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 xss cho phép chèn script vào tham s truy vn http sau ó thc thi trên máy user

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 tn công vào request thông qua gi mo cookie

D. Path Traveling tan công cho phép hacker truy cap vào các tep nam ngoài thu muc hien hành (web)

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 bao ve du lieu lon co the duoc phan loai ro rang, mo hinh bao mat nhieu muc

C. RBAC role based access control

D. ABAC attribute based access control

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 access control lists

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 kiem soat dua tren dinh danh

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?

pki = ha tang khóa công khai

A. Khóa công khai của Tùng

B. Khóa riêng của Tùng

C. Khóa riêng của bạn

D. Khóa công khai của bạn

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA ATTT

ĐỀ THI KẾT THÚC HỌC PHẦN
MÔN: CƠ SỞ ATTT
Thời gian làm bài thi: 90 phút

ĐỀ 01

Sinh viên viết đáp án ĐÚNG vào cột "ĐÁP ÁN"

STT	Câu hỏi	ĐÁP ÁN
1.	Khi thiết lập luật ACL cho bộ định tuyến, cần tuân thủ hướng dẫn chung nào? A. Không cho phép lưu lượng truy cập dựa trên địa chỉ IP. B. Không chặn lưu lượng dựa trên địa chỉ IP. C. Quy tắc đầu tiên phải là quy tắc từ chối tất cả. D. Quy tắc cuối cùng phải là quy tắc từ chối tất cả.	D
2.	Sắp xếp các phương pháp định danh theo thứ tự an toàn tăng dần? A. Thẻ thông minh, quét võng mạc, mật khẩu B. Quét võng mạc, mật khẩu, thẻ thông minh C. Tên người dùng và mật khẩu, thẻ thông minh, quét võng mạc D. ACL, tên người dùng và mật khẩu, quét võng mạc	C
3.	Giao thức nào sau đây không thể định tuyến? A. HTTP B. DNS khong dieu chinh duoc ip C. NetBIOS D. Telnet	C
4.	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. Encryptionware B. Mã độc C. Criminalware D. Ransomware	D
5.	Một máy trạm có địa chỉ IP là 169.254.46.86. Các quản trị viên máy chủ nhận ra dịch vụ DHCP đang ngoại tuyến, vì vậy họ bắt đầu dịch vụ DHCP. Lệnh nào sẽ được sử dụng tiếp theo trên máy trạm để ngay lập tức có được cấu hình TCP / IP hợp lệ? A. ping -t B. tracert a,b,c kiem tra ket noi C. netstat -a D. ipconfig / renew	D
6.	Một loại phần mềm độc hại thay thế một thư viện hợp lệ của chương trình bằng một thư viện khác chứa các mã điều khiển nhằm chiếm quyền kiểm soát chương trình đó. Mã độc này sử dụng kỹ thuật nào sau đây?	A

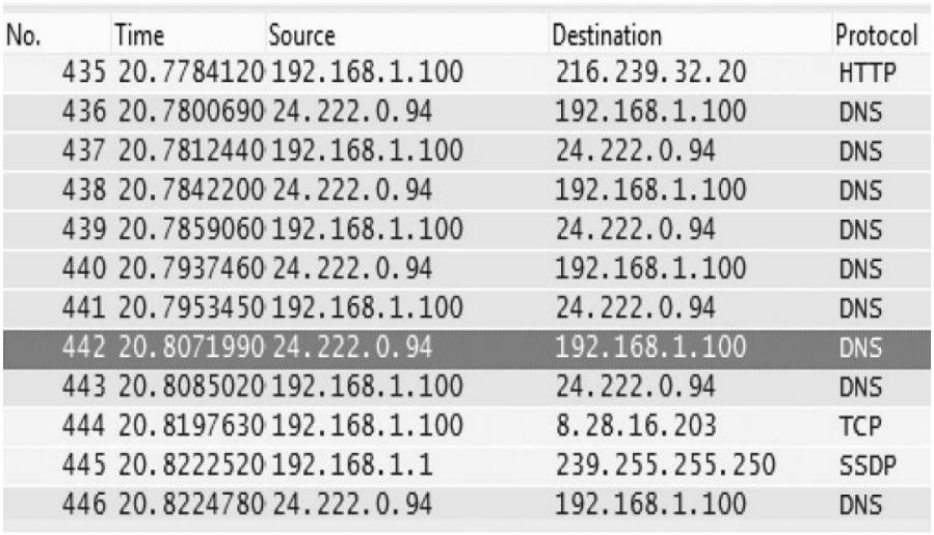
	A. DLL injection B. Pointer dereference C. Integer overflow D. Buffer overflow	
7.	Khi giám sát lưu lượng mạng, bạn nhận thấy rất nhiều kết nối IMAP giữa mạng của công ty bạn và địa chỉ IP không thuộc về máy chủ email của công ty. Nguyên nhân của những lưu lượng này là gì?? A. Các mã độc nâng cao B. Các ứng dụng nằm trong Whitelist C. DEP D. E-mail cá nhân	D
8.	Một hacker ngồi trong quán cà phê có điểm truy cập Internet và tiến hành thực hiện ARP poisoning mọi người kết nối với mạng không dây để tất cả lưu lượng truy cập qua máy tính xách tay hacker trước khi cô định tuyến lưu lượng truy cập vào Internet. Đây là loại tấn công nào? A. Rainbow tables B. Man in the middle C. DNS poison D. Spoofing	B
9.	Việc kiểm toán an ninh xác định thấy ba bộ định tuyến không dây không an toàn do sử dụng các cấu hình mặc định. Nguyên tắc bảo mật nào đã bị bỏ qua? A. Quản lý bản vá ứng dụng B. Kiện toàn an toàn thiết bị C. Xác thực đầu vào D. Nguyên tắc đặc quyền tối thiểu	B
10.	Có thể làm gì để bảo vệ dữ liệu sau khi thiết bị xách tay bị mất hoặc bị đánh cắp? A. Kích hoạt mã hóa. B. Thực hiện xóa dữ liệu từ xa. C. Kích hoạt khóa màn hình. D. Vô hiệu hóa phát hiện Bluetooth.?	B
11.	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 nắm bắt mọi thứ mà người dùng nhập vào. Đây là loại phần cứng nào? A. Smartcard B. Trojan C. Keylogger D. Bộ chuyển đổi PS/2	C
12.	Loại phần mềm nào giúp lọc bỏ các email rác không mong muốn? A. Anti-spam B. Antivirus C. Antispyware D. Anti-adware	A
13.	Khi lập kế hoạch thiết kế hạ tầng mạng, bạn quyết định sử dụng tường	B

	lửa phân tách giữa mạng Internet và mạng nội bộ. Bạn nên sử dụng tường lửa như thế nào? A. Quy tắc ACL cuối cùng sẽ cho phép tất cả. B. Sử dụng các thiết bị tường lửa từ các nhà cung cấp khác nhau. C. Quy tắc ACL đầu tiên nên từ chối tất cả. D. Sử dụng các thiết bị tường lửa từ cùng một nhà cung cấp	
14.	Những kỹ thuật kiểm thử ứng dụng nào giúp tìm kiếm những xử lý đầu vào không đúng? A. Fuzzing B. Overloading C. Kiểm thử xâm nhập D. Quét lỗ hổng	A
15.	Một đoạn mã độc sử dụng các cuộc tấn công từ điển vào máy tính để có quyền truy cập vào tài khoản quản trị. Đoạn mã này sau đó liên kết các máy tính bị xâm nhập với nhau nhằm mục đích nhận các lệnh từ xa. Thuật ngữ nào mô tả ĐÚNG NHẤT loại mã độc này? A. Exploit loi dung lo hong de tan cong B. Botnet C. Logic bomb D. Backdoor	B
16.	Bạn kiện toàn máy tính sử dụng Linux và đã vô hiệu hóa SSH và thay bằng Telnet. Bạn đảm bảo rằng mật khẩu được yêu cầu để truy cập Telnet. Bạn đã mắc phải lỗi nào trong trường hợp trên. A. Telnet bảo mật phải được bật xác thực khóa công khai. B. Chỉ nên sử dụng mật khẩu mạnh với Telnet. C. SSH nên được sử dụng thay vì Telnet. D. Cổng Telnet nên được thay đổi từ 23 thành 8080	C
17.	Sự khác biệt giữa rootkit và tấn công leo thang đặc quyền? A. Rootkit tự nhân bản. B. Sự leo thang đặc quyền là kết quả của một rootkit. leo tu ad len system C. Rootkit là kết quả của sự leo thang đặc quyền. D. Mỗi kiểu sử dụng một cổng TCP khác nhau.	B
18.	Chức năng User Account Control (UAC) trong Windows 8 cho phép người dùng có thể thay đổi các cài đặt của Windows nhưng trước khi thay đổi sẽ hiển thị lời nhắc để xác nhận lại sự thay đổi này cho người dùng. Điều này giúp chống lại tấn công nào? A. Leo thang đặc quyền B. Adware C. Spyware D. Worms	A
19.	Ai là người xác định cách gán nhãn dữ liệu? A. Người giám sát B. Chủ sở hữu C. Nhân viên bảo mật D. Quản trị viên hệ thống	B
20.	Bạn đã được yêu cầu triển khai một giải pháp dựa trên bộ định tuyến cho phép lưu lượng SSH đến từ một	b

	mạng con cụ thể. Bạn nên cấu hình cái gì? A. NIC B. ACL C. Proxy D. PSK	
21.	Một người dùng trên mạng của bạn nhận được e-mail từ ngân hàng nói rằng đã có sự cố bảo mật tại ngân hàng. Email tiếp tục bằng cách yêu cầu người dùng đăng nhập vào tài khoản ngân hàng của mình bằng cách theo liên kết được cung cấp và xác minh rằng tài khoản của cô ấy không bị giả mạo. Đây là loại tấn công nào? A. Phishing B. Spam C. Dictionary attack D. Spim	A
22.	Giao thức nào sử dụng cổng TCP 443? A. FTPS B. HTTP C. HTTPS D. SSH	C
23.	Hưng đang thực hiện việc theo dõi lưu lượng mạng Wi-Fi bằng cách sử dụng bộ phân tích gói tin và có thể đọc được các nội dung truyền qua mạng. Biện pháp nào sau đây có thể giữ cho các kết nối qua mạng được riêng tư? A. Cài đặt chứng chỉ số trên mỗi thiết bị truyền. B. Đặt mật khẩu quản trị viên mạnh cho bộ định tuyến Wi-Fi. C. Sử dụng xác thực thẻ thông minh. D. Mã hóa lưu lượng Wi-Fi.?	D
24.	Những thiết bị nào trong doanh nghiệp của bạn nên được cập nhật bản vá thường xuyên? (Chọn tất cả các đáp án đúng.) A. Mainframes B. Máy trạm C. Các máy ảo ảo hóa trên đám mây công cộng D. IP addresses	A,B
25.	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. Nâng cấp dung lượng RAM cho 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. Kích hoạt SSL trên máy chủ web.	b
26.	Người dùng ở trụ sở Đà Nẵng không thể kết nối với máy chủ web của công ty được đặt tại Hà Nội, nhưng họ có thể kết nối với các trang web khác trên Internet. Các kỹ thuật viên ở Hà Nội khẳng định máy chủ web đang chạy vì người dùng ở Hà Nội không gặp vấn đề gì khi kết nối với máy chủ web này. Bạn sử dụng công cụ ping đến máy chủ web ở	A

	Hà Nội nhưng không nhận được phản hồi. Bạn nên sử dụng công cụ nào tiếp theo? A. tracert B. ipconfig C. Telnet D. HTTP	
27.	Các nhà phát triển web tại công ty của bạn đang thử nghiệm mã trang web mới nhất của họ trước khi đi vào hoạt động để đảm bảo rằng nó hoạt động hiệu quả và an toàn. Trong quá trình thử nghiệm, họ cung cấp các URL không đúng định dạng với các tham số bất thường bổ sung cũng như sự phong phú của dữ liệu ngẫu nhiên. Thuật ngữ nào mô tả hành động của họ? A. Cross-site scripting B. Fuzzing C. Vá D. Debugging	B
28.	Là quản trị viên Windows, bạn cấu hình dịch vụ mạng Windows để chạy với tài khoản được tạo đặc biệt với các quyền hạn chế. Tại sao bạn cần làm điều này? A. Để ngăn chặn sâu máy tính xâm nhập vào mạng. B. Để ngăn chặn tin tặc nhận được các đặc quyền nâng cao do dịch vụ mạng bị xâm nhập. C. Dịch vụ mạng Windows sẽ không chạy với quyền quản trị. D. Các dịch vụ mạng Windows phải chạy với quyền truy cập hạn chế.	B
29.	Điều nào sau đây thể hiện TỐT NHẤT nguyên tắc đặc quyền tối thiểu? A. Phát hiện sử dụng Internet không phù hợp B. Phát hiện phần mềm độc hại đang chạy mà không có đặc quyền nâng cao C. Gán cho người dùng toàn quyền kiểm soát tài nguyên mạng D. Gán các quyền cần thiết để cho phép người dùng hoàn thành nhiệm vụ?	D
30.	Loại lỗ hổng nào dẫn đến việc ghi dữ liệu vượt ra ngoài ranh giới bộ nhớ dự kiến? A. Pointer dereference B. Integer overflow C. Buffer overflow D. Rò rỉ bộ nhớ	C
31.	Tùy chọn nào sẽ bảo vệ máy tính xách tay của nhân viên khi họ đi du lịch và kết nối với mạng không dây? A. Phần mềm tường lửa cá nhân B. Lọc địa chỉ MAC C. Ảo hóa D. Thẻ không dây tương thích 802.11n	A
32.	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?	D

	A. Zero day B. Worm C. Trojan D. Logic bomb	
33.	Biện pháp đối phó nào sau đây được thiết kế để bảo vệ chống lại cuộc tấn công vét cạn vào mật khẩu? A. Vá B. Khóa tài khoản C. Độ phức tạp của mật khẩu D. Mật khẩu mạnh	B
34.	Người quản lý của bạn đã đọc về các cuộc tấn công SQL Injecttion và đang tự hỏi có thể làm gì để bảo vệ chống lại chúng đối với các ứng dụng được phát triển nội bộ. Bạn muốn giới thiệu điều gì cho quản lý của mình? A. Vá B. Antivirus C. Xác thực đầu vào D. Tường lửa	C
35.	Bạn đang cấu hình một nhóm máy tính xách tay Windows cho nhân viên đi du lịch, một số người thích sử dụng chuột USB. Điều quan trọng là các máy móc càng an toàn càng tốt. Bạn nên cấu hình cái gì? (Chọn ba đáp án hợp lý nhất.) A. Tắt các cổng USB. B. Yêu cầu mã hóa thiết bị USB. C. Kích hoạt và cấu hình tường lửa Windows. D. Cài đặt và cấu hình phần mềm chống vi-rút. E. Kích hoạt chế độ lên lịch quản lý điện năng	B,C,D
36.	Mã hóa và ký điện tử lên e-mail bằng khóa công khai và khóa riêng có thể được thực hiện với công nghệ nào? A. 3DES B. DES C. Blowfish D. PGP	D
37.	Đâu là các hệ mật mã khối? (Chọn tất cả các đáp án đúng.) A. DES B. RSA C. RC4 D. AES	A,D
38.	Một nhân viên thu được lưu lượng truy cập mạng trên mạng LAN trong khoảng thời gian 24 giờ được biểu diễn như hình dưới. Nếu muốn xem lưu lượng truy cập mạng liên quan đến người dùng kết nối với các trang web thì anh ta cần lọc cột Giao thức nào trong cột giao thức trong hình?	A

	 A. HTTP B. DNS C. TCP D. SSDP	
39.	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 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	C
40.	Giao thức TCP / IP nào được thiết kế để đồng bộ hóa thời gian giữa các máy tính? A. SNMP B. Windows Time Service C. NTP network time protocol D. SMTP	C
41.	Chính sách bảo mật của công ty nhấn mạnh tính bảo mật dữ liệu và bạn phải cấu hình các thiết bị máy tính một cách phù hợp. Bạn nên làm những gì? (Chọn hai.) A. Cài đặt trình đọc thẻ thông minh để người dùng có thể nhận dạng chính họ trước khi gửi các tin nhắn e-mail quan trọng. B. Thực thi mã hóa thẻ SD trên điện thoại thông minh cấp cho nhân viên. C. Cấu hình một cụm chuyển đổi dự phòng máy chủ để đảm bảo rằng các tài liệu nhạy cảm luôn có sẵn. D. Đặt quyền truy cập tệp và thư mục để kiểm soát quyền truy cập tệp của người dùng.	B,D
42.	Bạn lưu trữ tài liệu cá nhân và bảng tính trên một dịch dụ 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? A. Quyền truy cập tệp B. Băm tập tin	D

	C. Sao lưu tệp D. Mã hóa tập tin	
43.	Dữ liệu quan trọng về mạng nội bộ của công ty bạn đã bị rò rỉ trực tuyến. Kẻ tấn công đã không tấn công mạng của bạn. Đây là vấn đề có thể xảy ra do nguyên nhân nào? A. Kiểm tra tính toàn vẹn của tệp B. Tường lửa dựa trên máy chủ C. Phương tiện truyền thông xã hội D. Lỗi DLP cho người dùng độc hại	C
44.	Mô hình bảo mật nào sử dụng phân loại dữ liệu và phân quyền người dùng dựa trên phân loại dữ liệu A. RBAC B. DAC C. PKI D. MAC	D
45.	Là quản trị viên máy chủ, bạn cấu hình cài đặt bảo mật sao cho mật khẩu phức tạp dài ít nhất tám ký tự phải được sử dụng cho tất cả tài khoản người dùng. Điều này là ứng dụng của nguyên tắc quản lý nào? A. Hết hạn B. Phục hồi C. Thông tin xác thực D. Vô hiệu hóa	C
46.	Phát biểu nào sau đây đúng? (Chọn tất cả các đáp án đúng.) A. Worms ghi lại tất cả các ký tự đã gõ vào một tệp văn bản. B. Worms tự phát tán sang các hệ thống khác. C. Worms có thể mang virus. D. Worms lây nhiễm vào đĩa cứng MBR.	B,C
47.	Bạn đang kiểm tra cấu hình bộ định tuyến của mình và phát hiện ra lỗ hổng bảo mật. Sau khi tìm kiếm trên Internet, bạn nhận ra rằng lỗ hổng này chưa được biết. Loại tấn công nào gây ảnh hưởng lớn nhất bộ định tuyến của bạn trong trường hợp này? A. Từ chối dịch vụ B. Phishing attack C. Zero-day exploit D. Ping of death	C
48.	Giải pháp nào sau đây đảm bảo an toàn cho việc truy cập một máy UNIX từ xa? A. SSH B. SSL C. SSO D. SHA	A
49.	Kiểu tấn công nào liên quan đến việc hacker gửi quá nhiều dữ liệu đến một dịch vụ hoặc ứng dụng thường dẫn đến việc hacker có quyền truy cập quản trị vào hệ thống? A. Tấn công ngày sinh nhật B. Typo squatting/URL hijacking C. Eavesdrop	D

	D. Buffer overflow	
50.	Phát biểu nào sau đây đúng với backdoors? (Chọn tất cả các đáp án đúng.) A. Chúng là mã độc. B. Chúng cho phép điều khiển quyền truy cập của người dùng thông qua cổng 26. C. Chúng được truy cập thông qua rootkit. D. Chúng cung cấp quyền truy cập vào tài khoản root Windows.	A,C
51.	Bạn đang kiểm tra một hệ thống của một người dùng sau khi cô ấy phàn nàn về tốc độ sử dụng Internet chậm hơn thường ngày. Sau khi phân tích hệ thống, bạn nhận thấy rằng địa chỉ MAC của cổng mặc định trong bộ đệm ARP đang tham chiếu sai địa chỉ MAC. Kiểu tấn công nào đã xảy ra? A. Brute force B. DNS poisoning C. Buffer overflow D. ARP poisoning	D
52.	Công nghệ nào sau đây đảm bảo tính toàn vẹn cho dữ liệu? A. 3DES B. RC4 C. AES D. MD5	D
53.	Bạn là nhân viên an toàn thông tin trong một cơ quan chính phủ. Bạn đang sửa đổi chính sách bảo mật USB. Những mục nào áp dụng cho bảo mật USB? (Chọn hai.) A. Không cho phép các ổ USB ngoài lớn hơn 1TB. B. Vô hiệu hóa cổng USB. C. Ngăn chặn dữ liệu của công ty bị sao chép vào thiết bị USB trừ khi mã hóa thiết bị USB được bật. D. Ngăn chặn dữ liệu công ty bị sao chép vào thiết bị USB trừ khi mã hóa cổng USB được bật.	B,C
54.	Quản trị viên mạng phải cấp quyền truy cập mạng phù hợp cho nhân viên mới. Điều nào sau đây là chiến lược tốt nhất? A. Cung cấp cho nhân viên mới tài khoản người dùng và các quyền cần thiết. B. Thêm tài khoản người dùng của nhân viên mới vào một nhóm. Đảm bảo rằng nhóm có các quyền cần thiết. C. Cung cấp cho nhân viên mới quyền quản trị mạng. D. Hỏi nhân viên mới những quyền mà cô ấy muốn.	B
55.	Trong khi thiết lập các cơ chế an toàn cho mạng, bạn triển khai một chính sách mật khẩu người dùng phức tạp. Mọi người dùng thường xuyên bày tỏ than phiền về việc quên mật khẩu. Những gì bạn nên cấu hình để làm giảm bớt những than phiền này? A. Hết hạn mật khẩu B. Thay đổi mật khẩu định kỳ C. Gợi ý mật khẩu D. Độ dài mật khẩu tối đa	C

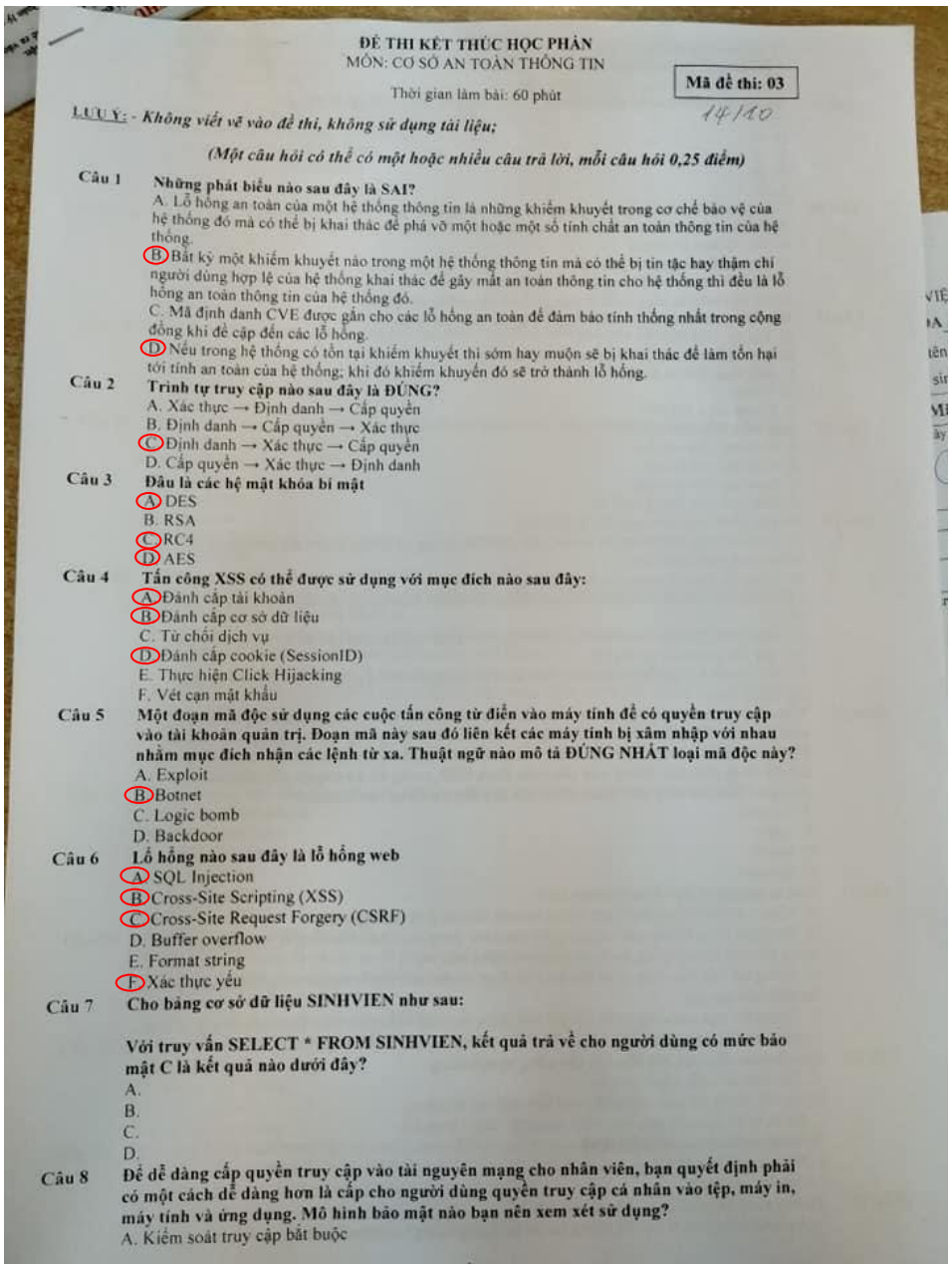
56.	Bạn đang định cấu hình thiết bị mã hóa mạng và phải tính đến các thiết bị khác có thể không hỗ trợ các thuật toán mới hơn và mạnh hơn. Phát biểu nào sau đây liệt kê các tiêu chuẩn mã hóa từ yếu nhất đến mạnh nhất? A. DES, 3DES, RSA B. 3DES, DES, AES C. RSA, DES, Blowfish D. RSA, 3DES, DES ma hoa mang khong dung blowfish	A
57.	Bạn quyết định rằng các máy tính LAN của bạn sẽ sử dụng mã hóa bất đối xứng với IPSec để bảo mật lưu lượng LAN. Trong khi đánh giá làm thế nào điều này có thể được thực hiện, bạn được trình bày với một loạt các lựa chọn các phương pháp và thuật toán mã hóa. Chọn phân loại chính xác của tiêu các thuật toán mật mã. A. Không đối xứng: RSA, AES Đối xứng: DES, 3DES B. Đối xứng: 3DES, DES Không đối xứng: Blowfish, RSA C. Đối xứng: 3DES, DES Không đối xứng: RC4, RSA D. Đối xứng: AES, 3DES Không đối xứng: RSA	D
58.	Thuật ngữ nào mô tả quá trình che dấu dữ liệu trong một tệp tin? A. Trojan B. Steganography C. Mã hóa D. Chữ ký số	B
59.	Khi chuyên gia an ninh cấp quyền cho các thư mục trên máy chủ tệp để cho phép các tài liệu của một phòng ban chỉ được phép truy cập và sửa đổi bởi các thành viên trong phòng ban đó thì mục tiêu an toàn thông tin nào đã được thỏa mãn? A. Bí mật B. Tính toàn vẹn C. Sẵn có D. An toàn	A
60.	Phương pháp tiếp cận mật mã nào sử dụng các điểm trên một đường cong để xác định các cặp khóa công khai và bí mật? A. RSA B. DES C. ECC D. PKI	C

Sinh viên KHÔNG được sử dụng mọi tài liệu, nộp bài làm kèm theo đề thi

Giáo viên ra đề
(Ký, ghi rõ họ tên)

Chủ nhiệm bộ môn
(Ký, ghi rõ họ tên)

khong can hoc dau hihi



ĐỀ THI KẾT THÚC HỌC PHẦN
MÔN: CƠ SỞ AN TOÀN THÔNG TIN

Thời gian làm bài: 60 phút

Mã đề thi: 03

14/10

LƯU Ý: - *Không viết vẽ vào đề thi, không sử dụng tài liệu;*

(Một câu hỏi có thể có một hoặc nhiều câu trả lời, mỗi câu hỏi 0,25 điểm)

Câu 1 **Những phát biểu nào sau đây là SAI?**
A. Lỗ hổng an toàn của một hệ thống thông tin là những khiếm khuyết trong cơ chế bảo vệ của hệ thống đó mà có thể bị khai thác để phá vỡ một hoặc một số tính chất an toàn thông tin của hệ thống.
B. Bất kỳ một khiếm khuyết nào trong một hệ thống thông tin mà có thể bị tin tặc hay thậm chí người dùng hợp lệ của hệ thống khai thác để gây mất an toàn thông tin cho hệ thống thì đều là lỗ hổng an toàn thông tin của hệ thống đó.
C. Mã định danh CVE được gắn cho các lỗ hổng an toàn để đảm bảo tính thống nhất trong cộng đồng khi đề cập đến các lỗ hổng.
D. Nếu trong hệ thống có tồn tại khiếm khuyết thì sớm hay muộn sẽ bị khai thác để làm tổn hại tới tính an toàn của hệ thống; khi đó khiếm khuyến đó sẽ trở thành lỗ hổng.

Câu 2 **Trình tự truy cập nào sau đây là ĐÚNG?**
A. Xác thực → Định danh → Cấp quyền
B. Định danh → Cấp quyền → Xác thực
C. Định danh → Xác thực → Cấp quyền
D. Cấp quyền → Xác thực → Định danh

Câu 3 **Đâu là các hệ mật khóa bí mật**
A. DES
B. RSA
C. RC4
D. AES

Câu 4 **Tấn công XSS có thể được sử dụng với mục đích nào sau đây:**
A. Đánh cắp tài khoản
B. Đánh cắp cơ sở dữ liệu
C. Từ chối dịch vụ
D. Đánh cắp cookie (SessionID)
E. Thực hiện Click Hijacking
F. Vét cạn mật khẩu

Câu 5 **Một đoạn mã độc sử dụng các cuộc tấn công từ điển vào máy tính để có quyền truy cập vào tài khoản quản trị. Đoạn mã này sau đó liên kết các máy tính bị xâm nhập với nhau nhằm mục đích nhận các lệnh từ xa. Thuật ngữ nào mô tả ĐÚNG NHẤT loại mã độc này?**
A. Exploit
B. Botnet
C. Logic bomb
D. Backdoor

Câu 6 **Lỗ hổng nào sau đây là lỗ hổng web**
A. SQL Injection
B. Cross-Site Scripting (XSS)
C. Cross-Site Request Forgery (CSRF)
D. Buffer overflow
E. Format string
F. Xác thực yếu

Câu 7 **Cho bảng cơ sở dữ liệu SINHVIEN như sau:**

Với truy vấn SELECT * FROM SINHVIEN, kết quả trả về cho người dùng có mức bảo mật C là kết quả nào dưới đây?
A.
B.
C.
D.

Câu 8 **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 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 9 **Trong mật mã khóa bí mật, số lượng khóa trong hệ thống 10 người dùng là**
A. 54
B. 45
C. 10
D. 20
E. 50

(10*9)/2

Câu 10 **Trong mã hóa dữ liệu sử dụng mật mã khóa công khai, phát biểu nào sau đây là ĐÚNG:**
A. Dữ liệu được mã hóa bằng khóa công khai, giải mã bằng khóa bí mật
B. Tốc độ thực thi nhanh
C. Mọi người đều có thể giải mã
D. Từ khóa công khai không thể tìm ra khóa bí mật
E. Dữ liệu mã hóa bằng khóa bí mật, giải mã bằng khóa công khai

Câu 11 **Xác thực nào dưới đây KHÔNG phải là xác thực đa nhân tố**
A. Thẻ từ + Mã PIN
B. Mật khẩu một lần (OTP – One Time Passowrd)
C. Mật khẩu + vị trí địa lý
D. Token
E. Smartcard + Mã PIN

Câu 12 **Mục đích của Chữ ký số:**
A. Đảm bảo tính xác thực
B. Đảm bảo tính bí mật
C. Đảm bảo tính toàn vẹn
D. Đảm bảo tính chống chối bỏ

Câu 13 **Những phát biểu nào sau đây là ĐÚNG?**
A. Tính toàn vẹn của thông tin là tính chất đảm bảo thông tin không bị sửa đổi khi truyền từ điểm nguồn tới điểm đích.
B. Thông tin lưu trữ cũng cần được đảm bảo tính toàn vẹn.
C. Nhiệm vụ đảm bảo tính toàn vẹn của thông tin là phát hiện sự sửa đổi thông tin nếu có sự sửa đổi đó.
D. Nhiệm vụ đảm bảo tính toàn vẹn của thông tin là tạo một bản sao của thông tin để thay thế bản gốc khi phát hiện sự sửa đổi.
E. Việc tạo và lưu giữ một hay nhiều bản sao của thông tin có thể giúp kiểm tra tính toàn vẹn của thông tin.

Câu 14 **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. Rootkit
B. Spam
C. Worm
D. Adware

Câu 15 **Đâu là những ví dụ về rò rỉ thông tin?**
A. Nhân viên bán hàng đọc được thông tin mật của công ty thương mại.
B. Từ ngoài vùng khiếm soát có thể nghe được nội dung cuộc họp của công ty, trong đó có thông tin mật, do hệ thống loa hoạt động với công suất lớn.
C. Thông tin mật của công ty bị đối thủ biết được do họ mua chuộc người trong nội bộ công ty đặt thiết bị nghe lén.
D. Thông tin mật của công ty bị đối thủ biết được do nhân viên gửi nhầm file chứa thông tin mật trong quá trình làm việc.

Câu 16 **Đâu là mục tiêu của mã độc khi tấn công người dùng**
A. Thu thập dữ liệu trên máy tính
B. Ăn cắp thông tin như mật khẩu, mã bảo mật thẻ tín dụng.
C. Sử dụng tài nguyên trên máy nạn nhân (để "đào" Bitcoin).
D. Mã hóa dữ liệu và đòi tiền chuộc.
E. Phá hủy dữ liệu trên máy nạn nhân.
F. Vét cạn mật khẩu

Câu 17 **Những phát biểu nào sau đây là đúng?**
A. An toàn thông tin là bảo vệ thông tin và hệ thống thông tin trước tấn công của tin tặc, bao

Commented [HNNQ1]: 9/ Công thức mật mã đối xứng (N*(n-1))/2
11/ 1 cái

ĐÁNH DẤU 12
MÀU ĐỎ: ĐÚNG
MÀU XANH: CÓ VẺ ĐÚNG
MÀU TÍM: HÊN XUI =))

An toàn thông tin bao gồm việc đảm bảo hoạt động ổn định của hệ thống thông tin trước khả năng xảy ra sự cố vật lý.
C. Một trong những nhiệm vụ của an toàn thông tin là ngăn chặn sự phát tán tin giả trên mạng để không gây tác động tiêu cực lên nhận thức của cộng đồng.

u 18 **Mô hình dưới đây thuộc mô hình nào**
A. Access Control List (ACM)
B. Access Capability (Profile)
C. RBAC
D. MAC

u 19 **Đâu KHÔNG phải là tính chất an toàn của thông tin?**
A. Tính bí mật
B. Tính cấp thiết
C. Tính chính xác
D. Tính sẵn sàng
E. Tính kịp thời

u 20 **Cho hàm băm H, từ H(x) không thể tìm được x là tính chất nào của hàm băm**
A. Nén
B. Kháng tiền ảnh
C. Kháng tiền ảnh thứ 2
D. Kháng va chạm

u 21 **Độ an toàn của mật khẩu nào dưới đây là lớn nhất (biết rằng mật khẩu có thể gồm chữ số, chữ cái hoa và thường)**
A. 12345678
B. 12a4567
C. A2a34567
D. 2a13456
E. 123456789012
F. 1a2345678

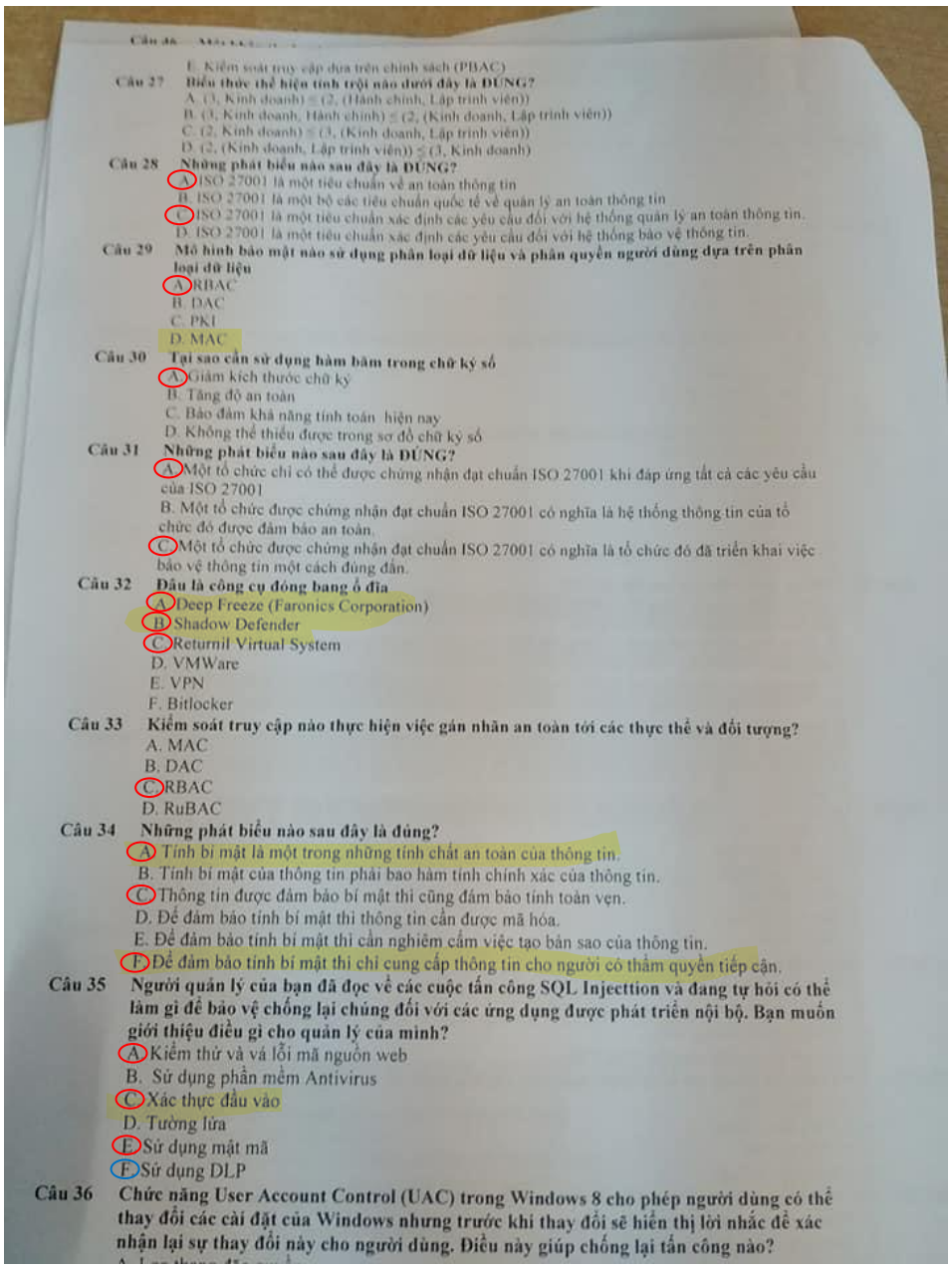
22 **Những phát biểu nào sau đây là SAI?**
A. Hiểm họa an toàn thông tin là bất kỳ sự tác động nào mà có thể dẫn đến sự phá vỡ một hoặc một số tính chất an toàn của thông tin.
B. Hiểm họa an toàn thông tin là những dự định của tin tặc tác động lên một hệ thống thông tin nhằm phá vỡ một hoặc một số tính chất an toàn của thông tin.
C. Hiểm họa an toàn thông tin là khả năng tiềm tàng trong tương lai về việc một hoặc một số tính chất an toàn của thông tin bị phá vỡ bởi tin tặc, hoặc thậm chí là bởi những người dùng hợp lệ trong hệ thống.
D. Mọi hành động dù là vô tình hay cố ý của người dùng hợp lệ trong hệ thống nếu có thể phá vỡ một hay một số tính chất an toàn của thông tin thì đều được coi là hiểm họa an toàn thông tin đối với hệ thống đó.

23 **Loại lỗ hổng nào dẫn đến việc ghi dữ liệu vượt ra ngoài ranh giới bộ nhớ dự kiến?**
A. Pointer dereferences
B. Integer overflow
C. Buffer overflow
D. Rò rỉ bộ nhớ
E. Stack overflow
F. Heap overflow

24 **Phát biểu nào sau đây ĐÚNG?**
A. Worms ghi lại tất cả các ký tự đã gõ vào một tệp văn bản.
B. Worms tự phát tán sang các hệ thống khác.
C. Worms có thể mang virus.
D. Worms lây nhiễm vào đĩa cứng MBR.

25 **Tính chất sao trong mô hình kiểm soát truy cập bắt buộc MAC nhằm**
A. Không đọc lên
B. Không đọc xuống
C. Không ghi lên
D. Không ghi xuống

26 **Ma trận kiểm soát truy cập (Acess Control Matrix) thuộc mô hình kiểm soát truy cập nào**
A. Kiểm soát truy cập bắt buộc (MAC)
B. Kiểm soát truy cập tùy chọn (DAC)
C. Kiểm soát truy cập dựa trên vai trò (RBAC)
D. Kiểm soát truy cập dựa trên thuộc tính (ABAC)



E. Kiểm soát truy cập dựa trên chính sách (PBAC)

Câu 27 **Biểu thức thể hiện tính trội nào dưới đây là ĐÚNG?**

A. (3, Kinh doanh) ≤ (2, (Hành chính, Lập trình viên))

B. (3, Kinh doanh, Hành chính) ≤ (2, (Kinh doanh, Lập trình viên))

C. (2, Kinh doanh) ≤ (3, (Kinh doanh, Lập trình viên))

D. (2, (Kinh doanh, Lập trình viên)) ≤ (3, Kinh doanh)

Câu 28 **Những phát biểu nào sau đây là ĐÚNG?**

A. ISO 27001 là một tiêu chuẩn về an toàn thông tin

B. ISO 27001 là một bộ các tiêu chuẩn quốc tế về quản lý an toàn thông tin

C. ISO 27001 là một tiêu chuẩn xác định các yêu cầu đối với hệ thống quản lý an toàn thông tin.

D. ISO 27001 là một tiêu chuẩn xác định các yêu cầu đối với hệ thống bảo vệ thông tin.

Câu 29 **Mô hình bảo mật nào sử dụng phân loại dữ liệu và phân quyền người dùng dựa trên phân loại dữ liệu**

A. RBAC

B. DAC

C. PKI

D. MAC

Câu 30 **Tại sao cần sử dụng hàm băm trong chữ ký số**

A. Giảm kích thước chữ ký

B. Tăng độ an toàn

C. Bảo đảm khả năng tính toán hiện nay

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

Câu 31 **Những phát biểu nào sau đây là ĐÚNG?**

A. Một tổ chức chỉ có thể được chứng nhận đạt chuẩn ISO 27001 khi đáp ứng tất cả các yêu cầu của ISO 27001

B. Một tổ chức được chứng nhận đạt chuẩn ISO 27001 có nghĩa là hệ thống thông tin của tổ chức đó được đảm bảo an toàn.

C. Một tổ chức được chứng nhận đạt chuẩn ISO 27001 có nghĩa là tổ chức đó đã triển khai việc bảo vệ thông tin một cách đúng đắn.

Câu 32 **Đâu là công cụ đóng băng ổ đĩa**

A. Deep Freeze (Faronics Corporation)

B. Shadow Defender

C. Returnil Virtual System

D. VMWare

E. VPN

F. Bitlocker

Câu 33 **Kiểm soát truy cập nào thực hiện việc gán nhãn an toàn tới các thực thể và đối tượng?**

A. MAC

B. DAC

C. RBAC

D. RuBAC

Câu 34 **Những phát biểu nào sau đây là đúng?**

A. Tính bí mật là một trong những tính chất an toàn của thông tin.

B. Tính bí mật của thông tin phải bao hàm tính chính xác của thông tin.

C. Thông tin được đảm bảo bí mật thì cũng đảm bảo tính toàn vẹn.

D. Để đảm bảo tính bí mật thì thông tin cần được mã hóa.

E. Để đảm bảo tính bí mật thì cần nghiêm cấm việc tạo bản sao của thông tin.

F. Để đảm bảo tính bí mật thì chỉ cung cấp thông tin cho người có thẩm quyền tiếp cận.

Câu 35 **Người quản lý của bạn đã đọc về các cuộc tấn công SQL Injecttion và đang tự hỏi có thể làm gì để bảo vệ chống lại chúng đối với các ứng dụng được phát triển nội bộ. Bạn muốn giới thiệu điều gì cho quản lý của mình?**

A. Kiểm thử và vá lỗi mã nguồn web

B. Sử dụng phần mềm Antivirus

C. Xác thực đầu vào

D. Tường lửa

E. Sử dụng mật mã

F. Sử dụng DLP

Câu 36 **Chức năng User Account Control (UAC) trong Windows 8 cho phép người dùng có thể thay đổi các cài đặt của Windows nhưng trước khi thay đổi sẽ hiển thị lời nhắc để xác nhận lại sự thay đổi này cho người dùng. Điều này giúp chống lại tấn công nào?**

leo thang dac quyen

C. Spyware
D. Worms

Câu 37 **Mã độc nào sau đây có khả năng tự nhân bản**
(A) Virus
B. Trojan
(C) Worm
D. Logic Bomb
E. Ransomware

Câu 38 **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 đến máy chủ của mình. Đây là dấu hiệu của kiểu tấn công nào?**
A. ARP poisoning
B. Cross-site scripting
(C) DNS poisoning
D. MAC flooding

Câu 39 **Không thể tìm được cặp (x,y) sao cho H(x) = H(y) là tính chất nào của hàm băm**
A. Kháng tiền ảnh
B. Nén
(C) Kháng va chạm
D. Kháng tiền ảnh thứ 2

Câu 40 **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. Zero day
B. Worm
C. Trojan
(D) Logic bomb

Câu 41 **Một hacker ngồi trong quán cà phê có điểm truy cập Internet và tiến hành thực hiện ARP poisoning mọi người kết nối với mạng không dây để tất cả lưu lượng truy cập qua máy tính xách tay hacker trước khi cô định tuyến lưu lượng truy cập vào Internet. Đây là loại tấn công nào?**
A. Rainbow tables
(B) Man in the middle
C. DNS poison
D. Spoofing

Câu 42 **Biện pháp đối phó nào sau đây được thiết kế để bảo vệ chống lại cuộc tấn công vét cạn vào mật khẩu?**
A. Cập nhật bản vá
(B) Tạm khóa, khóa tài khoản
C. Nâng cao độ phức tạp của mật khẩu
D. Sử dụng mật khẩu mạnh

Câu 43 **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. Encryptionware
B. Virus
C. Criminalware
(D) Ransomware
E. Worm

Câu 44 **Mã xác thực thông điệp (MAC – Message Authentication Code) nhằm:**
(A) Đảm bảo tính xác thực
B. Đảm bảo tính bí mật
C. Đảm bảo tính toàn vẹn
D. Đảm bảo tính chống chối bỏ

Câu 45 **Loại phần mềm nào giúp lọc bỏ các email rác không mong muốn?**
A. Anti-spam
B. Antivirus