NAME : _____

CLASS : _____

CSATTT-C3
40 Questions

DATE : _____

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

A Interruptions

B Interceptions

C Fabrications

D Modifications

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

A Sử dụng mã hóa để đảm bảo tính bí mật các thông điệp truyền

B Sử dụng tường lửa để ngăn chặn

C Sử dụng các hệ thống IPS/IDS

D Sử dụng chứng chỉ số để xác thực thông tin nhận dạng các bên

3. Đâu là một kỹ thuật tấn công DoS

A Ping of death

B DNS spoofing

C IP spoofing

D SYN requests

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

A các yêu cầu ICMP hoặc các yêu cầu phát quảng bá

B các yêu cầu HTTP hoặc các yêu cầu phát quảng bá

C các yêu cầu TCP hoặc các yêu cầu phát quảng bá

D các yêu cầu UPD hoặc các yêu cầu phát quảng bá

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

A Để vượt qua các hệ thống IPS và IDS

B Để đánh cắp các dữ liệu nhạy cảm trên máy trạm

C Để đánh cắp các dữ liệu nhạy cảm trên máy chủ

D Để vượt qua các hàng rào kiểm soát an ninh

6. 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 máy nạn nhân làm địa chỉ đích của gói tin

B Địa chỉ router làm địa chỉ nguồn của gói tin

C Địa chỉ máy nạn nhân làm địa chỉ nguồn của gói tin

D Địa chỉ router làm địa chỉ đích của gói tin

7. Pharming là kiểu tấn công vào...

A Máy chủ và máy khách web

B Máy chủ web

C Máy chủ cơ sở dữ liệu của trang web

D Máy khách/trình duyệt web

8. 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 Reflectors

B Requesters

C Injectors

D Forwarders

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

A Các file tài liệu của bộ phần mềm Open Office

B Các file tài liệu của bộ phần mềm Microsoft Office

C Các file tài liệu của bộ phần mềm Microsoft SQL

D Các file tài liệu của bộ phần mềm Microsoft Exchange

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

A Mức độ gây hại

B Tần suất tấn công

C Phạm vi tấn công

D Kỹ thuật tấn công

11. 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 UNION INSERT
B UNION SELECT
C INSERT SELECT
D SELECT UNION

12. Tấn công bằng mã độc có thể gồm:

A Tràn bộ đệm
B SQLi, XSS, CSRF và Buffer overflow
C Chèn mã XSS, CSRF
D Chèn mã SQL

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

A Vượt qua các khâu xác thực người dùng
B Chiếm quyền điều khiển hệ thống
C Chèn, xóa hoặc sửa đổi dữ liệu
D Đánh cắp các thông tin trong cơ sở dữ liệu

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

A Bắt tay 2 bước
B Xác thực người dùng
C Truyền dữ liệu
D Bắt tay 3 bước

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

A Vét cạn các mật khẩu có thể có
B Tìm mật khẩu trong từ điển các mật khẩu
C Lắng nghe trên đường truyền để đánh cắp mật khẩu
D Thử các từ có tần suất sử dụng cao làm mật khẩu trong từ điển

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

A Lây lan thông qua khả năng thực thi từ xa
B Lây lan thông qua Microsoft Office
C Lây lan thông qua dịch vụ POP
D Lây lan thông qua sao chép các file

17. Đâu là một biện pháp phòng chống tấn công SYN Floods?

A SYN Cache
B SYN Proxy
C SYN IDS
D SYN Firewall

18. Các zombie thường được tin tặc sử dụng để...

A Thực hiện tấn công tràn bộ đệm
B Thực hiện tấn công DDoS
C Thực hiện tấn công DoS
D Đánh cắp dữ liệu từ máy chủ cơ sở dữ liệu

19. Khác biệt cơ bản của vi rút và sâu là

A Vi rút có khả năng tự lây lan mà không cần tương tác của người dùng
B Vi rút có khả năng phá hoại lớn lơn
C Sâu có khả năng tự lây lan mà không cần tương tác của người dùng
D Sâu có khả năng phá hoại lớn lơn

20. 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

21. Tấn công nghe lén là kiểu tấn công:

A Thụ động
B Chủ động
C Chiếm quyền điều khiển
D Chủ động và bị động

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

A SQLmap
B SQLICheck
C SQLServer
D SQLite

23. 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 tài nguyên hệ thống
B Đánh cắp dữ liệu trong hệ thống
C Cản trở người dùng hợp pháp truy nhập các file dữ liệu của hệ thống
D Gây hư hỏng phần cứng máy chủ

24. Đâu là một kỹ thuật tấn công DoS?

A Smurf
B DNS spoofing
C DNS Cache Poisoning
D UDP Ping

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

A triệt tiêu được hết các mối đe dọa

B giảm thiểu các lỗ hổng bảo mật

C kiểm soát chặt chẽ người dùng

D triệt tiêu được hết các nguy cơ

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

A Người dùng

B Máy chủ

C Máy trạm

D Hệ điều hành & ứng dụng

27. 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 Viruses

B Trojans

C Worms

D Zombies

28. Kỹ thuật tấn công Smurf sử dụng giao thức ICMP và cơ chế gửi...

A Multicast

B Anycast

C Broadcast

D Unicast

29. 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 mạng.

C Mối đe dọa là bất kỳ một hành động tấn công nào vào hệ thống máy tính.

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

30. 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 trên máy chủ

C Đánh cắp toàn bộ cơ sở dữ liệu trên máy chủ

D Phá hỏng máy chủ

31. 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

32. 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 có khả năng cấm chèn mã

B Thủ tục cơ sở dữ liệu lưu trong cơ sở dữ liệu và chạy nhanh hơn câu lệnh trực tiếp

C Thủ tục cơ sở dữ liệu cho phép tách mã lệnh SQL khỏi dữ liệu người dùng

D Thủ tục cơ sở dữ liệu độc lập với các ứng dụng

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

A Virus, zombie, spyware

B Virus, worm, zombie

C Virus, worm, trojan

D Virus, trojan, zombie

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

A Modifications

B Interceptions

C Interruptions

D Fabrications

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

A Ẩn mã của virus

B Thay thế các chương trình

C Xáo trộn mã của virus

D Sửa đổi các chương trình

36. 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

37. 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 Role-Based

B MAC

C Rule-Based

D DAC

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

A Khả năng chống tấn công phát lại và chứa các ký tự từ nhiều dạng ký tự

B Chứa các ký tự từ nhiều dạng ký tự

C Độ dài lớn hơn hoặc bằng 8 ký tự

D Độ dài từ 8 ký tự trở lên, gồm chữ cái hoa, thường, chữ số và ký tự đặc biệt

39. Một trong các biện pháp hiệu quả để phòng chống macro viruses là:

A Cấm tự động thực hiện macro trong Microsoft Exchange

B Cấm tự động thực hiện macro trong Microsoft Office

C Sử dụng IPS/IDS

D Sử dụng tường lửa

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

A Fabrications

B Interceptions

C Interruptions

D Modifications

**Answer Key**

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