1 là:

a) 60
b) 90
c) 80
d) 70

158. Giải thuật mã hóa AES được thiết kế dựa trên...

a) mạng hoán vị-thay thế
b) mạng hoán vị-vernam
c) mạng hoán vị-xor
d) mạng xor-thay thế

159. Một trong các điểm yếu của các hệ mã hóa khóa đối xứng là:

a) Độ an toàn thấp
b) Chi phí tính toán lớn
c) Khó khăn trong cài đặt và triển khai hệ thống
d) Khó khăn trong quản lý và phân phối khóa

160. Số vòng lặp chuyển đổi cần thực hiện để chuyển bản rõ thành bản mã của giải thuật mã hóa AES với khóa 192 bít là:

a) 12
b) 16
c) 10
d) 14

161. Một trong các ứng dụng phổ biến của các hàm băm một chiều là để...

a) Mã hóa mật khẩu
b) Mã hóa địa chỉ
c) Mã hóa tên tài khoản
d) Mã hóa thẻ tín dụng

162. PGP đảm bảo tính xác thực thông điệp bằng cách:

a) Sử dụng hàm băm có khóa MAC
b) Mã hóa/giải mã thông điệp
c) Sử dụng hàm băm không khóa MDC
d) Tạo và kiểm tra chữ ký số

163. Kích thước khóa hiệu dụng của hệ mã hóa DES là:

a) 64 bít
b) 56 bít
c) 128 bít
d) 48 bít

164. Trong mã hóa dòng (stream cipher), dữ liệu được xử lý theo...

a) Từng bít
b) Từng bít hoặc từng byte/ký tự
c) Từng chuỗi ký tự
d) Từng byte

165. Trong hệ mật mã RSA, quan hệ toán học giữa khóa công khai e và số Phi(n) là:

a) e và Phi(n) không có quan hệ với nhau
b) Phi(n) là modulo nghịch đảo của e
c) e và Phi(n) là 2 số nguyên tố cùng nhau
d) Phi(n) là modulo của e

166. Các giải thuật mã hóa khóa đối xứng thông dụng gồm:

a) DES, 3-DES, AES
b) DES, 3-DES, RSA
c) DES, AES, PGP
d) DES, RSA, RC4

167. Trong hệ mật mã RSA, quan hệ toán học giữa khóa riêng d và khóa công khai e là:

a) d là modulo nghịch đảo của e
b) d và e không có quan hệ với nhau
c) d và e là 2 số nguyên tố cùng nhau
d) d là modulo của e

168. Giải thuật mã hóa AES vận hành dựa trên một ma trận 4x4, được gọi là...

a) Status
b) Stock
c) State
d) States

169. Đâu là một ứng dụng của mã hóa?

a) PGP
b) PPG
c) PGG
d) GPP

170. Phần xử lý chính của SHA1 làm việc trên một chuỗi được gọi là state. Kích thước của state là:

a) 160 bít
b) 150 bít
c) 170 bít
d) 180 bít

171. Trật tự các khâu xử lý trong các vòng lặp chính của giải thuật mã hóa AES là:

a) SubBytes, ShiftRows, MixColumns, AddRoundKey
b) SubBytes, MixColumns, ShiftRows, AddRoundKey
c) AddRoundKey, MixColumns, SubBytes, ShiftRows
d) AddRoundKey, MixColumns, ShiftRows, SubBytes

172. Văn bản sau khi được mã hóa gọi là gì?

a) Khóa công khai.
b) Văn bản mã.
c) Mật mã đối xứng.
d) Chứng chỉ.

173. Đặc tính nào sau đây không thuộc chức năng bảo mật thông tin trong các hệ thống mật mã?

a) Toàn vẹn.
b) Bảo mật.
c) Hiệu quả.
d) Không chối từ.

174. Ở hệ mật mã nào người gửi và người nhận thông diệp sử dụng cùng một khóa mã khi mã hóa công khai và giải mã?

a) RS.
b) Đối xứng.
c) Không đối xứng.
d) Difie-Hellman.

175. Chuẩn nào sau đây được chính phủ Mỹ sử dụng thay thế cho DES như là một chuẩn mã hóa dữ liệu?

a) ECC
b) 3DES
c) AES
d) DSA

176. Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng các khóa khác nhau khi mã hóa và giải mã ?

a) Không đối xứng
b) Đối xứng
c) Skipjack
d) Blowfish

177. Khi giá trị hàm băm của hai thông điệp khác nhau có giá trị tương tự nhau, ta gọi hiện tượng này là gì ?

a) Tấn công vào ngày sinh
b) Chữ ký số
c) Khóa công khai
d) Xung đột

178. Nếu muốn xem một tài liệu "bảo mật"được mã hóa trên hệ mật bất đối xứng do người khác gởi đến , bạn phải sử dụng khóa nào để giải mật tài liệu?

a) Khoá công khai của bạn
b) Khoá cá nhân của bên gửi
c) Khoá công khai của bên gửi
d) Khoá cá nhân của bạn

179. Đâu là một phương pháp mã hóa:

a) Vernam
b) Tất cả các phương án trên
c) Đổi chỗ/ hoán vị
d) Thay thế

180. Thuật giải MD5 cho ta một giá trị băm có độ dài :

a) 512 bit
b) 128 bit
c) 156 bit
d) 256 bit

181. Các hệ mã hóa khóa công khai sử dụng một cặp khóa: public key và private key. Các yêu cầu đối với public key và private key là:

a) Cả public key và private key đều cần giữ bí mật
b) Có thể công khai public key nhưng phải đảm bảo tính xác thực và cần giữ bí mật private key
c) Có thể công khai public key và cần giữ bí mật private key
d) Có thể công khai private key và cần giữ bí mật public key

182. Kích thức khóa có thể của hệ mã hóa AES là:

a) 64, 128 và 192 bit
b) 128, 256 và 512 bit
c) 128, 256 và 384 bit
d) 128, 160 và 192 bit

183. Kích thước khóa hiệu dụng của hệ mã hóa DES là:

a) 64 bit
b) 48 bit
c) 56 bit
d) 128 bit

184. Số lượng vòng lặp chuyển đổi cần thực hiện để chuyển bản rõ thành bản mã trong hệ mã hóa AES khóa 128 bit là:

a) 14
b) 10
c) 12
d) 16

185. Bước MixColumns (trộn cột) trong vòng lặp chuyển đổi trong hệ mã hóa AES thực hiện việc:

a) Trộn các dòng tương ứng của ma trận state với khóa

b) Bước MixColumns (trộn cột) trong vòng lặp chuyển đổi trong hệ mã hóa AES thực hiện việc:

c) Mỗi cột của ma trận state được nhân với một đa thức

d) Trộn các cột tương ứng của ma trận state với khóa

186. Phát biểu nào sau đây đúng với kỹ thuật mã hóa khóa bí mật

a) Mã hóa khóa bí mật sử dụng một mã (key) cho cả quá trình mã hóa và giải mã

b) Mã hóa khóa bí mật chỉ hoạt động theo chế độ mã hóa khối

c) Mã hóa khóa bí mật an toàn hơn mã hóa khóa công khai

d) Mã hóa khóa bí mật có thuật toán đơn giản hơn mã hóa khóa công khai

187. Ưu điểm của kỹ thuật mã hóa khóa công khai so với mã hóa khóa bí mật là:

a) Trao đổi khóa dễ dàng hơn

b) Chi phí tính toán thấp hơn

c) Quản lý dễ dàng hơn

d) Có độ an toàn cao hơn

188. Yêu cầu để đảm bảo sử dụng mã hóa đối xứng là

a) Có thuật toán encryption tốt,có một khóa bí mật được biết bởi người nhận/gửi và kênh truyền bí mật để phân phát key

b) Tất cả đều đúng

c) Có thuật toán encryption tốt và có một khóa bí mật được biết bởi người nhận/gửi

d) Có một kênh truyền phù hợp và một khóa bí mật được biết bởi người nhận/gửi

189. Các thuật tóan nào sau đây là thuật tóan mã hóa đối xứng

a) Triple–DES, RC4, RC5, Blowfish

b) Triple–DES, RC4, RC5, IDEA

c) RC4, RC5, IDEA, Blowfish

d) IDEA, Blowfish, AES, Elliptic Cure

190. Các phát biểu sau đây phát biểu nào đúng

a) Tấn công thông điệp thì thời gian giải mã tỷ lệ với kích thước khóa

b) Tất cả đều đúng

c) Hầu hết các thuật tóan mã hóa đối xứng đều dựa trên cấu trúc thuật toán Feistel

d) Hầu hết các thuật tóan mã hóa khối đều đối xứng

191. Mã hóa nào sau đây là một tiêu chuẩn dùng để phát triển cho việc tạo ra thông điệp an toàn?

a) Digital Signature Standard
b) Secure Hash Algorithm
c) Chữ kí dữ liệu tiêu chuẩn
d) Data Encryption Standard

192. Các yếu tố ảnh hưởng đến quá trình mã hóa

a) Thời gian thực hiện mã hóa và giải mã
b) Tất cả đều sai
c) Thuật toán mã hóa, giải mã, và tính an toàn của kênh truyền
d) Thực hiện mã hóa khối, mở rộng số bít xử lý

193. MAC là một từ cấu tạo bằng những chữ đầu của một nhóm nào liên quan đến mật mã ?

a) Các ủy ban đa tư vấn (Multiple advisory committees)
b) Kiểm soát truy cập phương tiện (Media access control)
c) Mã xác thực thông điệp (Message authentication code)
d) Kiểm soát truy cập bắt buộc (Mandatory access control)

194. Nội dung nào sau đây không cần sử dụng mật mã ?

a) Xác thực
b) Bảo mật
c) Truy cập
d) Toàn vẹn

195. Thuật giải MD5 dùng để :

a) Xác thực một thông điệp
b) Phân phối khoá mật mã
c) Bảo mật một thông điệp
d) Kiểm tra tính toàn vẹn dữ liệu

196. Trong DES mỗi hàm chọn Si được dùng để :

a) Biến đổi khối dữ liệu mã 32 bit thành 4 bit
b) Biến đổi khối dữ liệu mã 6 bit thành 4 bit
c) Biến đổi khối dữ liệu mã 16 bit thành 4 bit
d) Biến đổi khối dữ liệu mã 48 bit thành 32 bit

197. Hệ mật DES sử dụng khối khoá được tạo bởi :

a) 64 bit ngẫu nhiên
b) 128 bit ngẫu nhiên
c) 56 bit ngẫu nhiên và 8 bit kiểm tra “Parity”
d) 56 bit ngẫu nhiên

198. Hệ mật DES xử lý từng khối " plain text " có độ dài :

a) 48 bit
b) 32 bit
c) 64 bit
d) 56 bit

199. Số lượng các khóa phụ (subkey) cần được tạo ra từ khóa chính trong giải thuật DES là:

a) 16
b) 18
c) 12
d) 14

200. Sử dụng nhiêu bit với DES để có hiệu quả?

a) 32
b) 64
c) 16
d) 56

201. Thuật giải SHA là :

a) Hàm băm một chiều
b) Tất cả đều đúng
c) Hàm băm một chiều
d) Cho giá trị băm 160 bit

202. Quản trị văn phòng của bạn đang được huấn luyện để thực hiện sao lưu máy chủ. Phương pháp xác thực nào là lý tưởng đối với tình huống này ?

a) RBAC
b) Các mã thông báo bảo mật.
c) MAC
d) DAC

203. Phát biểu nào sau đây đúng với cơ chế điều khiển truy cập MAC:

a) MAC là cơ chế điều khiển truy cập được sử dụng rộng rãi nhất
b) MAC cho phép người tạo ra đối tượng có thể cấp quyền truy cập cho người dùng khác
c) MAC quản lý truyền quy cập chặt chẽ hơn các cơ chế khác
d) MAC cấp quyền truy cập dựa trên tính nhạy cảm của những thông tin và chính sách quản trị

204. Các loại khoá mật mã nào sau đây dễ bị crack nhất ?

a) 56 bit
b) 256 bit
c) 128 bit
d) 40 bit

205. Nguyên tắc bảo mật tài nguyên của mô hình Bell-La Padula là:

a) Đọc xuống và ghi lên
b) Đọc xuống và ghi xuống
c) Đọc lên và ghi xuống
d) Đọc lên và ghi lên

206. Tính bảo mật của kỹ thuật điều khiển truy nhập sử dụng mật khẩu dựa trên:

a) Độ khó đoán và tuổi thọ của mật khẩu
b) Số loại ký tự dùng trong mật khẩu
c) Tần suất sử dụng mật khẩu
d) Kích thước của mật khẩu

207. Phát hiện tấn công, xâm nhập dựa trên bất thường có tiềm năng phát hiện các loại tấn công, xâm nhập mới là do:

a) Không yêu cầu biết trước thông tin về chúng
b) Đã có chữ ký của các tấn công, xâm nhập mới
c) Các tấn công, xâm nhập mới thường dễ nhận biết
d) Không yêu cầu xây dựng cơ sở dữ liệu các chữ ký

208. Một trong các điểm yếu làm giảm hiệu quả của phát hiện tấn công, xâm nhập dựa trên bất thường là:

a) Không có khả năng phát hiện các cuộc tấn công Dos
b) Không có khả năng phát hiện tấn công, xâm nhập mới
c) Không có khả năng ngăn chặn tấn công, đột nhập
d) Tỷ lệ cảnh báo sai cao

209. Phát hiện tấn công, xâm nhập dựa trên bất thường dựa trên giả thiết:

a) Các hành vi tấn công, xâm nhập có quan hệ chặt chẽ với các dịch vụ được cung cấp
b) Các hành vi tấn công, xâm nhập gây ngắt quãng dịch vụ cung cấp cho người dùng
c) Các hành vi tấn công, xâm nhập gây tổn hại nghiêm trọng cho hệ thống
d) Các hành vi tấn công, xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường

210. Ưu điểm của điều khiển truy nhập dựa trên các đặc điểm sinh trắc học là:

a) Bảo mật cao và độ ổn định cao
b) Bảo mật cao và được hỗ trợ rộng rãi
c) Bảo mật cao và chi phí thấp
d) Bảo mật cao và luôn đi cùng với chủ thể

211. Một ưu điểm của tường lửa có trạng thái so với tường lửa không trạng thái là:

a) Lọc nội dung gói tốt hơn
b) Nhận dạng được các dạng tấn công và các phần mềm độc hại
c) Phân biệt được các gói tin thuộc về các kết nối mạng khác nhau
d) Chạy nhanh hơn

212. Các phương pháp xử lý, phân tích dữ liệu và mô hình hoá trong phát hiện tấn công, xâm nhập dựa trên bất thường, gồm:

a) Thống kê, đối sánh chuỗi, đồ thị
b) Thống kê, học máy, khai phá dữ liệu
c) Thống kê, học máy, đồ thị
d) Học máy, khai phá dữ liệu, agents

213. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập dựa trên vai trò - RBAC:

a) RBAC cấp quyền truy nhập dựa trên tính nhạy cảm của thông tin và chính sách quản trị
b) RBAC cho phép người tạo ra đối tượng có thể cấp quyền truy nhập cho người dùng khác
c) RBAC cấp quyền truy nhập dựa trên vai trò của người dùng trong tổ chức
d) RBAC là cơ chế điều khiển truy nhập được sử dụng rộng rãi nhất

214. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập DAC:

a) DAC cho phép người tạo ra đối tượng có thể cấp quyền truy nhập cho người dùng khác
b) DAC quản lý quyền truy nhập chặt chẽ hơn các cơ chế khác
c) DAC là cơ chế điều khiển truy nhập được sử dụng rộng rãi nhất
d) DAC cấp quyền truy nhập dựa trên tính nhạy cảm của thông tin và chính sách quản trị

215. Đâu là một công cụ có khả năng rà quét các lỗ hổng chèn mã SQL cho các trang web?

a) nmap
b) Microsoft Baseline Security Analyzer
c) Nessus vulnerability scanner
d) Acunetix Web Vulnerability Scanner

216. Danh sách điều khiển truy nhập ACL thực hiện việc quản lý quyền truy nhập đến các đối tượng cho người dùng bằng cách:

a) Các quyền truy nhập vào đối tượng cho mỗi người dùng được quản lý trong một ma trận

b) Mỗi người dùng được gán một danh sách các đối tượng kèm theo quyền truy nhập

c) Các quyền truy nhập vào đối tượng cho mỗi người dùng được quản lý riêng rẽ

d) Mỗi đối tượng được gán một danh sách người dùng kèm theo quyền truy nhập

217. Tường lửa không thể chống lại...

a) Các hiểm họa từ bên ngoài

b) Các hiểm họa từ bên trong

c) Tấn công giả mạo địa chỉ

d) Tấn công từ mạng Internet

218. Sự khác biệt chính giữa hệ thống ngăn chặn xâm nhập (IPS) và hệ thống phát hiện xâm nhập (IDS) là:

a) IDS phát hiện xâm nhập hiệu quả hơn

b) IDS có khả năng chủ động ngăn chặn xâm nhập

c) IPS có khả năng chủ động ngăn chặn xâm nhập

d) IPS phát hiện xâm nhập hiệu quả hơn

219. Tường lửa lọc gói có thể lọc các thông tin nào trong gói tin?

a) Chỉ lọc địa chỉ IP trong gói tin

b) Cả thông tin trong header và payload của gói tin

c) Chỉ các thông tin trong payload của gói tin

d) Chỉ các thông tin trong header của gói tin

220. Không nên sử dụng nhiều hơn 1 phần mềm quét virus chạy ở chế độ quét theo thời gian thực trên một máy tính vì:

a) Các phần mềm quét virus tấn công lẫn nhau

b) Các phần mềm quét virus xung đột với nhau

c) Các phần mềm quét virus không thể hoạt động

d) Các phần mềm quét virus chiếm nhiều tài nguyên

221. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập bắt buộc MAC:

a) MAC cho phép người tạo ra đối tượng có thể cấp quyền truy nhập cho người dùng khác

b) MAC là cơ chế điều khiển truy nhập được sử dụng rộng rãi nhất

c) MAC cấp quyền truy nhập dựa trên tính nhạy cảm của thông tin và chính sách quản trị

d) MAC quản lý quyền truy nhập chặt chẽ hơn các cơ chế khác

222. Đâu là một loại tường lửa?

a) Application server

b) Gateway server

c) Server gateway

d) Application-level gateway

223. Ví điện tử Paypal là một dạng...

a) Thẻ thông minh (smart card)

b) The ATM

c) Thẻ bài (token)

d) Khóa mã (encrypted key)

224. Dạng xác thực sử dụng các thông tin nào dưới đây đảm bảo độ an toàn cao hơn?

a) Tên truy nhập và mật khẩu

b) Thẻ ATM và số PIN

c) Thẻ ATM và tên truy nhập

d) Tên truy nhập và số PIN

225. Một trong các dạng khóa mã (encrypted keys) được sử dụng rộng rãi trong điều khiển truy nhập là:

a) Mobile-token

b) E-token

c) The ATM

d) Chứng chỉ số khóa công khai

226. Tại sao một hệ thống phát hiện xâm nhập dựa trên chữ ký không thể phát hiện các tấn công, xâm nhập mới?

a) Do chữ ký của chúng chưa tồn tại trong hệ thống

b) Do các tấn công, xâm nhập mới không gây ra bất thường

c) Do các tấn công, xâm nhập mới chỉ gây thiệt hại nhỏ

d) Do các tấn công, xâm nhập mới không có chữ ký

227. 23. Ưu điểm của thẻ bài (token) so với thẻ thông minh (smart card) trong điều khiển truy nhập là:

a) Có cơ chế xác thực đa dạng hơn
b) Có cơ chế xác thực mạnh hơn
c) Có chi phí rẻ hơn
d) Được sử dụng rộng rãi hơn

228. Phương pháp xác thực nào dưới đây có thể cung cấp khả năng xác thực có độ an toàn cao nhất?

a) Sử dụng chứng chỉ số
b) Sử dụng vân tay
c) Sử dụng mật khẩu
d) Sử dụng Smartcard

229. Đâu là các tính năng của kiểm soát truy nhập sử dụng tường lửa?

a) Kiểm soát dịch vụ và hướng
b) Kiểm soát virus và các malware khác
c) Kiểm soát người dùng và tin tặc
d) Kiểm soát dịch vụ và các phần mềm

230. Ba cơ chế điều khiển truy nhập thông dụng gồm:

a) DAC, MAC và BAC
b) DAC, MAC và RRAC
c) DAC, MAC và RBAC
d) DAC, BAC và RBAC

231. Mục đích chính của điều khiển truy nhập là để đảm bảo các thuộc tính an ninh của thông tin, hệ thống và các tài nguyên, gồm:

a) Tính bảo mật, tính toàn vẹn và tính sẵn dùng
b) Tính bảo mật, tính toàn vẹn và tính xác thực
c) Tính bí mật, tính toàn vẹn và tính xác thực
d) Tính bí mật, tính toàn vẹn và tính sẵn dùng

232. Số lượng nhân tố (factor) xác thực sử dụng trong điều khiển truy nhập dựa trên thẻ thông minh là:

a) 1
b) 3
c) 2
d) 4

233. Một nhiệm vụ chính của các hệ thống IDS/IPS là:

a) Giám sát lưu lượng mạng nhận dạng các dấu hiệu của tấn công, xâm nhập
b) Truy tìm và tấn công ngược lại hệ thống của tin tặc
c) Giám sát các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập
d) Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập

234. Hai dịch vụ quan trọng nhất của một hệ thống điều khiển truy nhập là:

a) Authentication và Administrator
b) Authenticator và Administrator
c) Administrator và Authorization
d) Authentication và Authorization

235. Tìm phát biểu đúng về phát hiện xâm nhập dựa trên chữ ký và phát hiện xâm nhập dựa trên bất thường:

a) Tính bảo mật, tính toàn vẹn và tính sẵn dùng
b) Phát hiện xâm nhập dựa trên chữ ký thường có tỷ lệ phát hiện đúng cao hơn
c) Tính bí mật, tính toàn vẹn và tính sẵn dùng
d) Tính bảo mật, tính toàn vẹn và tính xác thực

236. Tìm phát biểu đúng về dịch vụ xác thực trong điều khiển truy nhập:

a) Là quá trình xác minh nhận dạng của chủ thể
b) Là quá trình xác minh nhận dạng của người dùng
c) Là quá trình xác minh các thông tin nhận dạng của chủ thể yêu cầu truy nhập đối tượng
d) Là quá trình xác minh tính chân thực của thông tin nhận dạng người dùng cung cấp

237. Yếu tố nào cần được sử dụng kết hợp với một thẻ thông minh để xác thực?

a) Mã hóa khóa
b) Thẻ nhớ
c) PIN
d) Quét võng mạc

238. Qui trình xác thực nào sử dụng nhiều hơn một yếu tố xác thực để login?

a) Sinh trắc học
b) Kerberos
c) Thẻ thông minh
d) Đa yếu tố (multi-factor)

239. Một trong các nhược điểm chính của điều khiển truy nhập dựa trên các đặc điểm sinh trắc học là:

a) Khó sử dụng
b) Công nghệ phức tạp
c) Chi phí đắt
d) Không được hỗ trợ rộng rãi

240. Ưu điểm của mật khẩu một lần (OTP-One Time Password) so với mật khẩu truyền thống là:

a) Chống được tấn công phá mã
b) Chống được tấn công vét cạn
c) Chống được tấn công từ điển
d) Chống được tấn công phát lại

241. Kỹ thuật tấn công SYN Floods khai thác điểm yếu trong khâu nào trong bộ giao thức TCP/IP?

a) Truyền dữ liệu
b) Bắt tay 2 bước
c) Bắt tay 3 bước
d) Xác thực người dùng

242. 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) Quản trị
c) Xác thực
d) Xác thực và Trao quyền

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

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

244. Điều khiển truy nhập dựa trên luật (Rule-based access control) được sử dụng phổ biến trong:

a) Firewall
b) Kerberos
c) VPN
d) SSL/TLS

245. Phát hiện tấn công, xâm nhập dựa trên bất thường dựa trên giả thiết:

a) Các hành vi tấn công, xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường

b) Các hành vi tấn công, xâm nhập gây tổn hại nghiêm trọng cho hệ thống

c) Các hành vi tấn công, xâm nhập có quan hệ chặt chẽ với các dịch vụ được cung cấp

d) Các hành vi tấn công, xâm nhập gây ngắt quãng dịch vụ cung cấp cho người dùng

246. Các hệ thống phát hiện xâm nhập có thể thu thập dữ liệu đầu vào từ...

a) Các host

b) Mạng

c) Các router

d) Mạng và các host

247. Một hệ thống điều khiển truy nhập có thể được cấu thành từ các dịch vụ nào sau đây:

a) Xác thực, đăng nhập và kiểm toán (auditing)

b) Xác thực, trao quyền và quản trị

c) Xác thực, trao quyền và kiểm toán (auditing)

d) Xác thực, đăng nhập và trao quyền

248. Sau khi một user đã được định danh (identifed), điều gì cần phải làm trước khi họ log vào một mạng máy tính ?

a) Được phép truy cập với mức ưu tiên được thiết lập

b) Người quản trị phải enable để gõ vào

c) Họ phải nhập user ID đã được mã hóa

d) Xác thực với mật khẩu

249. Phát biểu nào sau đây đúng với cơ chế điều khiển truy cập DAC:

a) DAC cấp quyền truy cập dựa trên tính nhạy cảm của thông tin và chính sách quản trị

b) DAC quản lý quyền truy cập chặt chẽ hơn các cơ chế khác

c) DAC cho phép người tạo ra đối tượng có thể cấp quyền quy cập cho người dùng khác

d) DAC là cơ chế điều khiển truy cập được sử dụng rộng rãi nhất

250. Các hệ điều hành Microsoft Windows và Linux sử dụng các mô hình điều khiển truy cập nào dưới đây?

a) DAC và Role-BAC

b) MAC và Role-BAC

c) DAC và MAC

d) MAC và Rule-BAC

251. Phát biểu nào sau đây đúng với cơ chế điều khiển truy cập RBAC:

a) RBAC cấp quyền truy cập dựa trên tính nhạy cảm của thông tin và chính sách quản trị

b) RBAC cấp quyền truy cập dựa trên vai trò của người dùng trong tổ chức

c) RBAC là cơ chế điều khiển truy cập được sử dụng rộng rãi nhất

d) RBAC cho phép người tạo ra đối tượng có thể cấp quyền truy cập cho người dùng khác

252. Cho biết câu nào đúng trong các câu sau

a) Tất cả Firewall đều có chung thuộc tính là cho phép phân biệt hay đối xử khả năng từ chối hay truy nhập dựa vào địa chỉ nguồn

b) Tất cả đều đúng

c) Chức năng chính của Firewall là kiểm sóat luồng thông tin giữa mạng cần bảo vệ và Internet thông qua các chính sách truy nhập đã được thiết lập

d) Hệ thống Firewall thường bao gồm cả phần cứng lẫn phần mềm

253. Đối với Firewall lọc gói, hình thức tấn công nào sau đây được thực hiện

a) Nhái địa chỉ IP, tấn công vượt firewall,tấn công từng mẫu nhỏ

b) Nhái địa chỉ IP, tấn công vượt firewall, tấn công đường đi nguồn

c) Nhái địa chỉ IP, tấn công giữa, tấn công biên

d) Nhái địa chỉ IP, tấn công đường đi nguồn, tấn công từng mẫu nhỏ

254. Những chữ đầu của nhóm từ ACL là tên viết tắt của:

a) Access Control Library

b) Allowed Computer List

c) Access Control List

d) Arbitrary Code Language

255. Nên cài mức truy cập mặc định là mức nào sau đây?

a) No access

b) Full access

c) Write access

d) Read access

256. Sau khi một user được định danh và xác thực hệ thống, để cho phép user sử dụng tài nguyên bạn phải thực hiện điều gì?

a) Được enable
b) Phải được ủy quyền
c) Được truyền lại
d) Được mã hóa

257. Bộ lọc địa chỉ MAC được định nghĩa như :

a) Tường lửa cá nhân
b) Được phép truy cập đến một địa chỉ MAC nhất định.
c) Ngăn chặn truy cập từ một địa chỉ MAC nhất định.
d) Mã hóa địa chỉ MAC của thiết bị không dây.

258. Các mức độ nhạy cảm của thông tin được chia từ cao xuống thấp đối với an ninh quốc gia là:

a) Không phân loại (Unclassified - U), Mật (Confidential - C), Tối mật (Top Secret - T), Tuyệt mật (Secret - S).
b) Tối mật (Top Secret - T), Tuyệt mật (Secret - S), Mật (Confidential - C), Không phân loại (Unclassified - U).
c) Tuyệt mật (Secret - S), Tối mật (Top Secret - T), Mật (Confidential - C), Không phân loại (Unclassified - U).
d) Không phân loại (Unclassified - U), Mật (Confidential - C), Tuyệt mật (Secret - S), Tối mật (Top Secret - T).

259. Đặc tính nào của các thiết bị mạng như router hay switch, cho phép điều khiển truy cập dữ liệu trên mạng ?

a) Cập nhật vi chương trình (Firmware)
b) Danh sách điều khiển truy cập (ACL).
c) Tường lửa
d) Giao thức DNS

260. Yếu tố nào cần được sử dụng kết hợp với một thẻ thông minh để xác thực ?

a) PIN
b) Quét võng mạc
c) Mã hóa khóa
d) Thẻ nhớ

261. Phương pháp quét võng mạc thích hợp nhất đối với các dịch vụ nào sau đây?

a) Kiểm định
b) Xác thực
c) Bảo mật dữ liệu
d) Kiểm soát truy cập

262. Yếu tố nào sau đây được coi là hữu ích nhất trong việc kiểm soát truy cập khi bị tấn công từ bên ngoài ?

a) Sinh trắc học
b) Kerberos
c) Phần mềm antivirus
d) Đăng nhập hệ thống (System logs)

263. Điểm khác nhau chính giữa các hệ thống ngăn chặn đột nhập (IPS) và phát hiện đột nhập (IDS) là:

a) IDS có khả năng phát hiện và ngăn chặn tấn công tốt hơn IPS
b) IPS có khả năng chủ động ngăn chặn tấn công so với IDS
c) IPS có chi phí lớn hơn IDS
d) IPS có khả năng phát hiện và ngăn chặn tấn công tốt hơn IDS

264. Để đánh giá điểm mạnh của hệ thống IDS người ta dựa vào các yếu tố sau :

a) Cách thực hiện, biểu hiện mà nó ghi nhận, những đặc trưng ghép nối hoặc tích hợp
b) Khởi sự, Cách thực hiện, biểu hiện mà nó ghi nhận
c) Khởi sự, giám sát vị trí, những đặc trưng ghép nối hoặc tích hợp
d) Tất cả đều đúng

265. Khi thực hiện triển khai HIDS khó khăn gặp là

a) Chi phí lắp đặt cao, khó bảo quản và duy trì
b) Thường xuyên cài đặt lại phải khi hệ thống mạng thay đổi hệ điều hành
c) Thường xuyên phải cập nhật bảng vá lỗi
d) Giới hạn tầm nhìn mạng, phải xử lí với nhiều hệ điều hành khác trên mạng.

266. Bộ lọc gói thực hiện chức năng nào ?

a) Cho phép tất cả các gói rời mạng
b) Loại trừ sự xung đột trong mạng
c) Cho phép tất cả các gói đi vào mạng
d) Ngăn chặn các gói trái phép đi vào từ mạng bên ngoài

267. Hệ thống nào được cài đặt trên Host để cung cấp một tính năng IDS ?

a) VPN
b) N-IDS (Network-based IDS)
c) Network sniffer
d) H-IDS (Host-based IDS)

268. Tổ chức chính cấp phát chứng chỉ được gọi là :

a) RA
b) LRA
c) CA
d) CRL

269. Các phát biểu sau đây phát biểu là là đúng nhất

a) Firewall là một giải pháp giúp hệ thống phát hiện và ngăn chặn các truy cập trái phép
b) Firewall là một vành đai phòng thủ cho máy tính hoặc hệ thống trước những tấn công
c) Firewall là một phần mềm hoặc phần cứng có khả năng ngăn chặn tấn công từ bên trong và bên ngoài vào hệ thống.
d) Firewall là một điểm chặn của trong quá trình điều khiển và giám sát.

270. Các biện pháp được sử dụng để đảm bảo an toàn máy tính và dữ liệu là:

a) Vấn đề về phòng chống phần mềm độc hại, giám sát mạng
b) Việc sao lưu tạo dự phòng dữ liệu, đảm bảo dữ liệu không bị mất mát khi xảy ra sự cố
c) Các kỹ thuật và hệ thống pháp hiện, ngăn chặn tấn công, xâm nhập.
d) Đảm bảo an toàn hđh, máy tính, dịch vụ; sử dụng tường lửa, proxy.

271. Anh em có thấy Hà tư bản bóc lột vcl không? :<

a) Có
b) Bóc lột vl
c) Bắt anh em làm trâu làm ngựa
d) Yes

Phím trả lời

1. a) An ninh tổ chức, An ninh mạng và An ninh hệ thống
2. a) An toàn công nghệ thông tin và Đảm bảo thông tin
3. c) Do có nhiều thiết bị kết nối mạng Internet với nhiều nguy cơ và đe dọa
4. d) Việc đảm bảo các thuộc tính an ninh, an toàn của hệ thống thông tin
5. a) Quản lý bộ phận
6. b) Phòng vệ nhiều lớp có chiều sâu
7. a) Quản lý rủi ro
8. c) Bí mật và Toàn vẹn
9. b) Vùng mạng WAN
10. d) Là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép
11. c) Định kỳ cập nhật thông tin về các lỗ hổng từ các trang web chính thức
12. d) !$aLtNb83
13. d) Tăng khả năng mã tấn công được thực hiện
14. d) Điểm yếu hệ thống có thể xuất hiện trong cả các mô đun phần cứng và phần mềm
15. a) Quản lý cao cấp
16. b) Hệ thống phần cứng và Hệ thống phần mềm
17. c) Tất cả các khâu trong quá trình phát triển và vận hành
18. d) Giảm thiểu các lỗ hổng bảo mật
19. b) SQL Server 2000
20. d) Năm lần nổ lực login thất bại trên tài khoản “jsmith”
21. c) Điều khiển truy nhập, tường lửa, proxy và các giao thức bảo mật, ứng dụng dựa trên mật mã
22. d) An toàn máy tính và dữ liệu, An ninh mạng, Quản lý ATTT và Chính sách ATTT
23. c) Bí mật, Toàn vẹn và Sẵn dùng
24. a) Các điều kiện bên trong và bên ngoài hệ thống thay đổi theo thời gian
25. 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
26. c) Bảo vệ vật lý, VPN, hoặc mã hóa
27. c) Sử dụng kỹ thuật tạo dự phòng ngoại vi

28. c) Lập trình phần mềm
29. a) Lỗi tràn bộ đệm
30. c) Lớp an ninh hệ thống
31. a) Địa chỉ trở về của hàm
32. c) Phần mềm độc hại
33. b) vùng người dùng
34. d) vùng hệ thống và ứng dụng
35. b) vùng mạng WAN
36. d) Cân bằng giữa An toàn, Hữu dụng và Rẻ tiền
37. b) Tin tặc và các phần mềm độc hại
38. a) Giám đốc điều hành
39. d) Phần cứng (Hardware), phần mềm (Software), cơ sở dữ liệu (Databases), hệ thống mạng (Networks), tập các lệnh kết hợp (Procedures).
40. a) A = (Uptime)/(Uptime + Downtime).
41. d) Lập kế hoạch (Plan), Thực thi kế hoạch (Do), Giám sát kết quả thực hiện (Monitor), Thực hiện các kiểm soát (Control).
42. c) Chính sách an toàn ở mức người dùng (User security policy).
43. a) tính hợp lệ (validity) ... sự chính xác (accuracy).
44. d) Lớp an ninh cơ quan/tổ chức (Plant Security), Lớp an ninh mạng (Network Security), Lớp an ninh hệ thống (System Integrity).
45. c) Coi nhẹ hoặc vi phạm các chính sách an ninh an toàn; đưa CD/DVD/USB với các files cá nhân vào hệ thống; thiếu ý thức về vấn đề an ninh an toàn.
46. c) vùng truy cập từ xa
47. b) Đưa CD/DVD/USB với các files cá nhân vào hệ thống; người dùng tải ảnh, âm nhạc, video; truy nhập trái phép vào máy trạm.
48. b) Nhân viên
49. b) Tường lửa, mạng riêng ảo (VPN).
50. a) Sử dụng cơ chế cấm thực hiện mã trong dữ liệu
51. a) Tăng khả năng mã tấn công được thực hiện
52. d) Điểm yếu hệ thống có thể xuất hiện trong cả
53. a) Ngăn xếp (Stack) và vùng nhớ cấp phát
54. a) Bất kỳ điểm yếu nào trong hệ thống cho

các mô đun phần cứng và phần mềm

động (Heap)

phép mối đe dọa có thể gây tác hại

55. b) Tất cả các khâu trong quá trình phát triển và vận hành

56. d) Giảm thiểu các lỗ hổng bảo mật

57. d) SQL Server 2000

58. a) Các ứng dụng

59. c) Mã máy

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

61. d) Lập trình phần mềm

62. c) Lỗi tràn bộ đệm

63. c) Trojan horse

64. a) Intrusion Detection System

65. d) Nguy hiểm, Quan trọng, Trung bình, Thấp

66. a) Có thể khiến cho ứng dụng ngừng hoạt động, gây mất dữ liệu hoặc thậm chí giúp kẻ tấn công kiểm soát hệ thống

67. b) Không dùng user quản trị (root hoặc admin) để chạy các chương trình ứng dụng

68. d) Các dữ liệu được đưa ra bởi hệ thống

69. b) Dữ liệu / Khả năng

70. d) Đoạt quyền

71. b) Sử dụng các công cụ phân tích mã tự động tìm các điểm có khả năng xảy ra lỗi

72. c) Chọn mật khẩu đủ mạnh để sử dụng

73. d) Sử dụng mật khẩu và quyền phù hợp để truy cập

74. d) Người dùng được quyền truy nhập vào mọi tác vụ của hệ thống

75. a) Trật tự / Hành vi

76. d) Tất cả các đáp

77. c) Buffer Overflows

78. c) Khoảng thời gian / Chèn mã độc

79. d) Tất cả đều đúng

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

81. c) Sâu có khả năng tự lây lan mà không cần tương tác của người dùng

82. b) Interruptions

83. a) Thụ động

84. c) Modifications

85. b) Các yêu cầu ICMP hoặc các yêu cầu phát

86. a) Smurf

87. a) Fabrications

quảng bá

88. a) Broadcast

89. c) Máy khách/trình duyệt web

90. d) SQLmap

91. a) Phạm vi tấn công

92. c) Gửi thư rác, thư quảng cáo

93. c) Thử các từ có tần suất sử dụng cao làm mật khẩu trong từ điển

94. b) Lây lan thông qua khả năng thực thi từ xa

95. b) Ping of death

96. c) Cản trở người dùng hợp pháp truy nhập các tài nguyên hệ thống

97. c) Độ dài từ 8 ký tự trở lên, gồm chữ cái hoa, thường, chữ số và ký tự đặc biệt

98. d) Chiếm quyền điều khiển hệ thống

99. a) Sử dụng chứng chỉ số để xác thực thông tin nhận dạng các bên

100. a) Các file tài liệu của bộ phần mềm Microsoft Office

101. a) Người dùng

102. b) UNION SELECT

103. b) Kỹ thuật xã hội

104. a) Virus, worm, zombie

105. d) Sửa đổi các chương trình

106. d) Reflectors

107. a) Để vượt qua các hàng rào kiểm soát an ninh

108. d) DAC

109. a) Cấm tự động thực hiện macro trong Microsoft Office

110. d) SYN Cache

111. b) Thực hiện tấn công DDoS

112. a) Đánh cắp thông tin nhạy cảm của người dùng

113. a) SQLi, XSS, CSRF và Buffer overflow

114. a) Thủ tục cơ sở dữ liệu cho phép tách mã lệnh SQL khỏi dữ liệu người dùng

115. c) Tấn công chèn mã SQL

116. b) Sử dụng các thư viện lập trình an toàn //or sử dụng cơ chế cấm thực hiện mã trong dữ liệu (DEP)

117. c) Địa chỉ máy nạn nhân làm địa chỉ nguồn của gói tin

118. b) Zombies

119. c) Một lỗi hoặc một khiếm khuyết tồn tại trong hệ thống

120. c) Lỗ hổng là bất kỳ điểm yếu nào trong hệ thống cho phép

mối đe dọa có thể gây tác hại

121. a) Không thể triệt tiêu được hết các lỗ hỏng, nhưng có thể giảm thiểu các mối đe dọa, qua đó giảm thiểu khả năng bị tận dụng để tấn công

122. c) Interceptions

123. a) Sửa đổi dữ liệu trong file

124. a) Tràn bộ đệm

125. a) Dữ liệu đầu vào từ người dùng hoặc từ các nguồn khác không được kiểm tra hoặc kiểm tra không kỹ lưỡng

126. b) Người dùng được quyền truy nhập vào mọi tác vụ của hệ thống

127. a) Flooding attacks

128. d) Ngập lụt

129. a) Sử dụng mật khẩu mạnh

130. a) Một lượng lớn yêu cầu giả mạo với địa chỉ nguồn là địa chỉ máy nạn nhân đến một số lớn các máy khác được gửi đi

131. b) Kẻ tấn công bắt buộc người dùng truy cập vào đường dẫn giả mạo

132. d) Sử dụng phương pháp truyền tin TCP

133. c) Thường được “nhúng” vào các chương trình bình thường và thường hẹn giờ để “phát nổ” trong một số điều kiện cụ thể

134. c) Mã độc / Có ích

135. a) Thực thi gián tiếp các tác vụ, mà tác giả của chúng không thể thực hiện trực tiếp do không có quyền truy nhập

136. a) Kiểm soát / Tấn công

137. d) Giai đoạn phát tán: Virus kiểm soát những chương trình mà nó đã tiếp xúc

138. d) Cần sự đồng ý từ người dùng để lây lan từ máy này sang máy khá

139. d) Trojan horse

140. c) Mã hóa khóa bất đối xứng sử dụng khóa công khai

141. a) 16

142. b) (e = 7 , d =23)

143. b) Tạo một giá trị băm có độ dài cố định 160

144. d) Phương pháp mã hóa và không gian khóa

bit

145. c) XOR

146. b) 128 bit

147. b) MDC là loại hàm băm không khóa, còn MAC là loại hàm băm có khóa

148. d) Tốc độ chậm

149. b) Nén và dễ tính toán

150. d) Tính khó của việc phân tích số nguyên rất lớn

151. b) Bằng khoảng một nửa kích thước của modulo n

152. d) Sử dụng một khóa quá trình mã hóa và một khóa khác cho giải mã

153. d) Sử dụng một khóa chung cho cả quá trình mã hóa và giải mã

154. b) 16

155. b) Vào 6 bít và ra 4 bít

156. c) Checksum

157. c) 80

158. a) mạng hoán vị-thay thế

159. d) Khó khăn trong quản lý và phân phối khóa

160. a) 12

161. a) Mã hóa mật khẩu

162. a) Sử dụng hàm băm có khóa MAC

163. b) 56 bít

164. b) Từng bít hoặc từng byte/ký tự

165. c) e và Phi(n) là 2 số nguyên tố cùng nhau

166. a) DES, 3-DES, AES

167. a) d là modulo nghịch đảo của e

168. c) State

169. a) PGP

170. a) 160 bít

171. a) SubBytes, ShiftRows, MixColumns, AddRoundKey

172. b) Văn bản mã.

173. c) Hiệu quả.

174. a) RS.

175. c) AES

176. a) Không đối xứng

177. d) Xung đột

178. d) Khoá cá nhân của bạn

179. b) Tất cả các phương án trên

180. b) 128 bit

181. b) Có thể công khai public key nhưng phải đảm bảo tính xác thực và cần giữ bí mật private key

182. d) 128, 160 và 192 bit

183. c) 56 bit

184. b) 10

185. c) Mỗi cột của ma trận state được nhân với một đa thức

186. a) Mã hóa khóa bí mật sử dụng một mã (key) cho cả quá trình mã hóa và giải mã

187. a) Trao đổi khóa dễ dàng hơn

188. a) Có thuật toán encryption tốt,có một khóa bí mật được biết bởi người nhận/gửi và kênh truyền bí mật để phân phát key

189. b) Triple–DES, RC4, RC5, IDEA

190. b) Tất cả đều đúng

191. d) Data Encryption Standard

192. c) Thuật toán mã hóa, giải mã, và tính an toàn của kênh truyền

193. c) Mã xác thực thông điệp (Message authentication code)

194. d) Toàn vẹn

195. d) Kiểm tra tính toàn vẹn dữ liệu

196. b) Biến đổi khối dữ liệu mã 6 bit thành 4 bit

197. c) 56 bit ngẫu nhiên và 8 bit kiểm tra “Parity”

198. c) 64 bit

199. a) 16

200. b) 64

201. b) Tất cả đều đúng

202. c) MAC

203. d) MAC cấp quyền truy cập dựa trên tính nhạy cảm của những thông tin và chính sách quản trị

204. d) 40 bit

205. a) Đọc xuống và ghi lên

206. a) Độ khó đoán và tuổi thọ của mật khẩu

207. a) Không yêu cầu biết trước thông tin về chúng

208. d) Tỷ lệ cảnh báo sai cao

209. d) Các hành vi tấn công, xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường

210. d) Bảo mật cao và luôn đi cùng với chủ thể

211. c) Phân biệt được các gói tin thuộc về các kết nối mạng khác nhau

212. b) Thống kê, học máy, khai phá dữ liệu

213. c) RBAC cấp quyền truy nhập dựa trên vai trò của người dùng trong tổ chức

214. a) DAC cho phép người tạo ra đối tượng có thể cấp quyền truy nhập cho người dùng khác

215. d) Acunetix Web Vulnerability Scanner

216. d) Mỗi đối tượng được gán một danh sách người dùng kèm theo quyền truy nhập

217. b) Các hiểm họa từ bên trong

218. c) IPS có khả năng chủ động ngăn chặn xâm nhập

219. d) Chỉ các thông tin trong header của gói tin

220. b) Các phần mềm quét virus xung đột với nhau

221. c) MAC cấp quyền truy nhập dựa trên tính nhạy cảm của thông tin và chính sách quản trị

222. d) Application-level gateway

223. c) Thẻ bài (token)

224. b) Thẻ ATM và số PIN

225. d) Chứng chỉ số khóa công khai

226. a) Do chữ ký của chúng chưa tồn tại trong hệ thống

227. b) Có cơ chế xác thực mạnh hơn

228. b) Sử dụng vân tay

229. a) Kiểm soát dịch vụ và hướng

230. c) DAC, MAC và RBAC

231. d) Tính bí mật, tính toàn vẹn và tính sẵn dùng

232. c) 2

233. d) Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập

234. d) Authentication và Authorization

235. b) Phát hiện xâm nhập dựa trên chữ ký thường có tỷ lệ phát hiện đúng cao hơn

236. d) Là quá trình xác minh tính chân thực của thông tin nhận dạng người dùng cung cấp

237. c) PIN

238. d) Đa yếu tố (multi-factor)

239. c) Chi phí đắt

240. d) Chống được tấn công phát lại

241. c) Bắt tay 3 bước

242. c) Xác thực

243. a) Không dùng tài khoản có quyền quản trị để chạy các chương trình ứng dụng

244. a) Firewall

245. a) Các hành vi tấn công, xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường

246. d) Mạng và các host

247. b) Xác thực, trao quyền và quản trị

248. d) Xác thực với mật khẩu

249. c) DAC cho phép người tạo ra đối tượng có thể cấp quyền quy cập cho người dùng khác

250. a) DAC và Role-BAC

251. b) RBAC cấp quyền truy cập dựa trên vai trò của người dùng trong tổ chức

252. b) Tất cả đều đúng

253. c) Nhái địa chỉ IP, tấn công giữa, tấn công biên

254. c) Access Control List

255. a) No access

256. b) Phải được ủy quyền

257. c) Ngăn chặn truy cập từ một địa chỉ MAC nhất định.

258. b) Tối mật (Top Secret - T), Tuyệt mật (Secret - S), Mật (Confidential - C), Không phân loại (Unclassified - U).

259. b) Danh sách điều khiển truy cập (ACL).

260. a) PIN

261. d) Kiểm soát truy cập

262. d) Đăng nhập hệ thống (System logs)

263. b) IPS có khả năng chủ động ngăn chặn tấn công so với IDS

264. c) Khởi sự, giám sát vị trí, những đặc trưng ghép nối hoặc tích hợp

265. d) Giới hạn tầm nhìn mạng, phải xử lí với nhiều hệ điều hành khác trên mạng.

266. d) Ngăn chặn các gói trái phép đi vào từ mạng bên ngoài

267. d) H-IDS (Host-based IDS)

268. c) CA

269. b) Firewall là một vành đai phòng thủ cho máy tính hoặc hệ thống trước những tấn công

270. b) Việc sao lưu tạo dự phòng dữ liệu, đảm bảo dữ liệu không bị mất mát khi xảy ra sự cố

271. a) Có , b) lột vl Bóc , d) Yes , c) Bắt anh em làm trâu làm ngựa