COPYRIGHT ĐỖ ĐỨC MINH AT16H

Câu 1. Nguyên nhân nào sau đây có thể dẫn tới phá vỡ tính bí mật của thông tin trong hệ thống thông tin

A. Tấn công leo thang đặc quyền

B. Tấn công DoS, DDoS

C. Lỗi đường truyền

D. Mất điện

Câu 2. Phát biểu nào sau đây KHÔNG đúng về tính khả dụng trong an toàn thông tin?

A. Đảm bảo hệ thống luôn đáp ứng nhu cầu cho người dùng

B. Đảm bảo khả năng truy cập thông tin, tính năng của hệ thống thông tin mỗi khi người dùng hợp lệ có nhu cầu

C. Bị ảnh hưởng bởi tấn công DoS hoặc DDoS

D. Có thể bị ảnh hưởng do cấu hình sai

Câu 3. Phát biểu nào sau đây đúng về nguyên tắc hợp lý đầy đủ trong An toàn thông tin

A. Mục tiêu của nguyên tắc là đưa rủi ro của hệ thống về mức chấp nhận được vớichi phí bảo vệ không lớn hơn giá trị của hệ thống.

B. Áp dụng đầy đủ các biện pháp bảo vệ có thể có cho hệ thống

C. Các biện pháp bảo vệ làm ảnh hưởng đến hệ thống

D. Giảm thiểu hoàn toàn rủi ro cho hệ thống

Câu 4. Nguyên tắc mở trong an toàn thông tin quy định:

A. Hệ thống phải đảm bảo an toàn ngay cả khi kẻ tấn công biết được thông tin vềthuật toán và cơ chế bảo vệ

B. Yêu cầu mọi cơ chế bảo vệ và thuật toán đều phải được mở công khai

C. Không ai có thể tấn công vào các cơ chế bảo vệ và thuật toán của hệ thống ngoại trừ tác giả

D. Mở toàn bộ hệ thống và cơ chế bảo vệ cho người dùng

Câu 5. Hiểm họa an toàn thông tin nào sau đây không phụ thuộc vào sự hoạt động của hệ thống

A. Hiểm họa tự nhiên

B. Tấn công leo thang đặc quyền

C. Tấn công dò quét mật khẩu

D. Hiểm họa mã độc

Câu 6. Hiểm họa an toàn thông tin nào sau đây là hiểm họa thụ động?

A. Tấn công nghe lén đường truyền

B. Tấn công leo thang đặc quyền

C. Tấn công DDoS

D. Tấn công sử dụng mã độc

Câu 7. Tấn công truy cập trái phép thuộc loại hiểm họa an toàn thông tin nào sau đây?

A. Hiểm họa thụ động

B. Hiểm họa chủ động

C. Hiểm họa tự nhiên

D. Hiểm họa bên ngoài

Câu 8. Người quản trị của hệ thống nhận thấy rằng trên hệ thống máy chủ Web của công ty KMA tồn tại một loại mã độc cho phép vượt qua các cơ chế kiểm tra an toàn thông thường của hệ thống nhằm tạo điều kiện đăng nhập trái phép vào một chương trình hoặc hệ thống. Mã độc đó thuộc loại mã độc nào sau đây:

A. Backdoor

B. Virus

C. Worm

D. Trojan Horse

Câu 9. DarkC là một chương trình đọc văn bản nhưng lại chứa một số chức năng độc hại cho phép thu thập thông tin mà người dùng không biết. Vậy DarkC là dạng mã độc gì?

A. Trojan Horse

B. Virus

C. Backdoor

D. Zoombie

Câu 10. Mã độc nào sau đây có khả năng tự nhân bản chính nó?

A. Virus và Worm

B. Virus và Trojan Horse

C. Virus và Zoombie

D. Virus và Logic Bomb

Câu 11. Mã độc nào sau đây KHÔNG cần phát tán trong file khác?

A. Worm

B. Virus

C. Logic Borm

D. Backdoor

Câu 12. Hiểm họa An toàn thông tin nào sau đây có thể được giảm thiểu bằng cách sử dụng máy xén giấy

A. Vật lý
B. Spyware
C. Nhìn lén
D. Rootkit

Câu 13. Phát biểu nào sau đây đúng?

A. Worm có thể mang virus.

B. Worm ghi lại tất cả các ký tự đã gõ vào một tệp văn bản.

C. Worm lây nhiễm trong file

D. Worm lây nhiễm vào đĩa cứng MBR

Câu 14. Bạn nhận được một yêu cầu hỗ trợ kỹ thuật từ phòng kế toán báo cáo rằng khi người dùng trong phòng sử dụng các máy tính của họ để truy cập vào các trang

web, thì xuất hiện hiện tượng các quảng cáo bật lên liên tục xuất hiện. Sau khi tiến hành điều tra, bạn thấy rằng một trong những trang web mà một người trong phòng đã truy cập đã bị nhiễm mã Flash và lây nhiễm ra toàn bộ các máy trong phòng. Vấn đề nào đã xảy ra?

A. Worm mang Adware

B. Worm

C. Adware

D. Tấn công XSS

Câu 15. Bình là nhà phát triển phần mềm cho một công ty công nghệ cao. Anh ta tạo ra một chương trình kết nối với phòng chat và chờ nhận lệnh thu thập thông tin người dùng cá nhân. Bình nhúng chương trình này vào tệp AVI của một bộ phim nổi tiếng hiện tại và chia sẻ tệp này trên mạng chia sẻ tệp P2P. Chương trình của Bình được kích hoạt khi mọi người tải xuống và xem phim, cái gì sẽ được tạo ra?

A. Botnet

B. Tấn công DDoS

C. Logic Bomb

D. Worm

Câu 16. Một người dùng báo cáo sự cố bàn phím USB. Bạn kiểm tra mặt sau của máy tính để đảm bảo bàn phím được kết nối đúng cách và nhận thấy một đầu nối nhỏ giữa bàn phím và cổng USB của máy tính. Sau khi điều tra, bạn biết rằng phần cứng này thu thập mọi thứ mà người dùng nhập vào qua bàn phím. Đây là loại phần cứng nào?

A. Keylogger

B. Trojan

C. Smartcard

D. Bộ chuyển đổi PS/2

Câu 17. Sự khác biệt giữa rootkit và tấn công leo thang đặc quyền?

A. Sự leo thang đặc quyền là kết quả của một rootkit.

B. Rootkit tự nhân bản.

C. Rootkit là kết quả của sự leo thang đặc quyền.

D. Mỗi kiểu sử dụng một cổng TCP khác nhau.

Câu 18. Được phát hiện vào năm 1991, virus Michelangelo được cho là đã được kích hoạt để ghi đè lên 100 sector đĩa cứng đầu tiên với dữ liệu null mỗi năm vào ngày 6 tháng 3, đúng vào ngày sinh nhật của nghệ sĩ người Ý. Michelangelo thuộc loại virus nào?

A. Logic bomb

B. Worm

C. Trojan

D. Zero day

Câu 19. Tấn công Stuxnet được phát hiện vào tháng 6 năm 2010. Chức năng chính của nó là che giấu sự hiện diện của nó trong khi lập trình lại các hệ thống máy tính công nghiệp (gọi là PLC), cụ thể là máy ly tâm hạt nhân trong nhà máy điện hạt nhân Iran. Phần mềm độc hại đã được phát tán thông qua các ổ đĩa flash USB, trong đó nó truyền các bản sao của chính nó đến các máy chủ khác. Điều nào sau đây áp dụng cho Stuxnet?

A. Worm

B. Exploit

C. Trojan Horse

D. Adware

Câu 20. Khi truy cập vào các tài liệu trong một thư mục trên máy tính của bạn, bạn nhận thấy tất cả các tệp đã bị đổi tên thành các tên tệp ngẫu nhiên. Ngoài ra, bạn thấy một tài liệu chứa các hướng dẫn thanh toán để giải mã các tệp tin. Trong trường hợp này bạn đã nhiễm mã độc nào?

A. Ransomware

B. Mã độc

C. Criminalware

D. Encryptionware

Câu 21. Công ty muốn bạn đề xuất một số công cụ cài đặt trên máy tính để phòng chống mã độc, công cụ nào sau đây KHÔNG nên đề xuất.

A. VPN

B. Antivirus

C. Deep Freeze

D. Shadow Defender

Câu 22. Đâu là hành vi KHÔNG an toàn gây ra nguy cơ lây nhiễm mã độc trong hệ thống?

A. Sử dụng thiết bị lưu trữ di động

B. Cập nhật phần mềm, các bản vá, cho hệ điều hành

C. Vô hiệu hóa, gỡ bỏ những dịch vụ không cần thiết (đặc biệt các dịch vụ về mạng)

D. Vô hiệu hoá cơ chế tự động thực thi các tệp tin nhị phân và các tệp tin scripts

Câu 23. Tấn công Man-In-The-Middle có thể xảy ra khi nào?

(A) Khi kẻ tấn công kiểm soát được một thiết bị router trên đường truyền.

(B) Kẻ tấn công nằm ngay cùng vùng mạng của đối tượng mục tiêu.

(C) Kẻ tấn công nằm trên cùng vùng mạng với bất kỳ một thiết bị định tuyến nào được sử dụng bởi nạn nhân mục tiêu

(D) Tất cả các phương án trên

/D

Câu 24. Bạn là người xây dựng ứng dụng Web cho công ty, đâu là giải pháp bạn có thể áp dụng để phòng chống tấn công XSS cho website của bạn

A. Lọc dữ liệu đầu vào

B. Không mở các đường link từ những nguồn không đáng tin cậy

C. Cấu hình lại máy chủ Web

D. Thiết kế cơ sở dữ liệu an toàn

Câu 25. Tấn công nào sau đây có thể gây gián đoạn dịch vụ của hệ thống

A. Tràn bộ đệm

B. XSS

C. CRSF

D. Path Traveling

Câu 26. Thông tin nào sau đây KHÔNG được sử dụng để làm định danh cho người dùng?

A. Tên

B. Số điện thoại

C. Số Chứng minh nhân dân

D. Email

Câu 27. Công ty của bạn muốn xây dựng một hệ thống website bán hàng online, do chi phí không được dồi dào do đó giám đốc yêu cầu bạn đề xuất một phương án xác thực người dùng đơn giản và giá thành rẻ nhất. Nên dùng nhân tố xác thực nào sau đây?

A. Mật khẩu

B. Vân tay

C. Khuôn mặt

D. Địa chỉ IP

Câu 28. Giải pháp nào sau đây giúp hạn chế phương pháp tấn công vét cạn của kẻ tấn công

A. Dùng các nhóm ký tự khác nhau trong mật khẩu như hoa, thường, số và ký tự đặc biệt

B. Loại bỏ các mật khẩu có trong từ điển

C. Bắt buộc đổi mật khẩu khi lần đầu tiên ghi nhận người dùng trong hệ thống

D. Đưa ra sổ ghi lý lịch các MK

Câu 29. Giải pháp xác thực đa nhân tố nào sau đây được sử dụng cho xác thực qua mạng:

A. Mật khẩu + mật khẩu một lần OTP

B. Mật khẩu + Smart card

C. Thẻ từ, smartcard, token + mã PIN

D. Mật khẩu + Vân tay

Câu 30. Mô hình kiểm soát truy cập nào mà chủ của dữ liệu sẽ có toàn quyền trên dữ liệu đó

A. DAC

B. MAC

C. RBAC

D. ABAC

Câu 31. Mô hình kiểm soát truy cập nào yêu cầu duyệt tất cả danh sách khi cần tìm các đối tượng có thể được truy cập bởi một chủ thể

A. ACL

B. CL

C. DAC

D. MAC

Câu 32. Hệ thống có 3 người dùng: Alice: tạo ra file 1; John: tạo ra file 2; Sally: tạo ra file 3. Một file có ba quyền là: Đọc(R), Ghi(W), Thực thi (E). Các người dùng cấp quyền trên các file cho các người dùng khác như sau:

- Alice cấp quyền đọc, ghi cho John trên file 1 và chỉ quyền đọc trên file này cho Sally.
- John cấp quyền đọc, thực thi trên file 2 cho Alice.
- Sally cấp quyền đọc, thực thi trên file 3 cho Alice và quyền đọc, thực thi trên file này cho John

Ai là người có quyền đọc tất cả các file trên?

A. Alice và John

B. Alice và Sally

C. Alice

D. John

Câu 33. Trong mô hình MAC để đảm bảo tính bí mật quy tắc đọc, ghi dữ liệu nào sau đây cần được tuân thủ?

A. Đọc xuống và Ghi lên

B. Đọc lên và Ghi Xuống

C. Chỉ đọc ghi ở cùng mức nhãn an toàn

D. Chỉ đọc ghi ở mức nhãn an toàn thấp hơn

Câu 34. Thiết bị mạng nào truyền dữ liệu giữa các mạng khác nhau bằng cách kiểm tra địa chỉ mạng đích trong một gói?
A. Bộ định tuyến
B. Layer 2 Switch
C. Thiết bị cân bằng tải
D. NIC

Câu 35. Khi thiết lập luật ACL cho bộ định tuyến, cần tuân thủ hướng dẫn chung nào?

A. Quy tắc cuối cùng phải là quy tắc từ chối tất cả.

B. Không chặn lưu lượng dựa trên địa chỉ IP.

C. Quy tắc đầu tiên phải là quy tắc từ chối tất cả.

D. Không cho phép lưu lượng truy cập dựa trên địa chỉ IP.

Câu 36. Hệ thống mạng của bạn yêu cầu các bộ định tuyến có thể chặn lưu lượng dựa trên địa chỉ MAC. Loại quy tắc ACL nào cần được bộ định tuyến phải hỗ trợ trong trường hợp này?
A. Lớp 2
B. Lớp 1
C. Lớp 3
D. Lớp 4

Câu 37. Telnet được sử dụng cho mục đích nào sau đây?
A. Thực hiện quản lý dòng lệnh từ xa dạng rõ
B. Thực hiện quản lý dòng lệnh được mã hóa từ xa
C. Xác minh bộ định tuyến trong đường truyền
D. Buộc truy xuất các bản cập nhật hệ điều hành

Câu 38. Giao thức nào sau đây không có mã hóa?

A. SMTP

B. FTPS

C. SFTP

D. HTTPS

Câu 39. Do tình hình dịch Covid 19, công ty bạn muốn triển khai giải pháp cho phép nhân viên trong công ty được làm việc tại nhà. Yêu cầu đặt ra là mọi nhân viên đều có khả năng truy cập an toàn vào các tài nguyên trong mạng của công ty. Giải pháp nào nên được đề xuất trong trường hợp này:

A. Point to Site VPN

B. Site to Site VPN

C. Point to Point VPN

D. Firewall

Câu 40. Giao thức TCP / IP nào cung cấp cho quản trị viên một giao diện dòng lệnh từ xa cho các dịch vụ mạng?

A. Telnet

B. ARP

C. UDP

D. POP

Câu 41. Những giao thức TCP / IP nào sử dụng mã hóa để bảo mật đường truyền dữ liệu?

A. SSH, SCP, FTPS

B. SSH, SCP, Telnet

C. HTTPS, FTP, SSH

D. SCP, DNS, SSH

Câu 42. Công ty của bạn phát hành điện thoại thông minh cho nhân viên để sử dụng trong công việc. Chính sách công ty bắt buộc rằng tất cả dữ liệu lưu trữ trên điện thoại thông minh phải được mã hóa. Điều này nhắm đến tính chất nào của an toàn thông tin?

A. Bí mật

B. Tính toàn vẹn

C. Sẵn sàng

D. Trách nhiệm

Câu 43. Bạn là quản trị viên hệ thống mạng của công ty. Người quản lý của bạn yêu cầu bạn đánh giá các giải pháp sao lưu đám mây cho các văn phòng chi nhánh từ xa. Điều này áp dụng khái niệm an toàn nào sau đây?

A. Sẵn sàng

B. Tính toàn vẹn

C. Bí mật

D. Trách nhiệm

Câu 44. Alice phải gửi một tin nhắn e-mail quan trọng tới Bob, giám đốc nhân sự (HR). Chính sách của công ty nói rằng tin nhắn cho HR phải được ký điện tử. Khẳng định nào sau đây là đúng?

A. Khóa công khai của Alice được sử dụng để xác minh chữ ký số

B. Khóa công khai của Alice được sử dụng để tạo chữ ký số

C. Khóa riêng của Bob được sử dụng để tạo chữ ký số

D. Khóa riêng của Bob được sử dụng để xác minh chữ ký số

Câu 45. Sắp xếp các phương xác thực danh theo thứ tự an toàn tăng dần?

A. Tên người dùng và mật khẩu, thẻ thông minh, quét võng mạc

B. Quét võng mạc, mật khẩu, thẻ thông minh

C. Thẻ thông minh, quét võng mạc, mật khẩu

D. ACL, tên người dùng và mật khẩu, quét võng mạc

Câu 46. Mô hình kiểm soát truy cập ghi nhãn dữ liệu với các phân loại bảo mật khác nhau. Người dùng được xác thực phải gắn nhãn xác định để đọc dữ liệu được phân loại này. Loại mô hình kiểm soát truy cập này là gì?

A. Kiểm soát truy cập bắt buộc

B. Kiểm soát truy cập tùy ý

C. Kiểm soát truy cập dựa trên vai trò

D. Kiểm soát truy cập thời gian trong ngày

Câu 47. Để dễ dàng cấp quyền truy cập vào tài nguyên mạng cho nhân viên, bạn quyết định phải có một cách dễ dàng hơn là cấp cho người dùng quyền truy cập cá nhân vào tệp, máy in, máy tính và ứng dụng. Mô hình bảo mật nào bạn nên xem xét sử dụng?

A. Kiểm soát truy cập dựa trên vai trò

B. Kiểm soát truy cập tùy ý

C. Kiểm soát truy cập bắt buộc

D. Kiểm soát truy cập thời gian trong ngày

Câu 48. Công nghệ nào sau đây đảm bảo tính toàn vẹn cho dữ liệu?

A. MD5

B. RC4

C. AES

D. 3DES

Câu 49. Thuật toán nào sau đây sử dụng hai khóa liên quan về mặt toán học để truyền dữ liệu an toàn?

A. RSA

B. AES

C. 3DES

D. Blowfish

Câu 50. Công ty của bạn đã triển khai PKI. Bạn muốn mã hóa các tin nhắn e-mail bạn gửi cho một nhân viên khác là Tùng. Bạn cần sử dụng gì để mã hóa tin nhắn cho Tùng?

A. Khóa công khai của Tùng

B. Khóa riêng của Tùng

C. Khóa riêng của bạn

D. Khóa công khai của bạn