**CÂU HỎI NHẬP MÔN AN TOÀN BẢO MẬT THÔNG TIN**

**[(<8203319-C3>)] Nhập môn an toàn và bảo mật thông tin, , Chương 1**

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

+Là đặc tính của hệ thống trong đó thông tin được giữ bí mật không cho ai truy xuất.

+Là đặc tính của hệ thống trong đó tất cả thông tin được lưu trữ dưới dạng mật mã

+Là đặc tính của hệ thống trong đó chỉ có những người dùng được cho phép mới có thể truy xuất được thông tin

+Tất cả đều đúng

1. : Các cơ chế đảm bảo tính toàn vẹn của thông tin

+Gồm các cơ chế ngăn chặn và cơ chế phát hiện các vi phạm về toàn vẹn thông tin

+Mật mã hoá toàn bộ thông tin trong hệ thống

+Lưu toàn bộ thông tin trong hệ thống dưới dạng nén.

+Tất cả các cơ chế trên

1. : Các nguy cơ nào sau đây có thể ảnh hưởng đến tính khả dụng của hệ thống thông tin

+Thiết bị không an toàn.

+Các tấn công từ chối dịch vụ (DoS và DDoS).

+Virus và các loại phần mềm phá hoại khác trên máy tính.

+Tất cả các nguy cơ trên.

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

+Một người dùng có thể xem thông tin của các người dùng khác.

+Virus xóa mất các tập tin trên đĩa cứng.

+Mất điện thường xuyên làm hệ thống máy tính làm việc gián đọan.

+Tất cả các hành vi trên.

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

+Một người dùng có thể xem thông tin của các người dùng khác.

+Virus xóa mất các tập tin trên đĩa cứng.

+Mất điện thường xuyên làm hệ thống máy tính làm việc gián đọan.

+Tất cả các hành vi trên

1. : Để tìm bản rõ người thám mã sử dụng

+Kết hợp nhiều phương pháp tấn công khác nhau

+Chỉ sử dụng phương pháp giải bài toán ngược

+Sử dụng khóa bí mật

+Vét cạn khóa

1. : Chức năng chính của Virus là

+Lây nhiễm và sinh sản

+Sống ký sinh và lây nhiễm

+Tự phát triển độc lập và lây nhiễm

+Sống ký sinh và sinh sản

1. : Để đảm bảo an toàn thông tin, bằng cách

+Sử dụng phương pháp mã hóa

+Sử dụng tường lửa

+Phân quyền truy cập thông tin

+Kết hợp các biện pháp trên

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

+Tốc độ như nhau

+Mật mã công khai nhanh hơn

+Mật mã công khai chậm hơn

+Không so sánh được

1. : Giải mã là

+Quá trình tấn công hệ mật mã để tìm bản rõ và khóa bí mật

+Quá trình biến đổi thông tin từ dạng đọc được sang dạng không đọc được

+Quá trình biến đổi thông tin từ dạng không đọc được sang dạng đọc được.

+Giấu thông tin để không nhìn thấy

1. : Thám mã là

+Quá trình tấn công hệ mật mã để tìm bản rõ và khóa bí mật

+Quá trình biến đổi thông tin từ dạng đọc được sang dạng không đọc được

+Quá trình biến đổi thông tin từ dạng không đọc được sang dạng đọc được.

+Giấu thông tin để không nhìn thấy

1. : Mã hóa là

+Quá trình tấn công hệ mật mã để tìm bản rõ và khóa bí mật

+Quá trình biến đổi thông tin từ dạng đọc được sang dạng không đọc được

+Quá trình biến đổi thông tin từ dạng không đọc được sang dạng đọc được.

+Giấu thông tin để không nhìn thấy

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

+Một sinh viên sao chép bài tập của một sinh viên khác.

+Virus xóa mất các tập tin trên đĩa cứng.

+Mất điện thường xuyên làm hệ thống máy tính làm việc gián đọan.

+Tất cả các hành vi trên.

1. : Thế nào là tính khả dụng của hệ thống thông tin?

+Là tính sẵn sàng của thông tin trong hệ thống cho mọi nhu cầu truy xuất.

+Là tính sẵn sàng của thông tin trong hệ thống cho các nhu cầu truy xuất hợp lệ.

+Là tính dễ sử dụng của thông tin trong hệ thống.

+Tất cả đều sai.

1. : Chọn sai khi nói về các nguy cơ đối với sự an toàn của hệ thống thông tin:

+Những kẻ tấn công hệ thống (attacker) có thể là con người bên trong hệ thống.

+Người sử dụng không được huấn luyện về an toàn hệ thống cũng là một nguy cơ đối với hệ thống.

+Một hệ thống không kết nối vào mạng Internet thì không có các nguy cơ tấn công.

+Xâm nhập hệ thống (intrusion) có thể là hành vi xuất phát từ bên ngoài hoặc từ bên trong hệ thống.

16: Trojan là một phương thức tấn công kiểu

+Can thiệp trực tiếp vào máy nạn nhân để lấy các thông tin quan trọng

+Đánh cắp dữ liệu của nạn nhân truyền trên mạng

+Tấn công làm tê liệt hệ thống mạng của nạn nhân

+Điều khiển máy tính nạn nhân từ xa thông qua phần mềm cài sẵn trong máy nạn nhân

1. : 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 là do:

+Do không kết nối được tới máy nạn nhân.

+Do không cài đặt công cụ Metasploit vào ổ C:

+Do máy nạn nhân không cho phép tấn công.

+Do Phần mềm Anti Virus trên máy tấn công đã khóa (blocked) không cho thi hành.

1. : Virus máy tính không thể lây lan qua

+Mạng máy tính

+Đĩa CD

+Thẻ nhớ Flash

+Lưu trữ USB

1. : Phòng chống tấn công Tấn công từ chối dịch vụ phân bố (DDOS)

+Chỉ có thể dùng tường lửa

+Có thể hạn chế trong bằng cách lập trình

+Hiện nay đã có cách phòng chống hiệu quả

+Cách hiệu quả duy nhất là lưu trữ và phục hồi (backup và restore)

1. : SQL Injection là gì?

+Một ngôn ngữ lập trình đa năng

+Một loại khai thác bảo mật trong đó kẻ tấn công thêm mã Ngôn ngữ truy vấn mang tính cấu trúc (SQL) vào hộp nhập biểu mẫu của trang Web để truy cập vào tài nguyên hoặc thực hiện thay đổi dữ liệu.

+Một ngôn ngữ được ghi lại dựa trên nguyên mẫu, sử dụng chủ yếu dưới dạng javascript ở phía máy khách, được triển khai như một phần của trình duyệt Web để cung cấp các giao diện người dùng và trang web động nâng cao.

+Một chương trình đố vui của Mỹ về nhiều lĩnh vực: lịch sử, văn học, nghệ thuật, văn hóa đại chúng, khoa học, thể thao, địa lý, từ ngữ, và nhiều hơn nữa.

1. : Có thể ngăn chặn SQL Injection bằng cách nào?

+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 được cho phép).

+Không sử dụng SQL nữa

+Đặt mã của bạn ở chế độ công khai.

+Tất cả những cách trên.

1. : Cross-site scripting là gì?

+Một ngôn ngữ lập trình cho phép kiểm soát một hoặc nhiều ứng dụng.

+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.

+Một loại ngôn ngữ script chuyên dùng để điều khiển máy tính.

+Tài liệu hoặc tài nguyên thông tin phù hợp với World Wide Web và có thể được truy cập thông qua trình duyệt web và hiển thị trên màn hình hoặc thiết bị di động.

1. : Social Engineering là gì?

+Kĩ thuật sai khiến mọi người thực hiện hành vi nào đó hoặc tiết lộ thông tin bí mật.

+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 trình như đường giao thông, cầu, kênh đào, đập và các tòa nhà.

+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.

+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.

1. : Rootkit là gì?

+Một bộ kit được các nhà sinh học sử dụng khi làm việc với các loại thực vật.

+Tên mặc định của thư mục UNIX.

+Rootkit là được thiết kế để qua mặt các phương pháp bảo mật máy tính.

+Một máy chủ định danh cho vùng root của Domain Name System.

1. : Kiến trúc TCP / IP sử dụng bao nhiêu lớp?

+Bảy

+Sáu

+Năm

+Bốn

1. : Điều nào trong số này không phải là tấn công tiêu đề HTTP?

+Accept-Language

+Referer

+Response splitting

+Content-length

1. : Ngôn ngữ đánh dấu nào được thiết kế để mang dữ liệu?

+ICMP

+HTTP

+HTML

+XML

1. : Kiểu tấn công nào liên quan đến kẻ tấn công truy cập các tệp trong các thư mục khác với thư mục gốc?

+SQL injection

+Command injection

+XML injection

+directory traversal

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

+XML manipulation

+HTML packet

+SQL injection

+HTTP header

1. : Điều nào trong số này KHÔNG phải là tấn công dos?

+SYN flood

+Ping flood

+Smurf

+push flood

**[(<8203319-C3>)] Nhập môn an toàn và bảo mật thông tin, , Chương 2**

1. : Cơ sở của một cuộc tấn công SQL injection là gì?

+Để máy chủ SQL tấn công trình duyệt web máy khách

+để chèn lệnh SQL thông qua đầu vào người dùng chưa được lọc

+Để hiển thị mã SQL để nó có thể được kiểm tra

+Để liên kết các máy chủ SQL thành một botnet

1. : Hành động nào không thể thực hiện được thông qua tấn công SQL injection thành công?

+định dạng lại ổ cứng của máy chủ ứng dụng web

+Hiển thị danh sách số điện thoại của khách hàng

+Khám phá tên của các trường khác nhau trong bảng

+Xóa bảng cơ sở dữ liệu

1. : Tấn công phát lại

+Được coi là một loại tấn công dos

+Tạo bản sao truyền để sử dụng sau này

+Có thể được ngăn chặn bằng cách vá trình duyệt web

+Replay các cuộc tấn công hơn và hơn để lũ máy chủ

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

+Flash cookie

+Session cookie

+Ram cookie

+Secure cookie

1. : Plug-in trình duyệt.

+Chỉ hoạt động trên máy chủ web

+Có thể được nhúng bên trong trang web nhưng không thể thêm tiện ích

+Có chức năng bổ sung cho toàn bộ trình duyệt

+Đã được thay thế bằng tiện ích mở rộng của trình duyệt

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

+Buffer overflow

+Real number

+Heap size

+Integer overflow

1. : Kẻ tấn công sử dụng tràn bộ đệm để làm gì?

+Xóa tập tin chữ ký tràn bộ đệm

+Làm hỏng nhân để máy tính không thể khởi động lại

+Trỏ đến một khu vực khác trong bộ nhớ dữ liệu chứa mã phần mềm độc hại của kẻ tấn công

+Đặt virus vào nhân (kernel)

1. : Điều gì là duy nhất về tấn công cross-site scripting (XSS) so với các cuộc tấn công injection khác? +Mã SQL được sử dụng trong một cuộc tấn công XSS.

+XSS yêu cầu sử dụng trình duyệt.

+XSS không tấn công máy chủ ứng dụng web để ăn cắp hoặc làm hỏng thông tin của nó.

+Tấn công XSS hiếm khi được sử dụng nữa so với các cuộc tấn công injection khác.

1. : Cookie không được tạo bởi trang web đang được xem là gì?

+cookie chính chủ

+cookie của bên thứ hai

+cookie của bên thứ ba

+cookie của bên thứ tư

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

+privilege rights

+heap spray

+transitive

+vertical escalation

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

+Mặc dù các thiết bị bảo mật mạng truyền thống có thể chặn các cuộc tấn công mạng truyền thống, chúng không thể luôn chặn các cuộc tấn công ứng dụng web.

+Các bộ vi xử lý trên máy khách nhỏ hơn trên các máy chủ web và do đó chúng dễ bảo vệ hơn.

+Nhiều cuộc tấn công ứng dụng web khai thác lỗ hổng chưa biết trước đó.

+Bằng cách thiết kế các ứng dụng web phía máy chủ động, chấp nhận đầu vào của người dùng có thể chứa mã độc.

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

+Các thiết bị bảo mật mạng truyền thống bỏ qua nội dung lưu lượng HTTP, là phương tiện tấn công ứng dụng web.

+Các cuộc tấn công ứng dụng web sử dụng các trình duyệt web không thể được điều khiển trên máy tính cục bộ.

+Các thiết bị bảo mật mạng không thể ngăn chặn các cuộc tấn công từ tài nguyên web.

+Tính chất phức tạp của TCP / IP cho phép quá nhiều lần ping bị chặn.

1. : Trojan Horse là gì?

+Một chương trình độc hại mà lấy cắp tên người dùng và mật khẩu của bạn

+Gây hại như mã giả mạo hoặc thay thế mã hợp pháp

+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

+Một máy chủ đó là phải hy sinh cho tất cả các hacking nỗ lực để đăng nhập và giám sát các hoạt động hacking

1. : Khi một hacker cố gắng tấn công một máy chủ qua Internet nó được gọi là loại tấn công?

+Tấn công từ xa

+Tấn công truy cập vật lý

+Truy cập địa phương

+Tấn công nội bộ

1. : Kỹ thuật tấn công phổ biến trên Web là

+Chiếm hữu phiên làm việc.

+Tràn bộ đệm.

+Từ chối dịch vụ (DoS)

+Chèn truy vấn SQL

**[(<8203319-C3>)] Nhập môn an toàn và bảo mật thông tin, , Chương 3**

1. : nào đúng về Hashed Message Authentication Code (HMAC)

+Chỉ mã hóa khóa

+Mã hóa khóa và thông báo

+Chỉ mã hóa tin nhắn

+Chỉ mã hóa khóa DHE

1. : Phiên bản mới nhất của thuật toán băm bảo mật là gì?

+SHA-2

+SHA-3

+SHA-4

+SHA-5

1. : Hệ thống khóa công khai tạo ra các khóa công cộng ngẫu nhiên khác nhau cho mỗi phiên được gọi là +Trao đổi khóa công khai (PKE)

+Elliptic Curve Diffie-Hellman (ECDH)

+Diffie-Hellman (DH)

+Perfect forward secrecy (PFS)

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

+Tính từ bỏ(repudiation)

+Tính toàn vẹn (integrity)

+Tính không từ chối(non-repudiation)

+Tính khả dụng (availability)

1. : 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

+Khoá bí mật của Alice

+Khoá công khai của Alice

+Khoá bí mật của Bob

+Khoá công khai của Bob

1. : Thuật toán mã hóa bất đối xứng nào sử dụng số nguyên tố?

+EFS

+quantum computing

+ECC

+RSA

1. : Thuật toán mã hóa bất đối xứng nào an toàn nhất?

+SHA-2

+BTC-2

+RSA

+ME-14

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

+chứng minh tính toàn vẹn của thông điệp

+xác minh người nhận

+xác minh người gửi

+thực thi không từ chối

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

+Advanced Encryption Standard

+Data Encryption Standard

+Triple Data Encryption Standard

+Rivest Cipher (RC) 1

1. : Tiêu chuẩn mật mã khóa công khai (PKCS).

+Được chấp nhận rộng rãi trong ngành

+Chỉ được sử dụng để tạo khóa công khai

+Xác định các thuật toán băm được tạo ra như thế nào

+Đã được thay thế bởi PKI

1. : Điều nào trong số này KHÔNG phải là nơi khóa có thể được lưu trữ?

+Trong tokens

+Trong digests

+Trên hệ thống của người dùng cục bộ

+Nhúng trong chứng chỉ kỹ thuật số

1. : Cơ sở hạ tầng khóa công khai (PKI).

+T ạo mật mã khóa riêng

+Là quản lý chứng chỉ kỹ thuật số

+Yêu cầu sử dụng RA thay vì CA

+Tự động tạo khóa công khai / riêng tư

1. : Giao thức nào để truy cập an toàn vào máy tính từ xa.

+Secure Shell (SSH)

+Secure Sockets Layer (SSL)

+Secure Hypertext Transport Protocol (SHTTP)

+Transport Layer Security (TLS)

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

+SSL v2.0

+TLS v1.0

+TLS v1.1

+TLS v1.3

1. : Chứng chỉ số liên kết

+Khóa riêng tư của người dùng bằng khóa công cộng

+Một khóa riêng với chữ ký số

+Khóa công khai của người dùng bằng khóa riêng

+Danh tính của người dùng bằng khóa công khai của anh ấy

1. : Để đảm bảo kết nối mật mã an toàn giữa trình duyệt web và máy chủ web, điều nào sẽ được sử dụng.

+Web digital certificate

+Email web certificate

+Server digital certificate

+Personal digital certificate

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

+Tổ chức phát hành chứng chỉ (Certificate Authority - CA)

+Cơ quan Chữ ký (Signature Authority - SA)

+Người ký chứng chỉ (Certificate Signatory - CS)

+Bộ ký số (Digital Signer - DS)

1. : 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.

+Session keys

+Encrypted signatures

+Digital digests

+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. Tính đồng dư của một sô theo module nào đó

Câu 65: Một hệ thống mã hóa quy ước dùng khóa dài 128Bit. Nếu dùng phương pháp tấn công Brute force thì phải thử

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 2128 lần, thời gian thử là 18 năm.

Câu 66: Chứ 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 dùng được được ghi ở dạng điện tử với kết nối 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 tin.
4. Tất cả đều sai

Câu 67: RSA là giải thuật

1. Mã hóa công khai
2. Là tên của tổ chức quốc tế về mã hóa
3. Mã háo khóa bí mật
4. Tất cả đều 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:

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:

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

Câu 70: Người A chọn các thông số p=17,p=3, e=5. Hỏi 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 háo RSA, thực hiện theo quy trình mã trước kí sau, Người A có

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 háo RSA, thực hiện theo quy trình mã trước kí sau, Người A có

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

Câu 73: Người A và người B dùng sơ đồ kí và sơ đồ mã háo RSA, thực hiện theo quy trình mã trước kí sau, Người A có

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 encrytion signature

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

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

Câu 76: Phương thức nào sau đây là tốt nhất để mô tả 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 tự 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: Cho bản mã “EC” khóa k là:

8 3

7 3

Khi giả 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. Cm

Câu 78: Cho bản mã “SW” khóa k là:

7 2

3 3

Khi giả 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?

1. Pase
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?

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 lớn hơn
2. Mật mã hóa 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=15. Khi mã hóa bản rõ x với khóa trên theo hệ mã RSA sẽ thu:

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

Câu 83: Người A chọn các thông số p=17,q=3, e=5. Hổi 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:

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:

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

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

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

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

1. Bill
2. Sice
3. Viet
4. Hill

**[(<8203319-C3>)] Nhập môn an toàn và bảo mật thông tin, , Chương 4**

**Câu 88 [<DE>]:** Điều nào sau đây KHÔNG phải là activity phase control?

[<$>] Compensating control

[<$>] Detective control

[<$>] Resource control

[<$>] Deterrent control

**Câu 89 [<TB>]:** Điều nào sau đây KHÔNG phải là phương pháp phát hiện chuyển động?

[<$>] Tần số vô tuyến

[<$>] Độ ẩm

[<$>] Từ tính

[<$>] Hồng ngoại

**Câu 90 [<TB>]:** Điều nào có thể được sử dụng để bảo mật thiết bị di động.

[<$>] Mobile connector

[<$>] cable lock òa nh

[<$>] Mobile chain

[<$>] Security tab

**Câu 91 [<DE>]:** Bước đầu tiên trong việc bảo mật hệ điều hành là gì?

[<$>] Phát triển chính sách bảo mật.

[<$>] Triển khai quản lý bản vá.

[<$>] Cấu hình cài đặt và bảo mật của hệ điều hành.

[<$>] Thực hiện baselining phần mềm máy chủ.

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

[<$>] Chính sách tài khoản

[<$>] Quyền của người sử dụng

[<$>] Ánh xạ bàn phím(Keyboard Mapping)

[<$>] Dịch vụ hệ thống

**Câu 93 [<DE>]:** Điều nào cho phép thiết lập một cấu hình duy nhất và sau đó triển khai áp dụng cho nhiều hoặc tất cả người dùng.

[<$>] Thư mục hoạt động(Active Directory)

[<$>] Chính sách nhóm(Group Policy)

[<$>] Sao chép theo dõi (Snap-In Replication - SIR)

[<$>] Cấu hình lệnh(Command Configuration)

**Câu 94 [<DE>]:** Tuyên bố nào về phòng ngừa mất dữ liệu (data loss prevention - DLP) KHÔNG đúng?

[<$>] Nó chỉ có thể bảo vệ dữ liệu trong khi nó nằm trên máy tính cá nhân của người dùng.

[<$>] Nó có thể quét dữ liệu trên đĩa DVD.

[<$>] Nó có thể đọc bên trong các tập tin nén.

[<$>] Vi phạm chính sách có thể tạo báo cáo hoặc chặn dữ liệu.

**Câu 95 [<DE>]:** Một typical configuration baseline sẽ bao gồm mỗi phần sau NGOẠI TRỪ .

[<$>] Thay đổi bất kỳ cài đặt mặc định nào không an toàn

[<$>] Loại bỏ mọi phần mềm không cần thiết

[<$>] Cho phép các tính năng bảo mật của hệ điều hành

[<$>] Thực hiện đánh giá rủi ro an ninh

**Câu 96[<TB>]:** Cái nào sau đây là danh sách của người gửi email được chấp thuận?

[<$>] Blacklist

[<$>] whitelist

[<$>] Greylist

[<$>] Greenlist

**[(<8203319-C3>)] Nhập môn an toàn và bảo mật thông tin, , Chương 5**

**Câu 97 [<DE>]:** FTP sử dụng cổng gì ?

[<$>] 21

[<$>] 25

[<$>] 23

[<$>] 80

**Câu 98 [<DE>]:** Cổng nào được HTTPS sử dụng?

[<$>] 53

[<$>] 80

[<$>] 443

[<$>] 21

**Câu 99 [<DE>]:** Giao thức SSL dùng để

[<$>] Cung cấp bảo mật cho dữ liệu lưu thông trên dịch vụ HTTP

[<$>] Cung cấp bảo mật cho thư điện tử

[<$>] Cung cấp bảo mật cho Web

[<$>] Cung cấp bảo mật cho xác thực người dùng vào các hệ thống vận hành trên Flatform Window

**Câu 100[<DE>]:** Các lỗ hổng bảo mật trên hệ thống là do

[<$>] Dịch vụ cung cấp

[<$>] Bản thân hệ điều hành

[<$>] Con người tạo ra

[<$>] Dịch vụ cung cấp, bản thân hệ điều hành và con người tạo ra

**Câu 101[<DE>]:** Công cụ/cơ chế bảo mật cho mạng không dây là

[<$>] SSL

[<$>] TSL

[<$>] Giao thức PGP

[<$>] WEP

**Câu 102 [<DE>]:** Thiết bị nào cho phép ta kết nối đến một mạng LAN của công ty qua Internet thông qua một kênh

được mã hóa an toàn ?

[<$>] VPN

[<$>] WEP

[<$>] Modem

[<$>] Telnet

**Câu 103 [<TB>]:** Tính năng bảo mật nào KHÔNG cung cấp tính năng cân bằng tải?

[<$>] Ẩn các trang HTTP lỗi

[<$>] Xóa tiêu đề định danh máy chủ khỏi HTTP responses

[<$>] Lọc các gói dựa trên cài đặt giao thức

[<$>] Tấn công từ chối dịch vụ (dos)

**Câu 104 [<TB>]:** Chức năng nào mà bộ lọc nội dung Internet KHÔNG thực hiện?

[<$>] Lọc URL

[<$>] Kiểm tra phần mềm độc hại

[<$>] Kiểm tra nội dung

[<$>] Phát hiện xâm nhập

**Câu 105 [<TB>]:** Làm thế nào để network address translation (NAT) cải thiện bảo mật?

[<$>] Nó loại bỏ các gói không mong muốn.

[<$>] Nó lọc dựa trên giao thức.

[<$>] Nó che dấu địa chỉ IP của thiết bị NAT.

[<$>] NAT không cải thiện an ninh

**Câu 106 [<TB>]:** Làm thế nào để một mạng LAN ảo (VLAN) cho phép các thiết bị được nhóm lại?

[<$>] Dựa trên mạng con

[<$>] Hợp lý

[<$>] Trực tiếp đến trung tâm

[<$>] Chỉ xung quanh công tắc lõi

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

[<$>] Hub

[<$>] Switch

[<$>] Router

[<$>] Load balancer

**Câu 108 [<TB>]:** Điều nào trong số này KHÔNG phải là một cuộc tấn công chống lại một công tắc?

[<$>] Mạo danh địa chỉ MAC

[<$>] ARP poisoning

[<$>] MAC flooding

[<$>] Mạo danh địa chỉ ARP

**Câu 109 [<DE>]:** Câu nào về network address translation (NAT) là đúng?

[<$>] Nó có thể là trạng thái trạng thái hoặc không trạng thái.

[<$>] Nó thay thế địa chỉ MAC cho địa chỉ IP.

[<$>] Nó loại bỏ các địa chỉ riêng khi gói rời khỏi mạng.

[<$>] Nó chỉ có thể được tìm thấy trên các bộ định tuyến lõi

**Câu 110 [<DE>]:** Proxy ngược.

[<$>] Chỉ xử lý các yêu cầu gửi đi

[<$>] Giống như một máy chủ proxy

[<$>] Phải được sử dụng cùng với tường lửa

[<$>] Định tuyến các yêu cầu đến máy chủ chính xác

**Câu 111 [<TB>]:** Vị trí thích hợp nhất để cài đặt bộ lọc spam là gì?

[<$>] Trên máy chủ POP3

[<$>] Với máy chủ SMTP

[<$>] Trên máy khách lưu trữ cục bộ

[<$>] Trên máy chủ proxy

**Câu 112 [<TB>]:** Một tường lửa được sử dụng làm loại tường lửa bảo mật nhất là

[<$>] Lọc trạng thái gói

[<$>] Hệ thống phát hiện xâm nhập mạng phát lại

[<$>] Lọc gói không trạng thái

[<$>] Phân tích proxy ngược

**Câu 113 [<DE>]:** Loại nhật ký thiết bị nào chứa dữ liệu bảo mật có lợi nhất?

[<$>] Nhật ký email

[<$>] Nhật ký chuyển đổi

[<$>] Nhật tường lửa

[<$>] Nhật ký bộ định tuyến

**Câu 114 [<DE>]:** Loại nhật ký nào có thể cung cấp chi tiết về các yêu cầu đối với các tệp cụ thể trên hệ thống

[<$>] Event log

[<$>] Access log

[<$>] Audit log

[<$>] SysFile log

**Câu 115 [<TB>]:** Tấn công hệ thống tên miền (Domain Name System - DNS) nào thay thế một địa chỉ IP gian lận cho tên một biểu tượng

[<$>] DNS replay

[<$>] DNS masking

[<$>] DNS poisoning

[<$>] DNS forwarding

**Câu 116 [<DE>]:** Giao thức nào an toàn nhất để chuyển tệp?

[<$>] SCP

[<$>] SFTP

[<$>] FTPS

[<$>] FTP

**Câu 117 [<KH>]:** Nếu một nhóm người dùng phải được tách ra khỏi những người dùng khác, thiết kế mạng nào bảo mật nhất?

[<$>] Sử dụng VLAN.

[<$>] Kết nối chúng với các thiết bị switch và router khác.

[<$>] Sử dụng mặt nạ mạng con.

[<$>] Không thể tách người dùng trên mạng.

**Câu 118 [<DE>]:** Trong một mạng bằng cách sử dụng IEEE 802.1x, một supplicant.

[<$>] phải sử dụng IEEE 802.11d để kết nối với mạng

[<$>] đưa ra yêu cầu cho người xác thực

[<$>] liên hệ trực tiếp với máy chủ xác thực

[<$>] chỉ có thể là một thiết bị không dây

**Câu 119 [<KH>]:** Điều nào sau đây KHÔNG phải là mối quan tâm về bảo mật của môi trường ảo hóa?

[<$>] Các máy ảo phải được bảo vệ khỏi cả thế giới bên ngoài và cũng từ các máy ảo khác trên cùng một máy tính vật lý.

[<$>] Các thiết bị bảo mật vật lý không phải lúc nào cũng được thiết kế để bảo vệ các hệ thống ảo.

[<$>] Các máy chủ ảo rẻ hơn các máy chủ vật lý của chúng.

[<$>] Di chuyển trực tiếp có thể di chuyển ngay lập tức một máy chủ ảo hóa sang một trình siêu giám sát khác.

**Câu 120 [<DE>]:** Cái nào có thể được sử dụng để ẩn thông tin về mạng nội bộ ngoại trừ

[<$>] Protocol analyzer

[<$>] Subnetting

[<$>] Proxy server

[<$>] Network address translation (NAT)