



# Ngân hàng Atbmhttt: Chương 1 - Mô hình an toàn thông tin và hệ thống

An toàn và Bảo mật Hệ thống thông tin (Học viện Công nghệ Bưu chính Viễn thông)



Scan to open on Studocu

// Team All// Chắc chắn đúng bơi bỏ - Chưa chắc bơi đen :D //

## Chương 1+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, Tường 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. Mỗi đe dọa là bất kỳ một hành động tấn công nào vào hệ thống mạng.
  - B. Mỗi đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống.
  - C. Mỗi đe dọa là bất kỳ một hành động tấn công nào vào hệ thống máy tính.
  - D. Mỗi 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 cấm 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. Đây 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 chen 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 biến đầu vào của hàm
- B. Bộ đệm hoặc biến 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 hơn
  - D. Vi rút có khả năng phá hoại lớn hơn
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 UDP hoặc các yêu cầu phát quảng bá
  - D. Các yêu cầu HTTP hoặc các yêu cầu phát quảng bá
40. Đây 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. Vết 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

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

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. MAC
  - 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. Đây 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**

//Chương 3 :

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
2. Số lượng thao tác trong mỗi vòng xử lý của hàm băm MD5 là:
  - A. 14
  - B. 16**
  - C. 18
  - D. 12
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
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)**
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
6. Đây là một phương pháp mã hóa
  - A. OR
  - B. AND
  - C. NOT
  - D. XOR**
7. Kích thước khối dữ liệu xử lý của giải thuật mã hóa AES là:
  - A. 160 bit
  - B. 64 bit
  - C. 192 bit
  - D. 128 bit**
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
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
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
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
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
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
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
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
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
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
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
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
20. Các hộp thay thế s-box trong giải thuật DES có số bit đầu vào và đầu ra tương ứng là:
- A. Vào 4 bit và ra 4 bit  
B. Vào 6 bit và ra 6 bit  
C. Vào 8 bit và ra 6 bit  
**D. Vào 6 bit và ra 4 bit**
21. Một trong các ứng dụng phổ biến của các hàm băm là để tạo chuỗi...
- A. CheckError  
B. CheckTotal  
C. CheckNum  
**D. Checksum**
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**  
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
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
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
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
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 bit là:
- A. 10  
**B. 12**  
C. 16  
D. 14
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
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
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
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 MD5
- D. Tạo và kiểm tra chữ ký số

#### ///Chương 4:

- Nguyên tắc bảo mật tài nguyên của mô hình Bell-La Padula là:
  - Đọc lên và ghi lên
  - Đọc xuống và ghi xuống
  - Đọc xuống và ghi lên
  - Đọc lên và ghi xuống
- Tính bảo mật của kỹ thuật điều khiển truy nhập sử dụng mật khẩu dựa trên:
  - Tần suất sử dụng mật khẩu
  - Kích thước của mật khẩu
  - Độ khó đoán và tuổi thọ của mật khẩu
  - Số loại ký tự dùng trong mật khẩu
- Phát hiện tấn công, xâm nhập dựa trên bất thường có tiềm năng phát hiện các loại tấn công, xâm nhập mới là do:
  - Không yêu cầu biết trước thông tin về chúng
  - Đã có chữ ký của các tấn công, xâm nhập mới
  - Các tấn công, xâm nhập mới thường dễ nhận biết
  - Không yêu cầu xây dựng cơ sở dữ liệu các chữ ký
- Một trong các điểm yếu làm giảm hiệu quả của phát hiện tấn công, xâm nhập dựa trên bất thường là:
  - Không có khả năng ngăn chặn tấn công, đột nhập
  - Không có khả năng phát hiện các cuộc tấn công Dos
  - Tỷ lệ cảnh báo sai cao
  - Không có khả năng phát hiện tấn công, xâm nhập mới
- Phát hiện tấn công, xâm nhập dựa trên bất thường dựa trên giá thiết:
  - Các hành vi tấn công, xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường
  - Các hành vi tấn công, xâm nhập gây ngắt quãng dịch vụ cung cấp cho người dùng
  - Các hành vi tấn công, xâm nhập có quan hệ chặt chẽ với các dịch vụ được cung cấp

- D. Các hành vi tấn công, xâm nhập gây tổn hại nghiêm trọng cho hệ thống
6. Ưu điểm của điều khiển truy nhập dựa trên các đặc điểm sinh trắc học là:
- A. Bảo mật cao và độ ổn định cao
  - B. Bảo mật cao và chi phí thấp
  - C. Bảo mật cao và luôn đi cùng với chủ thể
  - D. Bảo mật cao và được hỗ trợ rộng rãi
7. Một ưu điểm của tường lửa có trạng thái so với tường lửa không trạng thái là:
- A. Lọc nội dung gói tốt hơn
  - B. Nhận dạng được các dạng tấn công và các phần mềm độc hại
  - C. Chạy nhanh hơn
  - D. Phân biệt được các gói tin thuộc về các kết nối mạng khác nhau
8. Các phương pháp xử lý, phân tích dữ liệu và mô hình hoá trong phát hiện tấn công, xâm nhập dựa trên bất thường, gồm:
- A. Thống kê, học máy, khai phá dữ liệu
  - B. Học máy, khai phá dữ liệu, agents
  - C. Thống kê, học máy, đồ thị
  - D. Thống kê, đối sánh chuỗi, đồ thị
9. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập dựa trên vai trò - RBAC:
- A. RBAC cho phép người tạo ra đối tượng có thể cấp quyền truy nhập cho người dùng khác
  - B. RBAC là cơ chế điều khiển truy nhập được sử dụng rộng rãi nhất
  - C. RBAC cấp quyền truy nhập dựa trên vai trò của người dùng trong tổ chức
  - D. RBAC cấp quyền truy nhập dựa trên tính nhạy cảm của thông tin và chính sách quản trị
10. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập DAC:
- A. DAC cho phép người tạo ra đối tượng có thể cấp quyền truy nhập cho người dùng khác
  - B. DAC cấp quyền truy nhập dựa trên tính nhạy cảm của thông tin và chính sách quản trị
  - C. DAC là cơ chế điều khiển truy nhập được sử dụng rộng rãi nhất
  - D. DAC quản lý quyền truy nhập chặt chẽ hơn các cơ chế khác
11. Đây là một công cụ có khả năng rà quét các lỗ hổng chèn mã SQL cho các trang web?
- A. nmap
  - B. Microsoft Baseline Security Analyzer
  - C. Nessus vulnerability scanner
  - D. Acunetix Web Vulnerability Scanner
12. Danh sách điều khiển truy nhập ACL thực hiện việc quản lý quyền truy nhập đến các đối tượng cho người dùng bằng cách:
- A. Các quyền truy nhập vào đối tượng cho mỗi người dùng được quản lý trong một ma trận
  - B. Các quyền truy nhập vào đối tượng cho mỗi người dùng được quản lý riêng rẽ
  - C. Mỗi người dùng được gán một danh sách các đối tượng kèm theo quyền truy nhập
  - D. Mỗi đối tượng được gán một danh sách người dùng kèm theo quyền truy nhập
13. Tường lửa không thể chống lại...
- A. Các hiểm họa từ bên trong
  - B. Các hiểm họa từ bên ngoài
  - C. Tấn công giả mạo địa chỉ
  - D. Tấn công từ mạng Internet
14. Sự khác biệt chính giữa hệ thống ngăn chặn xâm nhập (IPS) và hệ thống phát hiện xâm nhập (IDS) là:
- A. IPS phát hiện xâm nhập hiệu quả hơn

- B. IPS có khả năng chủ động ngăn chặn xâm nhập
  - C. IDS phát hiện xâm nhập hiệu quả hơn
  - D. IDS có khả năng chủ động ngăn chặn xâm nhập
15. Tường lửa lọc gói có thể lọc các thông tin nào trong gói tin?
- A. Chỉ các thông tin trong header của gói tin
  - B. Chỉ các thông tin trong payload của gói tin
  - C. Chỉ lọc địa chỉ IP trong gói tin
  - D. Cả thông tin trong header và payload của gói tin
16. Không nên sử dụng nhiều hơn 1 phần mềm quét virus chạy ở chế độ quét theo thời gian thực trên một máy tính vì:
- A. Các phần mềm quét virus xung đột với nhau
  - B. Các phần mềm quét virus không thể hoạt động
  - C. Các phần mềm quét virus chiếm nhiều tài nguyên
  - D. Các phần mềm quét virus tấn công lẫn nhau
17. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập bắt buộc MAC:
- A. MAC cho phép người tạo ra đối tượng có thể cấp quyền truy nhập cho người dùng khác
  - B. MAC quản lý quyền truy nhập chặt chẽ hơn các cơ chế khác
  - C. MAC cấp quyền truy nhập dựa trên tính nhạy cảm của thông tin và chính sách quản trị
  - D. MAC là cơ chế điều khiển truy nhập được sử dụng rộng rãi nhất
18. Đầu là một loại tường lửa?
- A. Server gateway
  - B. Application server
  - C. Application-level gateway
  - D. Gateway server
19. Ví điện tử Paypal là một dạng...
- A. Khóa mã (encrypted key)
  - B. The ATM
  - C. Thẻ bài (token)
  - D. Thẻ thông minh (smart card)
20. Dạng xác thực sử dụng các thông tin nào dưới đây đảm bảo độ an toàn cao hơn?
- A. Thẻ ATM và tên truy nhập
  - B. Tên truy nhập và số PIN
  - C. Thẻ ATM và số PIN
  - D. Tên truy nhập và mật khẩu
21. Một trong các dạng khóa mã (encrypted keys) được sử dụng rộng rãi trong điều khiển truy nhập là:
- A. E-token
  - B. Chứng chỉ số khóa công khai
  - C. The ATM
  - D. Mobile-token
22. Tại sao một hệ thống phát hiện xâm nhập dựa trên chữ ký không thể phát hiện các tấn công, xâm nhập mới?
- A. Do chữ ký của chúng chưa tồn tại trong hệ thống
  - B. Do các tấn công, xâm nhập mới không có chữ ký
  - C. Do các tấn công, xâm nhập mới không gây ra bất thường
  - D. Do các tấn công, xâm nhập mới chỉ gây thiệt hại nhỏ
23. Ưu điểm của thẻ bài (token) so với thẻ thông minh (smart card) trong điều khiển truy nhập là:
- A. Có cơ chế xác thực mạnh hơn

- B. Có cơ chế xác thực đa dạng hơn
  - C. Được sử dụng rộng rãi hơn
  - D. Có chi phí rẻ hơn
24. Phương pháp xác thực nào dưới đây có thể cung cấp khả năng xác thực có độ an toàn cao nhất?
- A. Sử dụng Smartcard
  - B. Sử dụng vân tay
  - C. Sử dụng chứng chỉ số
  - D. Sử dụng mật khẩu
25. Đầu là các tính năng của kiểm soát truy nhập sử dụng tường lửa?
- A. Kiểm soát dịch vụ và các phần mềm
  - B. Kiểm soát người dùng và tin tặc
  - C. Kiểm soát dịch vụ và hướng
  - D. Kiểm soát virus và các malware khác
26. Ba cơ chế điều khiển truy nhập thông dụng gồm:
- A. DAC, MAC và RRAC
  - B. DAC, BAC và RBAC
  - C. DAC, MAC và BAC
  - D. DAC, MAC và RBAC
27. Mục đích chính của điều khiển truy nhập là để đảm bảo các thuộc tính an ninh của thông tin, hệ thống và các tài nguyên, gồm:
- A. Tính bảo mật, tính toàn vẹn và tính xác thực
  - B. Tính bí mật, tính toàn vẹn và tính xác thực
  - C. Tính bảo mật, tính toàn vẹn và tính sẵn dùng
  - D. Tính bí mật, tính toàn vẹn và tính sẵn dùng
28. Số lượng nhân tố (factor) xác thực sử dụng trong điều khiển truy nhập dựa trên thẻ thông minh là:
- A. 1
  - B. 3
  - C. 2
  - D. 4
29. Một nhiệm vụ chính của các hệ thống IDS/IPS là:
- A. Truy tìm và tấn công ngược lại hệ thống của tin tặc
  - B. Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập
  - C. Giám sát lưu lượng mạng nhận dạng các dấu hiệu của tấn công, xâm nhập
  - D. Giám sát các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập
30. Hai dịch vụ quan trọng nhất của một hệ thống điều khiển truy nhập là:
- A. Authentication và Authorization
  - B. Authenticator và Administrator
  - C. Administrator và Authorization
  - D. Authentication và Administrator
31. Tìm phát biểu đúng về phát hiện xâm nhập dựa trên chữ ký và phát hiện xâm nhập dựa trên bất thường:
- A. Phát hiện xâm nhập dựa trên chữ ký thường có tỷ lệ phát hiện đúng cao hơn
  - B. Tính bảo mật, tính toàn vẹn và tính xác thực
  - C. Tính bảo mật, tính toàn vẹn và tính sẵn dùng



- D. Tính bí mật, tính toàn vẹn và tính sẵn dùng
32. Tìm phát biểu đúng về dịch vụ xác thực trong điều khiển truy nhập:
- A. Là quá trình xác minh tính chân thực của thông tin nhận dạng người dùng cung cấp
  - B. Là quá trình xác minh nhận dạng của chủ thể
  - C. Là quá trình xác minh các thông tin nhận dạng của chủ thể yêu cầu truy nhập đối tượng
  - D. Là quá trình xác minh nhận dạng của người dùng
33. Loại tấn công nào sau đây chiếm quyền truy nhập đến tài nguyên lợi dụng cơ chế điều khiển truy nhập DAC?
- A. Spoofing
  - B. Trojan horse
  - C. Man in the middle
  - D. Phishing
34. Đây là tên viết đúng của Hệ thống phát hiện đột nhập/xâm nhập?
- A. Intrusion Detector System
  - B. Intrusion Detecting System
  - C. Intrusion Detection System
  - D. Instruction Detection System
35. Một trong các nhược điểm chính của điều khiển truy nhập dựa trên các đặc điểm sinh trắc học là:
- A. Không được hỗ trợ rộng rãi
  - B. Chi phí đắt
  - C. Khó sử dụng
  - D. Công nghệ phức tạp
36. Ưu điểm của mật khẩu một lần (OTP-One Time Password) so với mật khẩu truyền thống là:
- A. Chống được tấn công từ điển
  - B. Chống được tấn công vét cạn
  - C. Chống được tấn công phá mã
  - D. Chống được tấn công phát lại
37. Kỹ thuật tấn công SYN Floods khai thác điểm yếu trong khâu nào trong bộ giao thức TCP/IP?
- A. Bắt tay 3 bước
  - B. Bắt tay 2 bước
  - C. Xác thực người dùng
  - D. Truyền dữ liệu

đáp án nhé :