Phát biểu nào đúng về chuẩn ISO 17799?
A. Được thiết lập đầu tiên vào năm 1999 bởi tổ chức ISO.
B. Là tiêu chuẩn mang tính tầm cao, theo lĩnh vực hẹp, thiên về thực tiễn.
C. Chỉ áp dụng trong số ít cơ quan tổ chức, các ứng dụng đơn ngành.
D. Là tiêu chuẩn tập trung chuyên sâu vào an toàn thông tin.

Khi nói về hacker, phát biểu nào sau đây là sai?
A. Cracker là một loại hacker.
B. Là người dùng kiến thức bản thân để tấn công hệ thống máy tính.
C. Là người rất am tường về hoạt động của máy tính và mạng máy tính.
D. Thâm nhập hệ thống với mục đích đánh cắp thông tin, phá hoại.

Việc tấn công chỉ với mục đích tìm kiếm thông tin là loại tấn công nào sau đây?
A. Truy cập.
B. Nghe lén.
C. Từ chối dịch vụ.
D. Do thám.

Trong quy trình xây dựng mạng an toàn, việc nào sau đây được làm sau cùng?
A. Lập kế hoạch và tiến hành xây dựng hệ thống.
B. Đánh giá nguy cơ gây mất an toàn.
C. Khảo sát hệ thống.
D. Kiểm tra, đánh giá hoạt động của 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.

Hiệu năng của một máy tính giảm bất thường, khi kiểm tra bạn thấy có phần mềm gián điệp (spyware). Người sử dụng máy tính khẳng định gần đây chỉ tải một phần mềm miễn phí phục vụ cho công việc của anh ta. Máy tính này đã bị nhiễm loại mã độc nào?
A. Logic bomb
B. Rootkit
C. Macro virus
D. Trojan horse

Một website bán hàng có cho phép người dùng nhận xét (review) về sản phẩm được bán. Kẻ tấn công nhập một đoạn mã javascript vào nội dung nhận xét. Đoạn mã này có thể được chạy khi người dùng khác xem thông tin nhận xét sản phẩm đó. Kỹ thuật tấn công này được gọi là:
A. SQL injection

B. Logic bomb
C. Session hijacking
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

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

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 là một quản trị mạng cho một trường đại học nhỏ. Anh ta phát hiện ra rằng một số máy trên mạng của mình bị nhiễm phần mềm độc hại. Phần mềm độc hại đó đang gửi một loạt các gói đến một mục tiêu bên ngoài mạng. Thuật ngữ nào mô tả tốt nhất cuộc tấn công này?
A. SYN flood
B. Botnet
C. Backdoor
D. DDoS

Hình thức tấn công bằng cách hủy kết nối (deauthorize) giữa một người dùng (user) với một tài nguyên (resource) được gọi là:
A. Session hijacking
B. Man-in-the-middle

C. Smurf attack
D. Disassociation

Nhân viên quản trị của công ty đã cài mã độc vào máy chủ, mã độc này sẽ kích hoạt khi nhân viên này nghỉ việc. Loại mã độc này được gọi là:
A. Worm
B. Trojan horse
C. Virus
D. Logic bomb

Một trong những người dùng của bạn không thể nhớ lại mật khẩu cho máy tính xách tay của họ. Bạn muốn khôi phục mật khẩu đó cho họ. Bạn có ý định sử dụng một công cụ / kỹ thuật phổ biến với những hacker và nó bao gồm các bảng tìm kiếm các giá trị băm được tính toán trước để khôi phục mật khẩu. Thuật ngữ nào mô tả tốt nhất tình huống này?
A. Dictionary attack
B. Social engineering
C. Backdoor
D. Rainbow table

Ai đó đã lục lọi trong thùng rác của công ty bạn để tìm kiếm tài liệu, sơ đồ hoặc thông tin nhạy cảm khác đã bị vứt đi. Thuật ngữ nào mô tả tình huống này?
A. Trash engineering
B. Social engineering
C. Trash diving
D. Dumpster diving

Jared chịu trách nhiệm về an ninh mạng tại công ty của mình. Anh ta đã phát hiện ra biểu hiện trên một máy tính chắc chắn là virus. Anh ta thậm chí đã xác định được một tập tin mà anh ta nghĩ có thể là virus. Tuy nhiên, sử dụng ba chương trình chống virus riêng biệt, anh thấy rằng không có chương trình nào phát hiện các tập tin đó nhiễm virus. Tình huống nào sau đây có khả năng xảy ra cao nhất?
A. Máy tính có một RAT
B. Máy tính có một logic bomb
C. Máy tính có một rootkit
D. Máy tính có một lỗ hổng zero-day

Frank đã phát hiện ra rằng ai đó có thể lấy thông tin từ điện thoại thông minh của mình bằng kết nối Bluetooth. Kẻ tấn công đã có thể lấy danh sách liên lạc của anh ta và một số email anh ta đã nhận được. Loại tấn công này được gọi là gì?
A. Session hijacking
B. Tấn công Backdoor
C. CSRF
D. Bluesnarfing

John đã phát hiện ra rằng một kẻ tấn công đang cố lấy mật khẩu mạng bằng cách sử dụng phần

mềm thử một số mật khẩu từ danh sách các mật khẩu phổ biến. Đây là loại tấn công nào?
A. Rainbow table
B. Brute force
C. Session hijacking
D. Dictionary attack

Loại mã độc nào tự nhân bản mà không cần người dùng phải kích hoạt một tập tin thực thi nào đó?
A. Virus
B. Trojan
C. Stealth virus
D. Worm

Khác biệt chính giữa hoạt động dò tìm lỗ hổng bảo mật (vulnerability scan) và kiểm tra bảo mật (penetration test) là gì?
A. Dò tìm lỗ hổng bảo mật được thực hiện bởi nhân viên của tổ chức, kiểm tra bảo mật được thực hiện bởi những người bên ngoài.
B. Dò tìm lỗ hổng bảo mật chỉ sử dụng tool có sẵn
C. Dò tìm lỗ hổng bảo mật thường là white-box test, kiểm tra bảo mật thường là black-box test
D. Dò tìm lỗ hổng bảo mật chỉ để tìm ra lỗi, kiểm tra bảo mật hướng đến cách khắc phục.

Hacker thực hiện xâm nhập một hệ thống và sử dụng nó làm cơ sở để tấn công một hệ thống khác có liên quan. Hoạt động đó gọi là:
A. Man-in-the-middle
B. Shimming(chèn code giữa main program và library)
C. Vishing(lừa đảo qua đường điện thoại - VoIP)
D. Pivot

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

Mục đích của việc xác thực là gì?
A. Chống giả mạo.
B. Bảo đảm hoạt động của giao thức.
C. Bảo đảm tính toàn vẹn.
D. Tất cả các ý trên.

Phương pháp xác thực nào dựa vào khóa bí mật dùng chung?
A. MAC-checksum, mã hóa khóa công khai.

B. Hàm băm, MAC-checksum.
C. Mã hóa thông điệp.
D. Mã hóa đối xứng, MAC-checksum.

Phương pháp xác thực nào còn tạo ra chữ ký số?
A. Mã hóa khóa bí mật.
B. Hàm băm.
C. MAC-checksum.
D. Mã hóa khóa công khai.

Khi dùng phương pháp Caesar để mã hóa, với k=5 và văn bản gốc "AANTOANMANG" thì văn bản mã hóa là:
A. FESYYFSRFSL
B. EFSYYFSRFSL
C. FFSYYFSRFSG
D. FFSYYFSRFSL

Khi dùng phương pháp Caesar để mã hóa, với k=15 và văn bản gốc "ANNINH" thì văn bản mã hóa là:
A. QDDYDH
B. QDEYDX
C. QQDYDX
D. QDDYDX

Khi dùng phương pháp mã hóa hàng rào để mã hóa, với chiều cao là 2 và văn bản gốc "WILLIAMSHACSKPEAR" thì văn bản mã hóa là:
A. WIASAKPAILMHCSER
B. WLLASAKPAILMHCSER
C. WILASAKPAILMHCSER
D. WLIMHCSERILASAKPA

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=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 sai khi nói về giới hạn của FireWall?
A. Không thể bảo vệ trước tấn công của Virus.
B. Không thể bảo vệ trước các mối nguy hại từ bên trong.
C. Không thể ngăn chặn các tấn công thông qua Dialup.
D. Không thể sử dụng để cài đặt VPN.

Phát biểu nào sai khi nói về phương thức đánh cắp bằng Packet Sniffer?
A. Có thể phát hiện và ngăn ngừa bằng cách xác thực với PIN và Password ngẫu nhiên.
B. Có thể ngăn ngừa bằng cách mã hóa thông tin lưu thông trên mạng.
C. Việc sử dụng Password ngẫu nhiên làm cho hacker bắt được Password không giá trị.
D. Không thể bắt đươc tất cả các gói tin lưu chuyển trong mạng.

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

Mật khẩu nào sao đây được xem là an toàn?
A. password99
B. 1234abcd
C. afghr12JK
D. !@2Afe43

Thứ tự các bước trong hoạt động mạng không dây như thế nào là đúng?
A. Probing (Thăm dò) - Beacon (Báo hiệu) - Authentication (Chứng thực) - Association (Ghép nối).
B. Beacon (Báo hiệu) - Probing (Thăm dò) - Association (Ghép nối)- Authentication (Chứng thực).
C. Probing (Thăm dò) - Authentication (Chứng thực) - Beacon (Báo hiệu) - Association (Ghép nối).
D. Beacon (Báo hiệu) - Probing (Thăm dò) - Authentication (Chứng thực) - Association (Ghép nối).

Các giao thức đường hầm nào sau đây chỉ làm việc trên các mạng IP?
A. SSH
B. IPX
C. PPTP
D. LSTP

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

Các thiết bị trên tầng mạng có vai trò gì?
A. Ghi nhận địa chỉ vật lý của thiết bị mạng.
B. Chuyển dữ liệu dựa trên địa chỉ MA
C. Là nơi người dùng truy cập vào mạng để truy xuất tài nguyên.
D. Vạch đường cho các gói tin.

Phát biểu nào sai khi nói về ứng dụng mạng?
A. Tấn công DNS Server để đánh lừa người dùng truy cập qua một địa chỉ giả mạo.
B. Server phục vụ chia sẻ file bị tấn công vì người dùng không quản lý được việc chia sẻ của mình
C. Mail Server có thể bị các dạng tấn công DoS, virus, tấn công giả mạo và tấn công relay.
D. FTP Server chỉ bị tấn công bởi người dùng bên ngoài mạng.

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 chứng thực 1 chiều từ Client.
D. Chỉ cho phép giao thức hợp lệ truy cập, khóa các giao thức khác.