Mục lục

Câu 1: Khái niệm đánh giá an toàn hệ thống thông tin.

- Theo NIST: đánh giá an toàn hệ thống thông tin (information security assessment) là quy trình xác định tính hiệu quả của một thực theer được đánh giá (ví dụ như máy tính, hệ thống, mạng, quy trình vận hành, con người…) đáp ứng các mục tiêu an ninh cụ thể.
    - Tập trung vào 3 phương pháp chính: kiểm thử (testing), kiểm tra (examination), phỏng vấn (interviewing).
- Theo SANS: đánh giá an toàn hệ thống thông tin là thước đo độ an toàn của hệ thống hoặc tổ chức, hay còn hiểu là cách thức thực hiện an toàn thông tin.
    - Dựa trên việc xác định các rủi ro, trong đó tập trung vào xác định điểm yếu và các tác động tới hệ thống.
    - Đánh giá an toàn dựa trên 3 phương pháp chính có liên quan đến nhau là: rà soát (reviewing), kiểm thử (testing), kiểm tra (examination).
    - Rà soát: bao gồm các kỹ thuật xem xét thụ động và thực hiện phỏng vấn. Thường được thực hiện thủ công.
    - Kiểm tra: xem xét cụ thể tại tổ chức từ mức hệ thống/mạng để xác định các điểm yếu an ninh tồn tại trong hệ thống.
    - Kiểm thử: đóng vai trò như kẻ tấn công. Thực hiện các phương pháp tìm kiếm lỗ hổng bảo mật trong mạng để thực hiện xâm nhập tới hệ thống hoặc mạng.

Câu 2: Tầm quan trọng của đánh giá an toàn hệ thống thông tin

- Xác định mức độ an ninh hiện tại của hệ thống thông tin trong một tổ chức.
    - Có cái nhìn toàn diện về các mối nguy hại tồn tại trong hệ thống mạng.
    - Có các giải pháp khắc phục, cải tiến hệ thống thông tin tiếp cận các mục tiêu an ninh.
    - Giảm thiểu các rủi ro.
- Cho phép trả lời các câu hỏi:
    - Các thông tin quan trọng là gì?
    - Hệ thống thông tin đã triển khai các giải pháp đảm bảo an ninh nào?
    - Tình hình an ninh thông tin hiện tại là như thế nào?
    - Có cần thêm các biện pháp để đối phó với vấn đề đảm bảo an ninh thông tin hay không?
    - Vấn đề nào cần ưu tiên trong lộ trình xử lý để đảm bảo an toàn thông tin một cách đầy đủ?

Câu 3: Các kỹ thuật đánh giá

- Kỹ thuật rà soát:
  - Là kỹ thuật kiểm tra được dùng để đánh giá hệ thống, ứng dụng, mạng, chính sách, thủ tục.
  - Bao gồm:
    - Rà soát tài liệu.
    - Rà soát nhật ký.
    - Rà soát tập luật.
    - Rà soát cấu hình hệ thống.
    - Thăm dò mạng…
- Kỹ thuật phân tích và xác định mục tiêu:
  - Xác định hệ thống, các cổng, dịch vụ và các lỗ hổng.
  - Bao gồm:
    - Phát hiện mạng.
    - Nhận dạng cổng và dịch vụ mạng.
    - Quét lỗ hổng.
    - Quét mạng không dây.
    - Kiểm tra an toàn ứng dụng.
- Kỹ thuật xác định điểm yếu mục tiêu:
  - Xác định sự tồn tại của các lỗ hổng trong hệ thống.
  - Bao gồm:
    - Bẻ mật khẩu.
    - Kiểm thử xâm nhập.
    - Kỹ nghệ xã hội.
    - Kiểm thử an toàn ứng dụng.

Câu 4: So sánh kiểm thử và kiểm tra

Kiểm tra	Kiểm thử
Nhiệm vụ: - Xem xét các tài liệu, quy trình, thủ tục để đảm bảo mọi thứ thực hiện theo đúng mục tiêu đề ra. - Ví dụ: xem xét tập luật của tường lửa, xem xét thủ tục đảm bảo an toàn trong đặt mật khẩu… Không ảnh hưởng tới hệ thống mạng thực tế. Có một cái nhìn toàn diện về hệ thống mạng đánh giá. Đòi hỏi sự phối hợp của nhiều người, nhiều bộ phận.	Nhiệm vụ: - Thử nghiệm các thử nghiệm tới hệ thống và mạng để xác định các lỗ hổng an toàn. - Ví dụ: kiểm thử xâm nhập hệ thống, kiểm thử xâm nhập hệ thống ứng dụng web, kiểm thử xâm nhập mạng wireless… Có thể ảnh hưởng tới hệ thống hoặc mạng thực tế. Không có cái nhìn toàn diện về hệ thống mạng đánh giá. Chỉ cần phối hợp của ban lãnh đạo và bộ phận quản trị mạng.

Câu 5: Rà soát hệ thống

- Là việc kiểm tra các quy trình áp dụng chính sách, thủ tục theo các tiêu chuẩn, quy định nhằm:
    - Tìm ra những kẽ hở và điểm yếu có thể ảnh hưởng tới kiểm soát an ninh của hệ thống.
    - Tinh chỉnh các kỹ thuật kiểm tra và kiểm thử khác.
- Bao gồm:
    - Kiểm tra chính sách bảo mật.
    - Kiểm tra kiến trúc, yêu cầu, các quy trình hoạt động chuẩn.
    - Kiểm tra các kế hoạch đảm bảo an toàn hệ thống.
    - Kiểm thử các bản ghi chép về những thỏa thuận và hợp đồng về việc liên kết hệ thống.
    - Kiểm tra kế hoạch phản ứng sự cố.
- Kiểm tra lại tài liệu không thể đưa ra kết luận các kiểm soát an ninh có vấn đề mà nó chỉ là một hướng tìm kiếm nhằm hỗ trợ cơ sở hạ tầng an ninh hệ thống.

Câu 6: Rà soát nhật ký

- Là việc kiểm tra lại các nhật ký nhằm:
    - Kiểm tra tính chính xác của việc ghi nhật ký.
    - Xác nhận rằng hệ thống đang hoạt động theo đúng các chính sách của tổ chức.
- Bao gồm:
    - Rà soát nhật ký tường lửa.
    - Rà soát nhật ký IDS.
    - Rà soát nhật ký máy chủ.
    - Rà soát nhật ký trên các thiết bị mạng.
- Rà soát nhật ký nên được thực hiện thường xuyên.
- Với hệ thống mạng có quy mô nhỏ, không có nhiều dữ liệu cần bảo vệ thì nên rà soát 1 tháng 1 lần.
- Với hệ thống mạng quy mô lớn, có nhiều tài nguyên quan trọng nên rà soát hàng ngày hoặc hàng tuần.
- Một số thông tin nhật ký hữu dụng khi thực hiện đánh giá:
    - Nhật ký của tường lửa và bộ định tuyến ghi chép lại các kết nối từ mạng nội bộ ra bên ngoài mà có tiềm năng là những kết nối của các thiết bị độc hại từ bên trong (ví dụ: rootkit, bot, trojan horse, spyware).
    - Nhật ký tường lửa về những thông tin kết nối không thành công và những nỗ lực truy cập trái phép.
    - Nhật ký ứng dụng ghi chép lại những nỗ lực kết nối trái phép, thay đổi tài khoản, sử dụng đặc quyền và sử dụng những thông tin của CSDL hoặc ứng dụng.
    - Nhật ký của các phần mềm phòng chống virus ghi chép những cập nhật thất bại, hoặc những phần mềm đã lỗi thời.

- Nhật ký bảo mật trong quản lý bản vá lỗi cụ thể nào đó hoặc trong hệ thống IDS/IPS có thể ghi chép lại những thông tin về những hệ thống dịch vụ và ứng dụng mà chưa được biết đến.

Câu 7: Rà soát tập luật

- Tập luật là tập hợp các quy tắc mà hệ thống hoặc mạng so sánh để quyết định nên làm gì hoặc hành động nào được chấp thuận.
- Ví dụ:
  - Tập luật tường lửa: cho phép hoặc từ chối một gói dữ liệu khi đi qua.
  - Tập luật IDS: cảnh báo khi có xâm nhập bất hợp pháp tới hệ thống.
  - Tập luật AV: xóa file khi xác định có chứa mã độc.
- Rà soát tập luật nhằm:
  - Tìm ra những lỗi hoặc lỗ hổng bảo mật trên các thiết bị an ninh: lỗ hổng bảo mật mạng, các vi phạm chính sách.
  - Tìm ra các thiếu sót hoặc không hiệu quả làm ảnh hưởng đến hiệu suất của bộ luật.
- Bao gồm:
  - Bộ luật thiết đặt cho tường lửa.
  - Luật thiết đặt cho hệ thống IDS/IPS.
  - Luật điều khiển, kiểm soát truy cập trên bộ định tuyến…
- Đối với danh sách điều khiển truy cập trên bộ định tuyến:
  - Chỉ giữ lại những luật cần thiết. Ví dụ những luật được thiết lập với mục đích tạm thời phải được gỡ bỏ ngay sau khi không cần tới.
  - Mặc định từ chối tất cả những lưu lượng mạng, chỉ chho phép những lưu lượng đã được cấp quyền theo chính sách được truy cập.
- Đối với tường lửa:
  - Chỉ giữ lại những luật cần thiết.
  - Luật thực thi việc truy cập đặc quyền tối thiểu.
  - Tạo những luật cụ thể trước rồi tạo một luật chung sau.
  - Không nên mở những cổng không cần thiết để thắt chặt an ninh.
  - Các luật được thiết lập không cho phép các truy cập vượt qua các rào cản an ninh khác.
- Đối với hệ thống IDS/IPS:
  - Những mẫu (signature) không cần thiết cần phải được vô hiệu quá hoặc gỡ bỏ.
  - Những mẫu cần thiết phải được kích hoạt, chỉnh sửa và bảo trì hợp lý.

Câu 8: Rà soát cấu hình hệ thống

- Là một quá trình kiểm tra nhằm:
  - Xác định những dịch vụ hoặc ứng dụng không cần thiết.
  - Xác định các tài khoản người dùng và thiết lập mật khẩu không hợp lý.
  - Xác định những thiết lập sao lưu và đăng nhập không phù hợp.
- Kiểm tra thông qua những file cấu hình hệ thống đã được lưu trữ sẵn trong các tập tin khác nhau trong các hệ điều hành.
- Ví dụ:
  - Hệ điều hành Windows: nơi lưu trữ file cấu hình hệ thống: "windows security policy settings".
  - Hệ điều hành Linux/Unix: nơi lưu trữ file cấu hình hệ thống: /etc.

Câu 9: Khám phá mạng

- Là việc phát hiện những máy chủ, máy trạm, thiết bị mạng đang hoạt động trong một mạng.
- Có hai phương pháp khám phá mạng là khám phá thụ động và khám phá chủ động.

	Khám phá thụ động	Khám phá chủ động
Nội dung	- Sử dụng công cụ dò quét mạng và theo dõi: lưu lượng mạng, các địa chỉ IP của những máy đang hoạt động, cách thức kết nối, xử lý thông tin trên mang, tần suất liên lạc giữa các máy trong mạng. - Được thực hiện từ một máy tính trong mạng nội bộ.	- Sử dụng công cụ tự động gửi trực tiếp các gói tin mong muốn (TCP, ICMP, UDP) tới các máy chủ để: xác định các máy chủ, máy trạm, trạng thái hoạt động của các máy, xác định cổng mạng và trạng thái hoạt động của các cổng, xác định hệ điều hành đang chạy.
Ưu điểm	- Không ảnh hưởng tới hoạt động của mạng	- Mất ít thời gian để thu thập thông tin. - Có thể thực hiện khám phá mạng từ một mạng khác mạng khám phá.
Nhược điểm	- Tốn thời gian để thu thập thông tin.	- Có thể gây nhiễu hoặc trễ mạng.

	- Không phát hiện được các thiết bị mạng hoặc máy chủ/ máy trạm không thực hiện nhận hoặc gửi gói tin trong khoảng thời gian giám sát.	- Có thể kích hoạt các tính năng cảnh báo từ các thiết bị IDS hoặc các thiết bị an ninh khác. - Thông tin có thể bị sai lệch.

Câu 10: Xác định cổng và dịch vụ mạng.

- Sử dụng công cụ dò quét để xác định các cổng, dịch vụ đang hoạt động.
- Quá trình truyền tin TCP: sử dụng quy tắc bắt tay 3 bước (tự nêu).
- Các phương pháp quét cổng:
    - **TCP connect**: client gửi gói tin chứa cờ SYN và một thông số cổng nhất định tới server. Server trả về gói SYN/ACK: cổng mở, server gửi về gói RST: cổng đóng. Client gửi tiếp đến server một gói tin ACK+RST.
    - **Quét Stealth (quét một nửa)**: client gửi gói tin chứa cờ SYN và một thông số cổng nhất định tới server. Server trả về gói SYN/ACK: cổng mở, server gửi về gói RST: cổng đóng. Client gửi tiếp đến server một gói tin RST.
    - **Quét XMAS**: client gửi những gói TCP với số cổng nhất định cần quét chứa nhiều thông số cờ như: FIN, URG, PSH tới server. Server gửi về gói RST: cổng đóng.
    - **Quét FIN:** client chưa có kết nối tới server nhưng vẫn tạo ra gói FIN với số cổng nhất định gửi tới server. Server gửi về gói ACK: cổng mở, server gửi về gói RST: cổng đóng.
    - **Quét NULL**: client gửi tới server những gói TCP với số cổng cần quét mà không chứa thông số cờ nào. Server gửi về gói RST: cổng đóng.
    - **Quét IDLE**:
        - Client gửi gói tin SYN/ACK tới mục tiêu là zombie để thăm dò số IPID.
        - Zombie khi nhận được gói tin sẽ từ chối kết nối bằng cách gửi lại gói tin RST.
        - Client gửi tới server một gói tin chứa cờ SYN kèm theo số hiệu cổng với địa chỉ IP là giả mạo địa chỉ IP của zombie.
        - Zombie sau khi nhận được gói tin SYN/ACK sẽ gửi lại cho server gói tin RST với số IPID tăng thêm 1.
        - Client gửi lại yêu cầu kết nối tới zombie với số IPID giống IPID đã thăm dò được từ trước.
        - Zombie tiếp tục gửi trả lời lại gói tin RST kèm theo số IPID tăng thêm: IPID tăng 2: cổng mở, IPID tăng 1: cổng đóng.

- **Quét UDP**: client gửi gói tin ICMP request tới server. Server gửi về gói tin ICMP type 3 code 3 với nội dụng là "unreachble": cổng đóng.
- **Xác định hệ điều hành**:
  - Dùng kỹ thuật fingerprinting.
  - Tạo các kết nối TCP đến máy đích và dựa vào gói SYN/ACK để lấy thông tin về hệ điều hành.
  - So sánh với CSDL.

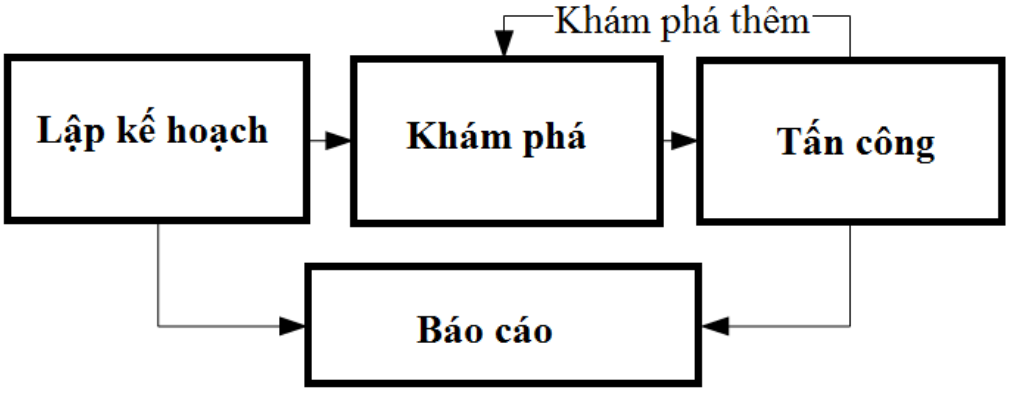
Câu 11: Xác định điểm yếu mục tiêu với bẻ mật khẩu.

- Bẻ mật khẩu là quá trình khôi phục mật khẩu từ các bảng băm mật khẩu: xác định tài khoản với các mật khẩu yếu.
- Các phương pháp bẻ mật khẩu:
  - Dictionary Attack: một từ điển được đưa vào ứng dụng crack để xác định tài khoản.
  - Brute Forcing Attack: thử kết hợp tất cả các ký tự cho đến khi tìm ra mật khẩu.
  - Hybrid Attack: tương tự tấn công từ điển, nhưng thêm 1 vài số và ký tự.
  - Syllable Attack: kết hợp tấn công từ điển và tấn công brute force.
  - Rule-based Attack: được sử dụng khi đã có 1 số thông tin về mật khẩu.

Câu 12: Kiểm thử xâm nhập

- Kiểm thử xâm nhập là kiểm tra độ an toàn của hệ thống thông tin. Người đánh giá bắt chước những tấn công thực tế để phá vỡ các tính năng bảo mật của ứng dụng, hệ thống của mạng.
- Kiểm thử xâm nhập hữu ích cho việc xác định:
  - Làm thế nào hệ thống cho phép các dạng tấn công phổ biến thực tế.
  - Mức độ tinh vi của kẻ tấn công cần để làm tổn hại hệ thống.
  - Biện pháp đối phó bổ sung có thể giảm thiểu các mối đe dọa đối với hệ thống.
  - Khả năng phòng vệ để phát hiện các cuộc tấn công và phản ứng thích hợp.
- Cần có sự cho phép chính thức để tiến hành các kiểm thử xâm nhập trước khi bắt đầu:
  - Các địa chỉ/ dải IP cụ thể được kiểm tra.
  - Các máy chủ bị hạn chế.
  - Một danh sách các kỹ thuật kiểm thử chấp nhận được và các công cụ.
  - Thời gian kiểm thử được tiến hành.
  - Xác định một thời hạn nhất định cho kiểm thử.
  - Địa điểm liên lac cho các đội kiểm thử xâm nhập vào các hệ thống và mạng đích.
  - Các biện pháp để ngăn chặn sự thực thi luật được gọi là các cảnh báo sai (được tạo ra bởi quá trình kiểm thử).
  - Xử lý thông tin thu thập được bởi các nhóm kiểm thử xâm nhập.

Các pha kiểm thử:



- Khám phá:
  - Thu thập thông tin: thông tin địa chỉ IP và tên máy chủ, tên nhân viên và thông ti liên hệ, thông tin hệ thống như tên và các chia sẻ, thông tin dịch vụ và ứng dụng.
  - Xác định điểm yếu: dò quét cổng và dịch vụ, dò quét lỗ hổng.
- Tấn công:
  - Giành quyền truy cập: thu thập thông tin từ giai đoạn khám phá để chính thức giành quyền truy cập vào mục tiêu.
  - Leo thang đặc quyền: nếu chỉ dành được quyền truy cập của người dùng thì người kiểm thử sẽ cố gắng để lấy được quyền điều khiển hệ thống (truy cập cấp quản trị).
  - Duyệt hệ thống: tiếp tục thu thập thông tin để xác định cơ chế làm việc của hệ thống và giành quyền truy cập vào những hệ thống khác nữa.
  - Cài đặt thêm công cụ: cài thêm công cụ kiểm thử để có được thêm nhiều thông tin hoặc quyền truy cập hoặc là cả hai.

Câu 13: Kỹ nghệ xã hội

- Tấn công kỹ nghệ xã hôi:
  - Là việc thử lừa một người nào đó tiết lộ thông tin mà có thể được sử dụng để tấn công các hệ thống hoặc mạng.
  - Ví dụ: tài khoản đăng nhập, mật khẩu…
- Kiểm thử sử dụng kỹ nghệ xã hội: ể kiểm tra nhận thức của người dùng về vấn đề an ninh, và có thể bộc lộ điểm yếu trong hành vi người dùng.
- Cách thức thực hiện kiểm thử:
  - Qua các cuộc hội thoại thực hiện trực tiếp
  - Qua điện thoại
  - Qua email, tin nhắn tức thời…
- Một hình thức của kỹ nghệ xã hội phổ biến là phishing:
  - Sử dụng email xác thực để yêu cầu thông tin.
  - Hướng người dùng đến một trang web giả mạo để thu thập thông tin.

Câu 14: Các vấn đề liên quan tới chuẩn bị (hậu cần) đánh giá:

1. **Lựa chọn đánh giá viên**

- Đánh giá viên cần có kinh nghiệm, có kỹ thuât và chuyên môn sẽ giảm thiểu các rủi ro liên quan trong tiến hành kiểm thử an toàn.
- Kiến thức chuyên môn tốt về an ninh bảo mật và mạng máy tính, bao gồm an toàn mạng, tường lửa, hệ thống phát hiện xâm nhập, hệ điều hành, lập trình và các giao thức mạng (như TCP/IP).
- Làm việc nhóm.
- Tính đặc thù của hệ thống.
- Tính cập nhật của kiến thức, phương thức cũng như các công cụ phục vụ cho việc đánh giá.
- Trách nhiệm của đánh giá viên:
    - Thông báo cho các bên liên quan về các hoạt động đánh giá an toàn an ninh.
    - Phát triển xây dụng kế hoạch đánh giá.
    - Thực thi việc kiểm tra, kiểm thử, thu thập các dữ liệu liên quan.
    - Phân tích các dữ liêu được thu thaapj và phát triển các khuyến nghị giản lược.
    - Thực hiện các kiểm tra và kiểm thử bổ sung khi cần thiết để xác nhận các hoạt động giản lược.
    - Phối hợp với tổ chức được đánh giá.
    - Đảm bảo các quyền được gán và duy trì các bản sao được ký duyệt của kế hoạch đánh giá.
    - Ký kết và tuân thủ các thỏa thuận về không tiết lộ thông tin bí mật của tổ chức.
    - Bảo vệ dữ liệu theo quy định của tổ chức, bao gồm việc xử lý, truyền nhận, lưu trữ và xóa tất cả các dữ liệu thu thập được cũng như các báo cáo kết quả.

2. **Lựa chọn vị trí**

- Khi thực hiện kiểm thử, đánh giá viên có thể làm việc tại chỗ hoặc từ xa.
- Đánh giá viên có thể yêu cầu các mức độ truy cập khác nhau tới mạng phụ thuộc vào công cụ mà họ sử dụng.
- Khi lựa chọn địa điểm cho hoạt động đánh giá, cần cân nhắc các rủi ro vốn có của việc sử dụng địa điểm bên ngoài.

3. **Lựa chọn tài nguyên và công cụ kỹ thuật**

- Hệ thống thông tin được phát triển để thực thi việc đánh giá an ninh cần đáp ứng các yêu cầu của loại hình đánh giá và các công cụ đánh giá được thực hiện.
- Ví dụ, đối với việc bẻ khóa mật khẩu, thường yêu cầu bộ nhớ và tốc độ tính toán cao, do đó đội kiểm thử có thể yêu cầu một máy chủ bẻ khóa mật khẩu chuyên dụng.
- Các công cụ nên được lấy từ các nguồn đáng tin cậy và đảm bảo.
- Người kiểm thử cần có các kiến thức, kinh nghiệm và sử dụng thành thạo tất cả các hệ điều hành trên hệ thống kiểm thử bởi vì các công cu kiểm thử hoặc hệ thống kiểm thử có thể thường xuyên thay đổi.
- Phát triển và duy trì bản sao cơ sở để tiến hành cho kiểm thử.

- Đội kiểm thử di động cần có một bộ kit phù hợp gồm hệ thống, bản sao, công cụ bổ sung, cáp, máy chiếu và các thiết bị khác mà đội cần cho thực hiện kiểm thử tại các địa điểm khác nhau.

Câu 15: Xử lý dữ liệu

Xử lý dữ liệu đảm bảo bảo vệ dữ liệu nhạy cảm của tổ chức bao gồm kiến trúc hệ thống, cấu hình an toàn, các lỗ hổng hệ thống.

1. **Thu thập dữ liệu**

- Thông tin liên quan đến kiến trúc, cấu hình của mạng được đnahs giá, cũng như các thông tin liên quan đến hoạt động của đánh giá viên.
    - Kiến trúc và cấu hình: tên hệ thống, địa chỉ IP, hệ điều hành, vị trí mạng vật lý và logic, cấu hình bảo mật và các lỗ hổng.
    - Hoạt động đánh giá: nhật ký ghi lại từng bước hoạt động đánh giá.

2. **Lưu trữ dữ liệu**

Bảo mật dữ liệu được thu thập trong suốt quá trình đánh giá bao gồm lỗ hổng, kết quả phân tích, đề xuất giảm thiểu là trách nhiệm của đánh giá viên:

- Kế hoạch đánh giá và ROE.
- Tài liệu về cấu hình an ninh hệ thống và kiến trúc mạng.
- Kết quả thu được từ các công cụ tự động và những phát hiện khác.
- Báo cáo kết quả đánh giá.
- Kế hoạch khắc phục và các mốc thời gian (POA&M).
- Việc truy cập tới thông tin lưu trên hệ thống phải được hạn chế phân quyền, và chỉ có những người có trách nhiệm và vai trò mới được phép truy cập.
- Dữ liệu này cũng cần được mã hóa theo chuẩn FIPS 140-2 để đảm bảo an toàn dữ liệu.
- Hệ thống đánh giá – như máy chủ, máy tính xách tay, các thiết bị di động cũng phải có những biện pháp bảo vệ về mặt logic và vật lý tại nơi hoạt động.

3. **Truyền dữ liệu**

Phương pháp truyền dữ liệu nhạy cảm bao gồm việc mã hóa các tệp trên chứa dữ liệu nhạy cảm, mã hóa kênh thông tin tuân the FIPS (VPN, SSL) và truyền các thông tin thông quâ việc giao nhận các bản copy.

4. **Hủy bỏ dữ liệu**

Khi các dữ liệu đánh giá không còn cần thiết, hệ thống đánh giá, các tài liệu sao lưu, các phương tiện cần phải được thu dọn sạch sẽ:

- Sắp xếp:
    - Không khuyến khích với dữ liệu đa phương tiện.
    - Thương thực hiện với những giấy tờ mà không chứa nội dung quan trọng.

- Làm sạch:
    - Thu dọn dữ liệu để đảm bảo tính bí mật của dữ liệu khỏi các tấn công theo vết bàn phím.
    - Tránh khôi phục từ các dữ liệu, các ổ đĩa hoặc các tiện ích khôi phục dữ liệu.
    - Chống được các tấn công dụa vào bàn phím từ các thiết bị đầu vào hoặc các công cụ tìm kiếm.
    - Một trong số các phương pháp được chấp nhận cho việc làm sạch thông tin là việc ghi đè dữ liệu (overwriting).
- Tẩy sách:
    - Quá trình thu dọn phương tiện là để bảo vệ tính bí mật của dữ liệu khỏi các tấn công.
    - Với một số dữ liệu, việc làm sạch vẫn chưa đủ hiệu quả để che dấu.
    - Ví dụ về việc làm sạch dữ liệu là thực thi các câu lệnh firmware Secure Arase (chỉ cho các ổ đĩa ATA – Advanced Technology Attachment) và khử từ.
- Tiêu hủy:
    - Phá hủy vật lý các thiết bị để không có khả năng sử dụng giúp tránh thu được dữ liệu lưu trong đó.
    - Phương pháp: đốt, đập nát, nung chảy, nghiền…

Lưu ý:

- Các tổ chức cần duy trì chính sách yêu cầu cho việc xử lý hủy bỏ hệ thống đánh giá.
- Chuẩn NIST SP 800-88 đưa ra một lược đồ luồng để hỗ trợ tổ chức trong việc xác định các phương pháp hủy bỏ dữ liệu áp dụng phù hợp từng hoàn cảnh.
- Các đánh giá viên từ bên thứ ba cũng cần hiểu yêu cầu hủy bỏ dữ liệu của các tổ chức có thể khác nhau và ở các bộ phận trong cùng tổ chức cũng có những yêu cầu khác nhau.

Câu 16: Hoạt động sau đánh giá: Lập báo cáo

1. **Thông tin về hệ thống**

- Giúp biết được các thông tin chung về mục tiêu, địa điểm, đối tượng thực hiện.
- Căn cứ pháp lý khi có sự cố xảy ra:
    - Địa điểm thực hiện đánh giá.
    - Thời gian thực hiện đánh giá.
    - Người thực hiện đánh giá.
    - Người theo dõi đánh giá.
    - Thông tin về hợp đồng đánh giá.
    - Phiên bản báo cáo…

2. **Cấu trúc hệ thống**

- Các thông tin về sơ đồ cấu trúc hệ thống đánh giá.
- Để dễ dàng cho người đọc báo cáo, người lập báo cáo cần tổng hợp các thông tin theo các mức độ rủi ro khác nhau:
    - Mức độ nguy hại.

- Công cụ sử dụng (nếu có).
- Cách thức kiểm tra.
- Kết quả.
- Mô tả về nguy hại có thể xảy đến.
- Các khuyến cáo để phòng chống rủi ro.

3. **Các rủi ro mức cao**
4. **Các rủi ro mức trung bình và mức thấp.**

Câu 17:Khái niệm kiểm định an toàn thông tin. Các dạng kiểm định an toàn thông tin

1. **Khái niệm kiểm định an toàn thông tin**
   - Kiểm định an toàn hệ thống thông tin là thực hiện các kiểm tra, đánh giá về vấn đề an toàn, an ninh thông tin nhằm xác định mức độ đảm bảo an toàn thông tin của tổ chức.
   - Là căn cứ khẳng định hệ thống đã đáp ứng được các điều kiện về an toàn.

2. **Các dạng kiểm định an toàn thông tin**

	Kiểm định an toàn thông tin toàn bộ	Kiểm định an toàn thông tin 1 phần
	Kiểm định toàn bộ các vấn đề về an toàn trong tổ chức	Kiểm định giới hạn trong một phần nhất định của tổ chức
Ưu điểm	- Tiếp cận toàn diện hệ thống. - Có một cái nhìn toàn diên về tình trạng an ninh thông tin của tổ chức	- Các kiểm tra diễn ra nghiêm ngặt hơn so với kiểm định toàn bộ
Nhược điểm	- Đòi hỏi nhiều thời gian - Việc kiểm tra có thể không được thực hiện một cách kỹ lưỡng.	- Chỉ có một số hạn chế các đối tượng được kiểm tra.

Câu 18: Quy trình kiểm định an toàn hệ thống thông tin

1. **Bước 1: chuẩn bị kiểm định**

- Thực hiện tại thời điểm bắt đầu kiểm định.
- Các công việc cần thực hiện:
    - Các bên liên quan thống nhất các điều khoản chung.
    - Ký kết các thỏa thuận liên quan.
    - Xác định đối tượng kiểm định, thời gian kiểm định, chuẩn bị hồ sơ tài liệu.
    - Tài liệu: tài liệu tổ chức, tài liệu kỹ thuật.

2. **Bước 2: tạo kế hoạch kiểm định**

- Chi tiết các công việc cần thực hiện trong toàn bộ quá trình kiểm định.
- Sử dụng trong suốt quá trình kiểm định.
- Thời gian thực hiện công việc:

Giai đoạn	Công việc	Thời gian
Bước 1	Chuẩn bị kiểm định	5%
Bước 2	Tạo kế hoạch kiểm định	15%
Bước 3	Xem xét tài liệu	20%
Bước 4	Kiểm thử trực tiếp	35%
Bước 5	Đánh giá kết quả	5%
Bước 6	Lập báo cáo kiểm định	20%

3. **Bước 3: xem xét tài liệu**

- Tiến hành kiểm tra, xem xét các tài liệu liên quan đến việc thực hiện an toàn hệ thống thông tin.
- Các công việc cần thực hiện:
    - Xác định các nguy hại có thể xảy đến.
    - Kiểm tra vấn đề áp dụng chính sách.
    - Kiểm tra các nguy cơ đã xảy đến trong thời gian gần.

4. **Bước 4: kiểm tra trực tiếp**

- Tiến hành kiểm tra tại mục tiêu.
- So sánh và kiểm tra lại các tài liệu được cung cấp với các điều kiện thực tế.
- Phương pháp kiểm tra:
    - Phỏng vấn.
    - Quan sát.
    - Phân tích các tập tin (bao gồm cả dữ liệu điện tử).
    - Kiểm tra kỹ thuật.
    - Phân tích dữ liệu.
    - Hỏi bằng văn bản.

5. **Bước 5: đánh giá kết quả**

- Được thực hiện bởi nhóm kiểm toán hoặc các cơ quan có thẩm quyền.
- Kết quả đánh giá là cơ sở chứng nhận tính an toàn của mục tiêu đánh giá và là điều kiện cấp chứng nhận đảm bảo an toàn thông tin.

6. **Bước 6: lập báo cáo kiểm định**

- Trình bày chi tiết các thông tin liên quan đến quá trình thực hiện kiểm định.

- Thông tin chung về tài nguyên kiểm định.
- Quy trình thực hiện kiểm định.
- Kết quả kiểm định.

Câu 19: Phương pháp luận đánh giá an toàn hệ thống thông tin

– Ý nghĩa của phương pháp luận:

+ Cung cấp tính thống nhất và có cấu trúc cho việc kiểm thử an toàn, từ đó có thể giảm thiểu rủi ro trong quá trình đánh giá.

+ Giúp dễ dàng trong việc chuyển giao quy trình đánh giá nếu có sự thay đổi nhân sự đánh giá.

+ Chỉ ra những hạn chế về tài nguyên kết hợp với các đánh giá an toàn.

+ Xây dựng phương pháp luận đánh giá an toàn thông tin theo các giai đoạn sẽ mang lại rất nhiều các ưu điểm và cung cấp một cấu trúc, điểm dừng tự nhiên cho quá trình chuyển đổi đánh giá viên

- Phương pháp luận chứa tối thiểu các pha:

+ Lập kế hoạch:

- Thực hiện các công việc chuẩn bị
- Thu thập các thông tin cần thiết phục vụ quá trình đánh giá

+ Thực thi:

- Xác định các lỗ hổng và xác nhận lỗ hổng

+ Hậu thực thi:

- Phân tích các lỗ hổng
- Đưa ra các khuyến cáo giảm nhẹ lỗ hổng
- Phát triển báo cáo

- Một số phương pháp luận được ứng dụng rộng rãi trong đánh giá an toàn hệ thống thông tin:

+ OSSTMM (Open Source Security Testing Methodology Manual): Phương pháp mở đánh giá an toàn thủ công

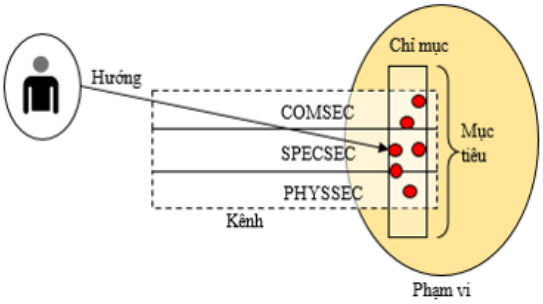
+ ISSAF(Information Systems Security Assessment Framework): Phương pháp đánh giá an toàn hệ thống thông tin

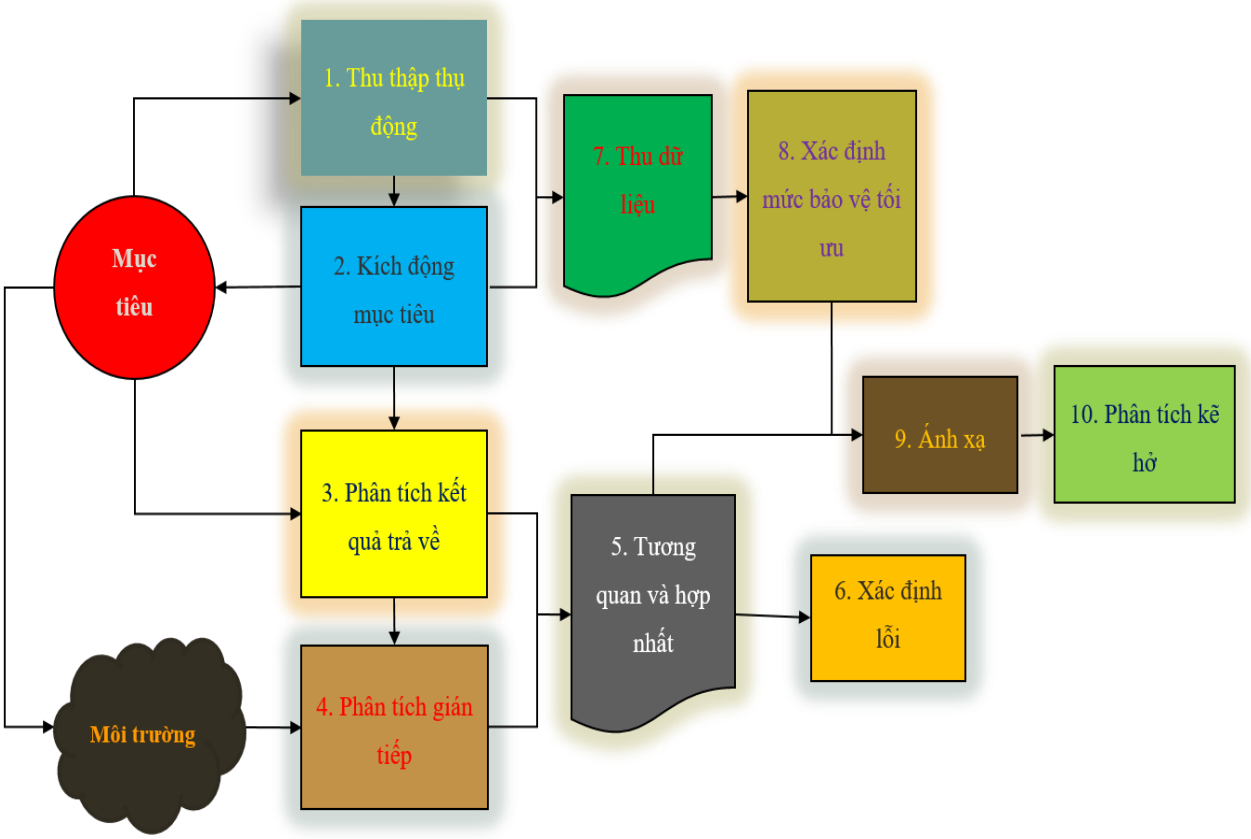
+ OWASP (The Open Web Application Security Project): Dự án mở về bảo mật ứng dụng web

Câu 20: Phương pháp luận OSSTMM

- Là một dự án của ISECOM, phát triển trong một cộng đồng mở
- Phương pháp khoa học mô tả chính xác các an ninh hoạt động đặc trưng thông qua kiểm thử một cách nhất quán và lặp đi lặp lại trên các kênh vật lý, tương tác con người, kết nối
- Phương pháp tiếp cận chia thành 4 nhóm chính:

+ Phạm vi
+ Kênh
+ Chỉ mục
+ Hướng





Bước 1: Thu thập dữ liệu thụ động ở trạng thái hoạt động bình thường để hiểu mục tiêu.

Bước 2: Kiểm thử tích cực những hoạt động bằng cách kích động những hoạt động vượt quá mức bình thường.

Bước 3: Phân tích dữ liệu nhận được trực tiếp từ các hoạt động đã kiểm thử.

Bước 4: Phân tích dữ liệu gián tiếp từ tài nguyên và người vận hành

Bước 5: Xem xét tương quan và hợp nhất thông tin thu được từ kết quả bước 3 và 4 để xác định các quy trình an ninh hoạt động.

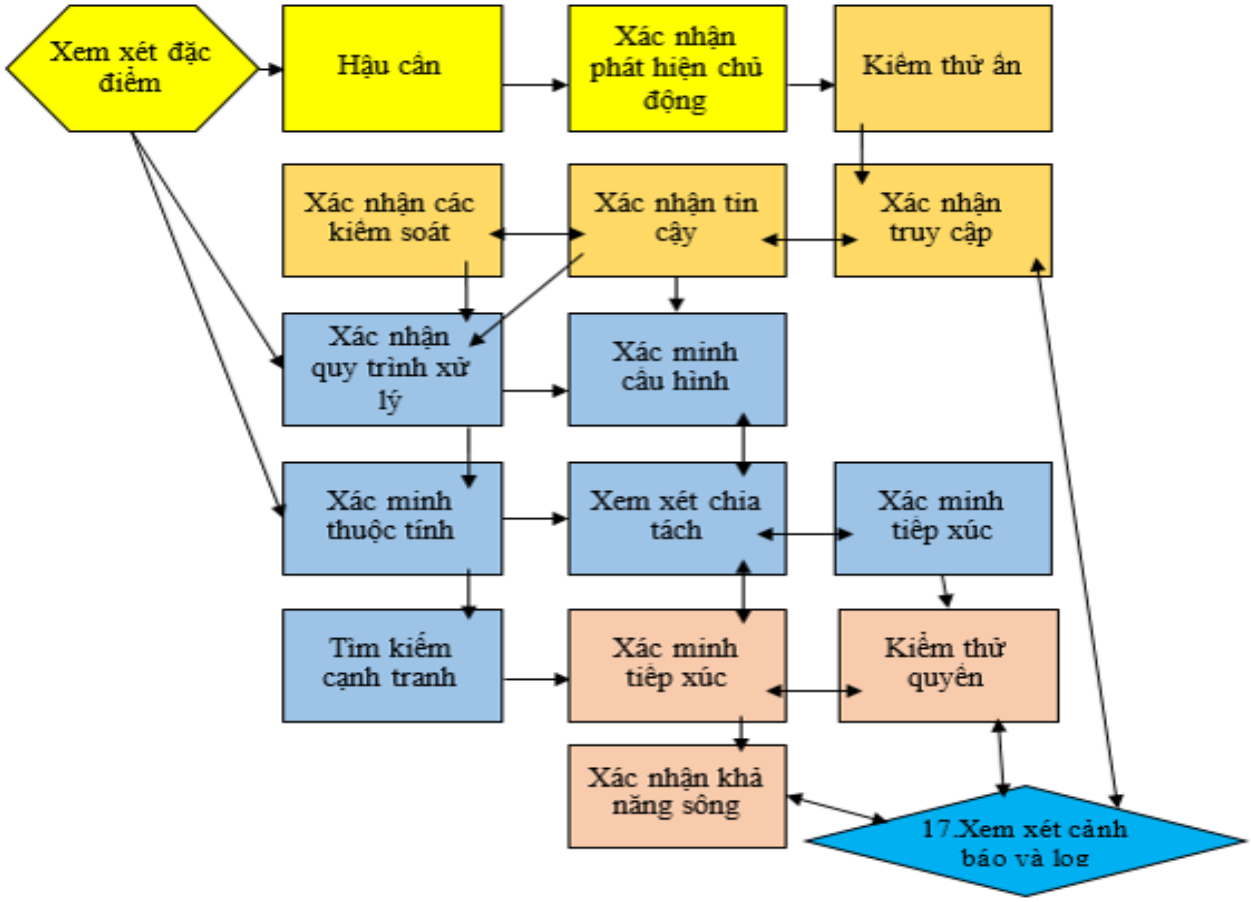
Bước 6: Xác định và hợp nhất các lỗi.

Bước 7: Thu thập số liệu từ các hoạt động cả bình thường và kích động.

Bước 8: Xem xét tương quan và hợp nhất thông tin giữa các bước 1 và 2 để xác định mức bảo vệ và kiểm soát tối ưu.

Bước 9: Ánh xạ trạng thái hoạt động tối ưu đến quy trình (bước 5).

Bước 10: Tạo một kẽ hở phân tích để xác định cái gì cần thiết nâng cao cho các quy trình và kiểm soát cần thiết cho bảo vệ và kiểm soát (bước 5) để đạt được trạng thái hoạt động tối ưu (bước 8) từ cái hiện hành.



Có tất cả 5 kênh, ứng với mỗi kênh sẽ lần lượt thực hiện 17 mô-đun, chia thành 4 giai đoạn: giai đoạn bắt đầu gồm 3 mô-đun đầu tiên, giai đoạn tương tác gồm các mô-đun từ 4 đến 7, giai đoạn điều tra gồm các mô-đun từ 8 đến 13 và giai đoạn can thiệp gồm các mô-đun còn lại – từ 14 đến 17. Như vậy, người kiểm thử phải thực hiện 17 * 5 = 85 phân tích trước khi đưa ra được báo cáo cuối cùng.

Câu 21: Phương pháp luận ISSAF

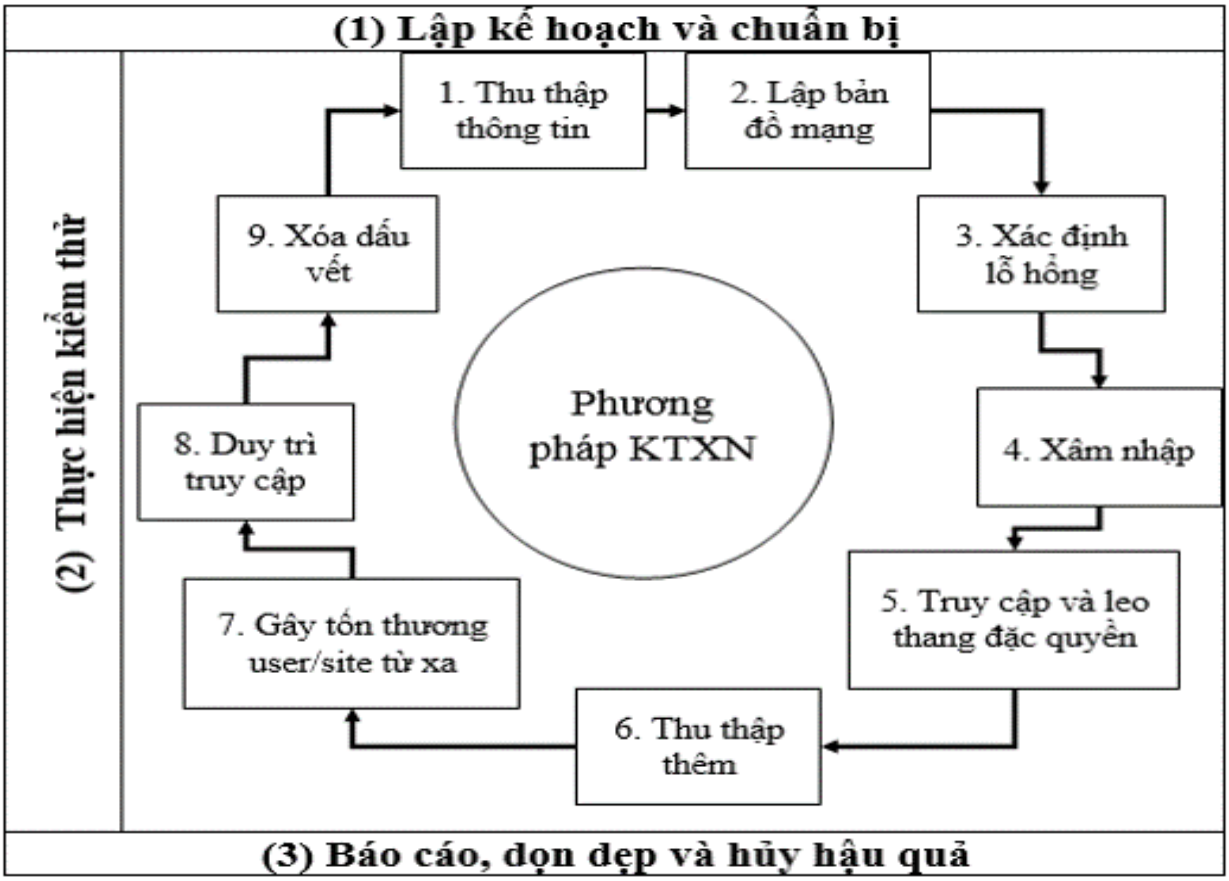
- Là phương pháp luận KTAN của tổ chức OISSG, ra đời năm 2003

- Là một khung làm việc KTAN nguồn mở, tập trung chính vào KTXN.

- Phát triển tập trung vào hai lĩnh vực của KTAN: quản lý và kỹ thuật.

  + Mặt quản lý thực hiện quản lý nhóm công việc và các kinh nghiệm thực tế tốt nhất phải được tuân thủ trong suốt quá trình kiểm thử

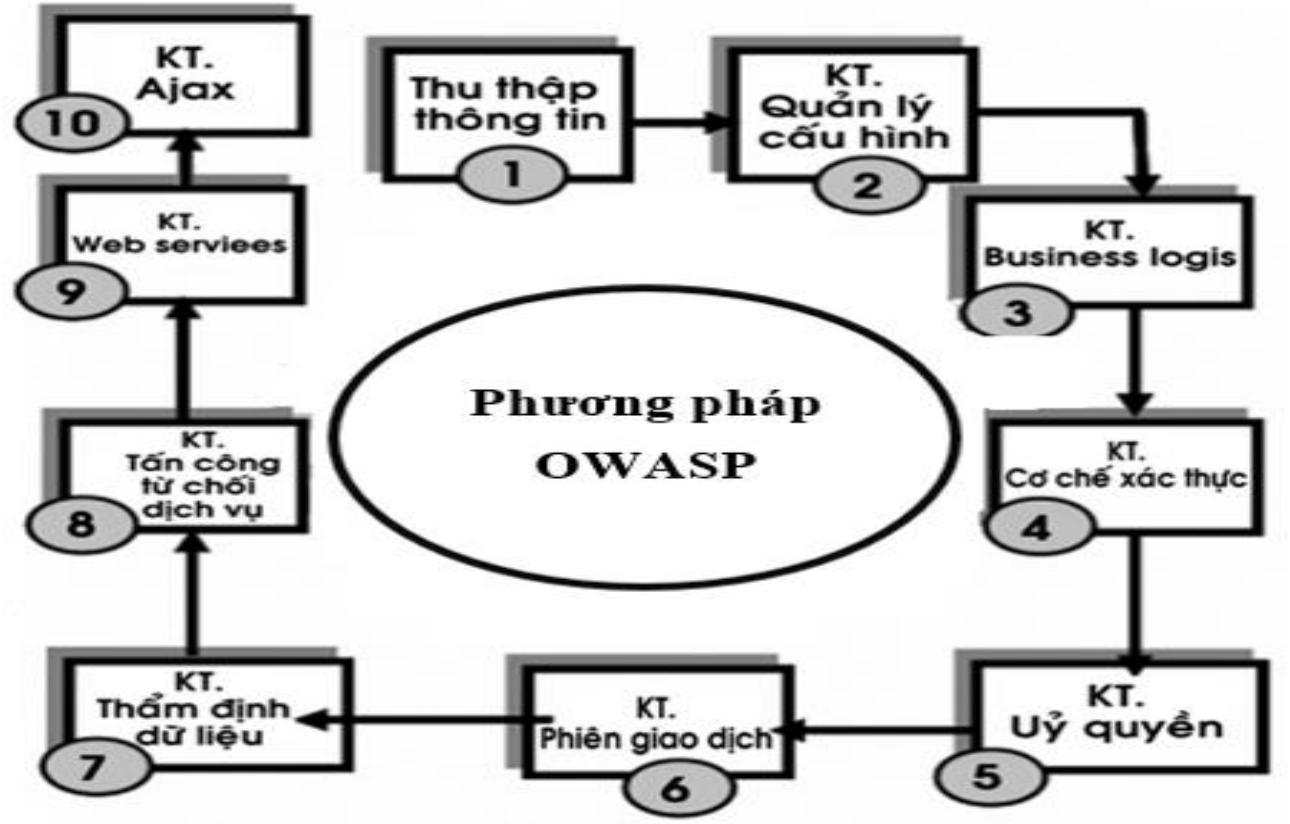
  + Mặt kỹ thuật thực hiện bộ quy tắc cốt lõi, thủ tục cần tuân thủ và tạo ra một quy trình đánh giá an ninh đầy đủ



Câu 22: Phương pháp luận OWASP

- Là dự án của tổ chức OWASP, là một tổ chức phi lợi nhuận, cộng đồng mở, mục tiêu chính là cải tiến an ninh các phần mềm ứng dụng, đặc biệt là ứng dụng web

- Theo OWASP, các ứng dụng web trên mạng hầu hết phải tiếp xúc với bên ngoài, nên nó sẽ là đối tượng đầu tiên chịu các cuộc tấn công phá hoại và sửa đổi trái phép



Câu 23:So sánh sự khác nhau giữa Kiểm định hệ thống an toàn thông tin và Đánh giá an toàn hệ thống thông tin?

Đánh giá ATHTTT là thước đo độ an toàn của hệ thống, là cách thức thực hiện an toàn thông tin. Việc đánh giá an toàn là đánh giá dựa trên việc xác định rủi ro, trong đó tập trung vào xác định các điểm yếu tác động trên hệ thống.

Mục đích của kiểm định ATHTTT là kiểm tra, đánh giá mức đọ an ninh thông tin trong 1 tổ chức nhằm xác định hệ thống công nghệ thông tin của tổ chức đó có đạt được các yêu cầu về an toàn theo các tiêu chí đã đề ra hay không

Kiểm định ATTT là 1 phương pháp xác định, đạt được và duy trì 1 mức độ thích hợp với yêu cầu bảo mật trong 1 tổ chức.