Final Test - Ôn tập an toàn thông tin

An toàn thông tin (Trường Đại học Sư phạm Kỹ Thuật Thành phố Hồ Chí Minh)

1. Tấn công DoS/DDoS làm ảnh hưởng đến tiêu chuẩn nào của an toàn thông tin?

a. Tính sẵn sàng
b. Tính toàn vẹn
c. Tính bí mật
d. Tính xác thực

2. Một hệ thống xác thực sinh trắc học cho phép một người giả mạo hình thức nhân viên công ty khi vào hệ thống là hiện tượng gì sau?

a. False negative
b. False positive
c. True negative
d. True positive

3. Cơ chế kiểm soát truy cập nào cho phép chủ sở hữu dữ liệu tạo và quản lý kiểm soát truy cập?

a. List Based Access Control (LBAC)
b. Attribute Based Access Control (ABAC)
c. Mandatory Access Control (MAC)
d. Role Based Access Control (RBAC)
e. Discretionary Access Control (DAC)

4. Trong mã hóa bất đối xứng (còn gọi là mã hóa hóa công khai). Bob muốn tạo chữ ký cho văn bản M để gửi cho Alice. Bob cần dùng khóa gì?

a. Khóa Public của Bob
b. Khóa Public của Alice
c. Khóa Private của Alice
d. Khóa Private của Bob

5. Trong mã hóa bất đối xứng (còn gọi là mã hóa hóa công khai). Alice cần mã hóa văn bản để gửi cho Bob thì Alice cần dùng khóa gì?

a. Khóa Public của Alice
b. Khóa Private của Alice
c. Khóa Private của Bob
d. Khóa Public của Bob

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

a. Cipher block chaining mode – CBC
b. Output feedback mode – OFB
c. Cipher feedback mode - CFB
d. Electronic codebook mode - ECB

7. Sắp xếp các thông tin cho đúng về độ dài đầu ra của các thuật toán mã hóa sau

DES – 64 bits
3DES – 64 bits
AES – 128 bits
SHA-512 – 512 bits
MD5 – 128 bits

8. Các khối xử lý nào được dùng trong mã hóa đối xứng AES?
a. ShiftRows
b. SubBytes
c. Straight P-box
d. MixRows
e. Shift left
f. Compression P-box

9. Diffie - Hellman là thuật toán dùng để
a. Tạo khoá
b. Hash khóa
c. Trao đổi khóa
d. Mã hóa khóa
e. Giải mã khóa

10. Kiểu tấn công nào sau đây không phải khai thác các lỗ hổng của ứng dụng Web?
a. Cross-site scripting
b. SQL Injection
c. Cross Site Request Forgery
d. Social Engineering

11. Điều nào sau đây sẽ bảo vệ tốt nhất trước cuộc tấn công cụ SQL Injection?
a. IDS

b. Firewall
c. Lọc dữ liệu người dùng nhập vào
d. Lưu lượng truy cập web được mã hóa

12. Tấn công nào có thể bỏ qua hệ thống xác thực để truy cập vào máy tính?
a. Front door
b. Brute Force
c. DoS
d. Backdoor

13. Công cụ nào dùng để quét cổng của máy tính
a. Ping
b. Tracert
c. Nmap
d. Nslookup
e. telnet

14. Hệ thống phát hiện xâm nhập dựa vào dấu hiệu (Signature-based IDS) hoạt động dựa vào yếu tố nào?
a. Các dấu hiệu tấn công
b. Các dấu hiệu bất thường
c. Nội dung website
d. Các dấu hiệu bình thường

15. dạng mã độc nào sau đây sống độc lập?
a. Rootkit
b. Logic boom
c. Trojan
d. Zombie
e. Worm

16. Tại sao các nhà phát triển phần mềm đính kèm theo các giá trị băm bằng hàm MD5 của các gói cập nhật cho phần mềm cùng với các gói đó để các khách hàng của họ có thể download từ Internet?
a. Khách hàng có thể xác thực tính toàn vẹn và gói cập nhật cho phần mềm sau khi download về

b. Khách hàng có thể khẳng định tính xác thực của Site mà họ download gói cập nhật về
c. Khách hàng có thể yêu cầu các bản cập nhật mới cho phần mềm trong tương lai bằng cách sử dụng giá trị hàm băm đính kèm theo
d. Khách hàng cần giá trị của hàm băm để có thể kích hoạt được phần mềm mới

17. Loại malware nào sau đây có thể ẩn các tiến trình và các tập tin trên hệ thống?
a. Trojan
b. Adware
c. Worm
d. Rootkit

18. Thuật toán mật mã nào sau đây dựa trên độ khó của bài toán phân tích các số lớn thành tích của hai thừa số nguyên tố ban đầu?
a. ECC
b. RSA
c. DES
d. Diffie-Hellman

19. Điều gì xảy ra khi máy X sử dụng kỹ thuật ARP spoofing để nghe lén thông tin từ máy Y?
a. X giả mạo địa chỉ MAC của Y
b. X giả mạo địa chỉ IP của Y
c. Y giả mạo địa chỉ MAC của X
d. Y giả mạo địa chỉ IP của X

20. Một máy chủ Web của một công ty được cấu hình các dịch vụ sau: HTTP, HTTPS, FTP, SMTP. Máy chủ này được đạt trong vùng DMZ. Những cổng nào cần phải mở trên Firewall để cho phép máy người dùng có thể sử dụng dịch vụ trên máy này?
a. 119, 23, 21, 80, 23
b. 434, 21, 80, 25, 20
c. 80, 20, 21, 25, 443
d. 110, 443, 21, 59, 25

21. Giao thức nào sau đây được dùng để mã hóa dữ liệu trao đổi giữa Web Browser và Web server?
a. IPSec
b. HTTP
c. SSL/TLS
d. VPN
e. SMTP

22. Cách tốt nhất để nhận ra hành vi bất thường và đánh ngờ trên hệ thống của bạn là gì?
a. Nhận biết các cuộc tấn công mới
b. Cấu hình IDS để phát hiện và báo cáo tất cả các lưu lượng bất thường
c. Biết các hoạt động bình thường của hệ thống là như thế nào
d. Nghiên cứu dấu hiệu hoạt động của các loại tấn công chính

23. Mô hình bảo mật theo chiều sâu (defense in depth) gồm các lớp bảo mật theo thứ tự từ trong ra ngoài là?
a. Layer 1 - Data security
b. Layer 2 - Application security
c. Layer 3 - Host security
d. Layer 4 - LAN security
e. Layer 5 - Perimeter security
f. Layer 6 - Physical security
g. Layer 7 - Policies, procedures, awareness

24. Trong an toàn thông tin, Ping Sweep được sử dụng để làm gì?
a. Để xác định các host đang hoạt động trên mạng
b. Để xác định vị trí của các host đang hoạt động trên mạng
c. Để xác định các cổng đang mở trên mạng
d. Để xác định vị trí của các tường lửa trên mạng

25. Điều nào sau đây mô tả tốt nhất cơ chế kiểm soát truy cập trong đó các quyết định kiểm soát truy cập dựa trên trách nhiệm của người dùng trong một tổ chức?
a. MAC (Mandatory Access Control)
b. RBAC (Role Based Access Control)
c. DAC (Discretionary Access Control)

d. Rule Based Access Control

26. Ma trận điều khiển truy cập (Access control matrix) thể hiện mối quan hệ giữa các thành phần nào sau đây?

a. Subject
b. Object
c. Rights/Permissions
d. Users
e. Security policy
f. Database

27. Từ ma trận điều khiển truy cập, ta có thể suy ra các thông tin nào sau đây?

a. Access control lists
b. Capability lists
c. Subjects orientation lists
d. Objects orientation list
e. Group policy objects

28. Access control liên quan đến 2 chức năng chính là?

a. Authentication
b. Authorization
c. Least privilege principle
d. Role Based Access Control
e. Rule Based Access Control

29. Trong HĐH Linux, để tắt chức năng phát sinh địa chỉ bộ nhớ ngẫu nhiên, sử dụng lệnh nào sau đây?

a. $sudo sysctl –w kernel.randomize_va_space=0
b. $sudo sysctl –w kernel.randomize_sa_space=0
c. $sudo sysctl –w kernel.randomize_ram_space=0
d. $sudo sysctl –w kernel.randomize_store_space=0
e. $sudo sysctl –w kernel.randomize_as_space=0

30. Trong tổ chức bộ nhớ của chương trình C, phần Data-Segment lưu các thông tin gì của chương trình?

a. Lưu các biến static/global đã được khởi tạo trong chương trình
b. Lưu các biến static/global chưa được khởi tạo trong chương trình

c. Lưu các biến cục bộ trong chương trình
d. Lưu các đối số của một hàm
e. Lưu mã nguồn thực thi

31. Việc gỡ bỏ những dịch vụ và giao thức không cần thiết gọi là?
a. Nonrepudiation
b. Hardening
c. Auditing
d. Hashing
e. Cleaning

32. Tại sao hacker hay sử dụng máy chủ proxy?
a. Để tạo kết nối mạnh mẽ hơn với mục tiêu
b. Để tạo một máy chủ ma trên mạng
c. Để có được kết nối truy cập từ xa
d. Để ẩn hoạt động của chúng trên mạng

33. Giải pháp Stackshield giúp phòng chống tấn công tràn bộ đệm trên stack thực hiện như sau:
a. Lưu trữ giá trị Return Address ở một nơi khác và sử dụng nó để kiểm tra xem giá trị ở Return Address có bị sửa đổi hay không
b. Sử dụng một vùng nhớ đệm an toàn giữa Return Address và Buffer. Sử dụng vùng nhớ đệm an toàn này để kiểm tra xem Return Address có bị sửa đổi hay không
c. Kiểm tra giá trị Return Address có bị sửa đổi hay không
d. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu

34. Giải pháp StackGuard giúp phòng chống tấn công tràn bộ đệm trên stack thực hiện như sau:
a. Lưu trữ giá trị Return Address ở một nơi khác và sử dụng nó để kiểm tra xem giá trị ở Return Address có bị sửa đổi hay không
b. Sử dụng một vùng nhớ đệm an toàn giữa Return Address và Buffer. Sử dụng vùng nhớ đệm an toàn này để kiểm tra xem Return Address có bị sửa đổi hay không
c. Kiểm tra giá trị Return Address có bị sửa đổi hay không
d. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu

35. Mục đích chính của các kỹ thuật điều khiển truy cập là?
a. Cung cấp tất cả các quyền truy cập cho người dùng
b. Giới hạn các quyền truy cập và các hành động cho người dùng hợp pháp được sử dụng
c. Ngăn chặn người dùng trái phép truy cập vào tài nguyên hệ thống
d. Bảo vệ máy tính khỏi virus

36. Một hệ thống kiểm soát truy cập chỉ cấp cho người dùng những quyền cần thiết để họ thực hiện công việc đang hoạt động theo nguyên tắc bảo mật nào?
a. Discretionary Access Control
b. Least Privilege
c. Mandatory Access Control
d. Separation of Duties

37. Để nâng cao việc phát triển các giải pháp an toàn cho một hệ thống CNTT, người ta tập trung đầu tư vào 3 vấn đề chính là?
a. Con người
b. Quy trình
c. Công nghệ
d. Đội ngũ chuyên gia bảo mật
e. Tăng chi phí đầu tư cho bảo mật
f. Đào tạo nâng cao nhận thức

38. Chuẩn nào sau đây liên quan đến an toàn thông tin?
a. ISO 27001
b. ISO 2015
c. ISO 9001
d. ISO 2600
e. ISO 21997

39. Cho mô tả sau: User Nam có quyền đọc và ghi trên file bt1. Nam cũng có quyền đọc trên file bt2 và có quyền thực thi trên file bt3. User Ha có quyền đọc trên file bt1. Hà có quyền đọc và ghi trên file bt2. Hà không có quyền truy cập trên file bt3. Xác định Clist (Capability list) đối với user Ha?
a. CList(Ha) = bt1: {read}, bt2: {read, write}, bt3: {}
b. CList(Ha) = bt1: {read, write}, bt2: {read, write}, bt3: {}

c. CList(Ha) = bt1: {read}, bt2: {read, write}, bt3: {read, write}
d. CList(Ha) = bt1: {read, write}, bt2: {write}, bt3: {read}
e. CList(Ha) = bt1: {}, bt2: {write}, bt3: {}

40. Cho mô tả sau: User Nam có quyền đọc và ghi trên file bt1. Nam cũng có quyền đọc trên file bt2 và có quyền thực thi trên file bt3. User Ha có quyền đọc trên file bt1. Hà có quyền đọc và ghi trên file bt2. Hà không có quyền truy cập trên file bt3. Xác định ACL (Access control list) đối với file bt2?
a. ACL(bt2) = Nam: {read}, Ha: {read, write}
b. ACL(bt2) = Nam: {read, write}, Ha: {read}
c. ACL(bt2) = Nam: {read, write}, Ha: {read, write}
d. ACL(bt2) = Nam: {read}, Ha: {read}
e. ACL(bt2) = Nam: {read, execute}, Ha: {read, write}

41. Mô hình AAA liên quan đến các chứng năng nào sau đây?
a. Authentication
b. Authorization
c. Accounting
d. Authenticity
e. Automation
f. Accessing

42. Phương pháp nào sau đây là TỐT NHẤT để giảm hiệu quả của các cuộc tấn công lừa đảo trên mạng?
a. Đào tạo nâng cao nhận thức người dùng
b. Xác thực 2 yếu tố
c. Phần mềm chống lừa đảo
d. Quét lỗ hổng cho hệ thống định kỳ

43. Điều nào sau đây KHÔNG đúng khi nói về lỗ hổng 0-day?
a. Là lỗ hổng nhà sản xuất chưa kịp vá
b. Là lỗ hổng phá hoại hệ thống trong vòng một ngày
c. Là lỗ hổng hacker chưa công bố rộng rãi
d. Là lỗ hổng nguy hiểm khi tấn công vào hệ thống chưa có giải pháp bảo vệ

44. Mục đích chính của chương trình nâng cao nhận thức bảo mật là?
a. Đảm bảo rằng mọi người đều hiểu chính sách và thủ tục của tổ chức

b. Thông báo cho mọi người rằng quyền truy cập vào thông tin sẽ được cấp khi người sử dụng có yêu cầu
c. Cảnh báo tất cả người dùng truy cập vào tất cả các hệ thống sẽ được theo dõi hàng ngày
d. Thông báo cho người dùng để tuân thủ các quy định liên quan đến bảo vệ dữ liệu và thông tin

45. Tấn công Buffer Overflow có hai loại là?
a. Heap và stack
b. Heap và network overflow
c. Stack và memory
d. Stack và SQL injection
e. SQL injection và XSS

46. Tấn công một máy tính bằng cách gửi các gói TCP handshake không đúng thứ tự đến đích (wrong order) xảy ra ở tầng nào?
a. Network Interface layer
b. Internet layer
c. Transport layer
d. Application layer
e. Network layer

47. Trong các giao thức dưới đây, giao thức nào cho phép xác thực user khi user gắn thiết bị vào port layer 2?
a. Radius
b. 802.11X
c. 802.3D
d. 802.3

48. Mục tiêu chính của an toàn thông tin là đảm bảo các tính chất theo mô hình C-I-A là?
a. Tính bí mật
b. Tính toàn vẹn
c. Tính sẵn sàng
d. Tính chống chối bỏ
e. Tính xác thực
f. Tính dễ mở rộng

49. Câu nào sau đây không phải là một cơ chế điều khiển truy cập?
a. Mandatory Access Control (MAC)
b. Role Based Access Control
c. Subjective Access Control
d. Attribute Based Access Control
e. Discretionary Access Control (DAC)

50. Điều nào sau đây là rủi ro tiềm ẩn khi chương trình chạy ở chế độ đặc quyền?
a. Nó có thể phục vụ cho việc tạo ra các đoạn mã phức tạp không cần thiết
b. Nó có thể không thực hiện việc phân chia xử lý các tác vụ
c. Nó có thể tạo ra việc loại bỏ các ứng dụng không cần thiết
d. Nó có thể cho phép mã độc được chèn vào