Người chịu trách nhiệm đánh giá, triển khai và quản lý việc bảo mật thông tin trong tổ chức được gọi là:
A. ISO
B. CISO
C. CIO
D. CTO

Trong quy trình xây dựng mạng an toàn, việc khảo sát hệ thống bao gồm các nội dung chính nào?
A. Khảo sát cơ cấu tổ chức, phân tích các nguy cơ, đề xuất các giải pháp an toàn.
B. Khảo sát cơ cấu tổ chức, phân tích các nguy cơ, xác định nhóm người sử dụng.
C. Khảo sát vật lý, xác định nhóm người sử dụng, xác định các nguy cơ.
D. Khảo sát vật lý, phân tích các vấn đề cần giải quyết, xác định nhóm người sử dụng.

Câu 0001: Việc hacker làm thay đổi bảng vạch đường của 1 router là loại đe dọa nào?
A. Chủ động.
B. Vô ý.
C. Cố ý.
D. Thụ động.

File virus có đặc điểm nào?
A. Lây lan thông qua các chương trình lậu.
B. Có từ lâu đời, chỉ lây qua đĩa mềm.
C. Lây trong các file Office có hỗ trợ macro.
D. Lây trong các file thực thi.

Kiểu tấn công bằng cách thực hiện theo dõi, điều chỉnh gói tin được gởi trên đường truyền gọi là:
A. zombie-in-the-middle
B. server-in-the-middle
C. man-in-the-middle
D. sniff-in-the-middle

Máy chủ A của công ty hiện không truy xuất được. Sau khi phân tích, bạn phát hiện rằng có rất nhiều gói tin quảng bá (broadcast) được gởi đến router mạng có địa chỉ trả về là máy chủ. Máy chủ này đang bị tấn công dạng:
A. SYN flood
B. ICMP flood
C. Buffer overflow
D. Smurf attack

Coleen là quản trị viên bảo mật web cho một trang web đấu giá trực tuyến. Một số ít người dùng phàn nàn rằng khi họ truy cập trang web và đăng nhập, họ được thông báo rằng dịch vụ đã ngừng

hoạt động và sẽ thử lại sau. Coleen kiểm tra và cô ấy có thể truy cập trang web mà không có bất kỳ vấn đề, ngay cả từ các máy tính bên ngoài mạng. Cô cũng kiểm tra nhật ký máy chủ web vàkhông có thông tin kết nối đến máy chủ web của những người dùng đó. Thuật ngữ nào sau đây có thể giải thích tốt nhất điều này?
A. Typosquatting
B. Cross-site request forgery
C. Cross-site scripting
D. SQL injection

Kiểu tấn công nào dựa trên việc tạo ra các bản ghi giả vào máy chủ DNS?
A. DNS poisoning
B. Bluejacking
C. Bluesnarfing
D. ARP poisoning

Phòng chống tấn công từ chối dịch vụ phân bố (DDoS)
A. Cách hiệu quả duy nhất là bakup và restore
B. Hiện nay đã có cách phòng chống hiệu quả
C. Chỉ có thể dùng tường lửa
D. Có thể hạn chế bằng cách lập trình

Sử dụng NFC (Near-field communication) sẽ dễ bị loại tấn công nào nhất?
A. Man-in-the-middle
B. Eavesdropping
C. Buffer overflow
D. Smurf attack

Bộ nhớ heap và stack sẽ bị ảnh hưởng bởi kiểu tấn công nào sau đây:
A. Rootkits
B. Buffer overflows
C. SQL injection
D. Cross-site scripting

Khi một chương trình có các biến, đặc biệt là các mảng và không kiểm tra các giá trị biên trước khi nhập dữ liệu, chương trình có thể bị tấn công bởi lỗi bảo mật nào?
A. XSS
B. CRSF
C. Logic bomb
D. Buffer overflow

Gerald là một quản trị mạng cho Công ty Acme. Người dùng đang báo cáo biểu hiện kỳ lạ trên máy tính của họ. Ông tin rằng điều này có thể là do phần mềm độc hại, nhưng cácbiểu hiện trên các máy tính đều khác nhau. Điều gì có thể giải thích tốt nhất điều này?
A. Đây không phải là phần mềm độc hại, nhưng lỗi phần cứng

B. Đây là một Boot sector virus
C. Đây là một macro virus
D. Đây là một polymorphic virus

Phương pháp nào sau đây không dùng để xác thực thông điệp?
A. Mã hóa thông điệp.
B. Mã xác thực thông điệp.
C. Hàm băm.
D. TSL.

Chứng minh thư là yếu tố xác thực dựa vào:
A. Cái người sử dụng có.
B. Đa yếu tố.
C. Cái mà người sử dụng sở hữu bẩm sinh.
D. Cái người sử dụng biết.

Trong phương pháp RSA, với p=7, q=13, e=11; khóa công khai nào là đúng?
A. {111, 11}
B. {72, 91}
C. {11, 72}
D. {11, 91}

Trong phương pháp RSA, với p=11, q=19, e=13; khóa công khai nào là đúng?
A. {19,13}
B. {11, 247}
C. {19, 143}
D. {13, 209}

Phát biểu nào là sai khi nói về Remote Access VPN?
A. Chia làm 3 loại Client-initiated, NAS-initiated, Site-to-Site VPN.
B. Client có thể sử dụng router, thiết bị phần cứng, phần mềm.
C. Cung cấp phương thức truy cập vào mạng công ty cho người dùng ở xa.
D. Còn được gọi là mạng Dialup riêng ảo.

Phát biểu nào đúng khi nói về giao thức trong IPSec?
A. AH không mã hóa dữ liệu.
B. AH chỉ mã hóa phần dữ liệu.
C. ESP không mã hóa header.
D. ESP không cung cấp chứng thực có giới hạn.

Phương pháp nào không có tác dụng ngăn ngừa tấn công hệ thống DNS?
A. Cài đặt hệ thống HIDS.
B. Hạn chế tối đa các dịch vụ khác trên DNS.

C. Thường xuyên cập nhật các bản sửa lỗi hệ thống.
D. Lưu lại file log, thường xuyên phân tích file log.

Phát biểu nào sai về an toàn Web?
A. Có nhiều công cụ đối phó các hiểm họa an toàn Web.
B. Các Web thường chứa nhiều lỗi bảo mật.
C. Tấn công Web Server sẽ làm tổn hại cả về kinh tế lẫn danh tiếng.
D. Web dễ bị tấn công theo cả 2 chiều.

Các tốt nhất để chống tấn công kiểu SQL injection cho Website là:
A. Cài đặt Firewall
B. Sử dụng giao thức HTTPS
C. Cập nhật thường xuyên Webserver
D. Kiểm tra tất cả dữ liệu người dùng nhập vào

HIDS không có ưu điểm nào sau đây?
A. Khả năng xác định user liên quan tới 1 event.
B. Phân tích được dữ liệu mã hóa.
C. Khả năng phát hiện các cuộc dò quét mạng.
D. Khả năng phát hiện tấn công trên 1 máy.

Mạng không dây bị tấn công dạng "Kẻ đứng giữa" (Man in the middle) vào giai đoạn nào sau đây?
A. Association (Ghép nối)
B. Probing (Thăm dò)
C. Beacon (Báo hiệu)
D. Authentication (Chứng thực)

Tấn công System Hacking là phương thức tấn công kiểu
A. Đanh cắp thông tin truyền trên mạng
B. Điều khiển máy tính từ xa thông qua các phần mềm cài sẵn
C. Can thiệp trực tiếp máy tính nạn nhân, đánh cắp thông tin
D. Tấn công làm tê liệt hệ thống máy nạn nhân

Giao thức nào là việc trên lớp IP để bảo vệ thông tin IP?
A. TACACS+
B. SSH
C. IPX
D. IPSec

Kỹ thuật nào cho phép ta kết nối một mạng LAN của công ty qua Internet thông qua một kênh được mã hóa an toàn?
A. WEP

B. VPN
C. Modem
D. Telnet

Cách nào sau đây là tốt nhất để ngăn chặn điểm yếu bảo mật trong hệ điều hành
A. Shutdown hệ thống khi không sử dụng
B. Cập nhật HĐH thường xuyên
C. Sao lưu hệ thống thường xuyên
D. Cài đặt lại HĐH thông dụng

Khi gia cố hệ điều hành cần quan tâm các vấn đề nào?
A. Hệ thống tập tin
B. Update
C. Hotfix
D. Tất cả các yếu tố trên

Phát biểu nào không đúng khi nói về FTP Server?
A. Cần cấu hình cẩn thận tài khoản vô danh (anonymous).
B. Nên tách biệt tài khoản FTP và tài khoản người dùng trên hệ điều hành.
C. FTP là giao thức an toàn vì thông tin chứng thực dưới dạng mã hóa.
D. Nên cô lập đĩa phục vụ FTP và đĩa chứa các dữ liệu quan trọng.