Phát biểu nào sai khi nói về tấn công từ chối dịch vụ?
A. Là hành động ngăn cản người dùng hợp pháp truy cập dịch vụ.
B. Gây ra hiện tượng tràn mạng, mất kết nối dịch vụ.
C. Làm cho Server không thể đáp ứng được yêu cầu từ Client.
D. Hacker muốn đánh cắp các thông tin truy cập.

Cơ chế bảo mật nào sau đây thuộc về kiểm soát vật lý?
A. Đặt mật khẩu
B. Mã hóa dữ liệu
C. Sử dụng phần mềm Antivirus
D. Thẻ nhân viên (ID card)

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. sniff-in-the-middle
D. man-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

Jared phát hiện ra rằng những kẻ tấn công đã thâm nhập mạng WiFi của mình. Họ đã có được quyền truy cập thông qua trang quản trị của AP (WAP) và đã đăng nhập với thông tin đăng nhập mà WAP gửi kèm. Điều gì mô tả tốt nhất vấn đề này?
A. Xảy ra Race conditions
B. Chưa vá lỗi
C. Áp dụng giao thức mã hóa yếu
D. Sử dụng cấu hình mặc định

Joanne quan tâm đến tấn công phi kĩ thuật. Cô đặc biệt lo ngại rằng công nghệ này có thể được sử dụng bởi kẻ tấn công để lấy thông tin về mạng, bao gồm cả mật khẩu. Biện pháp đối phó nào sẽ hiệu quả nhất trong việc chống lại tấn công phi kĩ thuật?
A. Tường lửa SPI
B. Sử dụng IPS
C. Đưa ra những chính sách mạnh
D. Đào tạo người dùng

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

Nguy cơ nào sau đây là nguy hiểm nhất khi sử dụng máy ảo (virtual machine):
A. Một máy ảo bị lỗi gây ảnh hưởng đến các máy ảo khác
B. Một máy ảo bị lỗi sẽ làm ảnh hưởng đến máy thật
C. Máy thật bị lỗi gây ảnh hưởng đến các máy thật khác

D. Máy thật bị lỗi sẽ làm tất cả máy ảo mà nó đang quản lý (host) dừng hoạt động

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

Cross-site scripting là kiểu tấn công vào ____ dựa trên sự tin tưởng của ____ đối với ____
A. user, website, user
B. website, website, user
C. user, website, website
D. user, user, website

Thuật ngữ *white-box testing* có nghĩa là gì?
A. Tester không biết thông tin về hệ thống
B. Tester không có quyền truy xuất hệ thống
C. Tester có quyền truy xuất hệ thống
D. Tester có đầy đủ thông tin về hệ thống

Bạn làm việc cho một công ty bán lẻ lớn xử lý việc mua qua thẻ tín dụng. Bạn đã được yêu cầu kiểm tra mạng công ty của bạn cho các vấn đề bảo mật. Thử nghiệm cụ thể mà bạn đang tiến hành bao gồm chủ yếu kiểm tra các chính sách, tài liệu và báo cáo sự cố trong quá khứ. Thuật ngữ nào sau đây mô tả đúng nhất về loại thử nghiệm này?
A. Quét lỗ hỏng (Vulnerability scan)
B. Kiểm tra sự xâm nhập (Penetration test)
C. Kiểm tra bảo mật (Security test)
D. Kiểm toán an ninh (Security audit)

Người dùng đang phàn nàn rằng họ không thể kết nối với mạng không dây. Bạn phát hiện ra rằng các WAP đang bị tấn công không dây (wireless attack) được thiết kế để chặn tín hiệu WiFi của chúng. Kiểu tấn công này thuộc loại gì?
A. Tấn công IV
B. Tấn công WPS
C. Botnet
D. Jamming

Fares là quản trị viên bảo mật mạng cho một công ty tạo ra các router và switches tiên tiến. Anh ta đã phát hiện ra rằng các mạng của công ty của anh ta đã phải chịu một loạt các cuộc tấn công có chủ định trong một khoảng thời gian. Thuật ngữ nào mô tả tốt nhất cuộc tấn công này?
A. Tấn công disassociation
B. Brute force
C. DDoS
D. APT
[<O A='D' C='C02' D='0.2'>]

Kiểu tấn công bằng cách nhúng mã độc vào file tài liệu (document) hoặc bảng tính (spreadsheet) được gọi là:
A. Logic bomb
B. Rootkit
C. Trojan horse
D. Macro virus

Hoạt động tấn công bằng cách bắt các gói tin chứa thông tin đăng nhập (login credential) và gởi lại (re-send) thông tin đó gọi là:
A. IP spoofing
B. Login spoofing
C. Session hijacking
D. Replay attack

Công ty Acme sử dụng certificate servernội bộ của riêng mình cho tất cả mã hóa nội bộ. Tuy nhiên, Certificate Authority (CA) của họ chỉ xuất bản CRL một lần mỗi tuần. Điều này có gây nguy hiểm không, và nếu vậy thì sao?
A. Không, đây là tiêu chuẩn cho tất cả các cơ quan cấp chứng chỉ
B. Có, điều này có nghĩa là sẽ dễ dàng giả mạo chứng chỉ
C. Không, vì điều này chỉ được sử dụng trong nội bộ
D. Có, điều này có nghĩa là một chứng chỉ bị thu hồi có thể được sử dụng trong tối đa bảy ngày

Loại virus nào có thể thay đổi mã của chính nó để tránh bị phần mềm chống virus phát hiện?
A. Boot sector
B. Hoax
C. Stealth
D. Polymorphic

Gerald là quản trị viên mạng cho một công ty dịch vụ tài chính nhỏ. Người dùng đang báo cáo những biểu hiện kỳ lạ có vẻ là do virus gây ra trên máy của họ. Sau khi cô lập các máy mà anh tin là bị nhiễm mã độc. Anh ấy thấy rằng tất cả các máy bị nhiễm đã nhận được một email có chủ định từ kế toán với một bảng tính Excel, và những người dùng đã mở bảng tính. Vấn đề có khả năng nhất trên các máy này là gì?
A. Boot sector virus
B. RAT
C. Trojan horse
D. Macro virus

Phát biểu nào đúng khi nói về chữ ký số?
A. Xác thực dựa vào việc sở hữu khóa bí mật.
B. Tạo mã băm của thông điệp với chiều dài cố định.
C. Tạo mã xác thực thông điệp chiều dài cố định.
D. Tạo dấu hiệu đặc trưng xác định duy nhất chủ thể.

Phương pháp vét cạn để phá mã không có đặc điểm nào sau đây?
A. Trung bình phải thử nửa số khóa.
B. Gặp khó khăn khi khóa quá dài.
C. Gặp khó khăn khi khóa quá nhiều.
D. Chắc chắn thành công trên thực tế.

Phương pháp nào sau đây có sử dụng việc xoay trái giá trị băm?
A. SHA-1
B. SHA-0
C. XOR
D. RXOR

Khi dùng phương pháp Caesar để mã hóa, với k=2 và văn bản gốc “SECURITY” thì văn bản mã hóa là:
A. UHEWTKVA
B. UGFWTKVA

C. UGEXTKVA
D. UGEWTKVA

Thuật toán DES mã hóa dữ liệu theo từng khối có kích thước:
A. 128 bit
B. 32 bit
C. 256 bit
D. 64 bit

Thuật toán Vigenère với văn bản gốc “BAOMATDL” và khóa “SECRET” có văn bản mã là:
A. TEQCEMVP
B. TEQCEFVP
C. TEQDEMPV
D. TEQDEMVP

Giao thức TCP/IP có bao nhiêu cổng (port) có thể bị tấn công?
A. 1024
B. 256
C. 16777216
D. 65535

Các cơ chế an toàn của IPSec là gì?
A. Quản lý khóa.
B. Bảo mật.
C. Xác thực.
D. Tất cả đều đúng.

Phát biểu nào sai khi nói về các kỹ thuật sử dụng trong FireWall?
A. Điều khiển dịch vụ xác định các loại dịch vụ mạng được truy cập.
B. Điều khiển hướng xác định hướng truy cập cho phép của từng loại dịch vụ.
C. Điều khiển người dùng xác định đối tượng có thể truy cập.
D. Điều khiển ứng xử lọc lưu thông mạng dựa vào IP và cổng.

Phương pháp nào ngăn ngừa tấn công Mail Relay?
A. Giới hạn dung lượng Mail box.
B. Sử dụng phương thức chống Relay Spam.
C. Sử dụng gateway SMTP riêng.
D. Tất cả các ý trên.

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

Phát biểu nào đúng khi nói về NIDS?
A. Xác định được việc attack có thành công hay không.
B. Không quản lý được nhiều host.
C. Không xảy ra tình trạng báo động giả.
D. Sử dụng dữ liệu trên toàn bộ mạng để phát hiện xâm nhập.

Trong mạng không dây, quá trình gửi và nhận dữ liệu diễn ra sau khi thực hiện bước nào?
A. Probing (Thăm dò)
B. Beacon (Báo hiệu)
C. Authentication (Chứng thực)
D. Association (Ghép nối)

Lệnh nào sau đây dùng để ẩn dấu ổ đĩa trong DISKPART
A. hide letter
B. hide volume
C. remove volume
D. remove letter
[<O A='D' C='C05' D='0.2'>]

Mức mã hóa WEP nào nên được thiết lập trên một mạng 802.11b
A. 28 bit
B. 40 bit
C. 16 bit
D. 128 bit
[<O A='D' C='C05' D='0.2'>]

Cơ cấu bảo mật mạng không dây nào sau đây là ít an toán nhất?
A. VPN
B. WEP 40 bit
C. WEP 128 bit
D. Định danh mạng

Để nâng cao tính an toàn của mạng không dây, ta cần làm gì?
A. Ẩn SSID.
B. Chọn WPA hoặc WPA2 cho chứng thực.
C. Lọc các máy trạm theo địa chỉ MAC.
D. Tất cả đều đúng.

Chính sách nào nên được thiết lập để ngăn chặn các cuộc tấn công ác ý vào user?
A. Hạn chế ngày hết hạn
B. Hạn chế thời gian
C. Disable tài khoản không dùng đến
D. Giới hạn số lần logon

Những vấn đề an toàn trên tầng liên kết dữ liệu bao gồm:
A. Bridge
B. Switch
C. Wireless Access Point
D. Tất cả các ý trên

Những vấn đề an toàn trên tầng mạng bao gồm:
A. Router
B. RAS
C. Layer 3 FireWall
D. Tất cả các ý trên
[<O A='D' C='C06' D='0.1'>]