NHẬP MÔN AN TOÀN VÀ BẢO MẬT THÔNG TIN

Câu 1: Thế nào là tính bảo mật của hệ thống thông tin?

1. Là đặc tính của hệ thống trong đó thông tin được giữ bí mật không cho ai truy cập
2. Là đặc tính của hệ thống trong đó tất cả thông tin được lưu trữ dưới dạng mật mã
3. Là đặc tính của hệ thống trong đó chỉ có những người dùng được cho phép mới có thể truy xuất được thông tin
4. Tất cả đều đúng

Câu 2: Các cơ chế đảm bảo tính toàn vẹn của thông tin

1. Gồm các cơ chế ngăn chặn và cơ chế phát hiện vi phạm về toàn vẹn thông tin
2. Mật mã hóa toàn bộ thông tin trong hệ thống
3. Lưu toàn bộ thông tin trong hệ thống dưới dạng nén
4. Tất cả các cơ chế trên

Câu 3: Các nguy cơ nào sau đây có thể ảnh hướng đến tính khả dụng của hệ thống thông tin

1. Các thiết bị không an toàn
2. Các tấn công từ chối dịch vụ (DoS và DDoS)
3. Virut và các loại phần mềm phá loại khác trên máy tính
4. Tất cả các nguy cơ trên

Câu 4: Hành vi nào sau đây ảnh hưởng đến tính bí mật của hệ thống thông tin

1. Một người dùng có thể xem thông tin của các người khác
2. Virut xóa mất các tập tin trên đĩa cứng
3. Mất điện thường xuyên làm hệ thống máy tính là việc gián đoạn
4. Tất cả các hành vi trên

Câu 5: Hành vi nào sau đây ảnh hưởng đến tính khả dụng của hệ thống thông tin

1. Một người dùng có thể xem thông tin của các người khác
2. Virut xóa mất các tập tin trên đĩa cứng
3. Mất điện thường xuyên làm hệ thống máy tính là việc gián đoạn
4. Tất cả các hành vi trên

Câu 6: Để tìm bản rõ người thám mã sử dụng

1. Kết hợp nhiều phương pháp tấn công khác nhau
2. Chỉ sử dụng phương pháp giải bài toán ngược
3. Chỉ sử dụng khóa bí mật
4. Vét cạn khóa

Câu 7: Chức năng chính của Virut là :

1. Lây nhiễm và sinh sản
2. Sống kí sinh và lây nhiễm
3. Tự phát triển độc lập và lây nhiễm
4. Sống kí sinh và sinh sản

Câu 8: Để đảm bảo an toàn thông tin bằng cách

1. Sử dụng phương pháp mã hóa
2. Sử dụng tường lửa
3. Phân quyền truy cập thông tin
4. Kết hợp các biện pháp trên

Câu 9: So sánh tốc độ mã hóa và giải mã của hệ mật mã công khai với hệ mật mã bí mật hiện đại (với cùng độ dài bản rõ và độ dài khóa) ?

1. Tốc độ như nhau
2. Mật mã công khai nhanh hơn
3. Mật mã công khai chậm hơn
4. Không so sánh được

Câu 10: Giải mã là:

1. Quá trình tấn công hệ mật mã để tìm bản rõ và khóa bí mật
2. Quá trình biến đổi thông tin từ dạng đọc sang dạng không đọc được
3. Quá trình biến đổi thông tin từ dạng không đọc được sang dạng đọc được
4. Giấu thông tin để không nhìn thấy

Câu 11: Thám mã là:

1. Quá trình tấn công hệ mật mã để tìm bản rõ và khóa bí mật
2. Quá trình biến đổi thông tin từ dạng đọc sang dạng không đọc được
3. Quá trình biến đổi thông tin từ dạng không đọc được sang dạng đọc được
4. Giấu thông tin để không nhìn thấy

Câu 12: Mã hóa là :

1. Quá trình tấn công hệ mật mã để tìm bản rõ và khóa bí mật
2. Quá trình biến đổi thông tin từ dạng đọc sang dạng không đọc được
3. Quá trình biến đổi thông tin từ dạng không đọc được sang dạng đọc được
4. Giấu thông tin để không nhìn thấy

Câu 13: Hành vi nào sau đây ảnh hưởng đến tính toàn vẹn của hệ thống thông tin

1. Một sinh viên sao chép bài tập của một sinh viên khác
2. Virut xóa mất các tập tin trên đĩa cứng
3. Mất điện thường xuyên làm hệ thống máy tính làm việc gián đoạn
4. Tất cả các hành vi trên

Câu 14: Thế nào là tính khả dụng của hệ thống thông tin

1. Là tính sẵn sàng của thông tin trong hệ thống cho mọi nhu cầu truy xuất
2. Là tính sẵn sàng của thông tin trong hệ thống cho mọi nhu cầu truy xuất hợp lệ
3. Là tính dễ sử dụng của thông tin trong hệ thống
4. Tất cả đều sai

Câu 15: Chọn câu sai khi nói về các nguy cơ đối với sự an toàn của hệ thống thông tin

1. Những kẻ tấn công hệ thống (attacker) có thể là con người bên trong hệ thống
2. Người sử dụng không được huấn luyện về an toàn hệ thống cũng là 1 nguy cơ đối với hệ thống
3. Một hệ thống không kết nối vào mạng Internet thì không có các nguy cơ tấn công
4. Xâm nhập hệ thống (intrusion) có thể là hành vi xuất phát từ bên ngoài hoặc từ bên trong hệ thống

Câu 16: Trojan là 1 phương pháp tấn công kiểu:

1. Can thiệp trực tiếp vào máy tính nạn nhân để lấy các thông tin quan trọng
2. Đánh cắp dữ liệu của nạn nhân truyền trên mạng
3. Tấn công làm tê liệt hệ thống mạng của nạn nhân
4. Điều khiển máy tính của nạn nhân từ xa thông qua phần mềm cài sẵn trong máy nạn nhân

Câu 17: Metasploit Framework là công cụ tấn công khai thác lỗ hổng để lấy Shell của máy nạn nhân. Ngay sau khi cài đặt chạy công cụ này thì gặp sự cố tất cả các lệnh gõ trên Metasploit không được thi hành. Nguyên nhân:

1. Do không kết nố được tới máy nạn nhân
2. Do không cài đặt công cụ Metasploit vào ổ C
3. Do máy nạn nhân không cho phép tấn công
4. Do phần mềm Anti Virut trên máy tấn công đã khóa (blocked) không cho thi hành

Câu 18: Virut máy tính không thể lây lan qua:

1. Mạng máy tính
2. Đĩa CD
3. Thẻ nhớ Flash
4. Lưu trữ USB

Câu 19: Phòng chống tấn công Tấn công từ chối dịch vụ (DDoS)

1. Chỉ có thể dùng tưởng lửa
2. Có thể hạn chế trong bằng cách lập trình
3. Hiện nay đã có cách phòng chống hiệu quả
4. Cách hiệu quả duy nhất là lưu trữ và khôi phục (backup và restore)

Câu 20: SQL Injection là gì?

1. Một ngôn ngữ lập trình đa năng
2. Một loại khai thác bảo mật trong đó kẻ tấn công thêm mã ngôn ngữ truy vấn mang tính cấu trúc (SQL) vào hôp nhập biểu mẫu của trang Web để truy cập vào tài nguyên hoặc thực hiện thay đổi dữ liệu
3. Một ngôn ngữ chỉ ghi lại dựa trên nguyên mẫu, sử dụng chủ yếu dưới dạng Javascript ở phía máy khách, được triển khai như 1 phần của trình duyệt Web để cung cấp các giao diện của người dùng và trang Web động năng cao
4. Một chương trình đố vui của Mỹ về nhiều lĩnh vực: lịch sử, văn hóa, nghệ thuật, văn hoái đại chúng, khoa học, thể thao, địa lý, từ ngữ và nhiều hơn nữa.

Câu 21: Có thể ngăn chặn SQL Injection bằng cách nào?

1. Bắt lỗi dữ liệu đầu vào của người dùng (đảm bảo rằng người dùng không thể nhập bất cứ điều gì khác ngoài những gì họ cho phép)
2. Không sử dụng SQL nữa
3. Đặt mật mã của bạn ở chế độ công khai
4. Tất cả nhưng cách trên

Câu 22: Cross-site scripting là gì?

1. Một ngôn ngữ lập trình cho phép kiểm soát một hoặc nhiều ứng dụng
2. Một loại lỗ hổng bảo mật máy tính thường được tìm thấy trong các ứng dụng Web, cho phép kẻ tấn công chèn tập lệnh phía máy khách vào các trang Web được người dùng khác xem.
3. Một loại ngôn ngữ script chuyên dùng để điều khiển máy tính.
4. Tài liệu hoặc tài nguyên thông tin phù hợp với World Wide Web và có thể được truy cập thông qua trình duyệt

Câu 23: Social Engineering là gì?

1. Kĩ thuật sai khiến mọi người thực hiện hành vi nào đó hoặc tiết lộ thông tin bí mật.
2. Một môn học kỹ thuật chuyên nghiệp liên quan đến việc thiết kế, thi công và bảo trì môi trường vật lý và tự nhiên, bao gồm các công
3. Một môn học kỹ thuật áp dụng các nguyên tắc của vật lý và khoa học vật liệu để phân tích, thiết kế, sản xuất và bảo trì các hệ thống cơ khí.
4. Sự điều khiển trực tiếp của con người đối với bộ gen của một sinh vật bằng cách sử dụng công nghệ DNA hiện đại.

Câu 24: Rootkit là gì?

1. Một bộ kit được các nhà sinh học sử dụng khi làm việc với các loại thực vật.
2. Tên mặc định của thư mục UNIX.
3. Rootkit là được thiết kế để qua mặt các phương pháp bảo mật máy tính.
4. Một máy chủ định danh cho vùng root của Domain Name System.

Câu 25: Kiến trúc TCP/IP sử dụng bao nhiêu lớp?

1. Bảy
2. Sáu
3. Năm
4. Bốn

Câu 26: Điều nào sau đây không phải là tấn công tiêu đề HTTP?

1. Accept-Language
2. Referer
3. Response splitting
4. Content-length

Câu 27: Ngôn ngữ đánh dấu nào được thiết kế để mang dữ liệu

1. TCMP
2. HTTP
3. HTML
4. XML

Câu 28:Kiểu tấn công nào liên quan đến tấn công truy cập các tệp trong các thư mục khác với thư mục gốc?

1. SQL Injection
2. Command Injection
3. XML Injection
4. Directory traversal

Câu 29: Kiểu tấn công nào sửa đổi các trường có chứa các đặc tính khác nhau của dữ liệu đang được truyền đi?

1. XML manipulation
2. HTML packet
3. SQL Injection
4. HTTP header

Câu 30: Điều nào trong số này KHÔNG phải là tấn cống DoS?

1. SYN flood
2. Ping flood
3. Smurf
4. Push flood

Câu 31: Cơ sở của 1 cuộc tấn công SQL Injection là gì ?

1. Để máy chủ SQL tấn công trình duyệt web máy khách
2. Để chèn câu lệnh SQL thông qua đầu vào người dùng chưa được lọc
3. Để hiện thị mã SQL để nó có thể được kiểm tra
4. Để lien kết các máy chủ SQL thành 1 botnet

Câu 32: Hành động nào không thể thực hiện được thông qua tấn công SQL Injection thành công?

1. Địng dạng lại ổ cứng của máy chủ ứng dụng web
2. Hiển thị danh sách số điện thoại của khách hành
3. Khám phá tên của các trường khác nhau trong bảng
4. Xóa bảng cơ sở dữ liệu

Câu 33: Tấn công phát lại :

1. Được coi là 1 loạt tấn công DoS
2. Tạo bản sao truyền để sử dụng sau này
3. Có thể được ngăn chặn bằng cách vá trình duyệt web
4. Replay các cuộc tấn công hơn và hơn để lũ máy chủ

Câu 34: Một tên khác cho 1 đối tượng được chia sẻ cục bộ là gì?

1. Flash cookie
2. Session cookie
3. Ram cookie
4. Secure cookie

Câu 35: Plug-in trình duyệt

1. Chỉ hoạt động trên máy chủ web
2. Có thể được nhúng bên trong trang web nhưng không thể thêm tiện ích
3. Có chức năng bổ sung cho toàn bộ trình duyệt
4. Đã được thay thế bằng tiện ích mở rộng của trình duyệt

Câu 36: Một kẻ tấn công muốn tấn công kích thước tối đa của 1 loại số nguyên sẽ thực hiện loại tấn công nào?

1. Buffer overflow
2. Real number
3. Heap size
4. Integer overflow

Câu 37: Kẻ tấn công sử dụng tràn bộ nhớ đệm để là gì?

1. Xóa tập tin chữ kí tràn bộ đệm
2. Làm hỏng nhận để máy tính không thể khởi động lại
3. Trỏ đến một khu vực khác trong bộ nhớ dữ liệu chứa mã phần mềm độc hại của kẻ tấn công
4. Đặt virut vào nhân (kernel)

Câu 38: Điều gì là duy nhất về tấn công cross-site scripting (XSS) so với các cuộc tấn công injection khác?

1. Mã SQL được sử dụng trong một cuộc tấn công XSS.
2. XSS yêu cầu sử dụng trình duyệt.
3. XSS không tấn công máy chủ ứng dụng web để ăn cắp hoặc làm hỏng thông tin của nó.
4. Tấn công XSS hiếm khi được sử dụng nữa so với các cuộc tấn công injection khác.

Câu 39: Cookie không được tạo bởi trang web đang được xem là gì?

1. Cookie chính chủ
2. Cookie của bên thứ hai
3. Cookie của bên thứ ba
4. Cookie của bên thứ tư

Câu 40: Loại tấn công nào được thực hiện bởi kẻ tấn công lợi dụng xâm nhập và truy cập trái phép được xây dựng thông qua 3 hệ thống thành công mà tất cả đều được tin tưởng lẫn nhau?

1. Privilege rights
2. Heap spray
3. Transitive
4. Vertical escalation

Câu 41: Điều nào trong số này KHÔNG phải là lý do tại sao việc bảo mật các ứng dụng web phía máy chủ là khó?

1. Mặc dù các thiết bị bảo mật mạng truyền thông có thể chặn các cuộc tấn công mạng truyền thông, chúng không thể luôn chặn các cuộc tấn công ứng dụng web
2. Các bộ vi xử lý trên máy khách nhỏ hơn trên các máy chủ web và do đó chúng dễ bảo vệ hơn
3. Nhiều cuộc tấn công ứng dụng web khái thác lỗ hổng chưa biết trước đó
4. Bằng cách thiết kế các ứng dụng web phía máy chủ chấp nhận đầu vào của người dùng có thể chứa mã độc

Câu 42: Tuyên bố nào là chính xác về lý do tại sao các thiết bị bảo mật mạng truyền thống không thể được sử dùng để chặn các cuộc tấn công ứng dụng Web?

1. Các thiết bị bảo mật mạng truyền thông bỏ qua nội dung lưu lượng HTTP, là phương tiện tấn công ứng dụng web
2. Các cuộc tấn công ứng dụng web sử dụng các trình duyệt web không thể được điều khiển máy tính cục bộ
3. Các thiết bị bảo mật mạng không thể ngăn ngừa các cuộc tấn công từ tài nguyên web
4. Tính chất phức tạp của TCP/IP cho phép quá nhiều nên Ping bị chặn

Câu 43: Trojan Horse là gì?

1. Một chương trình độc hại mà lấy cắp tên người dùng và mật khẩu của bạn
2. Gây hại như mã giả mạo hoặc thay thế mã hợp pháp
3. Một người sử dụng trái phép những người thu truy cập vào cơ sở dữ liệu người dùng của bạn và cho biết thêm mình như một người sử dụng
4. Một máy chủ đó là phải hy sinh cho tất cả các hacking nỗ lực để đăng nhập và giám sát các hoạt động của hacking

Câu 44: Một hacker cố gắng tấn công 1 máy chủ qua Internet nó được gọi là loại tấn công?

1. Tấn công từ xa
2. Tấn công truy cập vật lý
3. Truy cập địa phương
4. Tấn công nội bộ

Câu 45: Kĩ thuật tấn công phổ biến trên web là ?

1. Chiếm hữu phiên làm việc
2. Tràn bộ đệm
3. Từ chối dịch vụ (DoS)
4. Chèn câu truy vấn SQL

Câu 46: Câu nào đúng về Hashed Message Authentication Code (HMAC)

1. Chỉ mã hóa khóa
2. Mã hóa khóa và thông báo
3. Chỉ mã hóa tin nhắn
4. Chỉ mã hóa khóa DHE

Câu 47: Phiên bản mới nhất của thuật toán băm là gì?

1. SHA-2
2. SHA-3
3. SHA-4
4. SHA-5

Câu 48: Hệ thống khóa công khai tạo ra các khóa công cộng ngẫu nhiên khác nhau cho mỗi phiên được gọi là:

1. Trao đổi khóa công khai (PKE)
2. Elliptic Curve Diffie-Hellman (ECDH)
3. Diffie-Hellman (DH)
4. Perfect forward secrecy

Câu 49: Chứng minh rằng người dùng đã gửi một email được gọi là.

1. Tính từ bỏ(repudiation)
2. Tính toàn vẹn (integrity)
3. Tính không từ chối(non-repudiation)
4. Tính khả dụng (availability)

Câu 50: Nếu Bob muốn gửi một tin nhắn an toàn cho Alice bằng cách sử dụng một thuật toán mã hóa bất đối xứng, thì anh ta sử dụng khóa nào để mã hóa thông điệp

1. Khoá bí mật của Alice
2. Khoá công khai của Alice
3. Khoá bí mật của Bob
4. Khoá công khai của Bob

Câu 51: Thuật toán mã hóa bất đối xứng nào sử dụng số nguyên tố?

1. EFS
2. quantum computing
3. ECC
4. RSA

Câu 52: Thuật toán mã hóa bất đối xứng nào an toàn nhất?

1. SHA-2
2. BTC-2
3. RSA
4. ME-14

Câu 53: Chữ ký điện tử có thể cung cấp cho từng lợi ích sau đây NGOẠI TRỪ

1. chứng minh tính toàn vẹn của thông điệp
2. xác minh người nhận
3. xác minh người gửi
4. thực thi không từ chối

Câu 54: Thuật toán nào trong số này là thuật toán mật mã đối xứng mạnh nhất?

1. Advanced Encryption Standard
2. Data Encryption Standard
3. Triple Data Encryption Standard
4. Rivest Cipher (RC) 1

Câu 55:Tiêu chuẩn mật mã khóa công khia (PKCS)

1. Được chấp nhận rộng rãi trong ngành
2. Chỉ được sử dụng để tạo khóa công khai
3. Xác định các thuật toán băm được tạo ra như thế nào
4. Đã được thay thế bới PKI

Câu 56: Điều nào KHÔNG phải là nơi khóa có thể được lưu trữ

1. Trong tokens
2. Trong digests
3. Trên hệ thống của người dùng cục bộ
4. Nhúng trong chứng chỉ kĩ thuật số

Câu 57:Cơ sở hạ tầng của khóa công khai (PKI)

1. Tạo mật mã khóa riêng
2. Là quản lý chứng chỉ kĩ thuật số
3. Yêu cầu sử dụng RA thay vì CA
4. Tự động tạo khóa công khai riêng tư

Câu 58: Giao thức nào để truy cập an toàn vào máy tính từ xa

1. Secure Shell (SSH)
2. Secure Sockets Layer (SSL)
3. Secure Hypertext Transport Protocol (SHTTP)
4. Transport Layer Security (TLS)

Câu 59: Phương thức nào trong số này được coi là giao thức truyền mật mã yếu nhất?

1. SSL v2.0
2. TLS v1.0
3. TLS v1.1
4. TLS v1.3

Câu 60: Chứng chỉ số lien kết

1. Khóa riêng tư của người dùng bằng khóa công cộng
2. Khóa riêng tư với chữ kí số
3. Khóa công khóa của người dùng bằng khóa riêng
4. Danh tính của người dùng bằng khóa công khai của anh ấy

Câu 61: Đảm bảo kết nối mật mã an toàn giữa trình duyệt web và máy chủ web, điều nào sau đây được sử dụng?

1. Web digital certifieate
2. Email web certifieate
3. Server digital certifieate
4. Personal digital certifieate

Câu 62: Một thực thể cấp chứng chỉ kỹ thuật số là.

1. Tổ chức phát hành chứng chỉ (Certificate Authority - CA)
2. Cơ quan Chữ ký (Signature Authority - SA)
3. Người ký chứng chỉ (Certificate Signatory - CS)
4. Bộ ký số (Digital Signer - DS)

Câu 63: Điều nào là các khóa đối xứng để mã hóa và giải mã thông tin được trao đổi trong phiên và để xác minh tính toàn vẹn của nó.

1. Session keys
2. Encrypted signatures
3. Digital digests
4. Digital certificates

Câu 64: Thuật toán chia Euclid mở rộng dùng để?

1. Tính nhanh một lũy thừa với số lớn
2. Tính phần tử nghịch đảo của một số theo module nào đó
3. Kiểm tra nhanh một số nguyên tố lớn
4. Tìm đồng dư của một só theo module nào đó

Câu 65: Một hệ thống mã hoá quy ước dùng khoá dài 128 bit. Nếu dùng phương pháp tấn công brute force thì phải thử trung bình bao nhiêu lần và thời gian cần thiết để thực hiện nếu tốc độ xử lý là một tỉ lần trong một giây?

1. Phải thử 2128 lần, thời gian thử là 5,4 \* 1018 năm.
2. Phải thử 264 lần, thời gian thử là 5,4 \* 1018 năm.
3. Phải thử 2127 lần, thời gian thử là 5,4 \* 1018 năm.
4. Phải thử 212 lần, thời gian thử là 18 năm.

Câu 66: Chữ ký điện tử (số) là :

1. Các đặc tính của mật mã, được sử dụng để biến đổi mã hóa thông tin
2. Họ tên người gửi được ghi ở dạng điện tử và kết nối với thông tin
3. Biến đổi mã hóa văn bản được gắn vào văn bản cho phép người nhận khác kiểm tra tác giả và tính đích thực của thông
4. Tất cả đều sai

Câu 67: RSA là giải thuật

1. Mã hóa công khai
2. Là tên của một tổ chức quốc tế về mã hóa
3. Mã hóa khóa bí mật
4. Tất cả đề sai

Câu 68: Cho bản rõ “center” khóa k = 5. Khi mã hóa bản rõ với khóa k theo hệ mã dịch chuyển ta sẽ thu được bản mã nào sau đây?

1. HGRGXV
2. GRXVCN
3. VCMHGR
4. XVHGGR

Câu 69: Cho bản rõ “moday” khóa k = 18. Khi mã hóa bản rõ với khóa k theo hệ mã dịch chuyển ta sẽ thu được bản mã nào sau đây?

1. DAEGU
2. EARDY
3. YAEDR
4. ADERU

Câu 70: Người A chọn các thông số (p, q, e) = (17, 3, 5). Khóa công khai của A là gì?

1. (51, 5)
2. (32, 5)
3. (17, 3)
4. (17, 3, 5)

Câu 71: Người A và người B dùng sơ đồ kí và sơ đồ mã hóa RSA, thực hiện theo quy trình mã trước kí sau. Người A có khóa (p,q,e) = (17,3,5); Người B có khóa (p,q,e) = (11,5,13). A mã bản tin m = 10 gửi cho B. Hỏi A sử dụng khóa nào để mã?

1. (5, 51)
2. (13, 55)
3. 52
4. 55

Câu 72: Người A và người B dùng sơ đồ kí và sơ đồ mã hóa RSA, thực hiện theo quy trình mã trước kí sau. Người A có khóa (p,q,e) = (17,3,5); Người B có khóa (p,q,e) = (11,5,13). B kí lên bức điện x =10 bằng khóa nào sau đây? => khóa riêng

1. 13
2. 5
3. 37
4. 23

Câu 73: Người A và người B dùng sơ đồ kí và sơ đồ mã hóa RSA, thực hiện theo quy trình mã trước kí sau. Người A có khóa (p,q,e) = (17,3,5); Người B có khóa (p,q,e) = (11,5,13). B mã hóa thông tin gửi cho A thì B sử dụng khóa nào?

1. (5, 51)
2. 37
3. (55, 13)
4. 55

Câu 74: DES là viết tắt của từ nào?

1. Data encryption system
2. Data encryption standard
3. Data encoding standard
4. Data encryption signature

Câu 75: lNhững gì được sử dụng để tạo ra một chữ ký điện tử?

1. Khóa riêng của người nhận
2. Khóa công khai của người gửi
3. Khóa riêng của người gửi
4. Khóa công khai của người nhận

Câu 76: Phương thức nào sau đây là tốt nhất mô tả một chữ ký điện tử?

1. Một phương thức chuyển giao một chữ ký viết tay vào một tài liệu điện tử
2. Một phương pháp mã hóa thông tin bí mật
3. Một phương pháp để cung cấp một chữ ký điện tử và mã hóa
4. Một phương pháp để cho những người nhận của tin nhắn chứng minh nguồn gốc và sự toàn vẹn của một tin nhắn

Câu 77: 8: cho bản mã “EC” khóa k là:

8 3

7 3

Khi giải mã bản mã với khóa k theo hệ mã hill ta sẽ thu được bản rõ nào sau đây? Biết hàm mã hóa y=kx

1. cw
2. oy
3. yn
4. om

Câu 78: 8: cho bản mã “SW” khóa k là:

7 2

3 3

Khi giải mã bản mã với khóa k theo hệ mã hill ta sẽ thu được bản rõ nào sau đây? Biết hàm mã hóa y=kx

1. ma
2. mu
3. mi
4. sy

Câu 79: Cho bản mã “ICVM” khóa k là “GO”. Khi giải mã bản mã với khóa k theo hệ mã Vigenere ta sẽ thu được bản rõ nào sau đây?

1. page
2. copy
3. pase
4. cont

Câu 80: Cho bản mã “PMGQ” khóa k là “AM”. Khi giải mã bản mã với khóa k theo hệ mã Vigenere ta sẽ thu được bản rõ nào sau đây?

1. sage
2. seft
3. stef
4. page

Câu 81: Chức năng của các hàm băm (hash function)?

1. Tạo ra một khối thông tin ngắn cố định từ một khối thông tin gốc lớn hơn.
2. Mật mã hoá thông tin.
3. Xác thực nguồn gốc thông tin
4. Ngăn chặn việc phủ nhận hành vi của chủ thể thông tin.

Câu 82: Cho bản rõ x = 20 khóa công khai n = 161, e = 35. Khi mã hóa bản rõ x với khóa trên theo hệ mã RSA ta sẽ thu được bản mã nào sau đây

1. 13
2. 16
3. 83
4. 186

Câu 83: Người A chọn các thông số p =17, q = 3, e = 5. Hỏi khóa riêng của A là gì?

1. (51, 5)
2. (36, 5)
3. (51, 13)
4. (17, 3)

Câu 84: Cho bản mã y = 36 khóa riêng là p = 7, q = 23, e = 13. Khi giải mã bản mã y với khóa trên theo hệ RSA ta sẽ thu được bản rõ nào sau đây ?

1. 9
2. 19
3. 29
4. 92

Câu 85: Cho bản rõ x = 22 khóa công khai n = 265, e = 11. Khi mã hóa bản rõ x với khóa trên theo hệ mã RSA ta sẽ thu được bản mã nào sau đây?

1. 22
2. 28
3. 138
4. 238

Câu 86: Trong giải thuật mã hóa DES thực hiện bao nhiêu vòng lắp

1. 6
2. 8
3. 15
4. 16

Câu 87: Cho bản mã “RXVA” khóa k là “KP”. Khi giải mã bản mã với khóa k theo hệ mã Vigenere ta sẽ thu được bản rõ nào sau đây?

1. bill
2. sice
3. vief
4. hill

Câu 88: Điều nào sau đây KHÔNG phải là activity phase control?

1. Compensating control
2. Detective control
3. Resource control
4. Deterrrnt control

Câu 89: Điều nào sau đây không phải là phương pháp phát hiện chuyển động ?

1. Tần số vô tuyến
2. Độ ẩm
3. Từ tính
4. Hồng ngoại

Câu 90: Điều nào có thể được sử dụng để bảo mật thiết bị di động

1. Mobile connector
2. Cable lock
3. Mobile chain
4. Security tab

Câu 91:Bước đầu tiên trong việc bảo mật hệ điều hành là gì?

1. Phát triển chính sách bảo mật
2. Phát triển quản lý bản vá
3. Cấu hình cài đặt và bảo mật của hệ điều hành
4. Thực hiện baselining phần mềm máy chủ

Câu 92: Điều nào sau đây KHÔNG phải là cài đặt Microsoft Windows có thể được định cấu hình thông qua mẫu bảo mật?

1. Chính sách tài khoản
2. Quyền của người sử dụng
3. Ánh xạ bàn phím (Keyboard Mapping)
4. Dịch vụ hệ thống

Câu 93: Điều nào sau đây cho phép thiết lập 1 cấu hình duy nhất và sau đó triển áp dụng cho nhiều hoặc tất cả người dùng

1. Thư mục hoạt động (Actice Directory)
2. Chính sách nhóm (Group Policy)
3. Sao chép theo dõi (Snap-In Replication\_SIR)
4. Cấu hình lệch (Command Configuration)

Câu 94:Tuyên bố nào về phòng ngừa mất dữ liệu (data loss prevention-DLP) KHÔNG đúng?

1. Nó chỉ có thể bảo vệ dữ liệu trong khi nó nằm trên máy tính cá nhân của người dùng
2. Nó có thể quét dữ liệu trên đĩa DVD
3. Nó có thể đọc bên trong các tập tin nén
4. Vi phạm chính sách có thể tạo báo cáo hoặc chặn dữ liệu

Câu 95:Một typical Configuration baseline sẽ bao gồm mỗi phần sau NGOẠI TRỪ?

1. Thay đổi bất kì cài đặt mặc định nào không an toàn
2. Loại bỏ mọi phần mềm không cần thiết
3. Cho phép các tính năng bảo mật của hệ điều hành
4. Thực hiện đánh giá rủi ro an ninh

Câu 96: Cái nào sau đây là danh sách của người gửi email được chấp nhận

1. Blacklist
2. Whitelist
3. Greylist
4. greenlist

Câu 97: FTP sử dụng cổng gì?

1. 21
2. 25
3. 23
4. 80

Câu 98: Cổng nào được HTTPS sử dụng?

1. 53
2. 80
3. 443
4. 21

Câu 99: Giao thức SSL dùng để

1. Cung cấp bảo mật cho dữ liệu lưu thông trên dịch vụ HTTP
2. Cung cấp bảo mật cho thư viện điện tử
3. Cung cấp bảo mật cho web
4. Cung cấp bảo mật cho xác thực người dùng vào các hệ thống vận hành trên Flatform Window

Câu 100: Các lỗ hổng bảo mật trên hệ thống là do

1. Dịch vụ cung cấp
2. Bản than hệ điều hành
3. Con người tạo ra
4. Dịch vụ cung cấp, Bản than hệ điều hành, Con người tạo ra

Câu 101: Công cụ/ cơ chế bảo mật cho mạng không dây là

1. SSL
2. TSL
3. Giao thức PGP
4. WEP

Câu 102:Thiết bị nào cho phép ta kết nối đến 1 mạng LAN của công ty qua Internet thông qua 1 kênh được mã hóa an toàn

1. VPN
2. WEP
3. Modem
4. telnet

Câu 103: Tính năng bảo mật nào KHÔNG cung cấp tính năng cân bằng tải?

1. Ấn các trang HTTP lỗi
2. Xóa tiêu đề định dạng máy chủ khôi phục HTTP responses
3. Lọc các gói dựa trên cai đặt giao thức
4. Tấn công từ chối dịch vụ (DoS)

Câu 104: Chức năng nào mà bộ lọc nội dung Internet KHÔNG thực hiện?

1. Lọc URL
2. Kiểm tra phần mềm độc hại
3. Kiểm tra nội dung
4. Phát hiện xâm nhập

Câu 105: Làm thế nào để network address translation (NAT) cải thiện bảo mật?

1. Nó loại bỏ các gói không mong muốn
2. Nó lọc dựa trên giao thức
3. Nó che dấu địa chỉ IP của thiết bị NAT
4. NAT không cải thiện an ninh

Câu 106: Làm sao để 1 mạng LAN ảo (VLAN) cho phếp các thiết bị được nhóm lại?

1. Dựa trên mạng con
2. Hợp lý
3. Trực tiếp đến trung tâm
4. Chỉ xung quanh công tác lỗi

Câu 107: Thiết bị nào dễ dàng nhất để kẻ tấn công tận dụng lợi thế nắm bắt và phân tích các gói tin?

1. Hub
2. Switch
3. Router
4. Load balancer

Câu 108: Điều nào trong số này KHÔNG phải là 1 cuộc tấn công lại 1 công tắc

1. Mạo danh địa chỉ MAC
2. ARP poisoning
3. MAC flooding
4. Mạo danh địa chỉ ARP

Câu 109: Câu nào về network address translation (NAT) là đúng?

1. Nó có thể là trạng thái trạng thái hoặc không trạng thái
2. Nó thay đổi địa chỉ MAC cho địa chỉ IP
3. Nó loại bỏ các địa chỉ riêng khi gói rời khỏi trang
4. Nó chỉ có thể được tìm thấy trên các bộ định tuyến lỗi

Câu 110: Proxy ngược

1. Chỉ xử lý các yêu cầu được gửi đi
2. Giống như 1 máy chủ Proxy
3. Phải được sử dụng với tường lửa
4. Định tuyến các yêu cầu đến máy chủ chính xác

Câu 111: Vị trí thích hợp nhất để cài đặt bộ lọc spam là gì?

1. Trên máy chủ POP3
2. Với máy chủ SMTP
3. Trên máy khách lưu trữ cục bộ
4. Trên máy chủ Proxy

Câu 112: Một tường lửa được sử dụng làm loại tường lửa bảo mật nhất là:

1. Lọc trạng thái gói
2. Hệ thống phát triển xâm nhập mạng phát lại
3. Lọc gói không trạng thái
4. Phân tích Proxy ngược

Câu 113: Loại nhật kí thiết bị nào chứa dữ liệu bảo mật có lợi nhất?

1. Nhật kí email
2. Nhật kí chuyển đổi
3. Nhật tường lửa
4. Nhật kí bộ định tuyến

Câu 114: Loại nhật kí nào có thể cung cấp chi tiết về các yêu cầu đối với các tệp cụ thể trên hệ thống

1. Event log
2. Access log
3. Audit log
4. SysFile log

Câu 115: Tấn công hệ thống tên miền (Domain Name System-DNS) nào thay thế 1 địa chỉ IP gian lận cho tên 1 biểu tượng

1. DNS replay
2. DNS masking
3. DNS poisoning
4. DNS for warding

Câu 116: Giao thức nào an toàn nhất để chuyển tệp?

1. SCP
2. SFTP
3. FTPS
4. FTP

Câu 117: Nếu 1 nhóm người dùng phải được tách ra khỏi những người dùng khác, thiết kế mạng nào bảo mật nhất?

1. Sử dụng VLAN
2. Kết nối chúng với các thiết bị switch và router khác
3. Sử dụng mặt nạ mạng con
4. Không thể tách người dùng trên mạng

Câu 118: Trong 1 mạng bằng cách sử dụng IEEE 802.1x, 1 supplicant

1. Phải sử dụng IEEE 802.11d để kết nối với mạng
2. Đưa ra yêu cầu cho người xác thực
3. Liên hệ trực tiếp với máy chủ xác thực
4. Chỉ có thể là 1 thiết bị không dây

Câu 119: Điều nào sau đây KHÔNG phải là mối quan tâm về bảo mật của môi trường ảo hóa?

1. Các máy ảo phải được bảo vệ khỏi cả thế giới bên ngoài và cũng từ các máy ảo khác trên cùng 1 máy tính vật lý
2. Các thiết bị bảo mật vật lý không phải lúc nào cũng được thiết kế để bảo vệ các hệ thống ảo
3. Các máy tính chủ ảo rẻ hơn các máy chủ vật lý của chúng
4. Di chuyển trực tiếp có thể di chuyển ngay lập tức 1 máy chủ ảo hóa sang 1 trình siêu giám sát khác

Câu 120: Cái nào có thể được sử dụng để ẩn thông tin về mạng nội bộ ngoại trừ

1. Protocol analyzer
2. Subnetting
3. Proxy server
4. Network address translation (NAT)