Chị Tâm check đáp án đi

**Câu 1: Kiểu tấn công vào hệ mật nào sau đây dựa trên các lý thuyết về xác suất**

1. Từ điển
2. Ngày sinh
3. Vét cạn
4. KPA

**Câu 2: Phát biểu nào sau đây đúng?**

1. Virus làm tràn băng thông của hệ thống
2. Virus có khả năng tự lan truyền qua mạng
3. Virus ẩn dưới chương trình lành tính khác
4. Virus lây nhiễm qua file

**Câu 3: 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. MAC
2. Rule based access control
3. DAC
4. Role based access control

**Câu 4: Lý do nào giải thích ĐÚNG NHẤT tại sao cần sử dụng hàm băm trong chứ ký số**

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

**Câu 5: Công nghệ nào nên được áp dụng để loại bỏ việc các thông tin nhạy cảm được gửi ra bên ngoài hệ thống mạng của tổ chức**

1. DLP
2. HIDS
3. NIDS
4. VPN

**Câu 6: Nguyên tắc mở trong ATTT quy định**

1. Không ai có thể tấn công vào các cơ chế bảo vệ và thuật toán của hệ thống ngoại trừ tác giả
2. Mở toàn bộ hệ thống và cơ chế bảo vệ cho người dùng
3. Yêu cầu mọi cơ chế bảo vệ và thuật toán đều phải được mở rộng và công khai
4. Hệ thống phải đảm bảo an toàn ngay cả khi kẻ tấn công biết được thông tin về thuật toán và cơ chế bảo vệ.

**Câu 7: Điều nào sau đây là cần được thực hiện để cấu hình bộ chuyển mạch Ethernet một cách an toàn?**

1. Vô hiệu hóa các cổng không sử dụng và cấu hình các VLAN bổ sung.
2. Vô hiệu hóa các cổng không sử dụng và gán địa chỉ MAC cho các cổng được kích hoạt.
3. Vô hiệu hóa các cổng không sử dụng và định cấu hình các cổng được kích hoạt cho bán song công.
4. Vô hiệu hóa các cổng không sử dụng và định cấu trên các cổng được kích hoạt cho song công hoàn toàn.

**Câu 8: Cách nào sau đây là tốt nhất và đơn giản nhất để chống lại lỗ hổng trong hệ điều hành?**

1. Tắt hệ thống khi không sử dụng
2. Cài đặt lại hệ điều hành thông dụng
3. Cài đặt bản vá mới nhất
4. Sao lưu hệ thống thường xuyên

**Câu 9: Đâu là một thuật toán hàm băm?**

1. SHA
2. 2DES
3. Blowfish
4. Elgamal

**Câu 10: Đoạn mã nào sau đây có thể gây ra SQL Injection**

1. ‘OR 1=1//
2. ‘OR 1=1-- -
3. ‘OR ‘1’=1
4. ‘OR 1=1

**Câu 11: Trong mô hình MAC để đảm bảo tính bí mật khi quy tắc đọc, ghi dữ liệu nào sau đây cần được tuân thủ?**

1. Chỉ đọc ghi ở cùng mức nhãn an toàn
2. Chỉ đọc ghi ở mức nhãn toàn thấp hơn máy tính được bảo vệ ngay cả khi không kết nối đến mạng lan
3. Đọc xuống và ghi lên
4. Đọc lên và gây xuống

**Câu 12: Kiểu tấn công nào thử các mật khẩu thông dụng nhiều lần cho tới khi nào kết quả**

1. Birthday attack
2. Spraying attack
3. Dictionary attack
4. Replay attack

**Câu 13: Phát biểu nào sau đây đúng với hệ thống phát hiện xâm nhập mức mạng – NIDS**

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

**Câu 14: 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. Honeypot
2. Bot
3. Trojan
4. Worm

**Câu 15: Ma trận kiểm soát truy cập (Access Control Matrix) thuộc mô hình kiểm soát truy cập nào**

1. Kiểm soát truy cập bắt buộc (MAC)
2. Kiểm soát truy cập dựa trên vai trò (RBAC)
3. Kiểm soát truy cập dựa trên thuộc tính (ABAC)
4. Kiểm soát truy cập tùy chọn (DAC)

**Câu 16: Avra là một chương trình quét mã độc trong hệ thống nhưng là chứa một số chức năng cho phép thu thập thông tin mà người dùng không biết. Vậy Arva là dạng mã độc gì?**

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

**Câu 17: 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. Signature-based
3. Anomaly-based
4. Behavior-based

**Câu 18: người quản trị cấu hình các quyền trên thư mục “Operation” để nhóm “kế toán” có thể tạo, sửa và xóa nội dung trong thư mục. Nhóm “người quản lý” có thể đọc nội dung của thư mục và cả những người dùng khác đã bị từ chối truy cập. Bạn đã thực hiện hành động nào?**

1. Ủy quyền
2. phân quyền
3. định danh
4. xác thực

**Câu 19: Phát biểu nào sau đây sai**

1. SQL Injection cho phép đánh cắp được và khẩu của toàn bộ người dùng trong CSDL
2. lỗ hổng SQL Injection xuất hiện khi đầu vào lược sử dụng trong câu truy vấn SQL không được kiểm tra
3. Việc sử dụng PL-SQL tạo ra lỗ hổng SQL Injection
4. SQL Injection cho phép kẻ tấn công có thể truy cập máy chủ CSDL và thực thi các đoạn mã SQL dưới quyền của người dùng đang kết nối đến CSDL

**Câu 20: không sử dụng một liên kết chuyên dụng, phương pháp nào tốt nhất để kết nối 2 mảng có khoảng cách địa lý cách xa nhau để đảm bảo an toàn?**

1. VPN
2. DMZ
3. Tường lửa
4. VLAN

**Câu 21: Đâu KHÔNG phải là mục địch của chữ ký số**

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

**Câu 22: Trong hệ mất AES, kích thước bản rõ đầu vào là 156 bit, kích thuớc bản mã đầu ra là bao nhiêu?**

1. 1024 bit
2. 256 bit
3. 128 bit
4. 156 bit

Hệ mã AES tiêu chuẩn hoạt động với kích thước khối là **128 bit**. Tuy nhiên, nếu bạn có một bản rõ đầu vào với kích thước là 156 bit, bạn sẽ cần phải thêm đệm (padding) hoặc sử dụng một kỹ thuật nào đó để chia nó thành các khối 128 bit trước khi mã hóa.

Sau khi áp dụng quá trình này, kích thước của bản mã đầu ra sẽ tương ứng với tổng số bit của các khối 128 bit. Trong trường hợp này, nếu bạn thêm đệm vào bản rõ 156 bit để tạo thành một khối 128 bit và một khối 32 bit (được thêm đệm lên thành 128 bit), thì kích thước của bản mã đầu ra sẽ là **256 bit** (tức là hai khối 128 bit). Do đó, câu trả lời phù hợp nhất trong trường hợp này có thể là B. 256 bit.

**Câu 23: Bảng cầu vồng (rainbow table) được sử dụng cho kiểu tấn công nào sau đây**

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

**Câu 24: 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 vào bất cứ trang web nào cũng đều hiện lên những banner quảng cáo. Vấn đề nào đã xảy ra?**

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

**Câu 25: trong mật mã khóa bí mật, số lượng khóa dù cho liên lạc trong hệ thống 10 người dùng là:**

1. 20
2. 45 (C210)­
3. 10
4. 54

**Câu 26: một tập hợp của các công cụ phần mềm được sử dụng bởi hacker để trốn tránh việc phát hiện và đạt được quyền quản trị của máy tính hoặc mạng là:**

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

**Câu 27: Tấn công SQL Injection thuộc loại ATTT nào sau đây?**

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

**Câu 28: Giải pháp nào sau đây được sử dụng để xác thực vào các ứng dụng trên môi trường mạng internet**

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

**Câu 29: Công ty của bạn phát hành điện thoại thông minh cho nhân viên được 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 nhằm đến tính chất nào của an toàn thông tin.**

1. Bí mật
2. Tính toàn vẹn
3. Trách nhiệm
4. Sẵn sàng

**Câu 30: Đâu không phải là 1 hiểm họa xuất phát từ thư điện tử?**

1. Skimming
2. Kỹ nghệ xã hội
3. Phising
4. Mã độc

**Câu 31: Loại mã độc nào sau đây chỉ tồn tại trên bộ nhớ RAM**

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

**Câu 32: sắp xếp các phương thức xác thực danh theo thứ tự an toàn tăng dần**

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

**Câu 33: người quản trị của hệ thống nhận thấy rằng xuất phát từ một số trạm máy trong hệ thống mạng của công ty tồn tại một loại mã độc tự động lây lan qua mạng nội bộ. Mã độc đó thuộc loại mã độc nào sau đây**

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

**Câu 34: Bạn cần triển khai một giải pháp đảm bảo dữ liệu được lưu trữ trên ổ đĩa di động USB bị giả mạo. Bạn nên chọn giải pháp nào dưới đây?**

1. Băm và lưu trữ giá trị băm của tập tin
2. Mã hóa tập tin bằng khóa công khai
3. Mã hóa tập tin bằng mã khóa bí mật
4. Sao lưu tệp

**Câu 35: Bạn muốn mã hóa một tập tin với dung lượng 18GB, lựa chọn nào sau đây là phù hợp**

1. Mật mã đối xứng
2. RSA
3. Mật mã khóa công khai,
4. Hàm băm

**Câu 36: Trong các thuật toán sau, thuật toán nào đảm bảo tính toàn vẹn cho DL**

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

**Câu 37: Tấn công nào sau đây không thuộc tấn công kỹ nghệ xã hội**

1. Man in the middle (tấn công mạng)
2. Whaling
3. Vishing
4. Phishing

**Câu 38: Hiểm họa ATTT nào sau đây là hiêm họa tích cực**

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

**Câu 39: Phát biểu nào sau đây là đúng với hệ mật RSA**

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

**Câu 40: Tấn công nào sau đây có thể gây ảnh hưởng đến hoạt động của mảy chủ web**

1. Buffer overflow
2. CRSF
3. Directory Traversal
4. XSS

**Câu 41: Bạn lưu trữ tài liệu cá nhân trên một dịch vụ lưu trữ đám mây. Bạn muốn dữ liệu của mình chỉ khả dụng cho những người có khóa được chia sẻ đặc biệt. Bạn nên áp dụng điều gì cho các tài liệu và bảng tính của bạn**

1. Thiết đặt quyền truy cập tệp
2. Mã hóa tập tin
3. Băm tập tin
4. Sao lưu tập tin

**Câu 42: Đâu là hành vi KÉM an toàn nhất gây ra nguy cơ lây nhiễm mã độc trong hệ thống?**

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

**Câu 43: Một công ty cung cấp hải sản muốn bảo vệ hệ thống thông tin của mình để các cách thức chế biến của quán không bị tiết lộ với các đối thủ cạnh tranh. Tính chất nào cyar ATTT đang được xem xét?**

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

**Câu 44: Trên các hệ điều hành có các chức năng hiển thị các cảnh báo và chờ xác nhận từ phía người dùng trước khi trong khi người dùng có thể thay đổi cài đặt hệ thống. Mục tiêu của việc này để chống lại tấn công nào?**

1. Ransomware
2. DNS Poisoning
3. Vét cạn
4. Leo thang đặc quyền

**Câu 45: Mô hình bảo mật nào sử dụng phân loại dữ liệu và phân quyền người dùng dựa trên phân loại DL**

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

**Câu 46: Giá trị ngẫu nhiên được thêm vào trước khi băm mật khẩu được gọi là**

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

**Câu 47: Do tình hình dịch covid 19, công ty 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 các tài nguyên trong mạng của công ty. Giải pháp nào nên được đề xuất trong trường hợp này**

1. Site to site VPN
2. Point to point VPN
3. Point to site VPN
4. Firewall

**Câu 48: Tấn công nào sau đây không làm ảnh hưởng đến tính bí mật của DL trên amsy chủ web**

1. Command Injection
2. SQL Injection
3. XSS (ảnh hưởng chủ yếu đến tính toàn vẹn và sẵn sàng)
4. Directory Traversal

**Câu 49: Phát biểu nào sau đây là đúng về HIDS**

1. Các lưu lượng nghi ngờ đi vào mạng sẽ bị ngăn chặn
2. Không thể theo dõi được các lưu lượng bị mã hóa
3. Không phân tích các tệp nhật ký
4. Nó phải được cài đặt trên mỗi hệ thống khi cần

**Câu 50: Người dùng ký lên thư điện tử sẽ giúp đảm bảo?**

1. Tính toàn vẹn của thư
2. ĐẶc quyền tối thiểu
3. Phân quyền cho thư
4. Tính bí mật của thư

**Câu 51: Phát biểu nào sau đây KHÔNG đúng về tính toàn vẹn trong ATTT**

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

**Câu 52: Bạn phải gửi 1 email 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 riêng của HR được sử dụng để xác minh chữ ký số
2. Khóa công khai của bạn được sử dụng để xác minh chữ ký số
3. Khóa riêng của HR được sử dụng để tạo chữ ký số
4. Khóa công khai của bạn được sử dụng để tạo chữ ký số

**Câu 53: Mô hình kiểm soát truy cập nào là cố định sử dụng tập các quy định về quyền truy cập được định nghĩa trước cho các tệp tin trên hệ thống**

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

**Cây 54: Công việc nào sau đây cho phép xác định các tài nguyên, nguy cơ và rủi ro cũng như cách thức khắc phục và giảm thiểu ảnh hưởng của các nguy cơ đến hệ thống thông tin**

1. Lập bản đồ mạng
2. Đánh giá lỗ hổng
3. Quét cổng
4. Phân tích rủi ro

**Câu 55: Kiểu tấn công dựa trên sức mạnh của máy tính để thử sai toàn bộ khả năng có thể của khóa trên DL mã hóa:**

1. Ngày sinh nhật
2. Vét cạn
3. Phát lại
4. Từ điển

**Câu 56: Mã độc nào sau đây KHÔNG cẩn vật chủ**

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

**Câu 57: Đâu là chức năng của một C&C server**

1. Pentest
2. Phát tán tin rác
3. Điều chỉnh mạnh botnet
4. Xác thực, cấp quyền và kiểm soát

**Câu 58: 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**

1. Hỏi nhân viên mới những quyền mà họ muốn
2. Cung cấp cho nhân viên mới tài khoản người dùng và các quyền cần thiết
3. Thêm tài khoản người dùng của các nhân viên này vào 1 nhóm. Đảm bảo rằng nhóm có các đặc quyền cần thiết và thiết đặt thời gian hiệu lực cho tài khoản
4. Thêm tào khoản người dùng của các nhân viên này vào 1 nhóm. Đảm bảo rằng nhóm có các quyền cần thiết

**Câu 59: Phát biểu nào sau đây đúng về nguyên tắc đặc quyền tối thiểu trong ATTT**

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

**Câu 60: IPS có khả năng nào sau đây mà IDS không có**

1. Cảnh báo tấn công
2. Phát hiện tấn công
3. Giám sát tấn công
4. Ngăn chặn tấn công