CHƯƠNG 1: TỔNG QUAN AN NINH MẠNG

Câu 1: An ninh mạng (network security) là gì?

A. Khả năng bảo vệ phần cứng của máy tính
B. **Khả năng bảo vệ thông tin trong không gian của mạng máy tính**
C. Bảo vệ dữ liệu khỏi sự thay đổi
D. Đảm bảo tính sẵn sàng của hệ thống

Câu 2: Mục tiêu nào sau đây không phải là mục tiêu của một hệ thống an toàn mạng?

A. Sự bảo mật (confidentiality)
B. Tính toàn vẹn (integrity)
C. Tính sẵn dùng (availability)
D. **Tăng tốc độ xử lý của hệ thống**

Câu 3: Tại sao an ninh mạng lại cần thiết?

A. Vì mạng máy tính ngày càng phát triển
B. Để ngăn chặn các hành vi xâm nhập bất hợp pháp
C. Để bảo vệ dữ liệu khỏi bị đánh cắp
D. **Tất cả các lý do trên**

Câu 4: An toàn thông tin (information security) nhằm mục đích gì?

A. Bảo vệ phần mềm máy tính
B. **Bảo vệ môi trường thông tin kinh tế xã hội**
C. Ngăn chặn các cuộc tấn công từ chối dịch vụ
D. Đảm bảo tính sẵn sàng của phần cứng

Câu 5: Đe dọa có tổ chức (structured threat) thường có đặc điểm gì?

A. Mang tính tức thời và dễ phát hiện
B. **Được che giấu rất khó phát hiện**
C. Do hacker thiếu kinh nghiệm thực hiện
D. Chỉ sử dụng các công cụ miễn phí

Câu 6: Đe dọa từ bên trong mạng chiếm khoảng bao nhiêu phần trăm các vấn đề bảo mật?

A. 50%
B. 60%
C. **70%**
D. 80%

Câu 7: Đe dọa thụ động (passive threat) có đặc điểm gì?

A. Thay đổi dữ liệu của hệ thống
B. **Không thay đổi dữ liệu của hệ thống**
C. Gây ra sự cố ngừng hoạt động
D. Xâm nhập trái phép vào mạng

Câu 8: Hacker mũ trắng (white hat) có mục đích gì khi xâm nhập hệ thống?

A. Phá hoại dữ liệu
B. Đánh cắp thông tin
C. **Thực hiện với ý tốt, ví dụ như bảo mật hệ thống**
D. Gây rối loạn mạng

Câu 9: Hacker mũ xanh (blue hat) thường làm việc cho ai?

A. Chính phủ
B. **Các công ty lớn để tìm lỗi hệ thống**
C. Tổ chức tội phạm
D. Các nhóm hacker tự do

Câu 10: Loại tấn công nào sau đây không thuộc 3 loại tấn công chính được đề cập?

A. Do thám (reconnaissance)
B. Truy cập (access)
C. Từ chối dịch vụ (DoS)
D. **Tấn công phần cứng**

Câu 11: Tấn công đo thám (reconnaissance) nhằm mục đích gì?

A. Phá hủy hệ thống
B. **Thu thập thông tin để khai thác sau này**
C. Ngăn chặn dịch vụ hoạt động
D. Thay đổi dữ liệu

Câu 12: Kỹ thuật nào sau đây không thuộc tấn công đo thám?

A. Nghe lén (sniffing)
B. Quét địa chỉ IP (ping sweep)
C. Quét cổng (port sweep)
D. **Tấn công từ chối dịch vụ (DoS)**

Câu 13: Công cụ nào sau đây thường được dùng để nghe lén (sniffing)?

A. Fping
B. **Wireshark**
C. Nmap
D. Ping sweep

Câu 14: Kỹ thuật quét địa chỉ IP (ping sweep) hoạt động như thế nào?

A. Gửi gói tin TCP đến máy chủ
B. **Gửi gói ICMP request để kiểm tra host nào đang hoạt động**
C. Quét các cổng đang mở
D. Nghe lén dữ liệu truyền qua mạng

Câu 15: Tấn công truy cập (access) nhằm mục đích gì?

A. Thu thập thông tin
B. Ngăn chặn dịch vụ
C. **Xâm nhập trái phép vào hệ thống**
D. Gây rối loạn mạng

Câu 16: Tấn công từ chối dịch vụ (DoS) có mục tiêu chính là gì?

A. Đánh cắp dữ liệu
B. **Làm gián đoạn hoặc ngừng hoạt động của hệ thống**
C. Thay đổi thông tin
D. Thu thập thông tin

Câu 17: Phần mềm độc hại (malware) bao gồm những loại nào sau đây?

A. Virus, Worm, Trojan
B. Spyware, Adware, Rootkit
C. Keylogger, Cookie
D. **Tất cả các loại trên**

Câu 18: Virus máy tính có đặc điểm gì?

A. **Cần chương trình chủ để lây lan**
B. Tự nhân bản mà không cần chương trình chủ
C. Giả dạng phần mềm hợp pháp
D. Ghi lại thao tác bàn phím

Câu 19: Worm khác với Virus ở điểm nào?

A. Cần chương trình chủ để hoạt động
B. **Tự nhân bản và lây lan qua mạng**
C. Chỉ hoạt động trên phần cứng
D. Không gây hại cho hệ thống

Câu 20: Trojan hoạt động như thế nào?

A. Tự nhân bản qua mạng
B. Ghi lại thao tác người dùng
C. **Giả dạng phần mềm hợp pháp để lừa người dùng**
D. Tấn công từ chối dịch vụ

Câu 21: Spyware chủ yếu được sử dụng để làm gì?

A. Phá hủy dữ liệu
B. **Thu thập thông tin cá nhân mà không được phép**

C. Tự nhân bản qua mạng
D. Gây gián đoạn dịch vụ

Câu 22: Adware có mục đích chính là gì?

A. Đánh cắp dữ liệu
B. **Hiển thị quảng cáo không mong muốn**
C. Ghi lại thao tác bàn phím
D. Tấn công hệ thống

Câu 23: Rootkit có khả năng gì đặc biệt?

A. Ghi lại thao tác người dùng
B. **Ẩn hoạt động của phần mềm độc hại**
C. Hiển thị quảng cáo
D. Tự nhân bản qua mạng

Câu 24: Keylogger thuộc nhóm phần mềm nào?

A. Virus
B. **Spyware**
C. Worm
D. Trojan

Câu 25: Cookie được sử dụng để làm gì?

A. Phá hủy dữ liệu
B. **Theo dõi hoạt động người dùng trên web**
C. Ghi lại thao tác bàn phím
D. Tấn công từ chối dịch vụ

Câu 26: Yêu cầu cơ bản nào sau đây không thuộc hệ thống an toàn mạng?

A. Chứng thực (authentication)
B. Phân quyền (authorization)
C. Giám sát (monitoring)
D. **Tăng dung lượng lưu trữ**

Câu 27: Tính toàn vẹn (integrity) trong an ninh mạng nghĩa là gì?

A. Bảo vệ dữ liệu khỏi bị truy xuất
B. **Bảo đảm dữ liệu không bị thay đổi hay phá hoại**
C. Đảm bảo hệ thống luôn sẵn sàng
D. Ngăn chặn tấn công từ chối dịch vụ

Câu 28: Hacker mũ đen (black hat) thường có mục đích gì?

A. Bảo vệ hệ thống
B. **Phá hoại hoặc đánh cắp thông tin**
C. Tìm lỗi phần mềm
D. Làm việc cho chính phủ

Câu 29: Đe dọa vô tình (unintentional threat) có thể là gì?

A. Tấn công có chủ đích
B. **Sự kiện ngẫu nhiên gây hại cho hệ thống**
C. Nghe lén thông tin
D. Thay đổi dữ liệu

Câu 30: Công cụ nào sau đây không dùng để quét địa chỉ IP?

A. Fping
B. Network Sonar
C. **Wireshark**
D. Pinger

Dưới đây là 20 câu trắc nghiệm được xây dựng dựa trên nội dung tài liệu bạn cung cấp, tiếp nối số thứ tự từ bộ câu hỏi trước (bắt đầu từ câu 31). Các câu hỏi tập trung vào các khái niệm về chứng thực (Authentication), phân quyền (Authorization), giám sát (Accounting), và các mô hình bảo mật liên quan. Đáp án đúng được in đậm.

Câu 31: Kiến trúc AAA trong hệ thống mạng an toàn bao gồm những thành phần nào?

A. Authentication, Availability, Access
B. **Authentication, Authorization, Accounting**
C. Analysis, Authorization, Auditing
D. Authentication, Access, Administration

Câu 32: Chứng thực (Authentication) trong hệ thống mạng có mục đích gì?

A. Phân quyền cho người dùng
B. **Xác minh danh tính số của người gửi thông tin**
C. Ghi lại hoạt động của hệ thống
D. Quét hệ thống để tìm lỗ hổng

Câu 33: Điểm yếu nào sau đây không phải là điểm yếu của hệ thống chứng thực bằng tài khoản-mật khẩu?

A. Mật khẩu có thể bị quên
B. Mật khẩu dễ bị lộ
C. **Mật khẩu được mã hóa an toàn**
D. Dễ dàng bị dò tìm

Câu 34: Chứng thực 2 chiều (2-way authentication) khác với chứng thực 1 chiều ở điểm nào?

A. Chỉ yêu cầu mật khẩu từ một phía
B. **Cả hai bên đều phải xác nhận danh tính với nhau**
C. Không sử dụng username
D. Dữ liệu không được mã hóa

Câu 35: PAP (Password Authentication Protocol) có đặc điểm nào sau đây?

A. Dữ liệu được mã hóa bằng MD5
B. **Gửi trực tiếp username và password dưới dạng plaintext**
C. Chỉ hỗ trợ chứng thực 2 chiều
D. An toàn hơn CHAP

Câu 36: CHAP (Challenge Handshake Authentication Protocol) có ưu điểm gì so với PAP?

A. Gửi dữ liệu dưới dạng plaintext
B. **Dữ liệu được mã hóa và không gửi trực tiếp mật khẩu**
C. Hỗ trợ chứng thực 1 chiều
D. Dễ bị tấn công hơn PAP

Câu 37: Hệ thống Kerberos được phát triển bởi tổ chức nào?

A. Microsoft
B. Cisco
C. **MIT**
D. Linux Foundation

Câu 38: Hệ thống Kerberos hoạt động dựa trên nguyên lý nào?

A. Gửi mật khẩu trực tiếp qua mạng
B. **Mã hóa sử dụng khóa mật và bên thứ ba đáng tin cậy**
C. Sử dụng OTP để xác thực
D. Không cần đồng bộ hóa thời gian

Câu 39: Mật khẩu sử dụng một lần (OTP) thường đi kèm với điều kiện nào?

A. **Đồng bộ hóa thời gian với server xác thực**
B. Không cần thiết bị phần cứng
C. Chỉ sử dụng trong chứng thực 1 chiều
D. Dữ liệu gửi dưới dạng plaintext

Câu 40: Thẻ cứng (Token card) thường được dùng kết hợp với gì để tăng cường bảo mật?

A. **Số PIN hoặc mật khẩu**
B. Quét hệ thống
C. Ghi file nhật ký
D. Phân quyền DAC

Câu 41: Sinh trắc học (Biometrics) có nhược điểm nào sau đây?

A. **Đặc điểm người dùng có thể thay đổi theo thời gian**
B. Không cần thiết bị đọc
C. Luôn chính xác 100%
D. Không thể tích hợp với hệ thống mạng

Câu 42: Phân quyền (Authorization) có mục đích gì trong hệ thống mạng an toàn?

A. Xác minh danh tính người dùng
B. **Xác định quyền và sự cho phép của người dùng trong hệ thống**
C. Ghi lại hoạt động của người dùng
D. Quét lỗ hổng hệ thống

Câu 43: Điều khiển truy cập tùy quyền (DAC) khác với điều khiển truy cập bắt buộc (MAC) ở điểm nào?

A. Hệ thống quyết định quyền truy cập
B. **Chủ nhân tài nguyên quyết định quyền truy cập**
C. Không cho phép chủ nhân kiểm soát tài nguyên
D. Chỉ áp dụng cho ứng dụng đa tầng

Câu 44: Trong mô hình MAC, ai là người quyết định quyền truy cập vào tài nguyên?

A. Chủ nhân tài nguyên
B. Người dùng cuối
C. **Hệ thống hoặc người quản trị**
D. Ứng dụng tự động

Câu 45: Điều khiển truy cập dựa trên vai trò (RBAC) có ưu điểm gì?

A. Quyền được cấp trực tiếp cho người dùng
B. **Quyền được cấp thông qua vai trò, đơn giản hóa quản lý**
C. Không cần phân vai trò trong tổ chức
D. Phức tạp hơn DAC

Câu 46: Mô hình Bell La-Padula tập trung vào khía cạnh nào của bảo mật?

A. Tính toàn vẹn dữ liệu
B. **Phân loại mức bảo mật và quyền truy xuất**
C. Giám sát hoạt động người dùng
D. Điều khiển truy cập tùy quyền

Câu 47: Mô hình Biba khác với mô hình Bell La-Padula ở điểm nào?

A. Không phân loại mức bảo mật
B. **Tập trung vào kiểm tra tính toàn vẹn dữ liệu**
C. Cho phép sửa đổi dữ liệu ở cấp cao hơn
D. Không dựa trên cơ chế MAC

Câu 48: Giám sát (Accounting) trong hệ thống mạng an toàn không bao gồm hoạt động nào sau đây?

A. Ghi file nhật ký (Logging)
B. Quét hệ thống (Scanning)
C. Kiểm soát (Monitoring)
D. **Tạo mật khẩu mới cho người dùng**

Câu 49: File nhật ký (Log file) trong giám sát có vai trò gì?

A. Quét lỗ hổng hệ thống
B. **Ghi nhận các sự kiện và thời điểm xảy ra trong hệ thống**
C. Phân quyền cho người dùng
D. Mã hóa dữ liệu truyền qua mạng

Câu 50: Quét hệ thống (System scanning) giúp ích gì trong giám sát?

A. Ghi lại hoạt động của người dùng
B. **Phát hiện điểm yếu trong hệ thống để khắc phục**
C. Xác minh danh tính người dùng
D. Phân loại mức bảo mật dữ liệu

CHƯƠNG 2: AN TOÀN CHO CÁC THIẾT BỊ MẠNG

Câu 51: Mục tiêu chính của chương "An toàn cho các thiết bị mạng" là gì?

A. Cung cấp cách sử dụng thiết bị mạng
B. **Cung cấp cái nhìn tổng quan về cách đảm bảo an toàn cho các thiết bị mạng trên các tầng OSI**
C. Giới thiệu mô hình OSI
D. Hướng dẫn cài đặt phần mềm bảo mật

Câu 52: Điểm truy cập (access point) trên tầng 1 được định nghĩa là gì?

A. Thiết bị kết nối mạng không dây
B. **Nơi người dùng hợp lệ và không hợp lệ truy cập vào mạng để truy xuất tài nguyên**
C. Điểm kết nối giữa các switch
D. Địa chỉ IP của máy chủ

Câu 53: Điểm yếu của cáp đồng trục trên tầng 1 là gì?

A. Dễ bị nghe lén bằng thiết bị cảm ứng bao quanh dây cáp
B. **Có thể bị thu nhận tín hiệu bằng thiết bị cảm ứng mà không phát hiện được**
C. Không hỗ trợ truyền tín hiệu xa
D. Không thể mã hóa dữ liệu

Câu 54: Biện pháp bảo vệ cáp đồng trục bao gồm gì?

A. Mã hóa tín hiệu
B. **Cô lập đường cáp và không cho tiếp xúc trực tiếp**
C. Sử dụng bộ chia tín hiệu
D. Tăng cường khoảng cách truyền

Câu 55: Điểm yếu của cáp xoắn đôi (UTP/STP) trên tầng 1 nằm ở đâu?

A. Dễ bị ngắt kết nối
B. **Dễ bị thâm nhập qua switch hoặc patch-panel**
C. Không hỗ trợ mạng không dây
D. Tín hiệu không ổn định

Câu 56: Cách bảo vệ cáp xoắn đôi bao gồm biện pháp nào sau đây?

A. Sử dụng bộ lọc MAC
B. **Tách riêng switch trung tâm và gắn tủ khóa cho patch-panel**
C. Mã hóa dữ liệu bằng WPA
D. Giảm khoảng cách kết nối

Câu 57: Điểm yếu của cáp quang trên tầng 1 nằm ở đâu?

A. Dễ bị nghe lén qua bộ chia (splitter) tại các đầu nối
B. **Có thể bị chèn bộ chia tại đầu nối để nghe lén tín hiệu**
C. Không hỗ trợ truyền tín hiệu xa
D. Dễ bị ngắt kết nối vật lý

Câu 58: Tại sao mạng hồng ngoại (infrared) trên tầng 1 khó bị xâm nhập?

A. Tín hiệu được mã hóa mạnh
B. **Yêu cầu hai thiết bị phải "nhìn thấy nhau" và khoảng cách gần**
C. Sử dụng khóa WEP
D. Không cần thiết bị thu phát

Câu 59: Điểm yếu lớn nhất của mạng không dây dùng sóng radio (RF) là gì?

A. Khoảng cách truyền tín hiệu ngắn
B. **Ai trong phạm vi phủ sóng cũng có thể nhận được tín hiệu**
C. Không hỗ trợ mã hóa
D. Dễ bị ngắt kết nối

Câu 60: Cơ chế bảo mật nào được đề xuất cho mạng không dây dùng sóng radio?

A. Sử dụng ACL
B. **Cài đặt khóa WEP hoặc WPA để mã hóa dữ liệu**
C. Tắt SSID
D. Lọc gói tin

Câu 61: Nguy cơ lớn nhất khi sử dụng Modem trên tầng 1 là gì?

A. Dễ bị tấn công qua giao thức PAP
B. **Bị xâm nhập qua chương trình War Dialer khi gắn trực tiếp vào máy tính**
C. Không hỗ trợ VPN
D. Tín hiệu không ổn định

Câu 62: Cách ngăn ngừa xâm nhập qua Modem bao gồm gì?

A. Sử dụng WPA
B. **Giới hạn sử dụng và cấu hình Modem chỉ cho phép hướng gọi đi**
C. Lọc địa chỉ MAC
D. Tăng cường mã hóa tín hiệu

Câu 63: Trên tầng 2, switch có thể bị tấn công bằng cách nào?

A. Nghe lén tín hiệu qua cáp quang
B. **Giả mạo ARP để chuyển hướng lưu lượng qua máy của kẻ xâm nhập**
C. Sử dụng War Dialer
D. Chèn bộ chia tín hiệu

Câu 64: Kết quả của tấn công giả mạo ARP trên switch là gì?

A. Switch ngừng hoạt động
B. **Dữ liệu giữa các client đi qua máy của kẻ xâm nhập mà không bị phát hiện**
C. Địa chỉ IP bị thay đổi
D. Tín hiệu mạng bị gián đoạn

Câu 65: Biện pháp bảo mật nào được đề xuất cho Wireless Access Point trên tầng 2?

A. Sử dụng ACL
B. **Ẩn SSID và tạo bộ lọc MAC**
C. Tăng công suất tín hiệu
D. Giảm khoảng cách phủ sóng

Câu 66: Router trên tầng 3 có chức năng bảo mật nào sau đây?

A. Mã hóa dữ liệu bằng WPA
B. **Ngăn chặn broadcast và sử dụng ACL để chặn gói tin**
C. Lọc nội dung gói tin
D. Giám sát lưu lượng mạng

Câu 67: Tấn công tính năng vạch đường động (dynamic routing) của router diễn ra như thế nào?

A. Nghe lén tín hiệu qua cáp
B. **Giả mạo địa chỉ router và gửi thông tin vạch đường sai lệch**
C. Sử dụng War Dialer
D. Chèn bộ chia tín hiệu

Câu 68: Cách ngăn ngừa tấn công vạch đường động trên router là gì?

A. Sử dụng WPA
B. **Dùng giao thức vạch đường có mã hóa và cài đặt chứng thực**
C. Tắt SSID
D. Lọc địa chỉ MAC

Câu 69: Giao thức nào sau đây không an toàn khi sử dụng trên RAS (Remote Access Server)?

A. CHAP
B. **PAP**
C. MS-CHAP
D. EAP

Câu 70: Firewall trên tầng 3 hoạt động dựa trên cơ chế nào?

A. Lọc nội dung gói tin
B. **Lọc gói tin dựa trên địa chỉ IP hoặc cổng**
C. Giám sát trạng thái toàn bộ tầng
D. Mã hóa dữ liệu

Câu 71: Chính sách bảo mật nào được xem là tốt hơn cho Firewall trên tầng 3?

A. **Mặc nhiên cấm (deny by default)**
B. Mặc nhiên cho phép (allow by default)
C. Lọc theo nội dung
D. Cho phép tất cả lưu lượng

Câu 72: Ưu điểm lớn nhất của Firewall lọc gói trên tầng 3 là gì?

A. Kiểm tra nội dung gói tin
B. **Tốc độ nhanh do chỉ kiểm tra header**
C. Ngăn chặn tất cả tấn công
D. Hoạt động trên tầng ứng dụng

Câu 73: Hạn chế của Firewall trên tầng 3 là gì?

A. Tốc độ chậm
B. **Không quan tâm đến nội dung gói, dễ bỏ sót gói độc hại**
C. Khó cấu hình
D. Không hỗ trợ ACL

Câu 74: Proxy Server trên tầng 4 có vai trò gì?

A. **Cho phép truy xuất tài nguyên bên ngoài và ngăn chặn xâm nhập**
B. Lọc gói tin theo địa chỉ IP
C. Mã hóa dữ liệu bằng WPA
D. Quản lý switch trung tâm

Câu 75: Ưu điểm nào sau đây không phải của Proxy Server?

A. Tăng tốc độ truy xuất web
B. Lọc thông tin theo giao thức
C. **Hoạt động như switch trung tâm**
D. Ngăn chặn xâm nhập không mong muốn

Câu 76: Điểm yếu phổ biến của máy trạm (workstation) trên tầng 4 là gì?

A. Không hỗ trợ TCP/IP
B. **Ít được quan tâm bảo mật, dễ bị tấn công**
C. Không kết nối được mạng
D. Dễ bị ngắt tín hiệu

Câu 77: Biện pháp bảo mật nào không được đề xuất cho máy trạm?

A. Gỡ bỏ dịch vụ không cần thiết
B. Cập nhật bản vá lỗi
C. **Cài đặt phần mềm không rõ nguồn gốc**
D. Cài đặt tường lửa

Câu 78: Trên tầng 4, Proxy Server giúp giám sát lưu lượng mạng bằng cách nào?

A. Lọc gói tin theo cổng
B. **Lưu log file các truy cập**
C. Tắt SSID
D. Sử dụng ACL

Câu 79: Tại sao máy trạm thường kém an toàn hơn máy chủ trên tầng 4?

A. Không hỗ trợ mã hóa
B. **Ít được chú trọng bảo mật hơn so với máy chủ**
C. Không kết nối Internet
D. Không sử dụng TCP/IP

Câu 80: Biện pháp nào sau đây không liên quan đến bảo mật RAS trên tầng 3?

A. Sử dụng CHAP
B. Chứng thực qua RADIUS
C. **Ẩn SSID**
D. Kết hợp với smartcard

CHƯƠNG 3: GIA CỐ HỆ THỐNG

Câu 81: Mục tiêu chính của chương "Gia cố hệ thống" là gì?

A. Hướng dẫn cài đặt hệ điều hành
B. **Cung cấp cái nhìn tổng quan về các kỹ thuật gia cố hệ thống để ngăn chặn tấn công**
C. Giới thiệu các giao thức mạng
D. Hướng dẫn sử dụng phần mềm antivirus

Câu 82: Gia cố hệ thống được định nghĩa như thế nào?

A. Quá trình cài đặt bản cập nhật
B. **Quá trình làm cho hệ thống máy tính và mạng vững chắc, khó bị tấn công hơn**
C. Quá trình mã hóa dữ liệu
D. Quá trình sao lưu dữ liệu

Câu 83: Đối tượng nào sau đây không nằm trong danh sách cần gia cố?

A. Hệ điều hành
B. Hệ điều hành mạng
C. Ứng dụng mạng
D. **Phần cứng máy tính**

Câu 84: Nguyên tắc cấp quyền cho người dùng trong gia cố hệ thống tập tin là gì?

A. Cấp quyền tối đa để tiện sử dụng
B. **Cấp quyền tối thiểu vừa đủ để hoàn thành công việc**
C. Cấp quyền ngẫu nhiên theo yêu cầu
D. Không cấp quyền cho người dùng

Câu 85: Update trong gia cố hệ điều hành khác với Upgrade ở điểm nào?

A. Update tính phí, Upgrade miễn phí
B. **Update sửa lỗi và thay thế miễn phí, Upgrade bổ sung tính năng tính phí**
C. Update không cần kiểm tra, Upgrade cần kiểm tra
D. Update áp dụng cho phần cứng, Upgrade áp dụng cho phần mềm

---

Câu 86: Hotfix thường được sử dụng trong trường hợp nào?

A. Cập nhật toàn bộ hệ điều hành
B. **Sửa lỗi trên một số lượng ít máy trạm hoặc server**
C. Bổ sung tính năng mới
D. Gia cố ứng dụng mạng

Câu 87: Đặc điểm nào sau đây đúng với Patch trong gia cố hệ điều hành?

A. Được kiểm tra kỹ lưỡng trên nhiều hệ thống
B. **Chủ yếu liên quan đến vấn đề an toàn, sửa lỗi tạm thời**
C. Không cần sao lưu trước khi cài đặt
D. Tương tự Update nhưng tính phí

Câu 88: Biện pháp nào không được khuyến nghị khi gia cố Web Server?

A. Cài đặt bản cập nhật cho hệ điều hành
B. Đặt Web Server sau tường lửa
C. **Cho phép tài khoản anonymous toàn quyền truy cập**
D. Sử dụng chứng thực SSL khi cần

Câu 89: Mail Server có thể bị tấn công bằng cách nào sau đây?

A. Giả mạo ARP
B. **Tấn công relay hoặc DoS**
C. Nghe lén qua cáp quang
D. Chèn bộ chia tín hiệu

Câu 90: Biện pháp gia cố FTP Server bao gồm điều nào sau đây?

A. Gửi thông tin chứng thực dạng mã hóa
B. **Tách biệt tài khoản FTP với tài khoản hệ điều hành**
C. Cho phép truy cập anonymous không giới hạn
D. Đặt FTP Server ngoài DMZ

Câu 91: DNS Server dễ bị tấn công bằng cách nào?

A. Nghe lén tín hiệu
B. **Đánh lừa người dùng qua địa chỉ giả mạo**
C. Sử dụng War Dialer
D. Chèn mã độc vào hệ điều hành

Câu 92: Tại sao dịch vụ chia sẻ file và máy in cần được tắt khi không sử dụng?

A. Để tăng tốc độ mạng
B. **Để ngăn người ngoài thấy tài nguyên như người dùng nội bộ**
C. Để tiết kiệm băng thông
D. Để giảm tải cho hệ điều hành

Câu 93: Yếu tố nào cần chú ý khi gia cố Database Server?

A. **Mật khẩu đủ mạnh và sao lưu dữ liệu định kỳ**
B. Tắt hoàn toàn các port không dùng
C. Cho phép truy cập từ mọi địa chỉ IP
D. Không cần bản vá lỗi

Câu 94: Chính sách an ninh mạng được định nghĩa là gì?

A. Tập hợp các phần mềm bảo mật
B. **Tập hợp quy tắc xác định thao tác nào được phép trên mạng**
C. Danh sách các bản cập nhật
D. Hướng dẫn cài đặt hệ điều hành

Câu 95: Chính sách giới hạn truy cập nhằm mục đích gì?

A. Tăng tốc độ truy cập mạng
B. **Hạn chế truy cập vào dữ liệu và hệ thống không cần thiết**
C. Cho phép tất cả người dùng truy cập Internet
D. Giảm tải cho quản trị viên

Câu 96: Chính sách an ninh cho máy trạm không bao gồm vấn đề nào sau đây?

A. Quyền của người dùng cục bộ
B. Cài đặt phần mềm
C. **Cấu hình router**
D. Sử dụng thiết bị di động

Câu 97: Chính sách an ninh vật lý tập trung vào yếu tố nào?

A. Mã hóa dữ liệu
B. **Bảo vệ địa điểm và tài sản vật lý**
C. Lọc gói tin mạng
D. Giám sát lưu lượng truy cập

Câu 98: Bước đầu tiên khi xây dựng chính sách an ninh mạng là gì?

A. Cài đặt phần mềm bảo mật
B. **Phân tích rủi ro**
C. Giám sát hệ thống
D. Sao lưu dữ liệu

Câu 99: Nguyên tắc "Need to know" trong chính sách an ninh mạng có nghĩa là gì?

A. Cung cấp tất cả thông tin cho mọi người
B. **Chỉ cung cấp dữ liệu vừa đủ để thực hiện công việc**
C. Giới hạn truy cập vào phần cứng
D. Yêu cầu chứng thực SSL

Câu 100: Chính sách "Acceptable Use Policy" (AUP) quy định điều gì?

A. **Hoạt động nào được phép thực hiện trên mạng**
B. Cách cài đặt bản vá lỗi
C. Quy trình sao lưu dữ liệu
D. Cấu hình tường lửa

Câu 101: Yêu cầu nào sau đây không thuộc chính sách quản lý mật khẩu?

A. Mật khẩu phải đủ mạnh
B. Thay đổi mật khẩu định kỳ
C. **Sử dụng mật khẩu mặc định của hệ thống**
D. Không sử dụng lại mật khẩu cũ

Câu 102: Chính sách "Disposal and Destruction" liên quan đến việc gì?

A. Cài đặt phần mềm mới
B. **Xóa vĩnh viễn dữ liệu trên thiết bị trước khi thải bỏ**
C. Giám sát truy cập mạng
D. Cấu hình DNS Server

Câu 103: Chính sách nhân sự (HR Policy) quy định điều gì về chuẩn mực đạo đức?

A. **Mô tả loại hình nhân viên mong muốn và quy định đạo đức nghề nghiệp**
B. Quy định cách cài đặt phần mềm
C. Hướng dẫn cập nhật hệ điều hành
D. Quy định cấu hình mạng

Câu 104: Mục đích chính của pháp y máy tính (computer forensics) là gì?

A. Khôi phục dữ liệu bị mất
B. **Thu thập chứng cứ để phát hiện tội phạm**
C. Cài đặt lại hệ điều hành
D. Gia cố ứng dụng mạng

Câu 105: Vai trò nào sau đây không thuộc nhóm điều tra xâm nhập?

A. First Responder
B. Investigator
C. Crime Scene Technician
D. **Network Administrator**

Câu 106: Chuỗi hành trình (Chain of Custody) được sử dụng để làm gì?

A. Theo dõi lưu lượng mạng
B. **Ghi lại lịch sử ai điều khiển chứng cứ và khi nào**
C. Sao lưu dữ liệu
D. Cấu hình hệ điều hành

Câu 107: Công cụ nào sau đây hỗ trợ thu thập chứng cứ trong điều tra xâm nhập?

A. **Encase**
B. Microsoft Word
C. Notepad
D. Paint

Câu 108: Khi thu thập chứng cứ, điều nào không được phép?

A. Sao chép dữ liệu bằng phần mềm chuyên dụng
B. **Ghi đè lên file cấu hình**
C. Lưu trữ log file
D. Sử dụng Safeback

Câu 109: Ai là người thường phát hiện ra sự cố xâm nhập đầu tiên?

A. Quản trị viên
B. **Người dùng**
C. Hacker
D. Đội điều tra

Câu 110: Biện pháp nào được khuyến nghị khi khôi phục tạm thời sau xâm nhập?

A. Format lại ổ cứng
B. **Thay thế bằng hệ thống khác để giữ nguyên chứng cứ**
C. Shutdown hệ thống ngay lập tức
D. Khôi phục file đã xóa

CHƯƠNG 4: CĂN BẢN VỀ MẬT MÃ

Câu 111: Mục tiêu chính của chương về mật mã là gì?

A. Hướng dẫn cài đặt phần mềm mã hóa
B. **Cung cấp cái nhìn tổng quan về mật mã và ứng dụng trong an ninh mạng**
C. Giới thiệu các giao thức mạng cơ bản
D. Hướng dẫn sử dụng chứng chỉ số

Câu 112: Mật mã (cryptography) được định nghĩa như thế nào?

A. Quá trình sao lưu dữ liệu
B. **Nghệ thuật biến đổi dữ liệu gốc và khôi phục lại để sử dụng**
C. Quá trình tạo khóa ngẫu nhiên
D. Quá trình phân tích dữ liệu mạng

Câu 113: Giải thuật nào sau đây không thuộc nhóm mã hóa mà dùng để tạo "dấu vân tay" dữ liệu?

A. Đối xứng
B. Bất đối xứng
C. **Băm (hashing)**
D. RSA

Câu 114: Đầu ra của giải thuật băm MD5 có đặc điểm gì?

A. 160 bit
B. **128 bit hoặc 32 ký tự Hex**
C. 256 bit
D. Có thể dịch ngược về dữ liệu gốc

Câu 115: Giải thuật SHA-1 có ưu điểm gì so với MD5?

A. Nhanh hơn MD5
B. **Bảo mật hơn MD5 với đầu ra 160 bit**
C. Dễ dàng dịch ngược
D. Sử dụng khóa 128 bit

Câu 116: HMAC khắc phục điểm yếu nào của các giải thuật băm thông thường?

A. Tốc độ xử lý chậm
B. **Tấn công "Kẻ đứng giữa" (Man-in-the-middle)**
C. Không tạo được digest
D. Dữ liệu đầu ra quá dài

Câu 117: HMAC-SHA-1 sử dụng khóa có độ dài bao nhiêu?

A. 128 bit
B. **160 bit**
C. 192 bit
D. 256 bit

Câu 118: Mã hóa (encryption) khác với băm (hashing) ở điểm nào?

A. Băm tạo tính bí mật cho dữ liệu
B. **Mã hóa tạo sự bí mật, băm kiểm tra tính toàn vẹn**
C. Mã hóa không dùng khóa
D. Băm có thể giải mã ngược lại

Câu 119: Giải thuật mã hóa đối xứng sử dụng bao nhiêu khóa?

A. Hai khóa khác nhau
B. **Một khóa chung cho mã hóa và giải mã**
C. Không cần khóa
D. Ba khóa liên tiếp

Câu 120: Giải thuật DES có độ dài khóa thực tế là bao nhiêu bit?

A. 64 bit
B. **56 bit**
C. 128 bit
D. 168 bit

Câu 121: Tại sao DES hiện nay không còn được xem là an toàn?

A. Tốc độ mã hóa chậm
B. **Độ dài khóa ngắn (56 bit)**
C. Không hỗ trợ mạng Feistel
D. Không dùng được trong IPSec

Câu 122: 3DES cải thiện bảo mật so với DES bằng cách nào?

A. Tăng tốc độ mã hóa
B. **Sử dụng ba khóa 56 bit, tổng cộng 168 bit**
C. Giảm số chu trình Feistel
D. Chuyển sang mã hóa bất đối xứng

Câu 123: AES được gọi là gì trong tiếng Anh?

A. Advanced Encryption Standard
B. **Advanced Encryption Standard (Tiêu chuẩn mã hóa tiên tiến)**
C. Asymmetric Encryption System
D. American Encryption Standard

Câu 124: Độ dài khóa của AES có thể là bao nhiêu?

A. 56, 64, 128 bit
B. **128, 192, 256 bit**
C. 160, 192, 256 bit
D. 128, 256, 512 bit

Câu 125: Giải thuật mã hóa bất đối xứng sử dụng bao nhiêu khóa?

A. Một khóa chung
B. **Hai khóa: khóa công khai và khóa bí mật**
C. Ba khóa liên tiếp
D. Không cần khóa

Câu 126: Giải thuật RSA thuộc nhóm nào?

A. Băm
B. Đối xứng
C. **Bất đối xứng**
D. Trao đổi khóa

Câu 127: Diffie-Hellman (DH) chủ yếu được sử dụng để làm gì?

A. Mã hóa dữ liệu
B. **Trao đổi khóa an toàn**
C. Tạo chứng chỉ số
D. Kiểm tra tính toàn vẹn

Câu 128: Hạ tầng khóa công khai (PKI) có vai trò gì?

A. Tạo dữ liệu mã hóa
B. **Quản lý và phân phối khóa công khai, chứng chỉ số**
C. Kiểm tra tính toàn vẹn dữ liệu
D. Sao lưu dữ liệu

Câu 129: Nhà cung cấp chứng chỉ số (CA) có nhiệm vụ gì?

A. Tạo dữ liệu mã hóa
B. **Cung cấp và ký xác nhận chứng chỉ số**
C. Kiểm tra tính toàn vẹn dữ liệu
D. Lưu trữ khóa bí mật

Câu 130: Chứng chỉ số được tạo ra theo chuẩn nào?

A. RFC-3174
B. **X.509 version 3**
C. SHA-256
D. HMAC

Câu 131: Danh sách CRL (Certificate Revocation List) dùng để làm gì?

A. Lưu trữ khóa công khai
B. **Liệt kê các chứng chỉ số bị hủy bỏ**

C. Tạo chứng chỉ mới
D. Kiểm tra khóa bí mật

Câu 132: Chính sách chứng chỉ số (Certificate Policy) nên có đặc điểm nào?

A. Dài hơn 5 trang
B. **Rõ ràng, súc tích, giới hạn trong 2 trang**
C. Không cần xác nhận lãnh đạo
D. Chỉ mô tả kỹ thuật

Câu 133: CPS (Certificate Practice Statement) khác CP ở điểm nào?

A. CP mang tính kỹ thuật hơn
B. **CPS mô tả cách thực hiện chính sách (how), CP mô tả việc gì (what)**
C. CPS ngắn hơn CP
D. CPS không cần duy trì

Câu 134: Phương pháp nào sau đây không dùng để lưu trữ và phân phối khóa?

A. Trung tâm phân phối khóa (KDC)
B. Giải thuật trao đổi khóa (KEA)
C. **Mã hóa băm (hashing)**
D. Phần cứng như card, flash disk

Câu 135: Ưu điểm của quản lý khóa tập trung là gì?

A. Người dùng tự tạo khóa
B. **Dễ quản lý, tạo mới và phục hồi khóa**
C. Không bị ảnh hưởng nếu CA gặp sự cố
D. Không cần môi trường an toàn

Câu 136: Nhược điểm của quản lý khóa không tập trung là gì?

A. Tốc độ tạo khóa chậm
B. **Khó khôi phục khóa khi bị mất**

C. Dễ bị hacker tấn công
D. Ảnh hưởng toàn hệ thống

Câu 137: Khóa số được lưu trữ an toàn hơn khi sử dụng phương pháp nào?

A. Phần mềm
B. **Phần cứng như card hoặc flash disk**
C. File văn bản
D. Email mã hóa

Câu 138: Escrow trong quản lý khóa dùng để làm gì?

A. Tạo khóa mới
B. **Phục hồi khóa bí mật khi bị mất**
C. Hủy bỏ chứng chỉ số
D. Kiểm tra tính toàn vẹn

Câu 139: Khi nào khóa và chứng chỉ số bị tiêu hủy?

A. Khi hết hạn sử dụng
B. **Khi không còn sử dụng để tránh bị lợi dụng**
C. Khi tạm dừng sử dụng
D. Khi gia hạn thành công

Câu 140: Khóa số được sử dụng rộng rãi trong ứng dụng nào sau đây?

A. Sao lưu dữ liệu
B. **Bảo mật email (PGP, S/MIME)**
C. Tạo dấu vân tay dữ liệu
D. Kiểm tra tốc độ mạng

CHƯƠNG 5: AN TOÀN TRONG TRUYỀN THÔNG

Câu 141: Mục tiêu chính của chương về an toàn trong truyền thông là gì?

A. Hướng dẫn cài đặt phần mềm mạng
B. **Cung cấp cái nhìn tổng quan về các giải pháp tạo sự an toàn trong truyền thông**
C. Giới thiệu các thiết bị mạng cơ bản
D. Hướng dẫn sử dụng giao thức Telnet

Câu 142: Sau khi hoàn tất chương, sinh viên có khả năng nào sau đây?

A. Thiết kế giao diện mạng
B. **Mô tả các giao thức truy cập từ xa như PPP, Telnet, VPN**
C. Tạo phần mềm mã hóa
D. Quản lý cơ sở dữ liệu

Câu 143: Giao thức nào sau đây thuộc nhóm truy cập từ xa?

A. FTP
B. **PPP**
C. HTTP
D. LDAP

Câu 144: PPP (Point-to-Point Protocol) hoạt động ở tầng nào trong mô hình OSI?

A. Tầng 1
B. **Tầng 2**
C. Tầng 3
D. Tầng 4

Câu 145: Phương thức chứng thực nào của PPP không mã hóa thông tin?

A. CHAP
B. **PAP**
C. RSA
D. DSA

Câu 146: Telnet sử dụng cổng nào để truyền thông?

A. Cổng 22
B. **Cổng 23**
C. Cổng 80
D. Cổng 443

Câu 147: Điểm yếu chính của giao thức Telnet là gì?

A. Tốc độ chậm
B. **Dữ liệu truyền đi không được mã hóa (plaintext)**
C. Không hỗ trợ dòng lệnh
D. Chỉ hoạt động trên mạng nội bộ

Câu 148: Giao thức nào được đề xuất thay thế Telnet để tăng tính bảo mật?

A. FTP
B. **SSH**
C. HTTP
D. RADIUS

Câu 149: SSH (Secure Shell) sử dụng cổng nào mặc định?

A. Cổng 23
B. **Cổng 22**
C. Cổng 80
D. Cổng 443

Câu 150: SSH sử dụng giải thuật mã hóa nào sau đây?

A. MD5
B. **3DES**
C. SHA-1
D. HMAC

Câu 151: TACACS+ là giao thức riêng của hãng nào?

A. Microsoft
B. **Cisco**
C. IBM
D. Oracle

Câu 152: TACACS+ sử dụng giao thức vận chuyển nào và cổng nào?

A. UDP cổng 1812
B. **TCP cổng 49**
C. TCP cổng 23
D. UDP cổng 389

Câu 153: Điểm yếu của TACACS+ là gì?

A. Không hỗ trợ mã hóa
B. **Dễ bị tấn công replay nếu không thay đổi khóa thường xuyên**
C. Tốc độ xử lý chậm
D. Không hỗ trợ AAA

Câu 154: RADIUS sử dụng giao thức nào và cổng nào để chứng thực?

A. TCP cổng 49
B. **UDP cổng 1812**
C. TCP cổng 443
D. UDP cổng 23

Câu 155: Giao thức nào sau đây thuộc nhóm truy cập liên mạng?

A. PPP
B. **FTP**
C. SSH
D. VPN

Câu 156: HTTP sử dụng cổng nào mặc định?

A. Cổng 22
B. **Cổng 80**

C. Cổng 443
D. Cổng 21

Câu 157: Điểm yếu chính của HTTP là gì?

A. Tốc độ chậm
B. **Không chứng thực, không mã hóa**
C. Không hỗ trợ HTML
D. Chỉ hoạt động trên mạng nội bộ

Câu 158: HTTPS được xây dựng từ giao thức nào?

A. HTTP + FTP
B. **HTTP + TLS/SSL**
C. HTTP + SSH
D. HTTP + RADIUS

Câu 159: HTTPS sử dụng cổng nào mặc định?

A. Cổng 80
B. **Cổng 443**
C. Cổng 22
D. Cổng 21

Câu 160: SSL/TLS cung cấp bảo mật bằng cách nào?

A. Chỉ mã hóa đối xứng
B. **Mã hóa đối xứng, bất đối xứng và kiểm tra tính toàn vẹn**
C. Chỉ kiểm tra tính toàn vẹn
D. Chỉ chứng thực

Câu 161: Giao thức FTP sử dụng cổng nào cho kết nối điều khiển?

A. Cổng 20
B. **Cổng 21**
C. Cổng 80
D. Cổng 443

Câu 162: Điểm yếu chính của FTP là gì?

A. Tốc độ truyền dữ liệu chậm
B. **Không mã hóa dữ liệu, kể cả mật khẩu**
C. Không hỗ trợ tải lên
D. Chỉ hoạt động ở chế độ passive

Câu 163: FTPS sử dụng cổng nào cho kết nối điều khiển?

A. Cổng 21
B. **Cổng 990**
C. Cổng 443
D. Cổng 80

Câu 164: NetBIOS sử dụng các cổng nào để hoạt động?

A. TCP 80, 443
B. **TCP 137, 138, 139**
C. UDP 1812
D. TCP 21, 20

Câu 165: LDAP (Lightweight Directory Access Protocol) hoạt động ở cổng nào mặc định?

A. Cổng 443
B. **Cổng 389**
C. Cổng 636
D. Cổng 23

Câu 166: SLDAP (Secure LDAP) sử dụng công nghệ nào để tăng bảo mật?

A. RSA
B. **SSL/TLS**
C. CHAP
D. PAP

Câu 167: Một trong những biện pháp bảo trì Web Server là gì?

A. Tắt tính năng ghi log
B. **Cập nhật và vá lỗi thường xuyên**
C. Sử dụng cổng 80 thay vì 443
D. Không thực hiện backup

Câu 168: Công cụ nào được đề xuất để kiểm tra cấu hình Web Server?

A. FTP
B. **NMAP**
C. Telnet
D. LDAP

Câu 169: Chế độ Passive trong FTP khác chế độ Standard ở điểm nào?

A. Không sử dụng cổng 20
B. **Client chủ động kết nối đến cổng dịch vụ do Server cung cấp**
C. Server không trả lời Client
D. Không hỗ trợ tải xuống

Câu 170: TLS khác SSL ở điểm nào?

A. TLS không mã hóa dữ liệu
B. **TLS cung cấp các chức năng bảo mật nâng cao hơn và không tương thích với SSL**
C. TLS chỉ hỗ trợ mã hóa đối xứng
D. TLS sử dụng cổng 80

CHƯƠNG 6: CÁC MÔ HÌNH MẠNG AN TOÀN

Câu 171: Mục tiêu chính của Chương 6 về "Các mô hình mạng an toàn" là gì?

A. Hướng dẫn cài đặt phần mềm mạng
B. **Cung cấp cái nhìn tổng quan về cách thức xây dựng các mô hình mạng an toàn**
C. Giới thiệu các thiết bị mạng cơ bản
D. Hướng dẫn sử dụng giao thức Telnet

Câu 172: Sau khi hoàn tất chương, sinh viên có thể làm gì?

A. Thiết kế giao diện mạng
B. **Phân biệt được khái niệm về Intranet, Extranet và vùng DMZ**
C. Tạo phần mềm mã hóa
D. Quản lý cơ sở dữ liệu

Câu 173: Vùng an ninh (security zone) được định nghĩa như thế nào?

A. Một phần mềm bảo mật mạng
B. **Một phần của mạng được định nghĩa chung một mức an ninh**
C. Một giao thức mạng
D. Một thiết bị phần cứng

Câu 174: Vùng an ninh thường được chia thành mấy loại chính?

A. 2
B. **3**
C. 4
D. 5

Câu 175: Intranet là gì?

A. Một mạng công cộng
B. **Một mạng dùng riêng, sử dụng các giao thức và dịch vụ tương tự Internet**
C. Một mạng kết nối với đối tác bên ngoài
D. Một vùng phi quân sự

Câu 176: Đặc điểm nào sau đây không đúng về Intranet?

A. Tốc độ cao
B. Dễ dàng truy xuất tài nguyên
C. **Cho phép truy cập từ mạng bên ngoài mà không cần bảo mật**
D. Sử dụng các dạng mạng như Ethernet, Token Ring

Câu 177: Extranet khác Intranet ở điểm nào?

A. Không sử dụng giao thức Internet
B. **Có kết nối với mạng bên ngoài như khách hàng, đối tác**
C. Không yêu cầu tính bảo mật
D. Chỉ hoạt động trong mạng nội bộ

Câu 178: Công nghệ nào có thể được sử dụng để tăng bảo mật cho Extranet?

A. HTTP
B. **VPN hoặc PKI**
C. FTP
D. NAT

Câu 179: DMZ (Demilitarized Zone) là gì?

A. Một mạng nội bộ hoàn toàn kín
B. **Một vùng mạng được thiết kế đặc biệt, cho phép người dùng bên ngoài truy xuất có kiểm soát**
C. Một giao thức bảo mật
D. Một hệ thống mã hóa

Câu 180: Thiết bị nào kiểm soát và giới hạn truy cập vào vùng DMZ?

A. Router
B. **Firewall**
C. Switch
D. Gateway

Câu 181: Nếu vùng DMZ bị tấn công, điều gì xảy ra với mạng nội bộ?

A. Mạng nội bộ sẽ bị ảnh hưởng ngay lập tức
B. **Mạng nội bộ không bị ảnh hưởng nếu được thiết kế đúng**
C. Toàn bộ hệ thống sẽ ngừng hoạt động
D. Firewall sẽ tự động ngắt kết nối Internet

Câu 182: Dịch vụ nào sau đây thường được triển khai trong vùng DMZ?

A. LDAP
B. **Web, Email, FTP**
C. SSH
D. Telnet

Câu 183: Bastion Host trong vùng DMZ là gì?

A. Một thiết bị Firewall
B. **Máy tính có thể truy xuất từ cả mạng nội bộ và mạng bên ngoài**
C. Một giao thức bảo mật
D. Một hệ thống phát hiện xâm nhập

Câu 184: VLAN (Virtual LAN) được định nghĩa như thế nào?

A. Một mạng vật lý cố định
B. **Một nhóm luận lý các máy tính, thiết bị mạng không bị giới hạn bởi vị trí địa lý hay kết nối vật lý**
C. Một vùng phi quân sự
D. Một mạng chỉ dùng trong nội bộ

Câu 185: Giao thức nào thường được sử dụng cho đường trunk trong VLAN?

A. HTTP
B. **802.1Q hoặc ISL**
C. FTP
D. NAT

Câu 186: Trường VID trong frame VLAN có độ dài bao nhiêu bit?

A. 8
B. **12**
C. 16
D. 24

Câu 187: NAT (Network Address Translation) có chức năng chính là gì?

A. Tăng tốc độ truyền dữ liệu
B. **Che giấu địa chỉ bên trong mạng cục bộ khi giao tiếp với Internet**
C. Mã hóa dữ liệu
D. Phân chia VLAN

Câu 188: Loại NAT nào ánh xạ một địa chỉ cục bộ sang một địa chỉ thực cố định?

A. Dynamic NAT
B. **Static NAT**
C. PAT
D. VLAN NAT

Câu 189: PAT (Port Address Translation) khác Dynamic NAT ở điểm nào?

A. Chỉ sử dụng một địa chỉ công cộng duy nhất
B. **Ánh xạ nhiều địa chỉ cục bộ sang một địa chỉ thực với các cổng khác nhau**
C. Không sử dụng địa chỉ công cộng
D. Chỉ dùng cho mạng nội bộ

Câu 190: PAT thường được sử dụng trong trường hợp nào?

A. Khi có nhiều địa chỉ công cộng
B. **Khi nhiều máy cục bộ dùng chung một đường truyền Internet**
C. Khi không cần bảo mật
D. Khi mạng không kết nối Internet

CHƯƠNG 7: TƯỜNG LỬA

Câu 191: Mục tiêu chính của Chương 7 về "Tường lửa" là gì?

A. Hướng dẫn cài đặt phần mềm mạng
B. **Cung cấp cái nhìn tổng quan về các loại tường lửa và cách thức sử dụng**
C. Giới thiệu các giao thức mạng cơ bản
D. Hướng dẫn sử dụng hệ thống mã hóa

Câu 192: Sau khi hoàn tất chương, sinh viên có khả năng nào sau đây?

A. Thiết kế giao diện mạng
B. **Phân biệt được các loại tường lửa**
C. Tạo phần mềm mã hóa
D. Quản lý cơ sở dữ liệu

Câu 193: Firewall được đặt ở vị trí nào trong mô hình mạng máy tính?

A. Bên trong mạng nội bộ
B. **Giữa mạng nội bộ và mạng ngoài (Internet)**
C. Bên ngoài mạng nội bộ
D. Chỉ trong vùng DMZ

Câu 194: Mục tiêu thiết kế chính của Firewall là gì?

A. Tăng tốc độ truyền dữ liệu
B. **Chỉ cho phép lưu thông hợp lệ đi qua và ngăn chặn xâm nhập**
C. Mã hóa toàn bộ dữ liệu
D. Giám sát người dùng nội bộ

Câu 195: Kỹ thuật nào sau đây không thuộc chức năng của Firewall?

A. Điều khiển dịch vụ
B. Điều khiển hướng
C. **Mã hóa dữ liệu truyền đi**
D. Điều khiển người dùng

Câu 196: Firewall không thể ngăn chặn loại tấn công nào sau đây?

A. Tấn công từ Internet
B. **Tấn công qua đường truy xuất Dial-up không đi qua Firewall**
C. Tấn công giả mạo IP
D. Tấn công vạch đường

Câu 197: Khả năng nào sau đây thuộc về Firewall?

A. Bảo vệ hoàn toàn khỏi virus
B. **Ngăn chặn những kẻ trái phép từ ngoài mạng riêng**
C. Ngăn chặn tấn công từ bên trong
D. Tự động cập nhật phần mềm

Câu 198: Firewall tầng ứng dụng (Application Layer Firewall) có đặc điểm nào sau đây?

A. Hoạt động nhanh, phù hợp với mạng lớn
B. **Che giấu địa chỉ nguồn yêu cầu từ mạng nội bộ**
C. Chỉ lọc dựa trên địa chỉ IP
D. Không hỗ trợ dịch vụ Web

Câu 199: Firewall lọc gói (Packet Filtering) hoạt động dựa trên yếu tố nào?

A. Nội dung dữ liệu
B. **Địa chỉ IP nguồn và đích**
C. Trạng thái kết nối
D. Giao thức tầng ứng dụng

Câu 200: Firewall nào sau đây được Cisco PIX Firewall hỗ trợ?

A. Firewall tầng ứng dụng
B. **Firewall lọc gói và Firewall dây dự trạng thái**
C. Firewall duyệt sâu gói tin
D. Firewall dựa trên người dùng

Câu 201: Firewall dây dự trạng thái (Stateful Firewall) khác Firewall lọc gói ở điểm nào?

A. Chỉ kiểm tra địa chỉ IP
B. **Kiểm tra trạng thái kết nối ở tầng 4**
C. Không sử dụng quy tắc
D. Không hỗ trợ cổng dịch vụ

Câu 202: Firewall duyệt sâu gói tin (Deep Packet Layer) kiểm tra dữ liệu ở mức nào?

A. Chỉ tầng mạng
B. **Trên tất cả các tầng của mô hình OSI**
C. Chỉ tầng ứng dụng
D. Chỉ tầng liên kết dữ liệu

Câu 203: Thiết bị nào hỗ trợ Firewall duyệt sâu gói tin?

A. Cisco PIX Firewall
B. **IDS và Cisco Netscreen Firewall**
C. Router thông thường
D. Switch tầng 2

Câu 204: Trong cấu hình Packet Filter Firewall, quy tắc "Deny All" thường được đặt ở đâu?

A. Đầu bảng quy tắc
B. **Cuối bảng quy tắc như chính sách mặc nhiên**
C. Giữa bảng quy tắc
D. Không cần thiết

Câu 205: Quy tắc "Permit Our hosts * * 25" trong Packet Filter Firewall có ý nghĩa gì?

A. Chặn truy cập SMTP từ bên ngoài
B. **Cho phép máy nội bộ kết nối đến SMTP Server bên ngoài**
C. Cho phép mọi truy cập vào cổng 25
D. Ngăn chặn trả lời từ SMTP Server

Câu 206: Quy tắc nào sau đây ngăn chặn truy cập trực tiếp vào hệ thống Firewall?

A. Allow Any Any 192.168.1.1 Any
B. **Deny Any Any 192.168.1.1 Any**
C. Permit 192.168.1.1 Any Any Any
D. Deny 192.168.1.0 Any Any Any

Câu 207: Stateful Firewall theo dõi thông tin nào để quản lý lưu lượng?

A. Chỉ địa chỉ IP nguồn
B. **Địa chỉ IP, cổng nguồn/đích và trạng thái kết nối**
C. Nội dung gói tin
D. Giao thức tầng ứng dụng

Câu 208: Quy tắc "Allow Any Any 192.168.1.2 SMTP" trong Packet Filter Firewall có ý nghĩa gì?

A. Cho phép gửi email từ mạng nội bộ
B. **Cho phép người dùng bên ngoài gửi email vào máy 192.168.1.2**
C. Chặn truy cập SMTP từ bên ngoài
D. Ngăn chặn trả lời từ SMTP Server

Câu 209: Firewall có thể được sử dụng để làm gì ngoài việc lọc lưu lượng?

A. Mã hóa toàn bộ dữ liệu
B. **Cài đặt VPN và cung cấp NAT**
C. Phát hiện virus
D. Quản lý cơ sở dữ liệu

Câu 210: Hạn chế nào sau đây không đúng về Firewall?

A. Không bảo vệ khỏi nguy hại từ bên trong
B. Không ngăn chặn tấn công không qua Firewall
C. **Có thể bảo vệ hoàn toàn khỏi mọi loại virus**
D. Không ngăn chặn tấn công qua Dial-up

CHƯƠNG 8: HỆ THỐNG NGĂN NGỪA XÂM NHẬP MẠNG

Câu 211: IDS (Intrusion Detection System) được thiết kế để làm gì?

A. Ngăn chặn mọi cuộc tấn công mạng
B. **Giám sát và phát hiện các hoạt động xâm nhập trên mạng hoặc hệ thống máy tính**
C. Kiểm soát lưu lượng mạng như Firewall
D. Mã hóa dữ liệu truyền đi

Câu 212: IDS có mấy loại chính được đề cập trong tài liệu?

A. 1
B. **2**
C. 3
D. 4

Câu 213: Hệ thống IDS dựa trên chữ ký (Signature-Based IDS) hoạt động như thế nào?

A. Phát hiện hành vi không bình thường
B. **So sánh gói tin hoặc hành vi với cơ sở dữ liệu chữ ký xâm nhập đã biết**
C. Ngăn chặn tự động các cuộc tấn công
D. Giám sát hiệu suất mạng

Câu 214: Hệ thống IDS dựa trên hành vi (Anomaly-Based IDS) xác định xâm nhập dựa trên yếu tố nào?

A. Cơ sở dữ liệu chữ ký
B. **Hành vi không bình thường so với xu hướng đã biết**
C. Địa chỉ IP nguồn
D. Cổng dịch vụ

Câu 215: Network IDS được triển khai nhằm mục đích gì?

A. Bảo vệ từng máy chủ riêng lẻ
B. **Giám sát và phát hiện hoạt động xâm nhập trên toàn mạng máy tính**
C. Ngăn chặn tấn công trực tiếp
D. Kiểm soát quyền truy cập

Câu 216: Network IDS thường được triển khai ở đâu trong mạng?

A. Chỉ trên máy chủ
B. **Tại các cổng vào/ra, điểm trung chuyển hoặc nút cuối của mạng**
C. Bên ngoài mạng nội bộ
D. Chỉ trong vùng DMZ

Câu 217: Host IDS khác Network IDS ở điểm nào?

A. Giám sát toàn bộ lưu lượng mạng
B. **Giám sát và phân tích hoạt động xâm nhập trên từng máy chủ cụ thể**
C. Không sử dụng chữ ký
D. Không tạo cảnh báo

Câu 218: Host IDS theo dõi yếu tố nào trên máy chủ?

A. Chỉ lưu lượng mạng
B. **Thay đổi trong file, cấu hình, quyền truy cập và tài nguyên hệ thống**
C. Địa chỉ IP nguồn
D. Giao thức tầng ứng dụng

Câu 219: Ưu điểm chính của Network IDS là gì?

A. Ngăn chặn mọi cuộc tấn công
B. **Phát hiện sớm các cuộc tấn công mạng như virus hoặc tấn công từ chối dịch vụ**
C. Bảo vệ hoàn toàn máy chủ
D. Tăng tốc độ mạng

Câu 220: Ưu điểm của Host IDS là gì?

A. Giám sát toàn bộ mạng
B. **Phát hiện sớm các mối đe dọa trực tiếp vào máy chủ**
C. Không cần cài đặt trên máy chủ
D. Ngăn chặn tấn công từ bên ngoài

Câu 221: Chức năng quan trọng nhất của IDS là gì?

A. Ngăn chặn tấn công
B. **Phát hiện các hoạt động xâm nhập hoặc hành vi không chính thức**
C. Kiểm soát lưu lượng mạng
D. Ghi log mọi hoạt động

Câu 222: Khi phát hiện xâm nhập, IDS thực hiện hành động nào sau đây?

A. Ngăn chặn tự động
B. **Tạo cảnh báo để thông báo cho quản trị viên**
C. Mã hóa dữ liệu
D. Xóa dữ liệu bị tấn công

Câu 223: IDS sử dụng phương pháp nào để phân tích dữ liệu mạng?

A. Chỉ kiểm tra địa chỉ IP
B. **Phân tích gói tin và so sánh với cơ sở dữ liệu chữ ký hoặc hành vi**
C. Chỉ giám sát cổng dịch vụ
D. Không phân tích dữ liệu

Câu 224: Firewall khác IDS ở điểm nào?

A. Chỉ phát hiện xâm nhập
B. **Kiểm soát lưu lượng mạng dựa trên quy tắc, không chỉ phát hiện**
C. Không giám sát mạng
D. Không tạo cảnh báo

Câu 225: IPS (Intrusion Prevention System) khác IDS như thế nào?

A. Chỉ giám sát mà không ngăn chặn
B. **Không chỉ phát hiện mà còn ngăn chặn tự động các hoạt động xâm nhập**
C. Không tạo cảnh báo
D. Chỉ hoạt động trên máy chủ

Câu 226: Nhược điểm nào sau đây của IDS liên quan đến cảnh báo?

A. Không phát hiện được tấn công
B. **Có thể tạo cảnh báo giả khi nhầm lẫn hoạt động bình thường với xâm nhập**
C. Không ghi log sự kiện
D. Ngăn chặn quá nhiều lưu lượng

Câu 227: IDS có thể bị vượt qua bởi loại tấn công nào?

A. Tấn công từ chối dịch vụ
B. **Tấn công thông minh sử dụng kỹ thuật mới và tiên tiến**
C. Tấn công virus cơ bản
D. Tấn công giả mạo IP

Câu 228: Việc triển khai IDS có thể gây ra hiệu ứng phụ nào?

A. Tăng tốc độ mạng
B. **Ảnh hưởng đến hiệu suất mạng và tạo lưu lượng không cần thiết**
C. Ngăn chặn mọi tấn công
D. Giảm dung lượng lưu trữ

Câu 229: Chức năng "Ghi nhật ký" của IDS có mục đích gì?

A. Ngăn chặn tấn công
B. **Phục vụ cho việc theo dõi và phân tích sau xâm nhập**
C. Tạo cảnh báo tức thời
D. Kiểm soát lưu lượng mạng

Câu 230: Mục tiêu chính của Firewall so với IDS là gì?

A. Phát hiện hành vi không bình thường
B. **Ngăn chặn tấn công từ bên ngoài và kiểm soát quyền truy cập**
C. Giám sát từng máy chủ
D. Phân tích gói tin chi tiết