1. Trình tự truy cập:
   Định dạng Xác thực Cấp quyền
2. Các hệ mật khóa bí mật:
   DES; RC4; AES
3. Mục đích của tấn công XSS:
   - Đánh cắp tài khoản.
   - Đánh cắp cookie.
   - Thực hiện Click Hijacking
4. Một đoạn mã độc sử dụng các cuộc tấn công từ điển vào máy tính để có quyền truy cập vào tài khoản quản trị. Đoạn mã này sau đó liên kết các máy tính bị xâm nhập với nhau nhằm mục đích nhận các lệnh từ xa. Thuật ngữ này mô tả ĐÚNG NHẤT loại mã độc : BACKDOOR
5. Các lỗ hổng web là:
   - SQL Injection
   - Cross-Site Saipting
   - Cross-Site Request Forgery
   - Xác thực yếu
6. Mức bảo mật: TS > S > C > U
7. Để dễ dàng cấp quyền truy cập vào tài nguyên mạng cho nhân viên, bạn phải quyết định phải có một cách dễ dàng hơn là cấp cho người dùng quyền truy cập cá nhân vào tệp, máy in, máy tính và ứng dụng. Bạn nên xem xét sử dụng mô hình bảo mật: ”Kiểm soát truy cập tùy ý”.
8. Trong mật mã khóa bí mật, số lượng khóa trong hệ thống có 10 người dùng: 20
9. Mã hóa dữ liệu sử dụng mật mã khóa công khai nhằm:
   - Dữ liệu được mã hóa bằng khóa công khai, giải mã bằng khóa bí mật.
   - Từ khóa công khai không thể tìm khóa bí mật.
10. Xác thực đa nhân tố:
    - Thẻ từ, smartcard, token + mã PIN
    - Mật khẩu + mật khẩu một lần (OTP)
    - Mật khẩu + vị trí địa lý
11. Mục đích của chữ ký số:
    - Đảm bảo tính toàn vẹn
    - Đảm bảo tính xác thực
    - Đảm bảo tính bí mật
    - Đảm bảo tính chống chối bỏ
12. Phát biểu đúng về tính toàn vẹn:
    - Tính toàn vẹn của thông tin là tính chất đảm bảo thông tin không bị sửa đổi khi truyền từ điểm nguồn tới điểm đích.
    - Nhiệm vụ của đảm bảo tính toàn vẹn của thông tin là phát hiện sự sửa đổi thông tin nếu có sự sửa đổi đó.

- Việc tạo và lưu trữ một hay nhiều bản sao của thông tin giúp kiểm tra tính toàn vẹn của thông tin.

13. Tấn công Stuxnet vào nhà máy điện hạt nhật của IRAN: WORM
14. Ví dụ về rò rỉ thông tin:
    - Nhân viên bán hàng đọc được thông tin mật của công ty thương mai.
    - Từ ngoài vùng kiểm soát có thể nghe được nội dung cuộc họp của công ty, trong đó có thông tin mật, do hệ thống loa hoạt động với công suất lớn.
    - Thông tin mật của công ty bị đối thủ biết được do họ mua chuộc người trong nội bộ công ty đặt thiết bị nghe lén.
    - Thông tin mật của công ty bị đối thủ biết được do nhân viên gửi nhầm file chứa thông tin mật trong quá trình làm việc.
15. Mục tiêu của mã độc khi tấn công người dung:’
    - Thu thập dữ liệu trên máy tính.
    - Ăn cắp thông tin như mật khẩu, mã bảo mật thẻ tín dụng.
    - Sử dụng tài nguyên trên máy tính của nạn nhân (để “đào” Bitcon).
    - Mã hóa dữ liệu và đòi tiền chuộc.
    - Phá hủy dữ liệu trên máy tính nạn nhân.
    - Nghe lén thông tin như chụp màn hìn, ghi âm, quay màn hình, keylogger.
    - Sử dụng máy tính của nạn nhân để tạo một mạng botnet phục vụ cho các cuộc tấn công DDOS.
    - Sử dụng máy tính của nạn nhân để phát tán thư rác.
    - Làm hư hại thiết bị phần cứng.
16. KHÔNG phải là tính chất an toàn của thông tin:
    - Tính cấp thiết.
    - Tính chính xác
    - Tính kịp thời.
17. Hàm băm có các những tích chất sau:
    - Nén quan hệ giữa thông điệp và bản tóm lượt không phải là tương ứng 1:1.
    - Kháng tiền ảnh: từ H(x) không tìm được x.
    - Kháng tiền ảnh thứ hai: cho trước x, không thể tìm được x’ sao cho H(x) = H(x’).
    - Kháng va chạm: không thể tìm được cặp (x,y) sao cho H(x) = H(y).
18. Độ an toàn mật khẩu lớn nhất là: A2a34567
    Gồm chữ số, chữ hoa và chữ thường.
19. Loại lỗ hổng dẫn đến việc ghi dữ liệu vượt ra ngoài ranh giới bộ dự kiến:
    - Stack overflow
    - Heap overflow
20. Phát biểu đúng về sâu máy tính (WORMS):
    - Worms ghi tất cả các ký hiệu đã gõ vào một tệp văn bản.
    - Worms sự phát tán sang các hệ thống khác.
    - Worms có thể mang virus.

- Worms lây nhiễm vào đĩa cứng MBR.

21. Trong mô hình kiểm soát truy cập bắt buộc MAC có các tính chất:
    - Không ghi xuống.
    - Không đọc lên.
22. Ma trận kiểm soát truy cập (Acess Control Matrix) thuộc mô hình kiểm soát truy cập tùy chọn (DAC).
23. Biểu thức thể hiện tính trội: (2,(kinh doanh)) <= (3,(kinh doanh, lập trình viên)).
24. Phát biểu đúng về tiêu chuẩn ISO 27001:
    ISO 27001 là một tiểu chuẩn xác định các yêu cầu đối với hệ hệ thống quản lý an toàn thông tin.
25. Mô hình bảo mật RBAC sử dụng phân loại dữ liệu và phân quyền người dùng dựa trên phân loại dữ liệu.
26. Cần sử dụng hàm băm trong chữ ký số nhằm mục đích tăng độ an toàn.
27. Các công cụ đóng băng ổ đĩa:
    - Deep Freeze.
    - Shodow Defender.
    - Returnit Virtual System.
    - Reboot Restore RS.
28. Thực hiện việc gán nhãn an toàn tới các thực thể và đối tượng được áp dụng trong mô hình kiểm soát MAC.
29. Phát biểu đúng về tính bí mật:
    - Tính bí mật là một trong những tính an toàn của thông tin.
    - Đảm bảo tính bí mật thì thông tin cần đươc mã hóa.
    - Để đảm bảo tính bí mật thì chỉ cung cấp thông tin cho người có thẩm quyền.
30. Người quản trị của bạn đã đọc được về các cuộc tấn công SQL Injection… bạn muốn giới thiệu điều gì cho người quản trị.
    - Kiểm thử và vá lỗi mã nguồn web.
    - Xác thực đầu vào.
31. Mã độc tự nhân bản là: Worm, Virus.
32. Bạn nhận thấy lưu lượng truy cập đến cổng TCP 53 trên máy chủ của mình từ một địa chỉ IP không xác định là kiểu tấn công DNS poisoning.
33. Michelangelo thuộc loại virus TROJAN.
34. Tiến hành ARP poisoning mọi người kết nối với mạng không dây để tất cả lưu lượng truy cập qua máy tính xách tay hacker trước khi cố định tuyến lưu lượng truy cập vào Internet. Đây là loại tấn công **Man in the middle.**
35. Để bảo vệ chống lại cuộc tấn công vét cạn vào mật khẩu, biện pháp đối phó là: Nâng cao độ phức tạp của mật khẩu.
36. Bạn thấy một tài liệu chứa các hướng dẫn thanh toán để giải mã các tệp tin. Trong trường hợp này bạn đã nhiễm mã độc: RASOMWARE.
37. Mã xác thông điệp (MAC – Message Authentication Code) nhằm **đảm bảo tính toàn vẹn.**

38. Loại phần mềm **Antispam** giúp lọc bỏ các email rác không mong muốn.
39. Mật khẩu thuộc nhân tố xác thực là " cái người dùng biết".
40. Nhân tố xác thực chính:
    - Cái người dùng có.
    - Cái người dùng biết.
    - Cái thuộc về bản thể người dùng.

    Nhân tố xác thực phụ:

    - Đặc điểm hành vi của người dùng.
    - Vị trí người dùng.
41. Phát biểu về backdoors là: chúng là mã độc.
42. bạn lưu trữ dữ liệu trên dịch vụ lưu trữ đám mây… bạn nên áp dụng **quyền truy cập tệp** cho các tài liệu và bảng tính của bạn.
43. Một người dùng trên mạng của bạn nhân được email từ ngân hàng nói rằng đã có sự cố bảo mật tại ngân hàng. Email tiếp tục bằng cách yêu cầu người dùng đăng nhập tài khoản ngân hàng ….. Đây là loại tấn công **Phishing**