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

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

Kẻ tấn công sử dụng màn hình đăng nhập trên web, nhập vào nội dung: ‘ or ‘1’ = ‘1. Hình thức tấn công này là gì?
A. SQL injection
B. Cross-site request forgery
C. Cross-site scripting
D. ARP poisoning

Công ty của bạn đã thuê một công ty kiểm tra thâm nhập (Penetration Testing) để kiểm tra mạng. Đối với thử nghiệm, bạn đã cung cấp cho công ty chi tiết về các hệ điều hành bạn sử dụng, các ứng dụng bạn chạy và các thiết bị mạng. Thuật ngữ nàomô tả tốt nhất loại thử nghiệm này?
A. External test
B. Threat test
C. White - box test
D. Black - box test

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

Bạn là người quản lý cho các hoạt động mạng tại công ty của bạn. Một trong những kế toán viên nhìn thấy bạn trong hội trường và cảm ơn bạn vì nhóm của bạn đã cập nhật phần mềm chống virus của anh ấy. Khi bạn hỏi anh ta nghĩa là gì, anh ta đề cập rằng một trong những nhân viên của bạn, tên là Mike, đã gọi cho anh ta và kết nối từ xa để cập nhật chương trình chống virus. Bạn không có một nhân viên tên Mike. Điều gì đã xảy ra?
A. Giả mạo địa chỉ IP
B. Tấn công phi kỹ thuật (Social engineering)
C. Giả mạo địa chỉ MAC
D. Tấn công kẻ xen giữa (Man-in-the-middle attack)

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

Tập tin nào sau đây có khả năng chứa virus cao nhất?
A. database.dat.exe
B. harmful.docx
C. virus.exe
D. picture.gif

Bạn vừa đảm nhiệm vị trí CISO trong một ngân hàng. Bạn cần phải đảm bảo mọi thành phần trong hệ thống được an toàn. Một trong những vấn đề cần quan tâm là việc cấu hình hệ thống không đúng. Nội dung nào sau đây không thuộc về lỗi cấu hình (misconfiguration)?
A. Hệ điều hành chưa cập nhật bản sửa lỗi (patch)
B. Tài khoản và mật khẩu mặt định (default)
C. Còn chạy các dịch vụ (service) không cần thiết
D. Không có tường lửa

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

Phát biểu nào sai khi nói về phương pháp dùng mã xác thực thông điệp?
A. MAC giống giải thuật mã hóa nhưng không cần giải mã.
B. MAC là khối có kích thước cố định được thêm vào thông điệp.
C. MAC được tạo ra từ thông điệp và khóa bí mật chung.
D. Một MAC chỉ tương ứng với duy nhất thông điệp.

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.

RSA là gì?
A. Tên chuẩn an ninh mạng
B. Mã khóa riêng
C. Mã công khai

D. Tên của một tổ chức an ninh mạng

Giao thức được sử dụng để bảo mật giao tiếp giữa các hệ thống mạng TCP/IP gọi là:
A. SET
B. PEM
C. SSH
D. IPSec

Mã Caesar của "party" là
A. sduwy
B. sduwb
C. teuwb
D. tduwb

Thuật toán Autokeyvới văn bản gốc "BAOMATDL" và khóa "SECRET" có văn bản mã là:
A. TFQDEMEL
B. TEQDEMEL
C. TFQDELEM
D. TEQDELEM

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

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

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.

Các chuẩn IEEE 802.11 dùng trong mạng không dây, chuẩn nào có tốc độ cao nhất?
A. IEEE 802.11g
B. IEEE 802.11b
C. IEEE 802.11a

D. IEEE 802.11n

Sau khi cố gắng đăng nhập 3 lần, một user cảm thấy bị khóa hệ thống và không thể thực hiện bất kỳ nổ lực nào nữa. Vấn đề này phù hợp nhất với điều khiển
A. Cổng mạng disable
B. Tường lửa disable khi truy cập đến host
C. Hệ thống phát hiện xâm nhập và disable tài khoản user
D. User quên mật khẩu của họ

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

Phát biểu nào sai khi nói về IDS?
A. IDS là hệ thống phát hiện xâm nhập.
B. IDS có khả năng phát hiện các đoạn mã độc hoạt động trong hệ thống.
C. IDS bảo vệ thông tin mạng ở mức độ cao.
D. IDS là hệ thống phần cứng ngăn chặn các xâm nhập trái phép.

Phát biểu nào đúng khi nói về SSL?
A. SSL hoạt động bên dưới TCP/IP.
B. Dùng để xác thực và mã hóa thông tin.
C. SSL là phiên bản đặc biệt của TSL.
D. Là dịch vụ an toàn ở tầng liên kết.

Tiện ích nào sau đây là một phương thức bảo mật truy cập từ xa tốt hơn telnet
A. SSH
B. SSL
C. VPN
D. IPSec

Bạn được yêu cầu triển khai giải pháp để kiểm soát việc truy xuất web của người dùng trong công ty. Giải pháp tốt nhất là triển khai:
A. IDS
B. Honeypot
C. Khóa cổng 80
D. Proxy server

Phát biểu nào đúng khi nói về IDS với cơ chế phát hiện sự bất thường (Anomaly Detection Model)
A. Cơ sở dữ liệu là các hành động thông thường.

B. Đưa ra kết quả dựa vào phép so sánh khớp mẫu.
C. Không hiệu quả trong phát hiện kiểu tấn công mới.
D. Tìm kiếm dựa trên "độ khớp" của hành động thực tế.

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

RAS được bảo vệ bằng cách nào?
A. An toàn vì không sử dụng mạng công cộng Internet.
B. Sử dụng PAP để chứng thực, mã hóa mật khẩu khi truyền.
C. Chỉ cho phép giao thức hợp lệ truy cập, khóa các giao thức khác.
D. Chỉ chứng thực 1 chiều từ Client.

RAS sử dụng các phương pháp chứng thực nào?
A. PAP
B. SPAP
C. CHAP
D. Tất cả các ý trên