# CÂU HỎI ÔN TẬP

1. . Ứng dụng mạng nào có thể được sử dụng để phân tích và kiểm tra lưu lượng mạng ?
    a. IDS
    b. FTP
    c. Router
    d. Sniffer
2. . Cần phải làm gì để bảo vệ dữ liệu trên một máy tính xách tay nếu nó bị lấy cắp ?
    a. Khóa đĩa mềm
    b. Enable khi login và tạo mật khẩu trên HĐH
    c. Lưu trữ đều đặn trên CD-ROM
    d. Mã hóa dữ liệu
3. . Ta phải làm gì để ngăn chặn một ai đó tình cờ ghi đè lên dữ liệu trên một băng từ ?
    a. Xóa nó bằng nam châm
    b. Dán nhãn cẩn thận
    c. Thiết lập tab "Write-protect "
    d. Lưu giữ nó tại chỗ
4. . Phương tiện nào sau đây không bị ảnh hưởng bởi từ tính ?
    a. Đĩa mềm
    b. CD-ROM
    c. Flash card
    d. Băng từ
5. . Yếu tố nào cần được sử dụng kết hợp với một thẻ thông minh để xác thực ?
    a. PIN
    b. Quét võng mạc
    c. Mã hóa khóa
    d. Thẻ nhớ
6. . Loại media nào sau đây không phải là một thiết bị cơ động được ?
    a. Đĩa mềm
    b. Ổ đĩa đĩa CD
    c. Thẻ thông minh
    d. Băng từ
7. . Các thiết bị hay các ứng dụng bảo mật nào sau đây nên được sử dụng để theo dõi và cảnh báo các quản trị mạng về truy cập trái phép ?
    a. Chương trình Antivirus
    b. Switch
    c. Hệ thống phát hiện xâm nhập (IDS)
    d. Dụng cụ phân tích mạng

8. Vùng nào của cấu trúc liên kết bảo mật mạng chứa các máy chủ Intenet, như là web, FTP, và các máy chủ email ?

   a. DMZ

   b. VLAN

   c. VPN

   d. Intranet

9. . Loại mạng nào mô tả cấu hình mạng bên trong của một công ty dùng cho mô hình kinh doanh B2B ( Business to Business) ?

   a. VLAN

   b. Intranet

   c. Extranet

   d. VPN

10. . Dịch vụ mạng nào cho phép các địa chỉ mạng bên trong được "che dấu"( hidden) khỏi các mạng bên ngoài và cho phép vài host của mạng bên trong sử dụng các địa chỉ trùng với mạng bên ngoài ?

    a. NAT

    b. VPN

    c. VLAN

    d. IP spoofing

11. . Công nghệ nào được sử dụng để chia một mạng bên trong thành mạng logic nhỏ hơn, dễ sử dụng hơn ?

    a. NAT

    b. Tunneling

    c. VPN

    d. VLAN

12. . Không sử dụng một liên kết chuyên dụng , phương pháp tốt nhất để kết nối hai mạng được định vị trong các văn phòng có khoảng cách địa lý xa nhau là gì ?

    a. VLAN

    b. Tường lửa

    c. DMZ

    d. VPN

13. . Sau khi cố gắng login đến một trạm làm việc trong 3 lần, một user thấy đã bị khóa bên ngoài hệ thống và không thể thực hiện bất kỳ nổ lực nào hơn nữa. Vấn đề này phù hợp nhất với điều gì ?

    a. Tường lửa disable khi truy cập đến host

    b. User quên mật khẩu của họ

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

    d. Cổng mạng disable

14. . Đặc tính nào của các thiết bị mạng như  router hay switch, cho phép điều khiển truy cập dữ liệu trên mạng ?

    a. Tường lửa

    b. Danh sách điều khiển truy cập (ACL)

c. Cập nhật vi chương trình ( Firmware)

d. Giao thức DNS

15. Phần nào của một thiết bị phần cứng có thể được nâng cấp để cung cấp khả năng bảo mật tốt hơn và đáng tin hơn ?

    a. Vi chương trình (firmware)

    b. Cấu hình tập tin

    c. A & B đều đúng

    d. A và B đều sai

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

    a. TCP/IP

    b. ICMP

    c. IPX/SPX

    d. RIP

17. . Các giao thức nào sau đây cần xóa trên một máy chủ email để ngăn chặn một user trái phép khai thác các điểm yếu bảo mật từ phần mềm giám sát mạng ?

    a. IMAP

    b. POP3

    c. TCP/IP

    d. SNMP

18. . Điều gì cần được thực hiện với một email server để ngăn chặn user bên ngoài gởi email thông qua nó ?

    a. Cài đặt phần mềm antivirus và antispam

    b. Hạn chế chuyên tiếp tín hiệu SMTP

    c. Xoá quyền truy cập POP3 và IMAP

    d. Tất cả đều sai

19. . Điều gì có thể được thiết lập trên một server DHCP để ngăn chặn các máy trạm trái phép lấy được một địa chỉ IP từ server ?

    a. Quét cổng

    b. Thiết lập "Danh sách truy cập địa chỉ MAC"

    c. DNS

    d. Tất cả đều đúng

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

    a. Email

    b. Telnet

    c. ICMP

    d. WWW

21. . Kỹ thuật cho phép tạo kết nối ảo giữa hai mạng sử dụng một giao thức bảo mật được gọi là gì ?

    a. Tunelling

    b. VLAN

    c. Internet

d. Extranet

22. . Qui trình quyết định giá trị của thông tin hay thiết bị trong một tổ chức được gọi là gì?

    a. Đánh giá rủi ro

    b. Nhận dạng chuỗi

    c. Đánh giá tài nguyên thông tin

    d. Quét các điểm yếu

23. . Khi được hỏi về các mối đe dọa cho công ty từ phía các hacker. Loại thông tin nào sau đây sẽ giúp ích nhiều nhất ?

    a. Xác minh tài sản sở hữu

    b. Đánh giá rủi ro

    c. Nhận dạng mối đe dọa

    d. Các điểm yếu

24. . Khi một user báo cáo rằng hệ thống của anh ta đã phát hiện một virus mới. Điều gì sau đây cần làm như là bước đầu tiên để xử lý tình huống này ?

    a. Kiểm tra lại tập tin diệt virus hiện hành

    b. Định dạng lại đĩa cứng

    c. Cài đặt lại hệ điều hành

    d. Disable tài khoản email của anh ta

25. . Yếu tố nào sau đây được coi là hữu ích nhất trong việc kiểm soát truy cập khi bị tấn công từ bên ngoài ?

    a. Đăng nhập hệ thống ( System logs)

    b. Phần mềm antivirus

    c. Kerberos

    d. Sinh trắc học

26. . Ta muốn cài đặt một máy chủ cung cấp các dịch vụ Web đến các máy trạm thông qua Internet. Ta không muốn để lộ mạng bên trong để tránh rủi ro. Phương pháp nào để thực hiện điều này ?

    a. Cài đặt máy chủ trong mạng Intranet

    b. Cài đặt máy chủ trong một DMZ

    c. Cài đặt máy chủ trong một VLAN

    d. Cài đặt máy chủ trong mạng Extranet

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

    a. DoS

    b. Sâu

    c. Logic Bomb (bomb ngập lụt đường truyền)

    d. Social engineering (Khai thác giao tiếp)

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

    a. DoS

    b. DDoS

    c. Sâu

    d. Tấn công UDP

29. . Một máy chủ trên mạng có một chương trình đang chạy vượt quá thẩm quyền . Loại tấn công nào đã xảy ra ?

    a. DoS

    b. DDoS

    c. Back door

    d. Social engineering (Khai thác giao tiếp)

30. . Nổ lực tấn công để can thiệp vào một phiên liên lạc bằng việc thêm vào một máy tính giữa hai hệ thống được gọi là một …….?

    a. Tấn công dạng "Man in the middle"

    b. Tấn công cửa sau

    c. Sâu

    d. TCP/IP hijacking

31. . Ta đã phát hiện ra một chứng chỉ đã hết hiệu lực vẫn đang được sử dụng nhiều lần để giành được quyền logon. Đây là loại tấn công nào ?

    a. Tấn công dạng "Man in the middle"

    b. Tấn công cửa sau

    c. Tấn công chuyển tiếp (Relay Attack)

    d. TCP/IP hijacking

32. . Một máy chủ trên mạng không chấp nhận các kết nối TCP nữa. Máy chủ thông báo rằng nó đã vượt quá giới hạn của phiên làm việc. Loại tấn công nào có thể đang xảy ra ?

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

    b. Tấn công smurf

    c. Tấn công virus

    d. TCP/IP hijacking

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

    a. TCP

    b. IP

    c. UDP

    d. ICMP

34. . Tổ đặc trách thông báo rằng họ đã nhận một cuộc gọi khẩn cấp từ phó chủ tịch đêm qua yêu cầu logon vào ID và mật khẩu của ông ta. Đây là loại tấn công gì ?

    a. Giả mạo

    b. Tấn công chuyển tiếp

    c. Social engineering (Khai thác giao tiếp)

    d. Trojan

35. . Một virus được đính kèm chính nó vào boot sector của đĩa cứng và thông báo thông tin sai về kích thước các tập tin được gọi là gì ?

    a. Virus Trojan

    b. Stealth virus (virus ẩn danh)

    c. Sâu

d. Polymorphic virus

36. . Một chương trình nằm trong một chương trình khác được cài vào hệ thống gọi là một …….

a. Trojan Horse

b. Polymorphic virus

c. Sâu

d. Armored virus

37. . Các user nội bộ báo cáo hệ thống của họ bị lây nhiễm nhiều lần. Trong mọi trường hợp virus có vẻ là cùng một loại. Thủ phạm thích hợp nhất là gì?

a. Máy chủ có thể là vật mang virus

b. Ta có một sâu virus

c. Phần mềm antivirus của ta bị sự cố

d. Tấn công DoS đang thực hiện