**Câu 1:** Đâu là chức năng của một C&C Server?

A. Điều khiển mạng botnet

B. Phát tán tin rác

C. Pentest

D. Xác thực, cấp quyền và kiểm soát

**Giải thích:**

C&C Server (Command-and-Control Server) là máy chủ lệnh được sử dụng để đưa ra yêu cầu đối với các thiết bị kỹ thuật số bị nhiễm phần mềm độc hại như Ransomware hoặc Rootkit.

**Câu 2:** 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 dựa trên quy tắc – ACL - RuleBAC

B. Kiểm soát truy cập tùy ý - DAC

C. Kiểm soát truy cập bắt buộc - MAC

D. Kiểm soát truy cập dựa trên vai trò - RoleBAC

**Giải thích:**

Câu 3: Đâu không phải là một hiểm họa xuất phát từ thư điện tử?

A. Phishing

B. Skimming

C. Kỹ nghệ xã hội

D. Mã độc

Giải thích:

Câu 4: Mô hình truy cập được định nghĩa bởi người sở hữu hoặc tạo ra dữ liệu và cho phép người dùng có thể chia sẻ quyền với một số hạn chế nhất định:

A. Role-Base Access Control

B. DAC

C. Rule-Base Access Control

D. MAC

Giải thích:

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

A. Worm mang Ransomware

B. Exploit

C. Trojan Horse

D. Worm mang Scareware

Giải thích:

Câu 6:

Câu 7: Phát biểu nào sau đây đúng?

A. Virus lây nhiễm qua file

B. Virus ẩn dưới chương trình lành tính khác

C. Virus làm tràn băng thông của hệ thống

D. Virus có khả năng tự lan truyền qua mạng

Giải thích:

Câu 8: Trong các loại dưới đây, đâu là một phần mềm gián điệp?

A. Packet sniffer

B. Phần mềm quét lỗ hổng

C. Keylogger

D. Worm

Giải thích:

Câu 9: 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. Băm và lưu trữ giá trị băm của tập tin

D. Sao lưu tệp

Giải thích:

Câu 10:

Câu 11: Trong hệ mật mã AES, kích thước bản rõ đầu vào là 156 bit, vậy kích thước bản mã đầu ra là bao nhiêu?

A. 1024 bit

B. 156 bit

C. 128 bit

D. 256 bit

Giải thích:

Câu 12: Thuật toán nào sau đây không lọt vào vòng bầu chọn cuối cùng cho chuẩn mật mã AES?

A. Blowfish

B. MARS

C. Rijindael

D. RC6

Giải thích:

Câu 13: 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. Role-Base Access Control

B. Non-Discretionary Access Control

C. MAC

D. DAC

Chú thích:

Câu 14: Quản trị viên mạng phải cấp quyền truy cập mạng phù hợp cho các nhân viên thời vụ công ty. Quy tắc nào sau đây nên được áp dụng?

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

B. Hỏi nhân viên mới những quyền mà họ muốn

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

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

Chú thích:

Câu 15: Telnet được sử dụng cho mục đích nào sau đây?

1. Buộc truy xuất các bản cập nhật hệ điều hành
2. Xác minh bộ định tuyến trong đường truyền
3. Thực hiện quản lý dòng lệnh được mã hóa từ xa
4. Thực hiện quản lý dòng lệnh từ xa dạng rõ

Câu 16: Phát biểu nào sau đây KHÔNG đúng về tính toàn vẹn trong an toàn thông tin?

1. Có thể bị ảnh hưởng do lỗi đường truyền
2. Đảm bảo phát hiện ra sự thay đổi của thông tin
3. Có thể bị vi phạm bởi tấn công từ điển
4. Đảm bảo thông tin không bị thay đổi khi truyền dẫn

Câu 17: Điều nào sau đây đúng với hệ mật khóa bí mật?

1. Khóa bí mật được sử dụng để trao đổi khóa
2. Từ khóa công khai không thể suy ngược lại được khóa bí mật
3. Khóa mã hóa và giải mã được dùng chung
4. Từ khóa bí mật không thể sinh ra được khóa công khai

Câu 18: 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 cập này?

1. Kiểm soát truy cập dựa trên vai trò
2. Kiểm soát truy cập thời gian trong ngày
3. Kiểm soát truy cập bắt buộc
4. Kiểm soát truy cập tùy ý

Câu 20: Giá trị ngẫu nhiên được thêm vào trước khi băm mật khẩu được gọi là:

1. IV
2. DIP
3. Hash
4. Salt

Câu 21: Đâu không phải là mục đích của chữ ký số

1. Đảm bảo tính xác thực
2. Đảm bảo tính bí mật
3. Đảm bảo tính chống chối bỏ
4. Đảm bảo tính toàn vẹn

Câu 22: Nguyên nhân nào sau đây có thể dẫn tới phá vỡ tính toàn vẹn của thông tin trong hệ thống thông tin

1. Tấn công nhìn trộm
2. Lỗi đường truyền
3. Tấn công DoS, DDoS
4. Lộ khóa mã hóa

Câu 23: Mã độc nào sau đây KHÔNG cần vật chủ?

1. Logic Bomb
2. Virus
3. Backdoor
4. Worm

Câu 24: Đâu là hành vi KÉM an toàn nhất gây ra nguy cơ lây nhiễm mã độc trong hệ thống?

1. Vô hiệu hóa cơ chế tự động thực thi các tệp tin nhị phân và các tệp tin script
2. Cập nhật phần mềm, các bản vá cho hệ điều hành
3. Tải xuống tệp tin trên mạng
4. Cài đặt phần mềm từ chợ ứng dụng

Câu 26: Loại mã độc nào sau đây chỉ tồn tại trên bộ nhớ RAM

1. Fileless Virus
2. Rootkit
3. Logic Bomb
4. Backdoor

Câu 27: 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 biết. Vậy AVra là dạng mã độc gì?

1. Backdoor
2. Trojan Horse
3. Virus
4. Zombie

Câu 28: Tấn công SQL Injection thuộc loại hiểm họa an toàn thông tin nào sau đây?

1. Hiểm họa tích cực
2. Hiểm họa vô ý
3. Hiểm họa thụ động
4. Hiểm họa không phụ thuộc vào hệ thống

Câu 29: Sắp xếp các phương thức xác thực danh theo thứ tự an toàn tăng dần:

1. Mật khẩu, thẻ thông minh, vân tay
2. Vân tay, mật khẩu, thẻ thông minh
3. ACL, tên người dùng và mật khẩu, quét võng mạc
4. Thẻ thông minh, vân tay,mật khẩu

Câu 30: Sau khi cố gắng đăng nhập đến một máy tính trong 3 lần, một người dùng thấy đã bị khóa tài khoản, không được phép truy nhập vào hệ thống. Vấn đề này phù hợp nhất với điều gì dưới đây?

1. Tường lửa đã chặn khi truy cập đến máy tính
2. Hệ thống phát hiện xâm nhập đã vô hiệu hóa tài khoản của người dùng đó
3. Tài khoản đã bị vô hiệu hóa bởi chính sách an toàn
4. Cổng mạng bị vô hiệu hóa

Câu 31: Bảng cầu vồng (rainbow table) được sử dụng cho kiểu tấn công nào sau đây:

1. Phát lại
2. Vét cạn
3. Dùng lại
4. Từ điển

Câu 32: Với vị trí là một lập trình viên, làm thế nào để bạn có thể xây dựng được một website chống lại tấn công XSS:

1. Cài đặt máy chủ web an toàn
2. Lọc dữ liệu đầu vào
3. Không mở các đường link từ những nguồn không đáng tin cậy
4. Thiết kế cơ sở dữ liệu an toàn

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

1. HIDS
2. SSL
3. NIDS
4. IPS

Câu 34: 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?

1. Sử dụng mật khẩu mạnh
2. Tạm khóa, khóa tài khoản
3. Nâng cao độ phức tạp của mật khẩu
4. Cập nhật bản vá

Câu 35: Muốn giảm nhẹ rủi ro cho hệ thống thông tin, chúng ta cần

1. Nâng cao nhận thức người dùng
2. Loại trừ các điểm yếu bảo mật hệ thống
3. Trang bị hệ thống chống virus
4. Trang bị hệ thống tường lửa

Câu 36: Một công ty cung cấp hải sản muốn bảo vệ hệ thống thông tin của mình để các cách thức chế biến và đóng gói không bị tiết lộ với đối thủ cạnh tranh. Tính chất nào của an toàn thông tin đang được xem xét?

1. Tính sẵn sàng
2. Tính toàn vẹn
3. Tính chống chối bỏ
4. Tính bí mật

Câu 37: Tấn công XSS (Cross Site Scripting) xuất hiện ở tầng nào?

1. Tầng trình diễn (Presentation Layer)
2. Tầng ứng dụng (Application Layer)
3. Tầng mạng (Network Layer)
4. Tầng phiên (Session Layer)

Câu 38: 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?

1. Web-based
2. Behavior-based
3. Signature-based
4. Anomaly-based

Câu 39: 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?

1. Honeypoy
2. Trojan
3. Worm
4. Bot

Câu 40: Mã độc nào sau đây có khả năng tự lây lan mà không cần sự kích hoạt của con người?

1. Virus và Worm
2. Virus và Trojan Horse
3. Worm và Trojan
4. Worm

Câu 41: Bạn theo dõi và kiểm tra lưu lượng mạng hàng tuần để đảm bảo rằng mạng đang được sử dụng đúng cách.Khi làm như 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 nhật ký máy chủ của bạn, bạn nhận thấy nhiều lần thất bại trong việc thực hiện chuyển vùng máy chủ của mình. Đây là dấu hiệu của kiểu tấn công nào?

1. DNS poisoning
2. MAC flooding
3. Cross-site scripting
4. ARP poisoning

Câu 42: 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:

1. Backdoor
2. Spyware
3. Rootkit
4. Trojan

Câu 43: Trong các thuật toán sau, thuật toán nào đảm bảo tính toàn vẹn cho dữ liệu:

1. MD5
2. 3DES
3. AES
4. RC4

Câu 44: Giải pháp nào sau đây KHÔNG được sử dụng để phòng chống mã độc?

1. Antivirus
2. IDS
3. Phần mềm mã hóa đầu cuối
4. Deep Freeze

Câu 45: Người quản trị cấu hình quyền trên thư mục “Operation” để nhóm “kế toán” có thể tạo,sửa và xóa nội dung trong thư mục. Nhóm “quản lý” có thể đọc nội dung của thư mục và tất cả những người dùng khác đã bị từ chối truy cập. Bạn đã thực hiện hành động nào?

1. Uỷ quyền
2. Xác thực
3. Phân quyền
4. Định danh

Câu 46: Một máy tính trong mạng nội bộ truy cập vào trang web độc hại và làm lây nhiễm ra toàn bộ các máy trong hệ thống, làm cho các máy này khi truy cập phải bất cứ trang web nào cũng hiện lên những banner quảng cáo. Vấn đề nào đã xảy ra?

1. Worm mang Adware
2. Worm
3. Tấn công XSS
4. Adware

Câu 47: Bạn phải gửi một email quan trọng cho giám đốc nhân sự (HR). Chính sách của công ty yêu cầu rằng email này phải được ký điện tử. Khẳng định nào sau đây là đúng?

1. Khóa công khai của bạn được sử dụng để tạo chữ ký số
2. Khóa riêng của HR được sử dụng để tạo chữ ký số
3. Khóa riêng của HR được sử dụng để xác minh chữ ký số
4. Khóa công khai của bạn được sử dụng để xác minh chữ ký số

Câu 49: Giải pháp nào sau đây được sử dụng để xác thực vào các ứng dụng trên môi trường mạng Internet:

1. Thẻ từ, smartcard, token + mã PIN
2. Mật khẩu + Vân tay
3. Mật khẩu + Mật khẩu một lần OTP
4. Mật khẩu + Smart card

Câu 50: Mô hình bảo mật nào sử dụng phân loại dữ liệu và phân quyền người dùng dựa trên phân loại dữ liệu

1. RBAC
2. MAC
3. PKI
4. DAC

Câu 51: Trình tự truy cập nào sau đây là ĐÚNG?

1. Định danh -> Cấp quyền -> Xác thực
2. Cấp quyền -> Xác thực -> Định danh
3. Xác thực -> Định danh -> Cấp quyền
4. Định danh -> Xác thực -> Cấp quyền

Câu 52: Phát biểu nào sau đây đúng về nguyên tắc đặc quyền tối thiểu trong An toàn thông tin

1. 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
2. Không cho phép người dùng trao quyền cho nhau
3. Nguyên tắc đảm bảo rằng người dùng có ít thông tin nhất
4. Nguyên tắc đảm bảo rằng người dùng có quyền tối thiểu

Câu 53: Phát biểu nào sau đây là đúng với hệ mật RSA?

1. Thay thế cho hệ mật DES
2. Thay thế cho hệ mật AES
3. Là hệ mật mã đối xứng
4. Là hệ mật sử dụng một cặp khóa có liên hệ với nhau về mặt toán học

Câu 54: Mô hình kiểm soát truy cập nào trong đó các đối tượng có nhãn. Quyền truy cập được thiết lập bởi hệ thống và chủ sở hữu dữ liệu

1. Rule based access control
2. DAC
3. Role based access control
4. MAC

Câu 55: Tấn công nào sau đây KHÔNG làm ảnh hưởng đến tính bí mật của dữ liệu trên máy chủ web

1. XSS
2. SQL Injection
3. Command Injection
4. Directory Traversal

Câu 56: 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?

1. Nâng cấp dung lượng RAM cho máy chủ web
2. 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
3. Đặt bộ định tuyến giữa máy chủ web và Internet để điều tiết các kết nối HTTP đến
4. Kích hoạt SSL trên máy tính

Câu 57: Trong mô hình MAC để đảm bảo tính bí mật quy tắc đọc, ghi dữ liệu nào sau đây cần được tuân thủ?

1. Đọc lên và Ghi xuống
2. Chỉ đọc ghi ở mức nhãn an toàn thấp hơn
3. Đọc xuống và Ghi lên
4. Chỉ đọc ghi ở cùng mức nhãn an toàn

Câu 58: Lý do nào giải thích ĐÚNG NHẤT tại sao cần sử dụng hàm băm trong chữ ký số

1. Không thể thiếu được trong sơ đồ chữ ký số
2. Tăng độ an toàn chữ ký số
3. Đảm bảo tính chống chối bỏ
4. Giảm kích thước chữ ký số

Câu 59: Hiểm họa an toàn thông tin nào sau đây là hiểm họa tích cực?

1. Tấn công leo thang đặc quyền
2. Tấn công dò quét mật khẩu
3. Tấn công nghe lén đường truyền
4. Tấn công vét cạn

Câu 60: Phát biểu nào sau đây đúng với hệ thống phát hiện xâm nhập mức mạng-NIDS?

1. Máy tính được bảo vệ ngay cả khi không kết nối đến mạng LAN
2. Hoạt động trên từng máy cá nhân
3. Các lưu lượng mạng được phân tích để tìm ra các gói tin độc hại
4. Các gói tin độc hại bị ngăn cản