1. An toàn mạng là gì?  
   a) Chỉ là việc bảo vệ phần cứng máy tính  
   **b) Quá trình liên tục bảo vệ một đối tượng khỏi các tấn công**  
   c) Chỉ cần bảo vệ dữ liệu quan trọng  
   d) Bảo vệ người dùng khỏi virus máy tính
2. Nếu an ninh mạng không được quan tâm đúng mức, điều gì có thể xảy ra?  
   a) Không có vấn đề gì nghiêm trọng  
   b) Tăng tốc độ truy cập mạng  
   **c) Xâm nhập bất hợp pháp, đánh cắp dữ liệu**  
   d) Làm giảm chi phí bảo trì hệ thống
3. Vì sao an toàn mạng là cần thiết?  
   a) Giúp giảm thiểu chi phí mua phần mềm  
   **b) Đảm bảo hệ thống mạng hoạt động liên tục và an toàn**  
   c) Giúp tăng tốc độ xử lý của máy tính  
   d) Hạn chế việc cài đặt phần mềm mới
4. An toàn thông tin là gì?  
   **a) Khả năng bảo vệ môi trường thông tin kinh tế xã hội**  
   b) Bảo vệ chỉ riêng dữ liệu cá nhân của người dùng  
   c) Chỉ liên quan đến bảo mật mật khẩu  
   d) Tập trung vào phần cứng hệ thống
5. Điều nào không phải là mục tiêu của an toàn thông tin?  
   a) Đảm bảo việc sử dụng và phát triển thông tin  
   b) Đảm bảo lợi ích của cá nhân, tổ chức và quốc gia  
   **c) Giảm chi phí đầu tư**   
   d) Bảo vệ thông tin khỏi các cuộc tấn công
6. An toàn máy tính bao gồm bảo vệ thành phần nào?  
   a) Chỉ phần mềm hệ thống  
   b) Chỉ thiết bị phần cứng  
   **c) Phần cứng, phần mềm và dữ liệu**  
   d) Chỉ dữ liệu được mã hóa
7. An toàn mạng có nghĩa là gì?  
   **a) Bảo vệ thông tin trong không gian mạng**  
   b) Chỉ cần bảo vệ thiết bị kết nối Internet  
   c) Chỉ quan tâm đến bảo mật dữ liệu cá nhân  
   d) Tắt mạng khi không sử dụng
8. Điều nào dưới đây thuộc về an toàn máy tính?  
   a) Bảo vệ phần cứng như CPU, bộ nhớ  
   b) Bảo vệ dữ liệu và phần mềm  
   c) Bảo vệ hệ thống mạng khỏi tấn công  
   **d) Cả A, B, C**
9. Mục tiêu của hệ thống an toàn mạng là gì?  
   a) Chỉ bảo vệ dữ liệu khỏi bị đánh cắp  
   **b) Đảm bảo sự bảo mật, toàn vẹn và khả dụng**  
   c) Giảm chi phí đầu tư vào bảo mật hệ thống  
   d) Tăng tốc độ kết nối mạng
10. Tính toàn vẹn trong an toàn mạng có nghĩa là gì?  
    **a) Đảm bảo dữ liệu không bị thay đổi hay phá hoại**  
    b) Ngăn chặn người dùng truy cập vào mạng  
    c) Xóa dữ liệu không cần thiết khỏi hệ thống  
    d) Hạn chế việc sử dụng phần mềm bảo mật
11. Tính bảo mật nhằm đảm bảo điều gì?  
    **a) Dữ liệu không bị truy xuất hay theo dõi trái phép**  
    b) Người dùng có thể truy cập dữ liệu mọi lúc  
    c) Cho phép mọi người đều có quyền sử dụng hệ thống  
    d) Tăng tốc độ truyền tải dữ liệu
12. Các mối đe dọa của hệ thống mạng có thể đến từ đâu?  
    a) Chỉ từ bên ngoài hệ thống  
    b) Chỉ từ hacker chuyên nghiệp  
    **c) Cả từ bên ngoài và bên trong hệ thống**  
    d) Chỉ từ phần mềm độc hại
13. Đâu là một trong những loại mối đe dọa đối với mạng máy tính?  
    **a) Đe dọa có tổ chức và không tổ chức**  
    b) Đe dọa do virus tự động phát tán  
    c) Đe dọa do mất điện bất ngờ  
    d) Đe dọa từ các phần mềm hợp pháp
14. Đe dọa có tổ chức thường đến từ đâu?  
    **a) Hacker thành thạo và có động cơ rõ rệt**  
    b) Người dùng thông thường trong mạng  
    c) Nhân viên bảo trì hệ thống  
    d) Người dùng không có kiến thức về công nghệ
15. Đặc điểm của đe dọa không tổ chức là gì?  
    **a) Được thực hiện bởi hacker chưa có kinh nghiệm**  
    b) Luôn có mục đích rõ ràng và lâu dài  
    c) Không liên quan đến mạng máy tính  
    d) Chỉ xảy ra trong môi trường vật lý
16. Điều nào là đúng về đe dọa có tổ chức?  
    **a) Được hoạch định trước và khó phát hiện**  
    b) Không có kế hoạch rõ ràng  
    c) Chỉ xảy ra trên hệ thống nhỏ lẻ  
    d) Không liên quan đến tấn công mạng
17. Đe dọa từ bên trong mạng thường đến từ ai?  
    **a) Nhân viên có quyền truy cập hệ thống**  
    b) Chỉ từ hacker bên ngoài  
    c) Những người không liên quan đến tổ chức  
    d) Người dùng không có tài khoản trong mạng
18. Tại sao đe dọa từ bên trong mạng nguy hiểm?  
    **a) Vì người tấn công đã có quyền truy cập vào hệ thống**  
    b) Vì hệ thống mạng luôn dễ bị tấn công từ bên trong  
    c) Vì chỉ có người ngoài tổ chức mới có thể bảo vệ  
    d) Vì nó không thể bị phát hiện
19. Có bao nhiêu phần trăm các vấn đề bảo mật đến từ bên trong mạng?  
    a) 10%  
    b) 30%  
    c) 50%  
    **d) 70%**
20. Đâu là một ví dụ về đe dọa chủ động?  
    **a) Thay đổi bảng vạch đường của Router**  
    b) Nghe trộm thông tin trên đường truyền  
    c) Sao lưu dữ liệu định kỳ  
    d) Tắt máy chủ khi không sử dụng
21. Đe dọa thụ động là gì?  
    **a) Không làm thay đổi dữ liệu**   
    b) Gây thiệt hại ngay lập tức cho hệ thống  
    c) Luôn làm gián đoạn dịch vụ mạng  
    d) Không liên quan đến bảo mật thông tin
22. Đâu là ví dụ của đe dọa vô tình?  
    **a) Chế độ đặc quyền tự động đăng nhập**  
    b) Cố tình tấn công mạng trái phép  
    c) Cài đặt phần mềm gián điệp vào hệ thống  
    d) Đánh cắp dữ liệu người dùng
23. Hacker là ai?  
    **a) Người sử dụng kiến thức để thâm nhập hệ thống**   
    b) Chỉ là những lập trình viên phần mềm hợp pháp  
    c) Người không có kiến thức về bảo mật mạng  
    d) Nhân viên bảo trì hệ thống mạng
24. Hacker mũ trắng có đặc điểm gì?  
    **a) Xâm nhập với mục đích bảo mật và kiểm tra hệ thống**  
    b) Luôn thực hiện các cuộc tấn công phá hoại  
    c) Chuyên đánh cắp dữ liệu ngân hàng  
    d) Không quan tâm đến an ninh mạng
25. Hacker mũ đen thường làm gì?  
    **a) Tấn công hệ thống với mục đích xấu**  
    b) Giúp bảo vệ hệ thống khỏi nguy cơ tấn công  
    c) Là chuyên viên bảo mật trong các công ty  
    d) Chỉ nghiên cứu về công nghệ mà không tấn công hệ thống
26. Tấn công mạng là gì?  
    **a) Bất kỳ hành động nào gây hại cho hệ thống máy tính**  
    b) Chỉ bao gồm việc đánh cắp mật khẩu  
    c) Chỉ xảy ra khi hệ thống bị mất kết nối Internet  
    d) Là hoạt động vô hại với hệ thống
27. Có bao nhiêu loại tấn công mạng chính?  
    a) 2  
    **b) 3 (do thám, truy cập, dos)**  
    c) 4  
    d) 5
28. Tấn công do thám nhằm mục đích gì?  
    **a) Thu thập thông tin về hệ thống**   
    b) Phá hủy toàn bộ dữ liệu trên máy chủ  
    c) Ngăn chặn mọi truy cập vào hệ thống  
    d) Cài đặt phần mềm diệt virus tự động
29. Một trong những thông tin mà hacker thu thập khi do thám là gì?  
    **a) Địa chỉ IP**  (dịch vụ, cổng, hdh)  
    b) Số lượng người dùng trong công ty  
    c) Hình ảnh cá nhân của nhân viên  
    d) Dung lượng RAM của máy tính
30. Packet sniffer là gì?  
    **a) Một thiết bị hoặc chương trình dùng để nghe trộm dữ liệu trên đường truyền**  
    b) Công cụ giúp tăng tốc độ mạng  
    c) Phần mềm bảo vệ hệ thống khỏi hacker  
    d) Chương trình tối ưu hóa hiệu suất hệ thống
31. Hacker cần điều kiện gì để có thể nghe lén dữ liệu trên đường truyền?  
    **a) Kết nối vật lý đến đường truyền và có quyền nhận thông tin**  
    b) Có tài khoản quản trị viên của hệ thống  
    c) Cài đặt phần mềm diệt virus mạnh  
    d) Tắt tường lửa của hệ thống
32. Công cụ nào sau đây thường được sử dụng để nghe lén dữ liệu?  
    **a) Wireshark (Ngrep, Ethereal, Packet Inspector, Dsniff)**  
    b) Microsoft Word  
    c) Windows Defender  
    d) Photoshop
33. Kỹ thuật quét địa chỉ nhằm mục đích gì?  
    **a) Xác định các máy tính đang hoạt động trong mạng**  
    b) Xóa toàn bộ dữ liệu trên máy chủ  
    c) Ngăn chặn hacker xâm nhập hệ thống  
    d) Tự động cập nhật phần mềm bảo mật
34. Công cụ nào sau đây thường được sử dụng để quét địa chỉ?  
    **a) Helium pinger (Network Sonar)**  
    b) Microsoft Excel  
    c) VLC Media Player  
    d) Google Chrome
35. Khi một host không trả lời gói Ping, điều đó có thể có nghĩa là gì?  
    **a) Host không tồn tại, đang tắt hoặc hệ thống mạng chặn icmp**  
    b) Host đang gửi dữ liệu ngược lại  
    c) Hacker đã kiểm soát hoàn toàn host  
    d) Hệ điều hành của host bị lỗi
36. Kỹ thuật quét cổng nhằm mục đích gì?  
    **a) Xác định các dịch vụ mạng đang hoạt động trên hệ thống**  
    b) Tạo tường lửa để bảo vệ hệ thống  
    c) Ngăn chặn hacker sử dụng phần mềm độc hại  
    d) Dọn dẹp các file rác trong máy tính
37. Dãy số nào đại diện cho các cổng thông dụng?  
    **a) 0 – 1023**  
    b) 1024 – 49151(đăng ký)  
    c) 49152 – 65535 (dùng riêng)  
    d) 70000 – 99999
38. Công cụ nào sau đây được sử dụng để quét cổng?  
    **a) Nmap (Nessus)**  
    b) Adobe Photoshop  
    c) Google Drive  
    d) Windows Media Player
39. Kỹ thuật quét có tránh né nhằm mục đích gì?  
    **a) Quét cổng mà không để lại dấu vết trong log file**b) Xóa toàn bộ dữ liệu trên hệ thống mạng  
    c) Tăng tốc độ kết nối Internet  
    d) Chặn hacker xâm nhập hệ thống
40. Hacker có thể sử dụng phương pháp nào để tránh bị phát hiện khi quét cổng?  
    **a) Gửi gói tin gán cờ FIN trong TCP header**  
    b) Gửi email đến quản trị viên hệ thống  
    c) Cập nhật phần mềm diệt virus thường xuyên  
    d) Xóa lịch sử trình duyệt web
41. Công cụ nào hỗ trợ kỹ thuật quét tránh né?  
    **a) IPEye (Nmap,SuperScan, AWSPS)**  
    b) Microsoft Word  
    c) VLC Media Player  
    d) WinRAR
42. Kỹ thuật xác định hệ điều hành giúp hacker làm gì?  
    **a) Tìm ra hệ điều hành để khai thác lỗ hổng bảo mật**b) Tăng tốc độ mạng của hệ thống  
    c) Chặn các phần mềm độc hại tự động  
    d) Xóa dữ liệu trên thiết bị
43. Hacker dựa vào điều gì để xác định hệ điều hành của máy tính mục tiêu?  
    **a) Cách cài đặt bộ giao thức TCP/IP**   
    b) Tên người dùng trong hệ thống  
    c) Tốc độ truy cập Internet của máy tính  
    d) Hệ thống tường lửa được cài đặt
44. Công cụ nào thường được sử dụng để xác định hệ điều hành?  
    **a) Nmap (Queso)**  
    b) Adobe Photoshop  
    c) Winamp  
    d) Google Docs
45. Tấn công truy cập có mục đích gì?  
    **a) Chiếm lấy tài nguyên như file, mật khẩu, quyền điều khiển**  
    b) Cải thiện hiệu suất hệ thống  
    c) Tăng tốc độ kết nối mạng  
    d) Giúp hệ thống bảo mật hơn
46. Hacker thường làm gì trước khi thực hiện tấn công truy cập?  
    **a) Do thám để thu thập thông tin về hệ thống**   
    b) Thông báo cho quản trị viên hệ thống  
    c) Xóa toàn bộ dữ liệu trên máy chủ  
    d) Tắt kết nối Internet của hệ thống
47. Kỹ thuật ARP Spoofing được hacker sử dụng để làm gì?  
    **a) Giả mạo Gateway để nghe lén dữ liệu trong mạng LAN**  
    b) Tăng tốc độ truy cập Internet  
    c) Ngăn chặn virus xâm nhập vào hệ thống  
    d) Tạo firewall bảo vệ mạng
48. Một trong những cách có thể sử dụng để tấn công trong môi trường switch là gì?  
    **a) Làm tràn bảng CAM**   
    b) Cài đặt phần mềm diệt virus miễn phí  
    c) Giới hạn số lượng thiết bị kết nối vào mạng  
    d) Nâng cấp hệ thống bảo mật mạng
49. Kỹ thuật DNS Spoofing nhằm mục đích gì?  
    **a) Giả mạo DNS để chuyển hướng người dùng đến trang web giả mạo**  
    b) Ngăn chặn hacker truy cập hệ thống  
    c) Tăng tốc độ phản hồi của máy chủ DNS  
    d) Bảo vệ người dùng khỏi lừa đảo trực tuyến
50. Kỹ thuật tấn công sử dụng lại là gì?  
    **a) Lấy thông tin và sử dụng để tấn công sau này**  
    b) Tạo thêm lớp bảo mật cho hệ thống  
    c) Giúp tăng tốc độ xử lý mạng  
    d) Xóa sạch dữ liệu của hệ thống
51. Tấn công cướp giao dịch là gì?  
    **a) Chiếm quyền điều khiển một phiên giao dịch hợp lệ**b) Ngăn chặn hacker xâm nhập hệ thống  
    c) Tăng tốc độ kết nối Internet  
    d) Tạo firewall bảo vệ mạng
52. Điều kiện nào giúp hacker thực hiện thành công Session Hijacking?  
    **a) Chiếm được thông tin chứng thực của người dùng (cookie)**  
    b) Máy tính của hacker phải có cấu hình mạnh  
    c) Hệ thống phải có tường lửa mạnh  
    d) Người dùng phải cấp quyền truy cập cho hacker
53. Công cụ nào có thể hỗ trợ Session Hijacking?  
    **a) Juggernaut (ttywatcher, jhijack)**  
    b) Microsoft Excel  
    c) Google Drive  
    d) WinRAR
54. Kỹ thuật tấn công Man-in-the-Middle là gì?  
    **a) Chặn và thay đổi dữ liệu được truyền giữa hai bên**  
    b) Bảo vệ người dùng khỏi mã độc  
    c) Cải thiện tốc độ truyền tải mạng  
    d) Ngăn chặn tấn công DDoS
55. Công cụ nào có thể hỗ trợ tấn công Man-in-the-Middle?  
    **a) Ettercap (Burp Suite)**  
    b) Adobe Photoshop  
    c) VLC Media Player  
    d) Windows Defender
56. Kỹ thuật Backdoor là gì?  
    **a) Một chương trình giúp truy cập hệ thống mà không cần xác thực**  
    b) Phần mềm bảo vệ hệ thống khỏi hacker  
    c) Công cụ tăng tốc độ xử lý mạng  
    d) Một loại tường lửa đặc biệt
57. Một ví dụ điển hình về Backdoor là gì?  
    **a) NetBus (Subseven)**  
    b) Google Chrome  
    c) Microsoft Word  
    d) VLC Media Player
58. Kỹ thuật đánh lừa khai thác điều gì?  
    **a) Điểm yếu của con người thay vì hệ thống máy tính**  
    b) Lỗ hổng phần cứng của máy tính  
    c) Lỗi phần mềm trong hệ điều hành  
    d) Tăng tốc độ mạng của hệ thống
59. Tấn công lừa đảo thường diễn ra như thế nào?  
    **a) Hacker gửi email giả mạo**   
    b) Cài đặt phần mềm diệt virus lên hệ thống  
    c) Chặn hacker bằng tường lửa mạnh  
    d) Tăng tốc độ xử lý của máy chủ
60. Kỹ thuật giả dạng là gì?  
    **a) Giả mạo máy khác (IP, MAC, DNS) để nhận dữ liệu**   
    b) Tăng cường mã hóa dữ liệu để bảo vệ thông tin  
    c) Xóa toàn bộ dữ liệu trên hệ thống mạng  
    d) Cải thiện tốc độ xử lý của máy chủ
61. Kỹ thuật khai thác nhằm mục đích gì?  
    **a) Lợi dụng điểm yếu của hệ thống hay giao thức để tấn công**  
    b) Bảo vệ hệ thống khỏi hacker  
    c) Tăng tốc độ xử lý của máy tính  
    d) Giúp người dùng quản lý mật khẩu tốt hơn
62. Lỗi tràn bộ đệm (Buffer Overflow) là gì?  
    **a) Lỗi lập trình lợi dụng để thay đổi địa chỉ trả về và kiểm soát hệ thống**  
    b) Một phương pháp tối ưu hóa hiệu suất hệ thống  
    c) Một loại tấn công sử dụng phần mềm diệt virus  
    d) Cách bảo vệ hệ thống khỏi hacker
63. Ví dụ nổi tiếng về tấn công Buffer Overflow là gì?  
    **a) Sâu Morris (Code Red)**  
    b) Microsoft Word  
    c) Phần mềm diệt virus Norton  
    d) Hệ điều hành Windows Defender
64. Kỹ thuật tấn công mật khẩu nhằm mục đích gì?  
    **a) Đánh cắp hoặc bẻ khóa mật khẩu**   
    b) Tăng tốc độ xử lý dữ liệu trong mạng  
    c) Bảo vệ hệ thống khỏi hacker  
    d) Giúp người dùng tạo mật khẩu mạnh hơn
65. Một phương pháp tấn công mật khẩu phổ biến là gì?  
    **a) Dò tìm theo từ điển**   
    b) Mã hóa dữ liệu bằng thuật toán mạnh  
    c) Cập nhật phần mềm diệt virus  
    d) Tắt tường lửa hệ thống
66. Công cụ nào có thể được sử dụng để tấn công mật khẩu?  
    **a) John the Ripper (L0phtCrack, Brutus, Hydra, Cain And Abel)**  
    b) Microsoft Word  
    c) Google Chrome  
    d) VLC Media Player
67. Tấn công SQL Injection lợi dụng điều gì để tấn công hệ thống?  
    **a) Lỗ hổng trong kiểm tra dữ liệu đầu vào của web**  
    b) Sử dụng tường lửa mạnh để bảo vệ hệ thống  
    c) Tạo mật khẩu phức tạp hơn cho người dùng  
    d) Cập nhật phần mềm bảo mật thường xuyên
68. Hacker có thể làm gì khi thực hiện thành công một cuộc tấn công SQL Injection?  
    **a) Truy xuất, sửa đổi hoặc xóa dữ liệu trong cơ sở dữ liệu**  
    b) Tăng tốc độ truy cập Internet  
    c) Ngăn chặn các cuộc tấn công từ hacker khác  
    d) Giới hạn quyền truy cập của quản trị viên
69. Tấn công từ chối dịch vụ (DoS) có mục đích gì?  
    **a) Làm gián đoạn hoặc ngăn chặn người dùng hợp pháp truy cập dịch vụ**  
    b) Giúp tăng tốc độ xử lý mạng  
    c) Cải thiện hiệu suất hệ thống  
    d) Tạo thêm tường lửa bảo vệ mạng
70. Một kỹ thuật phổ biến trong tấn công DoS là gì?  
    **a) Làm lụt bằng SYN (SYN Flood)**  
    b) Cập nhật phần mềm bảo mật  
    c) Giới hạn quyền truy cập của người dùng  
    d) Xóa lịch sử trình duyệt web
71. Tấn công DoS SYN Flood hoạt động như thế nào?  
    **a) Gửi hàng loạt yêu cầu kết nối nhưng không hoàn tất xác thực**  
    b) Mã hóa dữ liệu để bảo vệ thông tin  
    c) Cập nhật phần mềm hệ thống để tăng cường bảo mật  
    d) Ngăn chặn hacker thực hiện tấn công SQL Injection
72. Khi máy chủ nhận quá nhiều yêu cầu SYN giả mạo, điều gì sẽ xảy ra?  
    **a) Máy chủ bị quá tải và không thể xử lý yêu cầu hợp lệ**  
    b) Máy chủ tự động chặn tất cả các kết nối từ Internet  
    c) Hệ thống mạng trở nên nhanh hơn  
    d) Người dùng có thể truy cập dịch vụ dễ dàng hơn
73. Tấn công từ chối dịch vụ phân tán (DDoS) khác gì với DoS?  
    **a) DDoS sử dụng nhiều máy tính bị kiểm soát để tấn công cùng lúc**  
    b) DoS luôn nguy hiểm hơn DDoS  
    c) DDoS chỉ có thể được thực hiện từ một máy tính duy nhất  
    d) DoS không thể bị phát hiện trong hệ thống mạng
74. Các máy tính bị kiểm soát để thực hiện DDoS được gọi là gì?  
    **a) Botnet**  
    b) Firewall  
    c) Proxy Server  
    d) Switch
75. Một số công cụ được hacker sử dụng để thực hiện DDoS là gì?  
    **a) Trinoo, Stacheldraht, TFN2K**  
    b) Microsoft Word, Excel, PowerPoint  
    c) Google Drive, Dropbox  
    d) VLC Media Player, WinRAR
76. Phần mềm có hại (Malware) là gì?  
    **a) Phần mềm gây hại hoặc đánh cắp thông tin từ hệ thống**b) Công cụ giúp tăng tốc độ Internet  
    c) Một loại phần mềm tối ưu hóa hiệu suất hệ thống  
    d) Chương trình giúp bảo vệ người dùng khỏi hacker
77. Virus máy tính có đặc điểm gì?  
    **a) Có thể tự nhân bản và lây lan từ máy này sang máy khác**  
    b) Chỉ lây nhiễm qua email  
    c) Không thể gây hại đến phần cứng  
    d) Không thể bị phát hiện bằng phần mềm diệt virus
78. Một loại virus phổ biến có thể lây qua tệp tin thực thi là gì?  
    **a) File virus**  
    b) Boot virus (lây qua đĩa mềm)  
    c) Macro virus (lây qua file office macro)  
    d) Browser virus
79. Sâu máy tính khác với virus như thế nào?  
    **a) Worm có đặc tính phá hoại mạng (chiếm băng thông, tài nguyên)**  
    b) Worm không thể tự động lây lan  
    c) Virus không thể bị phát hiện trong hệ thống mạng  
    d) Virus luôn nguy hiểm hơn worm
80. Một cách phổ biến mà worm sử dụng để lây lan là gì?  
    **a) Qua mạng và lỗ hổng bảo mật của hệ điều hành**  
    b) Qua ổ đĩa CD/DVD  
    c) Chỉ lây lan qua USB  
    d) Qua tin nhắn SMS
81. Một ví dụ về worm nổi tiếng là gì?  
    **a) Code Red**  
    b) Adobe Photoshop  
    c) Microsoft PowerPoint  
    d) VLC Media Player
82. Trojan Horse hoạt động như thế nào?  
    **a) Ngụy trang thành phần mềm hợp pháp nhưng thực hiện hành vi độc hại**  
    b) Nhân bản và lây lan như virus  
    c) Tự động sửa lỗi hệ điều hành  
    d) Tăng tốc độ truy cập Internet
83. Điểm khác biệt giữa Trojan và Virus là gì?  
    **a) Trojan không tự lây lan từ máy này sang máy khác**  
    b) Trojan có thể tự nhân bản như virus  
    c) Virus không thể bị phát hiện bằng phần mềm diệt virus  
    d) Trojan luôn vô hại với hệ thống
84. Phần mềm gián điệp (Spyware) có mục đích gì?  
    **a) Thu thập thông tin cá nhân của người dùng mà không có sự cho phép**  
    b) Bảo vệ hệ thống khỏi virus  
    c) Tăng tốc độ xử lý của máy tính  
    d) Ngăn chặn hacker xâm nhập hệ thống
85. Spyware thường lây nhiễm vào hệ thống bằng cách nào?  
    **a) Đi kèm với phần mềm miễn phí hoặc tệp tải xuống từ Internet**  
    b) Chỉ có thể lây qua email  
    c) Chỉ lây qua thiết bị USB  
    d) Không thể xâm nhập vào hệ thống mà không có sự đồng ý của người dùng
86. Phần mềm quảng cáo (Adware) là gì?  
    **a) Phần mềm tự động hiển thị quảng cáo không mong muốn**   
    b) Phần mềm diệt virus mạnh mẽ  
    c) Một loại tường lửa giúp bảo vệ hệ thống  
    d) Công cụ giúp tăng tốc độ mạng
87. Keylogger là gì (Nhóm gián điệp)?  
    **a) Phần mềm theo dõi và ghi lại thao tác bàn phím**b) Công cụ giúp tăng tốc độ gõ phím  
    c) Chương trình bảo vệ bàn phím khỏi bị hỏng  
    d) Công nghệ mã hóa bàn phím để bảo vệ dữ liệu
88. Hacker có thể sử dụng Keylogger để làm gì?  
    **a) Đánh cắp thông tin đăng nhập và dữ liệu cá nhân**   
    b) Cải thiện hiệu suất máy tính  
    c) Ngăn chặn virus tấn công hệ thống  
    d) Giúp người dùng nhớ mật khẩu dễ dàng hơn
89. Rootkit là gì (nhóm Trojan)?  
    **a) Bộ công cụ che giấu sự tồn tại của phần mềm độc hại**

b) Một phần mềm diệt virus mạnh mẽ  
c) Chương trình giúp tăng tốc độ mạng  
d) Công cụ hỗ trợ bảo trì hệ thống máy tính

1. Tại sao Rootkit nguy hiểm?  
   **a) Vì nó có thể ẩn mình trong hệ thống và khó bị phát hiện**  
   b) Vì nó giúp hệ thống hoạt động nhanh hơn  
   c) Vì nó tự động cập nhật phần mềm bảo mật  
   d) Vì nó chỉ làm chậm máy tính mà không gây hại khác
2. Cookie trên trình duyệt là gì?  
   **a) Một tệp tin nhỏ được website lưu trên máy tính để nhận diện người dùng**b) Một phần mềm diệt virus mạnh  
   c) Công cụ giúp tăng tốc độ kết nối Internet  
   d) Một loại tường lửa bảo vệ hệ thống
3. Tại sao cookie có thể là một rủi ro bảo mật?  
   **a) Vì nó lưu trữ thông tin cá nhân và có thể bị đánh cắp**  
   b) Vì nó làm giảm tốc độ xử lý của máy tính  
   c) Vì nó luôn chứa mã độc nguy hiểm  
   d) Vì nó tự động cài đặt phần mềm diệt virus
4. Kiến trúc nào là yêu cầu cơ bản của một hệ thống mạng an toàn?  
   a) TCP/IP  
   b) **AAA**  
   c) DNS  
   d) VPN
5. Kiến trúc AAA giúp nhà quản trị mạng biết được điều gì?  
   a) **Tình hình và mức độ an toàn của hệ thống**   
   b) Tốc độ đường truyền mạng  
   c) Danh sách thiết bị kết nối  
   d) Loại hệ điều hành đang sử dụng
6. AAA cung cấp những chức năng nào?  
   a) **Định danh, phân quyền và giám sát**   
   b) Chỉ giám sát hoạt động mạng  
   c) Bảo mật dữ liệu bằng mã hóa đơn giản  
   d) Tự động cập nhật phần mềm bảo mật
7. Chứng thực (Authentication) là gì?  
   a) Quá trình mã hóa dữ liệu trước khi gửi đi  
   b) **Quy trình xác minh nhận dạng số của phần gửi thông tin**  
   c) Quản lý tài nguyên mạng  
   d) Phân quyền truy cập hệ thống
8. Một điểm yếu của hệ thống giao dịch bằng tài khoản-mật khẩu là gì?  
   a) **Mật khẩu có thể bị quên, lộ hoặc dò tìm**  
   b) Mật khẩu không thể thay đổi  
   c) Hệ thống tự động chặn tài khoản sau 3 lần nhập sai  
   d) Mật khẩu có độ dài cố định
9. Chứng thực một chiều hoạt động như thế nào? (PAP)  
   a) **Client cung cấp tài khoản và mật khẩu cho Server**  
   b) Cả hai bên cùng xác thực lẫn nhau  
   c) Server gửi mã OTP cho Client để xác thực  
   d) Chỉ cần xác thực một lần duy nhất khi đăng ký
10. Chứng thực hai chiều khác với chứng thực một chiều ở điểm nào? (PAP, CHAP)  
    a) Chỉ cần xác thực trên Client  
    b) **Cả hai bên đều xác nhận với nhau bằng username và password**  
    c) Chỉ cần xác thực một lần duy nhất  
    d) Không cần sử dụng mật khẩu
11. Mục đích của chứng thực hai chiều là gì?   
    a) **Tăng cường bảo mật bằng cách yêu cầu cả hai bên xác nhận danh tính**  
    b) Giảm thời gian đăng nhập  
    c) Hạn chế số lần thay đổi mật khẩu  
    d) Tăng tốc độ kết nối Internet
12. Password Authentication Protocol (PAP) có đặc điểm gì?  
    a) **Gửi trực tiếp username và password dưới dạng plaintext**  
    b) Mã hóa mật khẩu bằng thuật toán mạnh  
    c) Chỉ chứng thực hai chiều  
    d) Bảo mật cao hơn CHAP
13. Challenge Handshake Authentication Protocol (CHAP) có ưu điểm gì so với PAP?  
    a) **Không gửi trực tiếp username và password trên đường truyền**  
    b) Không yêu cầu chứng thực  
    c) Không sử dụng mã hóa  
    d) Kém an toàn hơn PAP
14. CHAP sử dụng phương thức nào để bảo vệ dữ liệu?  
    a) **Mã hóa MD5**  
    b) Mã hóa theo thuật toán AES  
    c) Không mã hóa dữ liệu  
    d) Sử dụng mật khẩu tĩnh không thay đổi
15. Hệ thống Kerberos giúp giải quyết vấn đề gì trong chứng thực?  
    a) **Không truyền mật khẩu dưới dạng plaintext trên mạng**  
    b) Không yêu cầu nhập mật khẩu khi đăng nhập  
    c) Tăng tốc độ kết nối Internet  
    d) Chỉ hỗ trợ xác thực một chiều

\* Khóa được mã hóa có ttl ngắn.

1. Một trong những mục tiêu chính của Kerberos là gì?  
   a) **Chống lại tấn công sử dụng lại**   
   b) Hạn chế số lượng người dùng đăng nhập  
   c) Ngăn chặn tất cả các truy cập từ xa  
   d) Chặn hoàn toàn phần mềm độc hại
2. Kerberos giúp người dùng như thế nào khi truy cập nhiều dịch vụ?  
   a) **Không yêu cầu nhập lại mật khẩu cho từng dịch vụ**  
   b) Bắt buộc xác thực lại mỗi lần truy cập  
   c) Chỉ cho phép truy cập một dịch vụ duy nhất  
   d) Không hỗ trợ đăng nhập vào nhiều hệ thống
3. Hệ thống Kerberos có vai trò gì?  
   a) **Phát hành và quản lý khóa phiên để người dùng và dịch vụ có thể trao đổi thông tin**  
   b) Giám sát hoạt động mạng  
   c) Mã hóa tất cả dữ liệu truyền đi  
   d) Tự động đặt lại mật khẩu người dùng
4. Kerberos hoạt động dựa trên nguyên lý nào?  
   a) **Mã hóa sử dụng khóa**   
   b) Không sử dụng mã hóa  
   c) Lưu trữ mật khẩu dưới dạng plaintext  
   d) Chứng thực bằng sinh trắc học
5. Kerberos được tích hợp vào hệ điều hành nào?  
   a) **Solaris, Microsoft Windows, router Cisco**  
   b) Android và iOS  
   c) Chỉ hệ điều hành Linux  
   d) Chỉ hệ điều hành Windows
6. Điều kiện cần thiết để hệ thống Kerberos hoạt động hiệu quả là gì?  
   a) **Cần nhiều máy chủ để đảm bảo không ngưng trệ**   
   b) Chỉ cần một máy chủ duy nhất  
   c) Không cần đồng bộ hóa thời gian  
   d) Tất cả mật khẩu được lưu trữ dưới dạng plaintext
7. Tại sao hệ thống Kerberos cần đồng bộ hóa đồng hồ?  
   a) **Để ngăn chặn tấn công sử dụng lại**   
   b) Để tăng tốc độ kết nối mạng  
   c) Để giảm dung lượng dữ liệu truyền đi  
   d) Để giới hạn số lượng người dùng truy cập
8. Mật khẩu sử dụng một lần (OTP) giúp gì cho người dùng?  
   a) **Không phải lo lắng về việc mật khẩu bị đánh cắp hoặc mất**  
   b) Người dùng chỉ cần nhập mật khẩu một lần rồi sử dụng mãi mãi  
   c) Hệ thống tự động lưu mật khẩu cho lần sau  
   d) Không cần xác thực danh tính
9. OTP thường đi kèm với loại thiết bị nào?  
   a) **Thiết bị phần cứng**   
   b) Chỉ sử dụng trên điện thoại di động  
   c) Được lưu trên giấy để sử dụng lại  
   d) Không cần đến thiết bị phần cứng
10. OTP có thể được tạo ra bằng phương pháp nào?  
    a) **Hàm toán học, tín hiệu đồng bộ thời gian**  
    b) Dãy số cố định nhập vào hệ thống  
    c) Mật khẩu đơn giản do người dùng đặt  
    d) Lưu trữ trên hệ thống không thay đổi
11. Thẻ cứng (Token Card) là gì?  
    a) **Một giải pháp bảo mật kết hợp với chứng thực khác như PIN, mật khẩu**  
    b) Một loại thẻ nhớ để lưu trữ dữ liệu cá nhân  
    c) Một phương thức chứng thực dựa vào phần mềm  
    d) Một loại USB thông thường
12. Token Card có thể sử dụng bằng những thiết bị nào?  
    a) **PC card, USB, Bluetooth**  
    b) Chỉ có thể sử dụng trên điện thoại di động  
    c) Chỉ hoạt động trên máy tính có kết nối Internet  
    d) Không thể kết hợp với thiết bị phần cứng
13. Sinh trắc học được sử dụng để làm gì?  
    a) **Chứng thực dựa trên đặc điểm sinh học và hành vi**  
    b) Lưu trữ dữ liệu cá nhân của người dùng  
    c) Cải thiện tốc độ xử lý mạng  
    d) Ngăn chặn virus tấn công hệ thống
14. Một ví dụ về chứng thực sinh trắc học là gì?  
    a) **Nhận dạng khuôn mặt, dấu vân tay, mống mắt**  
    b) Sử dụng mật khẩu dài hơn  
    c) Nhập số PIN cố định  
    d) Chia sẻ thông tin đăng nhập với nhiều người
15. Một nhược điểm của sinh trắc học là gì?  
    a) **Thiết bị đọc không chính xác hoặc đặc điểm sinh học thay đổi**   
    b) Không thể bị làm giả  
    c) Luôn đảm bảo tính bảo mật tuyệt đối  
    d) Không cần bảo trì hoặc kiểm tra định kỳ
16. Phân quyền (Authorization) là gì?  
    a) **Xác định quyền và sự cho phép của người dùng trong hệ thống**  
    b) Chứng thực danh tính người dùng  
    c) Quản lý mật khẩu trên hệ thống  
    d) Tăng tốc độ truy cập mạng
17. Hai dạng chính của điều khiển truy cập trong phân quyền là gì?  
    a) **Điều khiển truy cập tùy quyền (DAC) và bắt buộc (MAC)**  
    b) Điều khiển truy cập vật lý và ảo  
    c) Chỉ có một loại duy nhất  
    d) Điều khiển truy cập dựa trên thời gian sử dụng
18. Điều khiển truy cập tùy quyền (DAC) là gì?  
    a) **Chủ sở hữu tài nguyên quyết định quyền truy cập**   
    b) Người dùng có quyền truy cập tất cả tài nguyên trên hệ thống  
    c) Hệ thống tự động cấp quyền truy cập cho mọi người dùng  
    d) Chỉ quản trị viên mới có quyền truy cập tài nguyên
19. Danh sách điều khiển truy cập (ACL) trong **DAC** có tác dụng gì?  
    a) **Định danh quyền truy cập cho một đối tượng**  
    b) Tự động ngăn chặn tất cả truy cập trái phép  
    c) Mã hóa toàn bộ dữ liệu trên hệ thống  
    d) Xóa toàn bộ lịch sử truy cập của người dùng
20. Điều khiển truy cập dựa theo vai trò (RBAC) trong **DAC** hoạt động như thế nào?  
    a) **Cấp quyền truy cập dựa trên vai trò trong tổ chức**  
    b) Mọi người dùng đều có cùng một mức truy cập  
    c) Người dùng không thể thay đổi quyền hạn của mình  
    d) RBAC không phân biệt giữa các vai trò khác nhau
21. Hệ điều hành nào sử dụng mô hình kiểm soát truy cập theo kiểu DAC?  
    a) **Linux và Windows**  
    b) Chỉ Windows  
    c) Chỉ Linux  
    d) Không có hệ điều hành nào
22. Điều khiển truy cập bắt buộc (MAC) khác gì so với DAC?  
    a) **Người dùng không có toàn quyền kiểm soát tài nguyên của mình**  
    b) Người dùng có thể tự do phân quyền truy cập tài nguyên  
    c) MAC chỉ áp dụng cho hệ điều hành Linux  
    d) MAC không giới hạn quyền truy cập
23. Ai quyết định quyền truy cập tài nguyên trong hệ thống sử dụng MAC?  
    a) **Người quản trị hệ thống**  
    b) Chủ sở hữu tài nguyên  
    c) Người dùng thông thường  
    d) Bất kỳ ai có tài khoản trong hệ thống
24. Hệ điều hành nào hỗ trợ MAC?  
    a) **UNIX, Linux, MS Windows, OpenBSD**  
    b) Chỉ Windows  
    c) Chỉ Linux  
    d) Chỉ hệ điều hành di động
25. Điều khiển truy cập bắt buộc (MAC) được sử dụng trong hệ thống nào?  
    a) **Hệ thống đa tầng với nhiều mức độ bảo mật khác nhau**  
    b) Hệ thống mạng cá nhân không có giới hạn quyền truy cập  
    c) Chỉ áp dụng trong các công ty nhỏ  
    d) Hệ thống không có phân cấp bảo mật
26. Để truy cập một đối tượng trong hệ thống MAC, người dùng cần gì?  
    a) **Mức độ tin cậy tương đương hoặc cao hơn yêu cầu**  
    b) Mật khẩu mặc định của hệ thống  
    c) Quyền quản trị viên  
    d) Không cần bất kỳ quyền nào
27. Chương trình ứng dụng không đáng tin trong MAC sẽ như thế nào?  
    a) **Bị hệ thống theo dõi, giám sát và kiểm soát quyền truy cập**  
    b) Được cấp quyền truy cập như mọi ứng dụng khác  
    c) Tự động được nâng cấp thành ứng dụng đáng tin  
    d) Được sử dụng mà không cần kiểm tra bảo mật
28. Điều khiển truy cập dựa trên vai trò (RBAC) hoạt động như thế nào?  
    a) **Người dùng nhận quyền truy cập thông qua vai trò thay vì được cấp trực tiếp**  
    b) Mọi người dùng có cùng một quyền truy cập  
    c) Người dùng phải yêu cầu cấp quyền riêng lẻ cho từng tài nguyên  
    d) Không có sự phân cấp quyền trong RBAC
29. Lợi ích của RBAC là gì?  
    a) **Giúp quản lý quyền truy cập dễ dàng hơn khi có nhiều hệ thống và ứng dụng**  
    b) Người dùng có thể tự do thay đổi vai trò của mình  
    c) Chỉ áp dụng trong mạng nội bộ nhỏ  
    d) Tăng tốc độ xử lý của hệ thống
30. Một nhược điểm của RBAC là gì?  
    a) **Việc thiết lập quyền truy cập có thể trở nên phức tạp với hệ thống lớn**  
    b) Không đảm bảo tính bảo mật cao  
    c) Không hỗ trợ trong hệ thống lớn  
    d) Chỉ áp dụng được cho một số ít người dùng
31. Chính sách bảo mật (Security Policy) xác định điều gì?  
    a) **Cách dữ liệu được truy xuất và yêu cầu bảo mật**  
    b) Cách tăng tốc độ xử lý của hệ thống  
    c) Cách giảm dung lượng lưu trữ dữ liệu  
    d) Cách giới hạn số lượng người dùng trong mạng
32. Mô hình bảo mật thông tin (Security Model) có vai trò gì?  
    a) **Mô tả chi tiết các chính sách bảo mật**   
    b) Xóa bỏ hoàn toàn các yêu cầu bảo mật  
    c) Tự động cấp quyền truy cập cho mọi người dùng  
    d) Ngăn chặn tất cả các truy cập từ bên ngoài
33. Mô hình Bell-LaPadula chủ yếu tập trung vào vấn đề gì?  
    a) **Bảo mật đa mức dựa trên cơ chế MAC**  
    b) Giới hạn số lượng người dùng có thể truy cập hệ thống  
    c) Cung cấp quyền truy cập tự do cho tất cả người dùng  
    d) Tăng tốc độ truyền dữ liệu trong mạng
34. Mô hình Biba khác gì so với Bell-LaPadula?  
    a) **Thêm kiểm tra tính toàn vẹn dữ liệu**  
    b) Không quan tâm đến bảo mật dữ liệu  
    c) Cho phép người dùng sửa đổi mọi thông tin  
    d) Không có sự phân cấp bảo mật
35. Mô hình Clark-Wilson nhấn mạnh điều gì?  
    a) **Bảo đảm tính toàn vẹn dữ liệu thông qua kiểm soát truy cập**   
    b) Bảo vệ quyền riêng tư cá nhân  
    c) Tăng cường tốc độ truy cập mạng  
    d) Cho phép người dùng thay đổi dữ liệu một cách tự do
36. Giám sát có mục đích gì trong an ninh mạng?  
    a) **Ghi nhận và phân tích các hoạt động xảy ra trong hệ thống**  
    b) Giới hạn quyền truy cập của người dùng  
    c) Tự động cấp quyền truy cập cho tất cả người dùng  
    d) Xóa bỏ hoàn toàn mọi dấu vết truy cập
37. Hình thức giám sát nào thường được sử dụng?  
    a) **Ghi file nhật ký, quét hệ thống, kiểm soát**   
    b) Lưu trữ tất cả dữ liệu trên máy chủ  
    c) Xóa dữ liệu người dùng sau mỗi lần đăng nhập  
    d) Giảm dung lượng lưu trữ hệ thống
38. Ghi file nhật ký có tác dụng gì?  
    a) **Ghi lại sự kiện và thời điểm xảy ra**   
    b) Tăng tốc độ xử lý của máy chủ  
    c) Xóa bỏ mọi truy cập không hợp lệ  
    d) Hạn chế quyền truy cập của người dùng
39. Log file thường được lưu dưới dạng nào?  
    a) **File text, mỗi dòng là một sự kiện**  
    b) File hình ảnh  
    c) File video  
    d) File âm thanh

\* Syslog: Server

1. Một yêu cầu quan trọng đối với file nhật ký là gì?  
   a) **Phải được lưu trữ trong thời gian dài và bảo quản cẩn thận**  
   b) Chỉ ghi lại khi có sự cố xảy ra  
   c) Tự động xóa sau mỗi lần khởi động lại hệ thống  
   d) Không cần kiểm tra hoặc sao lưu
2. Quét hệ thống có tác dụng gì?  
   a) **Theo dõi và kiểm tra các dịch vụ mạng đang hoạt động**   
   b) Tăng tốc độ truy cập Internet  
   c) Ngăn chặn mọi kết nối từ bên ngoài  
   d) Giới hạn số lượng người dùng trên hệ thống
3. Vì sao cần quét hệ thống định kỳ?  
   a) **Để phát hiện điểm yếu trong hệ thống và khắc phục**  
   b) Để xóa bỏ tất cả các kết nối từ xa  
   c) Để giảm dung lượng lưu trữ dữ liệu  
   d) Để giới hạn quyền truy cập của quản trị viên
4. Kiểm soát có ý nghĩa gì trong bảo mật?  
   a) **Theo dõi hoạt động hệ thống để phát hiện các nguy cơ bảo mật**  
   b) Tự động cấp quyền truy cập cho mọi người dùng  
   c) Xóa tất cả các file nhật ký cũ  
   d) Giới hạn số lượng thiết bị kết nối vào hệ thống
5. Tại sao chỉ kiểm tra log file sau khi có sự cố có thể là quá muộn?  
   a) **Vì nguy cơ đã xảy ra, gây thiệt hại trước khi kịp phản ứng**  
   b) Vì log file không có giá trị trong bảo mật hệ thống  
   c) Vì hệ thống sẽ tự động sửa lỗi  
   d) Vì hacker không để lại dấu vết trong log file
6. Công cụ phân tích log file giúp gì trong bảo mật?  
   a) **Phát hiện nguy cơ và cảnh báo sớm về các cuộc tấn công**  
   b) Xóa bỏ toàn bộ dữ liệu log file để tiết kiệm dung lượng  
   c) Tạo ra nhật ký giả để đánh lừa hacker  
   d) Chặn mọi kết nối Internet khi phát hiện lỗi

Chương 2

1. Điểm truy nhập (access points) là gì?  
   a) Chỉ dành cho người dùng hợp lệ  
   b) **Nơi người dùng hợp lệ và không hợp lệ truy cập vào mạng để truy xuất tài nguyên**  
   c) Chỉ có trên mạng không dây  
   d) Chỉ có trên tầng ứng dụng
2. Những vấn đề an toàn trên tầng vật lý bao gồm gì?  
   a) **Loại cáp, mạng không dây, modem**  
   b) Hệ điều hành và phần mềm bảo mật  
   c) Chỉ có firewall và IDS  
   d) Mã hóa dữ liệu truyền tải
3. Một trong những cách xâm nhập vào cáp đồng trục là gì?  
   a) **Gắn T-connector vào cáp để cài đặt thiết bị nghe lén**  
   b) Tạo firewall bảo vệ đường truyền  
   c) Chỉ có thể tấn công bằng phần mềm độc hại  
   d) Không thể nghe lén trên cáp đồng trục
4. Vì sao cách tấn công dùng T-connector dễ bị phát hiện?  
   a) **Vì khi lắp sẽ làm gián đoạn hoạt động mạng**  
   b) Vì cần có mật khẩu để truy cập vào mạng  
   c) Vì không thể gắn thiết bị vào cáp vật lý  
   d) Vì nó chỉ áp dụng cho mạng không dây
5. Cách bảo vệ cáp đồng trục khỏi bị nghe lén bằng thiết bị cảm ứng là gì?  
   a) **Cô lập và không cho tiếp xúc trực tiếp với cáp**  
   b) Tăng số lượng thiết bị kết nối vào mạng  
   c) Sử dụng mật khẩu mạnh hơn  
   d) Mã hóa toàn bộ dữ liệu truyền tải
6. Một cách phổ biến để thâm nhập vào hệ thống cáp xoắn đôi là gì?  
   a) **Gắn trực tiếp vào switch hoặc patch-panel**  
   b) Kết nối qua Bluetooth  
   c) Mã hóa gói tin truyền tải  
   d) Chỉ có thể xâm nhập bằng phần mềm độc hại
7. Cách bảo vệ switch và patch-panel trong hệ thống cáp xoắn đôi là gì?  
   a) **Tách riêng switch vào phòng quản trị mạng và có khóa**  
   b) Không cần bảo vệ vì chúng đã an toàn  
   c) Sử dụng Wi-Fi thay vì cáp vật lý  
   d) Chỉ dùng phần mềm diệt virus để bảo vệ
8. Điểm yếu lớn nhất của hệ thống cáp quang là gì?  
   a) **Các đầu nối (connector)**  
   b) Dễ bị nhiễm virus  
   c) Không thể truyền dữ liệu tốc độ cao  
   d) Cần sử dụng nhiều điện năng
9. Hacker có thể nghe lén trên cáp quang bằng cách nào?  
   a) **Chèn một bộ chia (splitter) vào đầu nối để thu thập tín hiệu**  
   b) Gắn trực tiếp thiết bị vào lõi cáp  
   c) Cắt đứt cáp để theo dõi tín hiệu  
   d) Gửi tín hiệu gây nhiễu để đọc dữ liệu
10. Vì sao cáp quang khó bị xâm nhập hơn cáp đồng trục?  
    a) **Cần có bộ thu phát tín hiệu đặc biệt**   
    b) Sử dụng điện áp cao hơn  
    c) Có thể bị phát hiện ngay khi có tín hiệu nhiễu  
    d) Không thể bị tấn công vật lý
11. Giới hạn lớn nhất của mạng không dây hồng ngoại là gì?  
    a) **Hai thiết bị phải gần nhau**  
    b) Không thể truyền dữ liệu  
    c) Không bị ảnh hưởng bởi vật cản  
    d) Bảo mật kém hơn sóng radio
12. Vì sao tấn công vào mạng hồng ngoại khó thực hiện?  
    a) **Vì hacker phải ở trong phạm vi gần giữa hai thiết bị**  
    b) Vì tín hiệu không thể bị giải mã  
    c) Vì mạng hồng ngoại không hỗ trợ truyền dữ liệu  
    d) Vì nó tự động mã hóa thông tin
13. Mạng không dây sử dụng sóng radio có nhược điểm gì?  
    a) **Bất kỳ ai trong phạm vi phủ sóng đều có thể nhận tín hiệu**  
    b) Chỉ hoạt động trong môi trường chân không  
    c) Tốc độ truyền tải rất chậm  
    d) Không thể sử dụng trong nhà
14. Cách bảo mật mạng không dây phổ biến là gì?  
    a) **Sử dụng các giao thức mã hóa như WEP và WPA**  
    b) Giảm băng thông kết nối  
    c) Giới hạn số lượng người dùng trong mạng  
    d) Không cho phép kết nối từ xa
15. Modem có nguy cơ bảo mật nào?  
    a) **Tấn công War Dialer để xâm nhập máy tính gắn trực tiếp vào Modem**  
    b) Không thể bị tấn công vì chỉ hỗ trợ mạng nội bộ  
    c) Mã hóa dữ liệu mặc định nên không thể bị xâm nhập  
    d) Luôn yêu cầu xác thực hai bước nên an toàn tuyệt đối
16. Cách bảo mật hệ thống modem tốt nhất là gì?  
    a) **Giới hạn sử dụng modem và chỉ cho phép hướng gọi đi**  
    b) Tắt modem khi không sử dụng  
    c) Chỉ sử dụng modem có tốc độ cao  
    d) Mã hóa tất cả các kết nối đầu vào
17. Thiết bị tầng 2 có đặc điểm gì nổi bật?  
    a) **Có thể ghi nhận địa chỉ MAC và chuyển dữ liệu dựa trên MAC**  
    b) Không có khả năng định tuyến dữ liệu  
    c) Chỉ hoạt động ở tầng ứng dụng của mô hình OSI  
    d) Chỉ hoạt động với mạng không dây
18. Những vấn đề an toàn trên tầng 2 bao gồm gì?  
    a) **Bridge, Switch, Wireless Access Point**  
    b) Chỉ có firewall bảo vệ thiết bị mạng  
    c) Mã hóa dữ liệu trước khi truyền đi  
    d) Tăng tốc độ truyền tải dữ liệu
19. Switch an toàn hơn Hub ở điểm nào?  
    a) **Mỗi cổng của switch chỉ nhận đúng thông tin của mình, không lan truyền toàn mạng**  
    b) Switch phát tất cả dữ liệu đến mọi cổng như Hub  
    c) Switch hoạt động mà không cần kiểm soát dữ liệu  
    d) Switch không hỗ trợ kiểm tra địa chỉ MAC
20. Tính năng SPAN (Switched Port Analyzer) trên switch dùng để làm gì?  
    a) **Copy tất cả các gói vào và ra từ một hoặc nhiều cổng để gửi đến 1 cổng**  
    b) Tăng tốc độ xử lý của switch  
    c) Mã hóa dữ liệu trong mạng  
    d) Giới hạn số lượng kết nối vào switch
21. Vì sao hacker có thể lợi dụng SPAN?  
    a) **Nếu có quyền quản trị switch có thể nghe lén trên toàn mạng**  
    b) SPAN không thể bị lợi dụng để tấn công  
    c) SPAN chỉ hoạt động trên mạng không dây  
    d) SPAN tự động ngăn chặn các truy cập trái phép
22. Hacker có thể tấn công switch bằng cách nào?  
    a) **Giả mạo gói ARP để chuyển hướng dữ liệu qua máy mình**  
    b) Ngắt kết nối vật lý của switch  
    c) Tạo firewall trên switch  
    d) Tăng băng thông mạng để làm quá tải switch
23. Khi hacker giả mạo ARP, điều gì sẽ xảy ra?  
    a) **Client1 và Client2 lưu trữ địa chỉ IP của nhau nhưng MAC của kẻ xâm nhập**  
    b) Mạng tự động phát hiện và ngăn chặn tấn công  
    c) Dữ liệu không bị ảnh hưởng  
    d) Tất cả các thiết bị trong mạng bị ngắt kết nối
24. Một hacker có thể làm gì với Access Point không được bảo mật?  
    a) **Kết nối vào WLAN mà không cần tài khoản**  
    b) Chỉ có thể nhìn thấy SSID nhưng không thể truy cập  
    c) Không thể thực hiện bất kỳ hành động nào nếu không có mật khẩu  
    d) Chỉ có thể truy cập nếu có địa chỉ MAC hợp lệ
25. Cách nào giúp bảo mật mạng không dây hiệu quả nhất?  
    a) **Ẩn SSID, cài đặt khóa, tạo bộ lọc MAC**  
    b) Giảm khoảng cách phát sóng của Access Point  
    c) Sử dụng Hub thay vì Switch  
    d) Giới hạn số lượng người dùng truy cập mạng
26. Tại sao nên sử dụng khóa mã hóa có độ dài lớn (128 bits)?  
    a) **Giúp giảm nguy cơ bị tấn công dò tìm mật khẩu**  
    b) Làm tăng tốc độ kết nối mạng  
    c) Giúp mạng không dây hoạt động ổn định hơn  
    d) Không ảnh hưởng đến bảo mật
27. Chức năng chính của các thiết bị trên tầng 3 là gì?  
    a) **Vạch đường cho các gói tin và sử dụng địa chỉ luận lý**  
    b) Quản lý địa chỉ MAC của các thiết bị trong mạng  
    c) Lưu trữ dữ liệu của người dùng  
    d) Cung cấp kết nối mạng không dây
28. Những thiết bị nào hoạt động trên tầng 3?  
    a) **Router, Remote Access Server, Layer 3 Firewall**  
    b) Switch, Hub, Access Point  
    c) Chỉ có Switch  
    d) Chỉ có Firewall
29. Tại sao tầng 3 cần có cơ chế bảo mật?  
    a) **Đế điều khiển lưu thông và chứng thực người dùng**  
    b) Vì chỉ tầng 1 và tầng 2 mới cần bảo mật  
    c) Vì tầng 3 không có chức năng định tuyến  
    d) Vì nó chỉ ảnh hưởng đến kết nối Wi-Fi
30. Router có vai trò gì trong hệ thống mạng?  
    a) **Tìm đường đi tốt nhất và ngăn chặn broadcast**  
    b) Lưu trữ dữ liệu người dùng trong hệ thống  
    c) Chỉ hoạt động như một firewall  
    d) Chỉ có nhiệm vụ cấp phát địa chỉ IP
31. Tính năng bảo mật quan trọng của router là gì?  
    a) ACL chặn gói tin dựa trên địa chỉ hoặc dịch vụ  
    b) Lọc gói tin dựa vào loại hay nội dung   
    c) Quality of Services để điều khiển lưu thông dựa theo độ ưu tiên dịch vụ  
    **d) Cả A, B, C**
32. Tại sao Telnet có thể gây nguy hiểm khi quản lý router từ xa?  
    a) **Vì mật khẩu không được mã hóa khi truyền trên mạng**  
    b) Vì Telnet không cho phép quản trị viên truy cập từ xa  
    c) Vì Telnet chỉ hoạt động trên mạng nội bộ  
    d) Vì Telnet tự động thay đổi mật khẩu mỗi lần kết nối
33. Một kiểu tấn công vào router là gì?  
    a) **Giả mạo địa chỉ của router trong mạng để gửi thông tin vạch đường sai**  
    b) Cài đặt firewall để bảo vệ router  
    c) Sử dụng giao thức an toàn hơn để truyền dữ liệu  
    d) Hạn chế số lượng kết nối đến router
34. Cách bảo vệ router khỏi bị tấn công định tuyến là gì?  
    a) **Dùng giao thức vạch đường có mã hóa và cài đặt chứng thực**  
    b) Giới hạn số lượng thiết bị trong mạng  
    c) Chỉ sử dụng router trong mạng nội bộ  
    d) Vô hiệu hóa tất cả cổng mạng trên router
35. RAS thường sử dụng giao thức nào để kết nối?  
    a) **Dial-up hoặc VPN**  
    b) Ethernet  
    c) Bluetooth  
    d) Wi-Fi

\* RAS sử dụng chứng thực: PAP, SPAP, CHAP, EAP( thêm smartcard, sinh trắc), RADIUS

1. Mandatory Callback trong RAS hoạt động như thế nào?  
   a) **Chỉ cho phép kết nối từ một số điện thoại được xác định trước**  
   b) Tự động cấp quyền truy cập cho tất cả người dùng  
   c) Giới hạn thời gian kết nối của người dùng  
   d) Yêu cầu nhập mật khẩu nhiều lần trước khi truy cập
2. Lợi ích của chứng thực hai chiều trong RAS là gì?  
   a) **Server sẽ gọi lại Client sau khi xác thực thành công để đảm bảo tính bảo mật**  
   b) Tăng tốc độ kết nối mạng  
   c) Giảm dung lượng dữ liệu được truyền qua mạng  
   d) Hạn chế số lượng thiết bị có thể kết nối
3. Cách nào giúp bảo mật RAS hiệu quả?  
   a) **Chỉ cho phép giao thức cần thiết và khóa các giao thức khác**  
   b) Chặn tất cả các kết nối từ xa  
   c) Không sử dụng mật khẩu khi truy cập  
   d) Tăng số lượng cổng mở để dễ dàng kết nối
4. Chức năng chính của firewall là gì?  
   a) **Ngăn chặn truy cập trái phép từ bên ngoài và kiểm soát truy cập từ bên trong**  
   b) Tăng tốc độ truyền tải dữ liệu  
   c) Cấp phát địa chỉ IP động cho các thiết bị trong mạng  
   d) Kiểm tra tốc độ kết nối Internet
5. Firewall có thể được chia thành những dạng nào?  
   a) **Lọc gói, lọc nội dung, duyệt trạng thái**  
   b) VPN, Telnet, SSH  
   c) Chỉ có phần cứng firewall, không có firewall phần mềm  
   d) Hub, Switch, Router
6. Firewall lọc gói hoạt động như thế nào?  
   a) **Dựa trên địa chỉ IP hoặc số cổng**   
   b) Mã hóa tất cả dữ liệu truyền tải  
   c) Chỉ giám sát mạng mà không thực hiện hành động ngăn chặn  
   d) Tự động cấp quyền truy cập cho mọi kết nối
7. Có bao nhiêu cơ chế thực hiện lọc gói trong firewall?  
   a) **Hai cơ chế: mặc nhiên cho phép và mặc nhiên cấm**   
   b) Ba cơ chế: mã hóa, giám sát và ghi log  
   c) Chỉ có một cơ chế duy nhất là chặn tất cả truy cập  
   d) Không có cơ chế nào, firewall tự động hoạt động theo mặc định
8. Chính sách bảo mật tốt nhất khi cấu hình firewall là gì?  
   a) **Mặc nhiên cấm tất cả truy cập trừ khi có quy tắc cho phép cụ thể**   
   b) Cho phép tất cả truy cập mặc định  
   c) Không cần cấu hình firewall nếu hệ thống có phần mềm diệt virus  
   d) Firewall chỉ cần hoạt động trên mạng nội bộ, không cần bảo vệ truy cập Internet
9. Firewall trên tầng 3 có ưu điểm gì?  
   a) **Tốc độ nhanh vì chỉ kiểm tra header của gói tin**  
   b) Tự động mã hóa dữ liệu truyền đi  
   c) Không cần cấu hình, hoạt động hoàn toàn tự động  
   d) Chặn tất cả các kết nối mạng
10. Một hạn chế của firewall trên tầng 3 là gì?  
    a) **Không quan tâm đến nội dung, bỏ sót gói độc hại (khó mở riêng 1 cổng cho 1 ứng dụng)**  
    b) Không thể kiểm soát lưu lượng mạng  
    c) Không hỗ trợ chặn địa chỉ IP  
    d) Chỉ hoạt động với các thiết bị không dây
11. Vì sao firewall trên tầng 3 dễ sử dụng?  
    a) **Các quy tắc rõ ràng và đơn giản**  
    b) Không yêu cầu cấu hình  
    c) Chỉ có một chế độ hoạt động duy nhất  
    d) Không cần cập nhật theo thời gian
12. Những vấn đề an toàn trên tầng 4 và cao hơn bao gồm gì?  
    a) **Proxy Server, Máy trạm, Máy chủ**   
    b) Chỉ có router và firewall  
    c) Mã hóa tất cả dữ liệu trên mạng  
    d) Chỉ tập trung vào phần cứng mạng
13. Vì sao tầng 4 và các tầng cao hơn cần bảo mật?  
    a) **Vì đây là nơi hệ điều hành và ứng dụng hoạt động**  
    b) Vì chỉ có tầng 3 mới quan trọng trong bảo mật  
    c) Vì không liên quan đến người dùng cuối  
    d) Vì chỉ ảnh hưởng đến tốc độ kết nối
14. Cách tốt nhất để bảo mật tầng 4 và cao hơn là gì?  
    a) **Cấu hình bảo mật cho từng hệ điều hành và ứng dụng riêng biệt**  
    b) Chặn tất cả truy cập mạng  
    c) Giảm số lượng người dùng truy cập vào hệ thống  
    d) Không cần bảo vệ vì đã có firewall
15. Proxy Server có chức năng gì?  
    a) **Bảo vệ mạng nội bộ và kiểm soát truy cập tài nguyên bên ngoài**  
    b) Chỉ có chức năng tăng tốc độ mạng  
    c) Không có tác dụng trong bảo mật  
    d) Chỉ lưu trữ dữ liệu của người dùng
16. Lợi ích quan trọng của Proxy Server là gì?  
    a) Tăng tốc độ truy cập web nhờ cơ chế lưu cache  
    b) Giám sát lưu thông nhờ lưu log  
    c) Lọc gói tin theo giao thức, địa chỉ  
    **d) Cả A, B, C**
17. Điểm yếu của Proxy Server là gì?  
    a) **Nếu kết hợp với các chức năng khác có thể tạo ra lỗ hổng bảo mật**  
    b) Không thể lọc nội dung truy cập  
    c) Không thể theo dõi lưu lượng mạng  
    d) Không thể chặn truy cập từ bên ngoài
18. Vì sao máy trạm dễ bị tấn công hơn máy chủ?  
    a) **It quan tâm đến bảo mật**   
    b) Máy trạm không thể cài đặt phần mềm bảo mật  
    c) Máy trạm luôn an toàn hơn máy chủ  
    d) Máy trạm không kết nối với mạng nên không bị tấn công
19. Một số lỗi bảo mật phổ biến mà người dùng máy trạm mắc phải là gì?  
    a) **Không thay đổi mật khẩu thường xuyên, cập nhật phần mềm diệt virus**  
    b) Luôn cập nhật phần mềm bảo mật kịp thời  
    c) Không cài đặt phần mềm không rõ nguồn gốc  
    d) Không mở email từ người lạ
20. Cách nào giúp tăng cường bảo mật cho máy trạm?  
    a) **Cập nhật bản vá, tường lửa và chính sách sử dụng nghiêm ngặt**  
    b) Không cần bảo vệ vì máy trạm ít quan trọng  
    c) Giới hạn số lượng thiết bị kết nối vào mạng  
    d) Không cài đặt phần mềm bảo mật để tránh xung đột hệ thống
21. Vì sao Server là mục tiêu tấn công chính của hacker?  
    a) **Vì chứa thông tin quan trọng mà hacker muốn đánh cắp**  
    b) Vì nó có tốc độ xử lý nhanh hơn máy trạm  
    c) Vì nó chỉ hoạt động nội bộ nên dễ bị xâm nhập  
    d) Vì không có cơ chế bảo vệ nào
22. Máy chủ có nguy cơ bị tấn công từ đâu?  
    a) **Từ chính các dịch vụ mà nó cung cấp**  
    b) Chỉ từ mạng nội bộ  
    c) Chỉ từ tấn công vật lý trực tiếp  
    d) Chỉ từ người dùng có tài khoản quản trị
23. Cách bảo vệ máy chủ hiệu quả nhất là gì?  
    a) **Đặt máy chủ sau firewall, có bảo vệ vật lý và cập nhật phần mềm thường xuyên**  
    b) Không sử dụng firewall để tránh chặn kết nối  
    c) Chỉ cập nhật phần mềm khi có lỗi nghiêm trọng  
    d) Giới hạn số lượng người dùng kết nối vào máy chủ

Chương 3

1. Gia cố hệ thống nhằm mục đích gì?  
   a) Làm cho hệ thống hoạt động nhanh hơn  
   b) Bảo vệ hệ thống khỏi virus  
   **c) Làm cho hệ thống vững chắc hơn, khó bị tấn công hơn**  
   d) Giúp hệ thống dễ dàng truy cập hơn
2. Những đối tượng nào cần được gia cố?  
   a) Hệ điều hành  
   b) Hệ điều hành mạng  
   c) Ứng dụng mạng  
   **d) Cả A, B, C**
3. Khi hệ thống được gia cố tốt, kẻ xâm nhập sẽ làm gì?  
   a) Tiếp tục tấn công cho đến khi thành công  
   **b) Bỏ ý định tấn công và tìm mục tiêu dễ dàng hơn**  
   c) Báo cáo lỗi hệ thống  
   d) Cài đặt phần mềm diệt virus
4. Gia cố cơ sở hạ tầng mạng giúp:  
   a) Cải thiện tốc độ truy cập mạng  
   **b) Cung cấp các tầng bảo vệ**c) Làm hệ thống dễ bị tấn công hơn  
   d) Giảm chi phí vận hành hệ thống
5. Những yếu tố nào quan trọng khi gia cố hệ điều hành?  
   **a) Hệ thống tập tin, cập nhật, hotfix, service pack, patch**  
   b) Chỉ cần cập nhật phần mềm diệt virus  
   c) Cài đặt thêm nhiều ứng dụng mạng  
   d) Xóa bỏ mọi phần mềm bảo mật
6. Patch trong hệ điều hành có chức năng gì?  
   a) Cải thiện tốc độ xử lý dữ liệu  
   **b) Vá lỗi và giải quyết các vấn đề bảo mật**  
   c) Xóa bỏ dữ liệu không cần thiết  
   d) Tăng dung lượng lưu trữ
7. Người dùng nên được cấp quyền như thế nào?  
   a) Quyền truy cập cao nhất để dễ dàng làm việc  
   **b) Vừa đủ để hoàn thành công việc**  
   c) Không cần cấp quyền truy cập  
   d) Cấp toàn bộ quyền để tránh nhầm lẫn
8. Tại sao cần phải nhóm người dùng có cùng yêu cầu truy cập?  
   **a) Dễ dàng quản lý quyền truy cập**  
   b) Tránh việc mất dữ liệu  
   c) Tăng tốc độ hệ thống  
   d) Không có tác dụng gì
9. Sau khi xác định rủi ro từ các phương thức truy cập, quản trị viên nên làm gì?  
   **a) Thiết lập chính sách điều khiển truy cập và các loại chứng thực**  
   b) Xóa tài khoản của người dùng không cần thiết  
   c) Cài đặt lại toàn bộ hệ thống  
   d) Không cần thực hiện hành động nào
10. Một bản cập nhật có thể bao gồm:  
    a) Nâng cao khả năng hoạt động   
    b) Bổ sung thêm tính năng mới  
    **c) Cả hai đáp án trên**  
    d) Không có tác dụng gì
11. Điểm khác biệt giữa **Update** và **Upgrade** là gì?  
    **a) Update miễn phí, Upgrade có tính phí**  
    b) Update bổ sung tính năng mới, Upgrade chỉ sửa lỗi  
    c) Cả hai đều miễn phí  
    d) Không có sự khác biệt
12. Hotfix thường được sử dụng trong trường hợp nào?  
    **a) Sửa một số vấn đề trên số ít máy trạm hoặc server**  
    b) Nâng cấp hệ điều hành  
    c) Cài đặt phần mềm diệt virus  
    d) Thay đổi phần cứng hệ thống
13. Hotfix có thể có nhược điểm gì?  
    a) Có thể gây gián đoạn hệ thống  
    b) Chỉ được kiểm thử trên một số ít thiết bị  
    c) Không đảm bảo hoạt động tốt trên tất cả các hệ thống  
    **d) Cả B và C**
14. Khi nào nên cài đặt Hotfix?  
    a) Ngay lập tức khi có bản mới  
    **b) Khi thật sự cần thiết**  
    c) Sau khi hệ thống bị tấn công  
    d) Không bao giờ
15. Bản vá lỗi (patch) thường được sử dụng để làm gì?  
    **a) Chỉnh sửa tạm thời các lỗi trong hệ điều hành**  
    b) Tăng tốc độ xử lý của máy tính  
    c) Cải thiện giao diện đồ họa  
    d) Xóa các tập tin rác trong hệ thống
16. So với bản cập nhật, bản vá lỗi có đặc điểm gì?  
    a) An toàn hơn và được kiểm thử trên nhiều hệ thống  
    **b) Không an toàn như bản cập nhật và cần backup trước khi cài đặt**  
    c) Hoàn toàn miễn phí và không cần kiểm tra trước khi cài đặt  
    d) Chỉ được sử dụng trên hệ điều hành cũ
17. Service Pack bao gồm những gì?  
    a) Chỉ các bản vá lỗi  
    **b) Tổng hợp update, hotfix, patch**   
    c) Phần mềm diệt virus  
    d) Một hệ điều hành mới
18. Ứng dụng mạng thường trở thành mục tiêu của hacker vì lý do nào?  
    **a) Dễ bị khai thác do các điểm yếu được công bố**  
    b) Hacker muốn giúp cải thiện bảo mật hệ thống  
    c) Ứng dụng mạng không có giá trị với hacker  
    d) Hệ điều hành có thể thay thế ứng dụng mạng
19. Tại sao một hệ điều hành an toàn vẫn có thể bị tấn công khi sử dụng dịch vụ mạng?  
    **a) Dịch vụ mạng có thể có lỗ hổng bảo mật**  
    b) Hệ điều hành không quan trọng trong bảo mật  
    c) Hacker chỉ nhắm vào hệ điều hành  
    d) Dịch vụ mạng giúp bảo vệ hệ thống khỏi tấn công
20. Hacker thường quan tâm đến Web Server vì lý do nào?  
    **a) Đây là điểm duy nhất có thể tấn công**   
    b) Web Server không có giá trị gì với hacker  
    c) Hacker không thể truy cập Web Server  
    d) Web Server không chứa thông tin quan trọng
21. Một bước quan trọng trong việc gia cố Web Server là gì?  
    **a) Đặt Website sau tường lửa hoặc proxy**  
    b) Xóa toàn bộ dữ liệu trên Web Server  
    c) Không cần cài đặt biện pháp bảo mật  
    d) Sử dụng hệ điều hành cũ hơn để tránh lỗi
22. Tại sao nên sử dụng chứng thực SSL trên Web Server?  
    **a) Giúp mã hóa dữ liệu truyền qua mạng**  
    b) Tăng tốc độ tải trang web  
    c) SSL không có tác dụng trong bảo mật  
    d) SSL giúp hacker dễ dàng truy cập hơn
23. Mail Server có thể bị tấn công theo những hình thức nào?  
    **a) DoS, Virus, giả mạo, Relay**  
    b) Chỉ có DoS  
    c) Chỉ bị tấn công bởi virus  
    d) Không thể bị tấn công
24. Một biện pháp quan trọng để bảo vệ Mail Server là gì?  
    **a) Cài đặt chương trình diệt virus dành riêng cho Server**  
    b) Tắt toàn bộ dịch vụ Mail Server  
    c) Không cho phép gửi email ra ngoài  
    d) Xóa tất cả email định kỳ
25. Tại sao cần cấu hình Relay Server chỉ cho phép người dùng hợp lệ gửi mail?  
    **a) Ngăn chặn việc sử dụng Mail Server để gửi spam**  
    b) Giúp tăng tốc độ gửi email  
    c) Giảm dung lượng lưu trữ email  
    d) Không có tác dụng gì
26. Vì sao giao thức FTP không an toàn?  
    **a) Gửi thông tin chứng thực ở dạng plaintext**  
    b) Mã hóa dữ liệu mạnh mẽ  
    c) Chỉ hoạt động trong mạng nội bộ  
    d) Không liên quan đến bảo mật
27. Biện pháp nào giúp gia cố bảo mật cho FTP Server?  
    a) Cấu hình cẩn thận tài khoản anonymous  
    b) Tách biệt tài khoản FTP và tài khoản người dùng  
    c) Cô lập đĩa FTP và đĩa chứa hệ thống  
    **d) Cả A, B, C**
28. Một kiểu tấn công phổ biến vào DNS Server là gì?  
    **a) Đánh lừa người dùng truy cập vào địa chỉ giả mạo**  
    b) Gửi email spam  
    c) Giảm hiệu suất mạng  
    d) Chặn toàn bộ kết nối Internet
29. Biện pháp bảo vệ DNS Server là gì?  
    a) Tách biệt hệ thống tên miền Internet và hệ thống miền cục bộ  
    b) Cập nhật giữa DNS Server trong vùng zone cho phép  
    c) ACL cho người dùng  
    **d) Cả A, B, C**
30. Tại sao cần yêu cầu DNS Server chứng thực lẫn nhau?  
    **a) Đảm bảo tính toàn vẹn và an toàn của DNS**  
    b) Giúp tăng tốc độ xử lý DNS  
    c) Giảm tải cho hệ thống mạng  
    d) Không cần thiết vì DNS tự động an toàn
31. Tại sao việc chia sẻ tài nguyên có thể gây rủi ro bảo mật?  
    **a) Người dùng không quản lý chặt chẽ quyền truy cập**  
    b) Máy in có thể bị hỏng  
    c) Hệ thống sẽ chạy chậm hơn  
    d) Không có rủi ro nào liên quan
32. Một trong những biện pháp gia cố Server chia sẻ file và máy in là gì?  
    **a) Tạo Server chuyên dụng cho việc chia sẻ tài nguyên**  
    b) Cho phép mọi người truy cập tự do  
    c) Xóa tất cả các file chia sẻ  
    d) Không sử dụng mạng nội bộ
33. Khi không sử dụng dịch vụ chia sẻ file và máy in, nên?  
    **a) Tắt dịch vụ trên Server và máy trạm**  
    b) Giữ nguyên trạng thái để tránh ảnh hưởng đến hệ thống  
    c) Chia sẻ toàn bộ dữ liệu với mọi người dùng  
    d) Cập nhật hệ điều hành mà không thay đổi thiết lập
34. Một biện pháp giúp bảo mật DHCP Server là gì?  
    **a) Dành chỗ và dùng bộ lọc địa chỉ MAC**   
    b) Cho phép tất cả thiết bị kết nối không giới hạn  
    c) Tắt DHCP hoàn toàn  
    d) Không quan tâm đến bảo mật DHCP
35. Database Server có những nguy cơ bảo mật nào?  
    **a) Nhiều hdh, port khác nhau**   
    b) Không có nguy cơ bảo mật nào  
    c) Chỉ bị tấn công nếu sử dụng phần mềm lỗi thời  
    d) Hacker không thể tấn công Database Server
36. Một trong những biện pháp quan trọng khi gia cố Database Server là gì?  
    **a) Cấu hình đúng dịch vụ và sử dụng mật khẩu mạnh**  
    b) Không cần quan tâm đến bảo mật Database Server  
    c) Chỉ dùng mật khẩu đơn giản để dễ nhớ  
    d) Cho phép tất cả người dùng truy cập dữ liệu
37. Tại sao cần backup dữ liệu Database Server định kỳ?  
    **a) Để khôi phục dữ liệu khi xảy ra sự cố**  
    b) Giảm tốc độ hoạt động của hệ thống  
    c) Xóa dữ liệu không cần thiết  
    d) Không có tác dụng gì
38. Chính sách an ninh mạng là gì?  
    **a) Quy định những thao tác nào trên mạng được xem là đúng**  
    b) Chỉ áp dụng cho hệ thống máy chủ  
    c) Không liên quan đến bảo mật thông tin  
    d) Chỉ tập trung vào bảo vệ phần cứng
39. Chính sách an ninh mạng bao gồm những quy tắc nào?  
    **a) Những thao tác cho phép và không cho phép**  
    b) Chỉ quy định việc sử dụng phần mềm  
    c) Không có quy tắc cụ thể  
    d) Chỉ áp dụng cho người quản trị hệ thống
40. Chính sách giới hạn truy cập giúp:  
    **a) Hạn chế quyền truy cập theo yêu cầu công việc**  
    b) Cung cấp quyền truy cập tối đa cho tất cả người dùng  
    c) Cho phép nhân viên tự do truy cập bất kỳ dữ liệu nào  
    d) Không ảnh hưởng đến bảo mật hệ thống
41. Một phương pháp phổ biến để giới hạn truy cập Internet là gì?  
    **a) Yêu cầu tài khoản và mật khẩu**  
    b) Cho phép truy cập không giới hạn  
    c) Chặn toàn bộ kết nối mạng  
    d) Không có phương pháp nào
42. VPN thường yêu cầu yếu tố nào để xác thực người dùng?  
    **a) Username, PIN, token**   
    b) Chỉ cần nhập username  
    c) Không cần xác thực  
    d) Mật khẩu mặc định của hệ thống
43. Máy trạm là gì?  
    **a) Máy tính kết nối vào mạng và sử dụng tài nguyên mạng**  
    b) Máy chủ quản lý toàn bộ hệ thống  
    c) Chỉ là thiết bị lưu trữ dữ liệu  
    d) Không liên quan đến bảo mật mạng
44. Chính sách an ninh cho máy trạm bao gồm những vấn đề nào?  
    **a) Lưu trữ file và cài đặt phần mềm**  
    b) Tắt máy khi không sử dụng  
    c) Xóa dữ liệu hàng ngày  
    d) Giới hạn số lần đăng nhập
45. Việc sử dụng thiết bị di động trong môi trường làm việc cần:  
    **a) Được kiểm soát để đảm bảo an toàn dữ liệu**  
    b) Không cần bất kỳ hạn chế nào  
    c) Cấm hoàn toàn tất cả thiết bị di động  
    d) Chỉ cần đăng ký với quản trị viên
46. Chính sách an ninh vật lý nhằm mục đích gì?  
    **a) Giới hạn truy cập vật lý để giảm nguy cơ tấn công**b) Chỉ áp dụng cho hệ thống phần mềm  
    c) Không quan trọng trong bảo mật  
    d) Chỉ áp dụng cho mạng không dây
47. Bước đầu tiên trong quá trình xây dựng chính sách an ninh mạng là gì?  
    **a) Phân tích rủi ro**  
    b) Cài đặt phần mềm diệt virus  
    c) Mua thiết bị bảo mật mới  
    d) Khóa tài khoản người dùng
48. Chính sách an ninh mạng gồm những thành phần nào?  
    **a) Quy định về quyền truy cập, bảo vệ dữ liệu, và giám sát hệ thống**  
    b) Chỉ quy định về mật khẩu  
    c) Chỉ áp dụng cho quản trị viên hệ thống  
    d) Không cần thành phần cụ thể nào
49. Quan tâm xứng đáng (Due Care) trong chính sách an ninh có nghĩa là gì?  
    **a) Người quản lý phải có trách nhiệm bảo vệ tài sản đó**  
    b) Chỉ cần bảo vệ dữ liệu, không cần bảo vệ thiết bị  
    c) Chỉ áp dụng cho hệ thống mạng nội bộ  
    d) Không liên quan đến an ninh mạng
50. Một trong những biện pháp của Due Care là gì?  
    **a) Sao lưu dữ liệu định kỳ**  
    b) Xóa tất cả dữ liệu mỗi ngày  
    c) Không cần quan tâm đến bảo trì hệ thống  
    d) Cấm nhân viên sử dụng email
51. Tại sao cần giám sát và ghi nhận sự kiện trong hệ thống?  
    **a) Để phát hiện và phân tích các cuộc tấn công**  
    b) Để theo dõi thời gian làm việc của nhân viên  
    c) Để tăng tốc độ truy cập mạng  
    d) Không cần thiết vì hệ thống tự bảo vệ
52. Người quản trị hệ thống có quyền gì trong việc giám sát hệ thống mạng?  
    **a) Theo dõi hoạt động trên hệ thống kể cả riêng tư**  
    b) Không có quyền giám sát bất kỳ hoạt động nào của người dùng  
    c) Chỉ giám sát khi có sự cho phép của từng nhân viên  
    d) Chỉ giám sát phần cứng, không theo dõi phần mềm
53. Tách biệt phận sự trong an ninh mạng có nghĩa là gì?  
    **a) Mỗi người chỉ được cấp quyền phù hợp với nhiệm vụ của mình**  
    b) Mọi nhân viên đều có quyền truy cập toàn bộ hệ thống  
    c) Không cần phân biệt quyền giữa các nhóm nhân viên  
    d) Chỉ áp dụng cho các hệ thống quan trọng
54. Một lợi ích của tách biệt phận sự là gì?  
    **a) Giúp dễ dàng xác định nguyên nhân khi có sự cố xảy ra**b) Giảm thời gian làm việc của nhân viên  
    c) Giúp hacker dễ dàng tấn công hệ thống  
    d) Không có lợi ích gì trong an ninh mạng
55. Hệ điều hành nào hỗ trợ việc tách biệt phận sự trong quản trị hệ thống?  
    **a) Windows 2000/2003 với Active Directory**  
    b) Windows XP  
    c) Linux Ubuntu  
    d) Không có hệ điều hành nào hỗ trợ
56. Chính sách "Cần biết" có nghĩa là gì?  
    **a) Chỉ cung cấp vừa đủ thông tin cho người có nhu cầu**   
    b) Mọi nhân viên có thể truy cập tất cả thông tin của công ty  
    c) Không cần giới hạn quyền truy cập vào dữ liệu  
    d) Cho phép nhân viên sử dụng thông tin tùy ý
57. Khi cài đặt Windows 2003, hệ thống yêu cầu gì để đảm bảo nguyên tắc "Cần biết"?  
    **a) Xác định nhu cầu của người dùng trước khi cấp quyền**  
    b) Cấp quyền truy cập mặc định cho tất cả nhân viên  
    c) Không yêu cầu bất kỳ xác thực nào  
    d) Tự động cấp quyền cao nhất cho tất cả tài khoản
58. Chính sách an ninh mạng của một tổ chức có thể được thiết lập dựa trên điều gì?  
    **a) Yêu cầu cụ thể của tổ chức**  
    b) Mặc định từ nhà sản xuất hệ điều hành  
    c) Quy định của hacker  
    d) Chính sách bảo mật của các tổ chức khác
59. Lợi ích của việc sử dụng các mẫu chính sách an ninh chuẩn hóa là gì?  
    **a) Giúp nhanh chóng xây dựng chính sách phù hợp**  
    b) Không cần quan tâm đến bảo mật nữa  
    c) Cho phép tất cả nhân viên truy cập dữ liệu tùy ý  
    d) Giảm chi phí phần cứng
60. Chính sách AUP (acceptable use policies) quy định điều gì?  
    **a) Những hoạt động được phép khi sử dụng máy tính và mạng**  
    b) Cách tăng tốc độ kết nối Internet  
    c) Chỉ áp dụng cho quản trị viên hệ thống  
    d) Không có tác dụng gì trong bảo mật
61. Một nội dung quan trọng trong chính sách AUP là gì?  
    **a) Không sử dụng tài nguyên mạng để đe dọa hoặc tấn công**   
    b) Cho phép truy cập không giới hạn vào tất cả các trang web  
    c) Không cần quản lý việc sử dụng tài nguyên mạng  
    d) Chỉ áp dụng cho hệ điều hành Windows
62. Chính sách AUP thường được thiết lập dưới dạng nào?  
    **a) Hợp đồng giữa công ty và nhân viên**  
    b) Một bài báo trên Internet  
    c) Chỉ là một quy tắc miệng  
    d) Một hướng dẫn không bắt buộc
63. Bao lâu thì mật khẩu nên được thay đổi theo chính sách bảo mật?  
    **a) 45 - 90 ngày**  
    b) Mỗi năm một lần  
    c) Không cần thay đổi nếu không bị lộ  
    d) Khi hệ thống yêu cầu
64. Chứng chỉ số có tác dụng gì trong bảo mật?  
    **a) Đảm bảo thông tin truyền đi đến đúng người nhận**  
    b) Chỉ dùng để xác thực trong mạng nội bộ  
    c) Không có tác dụng bảo mật  
    d) Giúp hệ thống chạy nhanh hơn
65. Khi loại bỏ thiết bị lưu trữ như đĩa cứng, cần làm gì để bảo vệ dữ liệu?  
    **a) Sử dụng phần mềm xóa dữ liệu chuyên dụng**   
    b) Chỉ cần xóa file bằng lệnh "Delete"  
    c) Gửi thiết bị đến trung tâm tái chế mà không kiểm tra  
    d) Định dạng lại ổ đĩa là đủ
66. Trong quá trình thuê nhân viên mới, công ty cần làm gì?  
    **a) Cấp thẻ, tạo tài khoản và phổ biến chính sách an ninh**  
    b) Không cần kiểm soát tài khoản mới  
    c) Cung cấp toàn quyền truy cập ngay từ đầu  
    d) Không yêu cầu nhân viên tuân theo chính sách an ninh
67. Khi nhân viên rời công ty, bước quan trọng nào cần thực hiện?  
    **a) Thu lại thẻ, khóa tài khoản nhưng không xóa**  
    b) Xóa toàn bộ thông tin của nhân viên ngay lập tức  
    c) Giữ tài khoản hoạt động trong vài tháng để kiểm tra  
    d) Không cần thực hiện hành động nào
68. Chính sách đạo đức nghề nghiệp trong HR Policy nhằm mục đích gì?  
    **a) Định hướng hành vi chuẩn mực của nhân viên**  
    b) Kiểm soát hoàn toàn cuộc sống cá nhân của nhân viên  
    c) Không cần thiết trong môi trường làm việc  
    d) Chỉ áp dụng cho cấp quản lý
69. Pháp y máy tính là gì?  
    **a) Quá trình thu thập chứng cứ để phát hiện tội phạm**  
    b) Chỉ là việc khôi phục dữ liệu bị mất  
    c) Quá trình bảo trì hệ thống máy tính  
    d) Chỉ áp dụng cho các hệ thống ngân hàng
70. Khi thực hiện điều tra pháp y máy tính, điều quan trọng nhất là gì?  
    **a) Tuân thủ các bước hợp pháp để giữ nguyên chứng cứ**  
    b) Xóa toàn bộ dữ liệu trên hệ thống  
    c) Cố gắng khôi phục hệ thống nhanh nhất có thể  
    d) Không quan tâm đến tính hợp pháp của chứng cứ
71. Tại sao nhận thức về an ninh mạng là quan trọng?  
    **a) Người dùng thường là người phát hiện sự cố đầu tiên**  
    b) Chỉ quản trị viên mới cần quan tâm đến an ninh mạng  
    c) Không cần thiết vì hệ thống có thể tự bảo vệ  
    d) Chỉ hacker mới cần hiểu về an ninh mạng
72. Khi phát hiện sự cố mạng, người dùng nên làm gì?  
    **a) Báo cáo ngay cho quản trị viên hệ thống**  
    b) Tự ý xử lý mà không cần báo cáo  
    c) Xóa hết dữ liệu liên quan để tránh trách nhiệm  
    d) Bỏ qua vì không quan trọng
73. Đội phản ứng nhanh trong an ninh mạng có nhiệm vụ gì?  
    **a) Xác định nguyên nhân, cô lập sự cố và hỗ trợ điều tra**  
    b) Xóa hết log hệ thống để tránh phát hiện  
    c) Cung cấp quyền truy cập không giới hạn cho tất cả người dùng  
    d) Không cần thiết trong tổ chức
74. Vai trò nào không thuộc quy trình điều tra xâm nhập hệ thống?  
    a) Thu thập   
    b) Kiểm tra   
    c) Bảo quản  
    d) Trình bày  
    **e) Xóa bỏ chứng cứ**
75. Chuỗi hành trình chứng cứ (Chain of Custody) là gì?  
    **a) Lịch sử về việc ai đã xử lý chứng cứ và vào thời điểm nào**  
    b) Một kỹ thuật bảo vệ hệ thống khỏi virus  
    c) Phương pháp mã hóa dữ liệu trên máy tính  
    d) Chỉ áp dụng cho hệ thống mạng nội bộ
76. Chứng cứ trong điều tra an ninh mạng có thể được thu thập từ đâu?  
    **a) Log file hệ điều hành và ứng dụng**  
    b) Dữ liệu ngẫu nhiên trên Internet  
    c) Tài khoản mạng xã hội của nhân viên  
    d) Chỉ có dữ liệu trên thiết bị di động
77. Công cụ nào có thể hỗ trợ thu thập chứng cứ an ninh mạng?  
    **a) Safeback, Encase, ProDiscover**  
    b) Microsoft Word, Excel  
    c) YouTube, Facebook  
    d) Paint, Notepad
78. Khi thu thập chứng cứ, điều quan trọng nhất cần đảm bảo là gì?  
    **a) Không làm thay đổi hoặc phá hỏng chứng cứ**  
    b) Xóa toàn bộ dữ liệu để tránh rò rỉ  
    c) Chỉ lưu trữ chứng cứ trong vòng 1 ngày  
    d) Không cần kiểm tra lại chứng cứ đã thu thập

Chương 4

1. Mật mã là gì?  
   a) Quá trình nén dữ liệu  
   **b) Nghệ thuật biến đổi dữ liệu gốc và khôi phục lại sau này**  
   c) Giải thuật sắp xếp dữ liệu  
   d) Phương pháp kiểm tra lỗi dữ liệu
2. Giải thuật nào sau đây KHÔNG thuộc nhóm giải thuật mật mã?  
   a) Băm   
   b) Mã hóa đối xứng (symmetric)  
   c) Mã hóa bất đối xứng (asymmetric)  
   **d) Giải thuật nén**
3. Yếu tố nào luôn được yêu cầu trong mật mã?  
   a) Chữ ký số  
   b) Mật khẩu người dùng  
   **c) Khóa**  
   d) Câu hỏi bảo mật
4. Chức năng chính của giải thuật băm là gì?  
   a) Mã hóa dữ liệu để bảo mật  
   **b) Tạo ra dấu vân tay (message digest) để kiểm tra tính toàn vẹn dữ liệu**  
   c) Nén dữ liệu để tiết kiệm không gian  
   d) Chia nhỏ dữ liệu thành nhiều phần
5. Một trong các giải thuật băm phổ biến là?  
   a) AES  
   b) RSA  
   **c) MD5 (không thể dịch ngược)**  
   d) DES
6. MD5 thường được sử dụng để làm gì?  
   a) Nén dữ liệu  
   **b) Tạo checksum để kiểm tra tính toàn vẹn**   
   c) Mã hóa dữ liệu  
   d) Giải mã dữ liệu
7. Đầu ra của MD5 có độ dài bao nhiêu?  
   a) 64 bits  
   **b) 128 bits**  
   c) 160 bits  
   d) 256 bits
8. SHA-1 có độ dài digest là bao nhiêu (dùng trong IPSec)?  
   a) 128 bits  
   **b) 160 bits**  
   c) 192 bits  
   d) 256 bits
9. SHA-1 thường được sử dụng trong ứng dụng nào?  
   a) **IPSec**  
   b) Nén dữ liệu  
   c) Bảo mật Wi-Fi  
   d) Phân tích dữ liệu
10. Điểm yếu chính của các giải thuật băm là gì?  
    a) Dễ bị nén dữ liệu sai  
    b) **Dễ bị tấn công Man-in-the-Middle**  
    c) Không thể kiểm tra tính toàn vẹn dữ liệu  
    d) Không có độ bảo mật cao
11. HMAC là gì?  
    a) Một thuật toán mã hóa đối xứng  
    b) Một biến thể của MD5  
    **c) Giải thuật băm có sử dụng thêm khóa bí mật (MAC)**  
    d) Một phương pháp nén dữ liệu
12. HMAC bổ sung yếu tố nào để tăng cường bảo mật?  
    a) **Thêm khóa bí mật (MAC) trước khi dùng giải thuật băm**  
    b) Mã hóa dữ liệu đầu vào trước khi băm  
    c) Thêm số ngẫu nhiên vào thuật toán  
    d) Tăng độ dài đầu ra của băm
13. HMAC-SHA-1 sử dụng khóa có độ dài bao nhiêu?  
    a) 64 bits  
    b) 128 bits  
    **c) 160 bits**  
    d) 256 bits
14. Mục đích chính của mã hóa là gì?  
    a) **Tạo ra sự bảo mật cho dữ liệu khi lưu trữ hoặc truyền đi**  
    b) Giúp nén dữ liệu hiệu quả hơn  
    c) Xóa bỏ dữ liệu sau khi sử dụng  
    d) Kiểm tra lỗi trong dữ liệu
15. Mã hóa sử dụng yếu tố nào để mã hóa và giải mã?  
    a) **Khóa**  
    b) Chữ ký số  
    c) Số ngẫu nhiên  
    d) Mã kiểm tra lỗi
16. Trong mã hóa bất đối xứng, có bao nhiêu khóa được sử dụng?  
    a) **2 khóa: một khóa mã hóa và một khóa giải mã**  
    b) 1 khóa duy nhất  
    c) 3 khóa với cơ chế vòng lặp  
    d) Không sử dụng khóa
17. Mã hóa đối xứng còn được gọi là gì?   
    a) Mã hóa công khai  
    b) Mã hóa không sử dụng khóa  
    c) **Mã hóa với khóa bí mật/chia sẻ**  
    d) Mã hóa không đối xứng
18. Giao thức bảo mật nào sau đây sử dụng mã hóa đối xứng?  
    a) **SSL**  
    b) SSH  
    c) PGP  
    d) HTTPS

\* DES, 3DES, AES, IDEA, CAST

1. Một trong những ưu điểm của mã hóa đối xứng là gì?  
   a) **Có tốc độ nhanh và cài đặt đơn giản hơn so với mã hóa bất đối xứng**  
   b) Không cần sử dụng khóa  
   c) Không thể bị tấn công  
   d) Không cần kiểm tra dữ liệu đầu vào
2. DES sử dụng độ dài khóa bao nhiêu bit?  
   a) 32 bits  
   b) 64 bits  
   c) **56 bits cho khóa, 8 bits kiểm tra, tổng cộng 64 bits**  
   d) 128 bits
3. Vì sao DES không còn được xem là an toàn?  
   a) **Do độ dài khóa ngắn (56), dễ bị vét cạn (tốc độ nhanh)**  
   b) Do tốc độ thực thi chậm  
   c) Vì không hỗ trợ mã hóa bất đối xứng  
   d) Vì không được tiêu chuẩn hóa
4. 3DES được tạo ra để thay thế cho DES vì lý do gì?  
   a) **Do DES không còn an toàn**  
   b) Vì DES quá nhanh  
   c) Vì DES không hỗ trợ mã hóa đối xứng  
   d) Vì DES không được sử dụng rộng rãi

\* 2TDES: khóa k1=k3, tốc độ chậm, thay bằng AES.

1. 3DES sử dụng bao nhiêu khóa để mã hóa dữ liệu?  
   a) 1 khóa  
   b) 2 khóa  
   c) **3 khóa**  
   d) 4 khóa
2. Tổng độ dài khóa trong 3DES là bao nhiêu bit?  
   a) **168 bits (3 x 56)**  
   b) 256 bits  
   c) 512 bits  
   d) 1024 bits
3. Khối dữ liệu của AES có kích thước bao nhiêu bit?  
   a) 64 bits  
   b) **128 bits**  
   c) 192 bits  
   d) 256 bits

\* AES dễ thực hiện, tốc độ cao, ít tốn bộ nhớ

1. Tùy vào độ dài khóa (128-192-256), AES có bao nhiêu vòng lặp mã hóa?  
   a) 5, 7 hoặc 9 vòng  
   b) 8, 10 hoặc 12 vòng  
   c) **10, 12 hoặc 14 vòng**  
   d) 16, 18 hoặc 20 vòng
2. Mã hóa bất đối xứng còn được gọi là gì?  
   a) **Mã hóa với khóa công khai**  
   b) Mã hóa không khóa  
   c) Mã hóa với khóa chia sẻ  
   d) Mã hóa đảo ngược
3. Trong mã hóa bất đối xứng, khóa nào dùng để mã hóa dữ liệu?  
   a) **Khóa công khai**   
   b) Khóa bí mật   
   c) Khóa phiên  
   d) Khóa tạm thời
4. Giải thuật nào sau đây KHÔNG thuộc nhóm mã hóa bất đối xứng?  
   a) RSA  
   b) DSA  
   c) **AES**  
   d) Diffie-Hellman
5. Trong RSA, khóa nào được sử dụng để mã hóa dữ liệu? (dùng trong IPSec)

\* Mã hóa: pub để mã, pri để giải

\* Chữ ký số: pri để mã, pub để giải

1. Vì sao RSA được xem là an toàn?  
   a) **Vì không thể tìm khóa bí mật từ dữ liệu mã hóa và khóa công khai (1024-2048)**  
   b) Vì sử dụng thuật toán băm  
   c) Vì có tốc độ mã hóa nhanh hơn AES  
   d) Vì không cần khóa để giải mã
2. DSA chủ yếu được sử dụng để làm gì?  
   a) Mã hóa dữ liệu  
   b) **Tạo chữ ký số (tốc độ tương đương RSA khi tạo, chậm hơn x10-40 khi kiểm tra)**  
   c) Nén dữ liệu  
   d) Kiểm tra lỗi
3. Độ dài khóa được khuyến nghị sử dụng hiện nay trong DSA là bao nhiêu?  
   a) **2048 bits (512-1024)**  
   b) 512 bits  
   c) 1024 bits  
   d) 4096 bits
4. Giải thuật Diffie-Hellman dùng để làm gì?  
   a) **Tạo khóa bí mật chia sẻ giữa hai bên trên đường truyền không an toàn**  
   b) Mã hóa dữ liệu trực tiếp  
   c) Tạo chữ ký số  
   d) Xác thực người dùng
5. Điểm yếu chính của Diffie-Hellman là gì?  
   a) **Dễ bị tấn công Man-in-the-Middle**  
   b) Không thể sử dụng trên mạng Internet  
   c) Không hỗ trợ mã hóa khóa công khai  
   d) Không thể trao đổi khóa giữa hai bên
6. Mật mã có thể cung cấp những dịch vụ an ninh nào?  
   a) Nén dữ liệu, kiểm tra lỗi, mã hóa  
   b) **Bảo mật, toàn vẹn, chứng thực, không thể phủ nhận**  
   c) Lưu trữ dữ liệu, kiểm tra lỗi, tối ưu hóa dữ liệu  
   d) Giảm dung lượng tệp tin, bảo vệ chống virus, phục hồi dữ liệu
7. Dữ liệu được bảo vệ khỏi truy cập trái phép bằng cách nào?  
   a) Chữ ký số  
   b) **Mã hóa**  
   c) Phân mảnh dữ liệu  
   d) Nén dữ liệu
8. Làm thế nào để kiểm tra dữ liệu có bị thay đổi hay không?  
   a) **Dùng giải thuật băm như MD5 hoặc SHA-1**  
   b) Dùng mã hóa AES  
   c) Dùng khóa công khai  
   d) Nén dữ liệu
9. Giải thuật nào sau đây KHÔNG dùng để kiểm tra tính toàn vẹn?  
   a) MD5  
   b) SHA-1  
   c) **RSA**  
   d) SHA-256
10. Mục đích chính của dịch vụ toàn vẹn dữ liệu là gì?  
    a) **Đảm bảo dữ liệu không bị thay đổi trong quá trình truyền**  
    b) Đảm bảo dữ liệu được mã hóa  
    c) Đảm bảo chỉ người nhận mới đọc được dữ liệu  
    d) Đảm bảo dữ liệu có thể được khôi phục
11. Chứng thực trong bảo mật thông tin là gì?  
    a) **Xác minh danh tính của một thực thể**  
    b) Bảo mật dữ liệu bằng mã hóa  
    c) Kiểm tra dữ liệu có bị thay đổi hay không  
    d) Ngăn chặn tấn công mạng
12. Phương pháp chứng thực là gì?  
    a) Sử dụng khóa bí mật chia sẻ  
    b) Sử dụng chữ ký số  
    c) Sử dụng số ngẫu nhiên được mã hóa  
    **d) Cả A, B, C**
13. Trong chứng thực, khóa nào được sử dụng để xác minh danh tính người gửi?  
    a) **Khóa bí mật của người gửi**  
    b) Khóa công khai của người nhận  
    c) Mã OTP  
    d) Chữ ký số
14. Tính không thể phủ nhận được thực hiện thông qua phương thức nào?  
    a) Mã hóa đối xứng  
    b) **Chữ ký số**   
    c) Mã hóa dữ liệu bằng AES  
    d) Tạo khóa công khai
15. Chữ ký số là gì?  
    a) **Thông tin đi kèm theo dữ liệu để xác định chủ sở hữu**  
    b) Một phương pháp mã hóa  
    c) Một dạng mật khẩu  
    d) Một kiểu dữ liệu mới
16. Chữ ký số sử dụng kết hợp phương pháp nào?  
    a) **Giải thuật băm và mã hóa**  
    b) Giải thuật nén và mã hóa  
    c) Chỉ sử dụng khóa công khai  
    d) Sử dụng mật khẩu tĩnh
17. Chữ ký số có thể áp dụng cho loại dữ liệu nào?  
    a) Văn bản  
    b) Hình ảnh  
    c) Video  
    d) **Cả A, B, C**
18. Chữ ký số là một phần của?  
    a) **Chữ ký điện tử**   
    b) Mật khẩu một lần (OTP)  
    c) Mã hóa đối xứng  
    d) Hệ thống xác thực hai yếu tố
19. Bước đầu tiên trong quá trình tạo chữ ký số là gì?  
    a) **Người gửi tạo tài liệu**  
    b) Mã hóa tài liệu  
    c) Người nhận giải mã chữ ký số  
    d) Tạo khóa công khai
20. Chữ ký số được tạo bằng cách nào?  
    a) **Băm tài liệu để tạo Digest, sau đó mã hóa Digest bằng khóa bí mật**  
    b) Nén dữ liệu và mã hóa  
    c) Dùng khóa công khai để mã hóa toàn bộ tài liệu  
    d) Chỉ dùng mã hóa đối xứng
21. Để xác thực chữ ký số, người nhận cần làm gì?  
    a) **Giải mã chữ ký số bằng khóa công khai ra Digest1, băm tài liệu để tạo Digest2 và so sánh với Digest1**  
    b) Giải mã tài liệu bằng khóa bí mật  
    c) Chỉ kiểm tra xem tài liệu có bị thay đổi hay không  
    d) Yêu cầu người gửi cung cấp mật khẩu
22. Hạ tầng khóa công khai (PKI) là gì?  
    a) **Hệ thống cung cấp chứng chỉ số và chứng thực**   
    b) Một thuật toán mã hóa dữ liệu  
    c) Một phương thức nén dữ liệu  
    d) Hệ thống quản lý mật khẩu

\* Mô hình PKI: Single CA, P2P CA, Phân cấp

1. Chứng chỉ số trong PKI được dùng để làm gì?  
   a) **Xác thực danh tính và đảm bảo an toàn trong giao dịch điện tử**  
   b) Nén dữ liệu để truyền nhanh hơn  
   c) Bảo vệ hệ điều hành khỏi virus  
   d) Tạo mật khẩu mạnh hơn
2. Điều gì giúp chứng chỉ số trở nên đáng tin cậy?  
   a) **Nó được ký bởi một CA đáng tin cậy**  
   b) Nó được mã hóa bằng thuật toán SHA-256  
   c) Nó được lưu trữ dưới dạng tệp văn bản  
   d) Nó không bao giờ hết hạn
3. CA có vai trò gì trong PKI?  
   a) **Cung cấp và ký xác nhận chứng chỉ số**  
   b) Mã hóa dữ liệu người dùng  
   c) Lưu trữ toàn bộ khóa bí mật của người dùng  
   d) Phát hành mật khẩu cho tài khoản trực tuyến
4. Khi người dùng muốn nhận chứng chỉ số, họ cần làm gì?  
   a) **Điền form đăng ký, mã hóa và gửi cho CA**  
   b) Tạo khóa công khai và tự ký chứng chỉ số  
   c) Gửi yêu cầu trực tiếp cho người nhận  
   d) Cung cấp mật khẩu tài khoản email
5. Chứng chỉ số được tạo theo tiêu chuẩn nào?  
   a) **X.509 version 3**  
   b) SHA-256  
   c) AES-128  
   d) RSA-2048
6. Khi nào chứng chỉ số có thể bị hủy bỏ?  
   a) **Khi khóa bí mật bị lộ hoặc thông tin thay đổi**  
   b) Khi người nhận từ chối chứng chỉ  
   c) Khi hệ thống không còn hỗ trợ thuật toán mã hóa  
   d) Khi tài khoản email bị khóa
7. Khi chứng chỉ số bị hủy bỏ, nó sẽ được đưa vào đâu?  
   a) **Danh sách thu hồi chứng chỉ (CRL)**  
   b) Kho lưu trữ dữ liệu số  
   c) Danh sách email đen  
   d) Danh sách tài khoản bị khóa
8. Khi xác minh chứng chỉ số, hệ thống cần kiểm tra điều gì?  
   a) **Xem chứng chỉ có trong danh sách CRL hay không**  
   b) Kiểm tra địa chỉ IP của người dùng  
   c) Kiểm tra xem chứng chỉ có hết hạn hay chưa  
   d) So sánh chứng chỉ với mật khẩu người dùng
9. Khóa số trong chứng chỉ số có vai trò gì?  
   a) **Dùng để mã hóa và giải mã thông tin**  
   b) Xác định địa chỉ IP của người dùng  
   c) Giảm dung lượng dữ liệu truyền tải  
   d) Tạo mật khẩu mạnh hơn
10. 2 phương pháp phổ biến để lưu trữ và phân phối khóa là gì?  
    a) **Trung tâm phân phối khóa (KDC) và giải thuật trao đổi khóa (KEA)**  
    b) Mật khẩu tĩnh và xác thực hai yếu tố  
    c) Sử dụng blockchain và trí tuệ nhân tạo  
    d) Dùng email để gửi khóa công khai
11. Điều gì quan trọng khi quản lý khóa số?  
    a) **Đảm bảo khóa được bảo vệ an toàn**   
    b) Chia sẻ khóa công khai với mọi người  
    c) Tạo khóa mới mỗi ngày  
    d) Lưu trữ khóa trong tệp văn bản đơn giản
12. Escrow trong quản lý khóa số là gì?  
    a) **Lưu trữ bản sao khóa bí mật trong hệ thống tập trung**  
    b) Hệ thống chia sẻ khóa công khai  
    c) Cơ sở dữ liệu quản lý email  
    d) Cách tạo mật khẩu tạm thời
13. Một rủi ro khi sử dụng Escrow là gì?  
    a) **Có thể bị hacker tấn công để lấy khóa bí mật**  
    b) Không thể khôi phục khóa khi cần  
    c) Không tương thích với hệ thống mã hóa  
    d) Không thể lưu trữ khóa đối xứng
14. Người dùng có thể làm gì để giảm rủi ro khi sử dụng Escrow?  
    a) **Lưu nhiều bản sao tại các công ty Escrow khác nhau**  
    b) Không sử dụng Escrow  
    c) Chia sẻ khóa bí mật với nhiều người  
    d) Giữ khóa trong tệp văn bản trên máy tính
15. Khi chứng chỉ số hết hạn, điều gì xảy ra?  
    a) **Chứng chỉ số sẽ bị hủy bỏ**  
    b) Chứng chỉ vẫn tiếp tục hoạt động nhưng với hạn chế  
    c) Chứng chỉ sẽ tự động gia hạn  
    d) Chứng chỉ sẽ được chuyển thành khóa công khai
16. Nếu phát hiện khóa bí mật bị lộ, người dùng cần làm gì?  
    a) **Yêu cầu hủy bỏ chứng chỉ số**  
    b) Đổi mật khẩu tài khoản email  
    c) Liên hệ với nhà cung cấp Internet  
    d) Vô hiệu hóa toàn bộ hệ thống
17. Khi chứng chỉ số bị hủy bỏ, số serial của nó được đưa vào đâu?  
    a) **Danh sách thu hồi chứng chỉ (CRL)**  
    b) Danh sách tài khoản bị khóa  
    c) Hệ thống giám sát bảo mật  
    d) Cơ sở dữ liệu mật khẩu
18. Người dùng có thể gia hạn chứng chỉ số khi nào?  
    a) **Trước khi chứng chỉ hết hạn**  
    b) Sau khi chứng chỉ hết hạn  
    c) Khi mất khóa bí mật  
    d) Khi khóa công khai bị thay đổi
19. Tại sao việc sử dụng khóa cũ có thể gây rủi ro bảo mật?  
    a) **Vì nó có thể bị lộ hoặc bị tấn công**  
    b) Vì nó không thể được mã hóa lại  
    c) Vì khóa cũ không thể sử dụng trên máy chủ mới  
    d) Vì nó làm giảm tốc độ xử lý dữ liệu
20. Khi khóa và chứng chỉ số không còn sử dụng, cần làm gì?  
    a) **Gỡ bỏ bằng phần mềm hoặc tiêu hủy phần cứng lưu trữ**  
    b) Lưu trữ lại trong một cơ sở dữ liệu an toàn  
    c) Chuyển giao khóa cho người khác sử dụng  
    d) Chuyển đổi chứng chỉ thành mật khẩu
21. Khi sử dụng khóa số, điều quan trọng cần xác định là gì?  
    a) **Khóa sẽ được sử dụng như thế nào**  
    b) Khóa có thể được chia sẻ với ai  
    c) Khóa có thể nén lại để tiết kiệm dung lượng  
    d) Khóa phải có mật khẩu đi kèm
22. Khóa được sử dụng rộng rãi trong ứng dụng nào?  
    a) **VPN như IPSec**  
    b) Trình duyệt web  
    c) Phần mềm đồ họa  
    d) Hệ thống quản lý tài chính
23. Giao thức bảo mật nào sử dụng khóa để mã hóa dữ liệu trên internet?  
    a) **HTTPS (SSL/TLS)**  
    b) FTP  
    c) DHCP  
    d) DNS
24. Khóa số có thể được sử dụng trong bảo mật email thông qua công nghệ nào?  
    a) **PGP, S/MIME**  
    b) IMAP  
    c) POP3  
    d) SMTP
25. Một trong những ứng dụng quan trọng của khóa số trong bảo mật mạng là gì?  
    a) **Truy cập từ xa an toàn bằng SSH**  
    b) Quản lý tệp tin  
    c) Sao lưu dữ liệu  
    d) Lưu trữ mật khẩu

Chương 5

1. Vì sao cần có cơ chế an toàn trên đường truyền trong truyền thông mạng?
   1. Do Internet ngày càng nhanh
   2. Do truyền thông mạng và làm việc từ xa phổ biến hơn
   3. Do các giao thức mạng và dịch vụ cần bảo mật
   4. **Tất cả các lý do trên**
2. Cơ chế an toàn trên mạng cần áp dụng cho?
   1. Đường truyền dữ liệu
   2. **Giao thức mạng và dịch vụ**
   3. Chỉ các thiết bị cá nhân
   4. Chỉ các ứng dụng nhắn tin
3. PPP (Point-to-Point Protocol) thuộc tầng nào trong mô hình OSI?
   1. Tầng 1
   2. **Tầng 2**
   3. Tầng 3
   4. Tầng 4

\* Dùng cho mạng IP, AppleTalk, cấp phát IP động, nén dữ liệu và điều khiển chất lượng đường nối kết

1. Cơ chế chứng thực nào của PPP không mã hóa dữ liệu?
   1. **PAP**
   2. CHAP (có mã hóa)
   3. IPSec
   4. SSH
2. Một trong những ưu điểm của PPP là gì?
   1. Bảo mật mạnh
   2. Tốc độ cao
   3. **Kết nối đơn giản, dễ sử dụng (- tốc độ thấp)**
   4. Không hỗ trợ cấp địa chỉ IP động
3. Telnet sử dụng cổng nào để hoạt động?
   1. 22
   2. 80
   3. **23**
   4. 443
4. Vì sao Telnet bị coi là không an toàn?
   1. **Dữ liệu truyền đi không được mã hóa**
   2. Chỉ chạy trên Windows
   3. Không hỗ trợ đăng nhập từ xa
   4. Không có cơ chế chứng thực
5. Để tăng cường bảo mật thay vì dùng Telnet, ta nên sử dụng giao thức nào?
   1. FTP
   2. **SSH**
   3. HTTP
   4. POP3
6. SSH sử dụng cổng mặc định nào?
   1. 21
   2. **22**
   3. 23
   4. 443
7. SSH cung cấp bảo mật bằng cách nào?
   1. Chỉ sử dụng mật khẩu để đăng nhập
   2. **Dùng cặp khóa công khai và khóa bí mật (định danh)**
   3. Chỉ mã hóa mật khẩu đăng nhập
   4. Không có cơ chế bảo mật
8. Các thuật toán nào được SSH sử dụng?
   1. RSA, DSA (chứng thực)
   2. DES, 3DES (mã hóa)
   3. Blowfish, IDEA (mã hóa)
   4. **Tất cả các thuật toán trên**
9. TACACS+ là giao thức của hãng nào?
   1. Microsoft
   2. **Cisco**
   3. IBM
   4. Google
10. TACACS+ sử dụng cổng nào?
    1. 22
    2. 23
    3. **TCP 49**
    4. 1812
11. TACACS+ có thể bị tấn công bằng cách nào?
    1. **Tấn công do chỉ dùng một khóa bí mật (hoặc tấn công replay)**
    2. Không có điểm yếu
    3. Do không mã hóa dữ liệu
    4. Không hỗ trợ chứng thực
12. TACACS+ cung cấp những dịch vụ nào?
    1. Authentication
    2. Authorization
    3. Accounting
    4. **Tất cả các dịch vụ trên (AAA)**
13. Thiết bị nào có thể sử dụng TACACS+ để chứng thực?
    1. Router
    2. Switch
    3. VPN
    4. **Tất cả các thiết bị trên**
14. TACACS+ mã hóa phần nào trong quá trình xác thực?
    1. Chỉ mật khẩu
    2. Chỉ dữ liệu truyền
    3. **Toàn bộ phiên giao dịch**
    4. Không mã hóa
15. RADIUS sử dụng giao thức nào để truyền dữ liệu (mã hóa mật khẩu và tên người dùng)?
    1. TCP
    2. **UDP**
    3. ICMP
    4. HTTP
16. RADIUS thường được sử dụng để làm gì?
    1. **Cung cấp dịch vụ AAA (PPP, PAP, CHAP)**
    2. Mã hóa toàn bộ dữ liệu truyền trên mạng
    3. Định tuyến gói tin trong mạng
    4. Bảo vệ chống tấn công DDoS
17. RADIUS sử dụng cổng nào cho quá trình xác thực?
    1. 49
    2. **UDP 1812**
    3. 23
    4. 22
18. WLAN có ưu điểm gì so với mạng có dây?
    1. Dễ dàng mở rộng
    2. Hỗ trợ tính di động
    3. Tốc độ cao và linh hoạt
    4. **Tất cả các ý trên**
19. WLAN sử dụng phương pháp truy cập nào để tránh xung đột dữ liệu?
    1. **CSMA/CA**
    2. CSMA/CD
    3. Token Ring
    4. FDDI
20. Chuẩn Wi-Fi nào có tốc độ cao nhất?
    1. Wi-Fi 4 (802.11n)
    2. Wi-Fi 5 (802.11ac)
    3. **Wi-Fi 6 (802.11ax)**
    4. Wi-Fi 3 (802.11g)
21. Chuẩn Wi-Fi nào chỉ hoạt động trên băng tần 5GHz? (1,3) - (2,5)
    1. 802.11b
    2. 802.11g
    3. **Wifi 2 (802.11a)**
    4. 802.11n
22. WLAN có những chế độ hoạt động nào?
    1. Infrastructure mode (cilent2ap)
    2. Ad-hoc mode (p2p)
    3. Peer-to-peer mode
    4. **Cả A và B**
23. SSID của mạng WLAN có độ dài bao nhiêu ký tự?
    1. 2- 16
    2. **2- 32**
    3. 4- 64
    4. 4- 128
24. Ở Bắc Mỹ, băng tần 2.4GHz được chia thành bao nhiêu kênh?
    1. 9
    2. **11 (Châu Âu 13)**
    3. 13
    4. 14
25. Để tránh nhiễu sóng khi sử dụng 3 AP trong cùng khu vực, nên chọn các kênh nào?
    1. **1, 6, 11**
    2. 2, 5, 8
    3. 3, 7, 10
    4. 4, 9, 13
26. Băng tần 5GHz có bao nhiêu kênh không chồng lấn?
    1. 3
    2. **24**
    3. 13
    4. 11
27. Trong mạng WLAN 5GHz, khoảng cách giữa các kênh là bao nhiêu MHz?
    1. 10 MHz
    2. **20 MHz (4 là 22)**
    3. 40 MHz
    4. 80 MHz
28. Các kênh không bị chồng lấn trong băng tần 5GHz là?
    1. 1, 6, 11
    2. **36, 48, 60**
    3. 2, 7, 13
    4. 3, 9, 14
29. Trong cùng một phạm vi địa lý, việc chọn kênh trong mạng WLAN cần tuân theo nguyên tắc nào?
    1. Chọn kênh ngẫu nhiên
    2. Chọn kênh gần nhau để tối ưu tốc độ
    3. **Chọn các kênh không bị chồng lấn nhau**
    4. Chỉ sử dụng kênh 1 và 11
30. Beacon trong mạng WLAN có chức năng gì?
    1. Mã hóa dữ liệu truyền tải
    2. Xác thực người dùng trước khi truy cập mạng
    3. **Frame gửi tín hiệu từ AP để thông báo sự hiện diện của mạng**
    4. Định tuyến lưu lượng mạng
31. Beacon trong WLAN được gửi như thế nào?
    1. Chỉ khi có thiết bị yêu cầu
    2. **Được gửi broadcast định kỳ**
    3. Chỉ gửi đến các thiết bị đã kết nối
    4. Được mã hóa và gửi qua cổng 443
32. Tín hiệu Beacon giúp thiết bị nào có thể tìm thấy mạng WLAN?
    1. Chỉ máy tính
    2. Chỉ điện thoại di động
    3. **Tất cả các thiết bị có hỗ trợ Wi-Fi**
    4. Chỉ các thiết bị đã đăng ký trước
33. Khi thiết bị thực hiện quá trình Probing trong WLAN, nó sẽ làm gì?
    1. **Kiểm tra xem có mạng WLAN đúng với SSID đã định trước hay không**
    2. Tự động kết nối với bất kỳ mạng Wi-Fi nào
    3. Mã hóa dữ liệu truyền đi
    4. Kiểm tra tốc độ đường truyền
34. Nếu không biết SSID của mạng, có thể tìm kiếm các mạng khả dụng bằng cách nào?
    1. Dùng lệnh Telnet
    2. **Gửi probe request không có SSID**
    3. Chờ AP gửi Beacon
    4. Kết nối trực tiếp qua địa chỉ IP
35. Trong WLAN, nếu chứng thực theo dạng mở (Open), thiết bị có cần key không?
    1. Có, luôn cần khóa bảo mật
    2. **Không, vì Open không yêu cầu khóa bảo mật**
    3. Chỉ cần khóa khi kết nối lần đầu
    4. Cần mã hóa AES để chứng thực
36. Nếu WLAN sử dụng mã hóa WEP, quá trình chứng thực cần gì?
    1. **Một Key được thiết lập trước**
    2. Chứng thực qua tài khoản email
    3. Dùng Telnet để xác thực
    4. Không cần chứng thực
37. Trong quá trình Association, hệ thống thực hiện điều gì?
    1. Chứng thực người dùng
    2. **Thiết lập kết nối tầng 2 và tạo port ảo giữa client và AP**
    3. Mã hóa toàn bộ dữ liệu
    4. Định tuyến lưu lượng qua firewall
38. Khi Association hoàn tất, thiết bị có thể làm gì?
    1. **Bắt đầu gửi và nhận dữ liệu qua WLAN**
    2. Chỉ nhận dữ liệu từ AP
    3. Tự động cấp quyền admin trên mạng
    4. Định danh lại SSID
39. War Driving là gì?
    1. Một kỹ thuật bảo mật cho mạng WLAN
    2. **Hành vi dò tìm các mạng Wi-Fi mở**
    3. Một phương pháp mã hóa dữ liệu
    4. Một giao thức truyền tải trong WLAN
40. War Driving có thể gây ra nguy cơ gì?
    1. Kẻ xấu sử dụng Internet miễn phí
    2. Tin tặc xâm nhập vào mạng Wi-Fi yếu
    3. Dữ liệu có thể bị đánh cắp nếu không mã hóa
    4. **Tất cả các nguy cơ trên**
41. Làm thế nào để hạn chế War Driving?
    1. Sử dụng SSID ẩn
    2. Cấu hình bảo mật WPA2/WPA3
    3. Hạn chế truy cập theo địa chỉ MAC
    4. **Tất cả các biện pháp trên**
42. Tấn công Man-in-the-Middle trong mạng WLAN có thể xảy ra ở giai đoạn nào?
    1. Khi thiết bị kết nối với AP lần đầu
    2. Khi AP gửi Beacon
    3. **Khi diễn ra quá trình Association**
    4. Khi thiết bị thực hiện Probing
43. Biện pháp nào giúp ngăn chặn tấn công MITM trong WLAN?
    1. Sử dụng mật khẩu mạnh
    2. **Cài đặt hệ thống ngăn chặn xâm nhập (IPS)**
    3. Giới hạn số lượng thiết bị có thể kết nối
    4. Tăng công suất phát của Access Point
44. Tấn công giả mạo Access Point là gì?
    1. Một kỹ thuật tối ưu hóa Wi-Fi
    2. Một phương pháp chứng thực an toàn
    3. **Tạo ra AP giả để lừa người dùng kết nối**
    4. Cấu hình sai địa chỉ IP trên AP
45. Một trong những nguyên nhân gây tấn công DoS trên WLAN là gì?
    1. Dùng mật khẩu yếu
    2. **Nhiễu sóng từ thiết bị điện tử khác**
    3. Quên cập nhật firmware AP
    4. Dùng SSID quá dài
46. Cách nào giúp giảm nguy cơ bị tấn công DoS trong WLAN?
    1. Sử dụng tần số 2.4GHz thay vì 5GHz
    2. Tắt tính năng bảo mật trên router
    3. **Giảm công suất phát và sử dụng bộ lọc MAC**
    4. Luôn để Wi-Fi ở chế độ mở
47. Giao thức bảo mật nào được xem là kém an toàn nhất trong WLAN?
    1. **Open (ko chứng thực, mã hóa)**
    2. WEP (chứng thực yếu, khóa tĩnh, mã hóa dễ bị phá)
    3. WPA (chứng thực mạnh: EAP , mã hóa cao)
    4. WPA2 (mã hóa AES, khóa động)
48. Giao thức nào hiện nay cung cấp bảo mật cao nhất cho WLAN?
    1. WEP
    2. WPA
    3. WPA2
    4. **WPA3**
49. WEP sử dụng thuật toán mã hóa nào?
    1. AES
    2. SHA-256
    3. **RC4**
    4. Blowfish
50. WEP có độ dài khóa phổ biến là bao nhiêu bit?
    1. 32-bit
    2. **64 hoặc 128-bit**
    3. 256-bit
    4. 512-bit
51. Tại sao WEP dễ bị tấn công?
    1. Sử dụng khóa động
    2. Không sử dụng bất kỳ mã hóa nào
    3. **Dễ bị bẻ khóa do sử dụng khóa tĩnh và lỗ hổng trong RC4**
    4. Không hỗ trợ chứng thực
52. EAP (Extensible Authentication Protocol) cung cấp gì cho mạng WLAN?
    1. Tăng tốc độ kết nối Wi-Fi
    2. **Chứng thực mạnh giữa client và server**
    3. Cấp phát địa chỉ IP tự động
    4. Giảm nhiễu tín hiệu
53. EAP hoạt động trên tầng nào của mô hình OSI?
    1. Tầng 3
    2. Tầng 4
    3. **Tầng 2**
    4. Tầng 7
54. Giao thức nào sau đây không thuộc họ EAP?
    1. PEAP
    2. **SSL**
    3. EAP-TLS
    4. EAP-TTLS
55. WPA được tạo ra nhằm thay thế giao thức nào?
    1. AES
    2. SSL
    3. **WEP**
    4. SSH
56. WPA2 sử dụng thuật toán mã hóa nào?
    1. RC4
    2. DES
    3. **AES**
    4. MD5
57. Điểm khác biệt chính giữa WPA3 và WPA2 là gì?
    1. WPA3 hỗ trợ tốc độ mạng nhanh hơn
    2. **WPA3 sử dụng Simultaneous Authentication of Equals (SAE) thay cho PSK**
    3. WPA3 không hỗ trợ mã hóa dữ liệu
    4. WPA3 không yêu cầu mật khẩu khi kết nối
58. WPA3-Personal sử dụng cơ chế nào để chống lại tấn công vét cạn?
    1. PSK (Pre-Shared Key)
    2. TKIP
    3. **Simultaneous Authentication of Equals (SAE)**
    4. WEP
59. WPA3-Enterprise sử dụng bộ mật mã có độ dài bao nhiêu bit?
    1. 128-bit
    2. **192-bit**
    3. 256-bit
    4. 512-bit
60. Trong mạng mở (Open Networks), WPA3 sử dụng cơ chế nào để mã hóa dữ liệu?
    1. WEP
    2. TKIP
    3. **Opportunistic Wireless Encryption (OWE)**
    4. SSL
61. VPN (Virtual Private Network) giúp gì cho doanh nghiệp?
    1. Giảm chi phí kết nối từ xa
    2. Bảo mật dữ liệu truyền qua mạng công cộng
    3. Kết nối an toàn giữa các chi nhánh
    4. **Tất cả các ý trên**
62. VPN giúp đảm bảo tính bảo mật bằng cách nào?
    1. Giấu địa chỉ IP của người dùng
    2. Mã hóa dữ liệu truyền qua mạng
    3. **Cả hai phương án trên**
    4. Không có cơ chế bảo mật
63. Đặc điểm nào đúng về VPN?
    1. Kết nối giữa hai thực thể bằng đường truyền vật lý riêng
    2. **Kết nối ảo, bảo mật, không thể truy cập từ bên ngoài**
    3. Chỉ sử dụng trong mạng nội bộ
    4. Không hỗ trợ mã hóa dữ liệu
64. VPN phù hợp với mô hình nào sau đây?
    1. Doanh nghiệp có nhiều chi nhánh
    2. Nhân viên làm việc từ xa
    3. Người dùng cá nhân muốn bảo vệ quyền riêng tư khi lướt web
    4. **Tất cả các mô hình trên**
65. VPN giúp tiết kiệm chi phí bằng cách nào?
    1. Giảm số lượng thiết bị mạng cần mua
    2. **Sử dụng Internet công cộng thay vì đường truyền thuê riêng**
    3. Không cần sử dụng tường lửa
    4. Miễn phí hoàn toàn cho tất cả người dùng
66. Site-to-Site VPN được sử dụng để làm gì?
    1. **Kết nối hai hoặc nhiều mạng LAN với nhau thông qua Internet**
    2. Kết nối máy tính cá nhân với mạng doanh nghiệp
    3. Tăng tốc độ duyệt web
    4. Kết nối mạng bằng Bluetooth
67. Site-to-Site VPN có thể chia thành mấy loại?
    1. 1
    2. **2 (Intranet VPN và Extranet VPN)**
    3. 3
    4. 4
68. Extranet VPN dùng để làm gì?
    1. Kết nối nội bộ các chi nhánh công ty
    2. **Kết nối công ty với đối tác, khách hàng thông qua mạng an toàn**
    3. Tạo một mạng riêng biệt không kết nối ra Internet
    4. Chỉ dùng cho quản trị viên mạng
69. Remote Access VPN giúp người dùng làm gì?
    1. **Kết nối từ xa vào mạng công ty qua Internet**
    2. Kết nối giữa các mạng LAN với nhau
    3. Tăng tốc độ duyệt web
    4. Giảm chi phí đường truyền nội bộ
70. Có bao nhiêu loại Remote Access VPN?
    1. 1
    2. **2 (Client-initiated và NAS-initiated)**
    3. 3
    4. 4
71. Client-initiated VPN hoạt động như thế nào?
    1. Người dùng kết nối trực tiếp qua đường truyền vật lý
    2. **Người dùng sử dụng phần mềm VPN Client để thiết lập kết nối**
    3. VPN tự động kết nối khi có mạng Wi-Fi
    4. Không yêu cầu xác thực
72. VPN Server có chức năng gì?
    1. Quản lý việc cấp phát địa chỉ IP cho client
    2. Xác thực người dùng kết nối từ xa
    3. Mã hóa dữ liệu truyền đi
    4. **Tất cả các chức năng trên**
73. Giao thức nào thường được sử dụng để tạo VPN?
    1. FTP
    2. **IPSec**
    3. HTTP
    4. SNMP
74. VPN có thể được triển khai trên tầng nào của mô hình OSI?
    1. Chỉ tầng mạng (Layer 3)
    2. **Nhiều tầng khác nhau tùy vào công nghệ VPN sử dụng**
    3. Chỉ tầng liên kết dữ liệu (Layer 2)
    4. Chỉ tầng ứng dụng (Layer 7)
75. Web VPN có khả năng nào sau đây?
    1. Truy cập website nội bộ
    2. Truy cập hệ thống file chia sẻ trên mạng
    3. Truy cập email qua POP, SMTP, IMAP
    4. **Tất cả các khả năng trên**
76. Giao thức nào được Web VPN sử dụng để mã hóa dữ liệu?
    1. WEP
    2. TKIP
    3. **SSL/TLS**
    4. MD5
77. Công nghệ Tunneling trong VPN có tác dụng gì?
    1. Tăng tốc độ truy cập mạng
    2. **Mã hóa và bảo vệ dữ liệu khi truyền qua mạng công cộng**
    3. Giúp VPN hoạt động mà không cần chứng thực
    4. Chỉ áp dụng cho kết nối mạng LAN
78. Trong công nghệ Tunneling, dữ liệu gốc được xử lý như thế nào?
    1. Gửi đi mà không thay đổi
    2. Được mã hóa một phần
    3. **Được bao gói trong một gói tin khác để bảo vệ**
    4. Chỉ mã hóa khi đi qua firewall
79. Tunneling có thể áp dụng cho những loại VPN nào?
    1. Chỉ Site-to-Site VPN
    2. **Cả Site-to-Site VPN và Remote Access VPN**
    3. Chỉ Web VPN
    4. Chỉ VPN không mã hóa
80. GRE (Generic Routing Encapsulation) hỗ trợ điều gì trong VPN?
    1. Chỉ hỗ trợ truyền dữ liệu TCP
    2. **Hỗ trợ nhiều giao thức bên trong IP Tunnel**
    3. Chỉ dùng cho mạng nội bộ LAN
    4. Không hỗ trợ mã hóa dữ liệu
81. MPLS (Multiprotocol Label Switching) thích hợp với mô hình nào?
    1. VPN cá nhân
    2. **ISP và doanh nghiệp lớn**
    3. Mạng Wi-Fi công cộng
    4. Chỉ áp dụng trong mạng LAN
82. L2TP sử dụng cổng nào để truyền dữ liệu?
    1. TCP 1723
    2. **UDP 1701**
    3. TCP 80
    4. UDP 443
83. Điểm khác biệt chính giữa L2TP và PPTP là gì?
    1. PPTP có khả năng mã hóa mạnh hơn L2TP
    2. **L2TP kết hợp với IPSec để mã hóa**
    3. PPTP không hỗ trợ Windows
    4. L2TP hoạt động ở tầng ứng dụng của mô hình OSI
84. PPTP có điểm yếu bảo mật nào?
    1. Không hỗ trợ mã hóa
    2. **Dễ bị tấn công do sử dụng MS-CHAP v2**
    3. Không hỗ trợ nhiều giao thức mạng
    4. Không tương thích với các hệ điều hành hiện đại
85. IPSec chủ yếu được sử dụng cho loại VPN nào?
    1. VPN Web
    2. **VPN bảo mật trên nền Internet**
    3. Mạng LAN riêng biệt
    4. Kết nối không mã hóa
86. IPSec cung cấp những tính năng bảo mật nào?
    1. Xác thực nguồn gốc dữ liệu
    2. Đảm bảo tính toàn vẹn của dữ liệu
    3. Mã hóa dữ liệu khi truyền trên mạng
    4. **Tất cả các tính năng trên**
87. IPSec sử dụng cổng nào để truyền dữ liệu?
    1. **TCP 50 và 51**
    2. UDP 443
    3. TCP 80
88. Chế độ Tunnel Mode trong IPSec được sử dụng khi nào?
    1. Khi truyền dữ liệu giữa hai thiết bị trên cùng một mạng LAN
    2. **Khi truyền dữ liệu qua mạng không tin cậy như Internet**
    3. Khi chỉ cần mã hóa phần tiêu đề (header) của gói tin
    4. Khi không cần mã hóa dữ liệu
89. Điểm khác biệt chính giữa Transport Mode (h-h) và Tunnel Mode (p-p) trong IPSec là gì?
    1. **Transport Mode chỉ mã hóa phần dữ liệu (payload), Tunnel Mode mã hóa cả dữ liệu và tiêu đề (header)**
    2. Transport Mode chỉ dùng trong mạng LAN, Tunnel Mode dùng trong Internet
    3. Tunnel Mode không hỗ trợ mã hóa dữ liệu
    4. Transport Mode an toàn hơn Tunnel Mode
90. Khi nào nên sử dụng Transport Mode thay vì Tunnel Mode?
    1. Khi kết nối giữa hai VPN Gateway
    2. Khi cần mã hóa toàn bộ gói tin
    3. **Khi truyền dữ liệu trực tiếp giữa hai thiết bị trên cùng một mạng**
    4. Khi không cần mã hóa dữ liệu
91. ESP trong IPSec cung cấp tính năng gì?
    1. Chỉ mã hóa phần tiêu đề (header) của gói tin
    2. **Mã hóa dữ liệu và cung cấp chứng thực giới hạn (bao gói dữ liệu payload)**
    3. Chỉ xác thực nguồn gốc dữ liệu
    4. Chỉ hỗ trợ mạng LAN
92. ESP khác với Authentication Header (AH) ở điểm nào?
    1. ESP chỉ xác thực mà không mã hóa
    2. **AH xác thực cả header còn ESP thì không**
    3. ESP không hỗ trợ mạng VPN
    4. AH mã hóa mạnh hơn ESP
93. ESP thường được sử dụng trong chế độ nào của IPSec?
    1. Transport Mode
    2. Tunnel Mode
    3. **Cả Transport Mode và Tunnel Mode**
    4. Không sử dụng trong IPSec
94. Authentication Header (AH) trong IPSec có tác dụng gì?
    1. **Đảm bảo tính toàn vẹn và mã hóa toàn bộ gói tin IP**
    2. Mã hóa toàn bộ nội dung gói tin
    3. Chỉ áp dụng cho mạng LAN
    4. Thay thế hoàn toàn ESP
95. Điểm hạn chế của AH so với ESP là gì?
    1. AH hỗ trợ mã hóa mạnh hơn ESP
    2. **AH không mã hóa dữ liệu mà chỉ xác thực**
    3. AH không đảm bảo tính toàn vẹn của dữ liệu
    4. AH không hỗ trợ giao thức TCP
96. AH sử dụng thuật toán nào để xác thực gói tin?
    1. **HMAC-SHA1, HMAC-MD5**
    2. AES-256
    3. Blowfish
    4. DES
97. Internet Key Exchange (IKE) trong IPSec có nhiệm vụ gì?
    1. Mã hóa dữ liệu trong quá trình truyền
    2. **Đảm bảo an toàn khi trao đổi khóa bí mật giữa hai bên khi thiết lập đường hầm**
    3. Giúp VPN hoạt động mà không cần xác thực
    4. Xóa dữ liệu sau khi truyền
98. ISAKMP (Internet Security Association and Key Management Protocol) có chức năng gì trong IPSec?
    1. Chỉ mã hóa gói tin
    2. Chỉ hỗ trợ xác thực
    3. **Đàm phán và cung cấp chứng thực**
    4. Định tuyến dữ liệu trên Internet
99. Giao thức nào được sử dụng để gửi email?
    1. **SMTP (Simple Mail Transfer Protocol)**
    2. POP3
    3. IMAP
    4. HTTP
100. Giao thức POP3 chủ yếu được sử dụng để làm gì?
     1. Gửi email
     2. **Nhận email từ máy chủ về**
     3. Mã hóa email khi truyền đi
     4. Quản lý danh sách email trong mạng LAN
101. MIME (Multipurpose Internet Mail Extensions) có tác dụng gì trong email?
     1. Tăng tốc độ gửi email
     2. Ngăn chặn spam
     3. **Hỗ trợ gửi email có đính kèm file**
     4. Bảo vệ email khỏi virus
102. S/MIME cung cấp tính năng gì cho email?
     1. **Chứng thực, mã hóa và chữ ký số**
     2. Nén email để tăng tốc độ truyền tải
     3. Tạo tài khoản email tự động
     4. Chặn spam và virus
103. S/MIME sử dụng thuật toán nào để mã hóa email?
     1. MD5
     2. **DES, 3DES, RC2 (chứng thực: RSA)**
     3. HTTP
     4. Telnet
104. Hệ thống nào hỗ trợ S/MIME?
     1. Windows Mail
     2. Outlook Express
     3. Thunderbird
     4. **Tất cả các hệ thống trên**
105. PGP sử dụng phương pháp mã hóa nào?
     1. Chỉ mã hóa đối xứng
     2. **Chỉ mã hóa bất đối xứng**
     3. Kết hợp mã hóa đối xứng và bất đối xứng
     4. Không sử dụng mã hóa
106. Một trong những tính năng chính của PGP là gì?
     1. Tăng tốc độ tải email
     2. Hỗ trợ chặn spam
     3. **Chứng thực và mã hóa email**
     4. Tự động xóa email sau khi đọc
107. \SPAM là gì?
     1. Email bị mã hóa
     2. **Email rác, thường chứa quảng cáo**
     3. Email bảo mật cao
     4. Email chỉ có thể đọc bằng phần mềm chuyên dụng
108. Phishing có tác hại gì?
     1. Gửi email nhanh hơn
     2. Giúp người dùng bảo vệ tài khoản
     3. **Lừa đảo người dùng vào trang web giả mạo**
     4. Là một phương pháp bảo mật email
109. Trojan trong email thường hoạt động như thế nào?
     1. Mã hóa email để bảo mật
     2. Tăng tốc độ tải email
     3. **Đính kèm mã độc vào email để lây nhiễm khi mở**
     4. Giúp lọc email spam
110. SMTP Relay có thể bị lạm dụng để làm gì?
     1. **Phát tán email rác (SPAM)**
     2. Tăng tốc độ gửi email
     3. Giảm chi phí sử dụng email
     4. Mã hóa nội dung email
111. Một trong những biện pháp hạn chế SMTP Relay bị lạm dụng là gì?
     1. Chỉ sử dụng POP3 để nhận email
     2. **Không cho phép gửi email ẩn danh từ bên ngoài mà không xác thực**
     3. Giảm kích thước email được gửi đi
     4. Chỉ gửi email vào ban đêm
112. SMTP Relay thường sử dụng cổng nào?
     1. 443
     2. **25**
     3. 110
     4. 21
113. Giao thức HTTP sử dụng cổng nào?
     1. 21
     2. **80**
     3. 443
     4. 25
114. HTTP có nhược điểm gì về bảo mật?
     1. Không hỗ trợ truyền dữ liệu
     2. Chỉ hoạt động trên mạng LAN
     3. **Không có cơ chế mã hóa, chứng thực**
     4. Không hỗ trợ trình duyệt web
115. HTTPS khác với HTTP ở điểm nào?
     1. Sử dụng thuật toán nén để giảm dung lượng trang web
     2. Tăng tốc độ tải trang
     3. **Sử dụng TLS/SSL để mã hóa dữ liệu**
     4. Chỉ hoạt động trên mạng LAN
116. HTTPS thường được sử dụng cho mục đích nào?
     1. Truy cập diễn đàn
     2. Đọc tin tức
     3. **Giao dịch ngân hàng, thanh toán trực tuyến**
     4. Chơi game trực tuyến
117. HTTPS sử dụng cổng nào?
     1. 80
     2. **443**
     3. 25
     4. 110
118. SSL hoạt động trên tầng nào của mô hình OSI?
     1. Tầng mạng
     2. **Tầng vận chuyển**
     3. Tầng liên kết dữ liệu
     4. Tầng vật lý
119. SSL/TLS cung cấp các tính năng bảo mật nào?
     1. Mã hóa dữ liệu
     2. Xác thực danh tính giữa client và server
     3. Đảm bảo tính toàn vẹn của dữ liệu
     4. **Tất cả các tính năng trên**
120. TLS là phiên bản nâng cấp của giao thức nào?
     1. HTTPS
     2. SSH
     3. **SSL**
     4. IPsec
121. Để giới hạn quyền truy cập vào website theo địa chỉ IP, có thể sử dụng cơ chế nào?
     1. **Firewall hoặc cấu hình trên Web Server**
     2. Cấu hình trình duyệt web
     3. Chỉ cần thay đổi giao thức từ HTTP sang HTTPS
     4. Không thể giới hạn theo IP
122. Công cụ nào giúp giám sát truy cập vào máy chủ Web?
     1. Wireshark
     2. **Log file và hệ thống IDS (Intrusion Detection System)**
     3. Telnet
     4. FTP
123. Một trong những cách bảo vệ trình duyệt Web là gì?
     1. Vô hiệu hóa tường lửa
     2. **Giới hạn các script thực thi như JavaScript, VBScript**
     3. Sử dụng mật khẩu yếu để dễ nhớ
     4. Chỉ sử dụng trình duyệt mặc định của hệ điều hành
124. Tại sao cần cẩn thận khi sử dụng cookie trên trình duyệt?
     1. Cookie làm chậm tốc độ duyệt web
     2. Cookie không liên quan đến bảo mật
     3. **Cookie lưu trữ thông tin nhạy cảm và bị đánh cắp**
     4. Cookie giúp tăng cường mã hóa dữ liệu
125. ActiveX có thể gây rủi ro bảo mật vì lý do nào?
     1. ActiveX giúp tải trang web nhanh hơn
     2. **ActiveX có thể bị lợi dụng để chạy mã độc trên máy tính người dùng**
     3. ActiveX không liên quan đến bảo mật
     4. ActiveX chỉ ảnh hưởng đến tốc độ mạng
126. FTP sử dụng cổng nào để truyền dữ liệu?
     1. 443
     2. **21 (điều khiển) và 20 (dữ liệu)**
     3. 80
     4. 25
127. FTP có nhược điểm gì về bảo mật?
     1. **Không mã hóa dữ liệu, kể cả mật khẩu**
     2. Không hỗ trợ truyền tập tin lớn
     3. Chỉ hoạt động trên mạng LAN
     4. Không hỗ trợ nhiều hệ điều hành
128. Có bao nhiêu chế độ hoạt động trong FTP?
     1. 1
     2. **2 (Standard mode và Passive mode)**
     3. 3
     4. 4
129. FTPS khác với FTP ở điểm nào?
     1. **Sử dụng SSL/TLS để mã hóa dữ liệu**
     2. Không cần mật khẩu để đăng nhập
     3. Chỉ hoạt động trên mạng nội bộ
     4. Không hỗ trợ truyền tập tin lớn
130. FTPS sử dụng cổng nào cho điều khiển?
     1. 21
     2. **990 (898 dữ liệu)**
     3. 25
     4. 110
131. NetBIOS hoạt động trên các cổng nào?
     1. 22, 23, 80
     2. 443, 110, 25
     3. **TCP 137, 138, 139**
     4. UDP 53, 67, 68
132. NetBIOS trên TCP (NBT) có chức năng gì?
     1. Hỗ trợ truyền dữ liệu không dây
     2. **Vận chuyển dữ liệu NetBIOS trên các mạng tầng 3 như IP**
     3. Mã hóa dữ liệu trên FTP
     4. Quản lý địa chỉ IP trên Internet

\* NetBIOS: dịch vụ vận chuyển và giao dịch

\* NetBIUI: giao thức tầng 4

1. Dịch vụ LDAP được sử dụng để làm gì?
   1. **Cung cấp truy cập đến cơ sở dữ liệu tài nguyên mạng**
   2. Gửi email đến nhiều người dùng
   3. Tăng tốc độ tải trang web
   4. Quản lý firewall
2. LDAP sử dụng cổng nào?
   1. 80
   2. **389 (TCP), 636 (SSL/TLS)**
   3. 25
   4. 110
3. Secure LDAP (SLDAP) khác LDAP thông thường ở điểm nào?
   1. Không yêu cầu xác thực người dùng
   2. **Sử dụng SSL/TLS để mã hóa dữ liệu**
   3. Chỉ hoạt động trên hệ điều hành Linux
   4. Không hỗ trợ Windows