Việc đầu tiên cần làm trong quy trình xây dựng mạng an toàn là gì?
A. Bảo trì và nâng cấp hệ thống.
B. Xác định và phân loại các nguy cơ.
C. Đánh giá hoạt động của hệ thống.
D. Khảo sát hệ thống.

Việc khai thác điểm yếu không phải từ hệ thống mà từ con người là kỹ thuật tấn công nào?
A. Replay
B. Bẻ khóa (Password)
C. Man-in-the-middle
D. Social engineering.

Bộ đệm một lần có đặc điểm:
A. Khóa chỉ xài một lần
B. Có thể không an toàn do phân phối
C. Sinh khóa ngẫu nhiên
D. Tất cả đều đúng

Người dùng truy vấn DNS tên miền *www.vlute.edu.vn* nhưng lại nhận được IP không đúng thực tế với tên miền đó. Hiện tượng này gọi là:
A. DoS
B. DNS caching
C. Smurf attack
D. DNS poisoning

Bạn là nhân viên quản trị mạng trong một công ty. Bạn nhận được báo cáo là hàng loạt máy tính trong công ty không thể kết nối mạng. Sau khi tìm hiểu, bạn phát hiện là tất cả máy tính đều không vào được mạng và có địa chỉ IP dạng 169.254.x.x. Hiện tượng này gọi là:
A. Smurf attack
B. Man-in-the-middle attack
C. DDoS
D. DHCP starvation

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

Một trong những nhân viên bán hàng trong công ty của bạn báo cáo rằng máy tính của anh ta đang cóhoạt động chậm hơn trước. Bạn kiểm tra nhưng không tìm thấy phần mềm độc hại. Tuy

nhiên, trong thư mục tạm thời của anh ấy, bạn tìm thấy các tập tin JPEG trông giống như ảnh chụp màn hình của máy tính để bàn của anh ấy. Điều nào sau đây là nguyên nhân có khả năng nhất?
A. Anh ấy cần update Windows của anh ấy
B. Có một backdoor trên máy tính của anh ấy
C. Anh ta đang đánh cắp dữ liệu từ công ty
D. Có phần mềm gián điệp trên máy tính của anh ấy

Frank đã được yêu cầu tiến hành một bài kiểm tra thâm nhập của một công ty kế toán nhỏ. Đối với thử nghiệm, anh ta chỉ được cung cấp tên công ty, tên miền cho trang web của họ và địa chỉ IP của bộ định tuyến cổng (gateway router) của họ. Những gì mô tả tốt nhất loại thử nghiệm này?
A. External test
B. Threat test
C. White - box test
D. Black - box test

John là nhân viên bán hàng cho một công ty ô tô. Gần đây anh ta đã tải xuống một chương trình từ một trang web không xác định và bây giờ các tập tin của khách hàng đã bị thay đổi phần mở rộngvà anh ta không thể mở chúng. Anh ta đã nhận được thông báo nói rằng các tệp của anh ta hiện được mã hóa và anh ta phải trả 0,5 bitcoin để được giải mã chúng. Điều gì đã xảy ra?
A. Máy của anh ấy có rootkit
B. Máy của anh ấy có logic bomb
C. Máy của anh ấy có boot sector
D. Máy của anh ấy có ransomware

Đây là một vấn đề bảo mật phổ biến cực kỳ khó kiểm soát trong môi trường lớn. Nó xảy ra khi người dùng có nhiều quyền (permissions) và đặc quyền (privileges) của máy tính hơn những gì được yêu cầu cho các tác vụ mà người dùng cần thực hiện. Thuật ngữ nào mô tả tốt nhất kịch bản này?
A. Excessive rights
B. Excessive access
C. Excessive permissions
D. Excessive privileges

Có một số máy tính phải sử dụng Windows XP do 1 ứng dụng cụ thể yêu cầu. Ứng dụng đó sẽ không chạy trên những hệ điều hành mới. Những mối quan tâm bảo mật nào nếu tình trạng này cung cấp cho bạn?
A. Không có mối quan tâm đặc biệt, điều này là bình thường
B. Các máy không thể phối hợp với SIEM từ khi XP sẽ không hỗ trợ điều đó
C. Các máy dễ bị tấn công DoS hơn.
D. Các máy móc không thể được bản vá, XP không còn được hỗ trợ

Fares đã phát hiện ra rằng những kẻ tấn công đã chọc thủng mạng không dây của mình. Họ dường như đã sử dụng một cuộc tấn công brute-force vào wifi đã thiết lập mã PIN để khai thác

WAP và khôi phục mật khẩu WPA2. Cuộc tấn công này được gọi là gì?
A. Evil twin
B. Rogue WAP
C. Tấn công IV
D. Tấn công WPS

Công ty Acme sử dụng certificate server nội 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

Phát biểu nào sai khi nói về mã đường cong Elip?
A. Ít tốn vùng nhớ xử lý hơn RSA
B. Dùng khóa công khai và khoa riêng để tính toán khóa phiên
C. Các tính toán là tương đương
D. Độ an toàn ít hơn RSA

Quá trình xác thực nào sử dụng nhiều yếu tố xác thực để logon?
A. CHAP
B. Kerberos
C. Sinh trắc học
D. Multi - Factor

Khóa riêng có đặc điểm
A. Thời gian thực hiện nhanh
B. Được thay thế bằng khóa công khai
C. Thời gian thực hiện chậm
D. Không an toàn

Trong phương pháp RSA, với p=11, q=7; giá trị phù hợp của e là bao nhiêu?
A. 15
B. 3
C. 5
D. 11

Phát biểu nào sai khi nói về khả năng của FireWall?
A. Là điểm chặn những kẻ trái phép từ ngoài mạng.
B. Bảo vệ mạng trước tấn công giả mạo và tấn công vạch đường.
C. Giám sát và cảnh báo các sự kiện bảo mật.
D. Bảo vệ trước các mối nguy hại từ bên trong.

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 cung cấp chứng thực có giới hạn.
D. ESP không mã hóa header.

Khi phát hiện hệ thống bị xâm nhập, người quản trị cần kiểm tra thông tin gì trước:
A. DNS logs
B. Event logs trong Windows
C. Performance logs
D. Firewall logs

Phương thức tấn công mật khẩu (Password attack) nào thường được sử dụng?
A. Packet sniffer
B. IP spoofing
C. Trojan House
D. Brute - force

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.

Biện pháp nào cung cấp giải pháp an toàn Web?
A. HTTP, FTP
B. TCP, IPSec
C. TCP, IP
D. SSL, TLS

IDS bao gồm các dạng nào?
A. NIDS và HIDS
B. SIDS và CIDS
C. Cả a, b đều đúng.
D. Cả a, b đều sai.

Trong SSL, thuật toán mã hóa nào mạnh nhất?
A. RC4 (khóa 40 bit)
B. RC2 (khóa 128bit)
C. RC2 (khóa 40 bit)
D. 3-DES

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

Kỹ thuật nghe lén trong môi trường Switch có thể thực hiện bằng cách nào?
A. Làm tràn bảng CAM
B. Đặt trùng MAC
C. Giả dạng ARP hoặc DNS
D. Tất cả các ý trên

Router có thể bị tấn công thông qua đường nào?
A. PPP
B. VPN
C. SLIP
D. Telnet