1,Để thực hiện tấn công Smuft, tin tặc phải giả mạo địa chỉ gói tin ICMP trong yêu cầu...  
D, Địa chỉ nạn nhân làm địa chỉ nguồn của gói tin

2, Tấn công bằng mã độc có thể gồm:  
C, SQLi, XSS, CSRF và Buffer overflow

3,Có thể phòng chống tấn công Smurt bằng cách cấu hình các máy và router không trả lời..  
C, Các yêu cầu ICMP hoặc các yêu cầu phát quảng bá.

4, Trong dạng tấn công vào mật khẩu dựa trên từ điển, tin tặc đáng cắp mất  
khẩu...  
A, Tìm mật khẩu trong từ điển các mật khẩu.  
B, Vét cạn các mật khẩu có thể có  
C, Thử các từ có tần suất sử dụng cao làm mật khẩu trong từ điển  
D, Lắng nghe trên đường truyền để đánh cắp mật khẩu

5, Đâu là một kỹ thuật tấn công DoS?  
A, UDP Ping C, DNS spoofing  
B, Smurf D, DNS Cache Poisoning

6, Đâu là một biện pháp phòng chống tấn công SYN Floods?  
A, SYN IDS C, SYN Cache  
B, SYN Proxy D, SYN Firewall

28,Kỹ thuật tấn công SYN Floods khai thác điểm yếu trong khâu nào của bộ  
giao thức TCP/IP?  
A, Bắt tay 3 bước

Chương 1 – 2 ( Part 1 )

1, Khi khai thác lỗi tràn bộ đệm, tin tặc thường chèn mã độc, gây tràn và ghi đè

để sử đổi thành phần nào sau đây của bộ nhớ ngăn xếp để chuyển hướng nhằm

thực hiện mã độc của mình:

A, Bộ đệm hoặc bến cục bộ của hàm

B, Địa chỉ trả về của hàm

C, Các biến đầu vào của hàm

D, Con trỏ khung ngăn xếp

2, Tấn công kiểu Social Engineering là dạng tấn công khai thác yếu tố nào sau

đây trong hệ thống?

A, Người dùng

B, Máy trạm

C, Máy chủ

D, Hệ điều hành và ứng dụng

3,Dạng tấn công chèn mã được tin tặc thực hiện phổ biến trên các trang web

nhằm đến các cơ sở dữ liệu là:

A, Tấn công chèn mã XSS

B, Tấn công chèn mã SQL

C, tấn công chèn mã html

D, tấn công chèn mã CSRF

4, Một trong các biện pháp có thê sử dụng để phòng chống tấn công người đứng

giữa là:

A, Sử dụng các hệ thống IPS/IDS

B, Sử dụng mã hóa để đảm bảo tính bí mật các thông điệp truyền

C, Sử dụng tường lửa để ngăn chặn

D, Sử dụng chứng chỉ số để xác thực thông tin nhận dạng các bên

5, Để đảm bảo an toàn cho hệ thống điều khiển truy nhập, một trong các biện

pháp phòng chống hiệu quả là:

A, Không cài đặt và chạy các chương trình tải từ các nguồn không tin cậy

B, Không dùng tài khoản có quyền quản trị để chạy các chương trình ứng dụng

C, Không cho phép chạy các chương trình điều khiển từ xa

D, Không mở các email của người lạ hoặc email quảng cáo.

6,Đâu là một trong các biện pháp phòng chống tấn công khai thác lỗi tràn bộ

đệm:

E, Sử dụng cơ chế cấm thực hiện mã trong dữ liệu

A, Sử dụng các kỹ thuật mật mã

B, Sử dụng các thư viện lập trình an toàn

C, Sử dụng tường lửa

D, sử dụng công nghệ xác thực mạnh

E B

7,Một trong các biện pháp hiệu quả để phòng chống macro viruses là:

A, Cấm tự động thực hiện macro trong Microsoft Office

B, Sử dụng tường lửa

C, Cẩm tự động thực hiện macro trong Microsoft Exchange

D, sử dụng IPS/IDS

8,Các lỗ hổng bảo mật thường tồn tại nhiều nhất trong thành phần nào của hệ

thống:

A, Các thành phần phần cứng

B, Các ứng dụng

C, Các dịch vụ mạng

D, Hệ điều hành

9,Đâu là một kỹ thuật tấn công DoS?

A, UDP Ping

B, DNS spoofing

C, DNS Cache Poisoning

D, Smuft

10, Trong tấn công khai thác lỗi tràn bộ đệm, tin tặc thường sử dụng shellcode

đó là dạng:

A, Mã hợp ngữ

B, Mã máy

C, Mã C/C++

D, Mã java

11, Lỗi tràn bộ đệm là lỗi trong khâu:

A, Quản trị phần mềm

B, Thiết kế phần mềm

C, Kiểm thử phần mềm

D, Lập trình phần mềm

12, Các vùng bộ nhớ thường bị tràn bao gồm:

A,Hàng đợi(Queue) và ngăn xếp(stack)

B, ngăn xếp(stack) và bộ nhớ đệm (cache)

C, Hàng đợi(Queue) và vùng cấp phát động (Heap)

D, ngăn xếp(stack) và vùng cấp phát động (Heap)

13,Một trong các cách virus thường sử dụng để lây nhiễm vào các chương trình

khác là:

A, Sửa đổi các chương trình

B, Xáo trộn mã của virus

C, Ẩn mã của virus

D, Thay thế các chương trình

14, Sâu SQL Slammer tấn công khai thác lỗi tràn bộ đệm trong hệ quản trị csdl:

A, SQL Server 2000

B, SQL Server 2012

C, SQL Server 2008

D, SQL Server 2003

15,Tại sao việc sử dụng thủ tục csdl (stored procedure) là một trong các biện

pháp hiệu quả để ngăn chặn triệt để tấn công chèn mã SQL?

A, thủ tục csdl độc lập với các ứng dụng

B,Thủ tục csdl lưu trong csdl và chạy nhanh hơn câu lênh trực tiếp

C, Thủ tục csdl có khả năng cấm chèn mã

D, Thủ tục csdl cho phép tách mã lệnh SQL khỏi dữ liệu người dùng

16,Trong tấn công khai thác lỗi tràn bộ đệm, tin tắc thường sử dụng một số lệnh

NOP (No Operation) ở phần đầu của mã tấn công. Mục đích của việc này là để:

A, Tăng khả năng mã tấn công được thực hiện

B, Tăng khả năng gây lỗi chương trình

C, Tăng khả năng gây tràn bộ đệm

D, Tăng khả năng phá hoại của mã tấn công

17, Troijan horses là dạng phần mềm độc hại thường dành quyền truy nhập vào

các file của người dùng khai thác cơ chế điều khiển truy nhập...

A, Role-Based

B, MAC

C, Rule-Based

D, DAC

18, Mật khẩu an toàn trong thời điểm hiện tại là mật khẩu có:

A, Độ dài lớn hơn hoặc bằng 8 ký tự

B, Độ dài từ 8 ký tự trở lên, gồm chữ cái hoa, thường, chữ số và ký tự đặc biệt

C, Chứa các ký tự từ nhiều dạng ký tự.

D, Khả năng chống tấn công phát lại và chứa các ký tự từ nhiều dạng ký tự

19,Đâu là dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần

mềm ứng dụng?

A, Lỗi tràn bộ đệm

B, Lỗi thiết kế

C, Lỗi cấu hình

D, Lỗi quản trị

\*20, NOTE Nguyên nhân của sự tồn tại các điểm yếu trong hệ thống có thể do:

A, Lỗi thiết kế, lỗi cài đặt và lập trình

B, Lỗi cấu hình hoạt động

C, Lỗi quản trị

D, Tất cả các khâu trong quá trình phát triển và vận hành.

A D

21, NOTE Một trong các biện pháp cụ thể cho quản lý, khắc phục các lỗ hổng báo mật

và tăng cường khả năng đề kháng cho hệ thống là:

A, Định kỳ nâng cấp hệ thống phần cứng

B, Định kỳ cập nhật các thông tin về các lỗ hổng từ các trang web chính thức

C, Định kỳ cập nhật các bản vá và nâng cấp hệ điều hành

D, Định kỳ nâng cấp hệ thống phần mềm

B C\*\*\*

22, Tìm phát biểu đúng trong các phát biểu sau:

A, Điểm yếu hệ thống chỉ xuất hiện trong các modun phần cứng

B, Điểm yếu hệ thống có thể xuất hiện trong cả mô đun phần cứng và phần

mềm

C, Điểm yếu hệ thống chỉ xuất hiện trong các mô đun phần mềm

D, Điểm yếu chỉ xuất hiện khi hệ thống bị tấn công

23, Biện pháp nào không thể phòng chống hiệu quả tấn công khai thác lỗi tràn

bộ đệm gồm:

A, Sử dụng các thư viện an toàn hoặc ngôn ngữ lập trình không gây tràn

B, Đặt cơ chế không cho phép thự hiện mã trong dữ liệu (DEP)

C, Sử dụng công cụ gỡ rối để ngăn chặn tràn trong thời gian vận hành

D, Kiểm tra mã nguồn để tìm điểm có có khả năng gây tràn và khắc phục.

24,Việc quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề

kháng cho hệ thống cần được thực hiện theo nguyên tắc chung là:

A, Cân bằng giữa an toàn, tin cậy và rẻ tiền

B, Cân bằng giữa an toàn, hữu dụng và rẻ tiền

C, Cân bằng giữa an toàn, rẻ tiền và chất lượng

D, Cân bằng giữa an toàn, hữu dụng và tin cậy

25,Trong 7 vùng cơ sở hạ tầng CNTT, vùng nào có mối đe dọa và nguy cơ nhất

A, vùng mạng WAN/Internet

B, Vùng truy nhập từ xa

C, Vùng mạng Lan

D, Vùng người dùng

26, Lỗ hổng bảo mật (Security vulnerability) là một điểm yếu tồn tại trong một

hệ thống cho phép tin tặc:

A, Khai thác nhằm đánh cắp thông tin hệ thống

B, Khai thác, tấn công phá hoại, gây tê liệt hệ thống

C, Khai thác nhằm chiếm quyền điều khiển hệ thống

D, Khai thác tổn hại đến các thuộc tính an ninh của hệ thống đó

27, ATTT gồm 2 lĩnh vực chính là:

A, An ninh mạng và An toàn hệ thống

B, An toàn máy tính và an toàn internet

C, An toàn máy tính và an ninh mạng

D, An toàn CNTT và đảm bảo thông tin

28, ATTT là gì?

A, là việc bảo vệ chống sử dụng, tiết lộ, sửa đổi, vận chuyển hoặc phá hủy

thông tin một cách trái phép

B, Là việc phòng chống đánh cắp thông tin

C, Là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi hoặc phá hủy thông

tin một cách trái phép.

D, Là việc phòng chống tấn công mạng

29, NOTE Các lỗ hổng an ninh trong HĐH máy chủ là mối đe dọa thuộc vùng nào

trong 7 vùng cơ sở hạ tầng CNTT?

A, Vùng mạng Lan

B, Vùng máy trạm

D, Vùng mạng Lan-to-Wan

C, Vùng mạng Wan

Câu 31, Một thông điệp có nội dung nhạy cảm truyền trên mạng bị sửa đổi. Các

thuộc tính an toàn nào bị vi phạm

A, bí mật, toàn vẹn và sẵn dùng

B, Bí mật và toàn vẹn

C, Bí mật

D, Toàn vẹn

32, Các thành phần chính của hệ thống máy tính

A, CPU, HĐH và các ứng dụng

B, CPU, bộ nhớ , HĐH và các ứng dụng

C, Hệ thống phần cứng và phần mềm

D, CPU, bộ nhớ, HĐ và hệ thống BUS truyền dẫn.

33,Tính bí mật của thông tin có thể đảm bảo bằng:

A, Bảo vệ vật lý

B, Bảo vệ vật lý, VPN hoặc mã hóa

C, Sử dụng VPN

D, Các kỹ thuật mã hóa

34,

Việc thực thi quản lý ATTT cần được thực hiện theo chu trình lặp lại là do:

A, Trình độ cao của tin tặc và công cụ tấn công ngày càng phổ biến

B, Số lượng và khả năng phá hoại của các phần mềm độc hại ngày càng tăng

C, Máy tính, HĐH và các phần mềm được nâng cấp nhanh chóng

D, Các điều kiện bên trong và bên ngoài hệ thống thay đổi theo thời gian

35: Biện pháp không thể phòng chống hiệu quả tấn công khai thác lỗi tràn bộ

đệm:

A, Sử dụng công cụ gỡ rối để ngăn chặn tràn trong thời gian vận hành

B, Sử dụng các thư viện an toàn hoặc ngôn ngữ lập trình không gây tràn

C, Kiểm tra mã nguồn để tìm kiếm có khả năng gây tràn và khắc phục

D, Đặt cơ chế không cho phép thực hiện mã trong dữ liệu( DEF)

36, Người sử dụng hệ thống thông tin quản lý trong mô hình 4 loại hệ thống

thông tin là:

A, Quản lý bộ phận

B, Quản lý cao cấp

C, Giám đốc điều hành

D, Nhân Viên

37,Một trong các nội dung quan trọng nhất của quản lý ATTT là:

A, Quản lý rủi ro

B, Quản lý các ứng dụng

C, Quản lý hệ điều hành

D, Quản lý hệ thống

38, Tại sao cần phải đảm bảo AT cho thông tin?

A, Do có quá nhiều phần mềm độc hại

B, Do có nhiều thiết bị kết nối mạng Internet

C, Do có nhiều thiết bị kết nối mạng Internet với nhiều mối đe dọa

D, Do có quá nhiều nguy cơ tấn công mạng

26. Hệ thống thông tin là:

A. Một hệ thống tích hợp các thành phần nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin, tri thức và các sản phẩm số

B. Một hệ thống gồm các thành phần phần cứng và phần mềm nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin

C. Một hệ thống gồm các thành phần phần cứng nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin, tri thức và các sản phẩm số

D. Một hệ thống gồm các thành phần phần mềm nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin, tri thức và các sản phẩm số

40,Một điểm yếu điển hình trong hệ thống điều khiển truy nhập là việc sử dụng

mật khẩu dễ đóa hoặc mật khẩu lưu dưới dạng rõ. Đây là điểm yếu thuộc khâu:

A, Quản trị

B, Trao quyền

C, Xác thực

D, Xác thực và trao quyền

**Chương 1-2 (Part 2)**

1. Mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin thường gồm các lớp:  
A. An ninh tổ chức, An ninh mạng và Điều khiển truy cập  
B. An ninh tổ chức, Tưởng lửa và Điều khiển truy cập  
C. An ninh tổ chức, An ninh mạng và An toàn hệ điều hành và ứng dụng  
D. An ninh tổ chức, An ninh mạng và An ninh hệ thống

2. An toàn thông tin gồm hai lĩnh vực chính là:  
A. An ninh mạng và An toàn hệ thống  
B. An toàn máy tính và An toàn Internet  
C. An toàn máy tính và An ninh mạng  
D. An toàn công nghệ thông tin và Đảm bảo thông tin

3. Tại sao cần phải đảm bảo an toàn cho thông tin?  
A. Do có nhiều thiết bị kết nối mạng Internet với nhiều nguy cơ và đe dọa  
B. Do có quá nhiều phần mềm độc hại  
C. Do có quá nhiều nguy cơ tấn công mạng  
D. Do có nhiều thiết bị kết nối mạng Internet

4. An toàn hệ thống thông tin là:  
A. Việc đảm bảo thông tin trong hệ thống không bị đánh cắp  
B. Việc đảm bảo cho hệ thống thông tin hoạt động trơn tru, ổn định  
C. Việc đảm bảo cho hệ thống thông tin không bị tấn công  
D. Việc đảm bảo các thuộc tính an ninh, an toàn của hệ thống thông tin

5. Người sử dụng hệ thống thông tin quản lý trong mô hình 4 loại hệ thống thông tin là:  
A. Quản lý cao cấp  
B. Giám đốc điều hành  
C. Nhân viên  
D. Quản lý bộ phận

6. Nguyên tắc cơ bản cho đảm bảo an toàn thông tin, hệ thống và mạng là:  
A. Phòng vệ nhiều lớp có chiều sâu  
B. Cần đầu tư trang thiết bị và chuyên gia đảm bảo an toàn  
C. Cần mua sắm và lắp đặt nhiều thiết bị an ninh chuyên dụng  
D. Cân bằng giữa tính hữu dụng, chi phí và tính năng

7. Một trong các nội dung rất quan trọng của quản lý an toàn thông tin là:  
A. Quản lý các ứng dụng  
B. Quản lý hệ thống  
C. Quản lý hệ điều hành  
D. Quản lý rủi ro

8. Một thông điệp có nội dung nhạy cảm truyền trên mạng bị sửa đổi. Các thuộc tính an toàn thông tin nào bị vi phạm?  
A. Bí mật, Toàn vẹn và sẵn dùng  
B. Bí mật và Toàn vẹn  
C. Bí mật  
D. Toàn vẹn

9. Nguy cơ bị tấn công từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS) thường gặp ở vùng nào trong 7 vùng cơ sở hạ tầng CNTT?  
A. Vùng máy trạm  
B. Vùng mạng WAN  
C. Vùng mạng LAN-to-WAN  
D. Vùng mạng LAN

10. An toàn thông tin (Information Security) là gì?  
A. Là việc phòng chống đánh cắp thông tin  
B. Là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép  
C. Là việc bảo vệ chống sử dụng, tiết lộ, sửa đổi, vận chuyển hoặc phá hủy thông tin một cách trái phép  
D. Là việc phòng chống tấn công mạng

11. Tìm phát biểu đúng trong các phát biểu sau:  
A. Mối đe dọa là bất kỳ một hành động tấn công nào vào hệ thống mạng.  
B. Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống.  
C. Mối đe dọa là bất kỳ một hành động tấn công nào vào hệ thống máy tính.  
D. Mối đe dọa là bất kỳ một hành động tấn công nào vào hệ thống máy tính và mạng.

12. Đây là một trong các biện pháp phòng chống tấn công khai thác lỗi tràn bộ đệm?  
A. Sử dụng tường lửa  
B. Sử dụng công nghệ xác thực mạnh  
C. Sử dụng các kỹ thuật mật mã  
D. Sử dụng cơ chế cẩm thực hiện mã trong dữ liệu

13. Trong tấn công khai thác lỗi tràn bộ đệm, tin tặc thường sử dụng một số lệnh NOP (No Operation) ở phần đầu của mã tấn công. Mục đích của việc này là để:  
A. Tăng khả năng phá hoại của mã tấn công  
B. Tăng khả năng gây tràn bộ đệm  
C. Tăng khả năng mã tấn công được thực hiện  
D. Tăng khả năng gây lỗi chương trình

14. Tìm phát biểu đúng trong các phát biểu sau:  
A. Điểm yếu hệ thống chỉ xuất hiện trong các mô đun phần mềm  
B. Điểm yếu chỉ xuất hiện khi hệ thống bị tấn công  
C. Điểm yếu hệ thống có thể xuất hiện trong cả các mô đun phần cứng và phần mềm  
D. Điểm yếu hệ thống chỉ xuất hiện trong các mô đun phần cứng

15. Các vùng bộ nhớ thường bị tràn gồm:  
A. Ngăn xếp (Stack) và vùng nhớ cấp phát động (Heap)  
B. Ngăn xếp (Stack) và Bộ nhớ đệm (Cache)  
C. Hàng đợi (Queue) và vùng nhớ cấp phát động (Heap)  
D. Hàng đợi (Queue) và Ngăn xếp (Stack)

16. Các thành phần chính của hệ thống máy tính gồm:  
A. CPU, Bộ nhớ, HDD, hệ điều hành và các ứng dụng  
B. CPU, hệ điều hành và các ứng dụng  
C. Hệ thống phần cứng và Hệ thống phần mềm

D. CPU, Bộ nhớ, HDD và Hệ thống bus truyền dẫn

17. Nguyên nhân của sự tồn tại các điểm yếu trong hệ thống có thể do:  
A. Lỗi thiết kế, lỗi cài đặt và lập trình  
B. Tất cả các khâu trong quá trình phát triển và vận hành  
C. Lỗi quản trị  
D. Lỗi cấu hình hoạt động

18. Trên thực tế, có thể giảm khả năng bị tấn công nếu có thể...  
A. Triệt tiêu được hết các nguy cơ  
B. Triệt tiêu được hết các mối đe dọa  
C. Giảm thiểu các lỗ hổng bảo mật  
D. Kiểm soát chặt chẽ người dùng

19. Sâu SQL Slammer tấn công khai thác lỗi tràn bộ đệm trong hệ quản trị cơ sở dữ liệu:  
A. SQL Server 2012  
B. SQL Server 2000  
C. SQL Server 2008  
D. SQL Server 2003

20. Các lỗ hổng bảo mật thường tồn tại nhiều nhất trong thành phần nào của hệ thống:  
A. Hệ điều hành  
B. Các dịch vụ mạng  
C. Các ứng dụng  
D. Các thành phần phần cứng

21. Các kỹ thuật và công cụ thường được sử dụng trong an ninh mạng bao gồm:  
A. VPN, SSL/TLS, PGP  
B. Điều khiển truy nhập  
C. Điều khiển truy nhập, tường lửa, proxy và các giao thức bảo mật, ứng dụng dựa trên mật mã  
D. Tường lửa, proxy

22. Các thành phần của an toàn thông tin gồm:  
A. An toàn máy tính, An ninh mạng, Quản lý ATTT và Chính sách ATTT  
B. An toàn máy tính và dữ liệu, An ninh mạng, Quản lý ATTT và Chính sách ATTT  
C. An toàn máy tính, An ninh mạng, Quản lý rủi ro ATTT và Chính sách ATTT  
D. An toàn máy tính, An toàn dữ liệu, An ninh mạng, Quản lý ATTT

23. Trong tấn công khai thác lỗi tràn bộ đệm, tin tặc thường sử dụng shellcode. Shellcode đó là dạng:  
A. Mã Java  
B. Mã C/C++  
C. Mã máy  
D. Mã Hợp ngữ

24. Các yêu cầu cơ bản trong đảm bảo an toàn thông tin và an toàn hệ thống thông tin gồm:  
A. Bảo mật, Toàn vẹn và Khả dụng  
B. Bảo mật, Toàn vẹn và Sẵn dùng  
C. Bí mật, Toàn vẹn và Sẵn dùng  
D. Bí mật, Toàn vẹn và không chối bỏ

25. Việc thực thi quản lý ATTT cần được thực hiện theo chu trình lặp lại là do  
A. Các điều kiện bên trong và bên ngoài hệ thống thay đổi theo thời gian  
B. Trình độ cao của tin tặc và công cụ tấn công ngày càng phổ biến  
C. Số lượng và khả năng phá hoại của các phần mềm độc hại ngày càng tăng  
D. Máy tính, hệ điều hành và các phần mềm được nâng cấp nhanh chóng

26. Hệ thống thông tin là:  
A. Một hệ thống tích hợp các thành phần nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin, tri thức và các sản phẩm số  
B. Một hệ thống gồm các thành phần phần cứng và phần mềm nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin  
C. Một hệ thống gồm các thành phần phần cứng nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin, tri thức và các sản phẩm số  
D. Một hệ thống gồm các thành phần phần mềm nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin, chuyển giao thông tin, tri thức và các sản phẩm số

27. Trong tấn công khai thác lỗi tràn bộ đệm, tin tặc thường sử dụng một số lệnh NOP (No Operation) ở phần đầu của mã tấn công. Mục đích của việc này là để:  
A. Tăng khả năng phá hoại của mã tấn công  
B. Tăng khả năng gây lỗi chương trình  
C. Tăng khả năng gây tràn bộ đệm  
D. Tăng khả năng mã tấn công được thực hiện

28. Tính bí mật của thông tin có thể được đảm bảo bằng:  
A. Bảo vệ vật lý  
B. Các kỹ thuật mã hóa  
C. sử dụng VPN  
D. Bảo vệ vật lý, VPN, hoặc mã hóa

29. Lỗ hổng bảo mật (Security vulnerability) là một điểm yếu tồn tại trong một hệ thống cho phép tin tặc:  
A. Khai thác nhằm đánh cắp các thông tin trong hệ thống  
B. Khai thác gây tổn hại đến các thuộc tính an ninh của hệ thống đó  
C. Khai thác, tấn công phá hoại và gây tê liệt hệ thống  
D. Khai thác nhằm chiếm quyền điều khiển hệ thống

30. Đảm bảo thông tin (Information assurance) thường được thực hiện bằng cách:  
A. Sử dụng kỹ thuật tạo dự phòng ra đĩa cứng  
B. Sử dụng kỹ thuật tạo dự phòng ra băng từ  
C. Sử dụng kỹ thuật tạo dự phòng ngoại vi  
D. Sử dụng kỹ thuật tạo dự phòng cục bộ

31. Lỗi tràn bộ đệm là lỗi trong khâu:  
A. Kiểm thử phần mềm  
B. Thiết kế phần mềm  
C. Lập trình phần mềm  
D. Quản trị phần mềm

32. Đâu là dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng?  
A. Lỗi tràn bộ đệm  
B. Lỗi quản trị  
C. Lỗi cấu hình  
D. Lỗi thiết kế

33. Quản lý các bản vá và cập nhật phần mềm là phần việc thuộc lớp bảo vệ nào trong mô hình tổng thể đảm bảo an toàn hệ thống thông tin?  
A. Lớp an ninh mạng  
B. Lớp an ninh hệ thống  
C. Lớp an ninh cơ quan/tổ chức  
D. Lớp an ninh hệ điều hành và phần mềm

34. Khi khai thác lỗi tràn bộ đệm, tin tặc thường chèn mã độc, gây tràn và ghi đè để sửa đổi thành phần nào sau đây của bộ nhớ Ngăn xếp để chuyển hướng nhằm thực hiện mã độc của mình:  
A. Các biển đầu vào của hàm  
B. Bộ đệm hoặc biển cục bộ của hàm  
C. Con trỏ khung ngăn xếp (sfp)  
D. Địa chỉ trở về của hàm

35. Khác biệt cơ bản của vi rút và sâu là:  
A. Vi rút có khả năng tự lây lan mà không cần tương tác của người dùng  
B. Sâu có khả năng tự lây lan mà không cần tương tác của người dùng  
C. Sâu Có khả năng phá hoại lớn lơn  
D. Vi rút có khả năng phá hoại lớn lớn

36. Dạng tấn công gây ngắt quãng dịch vụ hoặc kênh truyền thông cho người dùng bình thường là:  
A. Interceptions  
B. Fabrications  
C. Interruptions  
D. Modifications

37. Tấn công nghe lén là kiểu tấn công:  
A. Thụ động  
B. Chủ động  
C. Chiếm quyền điều khiển  
D. Chủ động và bị động

38. Dạng tấn công chặn bắt thông tin truyền trên mạng để sửa đổi hoặc lạm dụng là:  
A. Fabrications  
B. Modifications  
C. Interruptions  
D. Interceptions

39. Có thể phòng chống tấn công Smurf bằng cách cấu hình các máy và router không trả lời...  
A. Các yêu cầu ICMP hoặc các yêu cầu phát quảng bá  
B. Các yêu cầu TCP hoặc các yêu cầu phát quảng bá  
C. Các yêu cầu UPD hoặc các yêu cầu phát quảng bá  
D. Các yêu cầu HTTP hoặc các yêu cầu phát quảng bá

40. Đâu là một kỹ thuật tấn công Dos?  
A. UDP Ping  
B. DNS Cache Poisoning  
C. Smurf  
D. DNS spoofing

41. Dạng tấn công giả mạo thông tin thường để đánh lừa người dùng thông thường là:  
A. Modifications  
B. Fabrications  
C. Interruptions  
D. Interceptions

42. Kỹ thuật tấn công Smurf sử dụng giao thức ICMP và Cơ chế gửi...  
A. Unicast  
B. Multicast  
C. Anycast  
D. Broadcast

43. Trong tấn công DDoS phản chiếu hay gián tiếp, có sự tham gia của một số lượng lớn máy chủ trên mạng Internet không bị tin tặc  
chiếm quyền điều khiển. Các máy chủ này được gọi là...  
A. Reflectors  
B. Injectors  
C. Requesters  
D. Forwarders

44. Pharming là kiểu tấn công vào...  
A. Máy chủ web  
B. Máy chủ cơ sở dữ liệu của trang web  
C. Máy chủ và máy khách web  
D. Máy khách/trình duyệt web

45. Đây là một công cụ kiểm tra lỗ hổng tấn công chèn mã SQL trên các website:  
A. SQLCheck  
B. SQL Server  
C. SQLmap  
D. SQLite

46. Khác biệt cơ bản giữa tấn công DoS và DDoS là:  
A. Phạm vi tấn công  
B. Mức độ gây hại  
C. Kỹ thuật tấn công  
D. Tần suất tấn công

47. Mục đích chính của tấn công giả mạo địa chỉ IP là:  
A. Để vượt qua các hệ thống IPS và IDS  
B. Để vượt qua các hàng rào kiểm soát an ninh  
C. Để đánh cắp các dữ liệu nhạy cảm trên máy trạm  
D. Để đánh cắp các dữ liệu nhạy cảm trên máy chủ

48. Các máy tính ma/máy tính bị chiếm quyền điều khiển thường được tin tặc sử dụng để...  
A. Gửi các yêu cầu tấn công chèn mã  
B. Đánh cắp dữ liệu từ máy chủ cơ sở dữ liệu  
C. Gửi thư rác, thư quảng cáo  
D. Thực hiện tấn công tràn bộ đệm.

49. Trong dạng tấn công vào mật khẩu dựa trên từ điển, tin tặc đánh cắp mật khẩu của người dùng bằng cách:  
A. Tìm mật khẩu trong từ điển các mật khẩu  
B. Thử các từ có tần suất sử dụng cao làm mật khẩu trong từ điển  
C. Vét cận các mật khẩu có thể có  
D. Lắng nghe trên đường truyền để đánh cắp mật khẩu

50. Một trong các phương thức lây lan thường gặp của sâu mạng là:  
A. Lây lan thông qua sao chép các file  
B. Lây lan thông qua dịch vụ POP  
C. Lây lan thông qua khả năng thực thi từ xa  
D. Lây lan thông qua Microsoft Office

51. Đây là một kỹ thuật tấn công Dos?  
A. SYN requests  
B. DNS spoofing  
C. IP spoofing  
D. Ping of death

53. Mật khẩu an toàn trong thời điểm hiện tại là mật khẩu có:  
A. Chứa các ký tự từ nhiều dạng ký tự  
B. Khả năng chống tấn công phát lại và chứa các ký tự từ nhiều dạng ký tự  
C. Độ dài từ 8 ký tự trở lên, gồm chữ cái hoa, thường, chữ số và ký tự đặc biệt  
D. Độ dài lớn hơn hoặc bằng 8 ký tự

54. Một trong các mối đe dọa an toàn thông tin thường gặp là:  
A. Phần mềm nghe lén  
B. Phần mềm quảng cáo  
C. Phần mềm phá mã  
D. Phần mềm độc hại

55. Nguy cơ cao nhất mà một cuộc tấn công chèn mã SQL có thể gây ra cho một hệ thống là:  
A. Đánh cắp các thông tin trong cơ sở dữ liệu  
B. Chèn, xóa hoặc sửa đổi dữ liệu  
C. Vượt qua các khâu xác thực người dùng  
D. Chiếm quyền điều khiển hệ thống

56. Một trong các biện pháp có thể sử dụng để phòng chống tấn công người đứng giữa là:  
A. Sử dụng các hệ thống IPS/IDS  
B. Sử dụng chứng chỉ số để xác thực thông tin nhận dạng các bên  
C. Sử dụng mã hóa để đảm bảo tính bí mật các thông điệp truyền  
D. Sử dụng tường lửa để ngăn chặn

57. Macro viruses là loại viruses thường lây nhiễm vào...  
A. Các file tài liệu của bộ phần mềm Open Office  
B. Các file tài liệu của bộ phần mềm Microsoft Exchange  
C. Các file tài liệu của bộ phần mềm Microsoft SQL  
D. Các file tài liệu của bộ phần mềm Microsoft Office

58. Tấn công kiểu Social Engineering là dạng tấn công khai thác yếu tố nào sau đây trong hệ thống?  
A. Máy trạm  
B. Người dùng  
C. Máy chủ  
D. Hệ điều hành & ứng dụng

59. Câu lệnh SQL nào tin tặc thường sử dụng trong tấn công chèn mã SQL để đánh cắp các thông tin trong cơ sở dữ liệu?  
A. UNION INSERT  
B. UNION SELECT  
C. SELECT UNION  
D. INSERT SELECT

60. Phishing là một dạng của loại tấn công sử dụng...  
A. Kỹ thuật chèn mã  
B. Kỹ thuật giả mạo địa chỉ IP  
C. Kỹ thuật gây tràn bộ đệm  
D. Kỹ thuật xã hội

61. Các dạng phần mềm độc hại (malware) có khả năng tự nhân bản gồm:  
A. Virus, zombie, spyware  
B. Virus, trojan, zombie  
C. Virus, worm, trojan  
D. Virus, worm, zombie

62. Một trong các cách virus thường sử dụng để lây nhiễm vào các chương trình khác là:  
A. Ẩn mã của virus  
B. Thay thế các chương trình  
C. Xáo trộn mã của virus  
D. Sửa đổi các chương trình

63. Trong tấn công DDoS phản chiếu hay gián tiếp, có sự tham gia của một số lượng lớn máy chủ trên mạng Internet không bị tin tặc chiếm quyền điều khiển. Các máy chủ này được gọi là...  
A. Reflectors  
B. Requesters  
C. Forwarders  
D. Injectors

64. Mục đích chính của tấn công giả mạo địa chỉ IP là:  
A. Để vượt qua các hệ thống IPS và IDS  
B. Để vượt qua các hàng rào kiểm soát an ninh  
C. Để đánh cắp các dữ liệu nhạy cảm trên máy trạm  
D. Để đánh cắp các dữ liệu nhạy cảm trên máy chủ

65. Trojan horses là dạng phần mềm độc hại thường giành quyền truy nhập vào các file của người dùng khai thác cơ chế điều khiển truy nhập...  
A. МАС  
B. Role-Based  
C. Rule-Based  
D. DAC

66. Một trong các biện pháp hiệu quả để phòng chống Macro virus :  
A.Cấm tự động thực hiện macro trong Microsoft Exchange  
B.Sử dụng tường lửa  
C.Cấm tự động thực hiện macro trong Microsoft Office  
D.Sử dụng IPS/IDS

67. Đâu là một biện pháp phòng chống SYN Floods:  
A.SYN Firewalls  
B. SYN IDS  
C. SYN Proxy  
D. SYN Cache

68. Các zombie thường được tin tặc sử dụng để:  
A. Đánh cắp dữ liệu từ máy chủ CSDL  
B. Thực hiện tấn công DoS  
C. Thực hiện tấn công tràn bộ đệm  
D. Thực hiện tấn công DDoS

69. Tấn công kiểu Social Engineering có thể cho phép tin tặc:  
A. Đánh cắp toàn bộ dữ liệu trên máy chủ  
B. Phá hỏng máy chủ  
C. Đánh cắp thông tin nhạy cảm trong cơ sở dữ liệu máy chủ  
D. Đánh cắp thông tin nhạy cảm của người dùng

52. Tấn công từ chối dịch vụ (Dos - Denial of Service Attacks) là dạng tấn công có khả năng...  
A. Gây hư hỏng phần cứng máy chủ  
B. Cản trở người dùng hợp pháp truy nhập các tài nguyên hệ thống  
C. Đánh cắp dữ liệu trong hệ thống  
D. Cản trở người dùng hợp pháp truy nhập các file dữ liệu của hệ thống

**Chương 3**

1.Đâu không phải một giải thuật hàm băm?  
A. MD2  
B. MD3  
C.MD4  
D.MD5

2.Một hệ mã hóa gồm các khâu nào?  
A. Mã hóa và tạo khóa  
B. Tạo khóa và phân phối khóa  
C. Mã hóa và giải mã  
D. Tạo khóa và giải mã

3.Mã hóa là gì?  
A. Là hành động làm thông tin trở nên bí mật  
B. Là hành động xáo trộn bản rõ trở thành bản mã  
C. Là hành động xáo trộn bản mã thành bản rõ  
D. Là hành động khiến những người không liên quan không đọc được thông tin

4.Giải mã là gì?  
A. Là hành động làm thông tin trở nên bí mật  
B. Là hành động xáo trộn bản rõ trở thành bản mã  
C. Là hành động xáo trộn bản mã thành bản rõ  
D. Là hành động khiến những người không liên quan không đọc được thông tin

5.Như thế nào là một bộ mã hóa thông tin(Cipher)?  
A. Là một giải thuật để mã hóa và giải mã thông tin  
B. Là bộ khóa và chìa để giải mã  
C. Là bản rõ và bản mã  
D. Là một chuỗi dùng trong giải thuật mã hóa và giải mã

6.Như thế nào được gọi là Key?  
A. Là một giải thuật để mã hóa và giải mã thông tin  
B. Là bộ khóa và chìa để giải mã  
C. Là bản rõ và bản mã  
D. Là một chuỗi dùng trong giải thuật mã hóa và giải mã

7.Như nào được gọi là mã hóa khóa bí mật?  
A. Một khóa được sử dụng cho cả giải thuật mã hóa và giải mã  
B. Một cặp khóa được sử dụng, trong đó khóa công khai để mã hóa,  
khóa bí mật để giải mã.  
C. Một cặp khóa được sử dụng, trong đó khóa bí mật để mã hóa,  
khóa công khai để giải mã.  
D. Khóa công khai được sử dụng cho cả 2 giải thuật mã hóa và giải mã

8.Như nào được gọi là mã hóa khóa công khai?  
A. Một khóa được sử dụng cho cả giải thuật mã hóa và giải mã  
B. Một cặp khóa được sử dụng, trong đó khóa công khai để mã hóa,  
khóa bí mật để giải mã.  
C. Một cặp khóa được sử dụng, trong đó khóa bí mật để mã hóa,  
khóa công khai để giải mã.  
D. Khóa công khai được sử dụng cho cả 2 giải thuật mã hóa và giải mã

9.Không gian khóa là gì?  
A. Nơi lưu giữ khóa của hệ mã hóa  
B. Tổng số khóa bí mật của hệ mã hóa  
C. Tổng số khóa có thể có của một hệ mã hóa  
D. Tổng số khóa công khai của hệ mã hóa

10.Hàm băm là gì?  
A. Là hàm chia nhỏ đoạn mã thành các bit trong mã hóa dòng  
B. là hàm chia nhỏ đoạn mã thành các khối (block) trong mã hóa khối  
C. là một ánh xạ chuyển các dữ liệu có kích thước cố định về dữ liệu có kích thước thay đổi.  
D. là một ánh xạ chuyển các dữ liệu có kích thước thay đổi về dữ liệu có kích thước cố định.

10.Nếu sử dụng khóa có kích thước 64 bit thì không gian khóa là bao nhiêu?  
A. 64  
B. 2^64  
C.2^32  
D.32

11.Như thế nào là hàm băm 1 chiều?  
A. Là hàm băm mã hóa đơn giản nhưng giải mã rất phức tạp, không khả thi về mặt tính toán  
B. Là hàm băm chỉ có thể mã hóa mà không thể giải mã  
C. Là hàm hăm giải mã đơn giản, không an toàn  
D. Là hàm băm mã hóa rất phức tạp, không khả thi về mặt tính toán

12.Như nào được gọi là phá mã?  
A.là quá trình giải mã thông điệp đã bị mã hóa (ciphertext) mà không cần có trước thông tin về giải thuật mã hóa (Encryption algorithm) nhưng cần có khóa mã (Key).  
B. là quá trình giải mã thông điệp đã bị mã hóa (ciphertext) mà cần có trước thông tin về giải thuật mã hóa (Encryption algorithm) và khóa mã (Key).  
C. là quá trình giải mã thông điệp đã bị mã hóa (ciphertext) mà không cần có trước thông tin về giải thuật mã hóa (Encryption algorithm) và khóa mã (Key).  
D. là quá trình giải mã thông điệp đã bị mã hóa (ciphertext) mà cần có trước thông tin về giải thuật mã hóa (Encryption algorithm) nhưng không cần có khóa mã (Key).

13.Mã hoá thông tin có thể được sử dụng để đảm bảo  
an toàn thông tin trên đường truyền với các thuộc  
tính:  
A. Toàn vẹn, bí mật, xác thực, không thể chối bỏ  
B. Toàn vẹn, bảo mật, không thể chối bỏ  
C. Toàn vẹn, bảo mật, xác thực, trao quyền  
D. Toàn vẹn, bí mật, xác thực, trao quyền

14.Hệ mã hóa được cấu thành từ hai thành phần nào?  
A. Mã hóa và giải mã  
B. Bản mã và bản rõ  
C. Phương pháp mã hóa và tập các khóa  
D. Không gian khóa và bản mã

15.Hệ mã hóa được cấu thành từ hai thành phần nào?  
A. Mã hóa và giải mã  
B. Bản mã và bản rõ  
C. Giải thuật và không gian khóa  
D. Giải thuật và bản mã

16.Tính an toàn của một hệ mã hóa phụ thuộc vào  
A. Giữ bí mật bản mã  
B. Giữ bí mật mã hóa  
C. Giữ bí mật giải thuật  
D. Giữ bí mật khóa mã

17.Tính an toàn của một hệ mã hóa không nên phụ thuộc vào  
A. Giữ bí mật bản mã  
B. Giữ bí mật mã hóa  
C. Giữ bí mật giải thuật  
D. Giữ bí mật khóa mã

18.Mã hóa dòng là gì?  
A. là kiểu mã hóa mà từng bít (hoặc ký tự) của dữ liệu được kết hợp với từng bít (hoặc ký tự) tương ứng của khóa để tạo thành bản mã.  
B. là kiểu mã hóa mà dữ liệu được chia ra thành từng khối có kích thước cố định để mã hóa.  
C. Là kiểu mã hóa tất cả khối dữ liệu mà không chia ra thành các phần nhỏ hơn để mã hóa  
D. Là kiểu mã hóa tất cả dòng dữ liệu mà không chia ra thành các phần nhỏ hơn để mã hóa

19.Mã hóa khối là gì?  
A. là kiểu mã hóa mà từng bít (hoặc ký tự) của dữ liệu được kết hợp với từng bít (hoặc ký tự) tương ứng của khóa để tạo thành bản mã.  
B. là kiểu mã hóa mà dữ liệu được chia ra thành từng khối có kích thước cố định để mã hóa.  
C. Là kiểu mã hóa tất cả khối dữ liệu mà không chia ra thành các phần nhỏ hơn để mã hóa  
D. Là kiểu mã hóa tất cả dòng dữ liệu mà không chia ra thành các phần nhỏ hơn để mã hóa

20.Chế độ hoạt động của mã hóa khối?  
A. ECB, CBC, CFB, OFB  
B. AES, CBC, CFB, OFB  
C.ECB, DES, CFB, OFB  
D. ECB, CBC, CFB, RSA

21.Đâu là các tiêu chuẩn đánh giá hệ mã hóa  
A. Tính năng, độ an toàn, chế độ hoạt động, thuật toán, độ dễ cài đặt  
B. Tính năng, độ bảo mật, chế độ hoạt động, hiệu năng, độ dễ cài đặt  
C. Tính năng, độ an toàn, chế độ hoạt động, hiệu năng, độ dễ cài đặt  
D. Tính năng, độ an toàn, không gian khóa, hiệu năng, độ dễ cài đặt

22.Đâu là ứng dụng của các kỹ thuật mã hóa  
A. Dịch vụ xác thực  
B. Điều khiển truy cập  
C. Các công cụ đánh giá và phân tích logs  
D. Tất cả đều đúng

23.Đâu không phải là ứng dụng của các kỹ thuật mã hóa  
A. Tất cả đều là ứng dụng của các kỹ thuật mã hóa  
B. Các sản phẩm quản lý ATTT  
C. Các công cụ cho đảm bảo an toàn cho truyền thông không dây  
D. Các nền tảng bảo mật như PKI, PGP

24.Đâu là ứng dụng của mã hóa?  
A. Các nền tảng bảo mật như PKI, PGP  
B. Các giao thức bảo mật như SSL/TLS, SSH, SET, IPSec  
C. Các hệ thống như VPN.  
D. Cả A,B,C đều đúng

25.Đâu không phải là một phương pháp mã hóa?  
A. DDOS  
B. đổi chỗ  
C. XOR  
D. thay thế

26.Đâu là một phương pháp mã hóa?  
A. SQL injection  
B. Vernam  
C. sniffer  
D. DOS

27.Hàm băm nào có đầu ra từ 0-512 bit  
A. MD2  
B. MD4  
C. MD5  
D. MD6

28.Đâu là các giải thuật mã hóa đối xứng  
A.RSA,Rabin, ElGamal  
B. RSA, DES, AES  
C.DES, Triple-DES,AES, IDEA  
D.Blowfish, Twofish ,RC4, RC5, RSA

29.Đâu là các giải thuật mã hóa không đối xứng?  
A.RSA,Rabin, ElGamal  
B. RSA, DES, AES  
C.DES, Triple-DES,AES, IDEA  
D.Blowfish, Twofish ,RC4, RC5, RSA

30.Câu nào sai khi nói về giải thuật mã hóa đối xứng?  
A. Mã khóa công khai  
B. Khóa bí mật  
C. Chỉ sử dụng một khóa trong quá trình giải mã và mã hóa  
D. Mã hóa khóa riêng

31.Đâu không phải là một phương pháp mã hóa?  
A. MAC  
B. đổi chỗ  
C. Sách- khóa chạy  
D. Hàm băm

32.Hàm băm được ứng dụng như thế nào?  
A. Là các thuật toán chia nhỏ và tóm tắt thông điệp để đảm bảo tính bí mật của thông điệp  
B.là các thuật toán để tạo các bản tóm tắt của thông điệp được sử dụng để nhận dạng và đảm bảo tính toàn vẹn của thông điệp.  
C. Cả hai ý trên đều đúng  
D. Cả hai ý trên đều sai

33.Phương pháp vernam được triển khai như thế nào?  
A. thực hiện sắp xếp lại các giá trị trong một khối để  
tạo bản mã  
B. thường được dùng trong các bộ phim trinh thám, trong đó việc mã hóa và giải mã sử dụng các khóa mã chứa trong các cuốn sách.  
C. sử dụng một tập ký tự để nối vào các ký tự của bản rõ để tạo bản mã.  
D.sử dụng phép toán logic XOR để tạo bản mã

34.Câu nào đúng khi nói về giải thuật mã hóa không đối xứng?  
A. Mã khóa công khai  
B. Cả A và D đều đúng  
C. Chỉ sử dụng một khóa trong quá trình giải mã và mã hóa  
D. Sử dụng 1 cặp khóa trong đó khóa công khai dùng để mã hóa và khóa bí mật dùng để giải mã

35.Đâu không phải đặc điểm của mã hóa khóa đối xứng?  
A.Kích thước khóa tương đối ngắn (64, 128, 192 bít)  
B.Tốc độ chậm  
C.Độ an toàn cao  
D.Khó khăn trong quản lý và phân phối khóa.

36.Đâu không phải đặc điểm của mã hóa khóa công khai?  
A.Kích thước khóa lớn (1024 - 3072 bít)  
B.Tốc độ chậm  
C.Độ an toàn cao  
D.Khó khăn trong quản lý và phân phối khóa.

37.Không gian khóa của DES?  
A. 64  
B. 128  
C. 192  
D. 256

38.Đâu không phải hông gian khóa của AES?  
A. 64  
B. 128  
C. 192  
D. 256

39.Kích thước đầu vào của DES  
  
A. 64  
B. 128  
C. 192  
D. 256

40.Kích thước đầu vào của AES  
  
A. 64  
B. 128  
C. 192  
D. 256

41.Câu nào sau đây không phải đặc điểm của DES?  
A.Không gian khóa nhỏ (khóa 64 bít, trong đó thực sử dụng 56 bít)  
B. Des được coi là không an toàn  
C. DES sử dụng chung một giải thuật cho mã hóa và giải mã.  
D. DES là giải thuật mã hóa bất đối xứng

42.Mã hóa 3-DES được thực hiện như nào?  
A. 3 lần mã hóa bằng 3 khóa lần lượt là K1,K2,K3  
B. Dùng K1, K2 để mã hóa, K3 để giải mã  
C. Mã hóa bằng K3, giải mã bằng K2, mã hóa bằng K1  
D. Dùng K1 để mã hóa, K2 và K3 để giải mã

43.Câu nào sau đây sai khi nói về số vòng lặp trong mã hóa AES?  
A. 8 vòng lặp với khóa 64bit;  
B.10 vòng lặp với khóa 128 bít;  
C.12 vòng lặp với khóa 192 bít;  
D.14 vòng lặp với khóa 256 bít.

44.Bước nào sau đây thuộc vòng khởi tạo AES  
A.SubBytes;  
B.ShiftRows;  
C.MixColumns  
D.AddRoundKey.

45.Bước nào sau đây không thuộc vòng cuối AES  
A.SubBytes;  
B.ShiftRows;  
C.MixColumns  
D.AddRoundKey.

46.AES có bao nhiêu vòng lặp chính  
A. N với N là số vòng lặp  
B. N+1 với N là số vòng lặp  
C. N-1 với N là số vòng lặp  
D. N-2 với N là số vòng lặp

47.Các bước mở rộng khóa sử dụng thủ tục sinh  
khóa Rijndael:  
A. Rotword - Subbyte - Rcon - ShiftRow  
B. Rotword - Subbyte - MixColumns - ShiftRow  
C.AddRoundKey - Subbyte - Rcon - ShiftRow  
D.AddRoundKey - Subbyte - MixColumns - ShiftRow

48.Addroundkey trong AES sử dụng phép toán gì?  
A. NOR  
B. OR  
C. XOR  
D.AND

49.Đâu là đặc điểm không đúng trong việc sử dụng khóa của RSA?  
A.Khóa công khai (Public key) dùng để mã hóa;  
B.Khóa riêng (Private key) dùng để giải mã.  
C.Chỉ khóa riêng cần giữ bí mật. Khóa công khai có thể công bố rộng rãi.  
D. Khóa bí mật dùng để mã hóa, khóa công khai dùng để giải mã

50.Câu nào sau đây sai về thủ tục sinh khóa của RSA?  
A.Φ(n) = (p-1) x (q-1)  
B.(n, e) là khóa bí mật, (n, d) là khóa công khai.  
C.0 < e < Φ(n) và gcd(e, Φ(n)) = 1  
D.d ≡ e-1 mod Φ(n), hoặc (d x e) mod Φ(n) = 1

51.Câu nào sau đây không phải tính chất của MDC  
A. Tính năng là mã phát hiện sửa đổi  
B. Tính năng là mã xác thực thông điệp  
C. Thường được sử dụng để tạo chuỗi đại diện cho thông  
điệp và dùng kết hợp với các biện pháp khác để đảm bảo tính  
toàn vẹn của thông điệp;  
D.thuộc loại hàm băm không khóa;

52.Câu nào sau đây không phải tính chất của MAC  
A. Message authentication codes  
B. Tính năng là mã xác thực thông điệp  
C. được dùng để đảm bảo tính toàn vẹn của thông  
điệp mà không cần một biện pháp bổ sung khác;  
D.thuộc loại hàm băm không khóa;

53.Ứng dụng nào không phải của MD5?  
A.Chuỗi đảm bảo tính toàn vẹn thông điệp;  
B.Tạo chuỗi kiểm tra lỗi - Checksum;  
C.Mã hóa mật khẩu.  
D.Giải mã thông điệp

54.Đầu ra của MD5?  
A. 256  
B. 128  
C. 32  
D. 512

55.Đầu ra của SHA1?  
A. 256  
B. 128  
C. 160  
D. 512

56.Ứng dụng nào của SHA1?  
A.Chuỗi đảm bảo tính toàn vẹn thông điệp;  
B.Tạo chuỗi kiểm tra lỗi - Checksum;  
C.Mã hóa mật khẩu.  
D. đảm bảo tính xác thực và toàn vẹn thông điệp.

57.Kích thước các khối của MD5?  
A.512  
B.128  
C.256  
D.64

58.Kích thước các khối của SHA1?  
A.512  
B.128  
C.256  
D.64

59.Số vòng lặp của MD5?  
A. 4  
B. 16  
C. 80  
D. 6

60.Số vòng lặp của SHA1?  
A. 4  
B. 16  
C. 80  
D. 6

61.Số thao tác/vòng lặp của MD5?  
A. 4  
B. 16  
C. 80  
D. 6

62.Số thao tác/vòng lặp của SHA1?  
A. 4  
B. 16  
C. 80  
D. 6

63.Đâu là các thao tác/1 vòng lặp của SHA1?  
A. add - and - or - xor - rotate - mod  
B. add - nor - or - xor - rotate - mod  
C. sub - and - or - xor - rotate - mod  
D. add - and - or - xor - sub - mod

64.Đâu không phải hành động trong 1 thao tác của MD5  
A.Hàm F (4 hàm khác nhau cho mỗi vòng);  
B.Cộng modulo;  
C.Quay trái.  
D. Quay phải

**Chương 3 Part 2**

1, Đâu là một phương pháp mã hóa:

A, AND

B, NOT

C,OR

D,XOR

2, Một trong các điểm yếu của các hệ mã hóa khóa công khai là:

A,Độ an toàn thấp

B,Khó khăn trong quản lý và phân phối khóa.

C,Khó cài đặt trên thực tế.

E, Chi phí tính toán lớn

D, Tốc độ chậm

3,Điểm khác nhau chính giữa hai loại hàm băm MDC và MAC là:

A, MAC an toàn hơn MDC

B, MDC có khả năng chống đụng độ cao hơn MAC

C, MDC là loại hàm băm không khóa, còn MAC là loại hàm băm có khóa.

D, MDC an toàn hơn MAC.

4, Kích thước khóa hiệu dụng của hệ mã hóa DES là:

A, 64 bít

B, 48 bít

C,128 bít

D,56 bít

5, Đâu là một chế độ hoạt động (Modes of Operation) của mã hóa khối?

A, EBC

B, EEC

C,ECC

D,ECB

6, Một trong các ứng dụng phổ biến của các hàm băm 1 chiều là:

A, Mã hóa tên tài khoản

B, Mã hóa mật khẩu

C, Mã hóa thẻ tín dụng

D, Mã hóa địa chỉ

7, Tìm phát biểu đúng về mã hóa khóa bất đổi xứng (Asymmetric key

cryptography):

A, An toàn hơn khóa bí mật.

B, Sử dụng một khóa chung cho cả quá trình mã hóa và giải mã

C, Chỉ sử dụng kỹ thuật mã hóa khối

D, Sử dụng một khóa quá trình mã hóa và một khóa khác cho giải mã.

8, Giải thuật mã hóa AES vận hàng dựa trên một ma trận 4\*4, được gọi là:

A, Status

B, States

C,State

D,Stock

9, Các hộp thay thế S-Box trong giải thuật DES có số bít đầu vào và đầu ra

tương ứng là:

A, Vào 8 bit, ra 6 bít

B, Vào 6 bít, ra 4 bít

C, Vào 6 bít, ra 6 bít

D, Vào 4 bít, ra 4 bít.

10, Hai thuộc tính cơ bản và quan trọng nhất của một hàm băm là:

A, Một chiều và đầu ra cố định

B, Dễ tính toán và đầu ra cố định.

C, Nén và một chiều

D, Nén và dễ tính toán.

11, Trật tự các khâu xử lý trong các vòng lặp chính của giải thuật mã hóa AES:

A, AddRoundKey, MixColumns, ShiftRows, SubBytes

B, SubBytes, MixColumns, ShiftRows, AddRoundKey

C,SubBytes, ShiftRows, MixColumns, AddRoundKey

D, AddRoundKey, MixColumns, SubBytes, ShiftRows

12, Số lượng vòng lặp chính thực hiện xáo trộn dữ liệu theo hàm Feistel (F)

trong giải thuật DES là:

A, 16

B, 18

C,20

D,14

13, Trong hệ mã hóa RSA, quan hệ toán học giữa khóa riêng d và khóa công

khai e là:

A, d là modulo nghịch đảo của e

B, d và e là hai số nguyên tố cùng nhau

C, d là modulo của e

D, d và e không có quan hệ với nhau.

14, Số vòng lặp chuyển đổi cần thực hiện để chuyển bản rõ thành bản mã của

giải thuật mã hóa AES với khóa 192 bít là:

A, 12

B, 14

C,16

D,10

15, Các giải thuật mã hóa khóa đối xứng thông dụng gồm:

A, DES, 3DES, RSA

B, DES, AES, PGP

C, DES, 3DES, AES

D, DES, RSA, RC4

16, Trong quá trình xử lý thông điệp đầu vào tạo chuỗi băm, số lượng vòng xử

lý của hàm băm SHA1 là:

A, 70

B, 90

C,80

D,60

17,Một trong các điểm yếu của các hệ mã hóa khóa đối xứng là:

A, Khó khăn trong cài đặt và triển khai hệ thống.

B, Độ an toàn thấp

C,Khó khăn trong quản lý và phân phối khóa.

D, Độ phức tạp của giải thuật RSA

18, Độ an toàn của giải thuật RSA dựa trên

A, Khóa có kích thước lớn

B, Chi phí tính toán lớn

C, Tính khó của việc phân tích số nguyên lớn.

D, Độ phức tập của giải thuật RSA

19, Đâu là một ứng dụng của mã hóa.

A, PGP

B, PPG

C,PGG

D,GPP

20, Giải thuật mã hóa AES được thiết kế dựa trên:

A, Mạng hoán vị-XOR

B, Mạng XOR-thay thế

C, Mạng hoán vị-thay thế

D, Mạng hoán vị - vernam

Câu 21: Trong hệ mật mã RSA, quan hệ toán học giữa khóa công khai e và số

Phi(n) là:

A, e và Phi(n) là hai số nguyên tố cùng nhau

B, Phi(n) là modulo của e

C, Phi(n) là modulo nghịch đảo của e

D, E và Phi(n) không có quan hệ với nhau

Câu 22:Kích thức khối dữ liệu xử lý của giải thuật mã hóa AES là

A, 128

B, 160

C,64

D,192

Câu 23: Đâu là một chế độ hoạt động (Modes of Operation) của mã hóa khối

A, CBC

B, CCB

C,CBB

D,BCC

Câu 24, Phần xử lý chính của SHA1 làm việc trên một chuỗi được gọi là state

là:

A, 160

B, 150

C,170

D,180

Câu 25: Một hệ mã hóa (cryptosystem) được cấu thành từ hai thành phần chính

gồm:

A, Phương pháp mã hóa và chia khối

B, Giải thuật mã hóa và ký số

C, Phương pháp mã hóa và không gian khóa

D, Giải thuật mã hóa và giải mã

Câu 26: Số lượng thao tác trong mỗi vòng xử lý của hàm băm MD5 là

A, 16

B, 18

C,12

D,14

27,Một trong các ứng dụng phổ biến của các hàm băm là để tạo chuỗi...

A, checkError

B, CheckNum

C,CheckSum

D,CheckTotal

28, Trong mã hóa dòng (stream cipher), dữ liệu được xử lý theo...

A, Từng bit hoặc từng byte/ ký tự

B, Từng chuỗi ký tự

C, Từng bít

D, Từng Byte

29, Khi sinh cặp khóa RSA, các số nguyên tố p và q nên được chọn vói kích

thước:

A, q càng lớn càng tốt

B, bằng khoảng 1 nửa kích thước của moduno n

C, p càng lớn càng tốt

D, Không có yêu cầu về kích thước của p và q

Ngân hàng ATBM

1. Những chữ đầu của nhóm từ ACL là tên viết tắt của:

A. Arbitrary Code Language

B. Access Control Library

C. Access Control List

D. Allowed Computer List

C

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

A. Full access

B. No access

C. Read access

D. Write access

B

3. Sau khi một user được định danh và xác thực hệ thống, để cho phép user sử dụng

tài nguyên

bạn phải thực hiện điều gì?

A. Phải được ủy quyền

B. Được truyền lại

C. Được mã hóa

D. Được enable

A

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

A. Đọc

B. Sao chép

C. Hiệu chỉnh

D. Ghi

D

5. 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)

A

6. Các quyền truy cập tối đa nên dành cho user là gì ?

A. Ít nhất là quyền đọc và ghi

B. Không có quyền truy cập

C. Đủ để thực hiện công việc theo chức trách

D. Toàn quyền

C

7. Chính sách tài khoản nào nên được thiết lập để ngăn chặn các cuộc tấn công ác ý

vào tài khoản

của user?

A. Disable tài khoản không dùng đến

B. Hạn chế thời gian

C. Ngày hết hạn tài khoản

D. Giới hạn số lần logon

D

8. Sau khi một user đã được định danh (identifed), điều gì cần phải làm trước khi họ

log vào một mạng máy tính ?

A. Xác thực với mật khẩu

B. Họ phải nhập user ID đã được mã hóa

C. Được phép truy cập với mức ưu tiên được thiết lập

D. Người quản trị phải enable để gõ vào

A

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

C

10. Điều gì cần được thực hiện đối với tập tin mật khẩu để ngăn chặn một người

dùng trái phép crack vào các nội dung ?

A. Hủy bỏ tất cả các quyền truy cập

B. Mã hóa tập tin mật khẩu

C. Di chuyển ngoại tuyến đến một đĩa mềm

D. Sao chép đến một tập tin bù nhìn với một tên khác

B

11. Một IP flood theo các host phát tán trực tiếp đến một Web server là một ví dụ

của loại tấn công gì ?

A. Trojan Hors

B. Sâu

C. Tấn công IP

D. DoS phân tán (DDoS)

D

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. Tấn công đang đến từ nhiều host (DDoS)

C. Một tường lửa không thể ngăn chặn tấn công DoS

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

B

13. Cách bảo vệ nào sau đây là tốt nhất để chống lại tấn công DoS kiểu làm tràn

băng thông và bộ đệm của hệ thống

A. Subnet mask

B. Cài đặt phần mềm bảo vệ Antivirus

C. Disable web server

D. Chặn giao thức ICMP

D

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

A. 128 bit

B. 40 bit

C. 256 bit

D. 56 bit

B

15. 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

A

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

A. password83

B. reception

C. !$aLtNb83

D. LaT3r

C

17. Một người dùng đã mua một máy tính xách tay đã nhiễm virus.Trên máy không

chứa phần mềm Antivirus và chưa được kết nối với mạng.Cách tốt nhất để sửa chữa

máy tính xách tay là gì ?

A. Nối mạng máy tính xách tay và download phần mềm antivirus từ máy chủ

B. Khởi động máy tính xách tay với đĩa antivirus

C. Nối mạng máy tính xách tay và download phần mềm antivirus từ Internet

D. Kết nối máy tính xách tay đến một máy tính cá nhân khác và diệt virus từ đó

B

18. 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

D

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. Ngựa trojan

C. Logic bomb

D. Stealth virus

B

20. 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"

A

21. 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. Wireless

D. SSH

A

22. 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)

D

23. 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

B

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

A. SLIP

B. IPX

C. L2TP

D. PPTP

C

25. Mục đích của một máy chủ RADIUS là

A. Packet Sniffing

B. Mã hóa

C. Xác thực

D. Thỏa thuận tốc độ kết nối

C

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

A. 802.1X

B. 802.11b

C. 802.11a

D. 803.1

B

27. 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+

B

28. LAC ( L2TP Access Control) và LNS ( L2TP Network Server)) là các thành

phần của giao thức đường hầm nào ?

A. IPSec

B. PPP

C. PPTP

D. L2TP

D

\*29. NOTE Giao thức được sử dụng rộng rãi nhất để truy cập kiểu quay số đến một máy chủ

từ xa là

A. SLIP

B. PPP

C. RAS

D. Telnet

B

30. 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

C

31. 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

D

32. 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

C

33. 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

A

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

A. 803.11b

B. 802.11g

C. 802.11a

D. 802.11b

B

35. 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

A

36. 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

B

37. Bộ lọc địa chỉ MAC được định nghĩa như :

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

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

C. Mã hóa địa chỉ MAC của thiết bị không dây.

D. Tường lửa cá nhân

B

38. 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. Mã hóa WEP kết hợp với lọc địa chỉ MAC

D. Nhận dạng bảo mật mạng

C

39. 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

A

40. 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

C

41. 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

A

42. 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

D

43. 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

D

44. 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

C

45. Phương tiện nào sau đây không bị ảnh hưởng bởi từ tính ?

A. Đĩa mềm

B. CD-ROM

C. Flash card

D. Băng từ

B

46. Yếu tố nào cần được sử dụng kết hợp với một thẻ thông minh để xác thực ?

A. PIN

B. Quét võng mạc

C. Mã hóa khóa

D. Thẻ nhớ

A

47. Loại media nào sau đây không phải là một thiết bị cơ động được ?

A. Đĩa mềm

B. Ổ đĩa đĩa CD

C. Thẻ thông minh

D. Băng từ

B

48. Các thiết bị hay các ứng dụng bảo mật nào sau đây nên được sử dụng để theo

dõi và cảnh báo các quản trị mạng về truy cập trái phép ?

A. Chương trình Antivirus

B. Switch

C. Hệ thống phát hiện xâm nhập (IDS)

D. Dụng cụ phân tích mạng

C

49. Vùng nào của cấu trúc liên kết bảo mật mạng chứa các máy chủ Intenet, như là

web, FTP, và các máy chủ email ?

A. DMZ

B. VLAN

C. VPN

D. Intranet

A

50. Loại mạng nào mô tả cấu hình mạng bên trong của một công ty dùng cho mô

hình kinh doanh B2B ( Business to Business) ?

A. VLAN

B. Intranet

C. Extranet

D. VPN

B

51. Dịch vụ mạng nào cho phép các địa chỉ mạng bên trong được "che dấu"( hidden)

khỏi các mạng bên ngoài và cho phép vài host của mạng bên trong sử dụng các địa

chỉ trùng với mạng bên

ngoài ?

A. NAT

B. VPN

C. VLAN

D. IP spoofing

A

52. Công nghệ nào được sử dụng để chia một mạng bên trong thành mạng logic nhỏ

hơn, dễ sử dụng hơn ?

A. NAT

B. Tunneling

C. VPN

D. VLAN

D

53. Không sử dụng một liên kết chuyên dụng , phương pháp tốt nhất để kết nối hai

mạng được định vị trong các văn phòng có khoảng cách địa lý xa nhau là gì ?

A. VLAN

B. Tường lửa

C. DMZ

D. VPN

D

54. Sau khi cố gắng login đến một trạm làm việc trong 3 lần, một user thấy đã bị

khóa bên ngoài hệ thống và không thể thực hiện bất kỳ nổ lực nào hơn nữa. Vấn đề

này phù hợp nhất với điều gì ?

A. Cổng mạng disable

B. Tường lửa disable khi truy cập đến host

C. User quên mật khẩu của họ

D. Hệ thống phát hiện xâm nhập disable tài khoản của user

D

55. Đặc tính nào của các thiết bị mạng như router hay switch, cho phép điều khiển

truy cập dữ liệu trên mạng ?

A. Giao thức DNS

B. Cập nhật vi chương trình ( Firmware)

C. Tường lửa

D. Danh sách điều khiển truy cập (ACL)

D

56. Phần nào của một thiết bị phần cứng có thể được nâng cấp để cung cấp khả

năng bảo mật tốt hơn và đáng tin hơn ?

A. Vi chương trình (firmware)

B. Quét cổng

C. Flash memory

D. Cấu hình tập tin

C

57. Giao thức nào sau đây cần xóa trên thiết bị mạng quan trọng như router ?

A. TCP/IP

B. ICMP

C. IPX/SPX

D. RIP

B

58. Các giao thức nào sau đây cần xóa trên một máy chủ email để ngăn chặn một

user trái phép khai thác các điểm yếu bảo mật từ phần mềm giám sát mạng ?

A. IMAP

B. POP3

C. TCP/IP

D. SNMP

D

59. Điều gì cần được thực hiện với một email server để ngăn chặn user bên ngoài gởi

email thông qua nó ?

A. Cài đặt phần mềm antivirus và antispam.

B. Hạn chế chuyên tiếp tín hiệu SMTP.

C. Xoá quyền truy cập POP3 và IMAP

D. Enable login được mã hóa

B

60. Điều gì có thể được thiết lập trên một server DHCP để ngăn chặn các máy trạm

trái phép lấy được một địa chỉ IP từ server ?

A. Quét cổng

B. Thiết lập "Danh sách truy cập thư mục LDAP"

C. Phát hiện xâm nhập

D. DNS

B

61. Văn bản sau khi được mã hóa, được gọi là gì ?

A. Chứng chỉ

B. Mật mã đối xứng

C. Khóa công khai

D. Văn bản mã

B

62. Đặc tính nào sau đây không thuộc chức năng bảo mật thông tin trong các hệ

thống mật mã ?

A. Hiệu quả

B. Bảo mật

C. Toàn vẹn

D. Không chối từ

A

63. Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng cùng một khóa

mã khi mã hóa và giải mã ?

A. Không đối xứng

B. Đối xứng

C. RSA

D. Diffie-Hellman

B

64. Chuẩn nào sau đây được chính phủ Mỹ sử dụng thay thế cho DES như là một

chuẩn mã hoá dữ liệu?

A. DSA

B. ECC

C. 3DES

D. AES

D

65. Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng các khóa khác

nhau khi mã hóa và giải mã ?

A. Skipjack

B. Blowfish

C. Không đối xứng

D. Đối xứng

C

66. Các giao thức mã hóa và các thuật toán nào sau đây được sử dụng như là nền

tảng của hạ tầng cơ sở hạ tầng khóa công khai (PKI)?

A. MD4

B. SHA

C. Diffie-Hellman

D. Skipjack

C

67. Khi giá trị hàm băm của hai thông điệp khác nhau có giá trị tương tự nhau, ta

gọi hiện tượng này là gì ?

A. Tấn công vào ngày sinh

B. Xung đột

C. Chữ ký số

D. Khóa công khai

B

68. Thực thể nào sau đây cho phép phát hành , quản lý, và phân phối các chứng chỉ

số ?

A. Quyền cấp chứng chỉ (Certificate Authority)

B. Quyền đang ký (Registation Authority)

C. Chính phủ (NSA)

D. PKI

A

69. Tính hợp lệ của một chứng chỉ dựa vào điều gì ?

A. Tính hợp lệ của Quyền cấp chứng chỉ (CA)

B. Tính hợp lệ của người sở hữu

C. Tính hợp lệ của khóa công khai

D. Giai đoạn chứng chỉ được sử dụng

A

70. Trong một mô hình phân cấp ủy thác giữa các tổ chức chứng thực và các người

dùng cuối, mô hình nào sau đây được coi là xu hướng chung của việc phát hành

chứng chỉ?

A. Các chính sách thu hồi chứng chỉ

B. Các ngày hợp lệ

C. Khóa cá nhân

D. Chứng thực gốc ( Root Certificate)

D

71. Khi ta lưu giữ một khóa cá nhân trên đĩa cứng cục bộ, làm thế nào để bảo đảm

là nó được bảo mật ?

A. Cần bảo vệ bằng mật khẩu

B. Lưu trữ dữ liệu sao lưu vào đĩa mềm

C. Lưu trữ bản sao trong bì thư

D. Lưu trữ nó trong một thư mục tương tự như khóa công khai

A

72. Cách nào sau đây được coi là an toàn nhất để lưu trữ một khóa cá nhân ?

A. Lưu nó trên ổ cứng ở dạng bản rõ

B. Niêm phong nó trong một bao thư và để nó trong ngăn bàn

C. Mã hóa nó trên một thẻ thông minh

D. Lưu nó trên một thiết bị USB di dộng ở dạng bản rõ

C

73. Một quản trị mạng mới đây đã bị sa thải khỏi công ty. Cần phải làm gì với

chứng chỉ hiện hành của họ ?

A. Làm mới lại đối với người quản trị mới

B. Thu hồi lại chứng chỉ

C. Đình chỉ tạm thời

D. Hết hiệu lực

B

74. Các phương pháp sinh trắc học nào sau đây được coi là an toàn nhất ?

A. Phân tích chữ ký

B. Quét tiếng nói

C. Lấy dấu bàn tay / Lấy dấu ngón tay

D. Không quan trọng

C

75. Khi kết thúc công việc trên máy tính xách tay và ra ngoài khoảng 1 tiếng vào

buổi trưa. Ta nên làm gì trước khi ra ngoài ?

A. Nói với đồng nghiệp để mắt đến máy tính xách tay

B. Log out khỏi máy tính xách tay

C. Shut down và đóng máy lại

D. Chắc chắn rằng máy tính xách tay của ta được bảo vệ trên bàn làm việc hay được khóa

trong cabin

D

76. Một user gọi điện đến cho ta (với tư cách là người quản lý) thông báo họ bị mất

mật khẩu và cần truy cập ngay lập tức. Ta nên làm gì ?

A. Cung cấp truy cập ngay lập tức, và sau đó kiểm tra chứng cứ của họ

B. Tạo một login và mật khẩu tạm thời để họ sử dụng

C. Xác minh định danh của họ trước khi cấp quyền truy cập

D. Cho họ một mật khẩu riêng tạm thời

C

77. Trong khoảng thời gian nguồn điện bị sụt áp do quá tải bất thường, các thiết bị

nào sau đây là hữu dụng nhất trong việc duy trì các mức nguồn điện thích hợp ?

A. Dự phòng nguồn điện của máy phát điện

B. UPS

C. Ổn áp

D. Thanh nguồn điện

C

78. Quản trị văn phòng của bạn đang được huấn luyện để thực hiện sao lưu máy

chủ. Phương pháp xác thực nào là lý tưởng đối với tình huống này ?

A. MAC

B. DAC

C. RBAC

D. Các mã thông báo bảo mật

A

79. Phương pháp xác thực nào sử dụng một KDC để thực hiện xác thực ?

A. Chap

B. Kerberos

C. Sinh trắc học

D. Thẻ thông minh

B

80. Phương pháp xác thực nào gởi trả lại một "yêu cầu" (request) cho máy trạm và"

yêu cầu" đó được mã hóa và gởi trở lại máy chủ ?

A. Kerberos

B. Các mã thông báo bảo mật

C. DAC

D. CHAP

D

81. Qui trình xác thực nào sử dụng nhiều hơn một yếu tố xác thực để logon ?

A. Đa yếu tố ( multi-factor)

B. Sinh trắc học

C. Thẻ thông minh

D. Keberos

A

82. Các giao thức hay các dịch vụ nào sau đây nên loại bỏ trong mạng nếu có thể ?

A. Email

B. Telnet

C. WWW

D. ICMP

D

83. Mạng nào sau đây không phải là một vùng bảo mật ?

A. Internet

B. Intranet

C. Extranet

D. NAT

D

84. Các giao thức nào sau đây cho phép một tổ chức đưa một địa chỉ TCP/IP đơn lên

Internet ?

A. NAT

B. VLAN

C. DMZ

D. Extranet

A

85. Phương pháp quét võng mạc thích hợp nhất đối với các dịch vụ nào sau đây ?

A. Kiểm định

B. Xác thực

C. Kiểm soát truy cập

D. Bảo mật dữ liệu

C

86. Công nghệ nào sau đây dựa vào thuộc tính vật lý của user để xác thực ?

A. Thẻ thông minh

B. Sinh trắc học

C. Xác thực lẫn nhau

D. Các mã thông báo

B

87. Kỹ thuật cho phép tạo kết nối ảo giữa hai mạng sử dụng một giao thức bảo mật

được gọi là gì ?

A. Tunelling

B. VLAN

C. Internet

D. Extranet

B

88. Qui trình quyết định giá trị của thông tin hay thiết bị trong một tổ chức được gọi

là gì?

A. Đánh giá tài nguyên thông tin

B. Đánh giá rủi ro

C. Nhận dạng chuỗi

D. Quét các điểm yếu

A

89. Khi được hỏi về các mối đe dọa cho công ty từ phía các hacker. Loại thông tin

nào sau đây sẽ giúp ích nhiều nhất ?

A. Xác minh tài sản sở hữu

B. Đánh giá rủi ro

C. Nhận dạng mối đe dọa

D. Các điểm yếu

D

90. Khi một user báo cáo rằng hệ thống của anh ta đã phát hiện một virus mới. Điều

gì sau đây cần làm như là bước đầu tiên để xử lý tình huống này ?

A. Kiểm tra lại tập tin diệt virus hiện hành

B. Định dạng lại đĩa cứng

C. Cài đặt lại hệ điều hành

D. Disable tài khoản email của anh ta

D

91. Yếu tố nào sau đây được coi là hữu ích nhất trong việc kiểm soát truy cập khi bị

tấn công từ

bên ngoài ?

A. Đăng nhập hệ thống ( System logs)

B. Phần mềm antivirus

C. Kerberos

D. Sinh trắc học

A

92. Ta muốn cài đặt một máy chủ cung cấp các dịch vụ Web đến các máy trạm

thông qua Internet. Ta không muốn để lộ mạng bên trong để tránh rủi ro. Phương

pháp nào để thực hiện điều này ?

A. Cài đặt máy chủ trong mạng Intranet

B. Cài đặt máy chủ trong một DMZ

C. Cài đặt máy chủ trong một VLAN

D. Cài đặt máy chủ trong mạng Extranet

B

93. Phương pháp xác thực nào cung cấp tài liệu đáng tin cậy có hiệu lực trong suốt

một phiên làm việc đơn ?

A. Các mã thông báo

B. Chứng chỉ

C. Thẻ thông minh

D. Kerberos

B

94. Loại tấn công nào làm việc truy cập của user đến các tài nguyên mạng bị từ chối

?

A. DoS

B. Sâu

C. Logic Bomb (bomb ngập lụt đường truyền)

D. Social engineering (Khai thác giao tiếp)

A

95. Loại tấn công nào sử dụng nhiều hơn một máy tính để tấn công nạn nhân ?

A. DoS

B. DDoS

C. Sâu

D. Tấn công UDP

B

96. Một máy chủ trên mạng có một chương trình đang chạy vượt quá thẩm quyền .

Loại tấn công nào đã xảy ra ?

A. DoS

B. DDoS

C. Back door

D. Social engineering (Khai thác giao tiếp)

C

97. Nổ lực tấn công để can thiệp vào một phiên liên lạc bằng việc thêm vào một máy

tính giữa hai hệ thống được gọi là một .......?

A. Tấn công dạng "Man in the middle"

B. Tấn công cửa sau

C. Sâu

D. TCP/IP hijacking

A

98. Ta đã phát hiện ra một chứng chỉ đã hết hiệu lực vẫn đang được sử dụng nhiều

lần để giành được quyền logon. Đây là loại tấn công nào ?

A. Tấn công dạng "Man in the middle"

B. Tấn công cửa sau

C. Tấn công chuyển tiếp (Relay Attack)

D. TCP/IP hijacking

D

99. Một kẻ tấn công cố gắng dùng địa chỉ IP để tạo một hệ thống khác trong mạng

của ta nhằm giành quyền kiểm soát truy cập . Đây là loại tấn công nào ?

A. Tấn công dạng "Man in the middle"

B. Tấn công cửa sau

C. Sâu

D. TCP/IP hijacking

D

100. Một máy chủ trên mạng không chấp nhận các kết nối TCP nữa. Máy chủ thông

báo rằng nó đã vượt quá giới hạn của phiên làm việc. Loại tấn công nào có thể đang

xảy ra ?

A. Tấn công TCP ACK (tấn công kiểu SYNACK)

B. Tấn công smurf

C. Tấn công virus

D. TCP/IP hijacking

A

101. Tấn công smurf sử dụng giao thức nào để kiểm soát ?

A. TCP

B. IP

C. UDP

D. ICMP

D

102. Tổ đặc trách thông báo rằng họ đã nhận một cuộc gọi khẩn cấp từ phó chủ tịch

đêm qua yêu cầu logon vào ID và mật khẩu của ông ta. Đây là loại tấn công gì ?

A. Giả mạo

B. Tấn công chuyển tiếp

C. Social engineering (Khai thác giao tiếp)

D. Trojan

A

103. Hệ thống của bạn đã ngừng phản ứng lại với các lệnh của bàn phím. Lưu ý

rằng điều này xảy ra khi mở bảng tính và đã quay số qua internet. Loại tấn công

nào có thể đã xảy ra ?

A. Logic Bomb

B. Sâu

C. Virus

D. Tấn công ACK

D

104. Loại virus tự che giấu nó bằng cách ẩn trong mã nguồn của các phần mềm

antivirus được

gọi là gì ?

A. Armored virus

B. Polymorphic virus

C. Sâu

D. Stealth virus (Virus ẩn danh)

B

105. Một virus được đính kèm chính nó vào boot sector của đĩa cứng và thông báo

thông tin sai về kích thước các tập tin được gọi là gì ?

A. Virus Trojan

B. Stealth virus (virus ẩn danh)

C. Sâu

D. Polymorphic virus

B

106. Một chương trình nằm trong một chương trình khác được cài vào hệ thống gọi

là một .......

A. Trojan Horse

B. Polymorphic virus

C. Sâu

D. Armored virus

A

107. Các user nội bộ báo cáo hệ thống của họ bị lây nhiễm nhiều lần. Trong mọi

trường hợp virus có vẻ là cùng một loại. Thủ phạm thích hợp nhất là gì ?

A. Máy chủ có thể là vật mang virus

B. Ta có một sâu virus

C. Phần mềm antivirus của ta bị sự cố

D. Tấn công DoS đang thực hiện

A

108. Các log file trên hệ thống của bạn phát hiện một nổ lực giành quyền truy cập

đến một tài khoản đơn. Nổ lực này đã không thành công vào thời điểm đó. Theo

kinh nghiệm của bạn thì loại tấn công thích hợp nhất là gì ?

A. Tấn công đoán mật khẩu (Password Guessing)

B. Tấn công cửa sau

C. Tấn công bằng sâu

D. TCP/IP hijacking

A

109. Một user báo cáo là anh ta đang nhận một lỗi chỉ ra rằng địa chỉ TCP/IP của

anh ta đã bị sử dụng khi anh ta bật máy tính. Tấn công nào có thể đang thực hiện ?

A. Tấn công dạng "Man in the middle"

B. Tấn công cửa sau

C. Sâu

D. TCP/IP hijacking

D

110. Một đêm làm việc khuya và bạn phát hiện rằng ổ cứng của bạn hoạt động rất

tích cực mặc dù bạn không thực hiện bất kỳ thao tác nào trên máy tính. Bạn nghi

ngờ điều gì?

A. Khả năng ổ đĩa ngừng hoạt động sắp xảy ra

B. Một virus đang phát tán rộng trong hệ thống

C. Hệ thống của bạn đang chịu tác động của tấn công DoS

D. Tấn công TCP/IP hijacking đang cố gắng thực hiện

B

111. Bản ghi lỗi hệ thống email của bạn báo cáo một số lượng lớn các nổ lực logon

không thành công. Loại tấn công nào có thể đang xảy ra ?

A. Tấn công khai thác phần mềm (Software exploitation attack)

B. Tấn công cửa sau ( Back door Attack))

C. Sâu (Worm)

D. TCP/IP hijacking

D

112. Bộ lọc gói thực hiện chức năng nào ?

A. Ngăn chặn các gói trái phép đi vào từ mạng bên ngoài

B. Cho phép tất cả các gói rời mạng

C. Cho phép tất cả các gói đi vào mạng

D. Loại trừ sự xung đột trong mạng

A

113. Thiết bị nào lưu trữ thông tin về đích đến trong mạng ?

A. Hub

B. Modem

C. Firewall

D. Router

D

114. Giao thức nào được sử dụng rộng rãi hiện nay như là một giao thức truyền tải

đối với các kết nối quay số trên Internet ?

A. SLIP

B. PPP

C. PPTP

D. L2TP

A

115. Giao thức nào sau đây không phù hợp đối với các kết nối VPN WAN ?

A. PPP

B. PPTP

C. L2TP

D. IPSec

A

116. Giao thức nào sau đây tuy không phải là một giao thức đường hầm nhưng nó

sử dụng các giao thức đường hầm để bảo mật trên mạng?

A. IPSec

B. PPTP

C. L2TP

D. L2F

A

117. Một socket là sự kết hợp của các thành phần nào ?

A. TCP và port number

B. UDP và port number

C. IP và session number

D. IP và port number

D

118. Thiết bị nào giám sát lưu lượng mạng theo cách thụ động ?

A. Sniffer

B. IDS

C. Firewall

D. Web browser

A

119. Hệ thống nào chủ động thực hiện việc giám sát mạng, phân tích và có thể thực

hiện các bước phòng ngừa , bảo vệ mạng ?

A. IDS

B. Sniffer

C. Router

D. Switch

A

120. Hệ thống nào được cài đặt trên Host để cung cấp một tính năng IDS ?

A. Network sniffer

B. N-IDS (Network-based IDS)

C. H-IDS (Host-based IDS)

D. VPN

C

121. Khi kết nối giữa các thiết bị không dây đã hoàn tất , giao thức nào được sử

dụng?

A. WEP

B. WTLS

C. WAP

D. WOP

C

122. Giao thức nào hoạt động trên 2.4GHz và có một dải băng thông rộng 1Mbps

hay 2Mbps ?

A. 802.11 //1Mbps hoặc 2Mbps với băng thông 2.4GHz

B. 802.11a //54Mbps trong dải tần 5GHz

C. 802.11b //11Mbps trong băng thông 2.4GHz WIFI

D. 802.11g //Tốc độ hơn 20Mbps trên băng thông 2.4GHz

A

123. Giao thức nào được thiết kế để cung cấp bảo mật cho mạng không dây tương

đương với việc bảo mật của một mạng diện rộng ?

A. WAP

B. WTLS

C. WEP

D. IR

C

124. Điểm yếu nào sau đây là chủ yếu của môi trường mạng không dây ?

A. Phần mềm giải mã (Decryption software)

B. IP spoofing (Giả mạo IP)

C. A gap in the WAP (Một khe hở trong WAP)

D. Định vị nơi làm việc (Site survey)

D

125. Nếu ta muốn xác thực chữ ký của một người khác, khóa nào phải được sử

dụng?

A. Khóa công khai của bạn

B. Khoá cá nhân của bạn

C. Khoá cá nhân của người cần xác thực

D. Khoá công khai của người cần xác thực

D

126. Chữ ký số được sử dụng cho mục đích gì?

A. Để bảo mật tài liệu sao cho người ngoài không đọc được

B. Để kiểm tra định danh người gửi

C. Cung cấp chứng chỉ

D. Thu hồi một chứng chỉ

B

127. Nếu muốn xem một tài liệu "bảo mật"được mã hóa trên hệ mật bất đối xứng do

người khác gởi đến , bạn phải sử dụng khóa nào để giải mật tài liệu?

A. Khoá công khai của bạn

B. Khoá công khai của bên gửi

C. Khoá cá nhân của bên gửi

D. Khoá cá nhân của bạn

D

Chương 3 Tiếp

1. PGP đảm bảo tính bí mật thông điệp bằng cách sử dụng:

A. Mã hóa khóa bất đối xứng sử dụng khóa phiên

B. Mã hóa khóa đối xứng sử dụng khóa phiên

C. Mã hóa khóa bất đối xứng sử dụng khóa công khai

D. Mã hóa khóa đối xứng sử dụng khóa công khai

c

2. Số lượng thao tác trong mỗi vòng xử lý của hàm băm MD5 là:

A. 14

B. 16

C. 18

D. 12

B

3. Giao thức SSL sử dụng giao thức con SSL Handshake để khởi tạo phiên làm việc. SSL Handshake thực hiện việc trao đổi các khóa phiên dùng cho phiên làm việc dựa trên:

A. Chữ ký số

B. Mã hóa khóa bí mật

C. Mã hóa khóa công khai

D. Chứng chỉ số

D

4. Các thuộc tính cơ bản của chứng chỉ số khóa công khai (Public key digital certificate) gồm:

A. Số nhận dạng, khóa riêng của chủ thể, chữ ký của nhà cung cấp CA

B. Khóa công khai của chủ thể, thông tin địa chỉ chủ thể, thuật toán chữ ký sử dụng

C. Số nhận dạng, khóa riêng của chủ thể, thông tin định danh chủ thể

D. Khóa công khai của chủ thể, thông tin định danh chủ thể, chữ ký của nhà cung cấp (CA)

D

5. Một hệ mã hóa (cryptosystem) được cấu thành từ hai thành phần chính gồm:

A. Phương pháp mã hóa và chia khối

B. Giải thuật mã hóa và ký số

C. Phương pháp mã hóa và không gian khóa

D. Giải thuật mã hóa và giải mã

C

6. Đây là một phương pháp mã hóa

A. OR

B. AND

C. NOT

D. XOR

D

7. Kích thước khối dữ liệu xử lý của giải thuật mã hóa AES là:

A. 160 bit

B. 64 bit

C. 192 bít

D. 128 bit

D

8. Điểm khác nhau chính giữa hai loại hàm băm MDC và MAC là:

A. MDC là loại hàm băm không khóa, còn MAC là loại hàm băm có khóa

B. MDC có khả năng chống đụng độ cao hơn MAC

C. MDC an toàn hơn MAC

D. MAC an toàn hơn MDC

A

9. Chữ ký số (sử dụng riêng) thường được sử dụng để đảm bảo thuộc tính nào sau đây của thông điệp truyền đưa:

A. Tính bí mật

B. Tính không chối bỏ

C. Tính sẵn dùng

D. Tính toàn vẹn

D

10. Trong hệ chữ ký số RSA, việc tạo chữ ký số cho một thông điệp cần sử dụng một khóa. Khóa đó là:

A. Khóa riêng của người nhận

B. Khóa công khai của người nhận

C. Khóa công khai của người gửi

D. Khóa riêng của người gửi

C

11. Một trong các điểm yếu của các hệ mã hóa khóa công khai là:

A. Khó cài đặt trên thực tế

B. Khó khăn trong quản lý và phân phối khóa

C. Tốc độ chậm

D. Độ an toàn thấp

C

12. Phát biểu nào sau đây về chữ ký số là chính xác:

A. Chữ ký số là một chuỗi dữ liệu được tạo ra bằng cách mã hóa thông điệp sử dụng khóa bí mật

B. Chữ ký số là một chuỗi dữ liệu liên kết với một thông điệp và thực thể tạo ra thông điệp

C. Chữ ký số được sử dụng để đảm bảo tính bí mật và toàn vẹn thông điệp

D. Chữ ký số được sử dụng để đảm bảo tính bí mật, toàn vẹn và xác thực thông điệp

B

13. Hai thuộc tính cơ bản quan trọng nhất của một hàm băm là:

A. Nén và một chiều

B. Dễ tính toán và có đầu ra cố định

C. Một chiều và đầu ra cố định

D. Nén và dễ tính toán

D

14. Độ an toàn của hệ mật mã RSA dựa trên...

A. Độ phức tạp cao của giải thuật RSA

B. Chi phí tính toán lớn

C. Tính khó của việc phân tích số nguyên rất lớn

D. Khóa có kích thước lớn

C

15. Khi sinh cặp khóa RSA, các số nguyên tố p và q nên được chọn với kích thước...

A. p càng lớn càng tốt

B. Bằng khoảng một nửa kích thước của modulo n

C. Không có yêu cầu về kích thước của p và q

D. q càng lớn càng tốt

B

16. Tìm phát biểu đúng về mã hóa khóa bất đối xứng (Asymmetric key cryptography):

A. An toàn hơn mã hóa khóa bí mật

B. Sử dụng một khóa quá trình mã hóa và một khóa khác cho giải mã

C. Chỉ sử dụng kỹ thuật mã hóa khối

D. Sử dụng một khóa chung cho cả quá trình mã hóa và giải mã

B

17. Tìm phát biểu đúng về mã hóa khóa đối xứng (Symmetric key cryptography):

A. Sử dụng một khóa chung cho cả quá trình mã hóa và giải mã

B. Sử dụng một khóa quá trình mã hóa và một khóa khác cho giải mã

C. An toàn hơn mã hóa khóa công khai

D. Chỉ sử dụng kỹ thuật mã hóa khối

A

18. Sử dụng kết hợp chứng chỉ số khóa công khai và chữ ký số có thể đảm bảo:

A. Xác thực thực thể và toàn vẹn thông tin truyền

B. Xác thực thực thể và bí mật thông tin truyền

C. Bí mật và xác thực nguồn gốc thông tin truyền

D. Bí mật và toàn vẹn thông tin truyền

D

19. Số lượng vòng lặp chính thực hiện xáo trộn dữ liệu theo hàm Feistel (F) trong giải thuật DES là:

A. 14

B. 16

C. 18

D. 20

B

20. Các hộp thay thế s-box trong giải thuật DES có số bít đầu vào và đầu ra tương ứng là:

A. Vào 4 bít và ra 4 bít

B. Vào 6 bít và ra 6 bít

C. Vào 8 bít và ra 6 bít

D. Vào 6 bít và ra 4 bít

D

21. Một trong các ứng dụng phổ biến của các hàm băm là để tạo chuỗi...

A. CheckError

B. CheckTotal

C. CheckNum

D. Checksum

D

22. PGP đảm bảo tính bí mật thông điệp bằng cách sử dụng:

A. Mã hóa khóa bất đối xứng sử dụng khóa công khai và khóa bí mật

B. Mã hóa khóa đối xứng sử dụng khóa phiên

C. Mã hóa khóa đối xứng sử dụng khóa công khai

D. Mã hóa khóa bất đối xứng sử dụng khóa phiên

A

23. Trong quá trình xử lý thông điệp đầu vào tạo chuỗi băm, số lượng vòng xử lý của hàm băm SHA1 là:

A. 80

B. 90

C. 60

D. 70

A

24. Giải thuật mã hóa AES được thiết kế dựa trên...

A. mạng hoán vị-vernam

B. mạng xor-thay thế

C. mạng hoán vị-thay thế

D. mạng hoán vị-xor

C

25. Một trong các điểm yếu của các hệ mã hóa khóa đối xứng là:

A. Chi phí tính toán lớn

B. Khó khăn trong quản lý và phân phối khóa

C. Độ an toàn thấp

D. Khó khăn trong cài đặt và triển khai hệ thống

B

26. Số vòng lặp chuyển đổi cần thực hiện để chuyển bản rõ thành bản mã của giải thuật mã hóa AES với khóa 192 bít là:

A. 10

B. 12

C. 16

D. 14

B

27. Phát biểu nào sau đây về chữ ký số là chính xác:

A. Chữ ký số là một chuỗi dữ liệu được tạo ra bằng cách mã hóa thông điệp sử dụng khóa bí mật

B. Chữ ký số là một chuỗi dữ liệu liên kết với một thông điệp và thực thể tạo ra thông điệp

C. Chữ ký số được sử dụng để đảm bảo tính bí mật, toàn vẹn và xác thực thông điệp

D. Chữ ký số được sử dụng để đảm bảo tính bí mật và toàn vẹn thông điệp

B

28. Một trong các ứng dụng phổ biến của các hàm băm một chiều là để...

A. Mã hóa thẻ tín dụng

B. Mã hóa địa chỉ

C. Mã hóa mật khẩu

D. Mã hóa tên tài khoản

C

29. Giao thức SSL sử dụng giao thức con SSL Handshake để khởi tạo phiên làm việc. SSL Handshake thực hiện việc xác thực thực thể dựa trên:

A. Chứng chỉ số khóa công khai

B. Mã hóa khóa bí mật

C. Mã hóa khóa công khai

D. Chữ ký số

A

30. PGP đảm bảo tính xác thực thông điệp bằng cách:

A. Mã hóa/giải mã thông điệp

B. Sử dụng hàm băm có khóa MAC

C. Sử dụng hàm băm không khóa MDC

D. Tạo và kiểm tra chữ ký số

D