QUIZIZZ bảng tính

An toàn hệ điều hành 230 câu

Tổng số câu hỏi: 232

Thời gian làm bài: 2 giờ 57 phút

Tên người hướng dẫn: B21DCAT026_ Anh

Tên

Lớp học

Ngày

1. Đâu không phải tính năng/công cụ do hệ điều hành cung cấp?

a) Trình điều khiển thiết bị

b) Tính năng an toàn và bảo mật

c) Giao diện đồ họa

d) Thành phần quản trị mạng

2. Kiến trúc an toàn và quá trình thiết kế - xây dựng hệ thống có thể thực hiện theo cách ...

a) Kiến trúc an toàn phải được thực hiện trước toàn bộ

b) Kiến trúc an toàn có thể được thực hiện sau

c) Kiến trúc an toàn phải cần được thực hiện trước một bước

d) Có thể thực hiện song song các việc trên

3. Phần nhân an toàn cần phải nhỏ nhất có thể để ... của nó một cách dễ dàng

a) Xác định tính đúng đắn

b) Xác định tính toàn vẹn

c) Xác định tính ổn định

4. Kiến trúc an toàn tránh phụ thuộc vào tính bí mật để đảm bảo an toàn, ngoài trừ việc ...

a) Quản lí tài nguyên

b) Quản lí tài khoản

c) Quản lí tài khoản và mật khẩu

d) Quản lí mật khẩu

5. Danh sách kiểm soát truy cập được sử dụng thay thế ma trận kiểm soát truy cập do ma trận kiểm soát truy cập ...

a) Có hiệu quả sử dụng bộ nhớ kém

b) Là ma trận thưa

c) Kích thước quá lớn

d) Có tốc độ truy cập chậm

6. Nhân an toàn là phần cơ sở nền tảng có thể ... của hệ điều hành để đảm bảo an toàn cho hệ thống

a) Phân tích được
b) Thống kê được
c) Kiểm chứng được
d) Xác minh được

7. Các thuộc tính của bộ giám sát tham chiếu đảm bảo yêu cầu an toàn:

a) Ngăn chặn hoàn toàn, Chống xâm nhập, Xác minh được
b) Ngăn chặn một phần, Xác minh được
c) Chống xâm nhập, Xác minh được
d) Ngăn chặn một phần, Chống phá hoại, Xác minh được

8. Bộ giám sát tham chiếu bao gồm:

a) Giao tiếp và Kho chính sách
b) Giao tiếp, Mô đun xác thực và Kho chính sách
c) Giao tiếp và Mô đun xác thực
d) Mô đun xác thực và Kho chính sách

9. Kho chính sách là cơ sở dữ liệu gồm: Các trạng thái bảo vệ, ..., ...

a) Các nhãn tiến trình / Các trạng thái chủ thể
b) Các nhãn tiến trình / Các thao tác chủ thể
c) Các nhãn chủ thể / Các trạng thái tiến trình
d) Các nhãn trạng thái / Các trạng thái dịch chuyển

10. Các cơ chế an toàn không được ảnh hưởng tới người dùng theo nghĩa chúng phải ...

a) Trong suốt với người dùng bình thường
b) Trong suốt với người dùng quản trị
c) Đơn giản với người dùng bình thường
d) Đơn giản với người dùng quản trị

11. Truy cập hệ thống được mô tả bằng ... có thể thực hiện ... lên ...

a) Đối tượng, Thao tác, Chủ thể
b) Chủ thể, Đối tượng, Thao tác
c) Đối tượng, Chủ thể, Thao tác
d) Chủ thể, Thao tác, Đối tượng

12. Đâu là một cơ chế hay biện pháp bảo vệ?

a) Hệ thống bảo vệ bắt buộc
b) Danh sách kiểm soát truy cập
c) Ma trận bảo vệ
d) Hệ thống bảo vệ
e) Ma trận kiểm soát truy cập

13. Một trong số các quy tắc đảm bảo an toàn liên quan đến cấp quyền cho chủ thể là:

a) Quyền tối thiểu
b) Quyền liên tục
c) Không cấp quyền
d) Quyền tối đa

14. Đâu không phải là một yếu tố giúp xây dựng hệ điều hành an toàn?

a) Mục tiêu an toàn
b) Mô hình an toàn
c) Cơ chế bảo vệ
d) Mô hình đe dọa
e) Mô hình tin cậy

15. Các chức năng cơ bản của HĐH bao gồm:

a) Quản lí tiến trình, bộ nhớ và giao diện người dùng
b) Quản lí tiến trình, bộ nhớ và người dùng
c) Quản lí người dùng, đĩa và hệ thống file
d) Quản lí tiến trình, bộ nhớ, đĩa và hệ thống file

16. Các nhãn trong hệ thống bảo vệ bắt buộc chống lại việc xâm nhập nhờ chúng được xây dựng bởi người quản trị tin cậy sử dụng phần mềm tin cậy và chúng cũng không bị thay đổi bởi ...

a) Các tiến trình không tin cậy của người dùng
b) Các tiến trình không tin cậy của hệ thống
c) Các tiến trình tin cậy của người dùng
d) Các tiến trình tin cậy của hệ thống

17. CSDL về kiểm soát truy cập: Thể hiện trạng thái an toàn của hệ thống và Chứa các thông tin như ...

a) Quyền truy cập và các thuộc tính an ninh
b) Quyền truy cập và các thao tác
c) Các thao tác truy cập và các thuộc tính an ninh

18. Trong hệ điều hành an toàn, việc thực thi của các phần mềm không bị phá vỡ bởi ...

a) các chương trình người dùng nằm trong danh sách các phần mềm tin cậy
b) các chương trình không nằm trong danh sách các phần mềm tin cậy
c) các phần mềm ứng dụng
d) các phần mềm độc hại

19. Mục tiêu an toàn (security goals) xác định các thao tác có thể được thực hiện bởi hệ thống trong khi ngăn chặn ...

a) Các truy nhập phá hủy
b) Các truy nhập gây rối
c) Các truy nhập thông thường
d) Các truy nhập trái phép

20. Chính sách an toàn (security policy) mô tả các ... cần được thực hiện cho hệ thống thông tin

a) giám sát, hành động và hình thức
b) kiểm soát và quy trình
c) kiểm soát, hành động và quy trình
d) hành động và quy trình

21. Trong hệ điều hành an toàn, một phần mềm không được coi là tin cậy khi nó ...

a) Bị gây nhiễu
b) Bị phá hủy
c) Bị xâm nhập

22. Hệ điều hành không cung cấp gì?

a) Một số các dịch vụ và ứng dụng cơ bản cho người dùng
b) Môi trường cho các chương trình ứng dụng hoạt động
c) Một hệ thống toàn diện
d) Giao diện giữa người dùng và phần cứng máy tính / thiết bị tính toán

23. Trong ATHDH, tính sẵn dùng hạn chế các tài nguyên mà các chủ thể có thể sử dụng do các chủ thể này có thể ...

a) Chiếm quyền kiểm soát hệ thống
b) Làm cạn kiệt các tài nguyên hệ thống
c) Làm cạn kiệt các tài nguyên đó
d) Làm cạn kiệt các tài nguyên bộ nhớ

24. Các tập nhãn trong hệ thống bảo vệ bắt buộc chống lại việc xâm nhập nhờ chúng được xây dựng bởi ... và không thể thay đổi bởi ...

a) Người quản trị hệ thống / Tiến trình người dùng
b) Người quản trị tin cậy / Tiến trình hệ thống
c) Người quản trị hệ thống / Tiến trình hệ thống
d) Người quản trị tin cậy / Tiến trình người dùng

25. Các phần mềm tin cậy trong mô hình tin cậy bao gồm:

a) Các phần mềm xác định và thực hiện các yêu cầu an toàn của hệ thống
b) Các phần mềm xác thực và cấp quyền người dùng
c) Các phần mềm xác định và thực hiện các yêu cầu an toàn của người dùng
d) Các phần mềm xác thực, cấp quyền và quản trị người dùng

26. Mô hình đe dọa (Threat model) xây dựng tập các thao rác mà người tấn công có thể dùng để ...

a) Đánh cắp dữ liệu từ hệ thống
b) Truy cập trái phép vào hệ thống
c) Vô hiệu hóa hệ thống

27. Để đạt được độ tin cậy cao về an toàn của hệ thống, người thiết kế cần ... của các phần liên quan tới an toàn của thiết kế

a) Giảm thiểu kích cỡ và độ phức tạp
b) Giảm thiểu độ phức tạp tính toán và mã
c) Giảm thiểu kích cỡ mã nguồn và mã thực hiện
d) Giảm thiểu kích cỡ mã thực hiện và dữ liệu

28. Miền bảo vệ của ma trận kiểm soát truy cập bao gồm: Tập (1)... mà tiến trình có thể truy cập và Các (2)... mà tiến trình có thể sử dụng để truy cập tới các (1)...

a) Đối tượng, Thao tác
b) Chủ thể, Đối tượng
c) Chủ thể, Thao tác

29. Mô hình tin cậy (Trust model) của hệ thống định nghĩa tập ... mà hệ thống sử dụng để đảm bảo thực hiện chính xác các mục tiêu an toàn của hệ thống

a) Chủ thể và đối tượng
b) Phần mềm và dữ liệu
c) Thực thể và thao tác
d) Thực thể và đối tượng

30. Đâu không phải là một phiên bản của hệ điều hành Microsoft Windows?

a) Windows NT 3, 4
b) Windows XP
c) Windows Me
d) MS-DOC, PC-DOS

31. Các yêu cầu đảm bảo an toàn hệ điều hành gồm:

a) Tính bí mật, sẵn dùng
b) Tính bí mật, toàn vẹn và sẵn dùng
c) Tính toàn vẹn và sẵn dùng
d) Tính chống chối bỏ và xác thực được

32. Đâu không là hệ điều hành máy tính?

a) Windows 10
b) Cisco IOS
c) MacOS
d) Ubuntu

33. Hệ điều hành - OS (theo Wikipedia) là:

a) Một chương trình quản lí máy tính
b) Một chương trình giữa phần cứng và phần mềm
c) Một chương trình chính cung cấp giao diện cho người dùng sử dụng hệ thống máy tính
d) Một chương trình quản lí các tài nguyên phần cứng và phần mềm của thiết bị tính toán

34. Hệ thống bảo vệ bắt buộc là hệ thống chỉ có thể được sửa đổi bởi ... thông qua phần mềm tin cậy

a) Người quản trị hệ thống
b) Chủ thể tin cậy
c) Người dùng tin cậy
d) Người quản trị tin cậy

35. Trong an toàn hệ điều hành, tính bí mật giới hạn ...

a) Các đối tượng mà chủ thể có thể ghi / sửa đổi
b) Các đối tượng có thể được truy cập
c) Các tài nguyên mà các chủ thể có thể sử dụng

36. Các loại chính sách an toàn thông tin bao gồm:

a) Chính sách chung và chính sách cho đơn vị cụ thể
b) Chính sách chung cho từng tổ chức và chính sách cho từng đơn vị cụ thể
c) Chính sách chung và chính sách cho ứng dụng cụ thể
d) Chính sách toàn cục và chính sách cụ thể

37. Phần cứng hỗ trợ ảo hóa giúp cải thiện ... của các phần mềm ảo hóa và nhờ vậy dễ được người dùng chấp nhận hơn

a) Hiệu năng
b) Tính năng
c) Chất lượng
d) Tốc độ

38. Trong hệ thống các lớp bảo vệ, các lớp ... được bảo vệ chặt chẽ nhất vì trực tiếp truy cập / sử dụng các tài nguyên quan trọng

a) Lớp 2, 4
b) Lớp 1, 3
c) Lớp 1, 2
d) Lớp 0, 1

39. Trong các HĐH hiện nay: Không gian nhớ của tiến trình được quản lý và cấp phát theo khối nhớ hay ... với kích cỡ hợp lí

a) Trang
b) Đoạn
c) Mục
d) Phần

40. Hỗ trợ từ phần cứng cho phép ... giữa hệ thống ảo hóa và bộ phận giám sát (hệ thống chủ) và cấp các thiết bị vào/ra một cách an toàn cho các hệ thống ảo hóa

a) Trao đổi nhanh chóng
b) Chuyển đổi nhanh chóng
c) Trao đổi hiệu quả
d) Chuyển đổi hiệu quả

41. Trong mô hình các lớp bảo vệ, chủ thể có cấp độ ... thì không thể truy cập trực tiếp đối tượng có cấp độ ...

a) Thấp, thấp hơn
b) Thấp, cao hơn
c) Cao hơn và thấp hơn
d) Cao, thấp hơn

42. Các yêu cầu cơ bản với máy tính cho phép ảo hóa bao gồm:

a) Tính hiệu quả, Kiểm soát truy cập, Bình đẳng
b) Tính mềm dẻo, Kiểm soát truy cập, Bình đẳng
c) Tính mềm dẻo, Điều khiển truy cập, Bình đẳng
d) Tính hiệu quả, Kiểm soát tài nguyên, Bình đẳng

43. Các tiến trình dịch vụ có thể trao đổi thông tin với nhau qua:

a) Các kênh được kiểm soát hỗ trợ bởi HĐH
b) Các kênh giao tiếp tự phát triển
c) Các kênh được kiểm soát hỗ trợ bởi máy chủ dịch vụ
d) Các kênh giao tiếp cung cấp bởi các nền tảng CNTT

44. Yêu cầu bảo vệ bộ nhớ của hệ điều hành: Các tiến trình người dùng cần được cách ly về không gian bộ nhớ ... và các tiến trình hệ thống

a) Với tiến trình ngầm
b) Với nhân hệ điều hành
c) Với nhau
d) Với các dịch vụ

45. Trường hợp phần cứng không hỗ trợ vào/ra, tiến trình người dùng cũng không thể sinh ra ... mà không có sự can thiệp của hệ điều hành

a) Các tính năng
b) Các truy vấn
c) Các câu lệnh vào/ra
d) Các yêu cầu

46. Các lớp bảo vệ đặt ra các ranh giới chặt chẽ và các mô tả các ... được phép truy cập và các ... được phép thực hiện cho mỗi tiến trình hoạt động trong từng lớp

a) Tiến trình, Thao tác
b) Tài nguyên, Thao tác
c) Chủ thể, Thao tác
d) Tài nguyên, Tiến trình

47. Các cơ chế bảo vệ được thực hiện bằng phần cứng có các ưu điểm so với cơ chế bảo vệ được thực hiện bằng phần mềm do các cơ chế này:

a) Miễn nhiễm với các loại mã độc
b) Không bị tác động bởi các phần mềm khác
c) Được hỗ trợ mạnh bởi các hãng phát triển
d) Hoạt động trong môi trường cô lập

48. Hệ điều hành cần phải giám sát và ngăn chặn mọi yêu cầu truy cập trái phép của một ... đến không gian bộ nhớ của một tiến trình khác

a) Dịch vụ
b) Tiến trình người dùng
c) Tiến trình hệ thống
d) Tiến trình ngầm

49. Ảo hóa (Virtualization) theo nghĩa rộng là sự tách một tài nguyên hoặc một dịch vụ khỏi ... dùng để cung cấp nó

a) Các phương tiện vật lí
b) Các hệ thống phần cứng
c) Các đám mây dịch vụ
d) Các máy chủ

50. Khi hệ thống phân cấp các tiến trình theo các lớp bảo vệ (chế độ hệ thống/đặc quyền và chế độ người dùng) thì các tiến trình người dùng không được phép đọc ghi tùy tiện vào ...

a) Các file của hệ thống
b) Không gian nhớ của tiến trình khác
c) Dữ liệu của hệ thống
d) Không gian nhớ của hệ thống

51. Đâu là một phần mềm ảo hóa?

a) ESSi
b) EXSi
c) ESXn
d) ESXi

52. Root of Trust for storage (RTS) là cơ sở tin cậy cho việc ...

a) Tính toán
b) Báo cáo
c) Lưu trữ
d) Đo kiểm

53. RPL là trường trên thẻ chọn ...

a) Đoạn tổng hợp
b) Đoạn ngăn xếp
c) Đoạn dữ liệu
d) Đoạn mã

54. Bộ tham chiếu an toàn (SRM) là phần mềm ... và nhận các tham số đầu vào thẻ tiến trình, SID của đối tượng và tập thao tác, trả về kết quả của yêu cầu truy cập trên cơ sở ACL mà nó tìm thấy

a) Chạy trong lớp bảo vệ
b) Chạy trong không gian tùy chọn
c) Chạy trong không gian người dùng
d) Chạy trong nhân

55. Đâu là khóa dùng để mã hóa dữ liệu của dịch vụ mã hóa ổ cứng kết hợp với TPM để tăng khả năng bảo vệ do Microsoft cung cấp?

a) FVEK
b) SRK
c) VMK
d) FVMK

56. Câu lệnh vào/ra sẽ chỉ được thực hiện khi mức độ đặc quyền của đoạn mã ... với mức đặc quyền của lệnh vào/ra

a) bằng
b) nhỏ hơn hoặc bằng
c) nhỏ hơn
d) lớn hơn hoặc bằng

57. Tên đầy đủ của trường RPL là ...

a) Requested Previlege Level
b) Required Privilege Level
c) Requested Privilege Level
d) Required Previlege Level

58. Cơ chế ngăn chặn thực thi dữ liệu (DEP) là kĩ thuật bảo vệ bộ nhớ ở mức hệ thống được tích hợp vào hệ điều hành. Cụ thể, DEP cho phép hệ thống ... một hay nhiều trang bộ nhớ là không thực thi được

a) Kiểm soát
b) Xóa
c) Chặn
d) Đánh dấu

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

a) Các không gian nhớ của các tiến trình phải được cách ly với nhau và với phần nhân của hệ điều hành
b) Các không gian nhớ của tất cả các tiến trình phải được cách ly với nhau
c) Các không gian nhớ của các tiến trình phải được cách ly với nhau và với phần vỏ của hệ điều hành
d) Các không gian nhớ của các tiến trình phải được cách ly với nhau và hệ thống sẽ chặn tất cả các truy cập trái phép

60. Một trong các tài nguyên được bảo vệ đối với các thao tác của tiến trình người dùng là ...

a) dữ liệu
b) mã lệnh
c) kết nối mạng
d) bộ nhớ

61. Các máy tính và phần mềm được cung cấp từ nhiều nhà sản xuất và phân phối khác nhau dẫn đến khó khăn trong việc xác định mức độ ... của hệ thống máy tính cũng như là phần mềm

a) tin cậy và tính năng
b) ổn định và tin cậy
c) tin cậy và hiệu năng
d) ổn định và tính năng

62. HĐH Windows sử dụng biện pháp kiểm soát truy cập nào?

a) DAC
b) DAD
c) CDA
d) ADC

63. Đâu không phải là một bộ phận chức năng của TPM?

a) Bộ nhớ ổn định
b) Bộ nhớ thay đổi
c) Bộ nhớ chỉ đọc
d) Bộ mã hóa

64. Việc kiểm soát thực thi lệnh có đặc quyền cao được thực hiện thông qua thẻ mô tả cổng. Một trong các loại cổng này là ...

a) call-gate
b) cell-gate
c) ret-gate
d) tsk-gate

65. Mô-đun TPM cung cấp cơ sở để đảm bảo an toàn cho các chương trình máy tính trong quá trình hoạt động cũng như tương tác với nhau thông qua việc sử dụng các cơ chế ... và mã hóa

a) giải mã
b) sinh khóa
c) định danh
d) xác thực

66. Mục đích chính của việc bảo vệ khởi động sử dụng TPM là đảm bảo ... cho chuỗi khởi động

a) tính sẵn dùng
b) tính bí mật
c) tính xác thực
d) tính toàn vẹn

67. Chương trình người dùng bị đóng trong "..." do đoạn mã của phần nhân đặt ra

a) hộp có giám sát
b) báo đóng
c) hộp mở
d) hộp kín

68. Mô hình kiểm soát truy cập của Windows có ưu điểm là ...

a) mềm dẻo và có khả năng triển khai tốt
b) nhanh và có khả năng biểu diễn tốt
c) đơn giản và có khả năng biểu diễn tốt
d) mềm dẻo và có khả năng biểu diễn tốt

69. Đâu là người dùng không sở hữu file nào và không thuộc nhóm nào trong Unix/Linux?

a) root
b) noone
c) anyone
d) nobody

70. Hai thành phần cơ bản của TPM được sử dụng để bảo vệ các phần mềm trong quá trình khởi động máy tính gồm:

a) RMT và RTR
b) RMT và TRR
c) RTM và RTR
d) RTM và RRT

71. Windows registry là cơ sở dữ liệu toàn cục được tổ chức theo ... để lưu các dữ liệu của Windows và toàn bộ các chương trình

a) cấu trúc đa cấp
b) cấu trúc vô cấp
c) mô hình đa cấp
d) mô hình phân cấp

72. Đâu là một trong số các vấn đề/lỗ hổng tiêu biểu trong Unix/Linux?

a) Các file chia sẻ
b) Các tiến trình chia sẻ
c) Các tài nguyên chia sẻ
d) Các nội dung chia sẻ

73. Các hệ thống Unix hiện đại sử dụng kỹ thuật ... bộ nhớ

a) phân đoạn
b) phân trang
c) phân khúc
d) phân chương

74. Kiến trúc tập lệnh x86 hỗ trợ việc quản lí thực thi các chương trình bằng cách triển khai cơ chế bảo vệ theo lớp đặc quyền dựa trên kiểm soát truy cập đến ... của chương trình

a) các câu lệnh
b) các câu lệnh và dữ liệu
c) các dữ liệu và hàm
d) các dữ liệu

75. Chương trình chạy trong chế độ ... bị hạn chế truy cập tới bộ nhớ, các cổng vào/ra

a) quyền cao
b) bình đẳng
c) người dùng
d) độ nhân

76. Trong Unix/Linux, chuỗi quyền truy cập rwxr-xr-- biểu diễn ở dạng thập phân là:

a) 754
b) 741
c) 321
d) 654

77. Trong Windows cũng như Unix/Linux, các tiến trình không tin cậy của người dùng có thể sửa đổi quyền truy cập đến dữ liệu của họ một cách tùy ý. Nguyên nhân của vấn đề này là do các hệ điều hành này sử dụng cơ chế kiểm soát truy cập ...

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

78. Các lệnh dùng để thay đổi chủ sở hữu và quyền truy cập trong Unix/Linux là:

a) chown và chmode
b) chowner và chmod
c) chown và chmod
d) chowner và chmode

79. Đâu không phải là một ứng dụng của TPM?

a) Bảo vệ mật khẩu
b) Mã hóa đĩa
c) Ngăn chặn thực thi dữ liệu
d) Đảm bảo toàn vẹn nền tảng

80. Kiến trúc x86 sử dụng phương pháp ... để quản lý không gian nhớ chương trình nhờ vào việc tách biệt các chức năng của không gian nhớ

a) phân đoạn
b) phân trang
c) bộ nhớ ảo
d) phân chương

81. Giá trị CPL cho biết ... của đoạn mã được thực hiện

a) mức độ truy cập
b) quyền truy cập
c) mức độ bảo vệ
d) quyền thực thi

82. Đâu là một trong các vấn đề/ lỗ hổng bảo mật tiêu biểu của Windows?

a) Có quá nhiều lỗi tràn bộ đệm
b) Người dùng quản trị
c) Người dùng ít kinh nghiệm
d) Nhân quá lớn

83. Đâu là công thức tính toán cơ sở tin cậy cho các đoạn mã?

a) PCR = H(PCR|H(đoạn mã))
b) PCR = H(mã mới)
c) PCR = H(H(mã mới)|PCR)
d) PCR = H(PCR|H(mã mới))

84. Windows cung cấp giao diện lập trình cho phép một tiến trình xâm nhập các tiến trình khác, như các hàm CreateRemoteThread, ... hay WriteProcessMemory

a) NewProcess
b) CreateProcess
c) Closeprocess
d) OpenProcess

85. Kiến trúc x86 hỗ trợ cơ chế này thông qua bit cấm thực thi đặt tại trang nhớ. Bit cấm thực thi được gọi là:

a) execute-disable
b) non-execute
c) disable-execute
d) un-execute

86. Các HĐH hiện đại thường sử dụng cơ chế phân trang để quản lý bộ nhớ. Mỗi trang nhớ được mô tả bởi khoản mục bảng trang PTE chứa hai trường phục vụ cho việc bảo vệ là:

a) cờ bẫy và cờ đọc ghi
b) cờ giám sát và cờ đọc/ghi
c) cờ giám sát và cờ tràn
d) cờ chẵn lẻ và cờ giám sát

87. Trong ..., các giá trị băm được tính toán và lưu trữ cố định vào TPM cho tất cả các thành phần/chương trình trong chuỗi

a) cơ sở tin cậy động
b) cơ sở tin cậy TPM
c) cơ sở tin cậy tĩnh
d) cơ sở tin cậy gốc

88. Hệ thống tin cậy (Trusted System) là một hệ thống dựa vào một mức độ cụ thể để thực thi một ... cụ thể

a) cơ chế bảo mật
b) chính sách bảo vệ
c) chính sách bảo mật
d) cơ chế bảo vệ

89. Đâu là một trong các tính năng ngầm định nguy hiểm của Windows?

a) Windows Firewall
b) Windows Defender
c) Windows Remote Registry
d) Windows Remote Services

90. Mô-đun nền tảng tin cậy (TPM - Trusted Platform Module) là tiêu chuẩn quốc tế dành cho bộ xử lý mật mã an toàn, với tên tiếng Anh là:

a) Cryptographic processor
b) cryptoprocessor
c) Encryption processor
d) Cryptprocessors

91. Cơ chế bảo vệ theo ... được thực hiện nhằm hạn chế các thao tác mà chương trình người dùng có thể thực hiện

a) không gian nhân và không gian người dùng
b) đặc quyền tối thiểu
c) phân quyền người dùng
d) lớp đặc quyền

92. Đâu là một trong các vấn đề/lỗ hổng tiêu biểu trong Unix/Linux?

a) TOCTOU
b) TOUTTOC
c) TOCTTOU
d) TOUTOC

93. Đâu là một dịch vụ mã hóa ổ cứng kết hợp với TPM để tăng khả năng bảo vệ do Microsoft cung cấp?

a) Bitlocker
b) Doorlocker
c) Winlocker
d) HDDlocker

94. Cổng ngắt và cổng bẫy được dùng để xử lý các ..., như bộ định thời, ổ cứng và các ngoại lệ, như lỗi trang nhớ, chia 0

a) ngắt phần cứng
b) ngắt CPU
c) ngắt phần mềm
d) ngắt ngoại lệ

95. Giá trị RPL chỉ có thể thay đổi được bởi các câu lệnh thay đổi ...

a) luồng thực hiện
b) luồng mã lệnh
c) bất kỳ lệnh nào
d) luồng dữ liệu

96. Mô hình khái quát của cơ chế bảo vệ của Windows cho phép mô tả các tổ hợp quyền nhưng lại không có bất cứ ... cụ thể được xác định trong hệ thống

a) mô hình an toàn
b) nhân an toàn
c) mục tiêu an toàn
d) chính sách an toàn

97. Quá trình khởi động được bảo vệ trong Windows KHÔNG gồm giai đoạn nào trong các mục sau:

a) Nạp Master Boot Record
b) WinLoad
c) Nạp Boot Manager
d) Nạp NTFS manager

98. Hệ thống bảo vệ của Windows có khả năng mở rộng và dễ biểu diễn các quyền cũng như là người dùng của hệ thống. Thực tế cho thấy, các cải thiện về tính mở rộng và biểu diễn có ảnh hưởng ... đến tính an toàn của hệ thống

a) ít ảnh hưởng
b) không ảnh hưởng
c) tích cực
d) tiêu cực

99. Đâu là một trong các vấn đề/lỗ hổng bảo mật tiêu biểu của Windows?

a) Sổ nhật ký
b) Sổ đăng ký
c) Sổ ký gửi
d) Sổ đăng nhập

100. Các thông tin trong thẻ mô tả đoạn gồm:

a) Base, Limit và CPL
b) Base, Limit và RPL
c) Base, Limit và DPL
d) Base, Length và RPL

101. Hệ điều hành sử dụng ... với không gian địa chỉ thống nhất để quản lý các dạng bộ nhớ vật lý, do vậy cần phải thực hiện việc ... từ địa chỉ lo-gic của chương trình thành địa chỉ vật lý thực sự trước khi thao tác đọc/ghi bộ nhớ được diễn ra

a) bộ nhớ ảo / truy cập
b) bộ nhớ thực / ánh xạ
c) bộ nhớ thực / truy cập
d) bộ nhớ ảo / ánh xạ

102. Đâu là phần tên chung cho một HĐH Windows vừa có bản cho PC vừa có bản cho máy chủ?

a) Windows 2000
b) Windows 2008
c) Windows XP
d) Windows 2003

103. Unix sử dụng khái niệm ... cho tất cả các đối tượng lưu trữ hệ thống như lưu trữ thứ cấp (ổ đĩa), thiết bị vào/ra, mạng và liên lạc giữa các tiến trình

a) file
b) process
c) folder
d) item

104. Trong Unix/Linux, phần nhân tin cậy gồm các tiến trình nhân và cả các tiến trình chạy với định danh người dùng root. Điều này tạo ra ... cho các phần mềm an toàn quan trọng cũng như là nhân

a) hiệu năng cao
b) xung đột
c) bất ổn
d) lỗ hổng

105. Các thẻ mô tả đoạn nhớ được lưu trong hai bảng GDT và LDT. GDT và LDT tương ứng là:

a) Bảng mô tả nhân HĐH và Bảng mô tả chương trình người dùng
b) Bảng mô tả toàn bộ và Bảng mô tả cục bộ
c) Bảng mô tả toàn cục và Bảng mô tả cục bộ
d) Bảng mô tả đoạn mã và Bảng mô tả đoạn dữ liệu

106. Các cơ sở của tính đúng đắn trong Windows là ... và Windows có cơ sở tính toán tin cậy ... về kích cỡ cũng như hệ thống nhân có khả năng mở rộng

a) không đầy đủ / bị giới hạn
b) không chính tắc / không bị giới hạn
c) không khả thi / không bị giới hạn
d) không rõ ràng / bị giới hạn

107. Việc một tiến trình cố truy cập bộ nhớ không phải của mình sẽ gây ra ..., như là lỗi xâm phạm ô nhớ được bảo vệ, và làm cho tiến trình vi phạm phải chấm dứt hoạt động

a) lỗi ngoại lệ
b) lỗi phần cứng
c) lỗi hệ thống
d) lỗi phần mềm

108. Các mức độ đặc quyền của ... không liên quan tới vai trò người dùng trong hệ điều hành, dù là quản trị hay người dùng thông thường

a) nhân hệ điều hành
b) bộ xử lý
c) chương trình người dùng
d) bộ nhớ

109. Unix là hệ điều hành đầu tiên có ... và có giao diện chương trình (API) thuận tiện cho người phát triển

a) hiệu năng cao
b) tính khả dụng
c) tính dễ dùng
d) tính khả chuyển

110. BitLocker là dịch vụ ...

a) mã hóa dữ liệu trên ổ đĩa cứng
b) mã hóa dữ liệu trong CSDL
c) mã hóa dữ liệu truyền thông
d) mã hóa dữ liệu trên đám mây

111. Các chức năng của TPM được xây dựng bằng ..., song các chức năng an ninh cần được bảo vệ chặt chẽ được thực hiện thông qua ...

a) phần mềm / phần cứng
b) phần mềm / phần sụn
c) phần cứng / phần mềm
d) phần cứng / phần sụn

112. CPL là trường trên thẻ chọn ...

a) đoạn tổng hợp
b) đoạn dữ liệu
c) đoạn ngăn xếp
d) đoạn mã

113. Windows sử dụng danh sách kiểm soát truy cập ACL để đảm bảo an toàn. ACL bao gồm tập các mục kiểm soát truy cập. Một mục kiểm soát truy cập có tên viết tắt tiếng Anh là:

a) ACE
b) AEC
c) ACC
d) ECA

114. Hệ thống bảo vệ trong Unix/Linux sử dụng cơ chế kiểm soát truy cập ...

a) DAC
b) MAC
c) CAD
d) ACD

115. Giá trị này được duy trì bởi chính CPU và nó luôn bằng với ... hiện thời của CPU

a) mức bảo vệ
b) mức truy cập
c) quyền truy cập
d) quyền thực thi

116. Đâu không phải là một khái niệm công nghệ chính của một hệ thống tin cậy hoàn toàn?

a) Màn che bộ nhớ / thực thi được bảo vệ
b) Lưu trữ có niêm phong
c) Bộ nhớ phân đoạn
d) Đầu vào và đầu ra an toàn

117. Quá trình khởi động được bảo vệ và kết hợp với phần mềm chống mã độc trong Windows để nâng cao ... của hệ thống sử dụng BIOS truyền thống

a) tính toàn vẹn
b) tính bí mật
c) tính sẵn dùng
d) tính xác thực

118. Root of Trust for reporting (RTR) là cơ sở tin cậy cho việc ...

a) tính toán
b) lưu trữ
c) đo kiểm
d) báo cáo

119. TPM cung cấp hai cơ chế khác cho việc lưu trữ an toàn là ...

a) binding và saling
b) binding và sealing
c) billing và saling
d) billing và sealing

120. Root of Trust for Measurement (RTM) là cơ sở tin cậy cho việc ...

a) báo cáo
b) lưu trữ
c) đo kiểm
d) tính toán

121. Unix/Linux sử dụng các ... trong danh sách kiểm soát truy cập để xác định các quyền truy cập vào đối tượng của 3 nhóm chủ thể

a) bít chế độ
b) bít phân quyền
c) bít hệ thống
d) bít giám sát

122. Hệ thống Unix/Linux hiện đại cho phép ... thông qua các mô-đun có thể được nạp một cách linh hoạt vào nhân. Rootkit là dạng phần mềm độc hại khai thác tính năng này

a) bổ sung các tính năng
b) mở rộng nhân
c) sửa đổi nhân
d) bổ sung dịch vụ

123. Đâu là một trong các tính năng ngầm định nguy hiểm của Windows và các ứng dụng chạy trên Windows?

a) xp_cmdshell
b) MS C&C
c) xp_shellcmd
d) xp_cmdshells

124. Mục tiêu thiết kế của Unix là phát triển ... có thể ... giữa các người dùng với nhau

a) nền tảng chung / phân chia dễ dàng
b) nền tảng chia sẻ / chuyển đổi
c) nền tảng chung / chia sẻ dễ dàng
d) nền tảng riêng / chia sẻ dễ dàng

125. Mã của phần nhân hoạt động ở lớp ..., còn mã của chương trình người dùng hoạt động ở lớp ...

a) 3 và 1
b) 3 và 0
c) 0 và 3
d) 0 và 1

126. Việc lưu trữ an toàn hay tin cậy thường sử dụng ... một phần hoặc toàn bộ thiết bị lưu trữ nhằm đảm bảo tính bí mật của dữ liệu lưu trên thiết bị

a) chữ ký số
b) kỹ thuật mã hóa
c) kỹ thuật băm
d) kỹ thuật giấu tin

127. Đâu là một trong các vấn đề/lỗ hổng tiêu biểu của Unix/Linux?

a) Các biến môi trường
b) Các biến tĩnh
c) Các biến động
d) Các biển hệ thống

128. Tính toán tin cậy đòi hỏi thiết kế lại kiến trúc hệ thống sao cho các thành phần riêng lẻ được định nghĩa một cách ... các đặc tính của mình

a) khách quan
b) tường minh
c) chuẩn mực
d) đúng đắn

129. Đâu không phải là một khái niệm công nghệ chính của một hệ thống tin cậy hoàn toàn?

a) Khoá lưu trữ
b) Đầu vào và đầu ra an toàn
c) Khóa chứng thực
d) Lưu trữ có niêm phong

130. Đâu không phải là một ứng dụng của TPM?

a) Đảm bảo toàn vẹn giao dịch
b) Đảm bảo toàn vẹn nền tảng
c) Mã hoá đĩa
d) Quản lý bản quyền số

131. Vào/ra không ánh xạ thường ... tiến trình người dùng làm việc trực tiếp với các địa chỉ vật lý mà việc truy cập chỉ được kích hoạt từ hệ điều hành

a) chỉ dẫn
b) không cho phép
c) cho phép
d) cấp quyền cho

132. Các chương trình ứng dụng thường thuộc các lớp nào trong các lớp bảo vệ của hệ thống phân cấp không gian thực thi?

a) các lớp 1, 2
b) các lớp 0, 1
c) các lớp 3, 4
d) các lớp 0, 2

133. Trong HĐH hỗ trợ cơ chế ảo hóa bộ nhớ, các tiến trình người dùng truy cập bộ nhớ thông qua ... và con trỏ mô tả phần không gian nhớ lô-gic của tiến trình

a) bảng danh mục
b) bảng phân đoạn
c) bảng chỉ số
d) bảng cấp phát

134. Ảo hóa phần cứng làm giảm sự can thiệp của ... trong việc xử lý các vấn đề quản lý việc chuyển không gian địa chỉ và đặc quyền

a) phần mềm khách
b) phần mềm chủ
c) hệ thống chủ
d) hệ thống khách

135. Nếu tiến trình người dùng cố yêu cầu CPU thực hiện ... vượt quá quyền hạn thì CPU xử lý những yêu cầu này như là lỗi hoặc cố gắng khóa tiến trình lại

a) các đoạn mã
b) các truy cập tài nguyên
c) các lệnh
d) các tham chiếu file

136. Việc thay đổi không gian thực thi của chương trình chỉ được thực hiện thông qua lời gọi hàm ... tới các mục hợp lệ được phép cho trước

a) call
b) remote
c) API
d) system

137. Hệ điều hành cần phải phân biệt được các hoạt động của bản thân và các hoạt động của chương trình người dùng là do:

a) để đảm bảo hệ điều hành và ứng dụng ổn định và an toàn
b) để đảm bảo chương trình người dùng hoạt động ổn định và hiệu quả
c) để đảm bảo hệ thống hoạt động ổn định và an toàn
d) để đảm bảo hệ điều hành hoạt động ổn định và hiệu quả

138. Các thành phần có liên quan đến các cơ chế bảo vệ hệ thống gồm:

a) chủ thể, thao tác và đối tượng
b) chủ thể, tiến trình và đối tượng
c) người dùng, thao tác và các file
d) tiến trình, thao tác và file

139. Hệ điều hành là một chương trình quản lý các tài nguyên phần cứng và phần mềm của một ...

a) thiết bị tính toán
b) máy chủ
c) máy tính cá nhân
d) điện thoại thông minh

140. Kho chính sách là cơ sở dữ liệu gồm: các trạng thái bảo vệ, ... và các trạng thái dịch chuyển

a) các ID của trạng thái
b) trạng thái tự do
c) các tên trạng thái
d) các nhãn trạng thái

141. ... cho phép phần mềm xác định địa chỉ bộ đệm ảo

a) Vào/ra ánh xạ đầy đủ
b) Vào/ra ánh xạ trước
c) Vào/ra không ánh xạ
d) Vào/ra dựa trên lập trình

142. Việc ảo hóa bộ nhớ ... với tiến trình người dùng

a) đơn giản
b) trong suốt
c) dễ sử dụng
d) tin cậy

143. Các lớp bảo vệ được triển khai bằng cách kết hợp giữa ... trên thực tế

a) phần cứng và phần mềm
b) phần cứng và hệ điều hành
c) phần cứng và phần sụn
d) phần cứng và nhân

144. Để phần cứng hỗ trợ kiểm soát thao tác vào/ra cần có thêm một số kênh thông tin khác như:

a) Thiết bị vào/ra tới bộ nhớ và bộ xử lý
b) Thiết bị vào/ra tới phần mềm và nhân
c) Thiết bị vào/ra tới bộ nhớ và phần mềm
d) Thiết bị vào/ra tới phần mềm và phần cứng

145. Bình đẳng (máy tính cho phép ảo hóa):

a) Các hệ thống ảo chạy trên nền hệ điều hành không thể truy cập đến lớp 0 một cách trực tiếp mà phải thông qua bước chuyển không gian thực hiện (thay đổi đặc quyền)
b) Bất kỳ tiến trình nào đang chạy với sự hiện diện của tiến trình kiểm soát với môi trường thực thi không khác gì trường hợp không có tiến trình giám sát
c) Tất cả các câu lệnh bình thường được thực hiện trực tiếp bởi phần cứng mà không có sự can thiệp nào của các tiến trình giám sát
d) Không cho phép bất kỳ tiến trình nào ảnh hưởng tới các tài nguyên hệ thống như bộ nhớ và tính sẵn dùng của nó

146. Các không gian này thường được biểu diễn:

a) Chế độ người quản trị, Chế độ người dùng
b) Chế độ hệ thống, Chế độ người dùng
c) Chế độ đặc quyền
d) Chế độ người dùng

147. Với cơ chế chuyển đổi địa chỉ dựa trên các thẻ mô tả (descriptor), mỗi tiến trình có:

a) Chế độ truy cập và cơ chế ánh xạ
b) Tập các thẻ mô tả và thẻ ánh xạ
c) Tập các thẻ mô tả và chế độ truy cập
d) Con trỏ cơ sở và cơ chế ánh xạ

148. Trong các HĐH trước đây: con trỏ cơ sở cho biết:

a) vị trí bắt đầu
b) vị trí bắt đầu, và con trỏ giới hạn, xác định vị trí kết thúc
c) vị trí bắt đầu, vị trí kết thúc
d) vị trí bắt đầu của các trang trên bộ nhớ vật lý tùy thuộc theo trạng thái hoạt động của hệ điều hành

149. Các thao tác vào/ra là các thao tác đặc quyền được thực hiện chỉ bởi ...

a) phần mềm
b) người dùng
c) hệ điều hành và người dùng
d) hệ điều hành

150. Chỉ có hệ điều hành mới truy cập trực tiếp bộ nhớ nhờ các lệnh ...

a) đặc quyền
b) thông thường
c) gọi hàm
d) đặc biệt

151. Ảo hóa không bao gồm thành phần nào?

a) Phần mềm
b) Phần cứng máy tính
c) Hệ điều hành
d) Các thiết bị lưu trữ, các thiết bị mạng
e) Các ứng dụng

152. Lớp 2 trong không gian thực thi là:

a) các trình điều khiển vào/ra và tiện ích
b) chương trình ứng dụng
c) nhân hệ điều hành
d) phần còn lại của hệ điều hành

153. ... thường không cho phép tiến trình người dùng làm việc trực tiếp với các địa chỉ vật lý mà chỉ được kích hoạt từ hệ điều hành

a) Vào/ra ánh xạ đầy đủ
b) Vào/ra dựa trên lập trình
c) Vào/ra không ánh xạ
d) Vào/ra ánh xạ trước

154. Hệ thống phân cấp các không gian thực thi thành các ...

a) lớp người dùng
b) lớp chính sách
c) lớp đặc quyền
d) lớp bảo vệ

155. Các tiến trình người dùng truy cập bộ nhớ thông qua bảng chỉ số và con trỏ mô tả phần không gian nhớ .. của tiến trình

a) ảo
b) logic
c) tuyến tính
d) thực

156. Ảo hóa bao gồm:

a) ảo hóa đĩa
b) ảo hóa toàn bộ các tài nguyên
c) ảo hóa một số hay toàn bộ các tài nguyên
d) ảo hóa một số các tài nguyên

157. Phần cứng (CPU - bộ VXL) giúp làm đơn giản hóa việc chuyển đổi ngữ cảnh thông qua cơ chế ... lại các chương trình bị dừng bằng cách lưu lại trạng thái của các tiến trình và khôi phục đồng thời các thanh phi mà chương trình sử dụng

a) phân tích lại
b) khôi phục
c) xác minh
d) khởi động

158. ... là cơ chế đồng bộ theo nghĩa bộ xử lý kiểm soát trực tiếp từng đơn vị dữ liệu được trao đổi với thiết bị vào/ra

a) Vào/ra dựa trên lập trình
b) Vào/ra ánh xạ đầy đủ
c) Vào/ra không ánh xạ
d) Vào/ra ánh xạ trước

159. Tính hiệu quả (máy tính cho phép ảo hóa):

a) Các hệ thống ảo chạy trên nền hệ điều hành không thể truy cập đến lớp 0 một cách trực tiếp mà phải thông qua bước chuyển không gian thực hiện (thay đổi đặc quyền)

b) Bất kỳ tiến trình nào đang chạy với sự hiện diện của tiến trình kiểm soát với môi trường thực thi không khác gì trường hợp không có tiến trình giám sát

c) Tất cả các câu lệnh bình thường được thực hiện trực tiếp bởi phần cứng mà không có sự can thiệp nào của các tiến trình giám sát

d) Không cho phép bất kỳ tiến trình nào ảnh hưởng tới các tài nguyên hệ thống như bộ nhớ và tính sẵn dùng của nó

160. ... là các công nghệ ảo hóa giúp đơn giản hóa hệ thống chủ và đảm bảo hiệu năng gần như thật với hệ thống được ảo hóa

a) Intel với VT-i và AMD với AMD-V

b) Intel với AMD-i và AMD với VT-V

c) Intel với AMD-V và AMD với VT-i

d) Intel với VT-V và AMD với AMD-i

161. Trong chế độ hệ thống, tiến trình được phép truy cập toàn bộ không gian nhớ ... của máy tính

a) logic

b) vật lý và logic

c) ảo

d) vật lý

162. Các thành phần của hệ điều hành hoạt động tại lớp (lớp 0 / lớp 1):

a) thực hiện chỉnh sửa các thông tin người dùng

b) thực hiện chỉnh sửa các câu lệnh

c) thực hiện chỉnh sửa các tham số cấu hình hệ thống

d) thực hiện chỉnh sửa các tham số đầu vào

163. Khi hệ thống phân cấp các tiến trình theo các lớp bảo vệ (chế độ hệ thống/đặc quyền và chế độ người dùng) thì các tiến trình người dùng không được phép đọc ghi tùy tiện vào

a) không gian nhớ của tiến trình khác

b) dữ liệu của hệ thống

c) các file của hệ thống

d) không gian nhớ của hệ thống

164. Ảo hóa phần cứng làm giảm sự can thiệp của hệ thống chủ trong việc xử lý các vấn đề quản lý việc ... không gian địa chỉ và đặc quyền

a) chuyển đổi

b) ánh xạ

c) phân tích

d) chuyển

165. Kiểm soát tài nguyên (máy tính cho phép ảo hóa):

a) Các hệ thống ảo chạy trên nền hệ điều hành không thể truy cập đến lớp 0 một cách trực tiếp mà phải thông qua bước chuyển không gian thực hiện (thay đổi đặc quyền)

b) Không cho phép bất kỳ tiến trình nào ảnh hưởng tới các tài nguyên hệ thống như bộ nhớ và tính sẵn dùng của nó

c) Bất kỳ tiến trình nào đang chạy với sự hiện diện của tiến trình kiểm soát với môi trường thực thi không khác gì trường hợp không có tiến trình giám sát

d) Tất cả các câu lệnh bình thường được thực hiện trực tiếp bởi phần cứng mà không có sự can thiệp nào của các tiến trình giám sát

166. Việc chuyển đổi không gian thực hiện của các tiến trình được thực hiện nhờ câu lệnh ...

a) call

b) đặc biệt

c) gọi hàm

d) đặc quyền

167. ... là dạng vào/ra an toàn hơn gồm phần cứng thực hiện việc chuyển địa chỉ từ ảo sang địa chỉ vật lý với mỗi tham chiếu bộ nhớ được thực hiện bởi thiết bị

a) Vào/ra không ánh xạ

b) Vào/ra dựa trên lập trình

c) Vào/ra ánh xạ đầy đủ

d) Vào/ra ánh xạ trước

168. Các đặc trưng của mô hình Bell-La Padula:

a) Quyền truy cập được định nghĩa thông qua ma trận truy cập và thứ tự mức an toàn

b) Các chính sách an toàn ngăn chặn luồng thông tin đi xuống từ mức an toàn cao xuống mức thấp

c) Truy cập tài nguyên của hệ thống mà không có sự đồng ý của chủ sở hữu là không thể

d) Mô hình này chỉ xem xét luồng thông tin xảy ra khi có sự thay đổi hay quan sát một đối tượng

169. Chính sách là thuật ngữ trừu tượng mô tả ... mà hệ thống phải đáp ứng và hoàn thành theo cách an toàn và chấp nhận được

a) yêu cầu

b) hành động

c) điều khoản

d) mục tiêu và các kết quả

170. Trong mô hình Clark-Winson, các thuộc tính an toàn được mô tả qua các ... và cần được kiểm tra để đảm bảo các chính sách an ninh nhất quán với yêu cầu của chương trình

a) cơ sở an toàn
b) chính sách
c) mục tiêu an toàn
d) luật chứng thực

171. Mô hình HRU cho phép đánh giá ... của các thao tác thay đổi quyền này

a) tính an toàn
b) tính bảo mật
c) tính đúng đắn
d) tính chính xác

172. Xây dựng mô hình an toàn máy trạng thái liên quan đến:

a) các trạng thái bảo vệ
b) các chức năng của mô hình
c) các mục tiêu an toàn
d) các thành phần của mô hình và trạng thái an toàn khởi đầu

173. Mô hình phi chính tắc là:

a) Bell-PaLadula
b) Clak-Will
c) Bell-LaPadula
d) Clark-Winson

174. Mô hình luồng thông tin khắc phục hạn chế của mô hình dựa trên máy trạng thái là sự thiếu ... về luồng thông tin

a) dữ liệu
b) mô tả
c) phương tiện lưu trữ
d) bảo mật

175. Mô hình HRU sử dụng cách kiểm soát thông qua ...

a) mật khẩu
b) ma trận truy cập
c) định danh
d) danh sách truy cập

176. Mô hình HRU xử lý ... của các chủ thể và ... của các quyền này

a) thuộc tính và độ bảo mật
b) quyền truy cập và tính toàn vẹn
c) tiến trình và tính đúng đắn
d) thông tin và dữ liệu

177. Mô hình an toàn là biểu diễn dạng .. của các chính sách và ánh xạ mong muốn của người đề ra chính sách thành tập các .. phải được tuân thủ trong hệ thống

a) nhị phân / tiêu chuẩn
b) số học / điều khoản
c) ký hiệu / luật
d) văn bản / quy định

178. Luồng thông tin được sử dụng để mô tả các .. của hệ thống bằng cách phân tích các .. trong đồ thị luồng thông tin

a) chính sách an toàn / đỉnh
b) mục tiêu an toàn / cung
c) chính sách bảo vệ / liên kết
d) mục tiêu an toàn / liên kết

179. Chủ thể ở mức toàn vẹn .. có khả năng ghi vào đối tượng (dữ liệu) có mức toàn vẹn ... và có thể đọc dữ liệu ở mức toàn vẹn ...

a) thấp / cao hơn / thấp hơn
b) thấp / cao hơn / nào cũng được
c) cao / thấp hơn / cao hơn
d) cao / thấp hơn / cao hơn hoặc bằng

180. Mô hình luồng thông tin biểu diễn cách thức dữ liệu di chuyển giữa ... và ... trong hệ thống

a) tiến trình / vi xử lý
b) bộ nhớ / tiến trình
c) đối tượng / chủ thể
d) bộ nhớ / CPU

181. Trong mô hình Biba, chủ thể có yêu cầu an ninh .. không được sử dụng thông tin từ nguồn có độ tin cậy ..

a) thấp / cao hơn hoặc bằng
b) cao / thấp hơn hoặc bằng
c) thấp / cao
d) cao / thấp

182. CDI là viết tắt của:

a) Constrained Data Items
b) Contraned Data Items
c) Contrained Data Items
d) Constraned Data Items

183. Mô hình Bell-La Padula không đề cập đến việc thay đổi .. của các người dùng (chủ thể) của hệ thống

a) các tiến trình
b) các chương trình
c) mức truy cập
d) quyền truy cập

184. Mô hình Bell-La Padula là mô hình luồng thông tin phổ biến nhất hướng tới việc bảo vệ ...

a) tính toàn vẹn
b) tính đúng đắn
c) tính sẵn dùng
d) tính bí mật

185. Mô hình máy trạng thái gồm:

a) các trạng thái, thao tác/luồng dịch chuyển trạng thái
b) các thao tác, kỹ thuật dịch chuyển trạng thái
c) các trạng thái, thao tác/hàm dịch chuyển trạng thái
d) các thao tác và tiến trình dịch chuyển trạng thái

186. IVP là viết tắt của:

a) Intergrity Verfication Procedure
b) Intergrity Verfication Procedures
c) Integrity Verfication Procedure
d) Integrity Verfication Procedures

187. Mô hình Biba đảm bảo .. của dữ liệu

a) tính bí mật
b) tính đúng đắn
c) tính toàn vẹn
d) tính sẵn dùng

188. Một số mô hình an toàn thực thi các quy định và luật nhằm bảo vệ:

a) tính đúng đắn
b) tính xác thực
c) tính không chối bỏ
d) tính bí mật và toàn vẹn dữ liệu

189. Mô hình an toàn là khái niệm quan trọng trong .. và .. của hệ thống

a) thiết kế / phân tích an toàn
b) thiết lập / phân tích an ninh
c) độ an toàn / tính khả dụng
d) cài đặt / đánh giá

190. Mô hình an toàn tích hợp .. hay các mục tiêu cần phải được thực thi và đảm bảo trong hệ thống

a) cơ chế bảo vệ
b) chính sách bảo vệ
c) chính sách an toàn
d) mục tiêu an toàn

191. Mục tiêu mà mô hình HRU hướng tới là xây dựng mô hình .. có thể áp dụng được cho nhiều hệ thống .. khác nhau

a) tinh vi và máy tính hiện đại
b) an toàn và máy tính
c) an ninh và phần cứng
d) đơn giản và an toàn

192. Đồ thị luồng thông tin gồm:

a) đỉnh, ô vuông
b) đỉnh, cung, đường nét đứt
c) đỉnh, cung, chiều liên kết
d) cung, ô vương, đường kẻ

193. Mô hình Biba áp dụng hai quy tắc:

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

194. Nguyên tắc an toàn trong Bell-La Padula:

a) chỉ đọc xuống và chỉ ghi xuống
b) không đọc lên và không ghi xuống
c) không đọc lên và không ghi lên
d) chỉ đọc lên và chỉ ghi xuống

195. Trong mô hình Clark-Winson, tính toàn vẹn được dựa trên nguyên tắc các công việc (thủ tục) được định nghĩa tường minh và việc ... trách nhiệm

a) chịu
b) quản lý
c) phân chia
d) tách biệt

196. Nguyên tắc an toàn trong Bell-La Padula, các nhãn an toàn theo cấp độ bảo mật từ cao xuống thấp gồm

a) Secret > Top Secret > Confidential > Public
b) Top Secret > Confidential > Secret > Public
c) Top Secret > Secret > Confidential > Public
d) Confidential > Top Secret > Secret > Public

197. Các đặc trưng của mô hình an toàn bao gồm:

a) Thể hiện rõ ràng các chính sách an toàn
b) Chính xác và rõ ràng
c) Thể hiện các chính sách bảo mật
d) Căn bản / Cơ bản
e) Đơn giản, khái quát và dễ hiểu

198. Mô hình Bell-La Padula chứa:

a) kênh ngầm
b) kênh riêng

199. HRU là:

a) Hanison-Ruzo-Ullman
b) Harrison-Ruzzo-Ullman
c) Hirason-Rusio-Ullmun
d) Harison-Rusika-Ullmun

200. Mô hình Clark-Winson tập trung cho vấn đề .. dữ liệu

a) toàn vẹn
b) chính xác
c) bí mật
d) đúng đắn

201. Các đặc trưng của mô hình an toàn:

a) thể hiện chính sách an toàn
b) đảm bảo tính đúng đắn
c) chính xác và rõ ràng
d) khái quát, đơn giản, dễ hiểu
e) cơ bản

202. Các qui định chứng thực và thực thi cho thấy mô hình Clark-Winson yêu cầu:

a) Toàn vẹn, xác thực và sẵn dùng
b) Xác thực, định danh và bảo mật
c) Toàn vẹn, định danh và bí mật
d) Xác thực, kiểm toán và quản trị

203. Công cụ nào sử dụng ngôn ngữ mô tả dành cho các tiến trình song song?

a) Spin
b) SRK
c) FDR
d) Uppaal

204. Các đặc tả chính tắc bao gồm:

a) đặc tả hoạt động, đặc tả giao tiếp
b) đặc tả cơ bản, đặc tả chi tiết
c) đặc tả phần cứng, đặc tả phần mềm
d) đặc tả giao tiếp, đặc tả hành vi

205. Đặc tả yêu cầu phần mềm đưa ra các yêu cầu ...

a) chức năng
b) chức năng và phi chức năng
c) bắt buộc
d) phi chức năng

206. Các đặc tả chính tắc có thể dùng để chứng minh các thuộc tính về .. của hệ thống, đặc biệt là việc hệ thống .. phù hợp với các đặc tả của mô hình an toàn

a) xây dựng / phát triển
b) an toàn / an ninh
c) thiết kế / xây dựng
d) bí mật / an toàn

207. Kỹ thuật kiểm chứng mô hình dựa trên việc mô tả các hành vi có thể của hệ thống theo cách thức ... về mặt toán học

a) chính xác và rõ ràng
b) đúng đắn và hợp lý
c) đúng đắn và rõ ràng
d) chính xác và hợp lý

208. Đặc tả về an toàn của phần mềm là các mô tả về các yêu cầu .. của phần mềm

a) an ninh, bí mật
b) bí mật, toàn vẹn
c) an ninh, an toàn
d) sẵn dùng, toàn vẹn

209. Kiểm chứng hay chứng minh tính đúng của các đặc tả thường được thực hiện sử dụng các .. tự động do việc thực hiện thủ công hay gặp lỗi

a) phương pháp
b) công cụ
c) hàm
d) thuật toán

210. Đặc tả yêu cầu phần mềm là:

a) miêu tả của phần mềm được phát triển
b) minh họa của phần mềm được phát triển
c) một mô tả của phần mềm được phát triển
d) khắc họa của phần mềm được phát triển

211. Alloy

a) được dùng để phân tích tính nhất quán của các cấu trúc dữ liệu dựa trên lý thuyết tập hợp do trường MIT phát triển

b) được dùng để lập mô hình hệ thống theo thời gian thực

c) được dùng để lập mô hình hệ thống dị bộ

d) được dùng để lập mô hình phần mềm song song hay tiến trình dị bộ

212. Đặc tả hành vi

a) mô tả các trạng thái có thể của hệ thống và các thao tác làm thay đổi trạng thái

b) giúp cho việc phân rã các hệ thống lớn thành các hệ thống con

c) giúp cho việc phân tích các hệ thống lớn thành các hệ thống con

d) mô tả các hành vi có thể của hệ thống và các thao tác làm thay đổi hành vi

213. Đặc tả giao tiếp:

a) mô tả các hành vi có thể của hệ thống và các thao tác làm thay đổi hành vi

b) giúp cho việc phân rã các hệ thống lớn thành các hệ thống con

c) giúp cho việc phân tích các hệ thống lớn thành các hệ thống con

d) mô tả các trạng thái có thể của hệ thống và các thao tác làm thay đổi trạng thái

214. SMV, NuSMV:

a) được dùng để lập mô hình hệ thống theo thời gian thực

b) được dùng để lập mô hình hệ thống dị bộ

c) được dùng để lập mô hình phần mềm song song hay tiến trình dị bộ

d) được dùng để lập mô hình phần cứng (logic số) tuy nhiên cũng có thể dùng được cho lĩnh vực khác

215. Công cụ nào sử dụng ngôn ngữ riêng cho việc mô tả các mô hình cũng như các thuộc tính?

a) Spin

b) SRK

c) Uppaal

d) FDR

216. Việc đầu tiên công cụ phân tích tĩnh cần làm là chuyển mã chương trình thành ...

a) mô hình chương trình

b) mô hình đa cấp

c) mô hình phân cấp

d) mô hình tổng quát

217. Đâu là một kỹ thuật phân tích tĩnh?

a) Phân tích đoạn
b) Phân tích mã
c) Phân tích khoảng
d) Phân tích câu

218. Simulink Design Verifier:

a) được dùng để lập mô hình hệ thống dị bộ
b) được dùng để lập mô hình hệ thống theo thời gian thực
c) được dùng để kiểm chứng mô hình được sinh ra từ Simulink, một công cụ mô phỏng dựa trên luồng dữ liệu và máy trạng thái
d) được dùng để phân tích tính nhất quán của các cấu trúc dữ liệu dựa trên lý thuyết tập hợp do trường MIT phát triển

219. Các mô hình hệ thống được kiểm nghiệm tất cả các trạng thái có thể mà thỏa mãn các mô tả ở trên bằng ..

a) biểu thức
b) mô hình an toàn
c) thuật toán
d) mô hình không an toàn

220. Các đặc tả cung cấp thông tin ở ... mức

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

221. FDR:

a) được dùng để lập mô hình hệ thống theo thời gian thực
b) được dùng để lập mô hình hệ thống dị bộ
c) được dùng để lập mô hình phần cứng (logic số) tuy nhiên cũng có thể dùng được cho lĩnh vực khác
d) được dùng để lập mô hình phần mềm song song hay tiến trình dị bộ

222. Các giao tiếp thường được mô tả bằng tập các ... hay thành phần cho biết dữ liệu và các ... được truy cập thông qua giao tiếp

a) đối tượng / thao tác
b) chủ thể / thao tác
c) chủ thể / đối tượng
d) thao tác / chủ thể

223. Phân tích động phần mềm được thực hiện bằng cách chạy các đoạn mã hoặc cả phần mềm trên ...

a) hệ điều hành
b) phần mềm ảo hóa
c) máy ảo
d) bộ xử lý vật lý hay ảo

224. Uppaal:

a) được dùng để lập mô hình hệ thống theo thời gian thực
b) được dùng để lập mô hình hệ thống dị bộ
c) được dùng để lập mô hình phần mềm song song hay tiến trình dị bộ
d) được dùng để lập mô hình phần cứng (logic số) tuy nhiên cũng có thể dùng được cho lĩnh vực khác

225. Ở mức độ tổng quát, các đặc tả an toàn cần ... và gần với mô hình an toàn lựa chọn

a) linh hoạt
b) phức tạp
c) đơn giản
d) khái quát

226. Các phương pháp tiếp cận cho chứng minh đặc tả:

a) Chứng minh định lý và Kiểm chứng trạng thái
b) Chứng minh định lý và Kiểm chứng mô hình
c) Chứng minh biểu thức và Kiểm chứng trạng thái
d) Chứng minh biểu thức và Kiểm chứng mô hình

227. Các đặc tả cung cấp thông tin ở hai mức:

a) Khái quát và chi tiết
b) Phức tạp và rõ ràng
c) Trừu tượng và chi tiết
d) Trừu tượng và rõ ràng

228. Các đặc tả chính tắc trông giống như chương trình máy tính thông thường với các ...

a) biểu thức chính quy và phép toán
b) biểu thức logic và phép toán
c) biểu thức toán học và phép toán
d) biểu thức bất khả quy và phép toán

229. Bản thân hệ điều hành là tập hợp các ... mà mỗi phần mềm cung cấp một số chức năng của HĐH

a) dữ liệu
b) phần mềm
c) phần cứng và phần mềm
d) phần cứng

230. Spin

a) được dùng để lập mô hình hệ thống dị bộ

b) được dùng để lập mô hình phần mềm song song hay tiến trình dị bộ

c) được dùng để lập mô hình phần cứng (logic số) tuy nhiên cũng có thể dùng được cho lĩnh vực khác

d) được dùng để lập mô hình hệ thống theo thời gian thực

231. Đâu không phải là một công cụ kiểm chứng mô hình?

a) FDR

b) SMV, NuSMV

c) Alloy

d) SRK

e) Spin

232. Các hệ thống chứng minh và tích hợp đặc tả cho phép tạo ra một cách tự động các định lý dựa trên ...

a) các tiên đề, hàm, bất biến, các hạn chế và các thành phần khác của đặc tả

b) các tiên đề, hàm, bất biến, và các thành phần khác của đặc tả

c) các hạn chế và các thành phần khác của đặc tả

d) các tiên đề, biểu thức, hàm, bất biến, các hạn chế và các thành phần khác của đặc tả