Test attt - cơ sở văn hóa

Cơ sở văn hóa (Trường Đại học Sư phạm Kỹ Thuật Thành phố Hồ Chí Minh)

1. Một quản trị mạng mới thay thế hub bằng switch. Khi sử dụng phần mềm Sniffer bắt các gói tin trên mạng, người quản trị thấy được dữ liệu trao đổi giữa máy tính của anh ta và máy chủ, nhưng không thấy được các trao đổi giữa những máy khác trong mạng với máy chủ. Coi như switch hoạt động tốt, điều gì đã tạo ra hiện tượng trên?

a. Switch được cấu hình VLAN

b. Trừ thông tin broadcast và unknown unicast, switch không gửi thông tin ra tất cả các cổng

c. Phần mềm Sniffer không bắt được thông tin qua cổng Ethernet

d. Phần mềm Sniffer cấu hình sai

2. Đảm bảo dữ liệu không bị sửa đổi trong quá trình lưu trữ hay trong quá trình truyền qua mạng bởi những người dùng không hợp pháp gọi là?

a. Nonrepudiation

b. Integrity

c. Confidentiality

d. Availability

3. Mặc dù báo cáo quét lỗ hổng cho thấy không có lỗ hổng nào được phát hiện, nhưng một cuộc kiểm tra thâm nhập tiếp theo cho thấy có các lỗ hổng trên mạng. Thuật ngữ nào sau đây mô tả cho trường hợp này?

a. Passive scan

b. False negative

c. Active scan

d. False positive

4. Email Server nên được đặt ở vùng mạng nào?

a. DZM

b. INSIDE

c. DMZ

d. OUTSIDE

5. Đâu là mục tiêu chủ yếu của kiểu tấn công Social Engineering?

a. Peer to Peer Network

b. Email

c. Con người

d. Local Area Network

6. Quản trị viên bảo mật thiết lập một AP mới nhưng nhận ra quá nhiều người bên ngoài có thể kết nối với AP đó và truy cập trái phép. Các cách nào sau đây sẽ là cách TỐT NHẤT để giảm thiểu vấn đề này?

a. Tất cổng kết nối có dây

b. Disable SSID broadcast

c. MAC filtering

d. Sử dụng kênh 1, 4, 7 trong cấu hình AP

e. Sử dụng 802.11ax

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

a. Role Based Access Control

b. Authentication

c. Least privilege principle

d. Authorization

e. Rule Based Access Control

8. Khái niệm bảo mật nào khuyến khích quản trị viên cài đặt tường lửa, chương trình quét phần mềm độc hại (malware scanner) và IDS trên các host?

a. Endpoint security

b. Network access control (NAC)

C. SAFE

d. VLAN

e. RADIUS

9. Mục tiêu chính của an toàn thông tin là đảm bảo các tính chất theo mô hình C-I-A là?

a. Tính chống chối bỏ

b. Tính sẵn sàng

c. Tính toàn vẹn

d. Tính dễ mở rộng

e. Tính xác thực

f. Tính bí mật

10. Hệ thống IDS/IPS phát hiện xâm nhập dựa vào các kỹ thuật nào sau đây?

a. Role-based detection

b. Anomaly-based detection

c. Classify-based detection

d. Attribute-based detection

e. Signature-based detection

11. Giải pháp StackGuard giúp phòng chống tấn công tràn bộ đệm trên stack thực hiện như sau:

a. 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.

b. Kiểm tra chiều dài dữ liệu nhập trước khi thực hiện việc gán dữ liệu

c. Kiểm tra giá trị Return Address có bị sửa đổi hay không

d. 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.

12. Kiểu tấn công nào sau đây không phải khai thác các lỗ hổng của ứng dụng Web ?

a. Cross Site Request Forgery

b. SQL Injection

c. Cross-site scripting

d. Social Engineering

13. Theo bạn giải pháp nào cần được áp dụng với các tài khoản người dùng trong hệ thống của một nhân viên nghỉ việc?

a. Vô hiệu hóa các tài khoản của nhân viên đó và xóa ngay lập tức các dữ liệu được lưu trữ

b. Duy trì các tài khoản người dùng và giữ lại các dữ liệu được lưu trữ trong một thời gian

C. Vô hiệu hóa các tài khoản của nhân viên đó và giữ lại các dữ liệu được lưu trữ trong một thời gian

d. Không sử dụng các lựa chọn nào ở đây

14. Bạn là người tư vấn giải pháp an toàn thông tin, một khách hàng của bạn quan tâm đến việc chống lại giả mạo và nhiễm độc ARP trong mạng của họ. Giải pháp nào dưới đây KHÔNG áp dụng cho mục đích này?

a. Sử dụng firewall giữa các phân vùng trong LAN

b. Sử dụng công cụ giám sát ARP trong mạng

C. Sử dụng port security trên các switch

d. Nếu trong một mạng nhỏ thì sử dụng ARP tỉnh

15. Mô hình AAA liên quan đến các chứng năng nào sau đây?

a. Authentication

b. Automation

c. Authenticity

d. Authorization

e. Accounting

f. Accessing

16. Kiểu tấn công nào sau đây không phải kiểu tấn công từ chối dịch vụ?

a. Sử dụng Botnet

b. Ping of Death

c. Main-In-The-Middle (MITM)

d. ICMP Flood

e. Teardrop

17. 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}

b. ACL(bt2) Nam: (read, write), Ha: {read, write}

c. ACL(bt2) = Nam: {read}, Ha: {read, write}

d. ACL(bt2)= Nam: (read, write), Ha: (read)

e. ACL(bt2) = Nam: (read, execute), Ha: (read, write}

18. Phát biểu nào sau đây không đúng về vùng DMZ?

a. Để nâng cao sự bảo mật cho hệ thống

b. Thường chứa email server hoặc web server

c. Chứa các server chỉ phục vụ cho người dùng bên trong

d. Là nơi đặt các public server

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

a. Subjects orientation lists

b. Access control lists

c. Objects orientation list

d. Group policy objects

e. Capability lists

20. Việc tắt các port không sử dụng trên switch hay gỡ bỏ các dịch vụ, giao thức, phần mềm không cần thiết gọi là gì?

a. Hashing

b. Hardening

c. Unused-removing

d. Auditing

e. Non-repudiation

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

a. Subjects

b. Objects

c. Rights/Permissions

d. Data

e. Security policies

22. Muốn thay thế telnet với một giao thức an toàn hơn để quản lý các thiết bị mạng, ta cần sử dụng giao thức nào sau đây?

a. SMTP

b. SSH

d. SFTP

e. SNMP

C. HTTP

23. Điều nào sau đây xảy ra khi một chuỗi dữ liệu được gửi đến bộ đệm lớn hơn bộ đệm được thiết kế để xử lý?

a. Man in the middle attack

b. SYN flood

c. Brute Force attack

d. Buffer overflow

e. Spoofing attack

24. 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 yêu cầu các bản cập nhật mới cho phần mềm trong tương lai bằng cách sử dụng giá trị hàm băm đính kèm theo

b. Khách hàng có thể xác thực tính toàn vẹn của gói cập nhật cho phần mềm sau khi download về

c. Khách hàng có thể khẳng định tính xác thực của Site mà họ download gói cập nhật về

d. Khách hàng cần giá trị của hàm băm để có thể kích hoạt được phần mềm mới

25. Điều nào sau đây mô tả đúng nhất cơ chế kiểm soát truy cập cho phép chủ sở hữu dữ liệu tạo và quản lý kiểm soát truy cập?

a. MACS (Mandatory Access Control)

b. Rule Based Access Control

c. RBACS (Role Based Access Control)

d. LBACS (List Based Access Control)

e. DACs (Discretionary Access Control)

26. Một kiểu tấn công DoS sử dụng cơ chế bắt tay ba bước (three-way handshake) của TCP là?

a. SYN Flood

b. Buffer Overflow

c. Ping of Death

d. SQL Injection

e. Brute force

27. Điều nào sau đây không đúng khi nói về lỗ hổng 0-day?

a. Là lỗ hổng phá hoại hệ thống trong vòng một ngày

b. Là lỗ hổng nguy hiểm khi tấn công vào hệ thống chưa có giải pháp bảo vệ

c. Là lỗ hổng hacker chưa công bố rộng rãi

d. Là lỗ hổng nhà sản xuất chưa kịp và

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

a. Lưu các đối số của một hàm

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

c. Lưu các biến cục bộ trong chương trình

d. Lưu mã nguồn thực thi

e. Lưu các biến static/giobal **đã** được khởi tạo trong chương trình

29. Chuẩn nào sau đây liên quan đến an toàn thông tin?

a. ISO 2600

b. ISO 9001

c. ISO 2015

d. ISO 27001

e. ISO 21997

30. Tấn công Buffer Overflow có hai loại là?

a. SQL injection và XSS

b. Stack và memory

c. Heap và stack

d. Heap và network overflow

e. Stack và SQL injection

31. Công cụ nào dùng sau đây để quét cổng của máy tính?

a. ping

b. nslookup

c. telnet

d. nmap

e. tracert

32. Mã độc Rootkit thường trú ẩn ở đâu?

a. Text file

b. RAM

c. Boot Sector

d. Operation system

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

a. Cipher feedback mode - CFB

b. Output feedback mode - OFB

c. Cipher block chaining mode - CBC

d. Electronic codebook mode – ECB

34. Giả sử thuật toán RSA đã tạo ra cặp khóa pubic (7,187) và private (23,187). Message M= 12 sẽ được mã hóa thành gì?

a. 133

b. 17

c. 121

d. 177

35. Trong mật mã khóa công khai, nếu A muốn gửi thông điệp đến B

a. Thông điệp được mã hóa bằng khóa riêng của A

b. Thông điệp được mã hóa bằng khóa công khai của A

c. Thông điệp được mã hóa bằng khóa riêng của B

d. Thông điệp được mã hóa bằng khóa công khai của B

36. 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. Diffie-Hellman

b. DES

c. ECC

d. ZUC

e. RSA

37. Tại sao hacker hay sử dụng máy chủ proxy?

a. Để có được kết nối truy cập từ xa

b. Để tạo một máy chủ ma trên mạng

c. Để tạo kết nối mạnh mẽ hơn với mục tiêu

d. Để ẩn hoạt động của chúng trên mạng

38. Thuật toán nào dưới đây không phải là thuật toán mã hóa khối?

a. AES

O b. 3DES

O C. DES

d. RC4

39. Câu nào sau đây không phải là một mô hình điều khiển truy cập?

a. Role Based Access Control

b. Attribute Based Access Control

c. Discretionary Access Control (DAC)

d. Subjective Access Control

e. Mandatory Access Control (MAC)

40. Loại malware nào sau đây có thể ẩn các tiến trình và các tập tin trên hệ thống?

a. Worm

b. Rootkit

c. Trojan

d. Adware

41. Frank rất quan tâm đến các cuộc tấn công vào máy chủ thương mại điện tử của công ty. Ông đặc biệt lo lắng về tấn công SQL Injection. Điều nào sau đây sẽ bảo vệ tốt nhất trước cuộc tấn công cụ thể này?

a. Lưu lượng truy cập web được mã hóa

b. Lọc dữ liệu người dùng nhập vào

c. Firewall

d. IDS

42. Trong mật mã khóa công khai (PKI), để xác nhận mình là người gửi thông tin, người gửi sẽ sử dụng khóa nào?

a. Session key

b. Secret key

c. Public key (Chưa chắc)

d. Private key (Phân vân)

43. Nếu bạn chia sẻ quá nhiều thông tin trên phương tiện truyền thông xã hội, bạn có thể gặp rủi ro gì?

a. Tấn công giả mạo (Phishing)

b. Mã độc (malware)

c. Ransomware

d. Đánh cấp danh tính (Identity theft)

44. Giao thức nào sau đây thuộc mã khóa công khai?

a. AES

b. 3DES

c. DES

d. RSA

45. Điều nào sau đây là rủi ro tiềm ẩn khi chương trình chạy ở chế độ đặc quyền?

a. Nó có thể cho phép mã độc được chèn vào

b. Nó có thể tạo ra việc loại bỏ các ứng dụng không cần thiết

c. Nó có thể không thực hiện việc phân chia xử lý các tác vụ

d. Nó có thể phục vụ cho việc tạo ra các đoạn mã phức tạp không cần thiết

46. Công cụ nào dưới đây có thể dùng để xác định các kết nối mạng đang có trên máy tính?

a. Netstat

b. Tracert

c. Ipconfig

d. Ping

47. Rủi ro chính từ việc sử dụng phần mềm lỗi thời (outdated software) là gì?

a. Nó có thể không còn được hỗ trợ bởi các nhà cung cấp

b. Nó có thể không có tất cả các tính năng bạn cần

c. Nó có thể không có các tính năng bảo mật hiện đại nhất

d. Có thể dễ dàng xâm nhập hơn phần mềm mới hơn

48. Máy chủ web của một công ty được cấu hình những dịch vụ sau: HTTP, SSL, FTP, SMTP. Máy chủ này được đặt trong vùng DMZ. Đâu là những cổng cần phải mở trên tường lửa để cho phép các máy trạm có thể sử dụng dịch vụ trên máy này?

a. 434, 21, 80, 25, 20

O b. 119, 23, 21, 80, 23

c. 80, 20, 21, 25, 443

d. 110, 443, 21, 59,25

49. Mục đích chính của chương trình nâng cao nhận thức bảo mật là? (ransomware)

a. Đảm bảo rằng mọi người đều hiểu chính sách và thủ tục của tổ chức

b. Thông báo cho người dùng để tuân thủ các quy định liên quan đến bảo vệ dữ liệu và thông tin

c. Thông báo cho mọi người rằng quyền truy cập vào thông tin sẽ được cấp khi người sử dụng có yêu cầu

d. Cảnh báo tất cả người dùng truy cập vào tất cả các hệ thống sẽ được theo dõi hàng ngày

50. 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, write}

c.ACL(bt2) = Nam: {read}, Ha: {read}

d.ACL(bt2) = Nam: {read, execute}, Ha: {read, write}

e.ACL(bt2) = Nam: {read, write}, Ha: {read}