**Câu 1:** Đâu là hành vi KÉM an toàn nhất gây ra nguy cơ lây nhiễm mã độc trong hệ thống?

A. Cài đặt phần mềm từ chợ ứng dụng.

B. Vô hiệu hóa cơ chế tự động thực thi các tệp tin nhị phân và các tệp tin scrips.

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

D. Tải xuống tệp tin trên mạng.

**Câu 2:** Tùng tạo một file có tên Test.docx trên không gian lưu trữ đám mây của mình và chia sẻ nó cho các bạn cùng lớp. Điều nào sau đây mô tả đúng nhất về loại hệ thống kiểm soát truy nhập này?

A. Kiểm soát truy cập tùy ý

B. Kiểm soát truy cập thời gian trong ngày

C. Kiểm soát truy cập bắt buộc

D. Kiểm soát truy cập dựa trên vai trò

**Câu 3:** Một máy tính trong mạng nội bộ truy cập vào trang web độc hại và làm lây nhiễm ra toàn bộ các máy tính trong hệ thống làm cho các máy tính này khi truy cập vào bất cứ trang web nào cũng đều hiện lên những banner quảng cáo. Vấn đề nào đã xảy ra?

A. Worm mang Adware

B. Worm

C. Adware

D. Tấn công XSS

**Câu 4:** Với vị trí là một lập trình viên, làm thế nào để bạn có thể xây dựng được một website chống lại tấn công XS.

A. Cài đặt máy chủ web an toàn

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

C. Lọc dữ liệu đầu vào.

D. Thiết kế cơ sở dữ liệu an toàn

**Câu 5:** Mã độc Wannc Cry xuấ hiện năm 2017 lây lan qua lỗ hổng SMB của hệ điều hành Windows sau đó mỡ hóa và đòi tiền chuộc của nạn nhân? Mã độc này thuộc dạng nào?

A. Exploit

B. Trojan Horse

C. Worm mang Scareware

D. Worm mang Ransoware

**Câu 6:** Một hệ thống trong đó quản trị viên cần phải gán quyền truy cập cho người dùng dựa trên vị trí nghề nghiệp của họ. Lựa chọn nào sau đây là tốt nhất?

A. Non-Discretionary Access Control

B. DAC

C. Role-Based Access Control

D. MAC

**Câu 7:** Mã độc nào sau đây có khả năng tự lây lan mà không cần sự kích hoạt của con người?

A. Worm và Trojan

B. Worm

C. Virus và Trojan Horse

D. Virus và Worm

**Câu 8:** Bạn cần cấu hình IDS để ngăn chặn tấn công duyệt đường dẫn (directory traversal). Kiểu luật nào được sử dụng trong trường hợp này?

A. Anomaly-based

B. Behavior-based

C. Signature-based

D. Web-based

**Câu 9:** Một tập hợp của các công cụ phần mềm được sử dụng bởi hacker để trốn tránh các phần mềm phát hiện và được quyền quản trị của máy tính hoặc mạng là:

A. Spyware

B. Trojan

C. Backdoor

D. Rootkit

**Câu 10:** Một trang web không đáp ứng được một lượng lớn yêu cầu truy vấn HTTP đến máy chủ web. Giải pháp nào giúp tăng hiệu năng và giải quyết tình trạng này cho máy chủ web?

A. Kích hoạt SSL trên máy chủ web

B. Cài đặt hai máy chủ web lưu trữ cùng một nội dung. Cấu hình bộ cân bằng tải để phân phối kết nối HTTP đến giữa hai máy chủ web.

C. Đặt bộ định tuyến giữa máy chủ web và Internet để điều tiết các kết nối HTTP đến.

D. Nâng cấp dung lượng RAM cho máy chủ web.

**Câu 11:** Quản trị viên mạng phải cấp quyền truy cập mạng phù hợp cho các nhân viên thời vụ của công ty. Quy tắc nào sau đây nên được áp dụng.

A. Thêm tài khoản người dùng của các nhân viên này vào một nhóm. Đảm bào rằng nhóm có các quyền cần thiết và thiết đặt thời gian hiệu lực cho tài khoản.

B. Cung cấp cho nhân viên mới tài khoản người dùng và các quyền cần thiết.

C. Thêm tài khoản người dùng của các nhân viên này vào một nhóm. Đảm bảo rằng nhóm có các quyền cần thiết.

D. Hỏi nhân viên mới những quyền mà họ muốn.

**Câu 12**: Phát biểu nào sau đây đúng với hệ mật RSA

A. Thay thế cho hệ mật AES

B. Là hệ mật sử dụng một cặp khóa có liên hệ với nhau về mặt toán học.

C. Là hệ mật mã đối xứng

D. Thay thế cho hệ mật DES

Câu 13: Một tập hợp của các công cụ phần mềm được sử dụng bởi hacker để trốn tránh các phần mềm phát hiện và đạt được quyền quản trị của máy tính hoặc mạng là:

A. Spyware

B. Trojan

C. Backdoor

D. Rootkit

Câu 14: Kiểu tấn công nào thử các mật khẩu thông dụng nhiều lần cho đến khi đạt kết quả?

A. Birthdat attack

B. Replay attack

C. Dictionary attack

D. Spraying attack

Câu 15: Điều nào sau đây ĐÚNG với hệ mật khóa bí mật?

A. Khóa mã hóa và giải mã được dùng chung.

B. Khóa bí mật được sử dụng để trao đổi khóa

C. Từ khóa công khai không thể suy ngược lại được khóa bí mật.

D. Từ khóa bí mật không thể sinh ra được khóa công khai

Câu 16: Bộ định tuyến sử dụng loại kiểm soát truy cập nào để cho phép hoặc từ chối lưu lượng mạng?

A. Kiểm soát truy cập bắt buộc

B. Kiểm soát truy cập dựa trên vai trò

C. Kiểm soát truy cập tùy ý

D. Kiểm soát truy cập dựa trên quy tắc

Câu 17: Hệ thống nào sau đây đúng với hệ thống phát hiện xâm nhập mưc mạng – NIDS?

A. Các lưu lượng mạng được phân tích để tìm ra các gói tin độc hại

B. Máy tính được bảo vệ ngay cả khi không kết nối đến mạng LAN

C. các gói tin độc hại bị ngăn chặn.

D. Hoạt động trên từng máy cá nhân.

Câu 18: Đâu không phải là một hiểm họa xuất phát từ thư điện tử?

A. Phishing

B. Kỹ nghệ xã hội

C. Skimming

D. Mã độc

Câu 19: Tấn công XSS (Cross Site Scripting) xuất hiện ở tầng nào?

A. Tầng mạng – Network Layer

B. Tầng trình diễn – Presentation Layer

C. Tầng ứng dụng – Application layer

D. Tầng phiên – Session Layer

Câu 20: Phát biểu nào sau đây là KHÔNG ĐÚNG về tính toàn vẹn trong an toàn thông tin?

A. Đảm bảo thông tin không bị thay đổi khi truyền dẫn

B. Có thể bị ảnh hưởng do lỗi đường truyền.

C. Có thể bị vi phạm bởi tấn công từ điển

D. Đảm bảo phát hiện ra sự thay đổi của thông tin.

Câu 21: Bảng cầu vồng (Rainbow table) được sử dụng co kiểu tấn công nào sau đây?

A. Từ điển

B. Phát lại

C. Vét cạn

D. Dùng lại

Câu 22: Avra là một chương trình quét mã độc trong hệ thống nhưng lại chứa một số chức năng cho phép thu thập thông tin mà người dùng không biế. Vậy Avra là dạng mã độc gì?

A. Backdoor

B. Zoombie

C. Virus

D. Trojan Horse

Câu 23: Mô hình kiểm soát truy cập nào trong đó các đối tượng có nhẫn. quyền truy cập được thiết lập bởi hệ thống và chủ sở hữu dữ liệu.

A. MAC

B. DAC

C. Role based access control

D. Rule based access control

Câu 24: trong các thuật toán sau, thuật toán nào đame bảo tính toàn vẹn cho dữ liệu>

A. MD5

B. 3DES

C. AES

D. RC4

Câu 25: Phát biểu nào sau đây KHÔNG đúng về tính toàn vẹn trong an toàn thông tin?

A. Đảm bảo thông tin không bị thay đổi khi truyền dẫn

B. Có thể bị ảnh hưởng do lỗi đường truyền

C. Có thể bị vi phạm bởi tấn công từ điển

D. Đảm bảo phát hiện ra sự thay đổi của thông tin

Câu 26: Mã độc lây nhiễm vào máy tính cho phép kẻ tấn công điều khiển được máy tính đó là loại mã độc nào sau đây?

A. Trojan

B. Honeypot

C. Worm

D. Bot

Câu 27: Ma trận kiểm soát truy nhập (Acess Control Matrix) thuộc mô hình kiểm soát truy cập nào?

A. Kiểm soát truy cập dựa trên thuộc tính (ABAC)

B. Kiểm soát truy cập dựa trên vai trò (RBAC)

C. Kiểm soát truy cập tùy chọn (DAC)

D. Kiểm soát truy cập bắt buộc (MAC)

Câu 28: Bạn cần triển khai một giải pháp đảm bảo dữ liệu được lưu trữ trên ổ đĩa di động USB không bị giả mạo. Bạn nên chọn giải pháp nào dưới đây?

A. Mã hóa tệp tin bằng khóa bí mật

B. Mã hóa tập tin bằng khóa công khai

C. Sao lưu tệp

D. Băm và lưu trữ giá trị băm của tập tin

Câu 29: Phát biểu nào sau đây đúng về nguyên tắc đặc quyền tối thiểu trong an toàn thông tin?

A. Nguyên tắc đảm bảo rằng người dùng có quyền tối thiểu

B. Nguyên tắc đảm bảo rằng chỉ những người bắt buộc cần thông tin mới có quyền truy cập đến thông tin theo mức độ cần thiết.

C. Không cho phép người dùng trao quyền cho nhau

D. Nguyên tắc đảm bảo rằng người dùng có ít thông tin nhất

Câu 30: Đâu không phải là tính chất an toàn của thông tin?

A. Tính bí mật

B. Tính toàn vẹn

C. Tính chính xác

D. Tính sẵn sàng

Câu 31: Sau khi cố gắng đăng nhập đến một máy tính trong 3 lần, một người dùng thấy bị khóa tài khoản, không được phép truy nhập vào hệ thống. Vấn đề này phù hợp nhất với điều gì dưới đây?

A. Tường lửa đã chặn khi truy cập đến máy tính

B. Hệ thống phát hiện xâm nhập đã vô hiệu hóa tài khoản của người dùng đó

C. Tài khoản đã bị vô hiệu hóa bở chính sách an toàn

D. Cổng mạng bị vô hiệu hóa

Câu 32: Biện pháp đối phó nào sau đây được thiết kế tốt nhất để bảo vệ chống lại cuộc tấn công vét cạn vào mật khẩu?

A. Tạm khóa, khó tài khoản

B. Cập nhật bản vá

C. Nâng cao độ phức tạp của mật khẩu

D. Sử dụng mật khẩu mạnh

Câu 33: Một hệ thống muốn phát hiện ra các tấn công tiềm ẩn trong các lực lượng được mã hóa, công nghệ nào sau đây cho phép điều này?

A. SSL

B. HIDS

C. IPS

D. NIDS

Câu 34: Trong các loại dưới đây, đâu là một phần mềm gián điệp?

A. Keylogger

B. Phần mềm quét lỗ hổng

C. Packet sniffer

D. Worm

Câu 35: Lý do nào giải thích đúng nhất tại sao cần sử dụng hàm băm trong chữ ký số

A. Tăng độ an toàn chữ ký số

B. Giảm kích thước chữ ký số

C. Đảm bảo tính chống chối bỏ

D. Không thể thiếu được trong sơ đồ chữ ký số

Câu 36: Mô hình bảo mật nào sử dụng phân loại dữ liệu và phân quyền người dùng dựa trên phân loại dữ liệu?

A. DAC

B. PKI

C. RBAC

D. MAC

CÂU 37: Bạn theo dõi và kiểm tra lưu lượng mạng hàng tuần để đảm bảo rằng mạng đang được sử dụng đúng cách. Khi lam fnhuw vậy, bạn nhận thấy lưu lượng truy cập đến cổng TCP 53 trên máy chủ của mình từ một địa chỉ IP không xác định. Sau khi xem lại nhạt ký máy chủ của bạn, bạn nhận thấy nhiều lần thất bại trong việc thực hiện chuyển vùng đến máy chủ của mình. Đây là dấu hiệu của kiểu tán công nào?

A. ARP poisoning

B. Cross-site scripting

C. MAC flooding

D. DNS poisoning

Câu 38: Mã độc nào sau đây KHÔNG cần vật chủ?

A. Backdoor

B. Virus

C. Logic Borm

D. Worm

Câu 39: Đâu là một hệ mật đối xứng?

A. ECC

B. Elgamal

C. Blowfish

D. MD5

Câu 40: Đâu là một chức năng của một C&C Server?

A. Xác thực, cấp quyền và kiểm soát

B. Pentest

C. Phát tán tin rác

D. Điều khiển mạng Botnet

Câu 41: Bạn phải gửi một e-mail quan trọng cho gián đốc nhân sự (HR). Chính sách của công ty yêu cầu rằng e-mail này phải được ký điện tử. Khẳng định nào sau đây là đúng?

A. Khóa công khai của bạn được sử dụng để xác minh chữ kí số

B. Khóa công khai của bạn được sử dụng để tạo chữ kí số

C. Khóa riêng của HR được sử dụng để xác minh chữ kí số

D. Khóa riêng của HR được sử dụng để tạo chữ kí số

Câu 42: Những giao thức TCP/IP nào sử dụng mã hóa để bảo mật đường truyền dữ liệu?

A. HTTPS, FTP, SSH

B. SSH, SCP, FTPS

C. SCP, DNS, SSH

D. SSH, SCP, Telnet

Câu 43: Giải pháp nào sau đây được sử dụng để xác thực vào các ứng dụng trên ứng dụng môi trường mạng Internet:

A. Thẻ từ, smartcard, token + mã PIN

B. Mật khẩu + mật khẩu một lần OTP

C. Mật khẩu + smartcard

D. Mật khẩu + vân tay

Câu 44: Trong mô hình DAC để đảm bảo tính bí mật quy tắc đọc, ghi dữ liệu nào sau đây cần được tuân thủ

A. Đọc lên và ghi xuống

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

C. Đọc xuống và ghi lên

D. Chỉ đọc ghi ở cùng mức nhãn an toàn

Câu 45: Thuật toán nào sau đây không lọt vào vòng bầu chọn cuối cùng cho tiêu chuẩn mật mã AES?

A. MARS

B. Rijndael

C. Blowfish

D. RC6

Câu 46: Muốn giảm nhẹ rủi ro cho hệ thống thông tin, chúng ta cần

A. Trang bị hệ thống tường lửa

B. Trang bị hệ thống chống Virus

C. Nâng cao nhận thức người dùng

D. Loại trừ các điểm yếu bảo mật của hệ thống