**Cơ sở An toàn Thông tin 1**

# Chương 1 + chương 2

1. An toàn hệ thống thông tin là: Việc đảm bảo các thuộc tính an ninh, an toàn của hệ thống thông tin
2. An toàn thông tin (Information Security) là: Là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép
3. An toàn thông tin gồm hai lĩnh vực chính là: An toàn công nghệ thông tin và Đảm bảo thông tin
4. Biện pháp nào không thể phòng chống hiệu quả tấn công khai thác lỗi tràn bộ đệm? Sử dụng công cụ gỡ rối để ngăn chặn tràn trong thời gian vận hành
5. Các kỹ thuật và công cụ thường được sử dụng trong an ninh mạng bao gồm: Điều khiển truy nhập, tường lửa, proxy và các giao thức bảo mật, ứng dụng dựa trên mật mã
6. Các lỗ hổng an ninh trong hệ điều hành máy chủ là mối đe dọa thuộc vùng nào trong 7 vùng cơ sở hạ tầng CNTT? Vùng mạng LAN
7. Các lỗ hổng bảo mật thường tồn tại nhiều nhất trong thành phần nào của hệ thống: Các ứng dụng
8. Các thành phần chính của hệ thống máy tính gồm: Hệ thống phần cứng và Hệ thống phần mềm
9. Các thành phần của an toàn thông tin gồm: An toàn máy tính và dữ liệu, An ninh mạng, Quản lý ATTT và Chính sách ATTT
10. Các vùng bộ nhớ thường bị tràn gồm: Ngăn xếp (Stack) và Vùng nhớ cấp phát động (Heap)
11. Các yêu cầu cơ bản trong đảm bảo an toàn thông tin và an toàn hệ thống thông tin gồm: Bí mật, Toàn vẹn và Sẵn dùng
12. Đảm bảo thông tin (Information assurance) thường được thực hiện bằng cách: Sử dụng kỹ thuật tạo dự phòng ngoại vi
13. Dạng tấn công chèn mã được tin tặc thực hiện phổ biến trên các trang web nhắm đến các cơ sở dữ liệu là: Tấn công chèn mã SQL
14. Đâu là dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng? Lỗi tràn bộ đệm
15. Đâu là một trong các biện pháp phòng chống tấn công khai thác lỗi tràn bộ đệm? Sử dụng cơ chế cấm thực hiện mã trong dữ liệu
16. Để đảm bảo an toàn cho hệ thống điều khiển truy cập, một trong các biện pháp phòng chống hiệu quả là: Không dùng tài khoản có quyền quản trị để chạy các chương trình ứng dụng
17. Hệ thống thông tin là: 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
18. 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: Địa chỉ trở về của hàm
19. Lỗ hổng bảo mật (Security vulnerability) là một điểm yếu tồn tại trong một hệ thống cho phép tin tặc: Khai thác gây tổn hại đến các thuộc tính an ninh của hệ thống đó
20. Lỗi tràn bộ đệm là lỗi trong khâu: Lập trình phần mềm
21. Mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin thường gồm các lớp: An ninh tổ chức, An ninh mạng và An ninh hệ thống
22. Một điểm yếu điển hình trong hệ thống điều khiển truy cập là việc sử dụng mật khẩu dễ đoán hoặc mật khẩu được lưu ở dạng rõ. Đây là điểm yếu thuộc khâu: Xác thực
23. 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? Bí mật và Toàn vẹn
24. Một trong các biện pháp cụ thể cho quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống là: Định kỳ cập nhật các bản vá và nâng cấp hệ điều hành
25. Một trong các nội dung rất quan trọng của quản lý an toàn thông tin là: Quản lý rủi ro
26. Người sử dụng hệ thống thông tin quản lý trong mô hình 4 loại hệ thống thông tin là: Quản lý bộ phận
27. 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? Vùng mạng WAN
28. Nguyên nhân của sự tồn tại các điểm yếu trong hệ thống có thể do: Lỗi thiết kế, lỗi cài đặt và lập trình
29. Nguyên tắc cơ bản cho đảm bảo an toàn thông tin, hệ thống và mạng là: Phòng vệ nhiều lớp có chiều sâu
30. 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? Lớp an ninh hệ thống
31. Tại sao cần phải đảm bảo an toàn cho thông tin? Do có nhiều thiết bị kết nối mạng Internet với nhiều nguy cơ và đe dọa
32. Tìm phát biểu đúng trong các phát biểu sau: Điểm yếu hệ thống có thể xuất hiện trong cả các mô đun phần cứng và phần mềm
33. Tính bí mật của thông tin có thể được đảm bảo bằng: Bảo vệ vật lý, VPN, hoặc mã hóa
34. Trong 7 vùng của cơ sở hạ tầng CNTT, vùng nào có nhiều mối đe dọa và nguy cơ nhất? Vùng người dùng
35. 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: Tăng khả năng mã tấn công được thực hiện
36. Trong tấn công khai thác lỗi tràn bộ đệm, tin tặc thường sử dụng shellcode. Shellcode đó là dạng: mã máy
37. 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: Cân bằng giữa An toàn, Hữu dụng và Rẻ tiền
38. Việc thực thi quản lý ATTT cần được thực hiện theo chu trình lặp lại là do: Các điều kiện bên trong và bên ngoài hệ thống thay đổi theo thời gian
39. Sâu SQL Slammer được phát hiện vào năm: 2003
40. Trong các vùng hạ tầng CNTT, vùng nào dễ bị tấn công DoS, DDoS nhất? Vùng mạng WAN
41. Trong các vùng hạ tầng CNTT, vùng nào có các lỗ hổng trong các phần mềm ứng dụng của máy chủ? Vùng mạng LAN
42. Trong các vùng hạ tầng CNTT, vùng nào có các lỗ hổng trong quản lý phần mềm ứng dụng của máy chủ? Vùng hệ thống và ứng dụng
43. Tìm phát biểu đúng trong các phát biểu sau: Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống
44. Sâu SQL Slammer tấn công khai thác lỗi tràn bộ đệm trong hệ quản trị cơ sở dữ liệu: SQL Server 2000

# Chương 3

1. Dạng tấn công gây ngắt quãng dịch vụ hoặc kênh truyền thông cho người dùng bình thường là: Interruptions
2. Một trong các biện pháp có thể sử dụng để phòng chống tấn công người đứng giữa là: Sử dụng chứng chỉ số để xác thực thông tin nhận dạng các bên
3. Đâu là một kỹ thuật tấn công DoS: Ping of death
4. Có thể phòng chống tấn công Smurf bằng cách cấu hình các máy và router không trả lời: các yêu cầu ICMP hoặc các yêu cầu phát quảng bá
5. Mục đích chính của tấn công giả mạo địa chỉ IP là: Để vượt qua các hàng rào kiểm soát an ninh
6. Để thực hiện tấn công Smurf, tin tặc phải giả mạo địa chỉ gói tin ICMP trong yêu cầu tấn công. Tin tặc sử dụng: Địa chỉ máy nạn nhân làm địa chỉ nguồn của gói tin
7. Pharming là kiểu tấn công vào: Máy khách/trình duyệt web
8. 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: Reflectors
9. Macro viruses là loại viruses thường lây nhiễm vào: Các file tài liệu của bộ phần mềm Microsoft Office
10. Khác biệt cơ bản giữa tấn công DoS và DDoS là: Phạm vi tấn công
11. 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? UNION SELECT
12. Tấn công bằng mã độc có thể gồm: SQLi, XSS, CSRF và Buffer overflow
13. Nguy cơ cao nhất mà một cuộc tấn công chèn mã SQL có thể gây ra cho một hệ thống là: Chiếm quyền điều khiển hệ thống
14. Kỹ thuật tấn công SYN Floods khai thác điểm yếu trong khâu nào trong bộ giao thức TCP/IP? Bắt tay 3 bước
15. Trong dạng tấn công vào mật khẩu dựa trên từ điển, tin tặc đánh cắp mật khẩu của người dùng bằng cách: Thử các từ có tần suất sử dụng cao làm mật khẩu trong từ điển
16. Một trong các phương thức lây lan thường gặp của sâu mạng là: Lây lan thông qua khả năng thực thi từ xa
17. Đâu là một biện pháp phòng chống tấn công SYN Floods? SYN Cache
18. Các zombie thường được tin tặc sử dụng để: Thực hiện tấn công DDoS
19. Khác biệt cơ bản của vi rút và sâu là: Sâu có khả năng tự lây lan mà không cần tương tác của người dùng
20. Một trong các mối đe dọa an toàn thông tin thường gặp là: Phần mềm độc hại
21. Tấn công nghe lén là kiểu tấn công: Thụ động
22. Đâu là một công cụ kiểm tra lỗ hổng tấn công chèn mã SQL trên các website: SQLmap
23. Tấn công từ chối dịch vụ (DoS - Denial of Service Attacks) là dạng tấn công có khả năng: Cản trở người dùng hợp pháp truy nhập các tài nguyên hệ thống
24. Đâu là một kỹ thuật tấn công DoS? Smurf
25. Trên thực tế, có thể giảm khả năng bị tấn công nếu có thể: giảm thiểu các lỗ hổng bảo mật
26. Tấn công kiểu Social Engineering là dạng tấn công khai thác yếu tố nào sau đây trong hệ thống? Người dùng
27. Để thực hiện tấn công DDoS, tin tặc trước hết cần chiếm quyền điều khiển của một lượng lớn máy tính. Các máy tính bị chiếm quyền điều khiển thường được gọi là: Zombies
28. Kỹ thuật tấn công Smurf sử dụng giao thức ICMP và cơ chế gửi: Broadcast
29. Tìm phát biểu đúng trong các phát biểu sau: Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống.
30. Tấn công kiểu Social Engineering có thể cho phép tin tặc: Đánh cắp thông tin nhạy cảm của người dùng
31. Phishing là một dạng của loại tấn công sử dụng: Kỹ thuật xã hội
32. Tại sao việc sử dụng thủ tục cơ sở dữ liệu (Stored procedure) là một trong các biện pháp hiệu quả để ngăn chặn triệt để tấn công chèn mã SQL? Thủ tục cơ sở dữ liệu cho phép tách mã lệnh SQL khỏi dữ liệu người dùng
33. Các dạng phần mềm độc hại (malware) có khả năng tự nhân bản gồm: Virus, worm, zombie
34. Dạng tấn công giả mạo thông tin thường để đánh lừa người dùng thông thường là: Fabrications
35. Một trong các cách virus thường sử dụng để lây nhiễm vào các chương trình khác là: Sửa đổi các chương trình
36. Các máy tính ma/máy tính bị chiếm quyền điều khiển thường được tin tặc sử dụng để: Gửi thư rác, thư quảng cáo
37. 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: DAC
38. Mật khẩu an toàn trong thời điểm hiện tại là mật khẩu có: Độ dài từ 8 ký tự trở lên, gồm chữ cái hoa, thường, chữ số và ký tự đặc biệt
39. Một trong các biện pháp hiệu quả để phòng chống macro viruses là: Cấm tự động thực hiện macro trong Microsoft Office
40. Dạng tấn công chặn bắt thông tin truyền trên mạng để sửa đổi hoặc lạm dụng là: Interceptions

# Chương 4

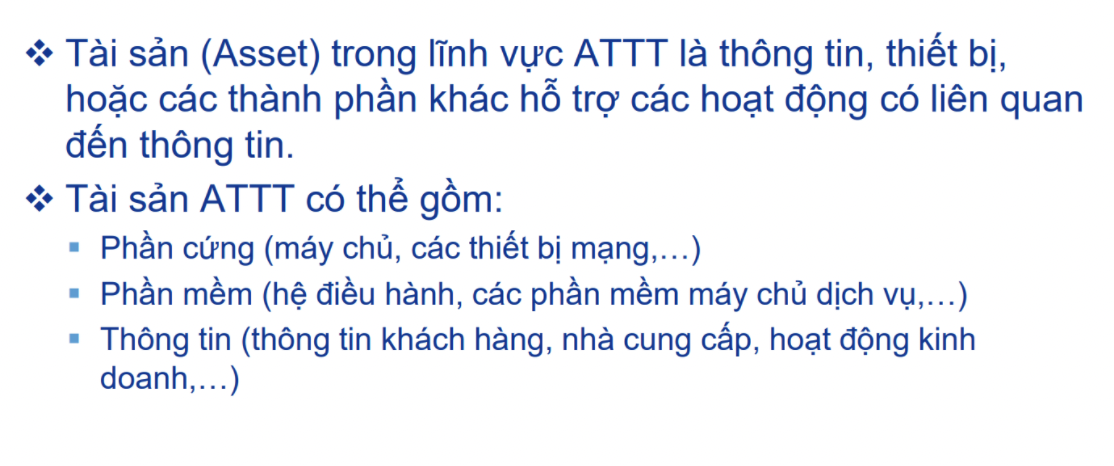
1. Đâu là một phương pháp mã hóa: XOR
2. Một trong các điểm yếu của các hệ mã hóa khóa công khai là: Tốc độ chậm
3. Điểm khác nhau chính giữa hai loại hàm băm MDC và MAC là: MDC là loại hàm băm không khóa, còn MAC là loại hàm băm có khóa.
4. Kích thước khóa hiệu dụng của hệ mã hóa DES là 56 bit
5. Đâu là một chế độ hoạt động (Modes of Operation) của mã hóa khối? ECB
6. Một trong các ứng dụng phổ biến của các hàm băm 1 chiều là: Mã hóa mật khẩu
7. Tìm phát biểu đúng về mã hóa khóa bất đối xứng (Asymmetric key cryptography): 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: State
9. Các hộp thay thế S-Box trong giải thuật DES có số bít đầu vào và đầu ra tương ứng là: Vào 6 bít, ra 4 bít
10. Hai thuộc tính cơ bản và quan trọng nhất của một hàm băm là: Nén và dễ tính toán.
11. Trật tự các khâu xử lý trong các vòng lặp chính của giải thuật mã hóa AES: SubBytes, ShiftRows, MixColumns, AddRoundKey
12. Số lượng vòng lặp chính thực hiện xáo trộn dữ liệu theo hàm Feistel (F) trong giải thuật DES là: 16
13. Trong hệ mã hóa RSA, quan hệ toán học giữa khóa riêng d và khóa công khai e là: d là modulo nghịch đảo của e
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: 12
15. Các giải thuật mã hóa khóa đối xứng thông dụng gồm: DES, 3DES, AES
16. Trong quá trình xử lý thông điệp đầu vào tạo chuỗi băm, số lượng vòng xử lý của hàm băm SHA1 là: 80
17. Một trong các điểm yếu của các hệ mã hóa khóa đối xứng là: Khó khăn trong quản lý và phân phối khóa.
18. Độ an toàn của giải thuật RSA dựa trên: Tính khó của việc phân tích số nguyên lớn.
19. Đâu là một ứng dụng của mã hóa: PGP
20. Giải thuật mã hóa AES được thiết kế dựa trên: Mạng hoán vị-thay thế (SPN)
21. Trong hệ mật mã RSA, quan hệ toán học giữa khóa công khai e và số Phi(n) là: e và Phi(n) là hai số nguyên tố cùng nhau
22. Kích thước khối dữ liệu xử lý của giải thuật mã hóa AES là: 128
23. Đâu là một chế độ hoạt động (Modes of Operation) của mã hóa khối: CBC
24. Phần xử lý chính của SHA1 làm việc trên một chuỗi được gọi là state là: 160
25. Một hệ mã hóa (cryptosystem) được cấu thành từ hai thành phần chính gồm: Phương pháp mã hoá và không gian khoá
26. Số lượng thao tác trong mỗi vòng xử lý của hàm băm MD5 là: 16
27. Một trong các ứng dụng phổ biến của các hàm băm là để tạo chuỗi: CheckSum
28. Trong mã hóa dòng (stream cipher), dữ liệu được xử lý theo: Từng bit hoặc từng byte/ ký tự
29. Khi sinh cặp khóa RSA, các số nguyên tố p và q nên được chọn với kích thước: Bằng khoảng 1 nửa kích thước của N (Tính theo bit)
30. Giải thuật mã hóa DES được thiết kế dựa trên: Mạng Feistel
31. Phần xử lý chính của MD5 làm việc trên một chuỗi được gọi là state là: 128
32. Liệt kê các chế độ hoạt động của mã hóa khối : ECB, CBC, CFB, OFB
33. Các hàm băm (Hash functions) là các thuật toán để tạo các bản tóm tắt của thông điệp được sử dụng để ... tính toàn vẹn của thông điệp: Nhận dạng và Đảm bảo
34. Kích thước khóa đầu vào của hệ mã hóa DES là 64 bit
35. Trong hàm F của mô hình Feistel trong DES gồm bao nhiêu bước: 4
36. Trong hàm F của mô hình Feistel trong DES có thứ tự các bước như thế nào: Expansion,XOR,Substitution,Permutation
37. Quá trình sinh khóa của DES có quay trái bao nhiêu vòng và mỗi vòng quay trái mấy bit? 16 vòng , 1 hoặc 2 bit
38. MD5 và SHA1 : Thông điệp phải chia thành các khối 512 bit
39. MD5 làm việc trên state 128 bit

# Chương 5

1. Tại sao một hệ thống phát hiện xâm nhập dựa trên chữ ký không thể phát hiện các tấn công, xâm nhập mới: Do chữ ký của chúng chưa tồn tại trong hệ thống
2. Không nên sử dụng nhiều hơn một phần mềm quét virus chạy ở chế độ quét theo thời gian thực trên một máy tính vì: Các phần mềm quét virus xung đột với nhau
3. Phát hiện tấn công, xâm nhập dựa trên bất thường dựa trên giả thiết: Các hành vi tấn công, xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường
4. Đâu là tên viết đúng của hệ thống xâm nhập/ đột nhập: Intrusion Detection System
5. Đâu là các tính năng của kiểm soát truy nhập sử dụng tường lửa: Kiểm soát dịch vụ và hướng; Kiểm soát người dùng và hành vi
6. Một hệ thống điều khiển truy nhập có thể được cấu thành từ các dịch vụ nào sau đây: Xác thực, trao quyền và quản trị
7. Một trong các dạng mã hóa ( encrypted Keys) được sử dụng rộng rãi trong điều khiển truy nhập là: Chứng chỉ số hóa công khai
8. Sự khác biệt chính giữa hệ thống ngăn chặn xâm nhập (IPS) và hệ thống phát hiện xâm nhập (IDS) là: IPS có khả năng chủ động ngăn chặn xâm nhập
9. Phương pháp xác thực nào dưới đây có thể cung cấp khả năng xác thực có độ an toàn cao nhất? Sử dụng vân tay
10. Điều khiển truy nhập dựa trên luật(Rule-based access control) được sử dụng phổ biến trong: Firewall
11. Một ưu điểm của tường lửa có trạng thái so với tường lửa không trạng thái là: Phân biệt được các gói tin thuộc về các kết nối mạng khác nhau
12. Tường lửa lọc gói có thể lọc các thông tin nào trong gói tin: Chỉ các thông tin trong header của gói tin
13. Tường lửa không thể chống lại: Tấn công hướng dữ liệu
14. Đâu là một công cụ có khả năng rà quét các lỗ hổng chèn mã SQL cho các trang web: Acunetix Web Vulnerability Scanner.
15. Nguyên tắc bảo mật tài nguyên của mô hình Bell-La Padula là: Đọc xuống và ghi lên
16. 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
17. Ưu điểm của thẻ bài (token) so với thẻ thông minh (smart card) trong điều khiển truy nhập là: Có cơ chế xác thực mạnh hơn
18. Nêu các loại tường lửa: Packet Router Gateway; Packet-Filtering Router; Application-Level Gateway; Circuit-Level gateway
19. Tìm phát biểu đúng về dịch vụ xác thực trong điều khiển truy nhập: là quá trình xác minh tính chân thực của thông tin nhận dạng người dùng cung cấp
20. 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: Tính bí mật, tính toàn vẹn và tính sẵn dùng
21. Ưu điểm của điều khiển truy nhập dựa trên các đặc điểm sinh trắc học là: Bảo mật cao và luôn đi cùng với chủ thể
22. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập bắt buộc MAC: MAC cấp quyền truy nhập dựa trên tính nhạy cảm của thông tin và chính sách quản trị
23. Một nhiệm vụ chính của các hệ thống IDS/IPS là: Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập.
24. Số lượng nhân tố (factor) xác thực sử dụng trong điều khiển truy nhập dựa trên thẻ thông minh là: 2
25. Dạng xác thực sử dụng các thông tin nào dưới đây đảm bảo độ an toàn cao hơn: Thẻ ATM và số PIN
26. Ưu điểm của mật khẩu một lần (OTP-One Time Password) so với mật khẩu truyền thống là: Chống được tấn công phát lại
27. Hai dịch vụ quan trọng nhất của một hệ thống điều khiển truy nhập là: Authentication và Authorization
28. Tìm phát biểu đúng về phát hiện xâm nhập dựa trên chữ ký và phát hiện xâm nhập dựa trên bất thường: Phát hiện xâm nhập dựa trên chữ ký thường có tỷ lệ phát hiện đúng cao hơn
29. Các hệ thống phát hiện xâm nhập có thể thu thập dữ liệu đầu vào từ: Mạng và các host
30. Một trong các nhược điểm chính của điều khiển truy nhập dựa trên các đặc điểm sinh trắc học là: Chi phí đắt
31. Danh sách điều khiển truy nhập ACL thực hiện việc quản lý quyền truy nhập đến các đối tượng cho người dùng bằng cách: Mỗi đối tượng được gán một danh sách người dùng kèm theo quyền truy nhập.
32. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập dựa trên vai trò - RBAC: RBAC cấp quyền truy nhập dựa trên vai trò của người dùng trong tổ chức
33. Tính bảo mật của kỹ thuật điều khiển truy nhập sử dụng mật khẩu dựa trên: Độ khó đoán và tuổi thọ của mật khẩu
34. Các phương pháp xử lý , phân tích dữ liệu và mô hình hóa trong phát hiện tấn công, xâm nhập bất thường gồm: Thống kê, học máy, khai phá dữ liệu
35. Ba cơ chế điều khiển truy nhập thông dụng gồm: DAC, MAC, RBAC
36. Loại tấn công nào sau đây chiếm quyền truy nhập đến tài nguyên lợi dụng cơ chế điều khiển truy nhập DAC: Trojan horse
37. Một trong các điểm yếu làm giảm hiệu quả của tấn công, xâm nhập dựa trên bất thường là: Tỷ lệ cảnh báo sai cao
38. Ví điện tử Paypal là một dạng: Thẻ bài (token)
39. Điều khiển truy nhập là quá trình mà trong đó người dùng được ... truy nhập đến các thông tin, các hệ thống và tài nguyên: Nhận dạng và Trao quyền
40. DAC hay dùng các kỹ thuật: Ma trận điều khiển truy nhập – ACM; Danh sách điều khiển truy nhập - ACL
41. Tường lửa (firewall) có thể là thiết bị phần cứng hoặc công cụ phần mềm được dùng để: Bảo vệ hệ thống và mạng cục bộ tránh các đe doạ từ bên ngoài.

# Chương 6

1. Quản lý an toàn thông tin (Information security management) là một tiến trình (process) nhằm ... các tài sản quan trọng của cơ quan, tổ chức, doanh nghiệp được bảo vệ ... với ...: Đảm bảo / Đầy đủ / Chi phí phù hợp
2. Quá trình quản lý ATTT cần được thực hiện liên tục theo chu trình do: Sự thay đổi nhanh chóng của công nghệ; Môi trường xuất hiện rủi ro liên tục thay đổi
3. Tài sản ATTT có thể gồm: Phần cứng, Phần mềm, Thông tin



1. Các phương pháp tiếp cận đánh giá rủi ro: Đường cơ sở; Không chính thức; Phân tích chi tiết rủi ro; Kết hợp
2. Mục đích của Phương pháp đường cơ sở là thực thi các kiểm soát an ninh ở mức cơ bản dựa trên: Các tài liệu cơ bản; Các quy tắc thực hành; Các thực tế tốt nhất của ngành đã được áp dụng
3. Quản lý ATTT có thể gồm các khâu: Xác định rõ mục đích đảm bảo ATTT; Xây dựng hồ sơ tổng hợp về các rủi ro; Đánh giá rủi ro với từng tài sản ATTT cần bảo vệ; Xác định và triển khai các biện pháp quản lý, kỹ thuật kiểm soát, giảm rủi ro về mức chấp nhận được
4. Trên cơ sở xác định mức rủi ro, có thể đề ra các biện pháp xử lý, kiểm soát rủi ro trong mức ... , với mức chi phí ...: Chấp nhận được / Phù hợp
5. Ưu điểm của phương pháp đường cơ sở: Không đòi hỏi các chi phí cho các tài nguyên bổ sung sử dụng trong đánh giá rủi ro chính thức; Cùng nhóm các biện pháp có thể triển khai trên nhiều hệ thống
6. Nhược điểm của phương pháp đường cơ sở: Không xem xét kỹ đến các điều kiện nảy sinh các rủi ro ở các hệ thống của các tổ chức khác nhau; Mức đường cơ sở được xác định chung nên có thể không phù hợp với từng tổ chức cụ thể
7. Phương pháp không chính thức liên quan đến việc: Thực hiện một số dạng phân tích rủi ro hệ thống CNTT của tổ chức một cách không chính thức; Sử dụng kiến thức chuyên gia của các nhân viên bên trong tổ chức, hoặc các nhà tư vấn từ bên ngoài; Không thực hiện đánh giá toàn diện các rủi ro đối với tất cả các tài sản CNTT của tổ chức
8. Ưu điểm của phương pháp không chính thức: Không đòi hỏi các nhân viên phân tích rủi ro có các kỹ năng bổ sung, nên có thể thực hiện nhanh với chi phí thấp; Việc có phân tích hệ thống CNTT của tổ chức giúp cho việc đánh giá rủi ro, lỗ hổng chính xác hơn và các biện pháp kiểm soát đưa ra cũng phù hợp hơn phương pháp đường cơ sở
9. Nhược điểm của phương pháp không chính thức: Do đánh giá rủi ro không được thực hiện toàn diện nên có thể một rủi ro không được xem xét kỹ, nên có thể để lại nguy cơ cao cho tổ chức; Kết quả đánh giá dễ phục thuộc vào quan điểm của các cá nhân
10. Phương pháp phân tích chi tiết rủi ro là phương pháp đánh giá ..., được thực hiện một cách ... và được chia thành nhiều giai đoạn: Toàn diện / Chính thức
11. Phương pháp phân tích chi tiết rủi ro bao gồm các bước: Nhận dạng các tài sản và các mối đe dọa và lỗ hổng đối với các tài sản này; Xác định xác suất xuất hiện các rủi ro và các hậu quả có thể có nếu rủi ro xảy ra với tổ chức; Lựa chọn các biện pháp xử lý rủi ro dựa trên kết quả đánh giá rủi ro của các giai đoạn trên
12. Ưu điểm của phương pháp phân tích chi tiết rủi ro: Cho phép xem xét chi tiết các rủi ro đối với hệ thống CNTT của tổ chức, và lý giải rõ ràng các chi phí cho các biện pháp kiểm soát rủi ro đề xuất; Cung cấp thông tin tốt nhất cho việc tiếp tục quản lý vấn đề an ninh của các hệ thống CNTT khi chúng được nâng cấp, sửa đổi
13. Nhược điểm của phương pháp phân tích chi tiết rủi ro: Chi phí lớn về thời gian, các nguồn lực và yêu cầu kiến thức chuyên gia trình độ cao; Có thể dẫn đến chậm trễ trong việc đưa ra các biện pháp xử lý, kiểm soát rủi ro phù hợp
14. Mục tiêu của phương pháp kết hợp: Cung cấp mức bảo vệ hợp lý càng nhanh càng tốt , Sau đó kiểm tra và điều chỉnh các biện pháp bảo vệ trên các hệ thống chính theo thời gian
15. Ưu điểm của phương pháp kết hợp: Việc bắt đầu bằng việc đánh giá rủi ro ở mức cao dễ nhận được sự ủng hộ của cấp quản lý, thuận lợi cho việc lập kế hoạch quản lý ATTT; Giúp sớm triển khai các biện pháp xử lý và kiểm soát rủi ro ngay từ giai đoạn đầu; Có thể giúp giảm chi phí với đa số các tổ chức
16. Nhược điểm của phương pháp kết hợp: Việc bắt đầu bằng việc đánh giá rủi ro ở mức cao dễ nhận được sự ủng hộ của cấp quản lý, thuận lợi cho việc lập kế hoạch quản lý ATTT; Giúp sớm triển khai các biện pháp xử lý và kiểm soát rủi ro ngay từ giai đoạn đầu; Có thể giúp giảm chi phí với đa số các tổ chức
17. Bộ chuẩn ISO ..... là bộ chuẩn về quản lý ATTT (Information Technology - Code of Practice for Information Security Management) được tham chiếu rộng rãi nhất: 27000
18. Năm 2007, ISO ..... được đổi tên thành ISO 27002 song hành với ISO 27001: 17799:2005
19. Bộ chuẩn ISO/IEC .... (được soạn thảo năm 2000 bởi International Organization for Standardization (ISO) và International Electrotechnical Commission (IEC)) là tiền thân của ISO 27000: 17799
20. ISO/IEC 27002 gồm ... điều: 127
21. ISO/IEC 27002 đề ra các khuyến nghị về quản lý ATTT cho những người thực hiện việc ... trong tổ chức của họ: Khởi tạo, thực hiện và duy trì an ninh an toàn
22. ISO 27001 cung cấp các thông tin để: Thực thi các yêu cầu của ISO/IEC 27002
23. ISO 27001 cung cấp các thông tin để thực hiện việc quản lý ATTT, nhưng: Nó chỉ tập trung vào các phần việc phải thực hiện; Không chỉ rõ cách thức thực hiện
24. ISO/IEC 27001:2005 bao gồm mấy phần: 4
25. Plan-Do-Check-Act -> Plan: Đề ra phạm vi , chính sách của ISMS và hướng tiếp cận đánh giá rủi ro; Nhận dạng , đánh giá rủi ro và các phương pháp xử lý rủi ro; Lựa chọn các mục tiêu kiểm soát và biện pháp kiểm soát; Chuẩn bị tuyên bố / báo cáo áp dụng
26. Plan-Do-Check-Act -> Do: Xây dựng và thực thi kế hoạch rủi ro; Thực thi các kiểm soát và các chương trình đào tạo chuyên môn và giáo dục ý thức; Quản lý các hoạt động và tài nguyên; Thực thi các thủ tục phát hiện và phản ứng lại các sự cố an ninh
27. Plan-Do-Check-Act -> Check: Thực thi các thủ tục giám sát và việc đánh giá thường xuyên tính hiệu quả của ISMS; Thực hiện việc kiểm toán (audit) nội bộ với ISMS; Thực thi việc đánh giá thường xuyên với ISMS bởi bộ phận quản lý; Ghi lại các hành động và sự kiện ảnh hưởng đến ISMS
28. Plan-Do-Check-Act -> Act: Thực hiện các cải tiến đã được nhận dạng , các hành động sửa chữa và ngăn chặn; Áp dụng các bài đã được học và Thảo luận kết quả với các bên quan tâm; Đảm bảo các cải tiến đạt được các mục tiêu
29. Các nhân viên đảm bảo an toàn cho thông tin phải hiểu rõ những khía cạnh pháp lý và đạo đức ATTT: Luôn nắm vững môi trường pháp lý hiện tại và các luật và các quy định luật pháp; Luôn thực hiện công việc nằm trong khuôn khổ cho phép của luật pháp
30. DMCA là viết tắt của luật gì: Digital Millennium Copyright Act
31. Luật: Gồm những điều khoản ... và Các điều luật thường được xây dựng từ ....: Bắt buộc hoặc cấm những hành vi cụ thể / Các vấn đề đạo đức
32. Đạo đức: Định nghĩa những hành vi xã hội ...: chấp nhận được
33. Đạo đức thường dựa trên .... Do đó hành vi đạo đức giữa các dân tộc, các nhóm người khác nhau là ...: các đặc điểm văn hóa / khác nhau
34. Khác biệt giữa luật và đạo đức: Luật được thực thi bởi các cơ quan chính quyền còn đạo đức thì không
35. Luật ATTT mạng của Việt Nam được Quốc hội thông qua vào tháng ... (86/2015/QH13) và có hiệu lực từ ...: tháng 11.2015 / 1/7/2016:
36. Luật ATTT mạng gồm ... chương với ... điều: 8 / 54
37. Luật An ninh mạng của Việt Nam được Quốc hội thông qua vào tháng ... và có hiệu lực từ 1/1/2019: 6/2018
38. Trách nhiệm của tổ chức: Là trách nhiệm trước luật pháp của tổ chức đó được mở rộng ngoài phạm vi luật hình sự và luật hợp đồng; Gồm cả trách nhiệm pháp lý phải hoàn trả và đền bù cho những hành vi sai trái; Nếu một nhân viên của 1 công ty/tổ chức thực hiện hành vi phạm pháp hoặc phi đạo đức, gây thiệt hại cho cá nhân, tổ chức khác, thì công ty/tổ chức đó phải chịu trách nhiệm về pháp lý, tài chính
39. Khác biệt giữa chính sách và luật: Luật luôn bắt buộc / Chính sách: thiếu hiểu biết chính sách là 1 cách bào chữa chấp nhận được
40. Các yêu cầu của chính sách gồm .. điều và bao gồm : 5 / Phổ biến , Xem xét , Có thể hiểu , Tuân thủ , Áp dụng đồng đều ( Bình đẳng)
41. Có ... kiểu luật và bao gồm: 4 / Luật dân sự , Luật hình sự , Luật công cộng , Luật riêng
42. Các luật ATTT của Mỹ gồm ... Loại và bao gồm: 5 / Các luật tội phạm máy tính , Các luật về sự riêng tư , Luật xuất khẩu và chống gián điệp , Luật bản quyền , Luật tự do thông tin
43. Quản lý an toàn thông tin (Information security management) là một tiến trình (process) nhằm đảm bảo các tài sản quan trọng của … được bảo vệ đầy đủ với … phù hợp: Cơ quan, tổ chức, doanh nghiệp / chi phí
44. Quản lý ATTT phải trả lời được 3 câu hỏi về: Tài sản, đe doạ có thể có, biện pháp ứng phó
45. Khâu không nằm trong việc quản lý ATTT: Đánh giá tình trạng hiện thời các tài sản cần bảo vệ
46. Quá trình quản lý ATTT cần được thực hiện liên tục theo chu trình do: Bảo trì và tăng cường hiệu năng
47. Phương pháp tiếp cận không dùng để đánh giá rủi ro ATTT: Chính thức
48. Các doanh nghiệp viễn thông nhà mạng thì phù hợp với phương pháp đánh giá rủi ro nào: Phân tích chi tiết
49. Điều nào sau đây không đúng về ISO 27001: Chỉ rõ cách thức thực hiện để thực hiện quản lý ATTT
50. Vai trò của nhân viên đảm bảo an toàn cho thông tin là rất quan trọng trong việc giảm thiểu rủi ro, đảm bảo an toàn cho … và giảm thiệt hại nếu xảy ra sự cố: Thông tin , hệ thống và mạng
51. Security and Freedom through Encryption Act, 1999 liên quan tới: Luật xuất khẩu và chống gián điệp

**Cơ sở An toàn Thông tin 2**

# Chương 1

1. Mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin thường gồm các lớp: An ninh tổ chức, An ninh mạng và An ninh hệ thống
2. An toàn thông tin gồm hai lĩnh vực chính là: An toàn công nghệ thông tin và Đảm bảo thông tin
3. Tại sao cần phải đảm bảo an toàn cho thông tin? Do có nhiều thiết bị kết nối mạng Internet với nhiều nguy cơ và đe dọa
4. An toàn hệ thống thông tin là: 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: Quản lý bộ phận
6. Nguyên tắc cơ bản cho đảm bảo an toàn thông tin, hệ thống và mạng là: Phòng vệ nhiều lớp có chiều sâu
7. Một trong các nội dung rất quan trọng của quản lý an toàn thông tin là: 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? Bí mật và 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? Vùng mạng WAN
10. An toàn thông tin (Information Security) là gì? Là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép
11. Một trong các biện pháp cụ thể cho quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống là: Định kỳ cập nhật thông tin về các lỗ hổng từ các trang web chính thức
12. Các mật khẩu nào sau đây là khó phá nhất đối với một hacker? !$aLtNb83
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: Tăng khả năng mã tấn công được thực hiện
14. Tìm phát biểu đúng trong các phát biểu sau: Điểm yếu hệ thống có thể xuất hiện trong cả các mô đun phần cứng và phần mềm
15. Người sử dụng hệ thống trợ giúp ra quyết định trong mô hình 4 loại hệ thống thông tin là: Quản lý cao cấp
16. Các thành phần chính của hệ thống máy tính gồm: Hệ thống phần cứng và Hệ thống phần mềm
17. Nguyên nhân của sự tồn tại các điểm yếu trong hệ thống có thể do: Tất cả các khâu trong quá trình phát triển và vận hành
18. Trên thực tế, có thể giảm khả năng bị tấn công nếu có thể: Giảm thiểu các lỗ hổng bảo mật
19. Sâu SQL Slammer tấn công khai thác lỗi tràn bộ đệm trong hệ quản trị cơ sở dữ liệu: SQL Server 2000
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 ? Năm lần nỗ lực login thất bại trên tài khoản “jsmith”
21. Các kỹ thuật và công cụ thường được sử dụng trong an ninh mạng bao gồm: Điều khiển truy nhập, tường lửa, proxy và các giao thức bảo mật, ứng dụng dựa trên mật mã
22. Các thành phần của an toàn thông tin gồm: An toàn máy tính và dữ liệu, An ninh mạng, Quản lý ATTT và Chính sách ATTT
23. Các yêu cầu cơ bản trong đảm bảo an toàn thông tin và an toàn hệ thống thông tin gồm: Bí mật, Toàn vẹn và Sẵn dùng
24. Việc thực thi quản lý ATTT cần được thực hiện theo chu trình lặp lại là do: Các điều kiện bên trong và bên ngoài hệ thống thay đổi theo thời gian
25. Hệ thống thông tin là: 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
26. Tính bí mật của thông tin có thể được đảm bảo bằng: Bảo vệ vật lý, VPN, hoặc mã hóa
27. Đảm bảo thông tin (Information assurance) thường được thực hiện bằng cách: Sử dụng kỹ thuật tạo dự phòng ngoại vi
28. Lỗi tràn bộ đệm là lỗi trong khâu: Lập trình phần mềm
29. Đâu là dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng? Lỗi tràn bộ đệm
30. 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? Lớp an ninh hệ thống
31. 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: Địa chỉ trở về của hàm
32. Một trong các mối đe dọa an toàn thông tin thường gặp là: Phần mềm độc hại
33. Trong các vùng hạ tầng CNTT, vùng nào có nhiều mối đe dọa nguy cơ nhất? vùng người dùng
34. Trong các vùng hạ tầng CNTT, vùng nào có các lỗ hổng trong quản lý phần mềm ứng dụng của máy chủ? vùng hệ thống và ứng dụng
35. Trong các vùng hạ tầng CNTT, vùng nào dễ bị tấn công DoS, DDoS nhất? vùng mạng WAN
36. 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: Cân bằng giữa An toàn, Hữu dụng và Rẻ tiền
37. Các mối nguy cơ đe dọa thường trực là: Tin tặc và các phần mềm độc hại
38. Người sử dụng hệ thống thông tin điều hành trong mô hình 4 loại hệ thống thông tin là: Giám đốc điều hành
39. Các phần của hệ thống thông tin dựa trên máy tính là: Phần cứng (Hardware), phần mềm (Software), cơ sở dữ liệu (Databases), hệ thống mạng (Networks), tập các lệnh kết hợp (Procedures).
40. Công thức tính tỉ lệ tính sẵn dùng: A = (Uptime)/(Uptime + Downtime).
41. Các bước thực thi quản lí ATTT: Lập kế hoạch (Plan), Thực thi kế hoạch (Do), Giám sát kết quả thực hiện (Monitor), Thực hiện các kiểm soát (Control).
42. Chính sách an toàn thông tin không bao gồm: Chính sách an toàn ở mức người dùng (User security policy).
43. Tính toàn vẹn liên quan đến … và … của dữ liệu => tính hợp lệ (validity) … sự chính xác (accuracy).
44. Các lớp phòng vệ điển hình để đàm bảo ATTT và an toàn HTTT: Lớp an ninh cơ quan/tổ chức (Plant Security), Lớp an ninh mạng (Network Security), Lớp an ninh hệ thống (System Integrity).
45. Các đe dọa với tầng người dùng bao gồm: Coi nhẹ hoặc vi phạm các chính sách an ninh an toàn; đưa CD/DVD/USB với các files cá nhân vào hệ thống; thiếu ý thức về vấn đề an ninh an toàn.
46. Trong các vùng hạ tầng CNTT, vùng nào dễ bị tấn công kiểu vét cạn (brute force) nhất? vùng truy cập từ xa
47. Các đe dọa với vùng máy trạm bao gồm: Đưa CD/DVD/USB với các files cá nhân vào hệ thống; người dùng tải ảnh, âm nhạc, video; truy nhập trái phép vào máy trạm.
48. Người sử dụng Hệ thống xử lý giao dịch trong mô hình 4 loại hệ thống thông tin là: Nhân viên
49. Đâu là 1 lớp phòng vệ an ninh mạng: Tường lửa, mạng riêng ảo (VPN).
50. Các biện pháp được sử dụng để đảm bảo an toàn máy tính và dữ liệu là: Việc sao lưu tạo dự phòng dữ liệu, đảm bảo dữ liệu không bị mất mát khi xảy ra sự cố

# Chương 2

1. Đây là một trong các biện pháp phòng chống tấn công khai thác lỗi tràn bộ đệm? Sử dụng cơ chế cấm thực hiện mã trong dữ liệu
2. 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: Tăng khả năng mã tấn công được thực hiện
3. Tìm phát biểu đúng trong các phát biểu sau: Điểm yếu hệ thống có thể xuất hiện trong cả các mô đun phần cứng và phần mềm
4. Các vùng bộ nhớ thường bị tràn gồm: Ngăn xếp (Stack) và vùng nhớ cấp phát động (Heap)
5. Lỗ hổng an ninh trong một hệ thống là: Bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại
6. Nguyên nhân của sự tồn tại các điểm yếu trong hệ thống có thể do: Tất cả các khâu trong quá trình phát triển và vận hành
7. Trên thực tế, có thể giảm khả năng bị tấn công nếu có thể: Giảm thiểu các lỗ hổng bảo mật
8. Đâu là biện pháp được sử dụng để phòng chống lỗi không kiểm tra đầu vào: Kiểm tra tất cả các dữ liệu đầu vào, đặc biệt dữ liệu nhập từ người dùng và từ các nguồn không tin cậy.
9. Các lỗ hổng bảo mật thường tồn tại nhiều nhất trong thành phần nào của hệ thống: Các ứng dụng
10. Trong tấn công khai thác lỗi tràn bộ đệm, tin tặc thường sử dụng shellcode. Shellcode đó là dạng: Mã máy
11. Lỗ hổng bảo mật (Security vulnerability) là một điểm yếu tồn tại trong một hệ thống cho phép tin tặc: Lỗ hổng bảo mật (Security vulnerability) là một điểm yếu tồn tại trong một hệ thống cho phép tin tặc:
12. Lỗi tràn bộ đệm là lỗi trong khâu: Lập trình phần mềm
13. Đâu là dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng? Lỗi tràn bộ đệm
14. Loại tấn công nào sau đây chiếm quyền truy nhập đến tài nguyên lợi dụng cơ chế điều khiển truy nhập DAC? Trojan horse
15. Đâu là tên viết đúng của Hệ thống phát hiện đột nhập/xâm nhập? Intrusion Detection System
16. Mức độ nghiêm trọng chia Microsoft là: Nguy hiểm, Quan trọng, Trung bình, Thấp
17. Tác hại của lỗi tràn bộ đệm là: Có thể khiến cho ứng dụng ngừng hoạt động, gây mất dữ liệu hoặc thậm chí giúp kẻ tấn công kiểm soát hệ thống
18. Đâu không phải là một trong các biện pháp phòng chống lỗi không kiểm tra đầu vào: Không dùng user quản trị (root hoặc admin) để chạy các chương trình ứng dụng
19. Các dạng dữ liệu không cần kiểm tra là: Các dữ liệu được đưa ra bởi hệ thống
20. Kẻ tấn công có thể kiểm tra tất cả các … đầu vào và thử tất cả các … có thể khai thác được => Dữ liệu / Khả năng
21. Khi kiểm soát truy cập bị lỗi, một người dùng bình có thể … của người quản trị và có toàn quyền truy nhập vào hệ thống => đoạt quyền
22. Đâu không phải là phương pháp phòng chống lỗ hổng điều khiển truy cập: Sử dụng các công cụ phân tích mã tự động tìm các điểm có khả năng xảy ra lỗi
23. Đâu không phải là 1 vấn đề xảy với cơ chế xác thực: Chọn mật khẩu đủ mạnh để sử dụng
24. Đâu là một thao tác an toàn đối với file: Sử dụng mật khẩu và quyền phù hợp để truy cập
25. Đâu không phải là 1 biện pháp khắc phục và tăng cường khả năng để kháng cho hệ thống: Người dùng được quyền truy nhập vào mọi tác vụ của hệ thống
26. Một điều kiện đấu tranh tồn tại khi có sự thay đổi … của 2 hay một số sự kiện gây ra sự thay đổi … của hệ thống => Trật tự / Hành vi
27. Các loại điểm yếu của hệ thống là: Có điểm yếu đã biết và đã được khắc phục; Có điểm yếu đã biết và chưa được khắc phục; Có điểm yếu chưa biết/chưa được phát hiện
28. Một trong các dạng lỗ hổng thường gặp trong hệ điều hành và các phần mềm ứng dụng là: Buffer Overflows
29. Trong điểm yếu bảo mật do các điều kiện tranh đua, Kẻ tấn công có thể lợi dụng … giữa 2 sự kiện để …, đổi tên file hoặc can thiệp vào quá trình hoạt động bình thường của hệ thống => Khoảng thời gian / Chèn mã độc
30. Các lỗ hổng bảo mật trên hệ thống là do: Dịch vụ cung cấp; Bản thân hệ điều hành; Con người tạo ra

# Chương 3

1. Tìm phát biểu đúng trong các phát biểu sau: Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống.
2. Khác biệt cơ bản của vi rút và sâu là: Sâu có khả năng tự lây lan mà không cần tương tác của người dùng
3. Dạng tấn công gây ngắt quãng dịch vụ hoặc kênh truyền thông cho người dùng bình thường là: Interruptions
4. Tấn công nghe lén là kiểu tấn công: thụ động
5. Dạng tấn công chặn bắt thông tin truyền trên mạng để sửa đổi hoặc lạm dụng là: Modifications
6. Có thể phòng chống tấn công Smurf bằng cách cấu hình các máy và router không trả lời: Các yêu cầu ICMP hoặc các yêu cầu phát quảng bá
7. Đâu là một kỹ thuật tấn công Dos? Smurf
8. Dạng tấn công giả mạo thông tin thường để đánh lừa người dùng thông thường là: Fabrications
9. Kỹ thuật tấn công Smurf sử dụng giao thức ICMP và Cơ chế gửi: Broadcast
10. Pharming là kiểu tấn công vào: Máy khách/trình duyệt web
11. Đây là một công cụ kiểm tra lỗ hổng tấn công chèn mã SQL trên các website: SQLmap
12. Khác biệt cơ bản giữa tấn công DoS và DDoS là: Phạm vi tấn công
13. Các máy tính ma/máy tính bị chiếm quyền điều khiển thường được tin tặc sử dụng để: Gửi thư rác, thư quảng cáo
14. Trong dạng tấn công vào mật khẩu dựa trên từ điển, tin tặc đánh cắp mật khẩu của người dùng bằng cách: Thử các từ có tần suất sử dụng cao làm mật khẩu trong từ điển
15. Một trong các phương thức lây lan thường gặp của sâu mạng là: Lây lan thông qua khả năng thực thi từ xa
16. Đây là một kỹ thuật tấn công Dos? Ping of death
17. Tấn công từ chối dịch vụ (Dos - Denial of Service Attacks) là dạng tấn công có khả năng: Cản trở người dùng hợp pháp truy nhập các tài nguyên hệ thống
18. Mật khẩu an toàn trong thời điểm hiện tại là mật khẩu có: Độ dài từ 8 ký tự trở lên, gồm chữ cái hoa, thường, chữ số và ký tự đặc biệt
19. Nguy cơ cao nhất mà một cuộc tấn công chèn mã SQL có thể gây ra cho một hệ thống là: Chiếm quyền điều khiển hệ thống
20. Một trong các biện pháp có thể sử dụng để phòng chống tấn công kiểu người đứng giữa là:Sử dụng chứng chỉ số để xác thực thông tin nhận dạng các bên
21. Macro viruses là loại viruses thường lây nhiễm vào: Các file tài liệu của bộ phần mềm Microsoft Office
22. Tấn công kiểu Social Engineering là dạng tấn công khai thác yếu tố nào sau đây trong hệ thống? người dùng
23. Câu lệnh SQL nào tin tặc thường sử dụng trong tấn công: UNION SELECT
24. Phishing là một dạng của loại tấn công sử dụng: Kỹ thuật xã hội
25. Các dạng phần mềm độc hại (malware) có khả năng tự nhân bản gồm: Virus, worm, zombie
26. Một trong các cách virus thường sử dụng để lây nhiễm vào các chương trình khác là: Sửa đổi các chương trình
27. 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: Reflectors
28. Mục đích chính của tấn công giả mạo địa chỉ IP là: Để vượt qua các hàng rào kiểm soát an ninh
29. 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: DAC
30. Một trong các biện pháp hiệu quả để phòng chống Macro virus : Cấm tự động thực hiện macro trong Microsoft Office
31. Đâu là một biện pháp phòng chống SYN Floods: SYN Cache
32. Các zombie thường được tin tặc sử dụng để: Thực hiện tấn công DDoS
33. Tấn công kiểu Social Engineering có thể cho phép tin tặc: Đánh cắp thông tin nhạy cảm của người dùng
34. Tấn công bằng mã độc có thể gồm: SQLi, XSS, CSRF và Buffer overflow
35. Tại sao việc sử dụng thủ tục cơ sở dữ liệu (Stored procedure) là một trong các biện pháp hiệu quả để ngăn chặn triệt để tấn công chèn mã SQL ? Thủ tục cơ sở dữ liệu cho phép tách mã lệnh SQL khỏi dữ liệu người dùng
36. Dạng tấn công chèn mã được tin tặc sử dụng phổ biến trên các trang web nhắm đến các cơ sở dữ liệu là: Tấn công chèn mã SQL
37. Đâu là một trong các biện pháp phòng chống tấn công khai thác lỗi tràn bộ đệm? Sử dụng các thư viện lập trình an toàn //or sử dụng cơ chế cấm thực hiện mã trong dữ liệu (DEP)
38. Để thực hiện tấn công Smurf, tin tặc phải giả mạo địa chỉ gói tin ICMP trong yêu cầu tấn công. Tin tặc sử dụng: Địa chỉ máy nạn nhân làm địa chỉ nguồn của gói tin
39. Để thực hiện tấn công DDOS, tin tặc trước hết cần chiếm quyền điều khiển của một lượng lớn máy tính. Các máy tính bị chiếm quyền điều khiển thường được gọi là: Zombies
40. Điểm yếu là: Một lỗi hoặc một khiếm khuyết tồn tại trong hệ thống
41. Tìm phát biểu đúng: Lỗ hổng là bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại
42. Đâu không phải là mối quan hệ giữa mối đe dọa và lỗ hổng: Không thể triệt tiêu được hết các lỗ hỏng, nhưng có thể giảm thiểu các mối đe dọa, qua đó giảm thiểu khả năng bị tận dụng để tấn công
43. Dạng tấn công liên quan đến việc nghe trộm trên đường truyền và chuyển hướng thông tin để sử dụng trái phép là: Interceptions
44. Đâu không phải là 1 kiểu tấn công thụ động: Sửa đổi dữ liệu trong file
45. Đâu không phải là 1 dạng tấn công: Tràn bộ đệm
46. Đâu là một nguyên nhân dẫn đến bị tấn công bằng mã độc: Dữ liệu đầu vào từ người dùng hoặc từ các nguồn khác không được kiểm tra hoặc kiểm tra không kỹ lưỡng
47. Đâu không phải là một biện pháp phòng chống dựa trên thiết lập quyền truy nhập người dùng phù hợp: Người dùng được quyền truy nhập vào mọi tác vụ của hệ thống
48. Trong tấn công DoS, việc gửi một lượng lớn yêu cầu gây cạn kiệt tài nguyên hệ thống hoặc băng thông đường truyền là loại tấn công nào: Flooding attacks
49. SYN floods là kỹ thuật gây … các gói tin mở kết nối TCP => Ngập lụt
50. Đâu không phải là cách phòng chống SYN floods: Sử dụng mật khẩu mạnh
51. Điểm khác biệt của Reflective DDoS so với DDoS là gì: Một lượng lớn yêu cầu giả mạo với địa chỉ nguồn là địa chỉ máy nạn nhân đến một số lớn các máy khác được gửi đi
52. Đâu không phải là 1 các tấn công kiểu Social Engineering: Kẻ tấn công bắt buộc người dùng truy cập vào đường dẫn giả mạo
53. Tìm phương án sai, Tấn công bằng bomb thư có thể thực hiện bằng: Sử dụng phương pháp truyền tin TCP
54. Chọn phát biểu đúng về logic bomb: Thường được “nhúng” vào các chương trình bình thường và thường hẹn giờ để “phát nổ” trong một số điều kiện cụ thể
55. Trojan horse là chương trình chứa …, thường giả danh những chương trình …, nhằm lừa người dùng kích hoạt chúng => Mã độc / Có ích
56. Trojan horse thường được sử dụng để: Thực thi gián tiếp các tác vụ, mà tác giả của chúng không thể thực hiện trực tiếp do không có quyền truy nhập
57. Zombie là một chương trình được thiết kế để giành quyền … một máy tính có kết nối Internet, và sử dụng máy tính bị kiểm soát để … các hệ thống khác => Kiểm soát / Tấn công
58. Tìm phát biểu sai trong các phát biểu sau về vòng đời của virus: Giai đoạn phát tán: Virus kiểm soát những chương trình mà nó đã tiếp xúc
59. Đâu không phải một phương pháp lây lan của Worms: Cần sự đồng ý từ người dùng để lây lan từ máy này sang máy khá
60. 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? Trojan horse

# Chương 4

1. PGP đảm bảo tính bí mật thông điệp bằng cách sử dụng: Mã hóa khóa bất đối xứng sử dụng khóa công khai
2. Số lượng thao tác trong mỗi vòng xử lý của hàm băm MD5 là: 16
3. Trong các cặp khoá sau đây của hệ mật RSA với p=5; q=7, cặp khóa nào có khả năng đúng nhất: ( e = 7, d =23)
4. Thuật giải SHA-1 dùng để: Tạo một giá trị băm có độ dài cố định 160 bit
5. Một hệ mã hóa (cryptosystem) được cấu thành từ hai thành phần chính gồm: Phương pháp mã hóa và không gian khóa
6. Đây là một phương pháp mã hóa: XOR
7. Kích thước khối dữ liệu xử lý của giải thuật mã hóa AES là: 128 bit
8. Điểm khác nhau chính giữa hai loại hàm băm MDC và MAC là: MDC là loại hàm băm không khóa, còn MAC là loại hàm băm có khóa
9. Một trong các điểm yếu của các hệ mã hóa khóa công khai là: Tốc độ chậm
10. Hai thuộc tính cơ bản quan trọng nhất của một hàm băm là: Nén và dễ tính toán
11. Độ an toàn của hệ mật mã RSA dựa trên...: Tính khó của việc phân tích số nguyên rất lớn
12. Khi sinh cặp khóa RSA, các số nguyên tố p và q nên được chọn với kích thước…: Bằng khoảng một nửa kích thước của modulo n
13. Tìm phát biểu đúng về mã hóa khóa bất đối xứng (Asymmetric key cryptography): Sử dụng một khóa quá trình mã hóa và một khóa khác cho giải mã
14. Tìm phát biểu đúng về mã hóa khóa đối xứng (Symmetric key cryptography): Sử dụng một khóa chung cho cả quá trình mã hóa và giải mã
15. Số lượng vòng lặp chính thực hiện xáo trộn dữ liệu theo hàm Feistel (F) trong giải thuật DES là: 16
16. Các hộp thay thế s-box trong giải thuật DES có số bít đầu vào và đầu ra tương ứng là: Vào 6 bít và ra 4 bít
17. Một trong các ứng dụng phổ biến của các hàm băm là để tạo chuỗi...: Checksum
18. Trong quá trình xử lý thông điệp đầu vào tạo chuỗi băm, số lượng vòng xử lý của hàm băm SHA1 là: 80
19. Giải thuật mã hóa AES được thiết kế dựa trên…: mạng hoán vị-thay thế
20. Một trong các điểm yếu của các hệ mã hóa khóa đối xứng là: Khó khăn trong quản lý và phân phối khóa
21. 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: 12
22. Một trong các ứng dụng phổ biến của các hàm băm một chiều là để...: Mã hóa mật khẩu
23. PGP đảm bảo tính xác thực thông điệp bằng cách: Sử dụng hàm băm có khóa MAC
24. Kích thước khóa hiệu dụng của hệ mã hóa DES là: 56 bít
25. Trong mã hóa dòng (stream cipher), dữ liệu được xử lý theo…: Từng bít hoặc từng byte/ký tự
26. Trong hệ mật mã RSA, quan hệ toán học giữa khóa công khai e và số Phi(n) là: e và Phi(n) là 2 số nguyên tố cùng nhau
27. Các giải thuật mã hóa khóa đối xứng thông dụng gồm: DES, 3-DES, AES
28. Trong hệ mật mã RSA, quan hệ toán học giữa khóa riêng d và khóa công khai e là: d là modulo nghịch đảo của e
29. Giải thuật mã hóa AES vận hành dựa trên một ma trận 4x4, được gọi là...: State
30. Đâu là một ứng dụng của mã hóa: PGP
31. Phần xử lý chính của SHA1 làm việc trên một chuỗi được gọi là state. Kích thước của state là: 160 bít
32. Trật tự các khâu xử lý trong các vòng lặp chính của giải thuật mã hóa AES là: SubBytes, ShiftRows, MixColumns, AddRoundKey
33. Văn bản sau khi được mã hóa gọi là gì: Văn bản mã.
34. Đặc tính nào sau đây không thuộc chức năng bảo mật thông tin trong các hệ thống mật mã: Hiệu quả.
35. Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng cùng một khóa mã khi mã hóa công khai và giải mã: RS
36. Chuẩn nào sau đây được chính phủ Mỹ sử dụng thay thế cho DES như là một chuẩn mã hóa dữ liệu: AES
37. Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng các khóa khác nhau khi mã hóa và giải mã: Không đối xứng
38. Khi giá trị hàm băm của hai thông điệp khác nhau có giá trị tương tự nhau, ta gọi hiện tượng này là gì: Xung đột
39. Nếu muốn xem một tài liệu “bảo mật”được mã hóa trên hệ mật bất đối xứng do người khác gửi đến , bạn phải sử dụng khóa nào để giải mật tài liệu: Khoá cá nhân của bạn
40. Đâu là một phương pháp mã hóa: Thay thế; Đổi chỗ/ hoán vị; Vernam; (Tất cả các phương án trên)
41. Thuật giải MD5 cho ta một giá trị băm có độ dài: 128 bit
42. Các hệ mã hóa khóa công khai sử dụng một cặp khóa: public key và private key. Các yêu cầu đối với public key và private key là: Có thể công khai public key nhưng phải đảm bảo tính xác thực và cần giữ bí mật private key
43. Kích thước khóa có thể của hệ mã hóa AES là: 128, 160 và 192 bit
44. Kích thước khóa hiệu dụng của hệ mã hóa DES là: 56 bit
45. Số lượng vòng lặp chuyển đổi cần thực hiện để chuyển bản rõ thành bản mã trong hệ mã hóa AES khóa 128 bit là: 10
46. Bước MixColumns (trộn cột) trong vòng lặp chuyển đổi trong hệ mã hóa AES thực hiện việc: Mỗi cột của ma trận state được nhân với một đa thức
47. Phát biểu nào sau đây đúng với kỹ thuật mã hóa khóa bí mật: Mã hóa khóa bí mật sử dụng một mã (key) cho cả quá trình mã hóa và giải mã: Ưu điểm của kỹ thuật mã hóa khóa công khai so với mã hóa khóa bí mật là: Trao đổi khóa dễ dàng hơn
48. Yêu cầu để đảm bảo sử dụng mã hóa đối xứng là: Có thuật toán encryption tốt,có một khóa bí mật được biết bởi người nhận/gửi và kênh truyền bí mật để phân phát key
49. Mã hóa nào sau đây là một tiêu chuẩn dùng để phát triển cho việc tạo ra thông điệp an toàn: Data Encryption Standard
50. Các yếu tố ảnh hưởng đến quá trình mã hóa: Thuật toán mã hóa, giải mã, và tính an toàn của kênh truyền
51. Nội dung nào sau đây không cần sử dụng mật mã: Toàn vẹn
52. Thuật giải MD5 dùng để: Kiểm tra tính toàn vẹn dữ liệu
53. Trong DES mỗi hàm chọn Si được dùng để: Biến đổi khối dữ liệu mã 6 bit thành 4 bit
54. Hệ mật DES sử dụng khối khóa được tạo bởi: 56 bit ngẫu nhiên và 8 bit kiểm tra “Parity”
55. Hệ mật DES xử lý từng khối “plain text” có độ dài: 64 bit
56. Số lượng các khóa phụ (subkey) cần được tạo ra từ khóa chính trong giải thuật DES là: 16
57. MAC là một từ cấu tạo bằng những chữ đầu của một nhóm nào liên quan đến mật mã: Mã xác thực thông điệp (Message authentication code)
58. Sử dụng bao nhiêu bit với DES để có hiệu quả? 64
59. Thuật giải SHA là: Hàm băm một chiều; Dùng trong thuật giải tạo chữ ký số; Cho giá trị băm 160 bit (Tất cả đều đúng)
60. Các loại khoá mật mã nào sau đây dễ bị crack nhất: 40 bit

# Chương 5

1. Nguyên tắc bảo mật tài nguyên của mô hình Bell-La Padula là: Đọc xuống và ghi lên
2. Tính bảo mật của kỹ thuật điều khiển truy nhập sử dụng mật khẩu dựa trên: Độ khó đoán và tuổi thọ của mật khẩu
3. 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
4. Một trong các điểm yếu làm giảm hiệu quả của phát hiện tấn công, xâm nhập dựa trên bất thường là: Tỷ lệ cảnh báo sai cao
5. 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
6. Ưu điểm của điều khiển truy nhập dựa trên các đặc điểm sinh trắc học là: Bảo mật cao và luôn đi cùng với chủ thể
7. Một ưu điểm của tường lửa có trạng thái so với tường lửa không trạng thái là: 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: Thống kê, học máy, khai phá dữ liệu
9. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập dựa trên vai trò - RBAC: RBAC cấp quyền truy nhập dựa trên vai trò của người dùng trong tổ chức
10. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập DAC: DAC cho phép người tạo ra đối tượng có thể cấp quyền truy nhập cho người dùng khác
11. Đâu là một công cụ có khả năng rà quét các lỗ hổng chèn mã SQL cho các trang web: 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: Mỗi đối tượng được gán một danh sách người dùng kèm theo quyền truy nhập
13. Tường lửa không thể chống lại...: Các hiểm họa từ bên trong
14. Sự khác biệt chính giữa hệ thống ngăn chặn xâm nhập (IPS) và hệ thống phát hiện xâm nhập (IDS) là: IPS có khả năng chủ động ngăn chặn xâm nhập
15. Tường lửa lọc gói có thể lọc các thông tin nào trong gói tin: Chỉ các thông tin trong header 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: Các phần mềm quét virus xung đột với nhau
17. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập bắt buộc MAC: MAC cấp quyền truy nhập dựa trên tính nhạy cảm của thông tin và chính sách quản trị
18. Đâu là một loại tường lửa: Application-level gateway
19. Ví điện tử Paypal là một dạng...: Thẻ bài (token)
20. Dạng xác thực sử dụng các thông tin nào dưới đây đảm bảo độ an toàn cao hơn: Thẻ ATM và số PIN
21. Một trong các dạng khóa mã (encrypted keys) được sử dụng rộng rãi trong điều khiển truy nhập là: Chứng chỉ số khóa công khai
22. Tại sao một hệ thống phát hiện xâm nhập dựa trên chữ ký không thể phát hiện các tấn công, xâm nhập mới? Do chữ ký của chúng chưa tồn tại trong hệ thống
23. Ưu điểm của thẻ bài (token) so với thẻ thông minh (smart card) trong điều khiển truy nhập là: Có cơ chế xác thực mạnh hơn
24. Phương pháp xác thực nào dưới đây có thể cung cấp khả năng xác thực có độ an toàn cao nhất: Sử dụng vân tay
25. Đâu là các tính năng của kiểm soát truy nhập sử dụng tường lửa: Kiểm soát dịch vụ và hướng
26. Ba cơ chế điều khiển truy nhập thông dụng gồm: 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: 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: 2
29. Một nhiệm vụ chính của các hệ thống IDS/IPS là: Giám sát lưu lượng mạng hoặc 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: Authentication và Authorization
31. Tìm phát biểu đúng về phát hiện xâm nhập dựa trên chữ ký và phát hiện xâm nhập dựa trên bất thường: Phát hiện xâm nhập dựa trên chữ ký thường có tỷ lệ phát hiện đúng cao hơn
32. Tìm phát biểu đúng về dịch vụ xác thực trong điều khiển truy nhập: Là quá trình xác minh tính chân thực của thông tin nhận dạng người dùng cung cấp
33. Một trong các nhược điểm chính của điều khiển truy nhập dựa trên các đặc điểm sinh trắc học là: Chi phí đắt
34. Ưu điểm của mật khẩu một lần (OTP-One Time Password) so với mật khẩu truyền thống là: Chống được tấn công phát lại
35. Kỹ thuật tấn công SYN Floods khai thác điểm yếu trong khâu nào trong bộ giao thức TCP/IP: Bắt tay 3 bước
36. Một điểm yếu điển hình trong hệ thống điều khiển truy cập là việc sử dụng mật khẩu dễ đoán hoặc mật khẩu được lưu ở dạng rõ. Đây là điểm yếu thuộc khâu: Xác thực
37. Để đảm bảo an toàn cho hệ thống điều khiển truy cập, một trong các biện pháp phòng chống hiệu quả là: Không dùng tài khoản có quyền quản trị để chạy các chương trình ứng dụng
38. Điều khiển truy nhập dựa trên luật (Rule-based access control) được sử dụng phổ biến trong: Firewall
39. Một hệ thống điều khiển truy nhập có thể được cấu thành từ các dịch vụ nào sau đây: Xác thực, trao quyền và quản trị
40. Sau khi một user đã được định danh (identifed), điều gì cần phải làm trước khi họ log vào một mạng máy tính: Xác thực với mật khẩu
41. Phát biểu nào sau đây đúng với cơ chế điều khiển truy cập DAC: DAC cho phép người tạo ra đối tượng có thể cấp quyền quy cập cho người dùng khác
42. Các hệ điều hành Microsoft Windows và Linux sử dụng các mô hình điều khiển truy cập nào dưới đây: DAC và Role-BAC
43. Phát biểu nào sau đây đúng với cơ chế điều khiển truy cập RBAC: RBAC cấp quyền truy cập dựa trên vai trò của người dùng trong tổ chức
44. Cho biết câu nào đúng trong các câu sau: Tất cả Firewall đều có chung thuộc tính là cho phép phân biệt hay đối xử khả năng từ chối hay truy nhập dựa vào địa chỉ nguồn; Chức năng chính của Firewall là kiểm soát luồng thông tin giữa mạng cần bảo vệ và Internet thông qua các chính sách truy nhập đã được thiết lập; Hệ thống Firewall thường bao gồm cả phần cứng lẫn phần mềm (Tất cả đều đúng)
45. Đối với Firewall lọc gói, hình thức tấn công nào sau đây được thực hiện: Nhái địa chỉ IP, tấn công giữa, tấn công biên
46. Những chữ đầu của nhóm từ ACL là tên viết tắt của: Access Control List
47. Nên cài mức truy cập mặc định là mức nào sau đây: No access
48. 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: Phải được ủy quyền
49. Bộ lọc địa chỉ MAC được định nghĩa như: Ngăn chặn truy cập từ một địa chỉ MAC nhất định.
50. Các mức độ nhạy cảm của thông tin được chia từ cao xuống thấp đối với an ninh quốc gia là: Tối mật (Top Secret - T), Tuyệt mật (Secret - S), Mật (Confidential - C), Không phân loại (Unclassified - U).
51. Đặc tính nào của các thiết bị mạng như router hay switch, cho phép điều khiển truy cập dữ liệu trên mạng: Danh sách điều khiển truy cập (ACL).
52. Yếu tố nào cần được sử dụng kết hợp với một thẻ thông minh để xác thực: Quét võng mạc
53. Phương pháp quét võng mạc thích hợp nhất đối với các dịch vụ nào sau đây: Kiểm soát truy cập
54. Yếu tố nào sau đây được coi là hữu ích nhất trong việc kiểm soát truy cập khi bị tấn công từ bên ngoài: Đăng nhập hệ thống ( System logs)
55. Điểm khác nhau chính giữa các hệ thống ngăn chặn đột nhập (IPS) và phát hiện đột nhập (IDS) là: IPS có khả năng chủ động ngăn chặn tấn công so với IDS
56. Để đánh giá điểm mạnh của hệ thống IDS người ta dựa vào các yếu tố sau: Khởi sự, giám sát vị trí, những đặc trưng ghép nối hoặc tích hợp
57. Khi thực hiện triển khai HIDS khó khăn gặp là: Giới hạn tầm nhìn mạng, phải xử lí với nhiều hệ điều hành khác trên mạng.
58. Bộ lọc gói thực hiện chức năng nào: Ngăn chặn các gói trái phép đi vào từ mạng bên ngoài
59. Hệ thống nào được cài đặt trên Host để cung cấp một tính năng IDS: H-IDS (Host-based IDS)
60. Tổ chức chính cấp phát chứng chỉ được gọi là: CA
61. Các phát biểu sau đây phát biểu là là đúng nhất: Firewall là một vành đai phòng thủ cho máy tính hoặc hệ thống trước những tấn công
62. Phát hiện tấn công, xâm nhập dựa trên bất thường dựa trên giả thiết: Các hành vi tấn công, xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường
63. Các hệ thống phát hiện xâm nhập có thể thu thập dữ liệu đầu vào từ: Mạng và các host
64. Yếu tố nào cần được sử dụng kết hợp với một thẻ thông minh để xác thực: PIN
65. Qui trình xác thực nào sử dụng nhiều hơn một yếu tố xác thực để login: Đa yếu tố ( multi-factor)

**Cơ sở An toàn Thông tin 3.1**

1. Mô hình tổng quát đảm bảo an toàn thông tin và hệ thống thông tin thường gồm các lớp: An ninh tổ chức, An ninh mạng và An ninh hệ thống
2. An toàn thông tin gồm hai lĩnh vực chính là: An toàn công nghệ thông tin và Đảm bảo thông tin
3. Tại sao cần phải đảm bảo an toàn cho thông tin? Do có nhiều thiết bị kết nối mạng Internet với nhiều nguy cơ và đe dọa
4. . An toàn hệ thống thông tin là: 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: Quản lý bộ phận
6. . Nguyên tắc cơ bản cho đảm bảo an toàn thông tin, hệ thống và mạng là: Phòng vệ nhiều lớp có chiều sâu
7. Một trong các nội dung rất quan trọng của quản lý an toàn thông tin là: 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? Bí mật và 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? Vùng mạng WAN
10. An toàn thông tin (Information Security) là gì? Là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép
11. Một trong các biện pháp cụ thể cho quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống là: Định kỳ cập nhật thông tin về các lỗ hổng từ các trang web chính thức
12. Các mật khẩu nào sau đây là khó phá nhất đối với một hacker? !$aLtNb83
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:Tăng khả năng mã tấn công được thực hiện
14. Tìm phát biểu đúng trong các phát biểu sau: Điểm yếu hệ thống có thể xuất hiện trong cả các mô đun phần cứng và phần mềm
15. Người sử dụng hệ thống trợ giúp ra quyết định trong mô hình 4 loại hệ thống thông tin là: Quản lý cao cấp
16. Các thành phần chính của hệ thống máy tính gồm: Hệ thống phần cứng và Hệ thống phần mềm
17. Nguyên nhân của sự tồn tại các điểm yếu trong hệ thống có thể do: Tất cả các khâu trong quá trình phát triển và vận hành
18. Trên thực tế, có thể giảm khả năng bị tấn công nếu có thể: Giảm thiểu các lỗ hổng bảo mật
19. Sâu SQL Slammer tấn công khai thác lỗi tràn bộ đệm trong hệ quản trị cơ sở dữ liệu: SQL Server 2000
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? Năm lần nỗ lực login thất bại trên tài khoản “jsmith”
21. Các kỹ thuật và công cụ thường được sử dụng trong an ninh mạng bao gồm: Điều khiển truy nhập, tường lửa, proxy và các giao thức bảo mật, ứng dụng dựa trên mật mã
22. Các thành phần của an toàn thông tin gồm: An toàn máy tính và dữ liệu, An ninh mạng, Quản lý ATTT và Chính sách ATTT
23. Các yêu cầu cơ bản trong đảm bảo an toàn thông tin và an toàn hệ thống thông tin gồm: Bí mật, Toàn vẹn và Sẵn dùng
24. Việc thực thi quản lý ATTT cần được thực hiện theo chu trình lặp lại là do: Các điều kiện bên trong và bên ngoài hệ thống thay đổi theo thời gian
25. Hệ thống thông tin là: 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
26. Tính bí mật của thông tin có thể được đảm bảo bằng: Bảo vệ vật lý, VPN, hoặc mã hóa
27. Đảm bảo thông tin (Information assurance) thường được thực hiện bằng cách: Sử dụng kỹ thuật tạo dự phòng ngoại vi
28. Lỗi tràn bộ đệm là lỗi trong khâu: Lập trình phần mềm
29. Đâu là dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng? Lỗi tràn bộ đệm
30. 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? Lớp an ninh hệ thống
31. 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: Địa chỉ trở về của hàm
32. Một trong các mối đe dọa an toàn thông tin thường gặp là: Phần mềm độc hại
33. Trong các vùng hạ tầng CNTT, vùng nào có nhiều mối đe dọa nguy cơ nhất?vùng người dùng
34. Trong các vùng hạ tầng CNTT, vùng nào có các lỗ hổng trong quản lý phần mềm ứng dụng của máy chủ? vùng hệ thống và ứng dụng
35. Trong các vùng hạ tầng CNTT, vùng nào dễ bị tấn công DoS, DDoS nhất? vùng mạng WAN
36. 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: Cân bằng giữa An toàn, Hữu dụng và Rẻ tiền
37. Các mối nguy cơ đe dọa thường trực là: Tin tặc và các phần mềm độc hại
38. Người sử dụng hệ thống thông tin điều hành trong mô hình 4 loại hệ thống thông tin là: Giám đốc điều hành
39. Các phần của hệ thống thông tin dựa trên máy tính là: Phần cứng (Hardware), phần mềm (Software), cơ sở dữ liệu (Databases), hệ thống mạng (Networks), tập các lệnh kết hợp (Procedures).
40. Công thức tính tỷ lệ tính sẵn dùng: A = (Uptime)/(Uptime + Downtime).
41. Các bước thực thi quản lý ATTT: Lập kế hoạch (Plan), Thực thi kế hoạch (Do), Giám sát kết quả thực hiện (Monitor), Thực hiện các kiểm soát (Control).
42. Chính sách an toàn thông tin không bao gồm: Chính sách an toàn ở mức người dùng (User security policy).
43. Tính toàn vẹn liên quan đến … và … của dữ liệu. => tính hợp lệ (validity) … sự chính xác (accuracy).
44. Các lớp phòng vệ điển hình để đàm bảo ATTT và an toàn HTTT: Lớp an ninh cơ quan/tổ chức (Plant Security), Lớp an ninh mạng (Network Security), Lớp an ninh hệ thống (System Integrity).
45. Các đe dọa với tầng người dùng bao gồm: Coi nhẹ hoặc vi phạm các chính sách an ninh an toàn; đưa CD/DVD/USB với các files cá nhân vào hệ thống; thiếu ý thức về vấn đề an ninh an toàn
46. Trong các vùng hạ tầng CNTT, vùng nào dễ bị tấn công kiểu vét cạn (brute force) nhất? vùng truy cập từ xa
47. Các đe dọa với vùng máy trạm bao gồm: Đưa CD/DVD/USB với các files cá nhân vào hệ thống; người dùng tải ảnh, âm nhạc, video; truy nhập trái phép vào máy trạm.
48. Người sử dụng Hệ thống xử lý giao dịch trong mô hình 4 loại hệ thống thông tin là: Nhân viên
49. Đâu là 1 lớp phòng vệ an ninh mạng: Tường lửa, mạng riêng ảo (VPN).
50. Đây là một trong các biện pháp phòng chống tấn công khai thác lỗi tràn bộ đệm? Sử dụng cơ chế cấm thực hiện mã trong dữ liệu
51. 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: Tăng khả năng mã tấn công được thực hiện
52. Tìm phát biểu đúng trong các phát biểu sau: Điểm yếu hệ thống có thể xuất hiện trong cả các mô đun phần cứng và phần mềm
53. Các vùng bộ nhớ thường bị tràn gồm: Ngăn xếp (Stack) và vùng nhớ cấp phát động (Heap)
54. Lỗ hổng an ninh trong một hệ thống là: Bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại
55. Nguyên nhân của sự tồn tại các điểm yếu trong hệ thống có thể do: Tất cả các khâu trong quá trình phát triển và vận hành
56. Trên thực tế, có thể giảm khả năng bị tấn công nếu có thể...Giảm thiểu các lỗ hổng bảo mật
57. Sâu SQL Slammer tấn công khai thác lỗi tràn bộ đệm trong hệ quản trị cơ sở dữ liệu:SQL Server 2000
58. các lỗ hổng bảo mật thường tồn tại nhiều nhất trong thành phần nào của hệ thống: Các ứng dụng
59. Trong tấn công khai thác lỗi tràn bộ đệm, tin tặc thường sử dụng shellcode. Shellcode đó là dạng: Mã máy
60. Lỗ hổng bảo mật (Security vulnerability) là một điểm yếu tồn tại trong một hệ thống cho phép tin tặc: Khai thác gây tổn hại đến các thuộc tính an ninh của hệ thống đó
61. Lỗi tràn bộ đệm là lỗi trong khâu: Lập trình phần mềm
62. Đâu là dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng? Lỗi tràn bộ đệm
63. Loại tấn công nào sau đây chiếm quyền truy nhập đến tài nguyên lợi dụng cơ chế điều khiển truy nhập DAC? Trojan horse
64. Đâu là tên viết đúng của Hệ thống phát hiện đột nhập/xâm nhập? intrusion Detection System
65. Mức độ nghiêm trọng chia Microsoft là: Nguy hiểm, Quan trọng, Trung bình, Thấp
66. Tác hại của lỗi tràn bộ đệm là: Có thể khiến cho ứng dụng ngừng hoạt động, gây mất dữ liệu hoặc thậm chí giúp kẻ tấn công kiểm soát hệ thống
67. Đâu không phải là một trong các biện pháp phòng chống lỗi không kiểm tra đầu vào: Không dùng user quản trị (root hoặc admin) để chạy các chương trình ứng dụng
68. Các dạng dữ liệu cần kiểm tra là: Các dữ liệu được đưa ra bởi hệ thống
69. Kẻ tấn công có thể kiểm tra tất cả các … đầu vào và thử tất cả các … có thể khai thác được => Dữ liệu / Khả năng
70. Khi kiểm soát truy cập bị lỗi, một người dùng bình có thể … của người quản trị và có toàn quyền truy nhập vào hệ thống => Đoạt quyền
71. Đâu không phải là phương pháp phòng chống lỗ hổng điều khiển truy cập: Sử dụng các công cụ phân tích mã tự động tìm các điểm có khả năng xảy ra lỗi
72. Đâu không phải là 1 vấn đề xảy với cơ chế xác thực: Chọn mật khẩu đủ mạnh để sử dụng
73. Đâu là một thao tác an toàn đối với file Sử dụng mật khẩu và quyền phù hợp để truy cập
74. Đâu không phải là 1 biện pháp khắc phục và tăng cường khả năng đề kháng cho hệ thống Người dùng được quyền truy nhập vào mọi tác vụ của hệ thống
75. Một điều kiện đấu tranh tồn tại khi có sự thay đổi … của 2 hay một số sự kiện gây ra sự thay đổi … của hệ thống => Trật tự / Hành vi
76. Các loại điểm yếu của hệ thống là Có điểm yếu đã biết và đã được khắc phục;Có điểm yếu đã biết và chưa được khắc phục; Có điểm yếu chưa biết/chưa được phát hiện
77. Một trong các dạng lỗ hổng thường gặp trong hệ điều hành và các phần mềm ứng dụng là Buffer Overflows
78. Trong điểm yếu bảo mật do các điều kiện tranh đua, Kẻ tấn công có thể lợi dụng … giữa 2 sự kiện để …, đổi tên file hoặc can thiệp vào quá trình hoạt động bình thường của hệ thống => Khoảng thời gian / Chèn mã độc
79. Các lỗ hổng bảo mật trên hệ thống là do: Dịch vụ cung cấp Bản thân hệ điều hành Con người tạo ra
80. Tìm phát biểu đúng trong các phát biểu sau: Tìm phát biểu đúng trong các phát biểu sau:
81. Khác biệt cơ bản của vi rút và sâu là: Sâu có khả năng tự lây lan mà không cần tương tác của người dùng
82. Dạng tấn công gây ngắt quãng dịch vụ hoặc kênh truyền thông cho người dùng bình thường là: Interruptions
83. Tấn công nghe lén là kiểu tấn công: Thụ động
84. Dạng tấn công chặn bắt thông tin truyền trên mạng để sửa đổi hoặc lạm dụng là: Modifications
85. Có thể phòng chống tấn công Smurf bằng cách cấu hình các máy và router không trả lời: Các yêu cầu ICMP hoặc các yêu cầu phát quảng bá
86. Đâu là một kỹ thuật tấn công Dos? Smurf
87. Dạng tấn công giả mạo thông tin thường để đánh lừa người dùng thông thường là: Fabrications
88. Kỹ thuật tấn công Smurf sử dụng giao thức ICMP và Cơ chế gửi: Broadcast
89. Pharming là kiểu tấn công vào: Máy khách/trình duyệt web
90. Đây là một công cụ kiểm tra lỗ hổng tấn công chèn mã SQL trên các website: SQLmap
91. Khác biệt cơ bản giữa tấn công DoS và DDoS là: Phạm vi tấn công
92. Các máy tính ma/máy tính bị chiếm quyền điều khiển thường được tin tặc sử dụng để: Gửi thư rác, thư quảng cáo
93. Trong dạng tấn công vào mật khẩu dựa trên từ điển, tin tặc đánh cắp mật khẩu của người dùng bằng cách: Thử các từ có tần suất sử dụng cao làm mật khẩu trong từ điển
94. Một trong các phương thức lây lan thường gặp của sâu mạng là: Lây lan thông qua khả năng thực thi từ xa
95. Đây là một kỹ thuật tấn công Dos? Ping of death
96. Tấn công từ chối dịch vụ (Dos - Denial of Service Attacks) là dạng tấn công có khả năng: Cản trở người dùng hợp pháp truy nhập các tài nguyên hệ thống
97. Mật khẩu an toàn trong thời điểm hiện tại là mật khẩu có: Độ dài từ 8 ký tự trở lên, gồm chữ cái hoa, thường, chữ số và ký tự đặc biệt
98. Nguy cơ cao nhất mà một cuộc tấn công chèn mã SQL có thể gây ra cho một hệ thống là: Chiếm quyền điều khiển hệ thống
99. Một trong các biện pháp có thể sử dụng để phòng chống tấn công kiểu người đứng giữa là:Sử dụng chứng chỉ số để xác thực thông tin nhận dạng các bên
100. Macro viruses là loại viruses thường lây nhiễm vào: Các file tài liệu của bộ phần mềm Microsoft Office
101. Tấn công kiểu Social Engineering là dạng tấn công khai thác yếu tố nào sau đây trong hệ thống? Người dùng
102. 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? UNION SELECT
103. Phishing là một dạng của loại tấn công sử dụng: Kỹ thuật xã hội
104. Các dạng phần mềm độc hại (malware) có khả năng tự nhân bản gồm: Virus, worm, zombie
105. Một trong các cách virus thường sử dụng để lây nhiễm vào các chương trình khác là: Sửa đổi các chương trình
106. 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: Reflectors
107. Mục đích chính của tấn công giả mạo địa chỉ IP là: Để vượt qua các hàng rào kiểm soát an ninh
108. 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: DAC
109. Một trong các biện pháp hiệu quả để phòng chống Macro virus : Cấm tự động thực hiện macro trong Microsoft Office
110. Đâu là một biện pháp phòng chống SYN Floods: SYN Cache
111. Các zombie thường được tin tặc sử dụng để: Thực hiện tấn công DDoS
112. Tấn công kiểu Social Engineering có thể cho phép tin tặc: Đánh cắp thông tin nhạy cảm của người dùng
113. Tấn công bằng mã độc có thể gồm: SQLi, XSS, CSRF và Buffer overflow
114. Tại sao việc sử dụng thủ tục cơ sở dữ liệu (Stored procedure) là một trong các biện pháp hiệu quả để ngăn chặn triệt để tấn công chèn mã SQL? Thủ tục cơ sở dữ liệu cho phép tách mã lệnh SQL khỏi dữ liệu người dùng
115. Dạng tấn công chèn mã được tin tặc sử dụng phổ biến trên các trang web nhắm đến các cơ sở dữ liệu là: Tấn công chèn mã SQL
116. Đâu là một trong các biện pháp phòng chống tấn công khai thác lỗi tràn bộ đệm? Sử dụng các thư viện lập trình an toàn //or sử dụng cơ chế cấm thực hiện mã trong dữ liệu (DEP)
117. Để thực hiện tấn công Smurf, tin tặc phải giả mạo địa chỉ gói tin ICMP trong yêu cầu tấn công. Tin tặc sử dụng: Địa chỉ máy nạn nhân làm địa chỉ nguồn của gói tin
118. Để thực hiện tấn công DDOS, tin tặc trước hết cần chiếm quyền điều khiển của một lượng lớn máy tính. Các máy tính bị chiếm quyền điều khiển thường được gọi là: Zombies
119. Điểm yếu là: Một lỗi hoặc một khiếm khuyết tồn tại trong hệ thống
120. Tìm phát biểu đúng: Lỗ hổng là bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại
121. Đâu không phải là mối quan hệ giữa mối đe dọa và lỗ hổng: Không thể triệt tiêu được hết các lỗ hỏng, nhưng có thể giảm thiểu các mối đe dọa, qua đó giảm thiểu khả năng bị tận dụng để tấn công
122. Dạng tấn công liên quan đến việc nghe trộm trên đường truyền và chuyển hướng thông tin để sử dụng trái phép là: Interceptions
123. Đâu không phải là 1 kiểu tấn công thụ động: Sửa đổi dữ liệu trong file
124. Đâu không phải là 1 dạng tấn công: Tràn bộ đệm
125. Đâu là một nguyên nhân dẫn đến bị tấn công bằng mã độc: Dữ liệu đầu vào từ người dùng hoặc từ các nguồn khác không được kiểm tra hoặc kiểm tra không kỹ lưỡng
126. Đâu không phải là một biện pháp phòng chống dựa trên thiết lập quyền truy nhập người dùng phù hợp: Người dùng được quyền truy nhập vào mọi tác vụ của hệ thống
127. Trong tấn công DoS, việc gửi một lượng lớn yêu cầu gây cạn kiệt tài nguyên hệ thống hoặc băng thông đường truyền là loại tấn công nào: Flooding attacks
128. SYN floods là kỹ thuật gây: các gói tin mở kết nối TCP Ngập lụt
129. Đâu không phải là cách phòng chống SYN floods: Sử dụng mật khẩu mạnh
130. Điểm khác biệt của Reflective DDoS so với DDoS là gì: Một lượng lớn yêu cầu giả mạo với địa chỉ nguồn là địa chỉ máy nạn nhân đến một số lớn các máy khác được gửi đi
131. Đâu không phải là 1 các tấn công kiểu Social Engineering: Kẻ tấn công bắt buộc người dùng truy cập vào đường dẫn giả mạo
132. Tìm phương án sai: Tấn công bằng bomb thư có thể thực hiện bằng Sử dụng phương pháp truyền tin TCP
133. Chọn phát biểu đúng về logic bomb: Thường được “nhúng” vào các chương trình bình thường và thường hẹn giờ để “phát nổ” trong một số điều kiện cụ thể
134. Trojan horse là chương trình chứa …, thường giả danh những chương trình …, nhằm lừa người dùng kích hoạt chúng => Mã độc / Có ích
135. Trojan horse thường được sử dụng để: Thực thi gián tiếp các tác vụ, mà tác giả của chúng không thể thực hiện trực tiếp do không có quyền truy nhập
136. Zombie là một chương trình được thiết kế để giành quyền … một máy tính có kết nối Internet, và sử dụng máy tính bị kiểm soát để … các hệ thống khác => Kiểm soát / Tấn công
137. Tìm phát biểu sai trong các phát biểu sau về vòng đời của virus: Giai đoạn phát tán: Virus kiểm soát những chương trình mà nó đã tiếp xúc

**Cơ sở An toàn Thông tin 3.2**

1. Đâu không phải một phương pháp lây lan của Worms: Cần sự đồng ý từ người dùng để lây lan từ máy này sang máy khá
2. 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? Trojan horse
3. PGP đảm bảo tính bí mật thông điệp bằng cách sử dụng: Mã hóa khóa bất đối xứng sử dụng khóa công khai
4. Số lượng thao tác trong mỗi vòng xử lý của hàm băm MD5 là: 16
5. Trong các cặp khoá sau đây của hệ mật RSA với p=5 ; q=7 , cặp khóa nào có khả năng đúng nhất : ( e = 7 , d =23)
6. Thuật giải SHA-1 dùng để : Tạo một giá trị băm có độ dài cố định 160 bit
7. Một hệ mã hóa (cryptosystem) được cấu thành từ hai thành phần chính gồm: Phương pháp mã hóa và không gian khóa
8. Giải thuật mã hóa và giải mã: XOR
9. Kích thước khối dữ liệu xử lý của giải thuật mã hóa AES là: 128bit
10. Điểm khác nhau chính giữa hai loại hàm băm MDC và MAC là: MDC là loại hàm băm không khóa, còn MAC là loại hàm băm có khóa
11. Một trong các điểm yếu của các hệ mã hóa khóa công khai là: Tốc độ chậm
12. Hai thuộc tính cơ bản quan trọng nhất của một hàm băm là: Nén và dễ tính toán
13. Độ an toàn của hệ mật mã RSA dựa trên: Tính khó của việc phân tích số nguyên rất lớn
14. Khi sinh cặp khóa RSA, các số nguyên tố p và q nên được chọn với kích thước: Bằng khoảng một nửa kích thước của modulo n
15. Tìm phát biểu đúng về mã hóa khóa bất đối xứng (Asymmetric key cryptography):Sử dụng một khóa quá trình mã hóa và một khóa khác cho giải mã
16. Tìm phát biểu đúng về mã hóa khóa đối xứng (Symmetric key cryptography): Sử dụng một khóa chung cho cả quá trình mã hóa và giải mã
17. Số lượng vòng lặp chính thực hiện xáo trộn dữ liệu theo hàm Feistel (F) trong giải thuật DES là: 16
18. Các hộp thay thế s-box trong giải thuật DES có số bít đầu vào và đầu ra tương ứng là: Vào 6 bit và ra 4 bit
19. Một trong các ứng dụng phổ biến của các hàm băm là để tạo chuỗi: checksum
20. Trong quá trình xử lý thông điệp đầu vào tạo chuỗi băm, số lượng vòng xử lý của hàm băm SHA1 là: 80
21. Giải thuật mã hóa AES được thiết kế dựa trên: mạng hoán vị-thay thế
22. Một trong các điểm yếu của các hệ mã hóa khóa đối xứng là: Khó khăn trong quản lý và phân phối khóa
23. 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: 12
24. Một trong các ứng dụng phổ biến của các hàm băm một chiều là để: Mã hóa mật khẩu
25. PGP đảm bảo tính xác thực thông điệp bằng cách: Sử dụng hàm băm có khóa MAC
26. Kích thước khóa hiệu dụng của hệ mã hóa DES là: 56 bit
27. Trong mã hóa dòng (stream cipher), dữ liệu được xử lý theo: Từng bít hoặc từng byte/ký tự
28. Trong hệ mật mã RSA, quan hệ toán học giữa khóa công khai e và số Phi(n) là: e và Phi(n) là 2 số nguyên tố cùng nhau
29. Các giải thuật mã hóa khóa đối xứng thông dụng gồm: DES, 3-DES, AES
30. Trong hệ mật mã RSA, quan hệ toán học giữa khóa riêng d và khóa công khai e là: d là modulo nghịch đảo của e
31. Giải thuật mã hóa AES vận hành dựa trên một ma trận 4x4, được gọi là: State
32. Đâu là một ứng dụng của mã hóa? PGP
33. Phần xử lý chính của SHA1 làm việc trên một chuỗi được gọi là state. Kích thước của state là: 160 bit
34. Trật tự các khâu xử lý trong các vòng lặp chính của giải thuật mã hóa AES là: SubBytes, ShiftRows, MixColumns, AddRoundKey
35. Văn bản sau khi được mã hóa gọi là gì? Văn bản mã.
36. Đặc tính nào sau đây không thuộc chức năng bảo mật thông tin trong các hệ thống mật mã? Hiệu quả.
37. Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng cùng một khóa mã khi mã hóa công khai và giải mã? RS
38. Chuẩn nào sau đây được chính phủ Mỹ sử dụng thay thế cho DES như là một chuẩn mã hóa dữ liệu? AES
39. Ở hệ mật mã nào người gửi và người nhận thông điệp sử dụng các khóa khác nhau khi mã hóa và giải mã ? Không đối xứng
40. Khi giá trị hàm băm của hai thông điệp khác nhau có giá trị tương tự nhau, ta gọi hiện tượng này là gì ? Xung đột
41. Nếu muốn xem một tài liệu “bảo mật”được mã hóa trên hệ mật bất đối xứng do người khác gửi đến , bạn phải sử dụng khóa nào để giải mật tài liệu? Khoá cá nhân của bạn
42. Đâu là một phương pháp mã hóa: Thay thế; Đổi chỗ/hoán vị; vernam
43. Thuật giải MD5 cho ta một giá trị băm có độ dài : 128 bit
44. Các hệ mã hóa khóa công khai sử dụng một cặp khóa: public key và private key. Các yêu cầu đối với public key và private key là: Có thể công khai public key nhưng phải đảm bảo tính xác thực và cần giữ bí mật private key
45. Kích thước khóa có thể của hệ mã hóa AES là: 128, 160 và 192 bit
46. Kích thước khóa hiệu dụng của hệ mã hóa DES là: 56 bit
47. Số lượng vòng lặp chuyển đổi cần thực hiện để chuyển bản rõ thành bản mã trong hệ mã hóa AES khóa 128 bit là: 10
48. Bước MixColumns (trộn cột) trong vòng lặp chuyển đổi trong hệ mã hóa AES thực hiện việc: Mỗi cột của ma trận state được nhân với một đa thức
49. Phát biểu nào sau đây đúng với kỹ thuật mã hóa khóa bí mật: Mã hóa khóa bí mật sử dụng một mã (key) cho cả quá trình mã hóa và giải
50. Ưu điểm của kỹ thuật mã hóa khóa công khai so với mã hóa khóa bí mật là: Trao đổi khóa dễ dàng hơn
51. Yêu cầu để đảm bảo sử dụng mã hóa đối xứng là: Có thuật toán encryption tốt,có một khóa bí mật được biết bởi người nhận/gửi và kênh truyền bí mật để phân phát key
52. Các thuật toán nào sau đây là thuật toán mã hóa đối xứng: Triple–DES, RC4, RC5, IDEA
53. Các phát biểu sau đây phát biểu nào đúng: Hầu hết các thuật toán mã hóa đối xứng đều dựa trên cấu trúc thuật toán Feistel; Tấn công thông điệp thì thời gian giải mã tỷ lệ với kích thước khóa; Hầu hết các thuật toán mã hóa khối đều đối xứng (tất cả đều đúng)
54. Mã hóa nào sau đây là một tiêu chuẩn dùng để phát triển cho việc tạo ra thông điệp an toàn? Data Encryption Standard
55. Các yếu tố ảnh hưởng đến quá trình mã hóa: Thuật toán mã hóa, giải mã, và tính an toàn của kênh truyền
56. MAC là một từ cấu tạo bằng những chữ đầu của một nhóm nào liên quan đến mật mã ? Mã xác thực thông điệp (Message authentication code)
57. Nội dung nào sau đây không cần sử dụng mật mã ? Toàn vẹn
58. Thuật giải MD5 dùng để : Kiểm tra tính toàn vẹn dữ liệu
59. Trong DES mỗi hàm chọn Si được dùng để : Biến đổi khối dữ liệu mã 6 bit thành 4 bit
60. Hệ mật DES sử dụng khối khóa được tạo bởi : 56 bit ngẫu nhiên và 8 bit kiểm tra “Parity”
61. Hệ mật DES xử lý từng khối “ plain text ” có độ dài : 64 bit
62. Số lượng các khóa phụ (subkey) cần được tạo ra từ khóa chính trong giải thuật DES là: 16
63. Sử dụng bao nhiêu bit với DES để có hiệu quả? 64
64. Thuật giải SHA là : Hàm băm một chiều; Hàm băm một chiều; Cho giá trị băm 160 bit (tất cả đều đúng)
65. 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 ? MAC
66. Phát biểu nào sau đây đúng với cơ chế điều khiển truy cập MAC: MAC cấp quyền truy cập dựa trên tính nhạy cảm của những thông tin và chính sách quản trị
67. Các loại khoá mật mã nào sau đây dễ bị crack nhất ? 40 bit
68. Nguyên tắc bảo mật tài nguyên của mô hình Bell-La Padula là: Đọc xuống và ghi lên
69. Tính bảo mật của kỹ thuật điều khiển truy nhập sử dụng mật khẩu dựa trên: Độ khó đoán và tuổi thọ của mật khẩu
70. 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
71. Một trong các điểm yếu làm giảm hiệu quả của phát hiện tấn công, xâm nhập dựa trên bất thường là: Tỷ lệ cảnh báo sai cao
72. 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
73. Ưu điểm của điều khiển truy nhập dựa trên các đặc điểm sinh trắc học là: Bảo mật cao và luôn đi cùng với chủ thể
74. Một ưu điểm của tường lửa có trạng thái so với tường lửa không trạng thái là: Phân biệt được các gói tin thuộc về các kết nối mạng khác nhau
75. Các phương pháp xử lý, phân tích dữ liệu và mô hình hóa trong phát hiện tấn công, xâm nhập dựa trên bất thường, gồm:Thống kê, học máy, khai phá dữ liệu
76. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập dựa trên vai trò - RBAC: RBAC cấp quyền truy nhập dựa trên vai trò của người dùng trong tổ chức
77. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập DAC: DAC cho phép người tạo ra đối tượng có thể cấp quyền truy nhập cho người dùng khác
78. Đâu là một công cụ có khả năng rà quét các lỗ hổng chèn mã SQL cho các trang web? Acunetix Web Vulnerability Scanner
79. Danh sách điều khiển truy nhập ACL thực hiện việc quản lý quyền truy nhập đến các đối tượng cho người dùng bằng cách: Mỗi đối tượng được gán một danh sách người dùng kèm theo quyền truy nhập
80. Tường lửa không thể chống lại: Các hiểm họa từ bên trong
81. Sự khác biệt chính giữa hệ thống ngăn chặn xâm nhập (IPS) và hệ thống phát hiện xâm nhập (IDS) là: IPS có khả năng chủ động ngăn chặn xâm nhập
82. Tường lửa lọc gói có thể lọc các thông tin nào trong gói tin? Chỉ các thông tin trong header của gói tin
83. 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: Các phần mềm quét virus xung đột với nhau
84. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập bắt buộc MAC: MAC cấp quyền truy nhập dựa trên tính nhạy cảm của thông tin và chính sách quản trị
85. Đâu là một loại tường lửa? Application-level gateway
86. Ví điện tử Paypal là một dạng: Thẻ bài (token)
87. Dạng xác thực sử dụng các thông tin nào dưới đây đảm bảo độ an toàn cao hơn? Thẻ ATM và số PIN
88. Một trong các dạng khóa mã (encrypted keys) được sử dụng rộng rãi trong điều khiển truy nhập là: Chứng chỉ số khóa công khai
89. Tại sao một hệ thống phát hiện xâm nhập dựa trên chữ ký không thể phát hiện các tấn công, xâm nhập mới? Do chữ ký của chúng chưa tồn tại trong hệ thống
90. Ưu điểm của thẻ bài (token) so với thẻ thông minh (smart card) trong điều khiển truy nhập là: Có cơ chế xác thực mạnh hơn
91. Phương pháp xác thực nào dưới đây có thể cung cấp khả năng xác thực có độ an toàn cao nhất? Sử dụng vân tay
92. Đâu là các tính năng của kiểm soát truy nhập sử dụng tường lửa? Kiểm soát dịch vụ và hướng
93. Ba cơ chế điều khiển truy nhập thông dụng gồm: DAC, MAC và RBAC
94. 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: Tính bí mật, tính toàn vẹn và tính sẵn dùng
95. Số lượng nhân tố (factor) xác thực sử dụng trong điều khiển truy nhập dựa trên thẻ thông minh là: 2
96. Một nhiệm vụ chính của các hệ thống IDS/IPS là: Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập
97. Hai dịch vụ quan trọng nhất của một hệ thống điều khiển truy nhập là: Authentication và Authorization
98. Tìm phát biểu đúng về phát hiện xâm nhập dựa trên chữ ký và phát hiện xâm nhập dựa trên bất thường: Phát hiện xâm nhập dựa trên chữ ký thường có tỷ lệ phát hiện đúng cao hơn
99. Tìm phát biểu đúng về dịch vụ xác thực trong điều khiển truy nhập: Là quá trình xác minh tính chân thực của thông tin nhận dạng người dùng cung cấp
100. Yếu tố nào cần được sử dụng kết hợp với một thẻ thông minh để xác thực? PIN
101. Quy trình xác thực nào sử dụng nhiều hơn một yếu tố xác thực để login? Đa yếu tố ( multi-factor)
102. Một trong các nhược điểm chính của điều khiển truy nhập dựa trên các đặc điểm sinh trắc học là: Chi phí đắt
103. Ưu điểm của mật khẩu một lần (OTP-One Time Password) so với mật khẩu truyền thống là: Chống được tấn công phát lại
104. Kỹ thuật tấn công SYN Floods khai thác điểm yếu trong khâu nào trong bộ giao thức TCP/IP? Bắt tay 3 bước
105. Một điểm yếu điển hình trong hệ thống điều khiển truy cập là việc sử dụng mật khẩu dễ đoán hoặc mật khẩu được lưu ở dạng rõ. Đây là điểm yếu thuộc khâu: Xác thực
106. Để đảm bảo an toàn cho hệ thống điều khiển truy cập, một trong các biện pháp phòng chống hiệu quả là: Không dùng tài khoản có quyền quản trị để chạy các chương trình ứng dụng
107. Điều khiển truy nhập dựa trên luật (Rule-based access control) được sử dụng phổ biến trong: Firewall
108. Phát hiện tấn công, xâm nhập dựa trên bất thường dựa trên giả thiết: Các hành vi tấn công, xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường
109. Các hệ thống phát hiện xâm nhập có thể thu thập dữ liệu đầu vào từ: Mạng và các host
110. Một hệ thống điều khiển truy nhập có thể được cấu thành từ các dịch vụ nào sau đây: Xác thực, trao quyền và quản trị
111. Sau khi một user đã được định danh (identifed), điều gì cần phải làm trước khi họ log vào một mạng máy tính ? Xác thực với mật khẩu
112. Phát biểu nào sau đây đúng với cơ chế điều khiển truy cập DAC: DAC cho phép người tạo ra đối tượng có thể cấp quyền quy cập cho người dùng khác
113. Các hệ điều hành Microsoft Windows và Linux sử dụng các mô hình điều khiển truy cập nào dưới đây? DAC và Role-BAC
114. Phát biểu nào sau đây đúng với cơ chế điều khiển truy cập RBAC: RBAC cấp quyền truy cập dựa trên vai trò của người dùng trong tổ chức
115. Cho biết câu nào đúng trong các câu sau: Tất cả Firewall đều có chung thuộc tính là cho phép phân biệt hay đối xử khả năng từ chối hay truy nhập dựa vào địa chỉ nguồn; Chức năng chính của Firewall là kiểm soát luồng thông tin giữa mạng cần bảo vệ và Internet thông qua các chính sách truy nhập đã được thiết lập; Hệ thống Firewall thường bao gồm cả phần cứng lẫn phần mềm (Tất cả đều đúng)
116. Đối với Firewall lọc gói, hình thức tấn công nào sau đây được thực hiện: Nhái địa chỉ IP, tấn công giữa, tấn công biên
117. Những chữ đầu của nhóm từ ACL là tên viết tắt của: Access Control List
118. Nên cài mức truy cập mặc định là mức nào sau đây? No access
119. 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? Phải được ủy quyền
120. Bộ lọc địa chỉ MAC được định nghĩa như : Ngăn chặn truy cập từ một địa chỉ MAC nhất định.
121. Các mức độ nhạy cảm của thông tin được chia từ cao xuống thấp đối với an ninh quốc gia là: Tối mật (Top Secret - T), Tuyệt mật (Secret - S), Mật (Confidential - C), Không phân loại (Unclassified - U).
122. Đặc tính nào của các thiết bị mạng như router hay switch, cho phép điều khiển truy cập dữ liệu trên mạng ? Danh sách điều khiển truy cập (ACL).
123. Yếu tố nào cần được sử dụng kết hợp với một thẻ thông minh để xác thực? PIN
124. Phương pháp quét võng mạc thích hợp nhất đối với các dịch vụ nào sau đây? Kiểm soát truy cập
125. Yếu tố nào sau đây được coi là hữu ích nhất trong việc kiểm soát truy cập khi bị tấn công từ bên ngoài? Đăng nhập hệ thống ( System logs)
126. Điểm khác nhau chính giữa các hệ thống ngăn chặn đột nhập (IPS) và phát hiện đột nhập (IDS) là: IPS có khả năng chủ động ngăn chặn tấn công so với IDS
127. Để đánh giá điểm mạnh của hệ thống IDS người ta dựa vào các yếu tố sau : Khởi sự, giám sát vị trí, những đặc trưng ghép nối hoặc tích hợp
128. Khi thực hiện triển khai HIDS khó khăn gặp là: Giới hạn tầm nhìn mạng, phải xử lý với nhiều hệ điều hành khác trên mạng.
129. Bộ lọc gói thực hiện chức năng nào? Ngăn chặn các gói trái phép đi vào từ mạng bên ngoài
130. Hệ thống nào được cài đặt trên Host để cung cấp một tính năng IDS ? H-IDS (Host-based IDS)
131. Tổ chức chính cấp phát chứng chỉ được gọi là : CA
132. Các phát biểu sau đây phát biểu là là đúng nhất: Firewall là một vành đai phòng thủ cho máy tính hoặc hệ thống trước những tấn công
133. Các biện pháp được sử dụng để đảm bảo an toàn máy tính và dữ liệu là: Việc sao lưu tạo dự phòng dữ liệu, đảm bảo dữ liệu không bị mất mát khi xảy ra sự cố

**Cơ sở An toàn Thông tin 4**

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: Địa chỉ trả về của hàm
2. Tấn công kiểu Social Engineering là dạng tấn công khai thác yếu tố nào sau đây trong hệ thống: Người dùng
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: Tấn công chèn mã SQL
4. Một trong các biện pháp có thể sử dụng để phòng chống tấn công người đứng giữa là: 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: Không dùng tài khoản có quyền quản trị để chạy các chương trình ứng dụng
6. Đâu là một trong các biện pháp phòng chống tấn công khai thác lỗi tràn bộ đệm: Sử dụng cơ chế cấm thực hiện mã trong dữ liệu
7. Một trong các biện pháp hiệu quả để phòng chống macro viruses là: ấm tự động thực hiện macro trong Microsoft Office
8. Các lỗ hổng bảo mật thường tồn tại nhiều nhất trong thành phần nào của hệ thống: Các ứng dụng
9. Đâu là một kỹ thuật tấn công DoS: Smurf
10. Trong tấn công khai thác lỗi tràn bộ đệm, tin tặc thường sử dụng shellcode đó là dạng: Mã máy
11. Lỗi tràn bộ đệm là lỗi trong khâu: Lập trình phần mềm
12. Một trong các các virus thường sử dụng để lây nhiễm và các chương trình khác là: Sửa đổi các chương trình
13. Sâu SQL Slammer tấn công khai thác lỗi tràn bộ đệm trong hệ quản trị csdl: SQL Server 2000
14. 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: Thủ tục csdl cho phép tách mã lệnh SQL khỏi dữ liệu người dùng
15. Các vùng bộ nhớ thường bị tràn bao gồm: ngăn xếp(stack) và vùng cấp phát động (Heap)
16. Trong tấn công khai thác lỗ 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: Tăng khả năng mã tấn công được thực hiện
17. Trojan 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…: DAC
18. Trojan 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…: Độ dài từ 8 ký tự trở lên, gồm chữ cái hoa, thường, chữ số và ký tự đặc biệt
19. Đâu là dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng: Lỗi tràn bộ đệm
20. Nguyên nhân của sự tồn tại các điểm yếu trong hệ thống có thể do: Tất cả các khâu trong quá trình phát triển và vận hành (Lỗi thiết kế, lỗi cài đặt và lập trình; Lỗi cấu hình; Lỗi quản trị)
21. Một trong các biện pháp cụ thể cho quản lý, khắc phục các lỗ hổng bảo mật và tăng cường khả năng đề kháng cho hệ thống là: Định kỳ cập nhật các thông tin về các lỗ hổng từ các trang web chính thức
22. Tìm phát biểu đúng trong các phát biểu sau: Điểm yếu hệ thống có thể xuất hiện trong cả mô đun phần cứng và phần mềm
23. Biện pháp nào không thể phòng chống hiệu quả tấn công khai thác lỗi tràn bộ đệm gồm: Sử dụng công cụ gỡ rối để ngăn chặn tràn trong thời gian vận hành
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: Cân bằng giữa an toàn, hữu dụng và rẻ tiền
25. Trong 7 vùng cơ sở hạ tầng CNTT, vùng nào có mối đe dọa và nguy cơ nhất: Vùng người dùng
26. Lỗ hổng bảo mật (Security vulnerability) là một điểm yếu tồn tại trong một hệ thống cho phép tin tặc: Khai thác tổn hại đến các thuộc tính an ninh của hệ thống đó
27. ATTT gồm 2 lĩnh vực chính là: An toàn CNTT và đảm bảo thông tin
28. ATTT là gì: Là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi hoặc phá hủy thông tin một cách trái phép
29. Các lỗ hổng an ninh trong HĐH máy chủ là mối đe dọa thuộc vùng nào trong 7 vùng cơ sở hạ tầng CNTT: Vùng mạng Lan
30. Một thông điệp có nội dung nhạy cảm truyền trên mạng bị sửa đổi. Các thuộc tính an toàn nào bị vi phạm: Bí mật và toàn vẹn
31. Các thành phần chính của hệ thống máy tính: Hệ thống phần cứng và phần mềm
32. Tính bí mật của thông tin có thể đảm bảo bằng: Bảo vệ vật lý, VPN hoặc mã hóa
33. Việc thực thi quản lý ATTT cần được thực hiện theo chu trình lặp lại là do: Các điều kiện bên trong và bên ngoài hệ thống thay đổi theo thời gian
34. Biện pháp không thể phòng chống hiệu quả tấn công khai thác lỗi tràn bộ đệm: Sử dụng công cụ gỡ rối để ngăn chặn tràn trong thời gian vận hành
35. Người sử dụng hệ thống thông tin quản lý trong mô hình 4 loại hệ thống thông tin là: Quản lý bộ phận
36. Một trong các nội dung quan trọng nhất của quản lý ATTT là: Quản lý rủi ro
37. Tại sao cần phải đảm bảo AT cho thông tin: Do có nhiều thiết bị kết nối mạng Internet với nhiều mối đe dọa
38. Một điểm yếu điển hình trong hệ thống điều khiển truy nhập là việc sử dụng mật khẩu dễ đoán hoặc mật khẩu lưu dưới dạng rõ. Đây là điểm yếu thuộc khâu: Xác thực
39. Tại sao một hệ thống phát hiện xâm nhập dựa trên chữ ký không thể phát hiện các tấn công, xâm nhập mới: Do chữ ký của chúng chưa tốn tại trong hệ thống
40. Không nên sử dụng nhiều hơn một phần mềm quét virus chạy ở chế độ quét theo thời gian thực trên một máy tính vì: Các phần mềm quét virus xung đột với nhau
41. Phát hiện tấn công, xâm nhập dựa trên bất thường dựa trên giả thiết: Phát hiện tấn công, xâm nhập dựa trên bất thường dựa trên giả thiết
42. Đâu là tên viết đúng của hệ thống xâm nhập/ đột nhập: Intrusion Detection System
43. Đâu là các tính năng của kiểm soát truy nhập sử dụng tường lửa: Kiểm soát dịch vụ và hướng
44. Một hệ thống điều khiển truy nhập có thể được cấu thành từ các dịch vụ nào sau đây: Xác thực, trao quyền và quản trị
45. Một trong các dạng mã hóa ( encrypted Keys) được sử dụng rộng rãi trong điều khiển truy nhập là: Chứng chỉ số hóa công khai
46. Sự khác biệt chính giữa hệ thống ngăn chặn xâm nhập (IPS) và hệ thống phát hiện xâm nhập (IDS) là: IPS có khả năng chủ động ngăn chặn xâm nhập
47. Phương pháp xác thực nào dưới đây có thể cung cấp khả năng xác thực có độ an toàn cao nhất: Sử dụng vân tay
48. Điều khiển truy nhập dựa trên luật(Rule-based access control) được sử dụng phổ biến trong: Firewall
49. Một ưu điểm của tường lửa có trạng thái so với tường lửa không trạng thái là: Phân biệt được các gói tin thuộc về các kết nối mạng khác nhau
50. Tường lửa lọc gói có thể lọc các thông tin nào trong gói tin: Chỉ lọc địa chỉ IP trong gói tin
51. Tường lửa không thể chống lại: Tấn công hướng dữ liệu,Các hiểm họa từ bên trong
52. Đâu là một công cụ có khả năng rà quét các lỗ hổng chèn mã SQL cho các trang web: Acunetix web vulnerability scanner
53. Nguyên tắc bảo mật tài nguyên của mô hình Bell-La Padula là: Đọc xuống và ghi lên
54. 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
55. Ưu điểm của thẻ bài (token) so với thẻ thông minh (smart card) trong điều khiển truy nhập là: Có cơ chế xác thực mạnh hơn
56. Đâu là một Loại trường lửa: Application-level gateway
57. Tìm phát biểu đúng về dịch vụ xác thực trong điều khiển truy nhập: là quá trình xác minh tính chân thực của thông tin nhận dạng người dùng cung cấp
58. 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: Tính bí mật, tính toàn vẹn và tính sẵn dùng
59. Ưu điểm của điều khiển truy nhập dựa trên các đặc điểm sinh trắc học là: Bảo mật cao và luôn đi cùng với chủ thể
60. Một nhiệm vụ chính của các hệ thống IDS/IPS là: Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập.
61. Số lượng nhân tố (factor) xác thực sử dụng trong điều khiển truy nhập dựa trên thẻ thông minh là: 2
62. Dạng xác thực sử dụng các thông tin nào dưới đây đảm bảo độ an toàn cao hơn: Thẻ ATM và số PIN
63. Ưu điểm của mật khẩu một lần (OTP-One Time Password) so với mật khẩu truyền thống là: Chống được tấn công phát lại
64. Hai dịch vụ quan trọng nhất của một hệ thống điều khiển truy nhập là: Authentication và Authorization
65. Tìm phát biểu đúng về phát hiện xâm nhập dựa trên chữ ký và phát hiện xâm nhập dựa trên bất thường: Phát hiện xâm nhập dựa trên chữ ký thường có tỷ lệ phát hiện đúng cao hơn
66. Các hệ thống phát hiện xâm nhập có thể thu thập dữ liệu đầu vào từ…: Mạng và các host
67. Một trong các nhược điểm chính của điều khiển truy nhập dựa trên các đặc điểm sinh trắc học là: Chi phí đắt
68. Danh sách điều khiển truy nhập ACL thực hiện việc quản lý quyền truy nhập đến các đối tượng cho người dùng bằng cách: Mỗi đối tượng được gán một danh sách người dùng kèm theo quyền truy nhập.
69. Phát biểu nào sau đây đúng với cơ chế điều khiển truy nhập bắt buộc MAC: MAC quản lý quyền truy nhập chặt chẽ hơn các cơ chế khác
70. Tính bảo mật của kỹ thuật điều khiển truy nhập sử dụng mật khẩu dựa trên: Độ khó đoán và tuổi thọ của mật khẩu
71. Các phương pháp xử lý , phân tích dữ liệu và mô hình hóa trong phát hiện tấn công, xâm nhập bất thường gồm: Thống kê, học máy, khai phá dữ liệu
72. Ba cơ chế điều khiển truy nhập thông dụng gồm: DAC, MAC, RBAC
73. Loại tấn công nào sau đây chiếm quyền truy nhập đến tài nguyên lợi dụng cơ chế điều khiển truy nhập DAC: Trojan horse
74. Một trong các điểm yếu làm giảm hiệu quả của tấn công, xâm nhập dựa trên bất thường là: Tỷ lệ cảnh báo sai cao
75. Ví điện tử Paypal là một dạng…: Thẻ bài (token)
76. Để thực hiện tấn công Smurf, tin tặc phải giả mạo địa chỉ gói tin ICMP trong yêu cầu…: Địa chỉ nạn nhân làm địa chỉ nguồn của gói tin
77. Tấn công bằng mã độc có thể gồm: SQLi, XSS, CSRF và Buffer overflow
78. Có thể phòng chống tấn công Smurf bằng cách cấu hình các máy và router không trả lời..: Các yêu cầu ICMP hoặc các yêu cầu phát quảng bá
79. Trong dạng tấn công vào mật khẩu dựa trên từ điển, tin tặc đánh cắp mật khẩu…: Thử các từ có tần suất sử dụng cao làm mật khẩu trong từ điển
80. Đâu là một kỹ thuật tấn công DoS: Smurf
81. Đâu là một biện pháp phòng chống tấn công SYN Floods: SYN Cache
82. Dạng tấn công chặn bắt thông tin truyền trên mạng để sửa đổi hoặc lạm dụng là: Modifications
83. Đâu là một kỹ thuật tấn công Dos: Ping of death
84. Phishing là một dạng của loại tấn công sử dụng…: Kỹ thuật xã hội
85. Các dạng tấn công phần mềm độc hại (malware) có khả năng tự nhân bản gồm: Virus, Worm, Zombie
86. Nguy cơ cao nhất mà cuộc tấn công chèn mã SQL có thể gây ra cho một hệ thống là: Chiếm quyền điều khiển hệ thống
87. Một trong các mối đe dọa an toàn thông tin thường gặp là: Phần mềm độc hại
88. Các zombie thường được tin tặc sử dụng để…: Thực hiện tấn công DdoS
89. Trên thực tế, có thể giảm khả năng bị tấn công nếu có thể…: Giảm thiểu các lỗ hổng bảo mật
90. Macro viruses là loại virus thường lây nhiễm vào: Các file tài liệu của bộ phần mềm Microsoft Office
91. Mục đích chính của tấn công giả mạo địa chỉ IP là: Để vượt qua hàng rào kiểm soát an ninh
92. Tấn công kiểu Social Engineering có thể cho phép tin tặc: Đánh cắp thông tin nhạy cảm của người dùng
93. Tấn công kiểu Social Engineering là dạng tấn công khai thác điểm yếu ở vùng nào sau đây: Người dùng
94. Các máy tính ma/ máy tính bị chiếm quyền điều khiển thường được tin tặc sử dụng để: Gửi thư rác, thư quảng cáo
95. Đâu là một công cụ kiểm tra lỗ hổng tấn công chèn mã SQL trên các Website: SQLmap
96. Sự khác biệt cơ bản giữa virut và sâu là: Sâu có khả năng tự lây lan mà không cần tương tác của người dùng.
97. Kỹ thuật tấn công Smurf sử dụng giao thức ICMP và cơ chế gửi..: Broadcast
98. Tấn công từ chối dịch vụ (DoS-Denial of Service Attacks) là dạng tấn công có khả năng: Cản trở người dùng hợp pháp truy nhập các tài nguyên hệ thống
99. Tìm phát biểu đúng trong các phát biểu sau: Mối đe dọa là bất kỳ một hành động tấn công nào gây hư hại đến các tài nguyên hệ thống.
100. Sự khác biệt cơ bản giữa tấn công DoS và DdoS: Phạm vi tấn công
101. Một trong các cách virus thường sử dụng để lây nhiễm vào các chương trình khác là: Sửa đổi các chương trình
102. Pharming là kiểu tấn công vào: Máy khách/ trình duyệt web
103. Kỹ thuật tấn công SYN Floods khai thác điểm yếu trong khâu nào của bộ giao thức TCP/IP: Bắt tay 3 bước
104. Để thực hiện tấn công DdoS, tin tặc trước hết cần chiếm quyền điều khiển của một lượng lớn máy tính. Các máy tính bị chiếm quyền điều khiển thường gọi là: Zombies
105. Tấn công gây ngắt quãng dịch vụ hoặc kênh truyền thông cho người dùng…: Interruptions
106. Một trong các cách hiệu quả để phòng chống macro viruses là: Cấm tự động thực hiện macro trong Microsoft Office
107. Một trong các phương thức lây lan thường gặp của sâu mạng là: Lây lan thông qua khả năng thực thi từ xa.
108. Tấn công nghe lén là kiểu tấn công: Thụ động
109. Một trong các biện pháp có thể sử dụng để phòng chống tấn công người đứng giữa là: Sử dụng chứng chỉ số để xác thực thông tin nhận dạng các bên.
110. Trong tấn công DdoS phản chiếu hay gián tiếp, có sự tham gia của một lượng lớn máy chủ trên mạng Internet không bị tin tặc chiếm quyền điều khiển, Các máy chủ này được gọi là: Reflectors
111. Đâu là một phương pháp mã hóa: XOR
112. Một trong các điểm yếu của các hệ mã hóa khóa công khai là: Tốc độ chậm
113. Điểm khác nhau chính giữa hai loại hàm băm MDC và MAC là: MDC là loại hàm băm không khóa, còn MAC là loại hàm băm có khóa
114. Kích thước khóa hiệu dụng của hệ mã hóa DES là: 56 bít
115. Đâu là một chế độ hoạt động (Modes of Operation) của mã hóa khối: ECB
116. Một trong các ứng dụng phổ biến của các hàm băm 1 chiều là: Mã hóa mật khẩu
117. Tìm phát biểu đúng về mã hóa khóa bất đối xứng (Asymmetric key cryptography): Sử dụng một khóa quá trình mã hóa và một khóa khác cho giải mã.
118. Giải thuật mã hóa AES vận hàng dựa trên một ma trận 4\*4, được gọi là: State
119. Các hộp thay thế S-Box trong giải thuật DES có số bít đầu vào và đầu ra tương ứng là: Vào 6 bit, ra 4 bit
120. Hai thuộc tính cơ bản và quan trọng nhất của một hàm băm là: Nén và dễ tính toán.
121. Trật tự các khâu xử lý trong các vòng lặp chính của giải thuật mã hóa AES: SubBytes, ShiftRows, MixColumns, AddRoundKey
122. Số lượng vòng lặp chính thực hiện xáo trộn dữ liệu theo hàm Feistel (F) trong giải thuật DES là: 16
123. Trong hệ mã hóa RSA, quan hệ toán học giữa khóa riêng d và khóa công khai e là: d là modulo nghịch đảo của e
124. 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: 12
125. Các giải thuật mã hóa khóa đối xứng thông dụng gồm: DES, 3DES, AES
126. Trong quá trình xử lý thông điệp đầu vào tạo chuỗi băm, số lượng vòng xử lý của hàm băm SHA1 là: 80
127. Một trong các điểm yếu của các hệ mã hóa khóa đối xứng là: Khó khăn trong quản lý và phân phối khóa.
128. Độ an toàn của giải thuật RSA dựa trên: Tính khó của việc phân tích số nguyên lớn.
129. Đâu là một ứng dụng của mã hóa: PGP
130. Giải thuật mã hóa AES được thiết kế dựa trên: Mạng hoán vị-thay thế
131. Trong hệ mật mã RSA, quan hệ toán học giữa khóa công khai e và số Phi(n) là: e và Phi(n) là hai số nguyên tố cùng nhau
132. Kích thức khối dữ liệu xử lý của giải thuật mã hóa AES là: 128
133. Đâu là một chế độ hoạt động (Modes of Operation) của mã hóa khối: CBC
134. Phần xử lý chính của SHA1 làm việc trên một chuỗi được gọi là state là: 160
135. Một hệ mã hóa (cryptosystem) được cấu thành từ hai thành phần chính gồm: Phương pháp mã hóa và không gian khóa
136. Số lượng thao tác trong mỗi vòng xử lý của hàm băm MD5 là: 16
137. Một trong các ứng dụng phổ biến của các hàm băm là để tạo chuỗi…: CheckSum
138. Trong mã hóa dòng (stream cipher), dữ liệu được xử lý theo…: Từng bit hoặc từng byte/ ký tự
139. Khi sinh cặp khóa RSA, các số nguyên tố p và q nên được chọn với kích thước: bằng khoảng 1 nửa kích thước của modulo n