QUIZIZZ

NAME : _____

CLASS : _____

CSATTT-C5
41 Questions

DATE : _____

1. 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 các tấn công, xâm nhập mới chỉ gây thiệt hại nhỏ

B Do các tấn công xâm nhập mới không gây ra bất thường

C Do chữ ký của chúng chưa tồn tại trong hệ thống

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

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

A Các phần mềm quét virus xung đột với nhau

B Các phần mềm quét virus chiếm nhiều tài nguyên

C Các phần mềm quét virus tấn công lẫn nhau

D Các phần mềm quét virus không thể hoạt động

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

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

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

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

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

4. Đâu là tên viết đúng của hệ thống xâm nhập/ đột nhập?

A Intrusion Detector System

B Intrusion Detection System

C Intrusion Detecting System

D Intruction Detection System

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

A Kiểu soát dịch vụ và các phần mềm

B Kiểm soát dịch vụ và hướng

C Kiểu soát người dùng và tin tặc

D Kiểu soát virus và malware khác

E Kiểu soát người dùng và hành vi

6. Một hệ thống điều kiển truy nhập có thể được cấu thành từ các dịch vụ nào sau đây?

A Xác thực, đăng nhập, trao quyền

B Xác thực, đăng nhập và kiểm toán

C Xác thực, trao quyền và kiểm toán

D Xác thực, trao quyền và quản trị

7. Một trong các dạng mã hóa (encrypted Keys) được sử dụng rộng rãi trong điều kiển truy nhập là:

A E-token

B Thẻ ATM

C Chứng chỉ số hóa công khai

D Mobile-token.

8. 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 phát hiện xâm nhập hiệu quả hơn

D IPS có khả năng chủ động ngăn chặn xâm nhập

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

A Sử dụng mật khẩu

B Sử dụng Smartcard

C Sử dụng vân tay

D Sử dụng chứng chỉ số

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

A VPN

B Firewall

C Kerberos

D SSL/TLS

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

A Nhận dạng được các tấn công và các phần mềm độc hại

B Chạy nhanh hơn

C Lọc nội dung gói tốt hơn

D Phân biệt được các gói tin thuộc về các kết nối mạng khác nhau

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

A Chỉ các thông tin trong header của gói tin

B Chỉ lọc địa chỉ IP trong gói tin

C Cả thông tin trong header và payload của gói tin

D Chỉ các thông tin trong payload của gói tin

13. Tường lửa không thể chống lại..

A Các hiểm họa từ bên ngoài

B Tấn công từ mạng Internet

C Tấn công giả mạo địa chỉ

D Tấn công hướng dữ liệu

14. 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 Acunetix Web Vulnerability Scanner

D Nessus Vulnerability Scanner

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

A Đọc xuống và ghi lên

B Đọc lên và ghi xuống

C Đọc lên và ghi lên

D Đọc xuống và ghi xuống

16. 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 Không yêu cầu xây dự csdl các chữ ký

D Các tấn công xâm nhập mới thường dễ nhận biết

17. Ưu điểm của thẻ bài (token) so với thẻ thông minh (smartcard) trong điều khiển truy nhập là:

A Có được cơ chế xác thực đa dạng hơn
B Được sử dụng rộng rãi hơn
C Chi phí rẻ hơn
D Có cơ chế xác thực mạnh hơn

18. Nêu các loại tường lửa

A Circuit Router
B Packet Router Gateway
C Packet-Filtering Router
D Application-Level Gateway
E Circuit-Level gateway

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

A là quá trình xác minh tính chân thực của thông tin nhận dạng người dùng cung cấp
B là quá trình xác minh các thông tin nhận dạng của chủ thể yêu cầu truy nhập đối tượng
C là quá trình xác minh, nhận dạng người dùng
D là quá trình xác minh nhận dạng của chủ thể

20. 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 bí mật, tính toàn vẹn, tính xác thực
B Tính bảo mật, tính toàn vẹn và tính các thực
C Tính bí mật, tính toàn vẹn và tính sẵn dùng
D Tính bảo mật, tính toàn vẹn và tính sẵn dùng.

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

A Bảo mật cao và chi phí thấp
B Bảo mật cao và độ ổn định cao
C Bảo mật cao và luôn đi cùng với chủ thể
D Bảo mật cao và được hỗ trợ rộng rãi

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

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

B. MAC quản lý quyền truy nhập chặt chẽ hơn các cơ chế khác

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

D. MAC là cơ chế điều khiển truy nhập được sử dụng rộng rãi nhất

23. 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. Giám sát các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập

C. Truy tìm và tấn công ngược lại hệ thống của tin tặc

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.

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

A. 3

B. 2

C. 1

D. 4

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

A. Thẻ ATM và tên truy nhập

B. Tên truy nhập và số PIN

C. Tên truy nhập và mật khẩu

D. Thẻ ATM và số PIN

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

A. Chống được tấn công phát lại

B. Chống được tấn công từ điển

C. Chống được tấn công vét cạn

D. Chống được tấn công phá mã

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

A. Authentication và Authorization

B. Authenticator và Administrator

C. Administrator và Authorization

D. Authentication và Administrator

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

A Phát hiện xâm nhập dựa trên bất thường không thể phát hiện các tấn công, xâm nhập mới

B , Phát hiện xâm nhập dựa trên bất thường thường có tỷ lệ phát hiện đúng cao hơn

C , Phát hiện xâm nhập dựa trên chữ ký thường có tỷ lệ phát hiện đúng cao hơn

D Phát hiện xâm nhập dựa trên chữ ký có thể phát hiện các tấn công, xâm nhập mới.

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

A Các router

B Các host

C Mạng

D Mạng và các host

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

A Chi phí đắt

B Không được hỗ trợ rộng rãi

C Khó sử dụng

D Công nghệ phức tạp

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

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

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

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

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

A RBAC là cơ chế điều khiển truy nhập được sử dụng rộng rãi nhất

B RBAC cấp quyền truy nhập dựa trên vai trò của người dùng trong tổ chức

C RBAC cấp quyền truy nhập dựa trên tính nhạy cảm của thông tin và chính sách quản trị

D , RBAC cho phép người tạo ra đối tượng có thể cấp quyền truy nhập cho người dùng khác

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

A Tần suất sử dụng mật khẩu

B Độ khó đoán và tuổi thọ của mật khẩu

C Kích thước của mật khẩu

D Số loại ký tự dùng trong mật khẩu

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

A Học máy, khai phá dữ liệu, agents

B Thống kê, đối sánh chuỗi, đồ thị

C Thống kê, học máy, đồ thị

D Thống kê, học máy, khai phá dữ liệu

35. Ba cơ chế điều kiển truy nhập thông dụng gồm

A DAC, MAC, RBAC

B DAC, MAC, BAC

C DAC, BAC, RBAC

D DAC, MAC, RRAC

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

A Phishing

B Trojan horse

C Man in the middle

D Spoofing

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

A Không có khả năng phát hiện tấn công, xâm nhập mới

B Không có khả năng ngăn chặn tấn công, đột nhập

C Tỷ lệ cảnh báo sai cao

D không có khả năng phát hiện các cuộc tấn công DoS

38. Ví điện tử Paypal là một dạng...

A Khóa mã (encrypted key)

B Thẻ bài (token)

C Thẻ thông minh (smartcard)

D Thẻ ATM

39. Điều khiển truy nhập là quá trình mà trong đó người dùng được ... truy nhập đến các thông tin, các hệ thống và tài nguyên

A Nhận dạng và Trao quyền

B Xác thực và Cho phép

C Kiểm chứng và Cấp phép

D Chứng mình danh tính và Trao quyền

40. DAC hay dùng các kỹ thuật :

A Ma trận điều khiển truy nhập - ACM

B Danh sách điều khiển truy nhập - ACL

C Hệ thống bảo vệ bắt buộc

41. Tường lửa (firewall) có thể là thiết bị phần cứng hoặc công cụ phần mềm được dùng để ...

A Bảo vệ hệ thống và mạng ngoại bộ tránh các đe doạ từ bên trong.

B Bảo vệ hệ thống và mạng cục bộ tránh các đe doạ từ bên ngoài.

C Bảo vệ hệ thống và mạng tránh các đe doạ từ bên ngoài và cả bên trong.

D Bảo vệ hệ thống và mạng nội bộ tránh các đe doạ.

Answer Key

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