Kỹ thuật tấn công nào cần có kết nối vật lý đến đường truyền, có quyền nhận thông tin và bộ giải mã?
A. Quét cổng.
B. Quét địa chỉ IP.
C. Xác định hệ điều hành.
D. Nghe lén.

Kỹ thuật nghe lén được dùng trong loại tấn công nào?
A. Do thám.
B. Truy cập và từ chối dịch vụ.
C. Từ chối dịch vụ.
D. Do thám, truy cập.

Phiên bản ISO 1799-2005 không bao gồm nội dung nào sau đây?
A. Chính sách an ninh chung
B. Tổ chức an toàn thông tin
C. An ninh nhân sự
D. Chính sách phát triển nhân sự

Phát biểu nào đúng khi nói về nguy cơ gây mất an ninh trong hệ thống?
A. Nguy cơ do con người bao gồm các vấn đề như: truy nhập trái phép, …
B. Nguy cơ do môi trường bao gồm các vấn đề như động đất, bão lụt, …
C. Nguy cơ do tự nhiên bao gồm các lỗi cố ý hay vô ý gây hại cho hệ thống.
D. Tất cả các ý trên.

Trong một hệ thống mạng, khi một chế độ đặc quyền tự động được login sẽ tạo ra mối đe dọa nào?
A. Chủ động.
B. Thụ động.
C. Cố ý
D. Vô ý.

Virus không có đặc điểm nào sau đây?
A. Có khả năng gây hại phần mềm.
B. Có khả năng gây hại phần cứng.
C. Tự nhân bản.
D. Tự hủy khi hết vòng đời.

Loại tấn công nào dựa vào việc kẻ tấn công chèn JavaScrip vào vùng nhập văn bản của người dùng mà loại văn bản này sẽ được xem bởi người dùng khác?
A. SQL injection
B. Clickjacking
C. Bluejacking

D. Cross-site scripting

Kiểu tấn công nào dựa trên việc gửi nhiều dữ liệu đến một biến mục tiêu hơn dữ liệu thực sự có thể giữ?
A. Bluesnarfing
B. Bluejacking
C. DDoS
D. Buffer overflow

Bạn có trách nhiệm đối phó với sự cố tại một ngân hàng cỡ trung bình. Bạn đã phát hiện ra rằng ai đó có thể thâm nhập thành công mạng của bạn và đánh cắp dữ liệu từ máy chủ cơ sở dữ liệu của bạn. Tất cả các máy chủ được cấu hình để chuyển tiếp nhật ký đến một máy chủ ghi nhật ký trung tâm. Tuy nhiên, khi bạn kiểm tra nhật ký trung tâm đó, không có mục nào sau 2:13 sáng hai ngày trước. Bạn kiểm tra các máy chủ và chúng đang gửi nhật ký đến đúng máy chủ, nhưng chúng không đến đó. Điều nào sau đây sẽ có nhiều khả năng để giải thích điều này?
A. Máy chủ đăng nhập của bạn có một backdoor
B. Máy chủ đăng nhập của bạn đã bị tấn công với mộtbuffer overflow
C. IDS của bạn đang gặp trục trặc và chặn việc truyền nhật ký
D. Switches của bạn đã bị nhiễm ARP poisoning

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. Cross-site request forgery
B. Cross-site scripting
C. SQL injection
D. Typosquatting

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

Trong khi điều tra phần mềm độc hại trên mạng công ty của bạn, bạn phát hiện ra một điều rất kỳ lạ. Có một tệp có cùng tên với DLL hệ thống Windows và thậm chí có cùng giao diện API, nhưng xử lý đầu vào rất khác nhau, để giúp kiểm soát hệ thống và có vẻ như các ứng dụng đã đính kèm vào tệp này, chứ không phải là hệ thống DLL thực. Những gì mô tả tốt nhất này?
A. Refactoring
B. Backdoor
C. Trojan horse
D. Shimming

Biểu hiện nào sau đây không là dấu hiệu khi bị nhiễm virus?
A. Máy chạy chậm hơn bình thường.
B. Vào trình duyệt hiện ngay những trang không mong muốn.
C. Một số tiện ích không hoạt động.
D. Yêu cầu chạy ứng dụng với quyền admin.

Bạn là quản trị viên bảo mật cho một ngân hàng. Bạn rất quan tâm đến việc phát hiện bất kỳ lỗ hổng hoặc thậm chí cố gắng xâm nhập mạng của bạn, bao gồm cả những vi phạm từ nhân viên nội bộ. Nhưng bạn không muốn báo động nhầm (false positives) để gián đoạn công việc. Thiết bị nào sau đây sẽ là lựa chọn tốt nhất trong tình huống này?
A. IPS
B. WAF
C. SIEM
D. IDS

Mạng không dây của bạn đã có lỗ hổng. Có vẻ như kẻ tấn công đã sửa đổi một phần dữ liệu được sử dụng với mật mã luồng (Stream cipher) và sử dụng điều này để lộ ra dữ liệu được mã hóa không dây. Cuộc tấn công này được gọi là gì?
A. Evil twin
B. Rogue WAP
C. Tấn công WPS
D. Tấn công IV

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

Bạn đang thực hiện một bài kiểm tra thâm nhập mạng của công ty bạn. Là một phần của bài kiểm tra, bạn sẽ được cung cấp thông tin đăng nhập với quyền truy cập tối thiểu và sẽ cố gắng truy cập vào quyền quản trị bằng tài khoản này. Cái này gọi là gì?
A. Climbing
B. Root grabbing
C. Session hijacking
D. Privilege escalation

Mô hình hệ mã hóa đối xứng không bao gồm thành phần nào sau đây?
A. Văn bản gốc.
B. Văn bản mã hóa.
C. Giải thuật mã hóa.

D. Khóa riêng.

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

Trong phương pháp RSA, với p=7, q=13; giá trị phù hợp của e là bao nhiêu?
A. 9
B. 72
C. 144
D. 11

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}

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.

Phát biểu nào sai khi nói về DMZ?
A. Truy cập vào DMZ được giới hạn bởi FireWall và Router.
B. Truy cập vào DMZ được điều khiển bởi FireWall và Router.
C. DMZ là vùng đặc biệt trong mạng cho phép người dùng truy xuất vào.
D. Nếu vùng DMZ bị tấn công sẽ ảnh hưởng đến mạng riêng.

Lời khuyên nào là đúng để ngăn ngừa tấn công mật khẩu?
A. Thường xuyên login với mật khẩu sai.
B. Cho phép truy cập từ xa với giao thức FTP.
C. Cho phép truy cập từ xa với giao thức Telnet.
D. Giới hạn số lần login sai.

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

D. SSL, TLS

Phát biểu nào sai khi nói về hệ thống phát hiện xâm nhập phần mềm?
A. Cần máy chủ khá mạnh
B. Cần không gian đĩa cứng lớn.
C. Có thể chạy trên nhiều loại hệ điều hành khác nhau.
D. Có 2 loại điển hình là Cisco IDS 4235, Cisco IPS 4200.

Trên mạng không dây, giao thức an toàn WEP có đặc điểm gì?
A. Chỉ dùng khóa 128 bit.
B. Không có lỗ hỏng bảo mật.
C. Sử dụng khóa riêng.
D. Dùng thuật toán RC4 để mã hóa.

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

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. Sao lưu hệ thống thường xuyên
C. Cài đặt lại HĐH thông dụng
D. Cập nhật HĐH thường xuyên

Các đối tượng cần gia cố bao gồm:
A. Hệ điều hành, ứng dụng mạng và các thiết bị mạng.
B. Hệ điều hành, ứng dụng mạng và các phần mềm ứng dụng khác.
C. Hệ điều hành, ứng dụng mạng và các thiết bị vào ra.
D. Hệ điều hành, ứng dụng mạng và hệ điều hành mạng.