Chọn các phát biểu đúng trong các phát biểu sau đây về chế độ mã hoá:

(I) trong chế độ mã hoá CBC, khối bản rõ được XOR với khối bản mã ở bước trước đó trước khi thực hiện mã hoá

(II) chế độ mã hoá CRT không yêu cầu sử dụng vector khởi tạo

(III) block cuối cùng trong chế độ mã hoá CBC sử dụng vector khởi tạo

(IV) chế độ mã hoá OFB có thể được sử dụng cho mã hoá dòng

I II IV

Phần mềm nào sau đây có thể giúp thăm dò mạng máy tính bằng cách quét danh sách địa chỉ IP và Port?

Angry IP Scanner

Chọn phát biểu sai về hệ thống mạng riêng ảo (VPN):

Các hệ thống VPN bao gồm 2 loại là site-to-site VPN và user VPN

Các thuật toán sử dụng trong VPN phải là các thuật toán nổi tiếng và mã hoá mạnh

VPN Server phải được cài đặt trên bức tường lửa hoặc bộ định tuyến biên

VPN sử dụng một số giao thức riêng biệt để tạo ra các đường hầm VPN

Giao thức nào sau đây là giao thức không an toàn?

Smtp

Chọn phát biểu đúng nhất về chữ ký số?

Hàm băm được sử dụng trong chữ ký số luôn luôn cho ra kết quả có độ dài ngắn hơn thông điệp gốc

Không tồn tại 2 thông điệp khác nhau bất kỳ có cùng giá trị chữ ký số (k chính xác)

Hàm băm được sử dụng trong chữ ký số phải được hiện thực trên phần cứng

Tất cả các câu trả lời đều sai

Điểm yếu của bộ lọc gói là:

Tất cả các câu trả lời đều đúng.

Không phát hiện giả mạo địa chỉ IP.

Không hỗ trợ các lược đồ xác thực người dùng.

Không xem xét dữ liệu ở tầng cao hơn.

Chọn phát biểu đúng nhất về công cụ cryptool?

Là công cụ phục vụ cho việc học tập…

Trong ngôn ngữ lập trình java, lớp keygenerator dùng để làm gì?

Tạo một khoá bí mật với một hệ mã đối xứng đã quy định

Khi cần truyền một thông điệp và dùng cả hai dịch vụ bí mật và xác thực của PGP thì phần nào sẽ được mã hóa đối xứng bằng khóa phiên?

Thông điệp và chữ ký số trên thông điệp

Tổ chức CA (Certification Authority) có trách nhiệm xác thực thông tin nào sau đây

Khoá công khai của người đã đăng ký

Đối với hệ mã hóa khóa công khai, khóa nào được sử dụng để xác minh chữ ký số trong một thông điệp:

Khóa công khai của người gửi

Đối với việc khởi tạo một IDS, sau khi đã xác định mục tiêu ta phải làm gì tiếp theo

Chọn thành phần, hệ thống để theo dõi

Trong chương trình apache, các tập tin cấu hình có phần đuôi mở rộng là:

Conf

Trong hệ mã hoá khoá công khai, giả sử A mã hoá thông điệp sử dụng khoá riêng của A và gởi thông điệp đã được mã hoá trên cho B, hãy chọn phát biểu đúng nhất?

Nếu B biết thông điệp đến từ A thì B Có thể giải mã thông điệp sử dụng khoá Công khai của A.

Có bao nhiêu khoá được sử dụng trong giải thuật triple des

2 or 3

Che dấu địa chỉ IP

VPN

Cho biết cấu hình bức tường lửa nào sau đây có khả năng ngăn chặn các vi phạm an ninh mạng khi bộ lọc gói trên bộ định tuyến kết nối với Internet bị thương tổn hay đã thỏa hiệp

a. single-homed bastion host

b. dual-homed bastion host

C. Screened subnet 4

d. Câu (b) và (C) đều đúng

dấu vân tay

những gì là chính bạn

https apache

mod_ssl

Giả sử mỗi người trong nhóm gồm N người muốn giao tiếp bí mật với (N-1) người còn lại sử dụng hệ thống sử dụng mã hoá đối xứng. Giao tiếp giữa 2 người bất kỳ không bị giải mã bởi những người còn lại trong nhóm. Hãy cho biết số lượng khoá cần thiết cho hệ thống trên là bao nhiêu?

N(N-1)/2

Hình thức tấn công nào sau đây là tấn công thụ động?

Phát lại

Giả mạo

Từ chối dịch vụ

Phân tích lưu lượng

app mã nguồn mở, ssl/tls trong thực tế:

openssl

Chuẩn bảo mật cho mạng cục bộ không dây nào dưới đây mà người khác không thể bị bẻ khoá hoặc giả mạo nhằm sử dụng không hợp pháp mạng cục bộ không dây?

a. Lọc địa chỉ MAC

b. Tất cả các câu trả lời đều sai (đoán là wpa2)

C. WEP

d. WPA

Các trạng thái của cổng (port) được xác định bởi chương trình NMAP có thể là?

a. Active, inactive, standby

b. Open, half-open, closed

C. Active, closed, unused

d. Open, filtered, unfiltered

Biện pháp nào sau đây là cần thiết để ngăn chặn lây nhiễm virus trên máy tính?

a. Cài đặt các bản vá lỗi cho các chương trình và hệ điều hành

b. Cài đặt chương trình phát hiện xâm nhập

C. Cài đặt chương trình bức tường lửa

d. Dọn rác máy tính

hydra, root, 192.168.1.105, rockyou.txt

hydra -l root -P rockyou.txt 192.168.1.105 -t 4 ssh

Trong giao dịch điện tử an toàn (SET), người mua hàng mã hoá thông tin thẻ (credit card) của mình sử dụng khoá nào sau đây?

Khoá Công khai của ngân hàng

Kỹ thuật trong wpa thay thế crc trong wep

Mic

Rsa, p=13,q=17, nếu puk=35 thì prk=?.

n = pq=221
ø(n) = (p-1)*(q-1) =192
e = 35
d = 11 (thoã điều kiện 35*11 mod 192 = 1)
Public Key: m = n = 221 và e = 35
Private Key: p = 13, q = 17 và d = 11
Mã hoá thông điệp:
B muốn gởi thông điệp đến A: plaintext = 5
B tính ciphertext = 5^{35} mod 221 = 125
B gởi ciphertext 125 đến A
Giải mã thông điệp:
A nhận được ciphertext: 125. Để giải mã thông điệp này, A sử dụng khoá riêng
Plaintext = 125^{11} mod 221 = 5
A giải mã được thông điệp: 5

Điều gì là phản ứng thích hợp cho một sự kiện bảo mật trên mạng?

a. Cài đặt bộ định tuyến mới

b. Thực hiện chính sách an ninh (sai)

C. Ngắt kết nối mạng(đoán)

d. Thực hiện các thủ tục an ninh

lớp signature thuộc gói java.security

firewall có thể chống lại

DOS

Shoulder surfing

Dumpster diving

Phishing

Thông tin nào sau đây không tồn tại trong các chứng chỉ X.509:

a. Tên của tổ chức CA cấp chứng chỉ

b. Khoá Công khai của thực thể được cấp chứng chỉ

c. Chữ ký số của tổ chức CA cấp chứng chỉ

d. Chữ ký số của thực thể được cấp chứng chỉ

pgp, bộ khoá: bộ khoá công khai

sha-1 dài 160

Cho biết phát biểu sai về dual signature trong các phát biểu sau:

a. Đối với giao dịch điện tử an toàn, dual signature được dùng nhằm để ngân hàng không thể biết được hash code của tài liệu đặt hàng.

b. Đối với giao dịch điện tử an toàn, dual signature được dùng để ký trên hai tài liệu gồm thông tin thanh toán (payment information – PO) và thông tin đặt hàng order information - OI).

C. Mục đích của dual signature là để liên kết hai thông điệp dành cho hai nơi nhận khác nhau.

d. Dual signature được dùng để ký trên hai tài liệu nối với nhau và mỗi tài liệu này có hash code riêng.

Nếu bạn thực hiện một bộ chính sách và thủ tục xác định thông tin công ty là bí mật và sau đó đào tạo nhân viên về các quy trình liên quan, bạn có thể ngăn chặn tấn công nào

a. Social engineering b. Man-in-the-middle C. Smurf d. Dos

Fail2ban centos 7, xem danh sách ip bị cấm cho ssh:

fail2ban-client status sshd

cốt lõi của an toàn thông tin: toàn vẹn, bí mật, sẵn sàng

Chọn phát biểu đúng về các phương pháp xác thực?

a. Trong giao thức xác thực dựa trên mật khẩu, để chống tấn công lập lại ta cần mã hoá mật khẩu trước khi gởi

b. Phương pháp xác thực dựa trên mật khẩu an toàn trước tấn công xen giữa

C. Trong giao thức xác thực dùng mã hoá khoá Công khai, SỐ Nonce được mã hoá sử dụng khoá công khai của bên nhận

d. Giao thức xác thực dùng mã hoá đối xứng chỉ hỗ trợ xác thực 1 chiều

Trong giải thuật DES, cho bảng thay thế S-Box như bên dưới:

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Hãy cho biết kết quả đầu ra tương ứng với khối chuỗi bit đầu vào: 100100 khi thực hiện chuyển đổi bằng S-Box này?

a. 0111

b. 0011

c. 1000

d. 1001

100100 tách ra 1-0010-0 lấy 1 đầu với 0 cuối là ra 10 = 2 => hàng 2 , 0010 =2 => cột 2
Hàng 2 cột 2 là số 9, là 1001

Chọn phát biểu SAI trong các phát biểu dưới đây?

a. Trong an toàn thông tin, việc hiện thực các giải pháp công nghệ đơn lẻ không thể cung cấp đủ sự an toàn

b. Khi có sự thay đổi về mặt công nghệ thì các chính sách an toàn thông tin của tổ chức cần phải được xem xét lại

C. Thông điệp trước khi thực hiện mã hoá (thông điệp gốc) được gọi là plaintext

d. Dịch vụ xác thực chỉ cung cấp khả năng xác thực các thực thể giao tiếp

Thuật ngữ nào sau đây không phải là một loại bức tường lửa (firewall)?

a. Packet filter

b. Circuit-level gateway

C. Application-level gateway

d. Proxy server gateway

Đâu là ngành học nghiên cứu các phương thức để thu được ý nghĩa của thông tin đã được mã hóa mà không cần sử dụng khoá?

a. Tất cả trả lời đều đúng

b. Cryptography(sai)

C. **Cryptanalysis**

d. Steganography

mã hoá dữ liệu trên máy và đòi tiền chuộc?

ransomware

Hình thức tấn công thụ động chống lại nguyên tắc cốt lõi nào của an toàn thông tin

Bí mật

Tấn công DOS (Denial of Service) thuộc loại tấn công nào trong kiến trúc an ninh OSI ?

Tấn công chủ động (Active Attack)

Cơ chế nào sau đây không cần thiết sử dụng để chống lại tấn công từ chối dịch vụ?

Mã hóa dữ liệu (encipherment)

Cơ chế nào không sử dụng cho dịch vụ xác thực?

Quản lý truy cập (access control)

Cho biết Code Red thuộc vào loại mã độc nào sau đây:

Một loại mã độc lai ghép

Đối với mã hóa DES, trong các phát biểu sau phát biểu nào là sai?

Dữ liệu được mã hóa trong các khối có chiều dài 64 bits.

DES dùng bộ tạo khóa để tạo ra các khóa con dùng cho mỗi vòng và chúng có chiều dài là 48 bits.

DES sử dụng khóa có chiều dài 64 bits.

S-box là một hàm thay thế không tuyến tính làm tăng độ phức tạp của phép biến đổi.

Hệ mã Double DES(2DES) không an toàn do tấn công gì?

Tấn công “meet in the midle”

Chế độ hoạt động nào sau đây mã hóa các khối một cách riêng biệt?

ECB

Đối với mã hóa khóa công khai, khóa nào được sử dụng để mã hóa một thông điệp:

Khóa công khai của người nhận

Đối với mã hóa khóa công khai, khóa nào được sử dụng để tạo chữ ký số trên một thông điệp:

Khóa riêng của người gửi

DAA(Data Authentication Algorithm) tạo ra mã xác thực thông điệp có kích thước là:

64 bits

Cho một hàm băm với kết quả băm có chiều dài là 128 bits. Hãy cho biết cần sửa đổi ít nhất bao nhiêu chỗ trong văn bản P sao cho xác xuất để có hai văn bản P_1 và P_2 mà giá trị băm của chúng bằng nhau là 0.5

64

Chữ ký số là một cơ chế xác thực nhằm:

Xác nhận danh tính của người tạo ra thông điệp.

Chống thoái thác về xuất xứ.

Xác minh tính toàn vẹn của thông điệp.

Cả ba câu trên đ**ều đúng.**

Cho biết phát biểu sai khi nói về các lược đồ tạo chữ ký số:

a. Lược đồ RSA tạo chữ ký có chiều dài lớn hơn so với lược đồ DSA.

b. Lược đồ DSA tạo chữ ký có chiều dài 512 bits.

c. DSA không thể dùng cho các vấn đề mã hóa dữ liệu và trao đổi khóa.

d. Lược đồ DSA tạo và xác minh chữ ký nhanh hơn so với lược đồ RSA.

Chữ ký số trong chứng chỉ X.509 được tạo dùng khóa nào sau đây:

Khóa riêng của đơn vị phát hành chứng chỉ.

Cho biết yêu cầu của truyền thông an toàn:

a. Thông điệp truyền nhận không thể phân tích mã.

b. Tất cả các câu trên đều đúng.

c. Thông điệp truyền nhận không thể giả mạo.

d. Thông điệp truyền nhận không thể thay đổi được.

Yêu cầu nào là cần thiết khi buộc phải sử dụng DES:

a. Thay đổi khóa thường xuyên để chống tấn công brute-force.

b. Cả ba câu trên đều đúng.

c. Thử khóa có yếu hay không trước khi sử dụng.

d. Xem xét sử dụng chế độ hoạt động CBC.

Thuật toán mã hóa đối xứng nào có thể sử dụng trong truyền thông an toàn hiện nay:

3DES, AES

Khi xác thực, thông tin nào sau đây là ví dụ về việc xác minh điều gì chính là bạn?

Vân tay (Fingerprint).

Loại hình tấn công an ninh nào cần xem xét đối với các giao thức xác thực?

Tấn công xen giữa.

Khi cần truyền một thông điệp và dùng cả hai dịch vụ bí mật và xác thực của PGP thì phần nào sẽ được mã hóa đối xứng bằng khóa phiên?

Thông điệp và chữ ký số trên thông điệp.

Chọn phát biểu sai trong các phát biểu sau khi PGP được sử dụng trong một hệ thống E-mail:

a. Hệ thống E-mail nói trên sẽ cung cấp các dịch vụ xác thực, bí mật, nén, tương thích e-mail và phân mảnh.

b. Nếu chỉ dùng dịch vụ xác thực thì thông điệp gởi đi sẽ không có mã hóa ở bất kỳ khối dữ liệu nào.

c. Nếu dùng dịch vụ tương thích e-mail thì mỗi nhóm 3 byte dữ liệu nhị phân được ánh xạ thành 4 ký tự ASCII.

d. Nếu dùng dịch vụ bí mật thì thông điệp gởi đi sẽ có mã hóa ở một số khối dữ liệu.

Khóa được sử dụng để mã hóa khóa phiên trong PGP khi dùng trên hệ thống E-mail là:

Khóa công khai của người nhận.

Cho biết phát biểu sai về chữ ký đôi(dual signature) trong các phát biểu sau:

a. Dual signature được dùng để ký trên hai tài liệu nối với nhau và mỗi tài liệu này có mã băm riêng.

b. Đối với giao dịch điện tử an toàn, dual signature được dùng nhằm để ngân hàng không thể biết được mã băm của tài liệu đặt hàng.

c. Mục đích của dual signature là để liên kết hai thông điệp dành cho hai nơi nhận khác nhau.

d. Đối với giao dịch điện tử an toàn, dual signature được dùng để ký trên hai tài liệu gồm thông tin thanh toán (payment information – PO) và thông tin đặt hàng (order information – OI).

SSL không có khả năng chống lại loại tấn công nào sau đây:

a. SYN Flooding

b. Man-in-the-Middle

c. Password Sniffing

d. Replay

Cho biết cấu hình bức tường lửa nào sau đây có khả năng ngăn chặn các vi phạm an ninh mạng khi bộ lọc gói trên bộ định tuyến kết nối với Internet bị thương tổn hay đã thỏa hiệp:

Dual-homed bastion host, Screened subnet

Chọn phát biểu sai khi nói về bộ lọc gói (packet filter):

a. Nó không xem xét dữ liệu ở tầng ứng dụng trong mô hình TCP/IP.

b. Nó có khả năng phát hiện các tấn công dạng giả mạo địa chỉ ở tầng mạng.

c. Nó không thể ngăn chặn các cuộc tấn công sử dụng các lỗ hổng ứng dụng cụ thể.

d. Chức năng ghi nhật ký (logging) của nó bị hạn chế.

Cho biết phát biểu nào sau đây không phải là mục tiêu thiết kế một bức tường lửa?

a. Tất cả thông tin từ bên trong ra bên ngoài và ngược lại phải đi qua bức tường lửa.

b. Chỉ các loại thông tin được cấp quyền thông qua chính sách an ninh cục bộ mới được phép đi qua bức tường lửa.

c. Tất cả các phát biểu đều đúng.

d. Tất cả thông tin di chuyển bên trong một mạng cục bộ phải đi qua bức tường lửa.

Chọn phát biểu sai trong các phát biểu sau khi nói về các loại bức tường lửa:

a. Application-level gateway còn được gọi là proxy server.

b. Circuit-level gateway cho phép thiết lập một kết nối TCP end to end.

c. Packet fiter quyết định lọc gói dựa trên thông tin các trường trong IP và TCP header.

d. Application-level gateway an toàn hơn Packet fitering router.

Cách thức để hạn chế tấn công SYN-Flooding trên bức tường lửa là:

a. Tất cả các câu trả lời đều đúng.

b. Chỉ cho phép gói SYN trên một số port nhất định.

c. Chặn những IP kết nối thất bại nhiều lần.

d. Cho phép nhận một lượng nhất định gói SYN trong một giây.

Hướng phát hiện thâm nhập bất hợp pháp nào liên quan đến việc thu thập hành vi người dùng hợp pháp trong một khoảng thời gian và sau đó phân tích đánh giá:

Phát hiện dựa trên thống kê

Cho biết phát biểu sai trong các phát biểu sau khi nói đến hệ thống phát hiện thâm nhập bất hợp pháp:

a. Để xây dựng hệ thống phát hiện thâm nhập bất hợp pháp ta có hai hướng tiếp cận là rule-based detection và behavior-based detection.

b. Một hệ thống phát hiện thâm nhập bất hợp pháp hiệu quả có thể kết hợp với bức tường lửa để ngăn chặn ngay các xâm nhập.

c. Nếu hệ thống phát hiện một xâm nhập đủ nhanh, kẻ xâm nhập có thể được xác định trước khi bị thiệt hại.

d. Nó cho phép ta thu thập thông tin về các kỹ thuật xâm nhập đã được sử dụng để tăng cường cho công tác phòng chống xâm nhập.

Đối với việc khởi tạo một IDS, sau khi đã xác định mục tiêu ta phải làm gì tiếp theo?

Chọn thành phần, hệ thống để theo dõi

Nếu một tổ chức muốn bảo vệ một máy chủ tránh bị người dùng hợp pháp phá hoại, hệ thống phát hiện thâm nhập bất hợp pháp nào là lựa chọn tốt nhất?

HIDS

Nếu một tổ chức muốn phát hiện các tấn công với chi phí thấp thì hệ thống phát hiện thâm nhập bất hợp pháp nào là lựa chọn tốt nhất?

NIDS

VPN là viết tắt của:

Virtual Private Network

Lợi ích chính của VPN so với các mạng chuyên dụng như frame relay, leased line hay dial-up truyền thống là gì?

Giảm chi phí

Trong VPN, thuật ngữ "tunneling" đề cập đến:

Đóng gói các gói tin bên trong các gói tin của một giao thức khác để tạo và duy trì mạch ảo

Những giao thức nào sau đây là giao thức VPN tunneling?

a. Tất cả các câu trả lời đều đúng

b. IPSec

c. L2TP

d. PPTP

Khác biệt giữa Firewall và VPN là gì?

Firewall chặn các thông điệp còn VPN thì mở ra con đường cho các thông điệp hợp lệ đi qua.

WEP được viết tắt là:

Wired Equivalent Privacy

Điểm yếu thật sự của WEP trong vấn đề mã hóa là:

Thuật toán lập lịch khóa của RC4

Tiêu chuẩn an ninh mạnh mẽ hơn được phát triển bởi IEEE để giải quyết các lỗ hổng chuẩn WLAN IEEE 802.11 là:

IEEE 802.11i

Khác biệt giữa WPA và WPA2 là:

WPA mã hóa dùng RC4 với TKIP/MIC, WPA2 mã hóa dùng AES.

Chọn phát biểu sai trong các phát biểu sau:

a. AES là mã hóa đối xứng

b. IEEE 802.11i thực thi an ninh trên port

c. WPA2 cho phép các client AES và TKIP được hoạt động trên cùng WLAN

d. WPA là một tập con của IEEE 802.11i

1. Chọn phát biểu sai khi nói về bộ lọc gói (packet filtering router)

a. Nó không xem xét dữ liệu ở tầng ứng dụng trong mô hình TCP/IP
b. Nó không có khả năng phát hiện các tấn công giả mạo địa chỉ ở tầng mạng
c. Nó không có khả năng phát hiện các tấn công dựa trên các lỗ hổng của các tầng từ tầng vận chuyển trở lên
d. Nó hầu như không hỗ trợ các lược đồ xác thực người dùng cao cấp
e. Tất cả đều đúng

2. Cho biết cấu hình bức tường lửa nào sau đây có khả năng phòng tránh các tấn công khi bộ lọc gói trên bộ định tuyến kết nối với Internet bị thương tổn hay đã tắt

a. Single-Homed Bastion Host
b. Dual- Homed Bastion Host.
c. Screened-subnet Firewall
d. **Câu b và c đều đúng**

3. Chọn phát biểu sai trong các phát biểu sau khi nói về các loại bức tường lửa

a. Packet filtering router quyết định lọc gói dựa trên thông tin các trường trong mỗi gói
b. Application-level gateway còn được gọi là proxy server.
c. Application-level gateway an toàn hơn Packet filtering router
d. Curcuit-level gateway cho phép thiết lập một kết nối TCP end to end

4. Chọn phát biểu sai khi nói về virus và worm

a. Cả virus và worm đều có khả năng lây lan và tạo bản sao

b. Cả virus và worm đều được đính kèm trong một chương trình

c. Worm có khả năng tái tạo chính nó

d. Virus có khả năng phát tán bản sao từ máy tính này sang máy tính khác

5. Cho biết thành phần tham gia trong giao dịch điện tử an toàn (SET- Secure Electronic Transaction) có trách nhiệm thanh toán các khoản mua hành của chủ thẻ

a. Cardholder
b. Merchant
c. Issuer
d. Acquier

6. Cho biết phát biểu sai về dual signature trong các phát biểu sau:

a. Mục đích của dual signature là để liên kết hai thông điệp dành cho hai nơi
b. Dual signature được đăng ký trên hai tài liệu nối với nhau và mỗi tài liệu
c. Đối với giao dịch điện tử an toàn, dual signature được dùng để ký trên hai tài liệu gồm thẻ thanh toán (Payment information- PI), và thông tin đặt hàng (Order information- OI)
d. Đối với giao dịch điện tử an toàn, dual signature được dùng nhằm để ngân hàng không thể biết được mã băm của tài liệu đặt hàng

7. Chế độ nào của IPsec không bảo vệ IP header

a. Tunnel
b. Transport
c. Cả 2 câu a và b đều đúng
d. Cả 2 câu a và b đều sai

8. Các giao thức được thiết kế bởi IETF nào an toàn cho gói dữ liệu ở tầng mạng trong mô hình mạng OSI

a. IPsec
b. SSL
c. PGP
d. Cả 3 câu trên đều đúng

9. Tham số nào của sự kết hợp bảo mật SA (Security Association) gồm các thông số xác thực, khóa, và thời gian sống của khóa

a. Security Parameters Index (SPI)
b. AH Information
c. ESP Information
d. Cả câu b và c đều đúng

10. Giao thức IKE (Internet Key Exchange) tạo các kết hợp bảo mật (SA- Security Association) nào sau đây

a. PGP
b. SSL
c. IPsec
d. Cả câu b và c đều đúng

11. Cho biết tấn công nào gây nguy hiểm cho sự an toàn của phương pháp trao đổi thông tin không chứng thực lẫn nhau

a. Ciphertext attack

b. Plaintext attack

c. Secret-text attack

d. **Các câu trên đều đúng** ?

12. SSL không cung cấp dịch vụ nào sau đây:

a. Authenticaiton

b. Confidentiality

c. Message Integrity

d. Compression

13. SSL không có khả năng chống lại dạng tấn công nào sau đây:

a. Man-in-the-middle-attack

b. IP Spoofing

c. SYN flooding

d. Cả 3 câu trên đều đúng

14. Giao thức nào của IPsec cung cấp dịch vụ xác thực và dịch vụ mã hóa thông tin trong Internet trong mô hình **TCP/IP**

a. AH (chỉ xác thực)

b. ESP (dùng UDP)

c. SSL

d. Cả ba câu trên đều đúng

15. Trong PGP, để gửi e-mail, người dùng cần có một bộ khóa, cho biết đó là bộ khóa nào:

a. Bộ khóa công khai

b. Bộ khóa riêng

c. Bộ khóa phiên

d. Cả 3 câu đều đúng

16. Chọn phát biểu sai khi nói về bức tường lửa

a. Tất cả truy cập mạng từ bên ngoài vào bên trong phải đi qua bức tường lửa

b. Tất cả truy cập mạng từ bên trong ra bên ngoài không nhất thiết phải qua bức tường lửa

c. Tất cả truy cập được phép được định nghĩa thông qua một chính sách thiết lập bởi người dùng.

d. Bức tường lửa chính nó phải là miễn dịch

17. Với SHA-512 cho biết phương trình để tính giá trị W_{17}

a. $W1 \oplus \sigma 0(W2) \oplus W10 \oplus \sigma 1(W15)$

b. $W0 \oplus \sigma 0(W2) \oplus W10 \oplus \sigma 1(W15)$

c. $W1 \oplus \sigma 1(W2) \oplus W10 \oplus \sigma 0(W15)$

d. $W0 \oplus \sigma 1(W2) \oplus W10 \oplus \sigma 0(W15)$

18. Chữ ký số (digital signature) sử dụng với các dịch vụ nào sau đây:

a. Xác thực (Authentication)
b. Không thể thoái thác (Nonrepudiation)
c. Tính toàn vẹn (Integrity)
d. Cả 3 câu đều đúng

19. Chọn phát biểu sai trong các phát biểu sau khi nói về các phiên SSL (SSL session):

a. Một kết nối SSL có một hoặc nhiều phiên SSL
b. Một kết nối SSL định nghĩa một bộ các tham số liên quan đến việc tạo phiên SSL
c. Kết nối SSL được sử dụng để tránh tốn kém trong việc thực hiện bảo mật cho mỗi phiên SSL.
d. Các câu trên đều sai

20. Cho biết giao thức nào sau đây không có trong kiến trúc SSL:

a. SSL Record Protocol

b. SSL Message Protocol

c. SSL Alert Protocol

d. SSL Change Cihper Spec Protocol

21. Cho biết tham số nào sau đây được định nghĩa trong mã hóa phía client và giải mã phía server:

a. Client Write Key

b. Server Write Key

c. Server Read Key

d. Client Read Key

Bảo mật trong Datamining yêu cầu:

A. Dữ liệu không thể truy xuất cho công cộng

B. Dữ liệu có thể truy xuất riêng phần

C. Dữ liệu phải được mã hóa

D. Dữ liệu có thể suy diễn

- Mục nào không là tấn công chủ động:

  A. Tấn công nghe lén (eavesdropping)

  B. Tấn công từ chối dịch vụ

  C. Tấn công replay

  D. Tấn công giả mạo (masquerade)

  Sai **A** là đáp án đúng

- **Câu 3:**

  X800 là một:

  A. Cơ chế an toàn

  B. Dịch vụ an toàn

  C. Là một tiêu chuẩn

  D. Một dịch vụ không đáp ứng yêu cầu không thể từ chối (non-reputation)

  Chính xác

- **Câu 4:**

  Audit (kiểm tra, kiểm toán) dùng trong an toàn CSDL nhằm:

  A. Xác thực đó là ai (authetication)?

  B. Cấp quyền ai có thể làm gì (authorization)?

  C. Ai đã làm gì?

  D. Tất cả các mục

  Sai **D** là đáp án đúng

- **Câu 5:**

Phần mềm ngăn chặn hành vi:

A. Theo dõi các hành vi trong thời gian thực của hệ thống

B. Phát hiện code có hại trước khi chúng thực hiện

C. Theo dõi các tham số của hệ thống

D. Tất cả đều đúng

Sai **D** là đáp án đúng

- **Câu 6:**

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

A. Chỉ có thể dùng tường lửa

B. Có thể hạn chế trong bằng cách lập trình

C. Hiện nay đã có cách phòng chống hiệu quả

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

Chính xác

- **Câu 7:**

Bộ đệm một lần:

A. Khóa chỉ xài 1 lần

B. Có thể không an toàn do phân phối

C. Sinh khóa ngẫu nhiên

D. Tất cả đều đúng

Sai **D** là đáp án đúng

- **Câu 8:**

Trong DAC, mô hình nào dung cấu trúc đồ thị tĩnh và đồ thị động:

A. Mô hình truy cập CSDL đa mức

B. Mô hình Take-grant

C. Mô hình ma trận truy cập

D. Mô hình Acten (Action. Entity)

Chính xác

- **Câu 9:**

RSA là giải thuật:

A. Mã công khai

B. Là tên của một tổ chức quốc tế về mã hóa

C. Mã khóa riêng

D. Tất cả đều sai

Sai **A** là đáp án đúng

- **Câu 10:**

Một trong hai cách tiếp cận tấn công mã đối xứng:

A. Tất cả đều sai

B. Tấn công tìm khóa

C. Tấn công duyệt toàn bộ

D. Tấn công tìm bản rõ

Sai **C** là đáp án đúng

- **Câu 11:**

Timestamp trong message:

A. Dùng để ghi nhận số lần trao đổi

B. Dùng để xác định thời gian hết hạn

C. Dùng để cho phép giao dịch

D. Tất cả đều đúng

Chính xác

- **Câu 12:**

Tích của 2 phép thế:

A. Tương đương với 2 phép hoán vị

B. Cho ta 1 phép thế phức tạp hơn

C. Thường dung trong mã hiện đại

D. Là một phép thế

Sai **D** là đáp án đúng

- **Câu 13:**

Mã khóa công khai:

A. Dùng 1 khóa để mã hóa và 1 khóa để giải mã

B. Có thể dung khóa public để mã hóa

C. A và B đều đúng

D. A và B đều sai

Sai **C** là đáp án đúng

- **Câu 14:**

Trong các thư mục tấn công RSA được lưu ý, không có:

A. Tấn công tính toán thời gian

B. Tấn công toán học

C. Tấn công bản rõ

D. Tấn công brute force

Sai **C** là đáp án đúng

- **Câu 15:**

Chỉ phát biểu sai. Mã đường cong elip:

A. Ít tốn vùng nhớ do xử lý ít hơn RSA

B. Dung khóa công cộng và khóa riêng để tính toán khóa phiên

C. Các tính toán là tương đương

D. Độ an toàn ít hơn RSA

Sai **D** là đáp án đúng

- **Câu 16:**

X=Ek(Y). Bản mã là:

A. Y

B. D

C. K

D. X

Sai **D** là đáp án đúng

- **Câu 17:**

Phát biểu nào là sai? Hàm hash:

A. Thường dung với lý do là thời gian mã hóa

B. Kết quả phụ thuộc mẫu tin

C. Thường dung để tạo chữ ký điện tử

D. Kích thước kết quả có độ dài phụ thuộc vào mẫu tin

Sai **D** là đáp án đúng

- **Câu 18:**

Trong giải thuật SHA 512, 80 từ:

A. Được tạo ra mặc định

B. Được tạo ra từ toàn bộ messenger

C. Được tạo a từ một phần của messenger

D. Tất cả đều sai

Chính xác

- **Câu 19:**

Trong mô hình ma trận truy cập ,"namesalary"....:

A. Time-Dependent

B. Date-Dependent

C. Context-Dependent

D. History-Dependent

Sai **C** là đáp án đúng

- **Câu 20:**

Chứng nhận chứa:

A. Chữ ký

B. Thông tin thuật toán tạo mã khoá

C. Thuật toán tạo chữ ký

D. Tất cả đều đúng

Sai **D** là đáp án đúng

- **Câu 21:**

Thám mã khi không biết khoá:

A. Bài toán dễ

B**. Bài toán khó**

C. A & B sai vì phụ thuộc vào khoá

D. A & B sai vì phụ thuộc vào giải thuật

Chính xác

- **Câu 22:**

Mã Ceaser của party là:

A. Sduwb

B. Tduwb

C. Teuwb

D. Tất cả đều có thể phụ thuộc vào

Sai **A** là đáp án đúng

- **Câu 23:**

Phát biểu sai? Kerberos:

A. Đáp ứng yêu cầu không chối cãi

B. Có thể bị tấn công

C. Có thể bị tấn công Password

D. Tất cả đều sai

Sai **A** là đáp án đúng

- **Câu 24:**

Khoá riêng có đặc điểm:

A. Thời gian thực hiện chậm

B. **Không** an toàn

C. Được thay thế bằng khoá công khai

D. Thời gian thực hiện nhanh

Chính xác

- **Câu 25:**

DAC trong DBMS có mấy mức:

A. 1 mức

B. **2 mức**

C. 3 mức

D. 5 mức

Chính xác

(I) **Câu 1:**

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

A. **Protocol an**alyzer

B. Subnetting

C. Proxy server

D. tmNetwork address translation (NAT)

Chính xác

(II) Câu 2:

Mã cổ điển là mã:

A. Mã đối xứng

B. Mã thay thế

C. Mã có hai khoá là khoá

D. Hoán vị

Sai **A** là đáp án đúng

(III) Câu 3:

Nên cài mức truy cập mặc định là mức nào sau đây?

A. Full access

B. No access

C. Read access

D. Write access

Sai **B** là đáp án đúng

(IV) Câu 4:

Quyền truy cập nào cho phép ta lưu giữ một tập tin?

A. Đọc

B. Sao chép

C. Hiệu chỉnh

D. Ghi

Sai **D** là đáp án đúng

(V) Câu 5:

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

A. Các **máy chủ ảo rẻ hơn các** máy chủ vật lý của chúng

B. 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

C. Các thiết bị bảo mật vật lý không phải lúc nào cũng được thiết kế để bảo vệ các hệ thống ảo

D. Di chuyển trực tiếp có thể di chuyển ngay lập tức một máy chủ ảo hóa sang một trình siêu giám sát khác

Chính xác

(VI) Câu 6:

Quyền truy cập nào cho phép ta hiệu chỉnh thuộc tính của một tập tin?

A. Hiệu **chỉnh (Modify**)

B. Sao chép (Copy)

C. Thay đổi (Change)

D. Biên tập (Edit)

Chính xác

(VII) Câu 7:

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

A. Kết nối chúng với các thiết bị switch và router khác

B. Sử dụng VLAN

C. Sử dụng mặt nạ mạng con

D. Không thể tách người dùng trên mạng

Sai **A** là đáp án đúng

(VIII) Câu 8:

Chính sách tài khoản nào nên được thiết lập để ngăn chặn các cuộc tấn công ác ý vào tài khoản của user?

A. Hạn chế thời gian

B. Ngày hết hạn tài khoản

C. Giới hạn số lần logon

D. Disable tài khoản không dùng đến

Sai **C** là đáp án đúng

(IX) Câu 9:

Chiều dài tối thiểu của mật khẩu cần phải là:

A. 12 đến 15 ký tự

B. 3 đến 5 ký tự

C. **8 ký tự**

D. 1 đến 3 ký tự

Chính xác

(X) Câu 10:

Một IP flood theo các host phát tán trực tiếp đến một Web server là một ví dụ của loại tấn công gì?

A. DoS phân tán (DDoS)

B. Tấn công IP

C. Trojan Hors

D. **A và B đúng**

Chính xác

(XI) Câu 11:

Giao thức nào an toàn nhất để chuyển tệp?

A. SFTP

B. SCP

C. FTPS

D. FTP

Sai **A** là đáp án đúng

(XII) Câu 12:

Để ngăn tấn công DoS, một quản trị mạng chặn nguồn IP với tường lửa, nhưng tấn công vẫn tiếp diễn. Điều gì có khả năng xảy ra nhất?

A. Sâu DoS đã lây nhiễm cục bộ

B. Phần mềm Antivirus cần được cài đặt trên máy chủ đích

C. A và B đều có thể xảy ra

D. A và B đều không thể xảy ra

Sai **C** là đáp án đúng

(XIII) Câu 13:

Các loại khoá mật mã nào sau đây dễ bị crack nhất?

A. 128 bit

B. **40 bit**

C. 256 bit

D. 56 bit

Chính xác

(XIV) Câu 14:

Cách nào sau đây là tốt nhất để chống lại điểm yếu bảo mật trong phần mềm HĐH?

A. **Cài đặt bản** service pack mới nhất

B. Cài đặt lại HĐH thông dụng

C. Sao lưu hệ thống thường xuyên

D. Shut down hệ thống khi không sử dụng

Chính xác

(XV) Câu 15:

Các mật khẩu nào sau đây là khó phá nhất đối với một hacker?

A. password83

B. reception

C. !$aLtNb83

D. LaT3r

Sai **C** là đáp án đúng

(XVI) Câu 16:

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

A. DNS poisoning

B. DNS replay

C. DNS masking

D. DNS forwarding

Sai **A** là đáp án đúng

(XVII) Câu 17:

Các tập tin nào sau đây có khả năng chứa virus nhất ?

A. database.dat

B. bigpic.jpeg

C. note.txt

D. **picture.gif.e**xe

Chính xác

(XVIII) Câu 18:

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

A. Access log

B. Event log

C. Audit log

D. SysFile log

Sai **A** là đáp án đúng

(XIX) Câu 19:

Loại mã nguồn độc hại nào có thể được cài đặt song không gây tác hại cho đến khi một hoạt động nào đó được kích hoạt?

A. Sâu

B. Trojan horse

C. Logic bomb

D. Stealth virus

Sai **B** là đáp án đúng

(XX) Câu 20:

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

A. Với **máy chủ S**MTP

B. Trên máy chủ POP3

C. Trên máy khách lưu trữ cục bộ

D. Trên máy chủ proxy

Chính xác

(XXI) Câu 21:

Trong suốt quá trình kiểm định một bản ghi hệ thống máy chủ, các mục nào sau đây có thể được xem như là một khả năng đe dọa bảo mật?

A. **Năm lần nổ lực** login thất bại trên tài khoản "jsmith"

B. Hai lần login thành công với tài khoản Administrator

C. Năm trăm ngàn công việc in được gởi đến một máy in

D. Ba tập tin mới được lưu trong tài khoản thư mục bởi người sử dụng là "finance"

Chính xác

(XXII) Câu 22:

Phương pháp thông tin truy cập từ xa nào được xem như kết nối điển hình đến Internet mọi lúc,nó làm gia tăng rủi ro bảo mật do luôn mở đối với mọi cuộc tấn công?

A. Cable modem & DSL

B. Dial-up

C. Dial-up

D. SSH

Sai **C** là đáp án đúng

(XXIII) Câu 23:

Tính năng bảo mật nào có thể được sử dụng đối với một máy trạm quay số truy cập từ xa sử dụng một username và mật khẩu?

A. Mã **hóa số đ**iện thoại

B. Kiểm tra chuỗi modem

C. Hiển thị gọi

D. Gọi lại (Call back)

Chính xác

(XXIV) Câu 24:

Tiện ích nào sau đây là một phương thức bảo mật truy cập từ xa tốt hơn telnet?

A. SSL

B. **SSH**

C. IPSec

D. VPN

Chính xác

(XXV) Câu 25:

Các giao thức đường hầm nào sau đây chỉ làm việc trên các mạng IP?

A. SSH

B. IPX

C. L2TP

D. PPTP

Sai **C** là đáp án đúng

Câu 1:

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

A. Protocol analyzer

B. Subnetting

C. Proxy server

D. tmNetwork address translation (NAT)

Chính xác

Câu 2:

Mã cổ điển là mã:

A. Mã đối xứng

B. Mã thay thế

C. Mã có hai khoá là khoá

D. Hoán vị

Sai A là đáp án đúng

Câu 3:

Nên cài mức truy cập mặc định là mức nào sau đây?

A. Full access

B. No access

C. Read access

D. Write access

Sai B là đáp án đúng

Câu 4:

Quyền truy cập nào cho phép ta lưu giữ một tập tin?

A. Đọc

B. Sao chép

C. Hiệu chỉnh

D. Ghi

Sai D là đáp án đúng

Câu 5:

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

A. Các máy chủ ảo rẻ hơn các máy chủ vật lý của chúng

B. 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

C. Các thiết bị bảo mật vật lý không phải lúc nào cũng được thiết kế để bảo vệ các hệ thống ảo

D. Di chuyển trực tiếp có thể di chuyển ngay lập tức một máy chủ ảo hóa sang một trình siêu giám sát khác

Chính xác

Câu 6:

Quyền truy cập nào cho phép ta hiệu chỉnh thuộc tính của một tập tin?

A. Hiệu chỉnh (Modify)

B. Sao chép (Copy)

C. Thay đổi (Change)

D. Biên tập (Edit)

Chính xác

Câu 7:

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

A. Kết nối chúng với các thiết bị switch và router khác

B. Sử dụng VLAN

C. Sử dụng mặt nạ mạng con

D. Không thể tách người dùng trên mạng

Sai A là đáp án đúng

Câu 8:

Chính sách tài khoản nào nên được thiết lập để ngăn chặn các cuộc tấn công ác ý vào tài khoản của user?

A. Hạn chế thời gian

B. Ngày hết hạn tài khoản

C. Giới hạn số lần logon

D. Disable tài khoản không dùng đến

Sai C là đáp án đúng

Câu 9:

Chiều dài tối thiểu của mật khẩu cần phải là:

A. 12 đến 15 ký tự

B. 3 đến 5 ký tự

C. 8 ký tự

D. 1 đến 3 ký tự

Chính xác

Câu 10:

Một IP flood theo các host phát tán trực tiếp đến một Web server là một ví dụ của loại tấn công gì?

A. DoS phân tán (DDoS)

B. Tấn công IP

C. Trojan Hors

D. A và B đúng

Chính xác

Câu 11:

Giao thức nào an toàn nhất để chuyển tệp?

A. SFTP

B. SCP

C. FTPS

D. FTP

Sai A là đáp án đúng

Câu 12:

Để ngăn tấn công DoS, một quản trị mạng chặn nguồn IP với tường lửa, nhưng tấn công vẫn tiếp diễn. Điều gì có khả năng xảy ra nhất?

A. Sâu DoS đã lây nhiễm cục bộ

B. Phần mềm Antivirus cần được cài đặt trên máy chủ đích

C. A và B đều có thể xảy ra

D. A và B đều không thể xảy ra

Sai C là đáp án đúng

Câu 13:

Các loại khoá mật mã nào sau đây dễ bị crack nhất?

A. 128 bit

B. 40 bit

C. 256 bit

D. 56 bit

Chính xác

Câu 14:

Cách nào sau đây là tốt nhất để chống lại điểm yếu bảo mật trong phần mềm HĐH?

A. Cài đặt bản service pack mới nhất

B. Cài đặt lại HĐH thông dụng

C. Sao lưu hệ thống thường xuyên

D. Shut down hệ thống khi không sử dụng

Chính xác

Câu 15:

Các mật khẩu nào sau đây là khó phá nhất đối với một hacker?

A. password83

B. reception

C. !$aLtNb83

D. LaT3r

Sai C là đáp án đúng

Câu 16:

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

A. DNS poisoning

B. DNS replay

C. DNS masking

D. DNS forwarding

Sai A là đáp án đúng

Câu 17:

Các tập tin nào sau đây có khả năng chứa virus nhất ?

A. database.dat

B. bigpic.jpeg

C. note.txt

D. picture.gif.exe

Chính xác

Câu 18:

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

A. Access log

B. Event log

C. Audit log

D. SysFile log

Sai A là đáp án đúng

Câu 19:

Loại mã nguồn độc hại nào có thể được cài đặt song không gây tác hại cho đến khi một hoạt động nào đó được kích hoạt?

A. Sâu

B. Trojan horse

C. Logic bomb

D. Stealth virus

Sai B là đáp án đúng

Câu 20:

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

A. Với máy chủ SMTP

B. Trên máy chủ POP3

C. Trên máy khách lưu trữ cục bộ

D. Trên máy chủ proxy

Chính xác

Câu 21:

Trong suốt quá trình kiểm định một bản ghi hệ thống máy chủ, các mục nào sau đây có thể được xem như là một khả năng đe dọa bảo mật?

A. Năm lần nổ lực login thất bại trên tài khoản "jsmith"

B. Hai lần login thành công với tài khoản Administrator

C. Năm trăm ngàn công việc in được gởi đến một máy in

D. Ba tập tin mới được lưu trong tài khoản thư mục bởi người sử dụng là "finance"

Chính xác

Câu 22:

Phương pháp thông tin truy cập từ xa nào được xem như kết nối điển hình đến Internet mọi lúc,nó làm gia tăng rủi ro bảo mật do luôn mở đối với mọi cuộc tấn công?

A. Cable modem & DSL

B. Dial-up

C. Dial-up

D. SSH

Sai C là đáp án đúng

Câu 23:

Tính năng bảo mật nào có thể được sử dụng đối với một máy trạm quay số truy cập từ xa sử dụng một username và mật khẩu?

A. Mã hóa số điện thoại

B. Kiểm tra chuỗi modem

C. Hiển thị gọi

D. Gọi lại (Call back)

Chính xác

Câu 24:

Tiện ích nào sau đây là một phương thức bảo mật truy cập từ xa tốt hơn telnet?

A. SSL

B. SSH

C. IPSec

D. VPN

Chính xác

Câu 25:

Các giao thức đường hầm nào sau đây chỉ làm việc trên các mạng IP?

A. SSH

B. IPX

C. L2TP

D. PPTP

Sai C là đáp án đúng

(XXVI) Câu 1:

Proxy ngược là gì?

A. Định **tuyến các yêu cầu** đến máy chủ chính xác

B. Chỉ xử lý các yêu cầu gửi đi

C. Giống như một máy chủ proxy

D. Phải được sử dụng cùng với tường lửa

Chính xác

(XXVII) Câu 2:

Mục đích của một máy chủ RADIUS là:

A. Packet Sniffing

B. Mã hóa

C. Xác thực

D. Thỏa thuận tốc độ kết nối

Sai **C** là đáp án đúng

(XXVIII) Câu 3:

Các giao thức xác thực nào sau đây là được sử dụng trong các mạng không dây?

A. 802.1X

B. 802.11b

C. 802.11a

D. 803.1

Sai **B** là đáp án đúng

(XXIX) Câu 4:

Các giao thức nào sau đây làm việc trên lớp IP để bảo vệ thông tin IP trên mạng?

A. IPX

B. IPSec

C. SSH

D. TACACS+

Sai **B** là đáp án đúng

(XXX) Câu 5:

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

A. Nó **loại bỏ các địa chỉ** riêng khi gói rời khỏi mạng

B. Nó có thể là trạng thái trạng thái hoặc không trạng thái

C. Nó thay thế địa chỉ MAC cho địa chỉ IP

D. Nó chỉ có thể được tìm thấy trên các bộ định tuyến lõi

Chính xác

(XXXI) Câu 6:

LAC (L2TP Access Control) và LNS (L2TP Network Server)) là các thành phần của giao thức đường hầm nào?

A. IPSec

B. PPP

C. PPP

D. L2TP

Sai **D** là đáp án đúng

(XXXII) Câu 7:

Giao thức được sử dụng rộng rãi nhất để truy cập kiểu quay số đến một máy chủ từ xa là:

A. SLIP

B. SLIP

C. A và B đều đúng

D. A và B đều sai

Sai **C** là đáp án đúng

(XXXIII) Câu 8:

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

A. **Mạo danh địa c**hỉ ARP

B. Mạo danh địa chỉ MAC

C. ARP poisoning

D. MAC flooding

Chính xác

(XXXIV) Câu 9:

Kỹ thuật nào được sử dụng để bảo đảm thông tin liên lạc qua một mạng không được bảo mật?

A. T**elnet**

B. SLIP

C. VPN

D. PPP

Chính xác

(XXXV) Câu 10:

Các thiết bị nào sau đây có thể sử dụng được trên mạng không dây?

A. Máy vi tính để bàn

B. Máy tính xách tay

C. PDA

D. **Tất cả các loại** trên

Chính xác

(XXXVI) Câu 11:

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

A. **Hub**

B. Switch

C. Router

D. Load balancer

Chính xác

(XXXVII) Câu 12:

Thiết bị nào được sử dụng để cho phép các máy trạm không dây truy cập vào một mạng LAN rộng?

A. 802.11b

B. Tường lửa

C. Điểm truy cập không dây (Wiless Access Point)

D. VPN

Sai **D** là đáp án đúng

(XXXVIII) Câu 13:

Các lỗ hổng bảo mật trên hệ thống là do?

A. Dịch vụ **cung cấp, bản** thân hệ điều hành và con người tạo ra

B. Dịch vụ cung cấp

C. Bản thân hệ điều hành

D. Con người tạo ra

Chính xác

(XXXIX) Câu 14:

Các chuẩn giao thức mạng không dây nào sau đây phân phối nội dung Wireless Markup Language (WML) đến các ứng dụng Web trên các thiết bị cầm tay (PDA)?

A. **WAP**

B. WEP

C. 802.11g

D. SSL

Chính xác

(XL) Câu 15:

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

A. Hợp lý

B. Dựa trên mạng con

C. Trực tiếp đến trung tâm

D. Chỉ xung quanh công tắc lõi

Chính xác

(XLI) Câu 16:

Các chuẩn giao thức mạng không dây IEEE nào sau đây là phổ biến nhất ?

A. 802.11b

B. 802.11a

C. 802.11g

D. Tất cả đều đúng

Sai **D** là đáp án đúng

(XLII) Câu 17:

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

A. **Nó loại bỏ các gói** không mong muốn

B. Nó lọc dựa trên giao thức

C. Nó che dấu địa chỉ IP của thiết bị NAT

D. NAT không cải thiện an ninh

Chính xác

(XLIII) Câu 18:

Mức mã hóa WEP nào nên được thiết lập trên một mạng 802.11b?

A**. 128 bit**

B. 40 bit

C. 28 bit

D. 16 bit

Chính xác

(XLIV) Câu 19:

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

A. **Phát hiện xâm** nhập

B. Lọc URL

C. Kiểm tra phần mềm độc hại

D. Kiểm tra nội dung

Chính xác

(XLV) Câu 20:

Cơ cấu bảo mật mạng không dây nào sau đây là ít an toàn nhất?

A. VPN

B. Mã hóa WEP 40 bit

C. Bảo mật định danh mạng

D. Mã hóa WEP 128 bit

Sai C là đáp án đúng

(XLVI) Câu 21:

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

A. **Lọc các gói dựa trê**n cài đặt giao thức

B. Ẩn các trang HTTP lỗi

C. Xóa tiêu đề định danh máy chủ khỏi HTTP responses

D. Tấn công từ chối dịch vụ (dos)

Chính xác

(XLVII) Câu 22:

Bộ lọc địa chỉ MAC được định nghĩa như:

A. Tường lửa cá nhân

B. Ngăn chặn truy cập từ một địa chỉ MAC nhất định

C. Được phép truy cập đến một địa chỉ MAC nhất định

D. Tất cả đều đúng

Sai **D** là đáp án đúng

(XLVIII) Câu 23:

Giao thức SSL dùng để:

A. **Cung cấp bảo mật** cho dữ liệu lưu thông trên dịch vụ HTTP

B. Cung cấp bảo mật cho thư điện tử

C. Cung cấp bảo mật cho Web

D. Cung cấp bảo mật cho xác thực người dùng vào các hệ thống vận hành trên Flatform Window

Chính xác

(XLIX) Câu 24:

Phương pháp điều khiển truy cập có hiệu quả và an toàn nhất đối với mạng không dây là:

A. Mã hóa WEP 40 bit

B. VPN

C. Nhận dạng bảo mật mạng

D. Mã hóa WEP 128 bit

Sai **C** là đáp án đúng

(L) Câu 25:

Cơ cấu bảo mật nào sau đây được sử dụng với chuẩn không dây WAP?

A. W**TLS**

B. SSL

C. HTTPS

D. Mã hóa WEP

Chính xác

Câu 1:

Proxy ngược là gì?

A. Định tuyến các yêu cầu đến máy chủ chính xác

B. Chỉ xử lý các yêu cầu gửi đi

C. Giống như một máy chủ proxy

D. Phải được sử dụng cùng với tường lửa

Chính xác

Câu 2:

Mục đích của một máy chủ RADIUS là:

A. Packet Sniffing

B. Mã hóa

C. Xác thực

D. Thỏa thuận tốc độ kết nối

Sai C là đáp án đúng

Câu 3:

Các giao thức xác thực nào sau đây là được sử dụng trong các mạng không dây?

A. 802.1X

B. 802.11b

C. 802.11a

D. 803.1

Sai B là đáp án đúng

Câu 4:

Các giao thức nào sau đây làm việc trên lớp IP để bảo vệ thông tin IP trên mạng?

A. IPX

B. IPSec

C. SSH

D. TACACS+

Sai B là đáp án đúng

Câu 5:

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

A. Nó loại bỏ các địa chỉ riêng khi gói rời khỏi mạng

B. Nó có thể là trạng thái trạng thái hoặc không trạng thái

C. Nó thay thế địa chỉ MAC cho địa chỉ IP

D. Nó chỉ có thể được tìm thấy trên các bộ định tuyến lõi

Chính xác

Câu 6:

LAC (L2TP Access Control) và LNS (L2TP Network Server)) là các thành phần của giao thức đường hầm nào?

A. IPSec

B. PPP

C. PPP

D. L2TP

Sai D là đáp án đúng

Câu 7:

Giao thức được sử dụng rộng rãi nhất để truy cập kiểu quay số đến một máy chủ từ xa là:

A. SLIP

B. SLIP

C. A và B đều đúng

D. A và B đều sai

Sai C là đáp án đúng

Câu 8:

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

A. Mạo danh địa chỉ ARP

B. Mạo danh địa chỉ MAC

C. ARP poisoning

D. MAC flooding

Chính xác

Câu 9:

Kỹ thuật nào được sử dụng để bảo đảm thông tin liên lạc qua một mạng không được bảo mật?

A. Telnet

B. SLIP

C. VPN

D. PPP

Chính xác

Câu 10:

Các thiết bị nào sau đây có thể sử dụng được trên mạng không dây?

A. Máy vi tính để bàn

B. Máy tính xách tay

C. PDA

D. Tất cả các loại trên

Chính xác

Câu 11:

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

A. Hub

B. Switch

C. Router

D. Load balancer

Chính xác

Câu 12:

Thiết bị nào được sử dụng để cho phép các máy trạm không dây truy cập vào một mạng LAN rộng?

A. 802.11b

B. Tường lửa

C. Điểm truy cập không dây (Wiless Access Point)

D. VPN

Sai D là đáp án đúng

Câu 13:

Các lỗ hổng bảo mật trên hệ thống là do?

A. Dịch vụ cung cấp, bản thân hệ điều hành và con người tạo ra

B. Dịch vụ cung cấp

C. Bản thân hệ điều hành

D. Con người tạo ra

Chính xác

Câu 14:

Các chuẩn giao thức mạng không dây nào sau đây phân phối nội dung Wireless Markup Language (WML) đến các ứng dụng Web trên các thiết bị cầm tay (PDA)?

A. WAP

B. WEP

C. 802.11g

D. SSL

Chính xác

Câu 15:

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

A. Hợp lý

B. Dựa trên mạng con

C. Trực tiếp đến trung tâm

D. Chỉ xung quanh công tắc lõi

Chính xác

Câu 16:

Các chuẩn giao thức mạng không dây IEEE nào sau đây là phổ biến nhất ?

A. 802.11b

B. 802.11a

C. 802.11g

D. Tất cả đều đúng

Sai D là đáp án đúng

Câu 17:

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

A. Nó loại bỏ các gói không mong muốn

B. Nó lọc dựa trên giao thức

C. Nó che dấu địa chỉ IP của thiết bị NAT

D. NAT không cải thiện an ninh

Chính xác

Câu 18:

Mức mã hóa WEP nào nên được thiết lập trên một mạng 802.11b?

A. 128 bit

B. 40 bit

C. 28 bit

D. 16 bit

Chính xác

Câu 19:

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

A. Phát hiện xâm nhập

B. Lọc URL

C. Kiểm tra phần mềm độc hại

D. Kiểm tra nội dung

Chính xác

Câu 20:

Cơ cấu bảo mật mạng không dây nào sau đây là ít an toàn nhất?

A. VPN

B. Mã hóa WEP 40 bit

C. Bảo mật định danh mạng

D. Mã hóa WEP 128 bit

Sai C là đáp án đúng

Câu 21:

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

A. Lọc các gói dựa trên cài đặt giao thức

B. Ẩn các trang HTTP lỗi

C. Xóa tiêu đề định danh máy chủ khỏi HTTP responses

D. Tấn công từ chối dịch vụ (dos)

Chính xác

Câu 22:

Bộ lọc địa chỉ MAC được định nghĩa như:

A. Tường lửa cá nhân

B. Ngăn chặn truy cập từ một địa chỉ MAC nhất định

C. Được phép truy cập đến một địa chỉ MAC nhất định

D. Tất cả đều đúng

Sai D là đáp án đúng

Câu 23:

Giao thức SSL dùng để:

A. Cung cấp bảo mật cho dữ liệu lưu thông trên dịch vụ HTTP

B. Cung cấp bảo mật cho thư điện tử

C. Cung cấp bảo mật cho Web

D. Cung cấp bảo mật cho xác thực người dùng vào các hệ thống vận hành trên Flatform Window

Chính xác

Câu 24:

Phương pháp điều khiển truy cập có hiệu quả và an toàn nhất đối với mạng không dây là:

A. Mã hóa WEP 40 bit

B. VPN

C. Nhận dạng bảo mật mạng

D. Mã hóa WEP 128 bit

Sai C là đáp án đúng

Câu 25:

Cơ cấu bảo mật nào sau đây được sử dụng với chuẩn không dây WAP?

A. WTLS

B. SSL

C. HTTPS

D. Mã hóa WEP

Chính xác

(LI) Câu 1:

Thiết bị nào sử dụng bộ lọc gói và các quy tắc truy cập để kiểm soát truy cập đến các mạng riêng từ các mạng công cộng , như là Internet?

A. Điểm truy cập không dây

B. Router

C. Tường lửa

D. Switch

Sai **C** là đáp án đúng

(LII) Câu 2:

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

A. Thiết bị không an toàn

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

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

D. Tất cả các nguy cơ trên

Sai **D** là đáp án đúng

(LIII) Câu 3:

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?

A. **VPN**

B. WEP

C. Modem

D. Telnet

Chính xác

(LIV) Câu 4:

Để tìm bản rõ người thám mã sử dụng:c

A. **Kết hợp nhiều phươ**ng pháp tấn công khác nhau

B. Chỉ sử dụng phương pháp giải bài toán ngược

C. Sử dụng khóa bí mật

D. Vét cạn khóa

Chính xác

(LV) Câu 5:

Chức năng chính của vius là:

A. **Sống ký sin**h và lây nhiễm

B. Lây nhiễm và sinh sản

C. Tự phát triển độc lập và lây nhiễm

D. Sống ký sinh và sinh sản

Chính xác

(LVI) Câu 6:

Ứng dụng mạng nào có thể được sử dụng để phân tích và kiểm tra lưu lượng mạng?

A. IDS

B. FTP

C. Router

D. Sniffer

Sai **D** là đáp án đúng

(LVII) Câu 7:

Cần phải làm gì để bảo vệ dữ liệu trên một máy tính xách tay nếu nó bị lấy cắp?

A. Khóa đĩa mềm

B. Enable khi login và tạo mật khẩu trên HĐH

C. Lưu trữ đều đặn trên CD-ROM

D. Mã hóa dữ liệu

Sai **D** là đáp án đúng

(LVIII) Câu 8:

Ta phải làm gì để ngăn chặn một ai đó tình cờ ghi đè lên dữ liệu trên một băng từ?

A. Xóa nó bằng nam châm

B. Dán nhãn cẩn thận

C. Thiết lập tab "Write-protect "

D. Lưu giữ nó tại chỗ

Sai **C** là đáp án đúng

(LIX) Câu 9:

Hành vi nào sau đây ảnh hưởng đến tính bảo mật hệ thống thông tin:

A. **Một người d**ùng có thể xem thông tin của các người dùng khác

B. Virus xóa mất các tập tin trên đĩa cứng

C. Mất điện thường xuyên làm hệ thống máy tính làm việc gián đoạn

D. Tất cả các hành vi trên

Chính xác

(LX) Câu 10:

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

A. **Mật mã công k**hai chậm hơn

B. Tốc độ như nhau

C. Mật mã công khai nhanh hơn

D. Không so sánh được

Chính xác

(LXI) Câu 11:

Giải mã là:

A. **Quá trình biến đ**ổi thông tin từ dạng không đọc được sang dạng đọc được

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

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

D. Giấu thông tin để không nhìn thấy

Chính xác

(LXII) Câu 12:

Thám mã là gì?

A. Quá **trình tấn công hệ** mật mã để tìm bản rõ và khóa bí mật

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

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

D. Giấu thông tin để không nhìn thấy

Chính xác

(LXIII) Câu 13:

Mã hóa là gì?

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

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

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

D. Giấu thông tin để không nhìn thấy

Chính xác

(LXIV) Câu 14:

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

A. **Virus xóa mất các t**ập tin trên đĩa cứng

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

C. Mất điện thường xuyên làm hệ thống máy tính làm việc gián đoạn

D. Tất cả các hành vi trên

Chính xác

(LXV) Câu 15:

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

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

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

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

D. Tất cả đều sai

Chính xác

(LXVI) Câu 16:

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

A. Một **hệ thống không k**ết nối vào mạng Internet thì không có các nguy cơ tấn công

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

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

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

Chính xác

(LXVII) Câu 17:

Trojan là một phương thức tấn công kiểu:

A. Điều **khiển máy tính nạn n**hân từ xa thông qua phần mềm cài sẵn trong máy nạn nhân

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

C. Đánh cắp dữ liệu của nạn nhân truyền trên mạng

D. Tấn công làm tê liệt hệ thống mạng của nạn nhân

Chính xác

(LXVIII) Câu 18:

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:

A. Do **Phần mềm An**ti Virus trên máy tấn công đã khóa (blocked) không cho thi hành

B. Do không kết nối được tới máy nạn nhân

C. Do không cài đặt công cụ Metasploit vào ổ

D. C: Do máy nạn nhân không cho phép tấn công

Chính xác

(LXIX) Câu 19:

Virus máy tính không thể lây lan qua:

A. **Đĩa CD**

B. Mạng máy tính

C. Thẻ nhớ Flash

D. Lưu trữ USB

Chính xác

(LXX) Câu 20:

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

A. Có **thể hạn chế tro**ng bằng cách lập trình

B. Chỉ có thể dùng tường lửa

C. Hiện nay đã có cách phòng chống hiệu quả

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

Chính xác

(LXXI) Câu 21:

Social Engineering là gì?

A. Kĩ **thuật sai khiến mọi n**gười thực hiện hành vi nào đó hoặc tiết lộ thông tin bí mật

B. 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

C. 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

D. 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

Chính xác

(LXXII) Câu 22:

Rootkit là gì?

A. **Rootkit là được th**iết kế để qua mặt các phương pháp bảo mật máy tính

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

C. Tên mặc định của thư mục UNIX

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

Chính xác

(LXXIII) Câu 23:

SQL Injection là gì?

A. 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

B. Một ngôn ngữ lập trình đa năng

C. 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

D. 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

Chính xác

(LXXIV) Câu 24:

Có thể ngăn chặn SQL Injection bằng cách nào?

A. **Bắt lỗi dữ liệu đầu vào c**ủa người dùng (đảm bảo rằng người dùng không thể nhập bất cứ điều gì khác ngoài những gì họ được cho phép)

B. Đặt mã của bạn ở chế độ công khai

C. Không sử dụng SQL nữa

D. Tất cả những cách trên.

Chính xác

(LXXV) Câu 25:

Cross-site scripting là gì?

A. **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

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

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

D. 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

Chính xác

Câu 1:

Thiết bị nào sử dụng bộ lọc gói và các quy tắc truy cập để kiểm soát truy cập đến các mạng riêng từ các mạng công cộng , như là Internet?

A. Điểm truy cập không dây

B. Router

C. Tường lửa

D. Switch

Sai C là đáp án đúng

Câu 2:

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

A. Thiết bị không an toàn

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

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

D. Tất cả các nguy cơ trên

Sai D là đáp án đúng

Câu 3:

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?

A. VPN

B. WEP

C. Modem

D. Telnet

Chính xác

Câu 4:

Để tìm bản rõ người thám mã sử dụng:c

A. Kết hợp nhiều phương pháp tấn công khác nhau

B. Chỉ sử dụng phương pháp giải bài toán ngược

C. Sử dụng khóa bí mật

D. Vét cạn khóa

Chính xác

Câu 5:

Chức năng chính của vius là:

A. Sống ký sinh và lây nhiễm

B. Lây nhiễm và sinh sản

C. Tự phát triển độc lập và lây nhiễm

D. Sống ký sinh và sinh sản

Chính xác

Câu 6:

Ứng dụng mạng nào có thể được sử dụng để phân tích và kiểm tra lưu lượng mạng?

A. IDS

B. FTP

C. Router

D. Sniffer

Sai D là đáp án đúng

Câu 7:

Cần phải làm gì để bảo vệ dữ liệu trên một máy tính xách tay nếu nó bị lấy cắp?

A. Khóa đĩa mềm

B. Enable khi login và tạo mật khẩu trên HĐH

C. Lưu trữ đều đặn trên CD-ROM

D. Mã hóa dữ liệu

Sai D là đáp án đúng

Câu 8:

Ta phải làm gì để ngăn chặn một ai đó tình cờ ghi đè lên dữ liệu trên một băng từ?

A. Xóa nó bằng nam châm

B. Dán nhãn cẩn thận

C. Thiết lập tab "Write-protect "

D. Lưu giữ nó tại chỗ

Sai C là đáp án đúng

Câu 9:

Hành vi nào sau đây ảnh hưởng đến tính bảo mật hệ thống thông tin:

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

B. Virus xóa mất các tập tin trên đĩa cứng

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

D. Tất cả các hành vi trên

Chính xác

Câu 10:

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

A. Mật mã công khai chậm hơn

B. Tốc độ như nhau

C. Mật mã công khai nhanh hơn

D. Không so sánh được

Chính xác

Câu 11:

Giải mã là:

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

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

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

D. Giấu thông tin để không nhìn thấy

Chính xác

Câu 12:

Thám mã là gì?

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

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

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

D. Giấu thông tin để không nhìn thấy

Chính xác

Câu 13:

Mã hóa là gì?

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

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

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

D. Giấu thông tin để không nhìn thấy

Chính xác

Câu 14:

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

A. Virus xóa mất các tập tin trên đĩa cứng

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

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

D. Tất cả các hành vi trên

Chính xác

Câu 15:

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

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

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

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

D. Tất cả đều sai

Chính xác

Câu 16:

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

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

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

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

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

Chính xác

Câu 17:

Trojan là một phương thức tấn công kiểu:

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

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

C. Đánh cắp dữ liệu của nạn nhân truyền trên mạng

D. Tấn công làm tê liệt hệ thống mạng của nạn nhân

Chính xác

Câu 18:

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:

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

B. Do không kết nối được tới máy nạn nhân

C. Do không cài đặt công cụ Metasploit vào ổ

D. C: Do máy nạn nhân không cho phép tấn công

Chính xác

Câu 19:

Virus máy tính không thể lây lan qua:

A. Đĩa CD

B. Mạng máy tính

C. Thẻ nhớ Flash

D. Lưu trữ USB

Chính xác

Câu 20:

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

A. Có thể hạn chế trong bằng cách lập trình

B. Chỉ có thể dùng tường lửa

C. Hiện nay đã có cách phòng chống hiệu quả

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

Chính xác

Câu 21:

Social Engineering là gì?

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

B. 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

C. 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

D. 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

Chính xác

Câu 22:

Rootkit là gì?

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

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

C. Tên mặc định của thư mục UNIX

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

Chính xác

Câu 23:

SQL Injection là gì?

A. 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

B. Một ngôn ngữ lập trình đa năng

C. 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

D. 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

Chính xác

Câu 24:

Có thể ngăn chặn SQL Injection bằng cách nào?

A. 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)

B. Đặt mã của bạn ở chế độ công khai

C. Không sử dụng SQL nữa

D. Tất cả những cách trên.

Chính xác

Câu 25:

Cross-site scripting là gì?

A. 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

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

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

D. 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

Chính xác

- **Câu 1:**

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

- A. Directory traversal
- B. SQL injection
- C. Command injection
- D. XML injection

Chính xác

- **Câu 2:**

Kiến trúc TCP / IP sử dụng bao nhiêu lớp?

- A. 4
- B. 5
- C. 6

D. 7

Chính xác

- **Câu 3:**

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

A. Content-length

B. Accept-Language

C. Referer

D. Response splitting

Chính xác

- **Câu 4:**

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

A. XML

B. ICMP

C. HTTP

D. HTML

Chính xác

- **Câu 5:**

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

A. HTTP header

B. XML manipulation

C. HTML packet

D. SQL injection

Chính xác

- **Câu 6:**

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

A. Push flood

B. SYN flood

C. Ping flood

D. Smurf

Chính xác

- **Câu 7:**

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

A. Để chèn câu lệnh SQL thông qua đầu vào người dùng chưa được lọc

B. Để máy chủ SQL tấn công trình duyệt web máy khách

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

D. Để liên kết các máy chủ SQL thành một botnet

Chính xác

- **Câu 8:**

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

A. Định dạng lại ổ cứng của máy chủ ứng dụng web

B. Hiển thị danh sách số điện thoại của khách hàng

C. Khám phá tên của các trường khác nhau trong bảng

D. Xóa bảng cơ sở dữ liệu

Chính xác

- **Câu 9:**

Tấn công phát lại là gì?

A. Tạo bản sao truyền để sử dụng sau này

B. Được coi là một loại tấn công dos

C. Có thể được ngăn chặn bằng cách vá trình duyệt web

D. Replay các cuộc tấn công hơn và hơn để lũ máy chủ

Chính xác

- **Câu 10:**

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

A. Flash cookie

B. Session cookie

C. Ram cookie

D. Secure cookie

Chính xác

- **Câu 11:**

Plug-in trình duyệt là gì?

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

B. Có chức năng bổ sung cho toàn bộ trình duyệt

C. Chỉ hoạt động trên máy chủ web

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

Chính xác

- **Câu 12:**

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

A. Integer overflow

B. Buffer overflow

C. Real number

D. Heap size

Chính xác

- **Câu 13:**

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

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

B. Xóa tập tin chữ ký tràn bộ đệm

C. Làm hỏng nhân để máy tính không thể khởi động lại

D. Đặt virus vào nhân (kernel)

Chính xác

- **Câu 14:**

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

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

B. Mã SQL được sử dụng trong một cuộc tấn công XSS

C. XSS yêu cầu sử dụng trình duyệt

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

Chính xác

- **Câu 15:**

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

A. cookie của bên thứ ba

B. cookie chính chủ

C. cookie của bên thứ hai

D. cookie của bên thứ tư

Chính xác

- **Câu 16:**

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?

A. transitive

B. privilege rights

C. heap spray

D. vertical escalation

Chính xác

- **Câu 17:**

Trojan Horse là gì?

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

B. Gây hại như mã giả mạo hoặc thay thế mã hợp pháp

C. 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

D. 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

Chính xác

- **Câu 18:**

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

A. Tấn công từ xa

B. Tấn công truy cập vật lý

C. Truy cập địa phương

D. Tấn công nội bộ

Chính xác

- **Câu 19:**

Kỹ thuật tấn công phổ biến trên Web là:

A. Từ chối dịch vụ (DoS)

B. Chiếm hữu phiên làm việc

C. Tràn bộ đệm

D. Chèn câu truy vấn SQL

Chính xác

- **Câu 20:**

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

A. Mã hóa khóa và thông báo

B. Chỉ mã hóa khóa

C. Chỉ mã hóa tin nhắn

D. Chỉ mã hóa khóa DHE

Chính xác

- **Câu 21:**

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

A. SHA-3

B. SHA-2

C. SHA-4

D. SHA-5

Chính xác

- **Câu 22:**

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

A. Perfect forward secrecy

B. Trao đổi khóa công khai (PKE)

C. Elliptic Curve Diffie-Hellman (ECDH)

D. Diffie-Hellman (DH

Chính xác

- **Câu 23:**

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

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

B. 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

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

Chính xác

- **Câu 24:**

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?

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

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

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

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

Chính xác

- **Câu 25:**

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

A. Tính không từ chối(non-repudiation)

B. Tính từ bỏ(repudiation)

C. Tính toàn vẹn (integrity)

D. Tính khả dụng (availability)

Chính xác

- **Câu 1:**

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

A. RSA

B. EFS

C. Quantum computing

D. ECC

Chính xác

- **Câu 2:**

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

A. RSA

B. SHA-2

C. BTC-2

D. ME-14

Chính xác

- **Câu 3:**

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:

A. Khoá công khai của Alice

B. Khoá bí mật của Alice

C. Khoá bí mật của Bob

D. Khoá công khai của Bob

Chính xác

- **Câu 4:**

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

A. xác minh người nhận

B. chứng minh tính toàn vẹn của thông điệp

C. xác minh người gửi

D. thực thi không từ chối

Chính xác

- **Câu 5:**

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

A. Advanced Encryption Standard

B. Data Encryption Standard

C. Triple Data Encryption Standard

D. Rivest Cipher (RC) 1

Chính xác

- **Câu 6:**

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

A. Secure Shell (SSH)

B. Secure Sockets Layer (SSL)

C. Secure Hypertext Transport Protocol (SHTTP)

D. Transport Layer Security (TLS

Chính xác

- **Câu 7:**

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

A. SSL v2.0

B. TLS v1.0

C. TLS v1.1

D. TLS v1.3

Chính xác

- **Câu 8:**

Chứng chỉ số liên kết:

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

B. Khóa riêng tư của người dùng bằng khóa công cộng

C. Một khóa riêng với chữ ký số

D. Khóa công khai của người dùng bằng khóa riêng

Chính xác

- **Câu 9:**

Tiêu chuẩn mật mã khóa công khai (PKCS):

A. Được chấp nhận rộng rãi trong ngành

B. Chỉ được sử dụng để tạo khóa công khai

C. Xác định các thuật toán băm được tạo ra như thế nào Đã được thay thế bởi PKI

Chính xác

- **Câu 10:**

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

A. Trong digests

B. Trong tokens

C. Trên hệ thống của người dùng cục bộ

D. Nhúng trong chứng chỉ kỹ thuật số

Chính xác

- **Câu 11:**

Cơ sở hạ tầng khóa công khai (PKI):

A. Là quản lý chứng chỉ kỹ thuật số

B. Tạo mật mã khóa riêng

C. Yêu cầu sử dụng RA thay vì CA

D. Tự động tạo khóa công khai / riêng tư

Chính xác

- **Câu 12:**

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

A. Server digital certificate

B. Web digital certificate

C. Email web certificate

D. Personal digital certificate

Chính xác

- **Câu 13:**

Một thực thể cấp chứng chỉ kỹ thuật số là:

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

B. Cơ quan Chữ ký (Signature Authority - SA)

C. Người ký chứng chỉ (Certificate Signatory - CS)

D. Bộ ký số (Digital Signer - DS)

Chính xác

- **Câu 14:**

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:

A. Session keys

B. Encrypted signatures

C. Digital digests

D. Digital certificates

Chính xác

- **Câu 15:**

Thuật toán chia Euclid mở rộng dùng để:

A. Tính phần tử nghịch đảo của một số theo module nào đó

B. Tính nhanh một lũy thừa với số lớn

C. Kiểm tra nhanh một số nguyên tố lớn

D. Tìm đồng dư của một só theo module nào đó

Chính xác

- **Câu 16:**

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

A. (51, 5)

B. (32, 5)

C. (17,3)

D. (17, 3, 5)

Chính xác

- **Câu 17:**

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?

- A. (13,55)
- B. (5,51)
- C. 52
- D. 55

Chính xác

- **Câu 18:**

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?

- A. 37
- B. (5, 51)
- C. (55, 13)
- D. 55

Chính xác

- **Câu 19:**

DES là viết tắt của từ nào?

- A. Data encryption standard
- B. Data encryption system
- C. Data encoding standard
- D. Data encryption signature

Chính xác

- **Câu 20:**

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

A. Khóa công khai của người gửi

B. Khóa riêng của người nhận

C. Khóa riêng của người gửi

D. Khóa công khai của người nhận

Chính xác

- **Câu 21:**

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?

A. Phải thử 2127 lần, thời gian thử là 5,4 * 1018 năm

B. Phải thử 2128 lần, thời gian thử là 5,4 * 1018 năm

C. Phải thử 264 lần, thời gian thử là 5,4 * 1018 năm

D. Phải thử 2128 lần, thời gian thử là 18 năm

Chính xác

- **Câu 22:**

Chữ ký điện tử (số) là:

A. 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

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

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

D. Tất cả đều sai

Chính xác

- **Câu 23:**

RSA là giải thuật?

A. Mã hóa công khai

B. Là tên của một tổ chức quốc tế về mã hóa

C. Mã hóa khóa bí mật

D. Tất cả đều sai

Chính xác

- **Câu 24:**

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?

A. HGRGXV

B. GRXVCN

C. VCMHGR

D. XVHGGR

Chính xác

- **Câu 25:**

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?

A. EARDY

B. DAEGU

C. YAEDR

D. ADERU

Chính xác

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

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

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

C. Một phương pháp mã hóa thông tin bí mật

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

Trong giải thuật mã hóa DES thực hiện bao nhiêu vòng lặp? 16

Bước đầu tiên trong việc bảo mật hệ điều hành là gì? Phát triển chính sách bảo mật

Điều nào sau đây KHÔNG phải là activity phase control? Resource control

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

Một typical configuration baseline sẽ bao gồm mỗi phần sau NGOẠI TRỪ: Thực hiện đánh giá rủi ro an ninh

Md5: 128bit

Một môi trường Kerberos đầy đủ dịch vụ bao gồm: Một máy chủ Kerberos, một số máy trạm, một số máy chủ ứng dụng

Đối với Kerberos, mỗi người dùng có: Một vé TGT và mỗi vé SGT cho mỗi dịch vụ mà người dùng truy cập đến

Dịch vụ xác thực X.509 dùng mã hóa dạng gì? Mã hóa khóa công khai

Chữ ký số trong chứng chỉ X.509 được tạo dùng khóa nào sau đây: Khóa riêng của đơn vị phát hành chứng chỉ

thủ tục xác thực nào được dùng để dùng cho các kết nối có tương tác? 2, 3 chiều

Chọn phát biểu sai trong các phát biểu sau khi PGP được sử dụng trong một hệ thống Email

A. Hệ thống E-mail nói trên sẽ cung cấp các dịch vụ xác thực, bí mật, nén, tương thích e-mail và phân mảnh

B. Nếu dùng dịch vụ bí mật thì thông điệp gởi đi sẽ có mã hóa ở một số khối dữ liệu

C. Nếu chỉ dùng dịch vụ xác thực thì thông điệp gởi đi sẽ không có mã hóa ở bất kỳ khối dữ liệu nào

D. Nếu dùng dịch vụ tương thích e-mail thì mỗi nhóm 3 byte dữ liệu nhị phân được ánh xạ thành 4 ký tự ASCII

Chế độ hoạt động của PGP khi thực hiện mã hóa đối xứng là: CFB

Thuật toán mã hóa nào sau đây là phù hợp với mã hóa đối xứng của PGP: 3DES với 2 khóa, aes

Cho biết mục tiêu nào sau đây là mục tiêu thiết kế một bức tường lửa?

Tất cả thông tin từ bên trong ra bên ngoài và ngược lại phải đi qua bức tường lửa

Chỉ các loại thông tin được cấp quyền thông qua chính sách an ninh cục bộ mới được phép đi qua bức tường lửa

CHƯƠNG 3: CÁC THUẬT TOÁN MẬT MÃ

HMAC

Câu nào đúng về Hashed Message Authentication Code (HMAC)

Mã hóa khóa và thông báo

Chữ ký điện tử

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

xác minh người nhận

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

Khóa công khai của người gửi

Chữ ký điện tử (số) là :

Biến đổi mã hóa văn bản được gắn vào văn bản cho phép người nhận khác kiểm

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

Thuật toán Euclide mở rộng

Thuật toán chia Euclid mở rộng dùng để

Tính phần tử nghịch đảo của một số theo module nào đó

RSA

Thuật toán mã hóa bất đối xứng
nào an toàn nhất

RSA
Thuật toán mã hóa bất đối
xứng sử dụng số nguyên tố

RSA
Bảo mật, chứng thực và không từ
chối với mã hoá khoá công khai

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 để mã hóa thông điệp

Khoá công khai của Alice
Chứng minh rằng người dùng đã
gửi một email được gọi là.

Tính không từ chối(non-repudiation)
RSA là giải thuật

Mã hóa công khai
PKCS (Tiêu chuẩn mật mã khóa công khai Public-Key Cryptography Standard)

Một thực thể cấp chứng chỉ kỹ thuật số là.

Tổ chức phát hành chứng chỉ
(Certificate Authority - CA

Tiêu chuẩn mật mã
khóa công khai (PKCS).

Được chấp nhận rộng rãi trong ngành

Cơ sở hạ tầng khóa công

khai (PKI)

Là quản lý chứng chỉ kỹ thuật số

Điều nào trong số này KHÔNG phải là nơi

khóa có thể được lưu trữ?

Trong digests

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

Perfect forward secrecy

Mã hoá đối xứng

Để mã hóa và giải mã thông tin được trao đổi trong phiên và

để xác minh tính toàn vẹn

Sesion keys

Một hệ thống mã hóa quy ước dùng khóa dài 128bit. Nếu dùng phương phát tấn công brute force thì phải thử trung bình số lần và thời gian cần thiết để thực hiện nếu tốc độ xử lý là 1 tỷ lần trong 1 giây

P

Phải thử 2 mũ 128 lần, thời gian thử là 5,4*10 mũ 18 năm

Thuật toán mật mã đối xứng mạnh nhất

Advanced Encryption Standard

DES là viết tắt của

Data encryption standard

Trong giải thuật mã hóa

DES thực hiện số vòng lặp

16

HÀM BĂM

Phiên bản mới nhất của thuật
toán băm bảo mật là

SHA-3

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.

Mấy câu đỏ có đáp án là

1	B	21	D	41	B
2	B	22	C	42	A
3	A	23	B	43	B
4	C	24	A	44	C
5	D	25	C	45	D
6	D	26	C	46	D
7	D	27	B	47	D
8	D	28	B	48	C
9	B	29	A	49	B
10	A	30	B	50	C
11	C	31	D	51	C
12	D	32	A	52	D
13	C	33	A	53	C
14	B	34	A	54	A
15	A	35	B	55	C
16	D	36	A	56	C
17	B	37	A	57	D
18	C	38	B	58	C
19	C	39	D	59	C
20	D	40	B	60	D

Câu 1. Một đoạn mã độc được đính vào tập tin khác để thực hiện việc nhân bản, có thể là

A. Worm B. Virus

C. Logic bomb D. Trojan

Câu 2. Tại sao hackers muốn che giấu dấu vết?

A. Để ngăn ngừa kẻ khác dùng những chương trình mình đã cài đặt trong hệ thống nạn nhân

B. Để ngăn ngừa phát hiện hoặc điều tra

C. Để ngăn ngừa sự xâm nhập

D. Để không cho những hackers khác dùng công cụ của mình

Câu 3. Một loại công nghệ có thể được dùng để mã hóa giao tiếp (encrypt communication) từ điểm A

đến điểm B trong mạng không tin cậy về bảo mật:

A. VPN B. VLAN

C. NAP D. NAT

Câu 4. Hacker có thể lấy được mật khẩu mà không phải sử dụng bất cứ công cụ hay chương trình máy

tính nào, thông qua kỹ thuật

A. Backdoors B. Sniffers

C. Social Engineering D. Trojan Horses

Câu 5. Hệ thống của bạn bị đứng (stop responding) khi gõ lệnh từ bàn phím. Bạn ghi nhận việc này cứ

sau mỗi lần mở file Excel và kết nối Internet. Có thể bạn là nạn nhân của kiểu tấn công sử dụng:

A. Virus B. Worm

C. ARP Poisoning D. Logic bomb

Câu 6. Kiểu tấn công khi kẻ gian khai thác điểm yếu để can thiệp vào cơ sở dữ liệu gọi là:

A. SQL tearing B. SQL manipulation

C. SQL cracking D. SQL injection

Câu 7. Tấn công đoán mật khẩu dựa vào tự điển (dictionary attack) là dạng tấn công

A. Dùng thuật toán và các giải thuật xử lý song song

B. Dùng giải thuật RSA để thực hiện

C. Sử dụng thuật toán brute force để đoán mật khẩu người dùng

D. Thử lần lượt và tuần tự các giá trị đã được khai báo trước

Câu 8. Phát biểu nào sau đây KHÔNG là một trong những mục đích của việc quét (scanning) trong

mạng máy tính:

A. Tìm những cổng mở (open ports) B. Tìm những dịch vụ chạy trên servers mục tiêu

C. Xác định hệ điều hành D. Thu thập số phone của nhân viên

Câu 9. Giải thuật RSA khác giải thuật DES (Data Encryption Standard) ở chỗ

A. Nó không thể tạo ra được chữ ký số B. Nó dùng khóa công khai để mã hóa

C. Nó dựa trên giải thuật mã hóa khóa đối xứng D. Tất cả các câu trả lời trên đều sai

Câu 10. Chọn câu trả lời đúng cho một loại công nghệ cho phép kết nối được thiết lập giữa hai mạng máy

tính sử dụng giao thức bảo mật:

A. Tunneling B. VLAN

C. Internet D. Extranet

Câu 11. Một thông điệp như sau được gửi đi “I love you”, bên nhận nhận được thông điệp có nội dung là

“I don’t love you”, quá trình truyền thông tin đã bị can thiệp ở giữa. Tính chất nào sau đây đã bị

ảnh hưởng sau quá trình truyền tin này:

A. Tính bí mật B. Tính sẵn sàng

C. Tính toàn vẹn D. Tính bí mật và tính sẵn sàng

Câu 12. Cụm từ viết tắt CIA trong an ninh mạng, được dùng để nói về:

A. Certificate, Integrity, Authentication B. Certificate, Integrity, Availability

C. Confidentiality, Inspection, Authentication D. Confidentiality, Integrity, Availability

Câu 13. Mặt hạn chế của mã hóa đối xứng là:

A. nó dễ dàng bị kẻ gian giải mã

B. nó chạy quá chậm nên khó có thể được dùng trên thiết bị di động

C. nó đòi hỏi khóa chung đươc chia sẻ một cách bí mật

D. nó chỉ được dùng trên Unix

Câu 14. Mã hóa bất đối xứng có ưu điểm nào so với mã hóa đối xứng?

A. An toàn hơn (more secure)

B. Giải thuật có cả vai trò quản lý khóa (key management)

C. Bất cứ ai có khóa công cộng đều có thể giải mã dữ liệu.

D. Nó dùng hàm băm

Câu 15. Chữ ký số (digital signature) dùng loại mã hóa nào sau đây?

A. Hashing và asymmetric B. Asymmetric và symmetric

C. Hashing và symmetric D. Tất cả các câu trả lời trên đều sai

Câu 16. Mục đích của một DMZ trong một mạng là

A. Cung cấp những kết nối dễ dàng đến Internet mà không làm ảnh hưởng firewall

B. Cho phép những cụm máy chủ (server farms) được chia nhỏ thành những đơn vị có chức năng tương tự nhau

C. Cung cấp một nơi cài bẫy và bắt giữ hackers

D. Thực hiện vai trò như một vùng đệm giữa những mạng tin cậy (trusted networks) và không tin cậy (untrusted networks)

Câu 17. SYN flood là một ví dụ cho kiểu tấn công nào?

A. Mã độc B. Từ chối dịch vụ

C. Man-in-the-middle D. Đánh lừa (spoofing)

Câu 18. Cuộc tấn công trong đó kẻ tấn công đơn giản chỉ lắng nghe dòng dữ liệu với hy vọng sẽ lấy được

thông tin nào đó, như User ID, số thẻ tín dụng, v.v., được gọi là

A. A man-in-the-middle attack B. A denial-of-service-attack

C. A sniffing attack D. A backdoor attack

Câu 19. Kẻ tấn công gởi lại những câu lệnh (command) và mã (codes) dùng trong giao dịch tài chính để

hòng thực hiện nhiều lần giao dịch ấy, kiểu tấn công này thuộc dạng:

A. Spoofing B. Man-in-the-middle

C. Replay D. Backdoor

Câu 20. SSL có thể được dùng để bảo mật cho

A. POP3 traffic B. HTTP traffic

C. SMTP traffic D. Tất cả các câu trả lời trên đều đúng

Câu 21. SSL KHÔNG cung cấp chức năng nào sau đây?

A. Toàn vẹn dữ liệu (Data integrity services)

B. Xác thực (Authentication services)

C. Bí mật dữ liệu (Data confidentiality services)

D. Tính sẵn sàng của dữ liệu (Availability of data)

Câu 22. SSL dùng cổng nào để mang HTTPS traffic?

A. TCP port 80 B. UDP port 443

C. TCP port 443 D. TCP port 8080

Câu 23. _____ là quá trình kiểm chứng hoặc kiểm thử tính hợp lệ của định danh khai báo.

A. Identification B. Authentication

C. Authorization D. Accountability

Câu 24. Hệ thống phát hiện xâm nhập (IDS) được thiết kế chủ yếu để thực hiện chức năng nào?

A. Phát hiện hành vi bất thường (Detect abnormal activity).

B. Phát hiện hư hỏng hệ thống (Detect system failures).

C. Đánh giá hiệu năng hệ thống (Rate system performance).

D. Kiểm thử hệ thống để phát hiện điểm yếu (Test a system for vulnerabilities)

Câu 25. Cuộc tấn công khi kẻ gian tự đặt vị trí của mình giữa Client và Server, làm gián đoạn giao dịch

và chiếm quyền giao dịch này, được gọi là cuộc tấn công:

A. Man-in-the-middle

B. Spoofing

C. Session Hijacking

D. Cracking

Câu 26. Câu trả lời nào sau đây KHÔNG được xem là xâm phạm tính bí mật (confidentiality)?

A. Trộm password (stealing passwords)

B. Nghe trộm (eavesdropping)

C. Phá hoại phần cứng (hardware destruction)

D. Man-in-the-middle

Câu 27. Loại cipher nào khi thay đổi vị trí các ký tự bên trong thông điệp để tăng tính bảo mật

A. Stream cipher

B. Transposition cipher

C. Block cipher

D. Substitution cipher

Câu 28. Dùng phương pháp mã hóa hoán vị Rail Fence với depth 2, thông điệp “I MUST PASS THIS

EXAM” hãy cho biết, sau khi mã hóa, thông điệp sẽ là gì?

A. IMUSTPASSTHISEXAM B. IUTASHSXMMSPSTIEA

C. IUMSTAPSSHTISXEAM D. MAXESIHTSSAPTSUMI

Câu 29. Trong phương pháp dùng khóa bất đối xứng, Alice muốn ký chữ ký số (digital signature) và

người nhận là Bob. Để đọc chữ ký số này, Bob phải dùng đến

A. public-key của Alice B. public-key của Bob

C. private-key của Alice D. private-key của Bob

Câu 30. Trong phương pháp dùng khóa bất đối xứng, Alice muốn gởi thông điệp bí mật và người nhận là

Bob. Để thực hiện việc này, Alice phải dùng đến

A. public-key của Alice B. public-key của Bob

C. private-key của Alice D. private-key của Bob

Câu 31. Chọn câu trả lời đúng cho một phương pháp cổ điển mã hóa dùng giải thuật thay thế

(substitution):

A. Rivest, Shamir, Adleman (RSA) B. Data Encryption Standard (DES)

C. Rail Fence D. Tất cả các câu trả lời trên đều sai

Câu 32. Mục tiêu của tường lửa là gì?

A. Bảo vệ một mạng máy tính trước các nguy cơ bảo mật từ bên ngoài

B. Ngăn chặn dữ liệu lưu thông ra khỏi mạng.

C. Block SNA traffic (Systems Network Architecture)

D. Giám sát lưu thông mạng (Monitor network Traffic)

Câu 33. Một dạng tấn công dựa vào xác suất 2 thông điệp khác nhau dùng hàm băm giống nhau để cho

ra giá trị giống nhau gọi là

A. Birthday attack B. Statistic attack

C. Differential cryptanalysis attack D. Known ciphertext attack

Câu 34. Dùng Caesar cipher, mã hóa thông điệp “I will pass this exam”, kết quả sẽ là:

A. L zloo sdvv wklv hadp B. M ampp texx xlmw ibeq

C. N bnqq ufyy jcfr D. Tất cả các câu trả lời trên đều sai

Câu 35. Để chống lại một cuộc tấn công thụ động (passive attack), người ta thường

A. tìm cách phát hiện (detect) ra cuộc tấn công, sau đó xử lý nó

B. tìm cách ngăn ngừa (prevent) cuộc tấn công này

C. không làm gì cả (vì đây chỉ là cuộc tấn công thụ động)

D. Tất cả các câu trả lời trên đều sai

Câu 36. Microsoft Windows dùng protocol nào sau đây để thực hiện lệnh tracert?

A. ICMP B. ARP

C. UDP D. FTP

Câu 37. Kiểu tấn brute-force khai thác điểm yếu của

A. Khóa (dùng mã hóa dữ liệu) B. Giải thuật (dùng mã hóa dữ liệu)

C. Cả 2 câu trả lời A và B đều đúng D. Cả 2 câu trả lời A và B đều sai

Câu 38. Ngay khi phát hiện hệ thống đã bị xâm nhập trái phép, để quá trình thu thập những bằng chứng

có hiệu quả và có độ tin cậy cao, hành động nào sau đây phải được ưu tiên thực hiện trước nhất

A. Dump bộ nhớ của hệ thống ra file B. Cách ly hệ thống khỏi mạng

C. Tạo disk image cho hệ thống bị xâm nhập D. Khởi động lại hệ thống

Câu 39. Những biện pháp nào dưới đây không giúp chống lại những phần mềm độc hại?

A. Bộ lọc chống spam B. Phần mềm phòng chống spyware

C. Chính sách cho việc cài đặt những patch D. Sử dụng password

Câu 40. Những ví dụ nào dưới đây ảnh hưởng tới tính bí mật thông tin của tổ chức?

A. Làm giả dữ liệu B. Sử dụng dữ liệu cho mục đích cá nhân

C. Mất cắp D. Tai nạn do xóa nhầm dữ liệu

Câu 41. Nghe trộm thuộc kiểu tấn công

A. Active B. Passive

C. Aggressive D. Masquerading

Câu 42. Xác thực thông điệp (Message authentication) là một cơ chế hoặc dịch vụ, dùng để kiểm tra

A. tính toàn vẹn của thông điệp B. tính bí mật của thông điệp

C. tính sẵn sàng của thông điệp D. Tất cả các câu trả lời trên đều sai

Câu 43. Steganography là một kỹ thuật dùng để

A. phát hiện giải thuật mã hóa mà người khác đã dùng thông qua ciphertext

B. giấu một thông điệp bên trong một thông điệp khác, như file văn bản, hình ảnh, audio, video, ...

C. truy tìm tất cả các khả năng của khóa

D. Tất cả các câu trả lời đều sai

Câu 44. Chọn câu trả lời đúng cho mục tiêu của sinh trắc học (biometrics) trong kiểm soát truy cập:

A. Authorization B. Availability

C. Authentication D. Accountability

Câu 45. Hàm băm (hash function) là hàm, thỏa mãn các điều kiện sau:

A. input có thể có độ dài khác nhau, cho ra output có độ dài bằng với input tương ứng

B. input có thể có độ dài khác nhau, cho ra output cũng có độ dài khác nhau

C. input có độ dài bằng nhau, cho ra output có độ dài khác nhau

D. input có thể có độ dài khác nhau, cho ra output có độ dài bằng nhau

Câu 46. Yêu cầu cơ bản cần thiết đối với chữ ký số (digital signature) là gì?

A. Có giá trị phụ thuộc vào thông điệp đã ký B. Dùng thông tin mà duy nhất người ký biết

C. Không thể giả mạo được (về mặt tính toán) D. Tất cả các câu trả lời trên đều đúng

Câu 47. Khái niệm zombie trong an ninh mạng được chỉ đến

A. Máy tính của hacker

B. Mục tiêu chính của cuộc tấn công DDoS

C. Một hệ thống các host bị hại, và cũng là mục tiêu chính của cuộc tấn công DDoS

D. Một hệ thống bị hại, không là mục tiêu chính, được dùng để thực hiện cuộc tấn công DDoS

Câu 48. Bạn nhận được tín hiệu báo động, trên server trong mạng máy tính có một chương trình đang

chạy trái phép (bypass authorization). Cuộc tấn công nào đang được nói đến?

A. Deface Attack B. DDoS

C. Backdoor D. Social engineering

Câu 49. Kiểu tấn công Buffer Overflow được thực hiện bằng cách:

A. tác động làm tràn buffer của các thiết bị mạng, như router

B. tác động làm tràn bộ nhớ của biến trong đoạn code chương trình

C. tác động làm cho mục tiêu không còn đủ tài nguyên để đáp ứng yêu cầu của client

D. Tất cả các câu trả lời trên đều sai

Câu 50. Chữ ký số cung cấp thành phần bảo mật nào?

A. Cung cấp khả năng mã hóa dữ liệu mật của cá nhân

B. Đảm bảo tính riêng tư của cá nhân

C. Chỉ ra nguồn dữ liệu và xác minh tính toàn vẹn dữ liệu

D. Cung cấp framework về luật và quy trình

Câu 51. Trong lĩnh vực mạng máy tính, cổng (port) được dùng để xác định:

A. Địa chỉ của một ứng dụng trên Internet

B. Địa chỉ của một máy tính trên Internet

C. Địa chỉ của một ứng dụng trên một máy tính

D. Tất cả các câu trả lời trên đều sai

Câu 52. Chọn câu trả lời đúng cho công cụ phù hợp nhất dùng để mã hóa thư điện tử:

A. SSH B. IPSEC

C. TLS D. PGP

Câu 53. Chữ ký tay trên tài liệu giấy thuộc kiểu xác thực nào sau đây:

A. Xác thực dựa trên điều người dùng biết B. Xác thực dựa trên điều người dùng có

C. Xác thực dựa trên yếu tố sinh trắc học D. Tất cả các câu trả lời trên đều sai

Câu 54. Trong các đáp án dưới đây, đáp án nào KHÔNG đúng?

A. 1 xor 1 = 1 B. 0 xor 0 = 0

C. 1 xor 0 = 1 D. 0 xor 1 = 1

Câu 55. Chọn câu trả lời đúng cho một đoạn mã độc được giấu bên trong một chương trình hữu dụng,

không có khả năng tự nhân bản:

A. Worm B. Virus

C. Trojan D. Tất cả các câu trả lời trên đều sai

Câu 56. Cuộc tấn công khi kẻ gian giả làm người dùng hợp lệ và tạo kết nối đến server gọi là

A. Session hijacking B. DDoS

C. Spoofing D. Social Engineering

Câu 57. Công cụ nào sau đây được dùng nhiều nhất được dùng để đọc tập tin logs lớn để tìm kiếm những

vấn đề liên quan đến xâm nhập:

A. Text editor B. Vulnerability scanner

C. Password cracker D. IDS

Câu 58. Dùng DES (Data Encryption Standard), input plaintext block có độ dài là

A. 32 bit B. 56 bit

C. 64 bit D. 128 bit

Câu 59. Virus không thể xâm nhập vào thành phần nào sau đây của một hệ thống:

A. File B. System sectors

C. Memory D. DLL files

Câu 60. Để phát hiện tấn công an ninh mạng trên một hệ thống đơn lẻ, thành phần nào sau đây có thể

được dùng đến

A. Firewall B. Honeypot

C. NIPS D. HIDS

Câu 1. Khả năng chia sẻ kết nối internet được tích hợp sẵn trong các Hệ điều hành

Windows 98SE, Windows 2000, Windows XP, Windows Server 2003/2008

Câu 2. Phương thức thông dụng để chia sẻ một kết nối internet cho nhiều máy khác trong mạng là:

NAT (Network Address Translation)

Câu 3. Máy Windows Server 2003 có 2 thiết bị giao tiếp mạng: một giao tiếp Internet và một giao tiếp với các Client. Người quản trị triển khai NAT trên Windows Server này để chia sẻ kết nối internet. Sau khi triển khai xong thì Server giao tiếp internet tốt, còn các Client thì không giao tiếp được mặc dùng đã khai báo đúng và đủ các thông số IP cho Clients. Nguyên nhân dẫn đến tình trạng trên:

Khi triển khai NAT, người quản trị đã chọn sai thiết bị giao tiếp internet

Câu 4. Một máy Windows Server 2003 tên SERVER1 trước đây được xây dựng thành một FTP Server cung cấp Files cho người dùng nội bộ và người dùng các chi nhánh của Doanh nghiệp. Doanh nghiệp dùng SERVER1 để chia sẻ kết nối internet kiểu SecureNAT cho các máy khác. Khi người Quản trị thực hiện SecureNAT bằng Wizard của RRAS. Anh ta chọn "Network Address Translation (NAT)" và click "Next" cho đến khi "Finish". Kết quả:

Người dùng tại các chi nhánh sẽ không truy cập dữ liệu trong FTP trên SERVER1 được

Câu 5. Một máy tính kết nối internet bằng công nghệ ADSL. Khi kết nối internet thành công, ISP sẽ cấp một địa chỉ IP. Trong trường hợp không có một sự can thiệp nào khác, hãy chọn phát biểu chính xác.

Địa chỉ IP đó được cấp cho thiết bị mạng cổng RJ-11 trên ADSL modem

Câu 6. Trước đây, phòng Kỹ thuật của một Doanh nghiệp chỉ có một máy tính chạy Windows Server 2003 tên SERVER1. Người quản trị thường sử dụng Remote Desktop để điều hành máy này từ nhà anh ta. Doanh nghiệp trang bị thêm cho Phòng Kỹ thuật 10 máy tính và dùng máy SERVER1 chia sẻ kết nối internet bằng SecureNAT. Sau khi chia sẻ kết nối internet thành công, người quản trị không còn sử dụng Remote Desktop để điều hành máy SERVER1 từ nhà được nữa. Giải pháp tối ưu nhất để khắc phục vấn đề này:

Trên Basic Firewall của máy SERVER1: mở port 3389 chuyển về IP address của chính máy SERVER1

Câu 7. Trường Đào tạo CNTT iSPACE có nhiều chi nhánh. Các nhân viên kế toán ở các Chi nhánh muốn chia sẻ những thông tin kế toán với nhau. Giải pháp nào sau đây là khả thi hiện nay?

Với đường truyền Internet có sẵn, triển khai hệ thống VPN cho các Chi nhánh

Câu 8. Một gói tin có hỗ trợ IPSec được mã hóa cả Header và Content. Phương thức mã hóa này có tên gọi:

ESP

Câu 9. Trường Đào tạo CNTT iSPACE dự tính triển khai kết nối VPN Site-to-Site giữa các Chi nhánh nhưng vẫn còn lo ngại về độ an toàn của dữ liệu khi truyền trên hạ tầng internet. Là người quản trị mạng tại trường, bạn chọn giải pháp nào dưới đây để khắc phục khó khăn trên?

Sử dụng IPSec kết hợp với giao thức L2TP

Câu 10. Các nhân viên thuộc Chi nhánh Biên Hòa có nhu cầu truy cập dữ liệu trên các máy tính trong phòng Kế toán của Chi nhánh Phú Nhuận. Là một người quản trị mạng tại iSPACE, bạn chọn giải pháp nào là tối ưu nhất:

Thiết lập VPN kiểu Site-to-Site giữa 2 chi nhánh

- **Câu 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)

- **Câu 2: Bộ đệm một lần**
    - Khóa chỉ xài 1 lần
    - Có thể không an toàn do phân phối
    - Sinh khóa ngẫu nhiên
    - Tất cả đều đúng
- **Câu 3: Trong DAC, mô hình nào dung cấu trúc đồ thị tĩnh và đồ thị động**
    - Mô hình truy cập CSDL đa mức
    - Mô hình Take-grant
    - Mô hình ma trận truy cập
    - Mô hình Acten (Action. Entity)
- **Câu 4: RSA là giải thuật**
    - Mã công khai
    - Là tên của một tổ chức quốc tế về mã hóa
    - Mã khóa riêng
    - Tất cả đều sai
- **Câu 5: Một trong hai cách tiếp cận tấn công mã đối xứng**
    - Tấn công tìm khóa
    - Tấn công duyệt toàn bộ
    - Tấn công tìm bản rõ
    - Tất cả đều sai
- **Câu 6: Cơ cấu bảo mật nào sau đây được sử dụng với chuẩn không dây WAP?**
    - WTLS
    - SSL
    - HTTPS
    - Mã hóa WEP
- **Câu 7: Phương pháp điều khiển truy cập có hiệu quả và an toàn nhất đối với mạng không dây là**
    - Mã hóa WEP 40 bit
    - VPN
    - Nhận dạng bảo mật mạng

- Mã hóa WEP 128 bit

- **Câu 8: Bộ lọc địa chỉ MAC được định nghĩa như**

  - Tường lửa cá nhân
  - Ngăn chặn truy cập từ một địa chỉ MAC nhất định
  - Được phép truy cập đến một địa chỉ MAC nhất định
  - Tất cả đều đúng

- **Câu 9: Cơ cấu bảo mật mạng không dây nào sau đây là ít an toàn nhất?**

  - VPN
  - Mã hóa WEP 40 bit
  - Bảo mật định danh mạng
  - Mã hóa WEP 128 bit

- **Câu 10: Mức mã hóa WEP nào nên được thiết lập trên một mạng 802.11b?**

  - 128 bit
  - 40 bit
  - 28 bit
  - 16 bit

- **Câu 1. Yêu cầu để đảm bảo sử dụng mã hóa đối xứng là**

  - Có thuật toán encryption tốt,có một khóa bí mật được biết bởi người nhận/gửi và kênh truyền bí mật để phân phát key
  - Có một kênh truyền phù hợp và một khóa bí mật được biết bởi người nhận/gửi
  - Có thuật tóan encryption tốt và có một khóa bí mật được biết bởi người nhận/gửi
  - Tất cả đều đúng

- **Câu 2. Các thuật tóan nào sau đây là thuật tóan mã hóa đối xứng**

  - Triple –DES, RC4, RC5, Blowfish
  - Triple –DES, RC4, RC5, IDEA
  - RC4, RC5, IDEA, Blowfish
  - IDEA, Blowfish, AES, Elliptic Cure

- **Câu 3. Các phát biểu sau đây phát biểu nào đúng**

- Hầu hết các thuật tóan mã hóa đối xứng đều dựa trên cấu trúc thuật tóan Feistel
- Tấn công thông điệp thì thời gian giải mã tỷ lệ với kích thước khóa
- Hầu hết các thuật tóan mã hóa khối đều đối xứng
- Tất cả đều đúng

- **Câu 4. Cơ chế bảo mật SSL hoạt động trên tầng**

  - Network, Transport
  - Network, Session
  - Application, Session
  - Tất cả đều sai

- **Câu 5. Keberos là dịch vụ ủy thác**

  - Xác thực trên Web
  - Xác thực X.509
  - Xác thực trên Server
  - Xác thực trên các máy trạm với nhau

- **Câu 6. PGP là giao thức để xác thực**

  - Quyền đăng cập vào hệ thống máy chủ Windows
  - Bảo mật cho thư điện tử
  - Thực hiện mã hóa thông điệp theo thuật toán RSA
  - Địa chỉ của máy trạm khi kết nối vào Internet

- **Câu 7. Công cụ/cơ chế bảo mật cho mạng không dây là**

  - SSL
  - TSL
  - Giao thức PGP
  - WEP

- **Câu 8. Giao thức SSL và TSL hoạt động ở tầng nào của mô hình OSI**

  - Network
  - Sesion
  - Transport
  - Từ tầng Trasport trở lên

- **Câu 9. 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 Windows

- **Câu 10. Các dạng sau đây, dạng nào là của virus**

- sealth, cư trú bộ nhớ, macro, đa hình, file
- stealth, cư trú bộ nhớ, macro, lưỡng tính, file
- virus ký sinh, file, boot secctor, stealth, cư trú bộ nhớ, macro
- virus ký sinh, cư trú bộ nhớ, boot secctor, Stealth, đa hình, macro

- **Câu 11. Virus Macro chỉ có khả năng tấn công vào các file**

- MS.Exel, MX Word, MS.Outlook Mail
- MS.Exel, MX Word, MS.Power Point
- MS.Exel, MX Word,Yahoo Mail
- Tất cả các loại file

- **Câu 12. Các giao thức bảo mật trên Internet như SSL, TLS và SSH hoạt động ở tầng nào trên mô hình OSI**

- Tầng Network
- Tầng Transport
- Từ tầng Transport trở lên đến tầng 7
- Tầng Session

- **Câu 13. Kỹ thuật tấn công phổ biến trên Web là**

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

- **Câu 14. Các lỗ hổng bảo mật trên hệ thống là do**

- Dịch vụ cung cấp
- Bản thân hệ điều hành
- Con người tạo ra
- Tất cả đều đúng

- **Câu 15. Cho biết câu nào đúng trong các câu sau**

  - Tất cả Firewall đều có chung thuộc tính là cho phép phân biệt hay đối xử khả năng từ chối hay truy nhập dựa vào địa chỉ nguồn
  - Chức năng chính của Firewall là kiểm sóat luồng thông tin giữa mạng cần bảo vệ và Internet thông qua các chính sách truy nhập đã được thiết lập
  - Hệ thống Firewall thường bao gồm cả phần cứng lẫn phần mềm
  - Tất cả đều đúng

1.Yêu cầu để đảm bảo sử dụng mã hóa đối xứng là
a.Có thuật tóan encryption tốt,có một khóa bí mật được biết bởi người nhận/gởi và kênh truyền bí mật để phân phát key
b.Có một kênh truyền phù hợp và một khóa bí mật được biết bởi người nhận/gởi
c.Có thuật tóan encryption tốt và có một khóa bí mật được biết bởi người nhận/gởi
d.Tất cả đều đúng
2.Các thuật tóan nào sau đây là thuật tóan mã hóa đối xứng
a.Triple –DES, RC4, RC5, Blowfish
b.Triple –DES, RC4, RC5, IDEA
c.RC4, RC5, IDEA, Blowfish
d.IDEA, Blowfish, AES, Elliptic Cure
3.Các phát biểu sau đây phát biểu nào đúng
a. Hầu hết các thuật tóan mã hóa đối xứng đều dựa trên cấu trúc thuật tóan Feistel
b.Tấn công thông điệp thì thời gian giải mã tỷ lệ với kích thước khóa
c.Hầu hết các thuật tóan mã hóa khối đều đối xứng
d.Tất cả đều đúng
4.Cơ chế bảo mật SSL hoạt động trên tầng
a.Network, Transport
b.Network, Session
c.Application, Session
d.Tất cả đều sai
5.Keberos là dịch vụ ủy thác
a. Xác thực trên Web
b. Xác thực X.509
c. Xác thực trên Server
d. Xác thực trên các máy trạm với nhau
6.PGP là giao thức để xác thực
a. Quyền đăng cập vào hệ thống máy chủ Window

b. Bảo mật cho thư điện tử
c. Thực hiện mã hóa thông điệp theo thuật tóan RSA
d. Địa chỉ của máy trạm khi kết nối vào Internet
7. Công cụ/cơ chế bảo mật cho mạng không dây là
a. SSL
b. TSL
c. Giao thức PGP
d. WEP
8. Giao thứ SSL và TSL hoạt động ở tầng nào của mô hình OSI
a. Network
b. Sesion
c. Transport
d. Từ tầng Trasport trở lên
9. Giao thức SSL dùng để
a. Cung cấp bảo mật cho dữ liệu lưu thông trên dịch vụ HTTP
b. Cung cấp bảo mật cho thư điện tử
c. Cung cấp bảo mật cho Web
d. Cung cấp bảo mật cho xác thực người dùng vào các hệ thống vận hành trên Flatform Window
10.Chức năng chính của Virus là
a. Lây nhiễm và sinh sản
b. Sống ký sinh và lây nhiễm
c. Tự phát triển độc lập và lây nhiễm
d. Tất cả đều đúng
11.Hoạt động của virus có 4 giai đoạn
a. Nằm im, lây nhiễm, tàn phá và tự hủy
b. Lây nhiễm, tấn công, hủy diệt và tự hủy
c. Nằm im, lây nhiễm, khởi sự và tàn phá
d. Lây nhiễm, khởi sự, tàn phát, kích hoạt lại
12.Các dạng sau đây, dạng nào là của virus
a.sealth, cư trú bộ nhớ, macro, đa hình, file
b.stealth, cư trú bộ nhớ, macro, lưỡng tính, file
c.virus ký sinh, file, boot secctor, stealth, cư trú bộ nhớ, macro
d.virus ký sinh, cư trú bộ nhớ, boot secctor, Stealth, đa hình, macro
13. Virus Macro chỉ có khả năng tấn công vào các file
a. MS.Exel, MX Word, MS.Outlook Mail
b. MS.Exel, MX Word, MS.Power Point
c. MS.Exel, MX Word,Yahoo Mail
d.Tất cả các loại file
14. Các giao thức bảo mật trên Internet như SSL, TLS và SSH hoạt động ở tầng nào trên mô hình OSI
a.Tầng Network
b.Tầng Transport

c.Từ tầng Transport trở lên đến tầng 7
d.Tầng Session
15. Kỹ thuật tấn công phổ biến trên Web là
a. Chiếm hữu phiên làm việc.
b.Tràn bộ đệm.
c.Từ chối dịch vụ (DoS)
d.Chèn câu truy vấn SQL.
16. Các lỗ hổng bảo mật trên hệ thống là do
a. Dịch vụ cung cấp
b. Bản thân hệ điều hành
c. Con người tạo ra
d. Tất cả đều đúng
17. Cho biết câu nào đúng trong các câu sau
a. Tất cả Firewall đều có chung thuộc tính là cho phép phân biệt hay đối xử khả năng từ chối hay truy nhập dựa vào địa chỉ nguồn
b. Chức năng chính của Firewall là kiểm sóat luồng thông tin giữa mạng cần bảo vệ và Internet thông qua các chính sách truy nhập đã được thiết lập
c. Hệ thống Firewall thường bao gồm cả phần cứng lẫn phần mềm
d. Tất cả đều đúng
18. Loại Firewall nào sau đây cho phép hoạt động ở lớp phiên (session) của mô hình OSI
a. Packet filtering firewall
b. Circuit level firewall
c. Application level firewall
d. Stateful multilayer inspection firewall
19.Những giao thức WAN nào có thể được định hình trên một kết nối tuần tự không đồng bộ (Chọn 2)
a. PPP
b. ATM
c. HDLC
d. SDLC
20. Khi thuê một giải pháp VPN, những loại tấn công nào bạn cần phải xét đến ?
a. Denial of Service (DoS) attacks, Internet Viruses..
b. Distributed Denial of Service (DDoS) attacks.
c. **D**ata confidentiality, IP Spoofing.
d. Network mapping, Internet Viruses.
21. Các phát biểu sau đây phát biểu là là đúng nhất
a.Fire wal là một vành đai phòng thủ cho máy tính hoặc hệ thống trước những tấn công
b.Là một điểm chặn của trong quá trình điều khiển và giám sát.
c. Là một phần mềm hoặc phần ứng có khả năng ngăn chặn tấn công từ bên trong và bên ngoài vào hệ thống.
d.Là một giải pháp giúp hệ thống phát hiện và ngăn chặn các truy cập trái phép
22. Bảo mật thư điện tử là nhằm đảm bảo

a.Tính tin cẩn (confidentiality), Tính xác nhận, Toàn vẹn thông điệp (integrity), Sự thối thác ban đầu (non-repudiation of origin)
b. Tính xác nhận,Toàn vẹn thông điệp(integrity), Sự thối thác ban đầu (non-repudiation of origin), tính bền vững
c.Sự thối thác ban đầu (non-repudiation of origin), tính bền vững, tính ổn khi gởi và nhận
d.Tất cả đều đúng

23. Các giao thức được để bảo mật thư điện tử là
a.GPG, S/MINE
b.SHA-1, S/MINE
c.CAST-128 / IDEA/3DES
d. Keboros, X.509

24. Chữ ký điện tử (digital signature) sử dụng thuật tóan nào sau đây
a. RSA,MD5
b. RSA,MD5, Keboros
c. MD5, SHA,RSA
d.Không dùng thuật tóan nào nêu trên

25. Chữ ký điện tử là
a.Là một chuỗi đã được mã hóa theo thuật tóan băm và đính kèm với văn bản gốc trước khi gởi.
b.Đoạn dữ liệu ngắn đính kèm với văn bản gốc để chứng thực tác giả của văn bản và giúp người nhận kiểm tra tính toàn vẹn của nội dung văn bản gốc.
c.a và b đều đúng
d.Tất cả cả đều sai

26. Các bước mã hóa của chứ ký điện tử
a.Dùng giải thuật băm để thay đổi thông điệp cần truyền đi, Sử dụng khóa private key của người gửi để mã hóa message digest thu được ở bước trên, sau đó gộp digital signature vào message ban đầu.
b.Dùng giải thuật băm để thay đổi thông điệp cần truyền đi, sử dụng khóa private key của người gửi để mã hóa message digest thu được ở bước trên, sau đó gộp digital signature vào message ban đầu và nén dữ liệu gởi đi.
c.Chỉ sử dụng giải thuật băm để thay đổi thông điệp cần truyền đi và sử dụng khóa private key của người gửi để mã hóa message digest thu được ở bước trên.
d.Tất cả đều đúng

27. Các bước kiểm tra của chứ ký điện tử
a. Gồm các bước
1.Dùng public key của người gửi (khóa này được thông báo đến mọi người) để giải mã chữ ký số của message,
2.Dùng giải thuật (MD5 hoặc SHA) băm message đính kèm, So sánh kết quả thu được ở bước 1 và 2.
3.Nếu trùng nhau, ta kết luận message này không bị thay đổi trong quá trình truyền và message này là của người gửi.

b.Chỉ có bước 1 và 2
c.Gồm các bước

1.Dùng public key của người gửi (khóa này được thông báo đến mọi người) để giải mã chữ ký số của message,

2.Dùng giải thuật (MD5 hoặc SHA) băm message đính kèm, So sánh kết quả thu được ở bước 1 và 2.

3.Nén dữ liệu rồi gởi đi

d.Không có bước nào ở trên là đúng

28. Việc xác thực người dùng khi đăng cập vào hệ thống Window XP, 2000 hoặc 2003 sử dụng giải thuật

a.RSA

b.Keberos

c.MD5

d.SHA

29. Để thực hiện tấn công bằng Trojan, kẻ tấn công chỉ cần

a.Tạo 1 file chạy (*.exe, *.com) vận hành trên máy nạn nhân là đủ

b. Cho máy nạn nhân lây nhiễm một loại virus bất kỳ nào đó.

c. Thực hiện đồng thời 2 file, một file vận hành trên máy nạn nhân, file còn lại hoạt động điều khiển trên máy kẻ tấn công.

d. Không có điều nào đúng.

30. Giao thức bảo mật IPSec hoạt động ở tầng

a. Chỉ ở tầng transport ở mô hình OSI

b.Từ tầng 4 tới tầng 7 ở mô hình OSI

c.Network Layer ở mô hình OSI

d.Tất cả đều sai

31. Cho biết phát biểu sau đây phát biểu nào là đúng nhất về registry

a.Regỉstry là một cơ sở dữ liệu dùng để lưu trữ thông tin về những sự thay đổi, những lựa chọn, những thiết lập từ người sử dụng Windows.

b.Regỉstry là một phần mềm tiện ích hỗ trợ cho người dùng thay đổii cấu hình Window khi cần thiết

c. Regỉstry là một thành phần của hệ điều hành Window

d. Tất cả đều đúng

32.Có bao nhiêu kiểu dữ liệu trong Registry

a. 5 b. 4 c. 6 d. 7

33. Các kiểu dữ liệu dùng trong registry là

a.interger, real,text,string

b.HKEY_CLASSES_ROOT, -USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG, HKEY_DYN_DATA

c.HKEY_CLASSES_ROOT, -USER, HKEY_LOCAL_MACHINE, REG_BINARY

d.REG_BINARY, REG_DWORD, REG_EXPAND_SZ, REG_MULTI_SZ, REG_SZ

34. Để ẩn tất cả các ổ đĩa trong registry (A,B,C,D…) thì biến REG_DWORD trong Userkey và Systemkey có giá trị là bao nhiêu

a. 65656000
b. 67188270
c. 67108863
d.Tất cả đều sai

35. Để sử dụng xác thực Keberos V5 ở tất cả máy trạm Window98, người ta thực hiện :
a. Update window 98 lên XP hoặc Window 2000
b. Cài đặt tiện ích Distributed Security Client trên tất cả các máy chạy Window 98
c. Chỉ cần cài đặt Active Directory trên Server hệ thống
d. Không thể thực hiện được

36. Khi cài đặt Window 2000 Server trên hệ thống NTFS, nhưng không thấy có hiển thị mục Security ở Security tables vì ?
a. Update Window 2000 mà không remote trước khi cài đặt
b. Cài đặt Window 2000 nhiều lần trên Server
c. Bản Window 2000 không có bản quyền
d. Tất cả đều đúng

37. Dịch vụ Active Directory thực hiện các chức năng sau
a. Tổ chức và xây dựng các domain; xác thực và cấp quyền cho các đối tượng
b. Duy các hoạt động của các dịch vụ bảo mật cho Window Server và xác thực, cấp quyền cho các đối tượng
c. Chỉ thực hiện việc xác thực và cấp các quyền cho users và groups
d. Quản lý tài nguyên và người dùng; xác thực và cấp các quyền cho users và groups; giám sát hoạt động của các user

38. Thuật tóan thực hiện trong cơ chế bảo mật IP (IP Sec) ở Window sử dụng là
a.MD5 và SHA1
b. Kerberos và DES
c. DES hoặc 3DES (triple DES).
d.Tất cả đều sai

39. Trong Window 98,XP Registry được lưu trữ ở đâu ?
a.Được lưu trong file **Classes.dat** trong thư mục Windows
b.Được lưu trong thư mục "Windows\ System32\ Config
c.Trong 2 file: user.dat và system.dat trong thư mục Windows
d.Tất cả đều sai

40. Để thực hiện sửa đổi cấu hình trên registry ta thực hiện như sau:
a. Gõ regedit vào cửa sổ Run
b. Bấm Ctrl+ Esc+ r rồi bấm Enter
c. a và b đúng
d.Tất cả đều sai

41.Quy trình crack một sản phẩm phần mềm đơn giản gồm mấy bước
a. 3 b.4 c.5 **d.3 hoặc 4**

42. Hai giao thức sử dụng trong IPSec (IPSec Protocol) gồm
a.IP Authentication Header, TCP/IP
b.TCP/IP, IP Encapsulating Security Payload

c.IP Authentication Header, IP Encapsulating Security Payload
d.Tất cả đều đúng
43. Các điểm khác nhau cơ bản giữa dịch vụ X.509 và Kerberos là
a. Dựa trên mã hóa đối xứng
b. Được sử dụng trong dịch vụ mail
c. Xác thực nhiều chiều
d. Tất cả đều đúng
44. Các chức năng cơ bản của kỹ thuật tấn công Sniffer
a**.** Tự động chụp các tên người sử dụng (Username) và mật khẩu không được mã hoá, Chuyển đổi dữ liệu trên đường truyền, phân tích những lỗi đang mắc phải trên hệ thống lưu lượng của mạng.
b. Bắt gói tin trên đường truyền, phân tích lỗi và giải mã gói tin
c. Bắt gói tin trên đường truyền, mã hóa vag giải mã dữ liệu
d.Tất cả đều đúng
45. Các bước tấn công của Web Server theo trình tự sau :
a. Thăm dò, Scan, Giành quyền truy cập, Duy trì truy cập, Xóa vết
b. Scan, Thăm dò, Giành quyền truy cập, Duy trì truy cập, Xóa vết
c. Thăm dò, Scan, Duy trì truy cập, Giành quyền truy cập, Xóa vết
d. Giành quyền truy cập, Duy trì truy cập, Scan, Thăm dò
46. Hiện tượng này do loại chương trình nguy hiểm nào gây ra : Làm mất một số file, làm phân mãnh ổ đĩa, gây tác hại vào những ngày, tháng đặc biệt v.v…
a. Virrus,Zombie **b. Worm, Virus** c. Logicbomb, Virus d.Trapdoors, Trojan
47.Để đánh giá điểm mạnh của hệ thống IDS người ta dựa vào các yếu tố sau :
a.Khởi sự, Cách thực hiện, biểu hiện mà nó ghi nhận
b.Khởi sự, giám sát vị trí, những đặc trưng ghép nối hoặc tích hợp
c. Cách thực hiện, biểu hiện mà nó ghi nhận, những đặc trưng ghép nối hoặc tích hợp
d.Tất cả đều đúng
48. Hai cơ chế chính của hệ thống IDS Trigger để phát hiện khi có một kẻ xâm nhập tấn công mạng là :
a.Phát hiện biểu hiện không bình thường, phát hiện sử dụng không đúng
b.Phát hiện hiện tượng trùng lặp, phát hiện không bình thường
c. Phát hiện thay đổi, phát hiện sử dụng bất bình thường
d.Tất cả đều đúng
49.Mục tiêu là phân tích mật mã là gì?
a. Để xác định thế mạnh của các thuật toán một
b. Để tăng cường chức năng thay thế trong một thuật toán mật mã
c. Để giảm chức năng transposition trong một thuật toán mật mã
d. Để xác định hoán vị sử dụng
50. Điều gì sẽ xãy ra khi một thông báo đã được sửa đổi?
a. Khoá công cộng đã được thay đổi
b. Chìa khóa cá nhân đã được thay đổi
c. Thông điệp số đã được thay đổi

d.Tin nhắn đã được mã hóa đúng cách

51.Mà hóa nào sau đây là một tiêu chuẩn dùng để phát triển cho việc tạo ra thông điệp an toàn?

a. Data Encryption Standard

b. Digital Signature Standard

c. Secure Hash Algorithm

d. Chữ kí dữ liệu tiêu chuẩn

52.Nếu kẻ tấn công lấy trộm một mật khẩu có chứa một chiều mật khẩu đã mật mã, loại tấn công, cô sẽ thực hiện để tìm mật khẩu đã mật mã?

a. Tấn công Man-in-the-middle

b. Tấn công Birthday

c. Tấn công Denial of Service

d. Tấn công Dictionary

53.Lợi thế của RSA là gì so với DSS?

a.Nó có thể cung cấp cho chữ ký số và mã hóa các chức năng

b.Nó sử dụng nguồn tài nguyên ít hơn và mã hóa nhanh hơn bởi vì nó sử dụng các phím đối xứng

c.Nó là một thuật toán mật mã khối so với một thuật toán mật mã dòng

d.Nó sử dụng một lần mã hóa pad

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

a. Khóa riêng của người nhận

b. Khóa công khai của người gửi

c. Khóa riêng của người gửi

d. Khóa công khai của người nhận

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

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

b. Một phương pháp mã hóa thông tin bí mật

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

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

56. Sử dụng nhiêu bit với DES để có hiệu quả?

a.56 **b.64** c.32 d.16

57.Các yếu tố ảnh hưởng đến quá trình mã hóa

a. Thuật toán mã hóa, giải mã, và tính an toàn của kênh truyền

b. Thời gian thực hiện mã hóa và giải mã

c. Thực hiện mã hóa khối, mở rộng số bít xử lý

d. Tất cả đều sai

58. Đối với Firewall lọc gói, hình thức tấn công nào sau đây được thực hiện

a. Nhái địa chỉ IP, tấn công giữa, tấn công biên

b. Nhái địa chỉ IP, tấn công đường đi nguồn, tấn công từng mẫu nhỏ

c. Nhái địa chỉ IP, tấn công vượt firewall,tấn công từng mẫu nhỏ

d. Nhái địa chỉ IP, tấn công vượt firewall, tấn công đường đi nguồn

59.Ai là người tham gia vào việc phát triển đầu tiên hệ thống mã hóa khóa công?

a. Adi Shamir
b. Ross Anderson
c. Bruce Schneier
d. Martin Hellman
60. DES là viết tắt của từ nào ?
a. Data encryption system
b. Data encryption standard
c. Data encoding standard
d. Data encryption signature
61. Các phát biểu sau đây, phát biểu nào tốt nhất mô tả một hacker mũ trắng?
A. Chuyên gia bảo mật
B. Cựu Hacker mũ đen
C. Cựu Hacker mũ xám
D. Hacker hiểm độc
62. Giai đoạn đầu của hacking là gì?
A. Duy trì truy cập
B. Gaining truy cập
C. Trinh sát
D. Dò tìm (Scanning)
63. Khi một hacker cố gắng tấn công một máy chủ qua Internet nó được gọi là loại tấn công?
A. Tấn công từ xa
B. Tấn công truy cập vật lý
C. Truy cập địa phương
D. Tấn công tấn công nội
64. Công cụ nào sau đây đúng là một công cụ để thực hiện footprinting không bị phát hiện?
A. Whois search
B. Traceroute
C. Ping sweep
D. Host scanning
65. Bước tiếp theo sẽ được thực hiện sau khi footprinting là gì?
A. Scanning
B. Enumeration
C. System hacking
D. Active information gathering
66. Footprinting là gì?
A. đo dấu vết của một hacker có đạo đức
B. tích luỹ dữ liệu bằng cách thu thập thông tin về một mục tiêu
C. quét một mạng lưới mục tiêu để phát hiện hệ điều hành các loại
D. sơ đồ bố trí vật lý của một mạng của mục tiêu
67. Lý do tốt nhất để thực hiện một chính sách bảo mật là gì?
A. Tăng an ninh.

B. Nó làm cho khó hơn việc thi hành bảo mật.
C. Hạn chế quyền hạn của nhân viên
D. Làm giảm an ninh.

68. FTP sử dụng cổng gì ?

A. 21
B. 25
C. 23
D. 80

69. Cổng nào được HTTPS sử dụng?

A. 443
B. 80
C. 53
D. 21

70. Trojan Horse là gì?

A. một chương trình độc hại mà lấy cắp tên người dùng và mật khẩu của bạn
B. gây hại như mã giả mạo hoặc thay thế mã hợp pháp
C. 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
D. 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

71. John muốn cài đặt một ứng dụng mới vào máy chủ của Windows 2000. Ông muốn đảm bảo rằng các ứng dụng bất kỳ ông sử dụng chưa được cài Trojan. Ông có thể làm gì để giúp đảm bảo điều này?

A. So sánh chữ ký MD5 của tập tin với một trong những công bố trên các phương tiện truyền thông phân tán
B. Xin các ứng dụng thông qua SSL
C. So sánh chữ ký virus của file với một trong những công bố trên các phương tiện truyền thông
D. Cài đặt các ứng dụng từ đĩa CD-ROM

72. Hầu hết các lỗi SQL Injection đều là do (chọn 2 phương án)

a. câu lệnh SQL sai
b. trình duyệt Web không hỗ trợ
c. User làm cho câu lệnh SQL sai
d. Sử dụng Hệ quản trị CSDL không có bản quyền

73. Chính sách bảo mật là

a. Cơ chế mặc định của hệ điều hành
b. phương thức xác định các hành vi "phù hợp" của các đối tượng tương tác với hệ thống
c. các tập luật được xây dựng nhằm bảo vệ các tấn công bất hợp pháp từ bên ngoài
d. Tất cả đều đúng

74. Các loại mục tiêu của chiến tranh thông tin

a. Website, E-commerce server
b. Internet Relay Chat (IRC), Domain Name System (DNS)

c. ISP, Email server
d. Tất cả đều đúng
75. Khi thực hiện triển khai HIDS khó khăn gặp là
a. Chi phí lắp đặt cao, khó bảo quản và duy trì
b. Giới hạn tầm nhìn mạng, phải xử lí với nhiều hệ điều hành khác trên mạng.
c. Thường xuyên phải cập nhật bảng vá lỗi
d. Thường xuyên cài đặt lại phải khi hệ thống mạng thay đổi hệ điều hành

4)loại nào nhân bản trong máy :

5)Loại nào không nhân bản khi chạy 1 ứng dụng có lợi:

Câu 4 5: worn-virus-**trojan**-logic bomb

8)Kiểu tấn công chỉ nghe ngóng thông tin để bắt được 1 cái gì đó :Pass,account,… thuộc nhóm:DoS-man in the middle….

9)Kiểu tấn công dùng từ điển của hacker thuộc nhóm nào: DoS-hacking-…

10)Buffer overload là kiểu tấn công:

-Làm tràn buffer

-Làm tràn bộ nhớ đệm

-Làm vượt quá khả năng tính toán cho các biến ….

11)RSA dùng để mã hóa thông điệp có kích thước : 32bit-64bit-32byte-64byte

13) Chế độ hoạt động của PGP khi thực hiện mã hóa đối xứng là:-CBC- ECB -CFB - OFB
15) Cơ chế bảo mật SSL hoạt động trên tầng-.Network, Transport -Network, Session -Application, Session

17)Sử dụng tên người dùng giả là kiểu tấn công gì ? -sniffing-…

18)Zombie máy tính là gì? -> Liên quan đến cuộc tấn công DDOS ấy , hình như nó là các máy con bị điều khiển để cùng mục đích tấn công vào một nạn nhân nào đó …

1. Nghe lén: passive
2. Đứng giữa lấy thông tin là kiểu tấn công gì? Man in the middle
3. CIA: confidentiality - itegrility – availability
4. Khóa công khai: gửi thông điệp thì dùng khóa công khai của ng nhận
5. Chữ kí số thì dùng khóa bí mật của người gửi
6. Chữ kí số đc dùng khóa của cơ sở hay công ty gì đó, nói chung là cái chỗ đc chứng nhận và chỗ đó dùng khóa bí mật của nó để mã hóa chữ kí số (câu này hàm ý vậy, ko nhớ chính xác nội dung)

1. DDOS: active
2. Mã chuyển vị là transition
3. DES dùng block 64 bit, key 56 bit
4. Tracert traceroute (tiếng Việt tạm dịch là công cụ truy vết) là một công cụ chẩn đoán mạng máy tính để hiển thị các tuyến đường (đường dẫn) và đo lường sự chậm trễ quá cảnh của các gói dữ liệu trên một giao thức Internet (IP) mạng.