Chương 1

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

Tất cả các nguy cơ trên.
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.

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

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

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

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 thông tin được giữ bí mật không cho ai truy xuất.
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

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

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

5. 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

6. Chức năng chính của Virus là

Sống ký sinh và lây nhiễm
Lây nhiễm và sinh sản
Tự phát triển độc lập và lây nhiễm
Sống ký sinh và sinh sản

7. Để đảm bảo an toàn thông tin, bằng cách

Kết hợp các biện pháp trên
Sử dụng phương pháp mã hóa
Sử dụng tường lửa
Phân quyền truy cập thông tin

8. 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 đoạn.
Tất cả các hành vi trên.

9. 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)?

Mật mã công khai chậm hơn
Tốc độ như nhau
Mật mã công khai nhanh hơn
Không so sánh được

10. Giải mã là

Quá trình biến đổi thông tin từ dạng không đọc được sang dạng đọc được.
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
Giấu thông tin để không nhìn thấy

11. 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

12. Mã hóa là

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

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

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

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

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

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

Một hệ thống không kết nối vào mạng Internet thì không có các nguy cơ tấn công.
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.
Xâm nhập hệ thống (intrusion) có thể là hành vi xuất phát từ bên ngoài hoặc từ bên trong

Chương 2

16. Trojan là một phương thức tấn công kiểu

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

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 là do:

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

18. Virus máy tính không thể lây lan qua

Đĩa CD
Mạng máy tính
Thẻ nhớ Flash
Lưu trữ USB

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

Có thể hạn chế trong bằng cách lập trình
Chỉ có thể dùng tường lửa
Hiện nay đã có cách phòng chống hiệu quả
Cách hiệu quả duy nhất là lưu trữ và phục hồi (backup và restore)

20. 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.

21. Rootkit là gì?

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

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

22. SQL Injection là gì?

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 lập trình đa năng
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.

23. 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.

24. Cross-site scripting là gì?

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

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

directory traversal
SQL injection
Command injection
XML injection

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

Bốn
Bảy
Sáu
Năm

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

Content-length
Accept-Language
Referer
Response splitting

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

XML
ICMP
HTTP
HTML

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

HTTP header
XML manipulation
HTML packet
SQL injection

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

push flood
SYN flood
Ping flood
Smurf

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

để chèn câu lệnh SQL thông qua đầu vào người dùng chưa được lọc
Để máy chủ SQL tấn công trình duyệt web máy khách
Để hiển thị mã SQL để nó có thể được kiểm tra
Để liên kết các máy chủ SQL thành một botnet

32. 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

33. Tấn công phát lại

Tạo bản sao truyền để sử dụng sau này
Được coi là một loại tấn công dos
Có thể được ngăn chặn bằng cách vá trình duyệt web
Replay các cuộc tấn công hơn và hơn để lũ máy chủ

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

Flash cookie
Session cookie
Ram cookie
Secure cookie

35. Plug-in trình duyệt.

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

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

Integer overflow
Buffer overflow
Real number
Heap size

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

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

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

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

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

cookie của bên thứ ba
cookie chính chủ
cookie của bên thứ hai
cookie của bên thứ tư

40. Câu 40 [<DE>]: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?

Transitive
privilege rights
heap spray
vertical escalation

41. 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

42. 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

43. Kỹ thuật tấn công phổ biến trên Web là

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

Chương 3

44. Câu nào đúng về Hashed Message Authentication Code (HMAC)

Mã hóa khóa và thông báo
Chỉ mã hóa khóa
Chỉ mã hóa tin nhắn
Chỉ mã hóa khóa DHE

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

SHA-3
SHA-2
SHA-4
SHA-5

46. Hệ thống khóa công khai tạo ra các khóa công cộng ngẫu nhiên khác nhau cho mỗi phiên được gọi là

Perfect forward secrecy
Trao đổi khóa công khai (PKE)
Elliptic Curve Diffie-Hellman (ECDH)
Diffie-Hellman (DH)

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

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

48. 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.

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

Tính không từ chối(non-repudiation)

Tính từ bỏ(repudiation)
Tính toàn vẹn (integrity)
Tính khả dụng (availability)

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

RSA
EFS
quantum computing
ECC

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

RSA
SHA-2
BTC-2
ME-14

52. 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 công khai của Alice
Khoá bí mật của Alice
Khoá bí mật của Bob
Khoá công khai của Bob

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

xác minh người nhận
chứng minh tính toàn vẹn của thông điệp
xác minh người gửi
thực thi không từ chối

54. 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

55. 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)

56. 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

57. Chứng chỉ số liên kết

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

58. 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

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

Trong digests
Trong tokens
Trên hệ thống của người dùng cục bộ
Nhúng trong chứng chỉ kỹ thuật số

60. Cơ sở hạ tầng khóa công khai (PKI).

Là quản lý chứng chỉ kỹ thuật số
T ạo mật mã khóa riêng
Yêu cầu sử dụng RA thay vì CA
Tự động tạo khóa công khai / riêng tư

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

Server digital certificate
Web digital certificate
Email web certificate
Personal digital certificate

62. 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)

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.

Session keys
Encrypted signatures
Digital digests
Digital certificates

64. Thuật toán chia Euclid mở rộng dùng để

Tính phần tử nghịch đảo của một số theo module nào đó
Tính nhanh một lũy thừa với số lớn
Kiểm tra nhanh một số nguyên tố lớn

Tìm đồng dư của một số theo module nào đó

65. Người A chọn các thông số p =17, q = 3, e = 5. Hỏi khóa công khai của A là gì?

(51, 5)
(32, 5)
(17,3)
(17, 3, 5)

66. 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?

(13,55)
(5,51)
52
55

67. 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?

37
13
5
23

68. 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?

37
(5, 51)
(55, 13)
55

69. DES là viết tắt của từ nào ?

Data encryption standard
Data encryption system
Data encoding standard
Data encryption signature

70. Những gì được sử dụng để tạo ra một chữ ký điện tử?

Khóa công khai của người gửi
Khóa riêng của người nhận
Khóa riêng của người gửi
Khóa công khai của người nhận

71. 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?

Phải thử 2^{127} lần, thời gian thử là 5,4 * 10^{18} năm.

Phải thử 2^{128} lần, thời gian thử là 5,4 * 10^{18} năm.

Phải thử 2^{64} lần, thời gian thử là 5,4 * 10^{18} năm.

Phải thử 2^{128} lần, thời gian thử là 18 năm.

72. Chữ ký điện tử (số) là :

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

Các đặc tính của mật mã, được sử dụng để biến đổi mã hóa thông tin

Họ tên người gửi được ghi ở dạng điện tử và kết nối với thông tin

Tất cả đều sai

73. RSA là giải thuật

Mã hóa công khai

Là tên của một tổ chức quốc tế về mã hóa

Mã hóa khóa bí mật

Tất cả đều sai

74. 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?

HGRGXV

GRXVCN

VCMHGR

XVHGGR

75. 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?

EARDY

DAEGU

YAEDR

ADERU

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

Một phương pháp để cho những người nhận của tin nhắn chứng minh nguồn gốc và sự toàn vẹn của một tin nhắn

Một phương thức chuyển giao một chữ ký viết tay vào một tài liệu điện tử

Một phương pháp mã hóa thông tin bí mật

Một phương pháp để cung cấp một chữ ký điện tử và mã hóa

77. cho bản mã "EC" khóa k là:

$$\begin{matrix} 8 & 3 \\ 7 & 3 \end{matrix}$$

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

cw
oy
yn
om

78. cho bản mã “SW” khóa k là:

$$\begin{matrix} 7 & 2 \\ 3 & 3 \end{matrix}$$

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

sy
ma
mu
mi

79. 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?

238
22
28
138

80. Trong giải thuật mã hóa DES thực hiện bao nhiêu vòng lặp?

16
6
8
15

81. 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?

hill
bill

sice
viet

82. 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?

copy
page

pase
cont

83. 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?

page
sage

seft
stef

84. Chức năng của các hàm băm (hash function)?

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

85. 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

83
13
16
186

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

(51 , 13)
(51, 5)
(36, 5)
(17, 3)

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

29
9
19
92

Chương 4

88. Bước đầu tiên trong việc bảo mật hệ điều hành là gì?

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

89. Điều nào sau đây KHÔNG phải là activity phase control?

Resource control
Compensating control
Detective control
Deterrent control

90. Điều nào sau đây KHÔNG phải là phương pháp phát hiện chuyển động?

Độ ẩm
Tần số vô tuyến
Từ tính
Hồng ngoại

91. Điều nào có thể được sử dụng để bảo mật thiết bị di động.

cable lock
Mobile connector
Mobile chain
Security tab

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

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

93. 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.

94. Một typical configuration baseline sẽ bao gồm mỗi phần sau NGOẠI TRỪ .

Thực hiện đánh giá rủi ro an ninh
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

95. Cái nào sau đây là danh sách của người gửi email được chấp thuận?

whitelist
Blacklist
Greylist
Greenlist

96. 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.

Chính sách nhóm(Group Policy)
Thư mục hoạt động(Active Directory)
Sao chép theo dõi (Snap-In Replication - SIR)
Cấu hình lệnh(Command Configuration)

Chương 5

97. Công cụ/cơ chế bảo mật cho mạng không dây là

WEP
SSL
TSL
Giao thức PGP

98. 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

99. FTP sử dụng cổng gì ?

21

25

23

80

100. Cổng nào được HTTPS sử dụng?

443

53

80

21

101. 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

102. Tính năng bảo mật nào KHÔNG cung cấp tính năng cân bằng tải?

Lọc các gói dựa trên cài đặt giao thức

Ẩn các trang HTTP lỗi

Xóa tiêu đề định danh máy chủ khỏi HTTP responses

Tấn công từ chối dịch vụ (dos)

103. Chức năng nào mà bộ lọc nội dung Internet KHÔNG thực hiện?

Phát hiện xâm nhập

Lọc URL

Kiểm tra phần mềm độc hại

Kiểm tra nội dung

104. 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

105. Làm thế nào để một mạng LAN ảo (VLAN) cho phép các thiết bị được nhóm lại?

Hợp lý

Dựa trên mạng con

Trực tiếp đến trung tâm

Chỉ xung quanh công tắc lõi

106. Các lỗ hổng bảo mật trên hệ thống là do

Dịch vụ cung cấp, bản thân hệ điều hành và con người tạo ra
Dịch vụ cung cấp
Bản thân hệ điều hành
Con người tạo ra

107. 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

108. Điều nào trong số này KHÔNG phải là một cuộc tấn công chống lại một công tắc?

Mạo danh địa chỉ ARP
Mạo danh địa chỉ MAC
ARP poisoning
MAC flooding

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

Nó loại bỏ các địa chỉ riêng khi gói rời khỏi mạng.
Nó có thể là trạng thái trạng thái hoặc không trạng thái.
Nó thay thế địa chỉ MAC cho địa chỉ IP.
Nó chỉ có thể được tìm thấy trên các bộ định tuyến lõi

110. Proxy ngược.

Định tuyến các yêu cầu đến máy chủ chính xác
Chỉ xử lý các yêu cầu gửi đi
Giống như một máy chủ proxy
Phải được sử dụng cùng với tường lửa

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

Với máy chủ SMTP
Trên máy chủ POP3
Trên máy khách lưu trữ cục bộ
Trên máy chủ proxy

112. Loại nhật ký nào có thể cung cấp chi tiết về các yêu cầu đối với các tệp cụ thể trên hệ thống

Access log
Event log
Audit log
SysFile log

1. 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 poisoning
DNS replay
DNS masking
DNS forwarding

113. Giao thức nào an toàn nhất để chuyển tệp?

SFTP
SCP
FTPS
FTP

114. Nếu một nhóm người dùng phải được tách ra khỏi những người dùng khác, thiết kế mạng nào bảo mật nhất?

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

115. Trong một mạng bằng cách sử dụng IEEE 802.1x, một supplicant.

đưa ra yêu cầu cho người xác thực
phải sử dụng IEEE 802.11d để kết nối với mạng
liên hệ trực tiếp với máy chủ xác thực
chỉ có thể là một thiết bị không dây

116. Điều nào sau đây KHÔNG phải là mối quan tâm về bảo mật của môi trường ảo hóa?

Các máy chủ ảo rẻ hơn các máy chủ vật lý của chúng.
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.
Di chuyển trực tiếp có thể di chuyển ngay lập tức một máy chủ ảo hóa sang một trình siêu giám sát khác.

117. 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)