MỤC LỤC

[Câu 1: Phương pháp luận đánh giá an toàn hệ thống thông tin 2](#_Toc516695282)

[Câu 2: Các kỹ thuật đánh giá 6](#_Toc516695283)

[Câu 3: So sánh kiểm thử (testing) và kiểm tra (Examination), kiểm thử và kiểm tra 6](#_Toc516695284)

[Câu 4: Rà soát tài liệu 7](#_Toc516695285)

[Câu 6 : Dò quét mạng 9](#_Toc516695286)

[Câu 7: Khám phá mạng 10](#_Toc516695287)

[Câu 8: Dò quét mạng không dây 11](#_Toc516695288)

[Câu 9 : Bẻ mật khẩu 15](#_Toc516695289)

[Câu 10: Kiểm thử xâm nhập 15](#_Toc516695290)

[Câu 11: Kỹ nghệ xã hội 19](#_Toc516695291)

[Câu 12: Xử lý dữ liệu 19](#_Toc516695292)

[Câu 13: Các rủi ro mức cao, mức trung bình, mức thấp 21](#_Toc516695293)

[Câu 14: Khái niệm kiểm định an toàn hệ thống thông tin 23](#_Toc516695294)

[Câu 15: Các dạng kiểm định an toàn thông tin 23](#_Toc516695295)

[Câu 16: Các tiêu chuẩn kiểm định an toàn thông tin 24](#_Toc516695296)

[Câu 17: Quy trình kiểm định an toàn hệ thống thông tin 26](#_Toc516695297)

# Câu 1: 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 thấp 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

* 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

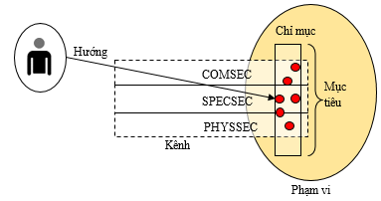
- Phương pháp tiếp cận chia thành 4 nhóm chính:

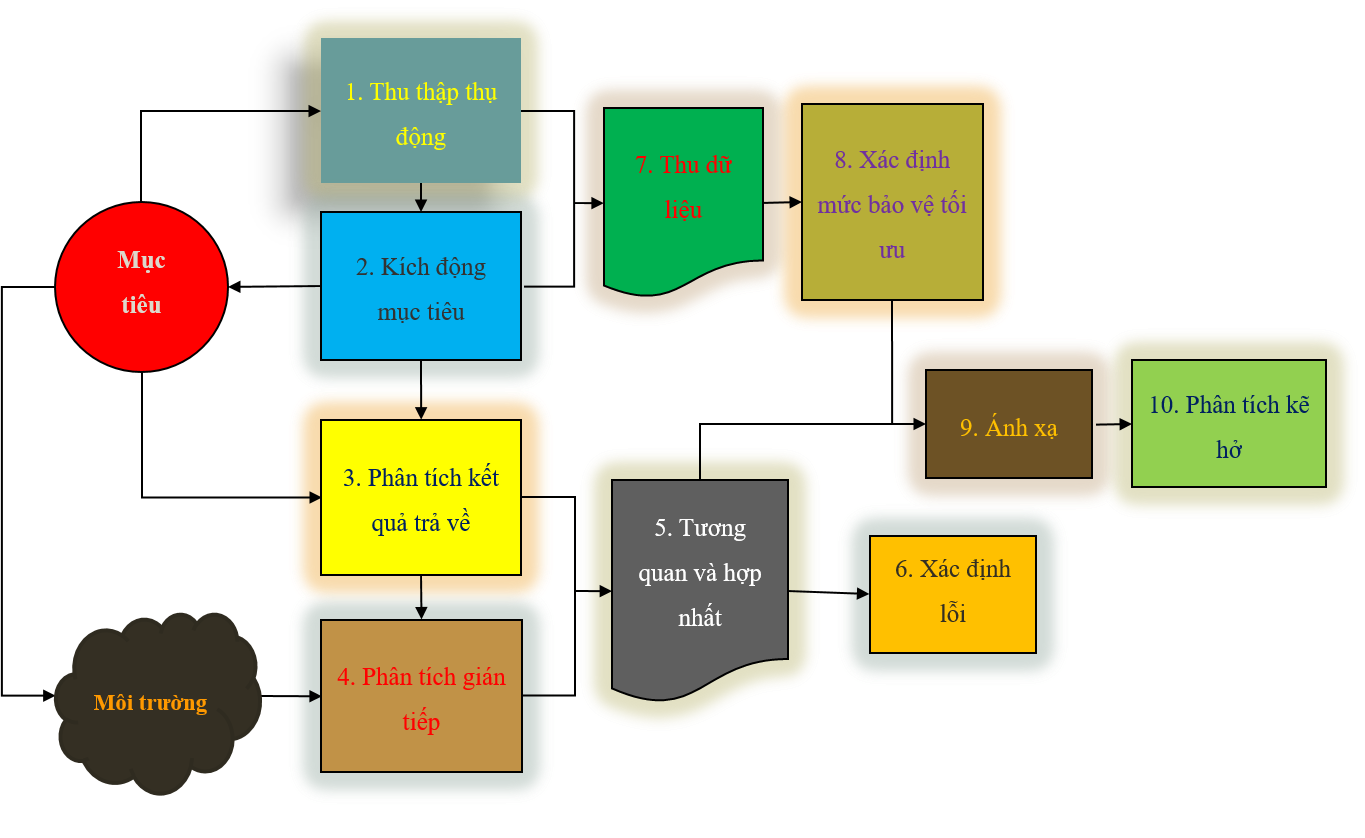
+ Phạm vi

+ 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.

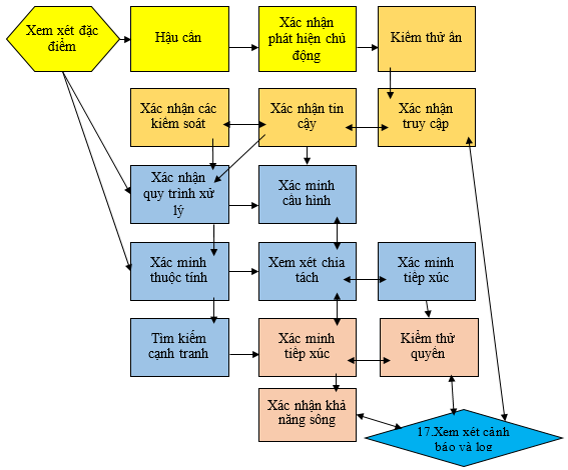
Bước 6: Xác định và hợp nhất các lỗi.

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

* ISSAF

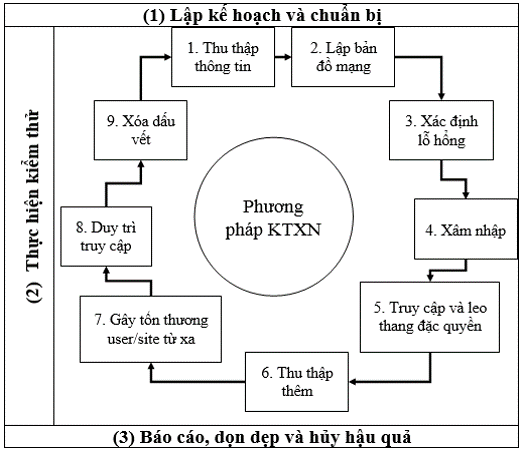
- Là phương pháp luận KTAN của tổ chức OISSG, ra đời năm 2003

- 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

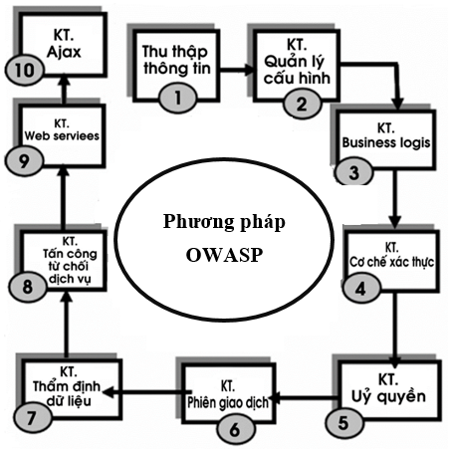
+ Mặt kỹ thuật thực hiện bộ quy tắc cốt lõi, thủ tục cần tuân thủ và tạo ra một quy trình đánh giá an ninh đầy đủ



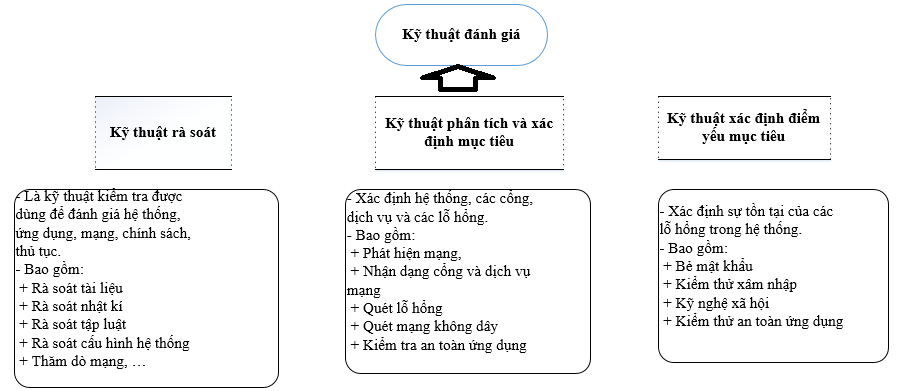
* OWASP

- 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 2: Các kỹ thuật đánh giá



# Câu 3: So sánh kiểm thử (testing) và kiểm tra (Examination), 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 hoặc 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 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 sự phối hợp của ban lãnh đạo và bộ phận quản trị mạng |

**So sánh kiểm thử và kiểm tra**

|  |  |
| --- | --- |
| Kiểm tra | Kiểm thử |
| - 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 | - 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 4: Rà soát tài liệu

- 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 tra 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 5: 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 cho 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 hóa hoặc gỡ bỏ.
  + Những mẫu cần thiết phải được kích hoạt, chỉnh sửa và bảo trì hợp lý.

# Câu 6 : Dò quét mạng

- Là kỹ thuật theo dõi thụ động những liên lạc trong mạng, giải mã các giao thức, kiểm tra các tiêu đề của gói tin và các thành phần thực thi để đánh dấu những thông tin liên quan

- Được sử dụng như một kỹ thuật rà soát

- Thực hiện việc dò quét mạng nhằm:

+ Chặn bắt và phát lại những liên lạc mạng.

+ Thực hiện việc khám phá mạng thụ động (ví dụ: xác định các thiết bị đang hoạt động trên mạng).

+ Xác định các hệ điều hành, ứng dụng, dịch vụ và các giao thức (ví du: telnet, fpt, …).

+ Xác định những hành vi trái phép hoặc không thích đáng (ví dụ: truyền tải thông tin nhạy cảm mà không được mã hóa).

+ Thu thập thông tin (ví dụ: những tài khoản và mật khẩu không được mã hóa).

- Dò quét mạng có thể gây ảnh hưởng tới hệ thống và mạng:

+ Băng thông mạng

+ Hiệu suất hoạt động của máy tính

- Công cụ sử dụng cho việc dò quét mạng gọi là sniffer.

- Để thực hiện dò quét:

+ Kết nối tới một thiết bị trong hệ thống mạng: hub hoặc switch với chức năng span port

- Có thể triển khai dò quét mạng tại nhiều địa điểm khác nhau

- Những địa điểm thường tiến hành dò quét là:

+ Tại vành đai, để đánh giá lưu lượng mạng vào ra.

+ Sau tường lửa, để đánh giá độ chính xác của các luật lọc lưu lượng.

+ Sau IDS/IPS, để xác định các mẫu có được kích hoạt và phản hồi hợp lý.

+ Trước hệ thống hoặc ứng dụng quan trọng, để đánh giá hoạt động của chúng.

+ Trong một phân đoạn mạng, để xác nhận giao thức đã được mã hóa.

- Hạn chế của dò quét mạng:

+ Khó để biết được nội dung các gói tin đã mã hóa

+ Thường chỉ có thể dò quét được khu vực mạng nơi mà các công cụ dò quét được triển khai

# Câu 7: Khám phá mạng

- Là việc phát hiện những máy chủ, máy trạm, thiết bị mạng đang hoạt động trong một mạng

- Phương pháp thực hiện:

+Thụ động

+ Chủ động

* Khám phá mạng thụ động

- 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 mạng

+ Tần suất liên lạc giữa các máy trong mạng

- Được thực hiện từ một máy tính trong mạng nội bộ

- Ưu điểm:

+ Không ảnh hưởng tới hoạt động của mạng

- Nhược điểm:

+ Tốn nhiều thời gian để thu thập thông tin

+ 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.

* Khám phá mạng chủ động

- Sử dụng công cụ tự động gửi trực tiếp các gói tin mong muốn (ví dụ: ICMP, TCP, 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

- Ví dụ: ping, telnet, …

- Sử dụng ping để khám phá mạng:

+ Gửi gói ICMP echo requests tới các địa chỉ IP trong phân vùng mạng

+ Nếu máy hoạt động thì sẽ trả về một ICMP echo reply

- Ưu điểm:

+ 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:

+ Có thể gây nhiễu hoặc trễ mạng

+ Có thể kịch 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 8: Dò quét mạng không dây

- Mạng không dây

+ Là mạng sử dụng công nghệ cho phép hai hay nhiều thiết bị kết nối với nhau thông qua sóng vô tuyến

+ Không cần kết nối vật lý hay chính xác là không cần sử dụng dây mạng

- Mạng không dây được chia thành 5 nhóm:

+ WPAN *(Wireless Personal Area Network)*

+ WLAN *(Wireless Local Area Network)*

+ WMAN *(Wireless Metropolian Area Network)*

+ WWAN *(Wireless Wide Area Network)*

+ WRAN *(Wireless Regional Area Network)*

* **WPAN**: Mạng vô tuyến cá nhân

- Bao gồm các công nghệ vô tuyến có vùng phủ nhỏ tầm vài mét đến hàng chục mét tối đa

- Phục vụ mục đích nối kết các thiết bị ngoại vi: máy in, bàn phím, chuột, đĩa cứng, khóa USB, đồng hồ,...với điện thoại di động, máy tính

- Ví dụ: Bluetooth

* **WLAN:** Mạng vô tuyến cục bộ

- Bao gồm các công nghệ có vùng phủ tầm vài trăm mét.

- Ví dụ: Wi-Fi

* **VMAN**: Mạng vô tuyến đô thị

- Vùng phủ sóng tầm vài km ( tối đa khoảng 4-5km)

- Ví dụ: WiMax

* **WWAN**: Mạng vô tuyến diện rộng

- Vùng phủ sóng tầm vài km đến chục km

- Ví dụ : UMTS/GSM/CDMA2000

* **WRAN**: Mạng vô tuyến khu vực

- Vùng phủ sóng lên đến tầm 40-100km

- Đại diện là công nghệ 802.22 đang được nghiên cứu và phát triển bởi IEEE

- Mục đích:

+ Mang công nghệ truyền thông đến các vùng xa xôi hẻo lánh

+ Khó triển khai các công nghệ khác

* Wifi ( Wireless Fidelity)

- Là hệ thống mạng không dây sử dụng sóng vô tuyến, giống như điện thoại di động, truyền hình và radio

- Cho phép truy cập Internet tại những khu vực có sóng

- **Chuẩn thông dụng của WiFi hiện nay**:

+ 802.11a

+ 802.11b

+ 802.11g

+ 802.11n

* 802.11:

- Là chuẩn không dây đầu tiên

- Sử dụng tần số 2,4GHz

- Dùng kỹ thuật trải phổ trực tiếp

- Hỗ trợ băng thông tối đa là 2Mbps

* 802.11b:

- Mở rộng từ chuẩn 802.11 (tháng 6/1999)

- Hỗ trợ tốc độ lên đến 11Mbps

- Sử dụng kỹ thuật điều chế khóa mã bù và dùng kỹ thuật trải phổ trực tiếp

- Ưu điểm:

+ Giá thấp

+ Tầm phủ sóng tốt

+ Không dễ bị che khuất

- Nhược điểm:

+ Tốc độ thấp

+ Có thể bị nhiễu bởi các thiết bị gia dụng

* 802.11a:

- Phát triển dựa trên chuẩn 802.11

- Sử dụng tần số 5GHz

- Tốc độ 54Mbps

- Tránh được can nhiễu từ các thiết bị dân dụng

- Sử dụng kỹ thuật trải phổ theo phương pháp đa phân chia tần số trực giao

- Ưu điểm:

+ Tốc độ nhanh

+ Tránh xuyên nhiễu bởi các thiết bị khác

- Nhược điểm:

+ Giá thành cao

+ Tầm phủ sóng ngắn

+ Dễ bị che khuất

* 802.11g:

- Phát triển dựa trên chuẩn 802.11a và 802.11b

- Hỗ trợ băng thông 54Mbps

- Sử dụng tần số 2,4GHz

- Tương thích với 802.11b

- Sử dụng kỹ thuật trải phổ theo phương pháp đa phân chia tần số trực giao

- Ưu điểm:

+ Tốc độ nhanh

+ Tầm phủ sóng tốt

+ Không dễ bị che khuất

- Nhược điểm:

+ Giá thành cao (cao hơn 802.11b)

+ Có thể bị nhiễu bởi các thiết bị gia dụng

* 802.11n:

- Phát triển nhằm để cải thiện tính năng của 802.11g

- Hỗ trợ hỗ trợ tốc độ lên đến 100Mbps

- Tầm phủ sóng tốt hơn các chuẩn Wi-Fi trước đó nhờ tăng cường độ tín hiệu

- Ưu điểm:

+ Tốc độ nhanh

+ Tầm phủ sóng tốt

+ Chống nhiễu từ các tác động của môi trường

- Nhược điểm:

+ Giá thành cao (cao hơn 802.11g)

+ Sử dụng nhiều luồng tín hiệu có thể gây nhiễu với các thiết bị 802.11b/g kế cận

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **802.11a** | **802.11b** | **802.11g** | **802.11n** |
| **Năm phê chuẩn** | Tháng 7/1999 | T7/1999 | T6/2003 | T9/2009 |
| **Tốc độ tối đa** | 54Mbps | 11Mbps | 54Mbps | 300Mbps hay cao hơn |
| **Điều chế** | OFDM | DSSS hay CCK | DSSS hay CCK hay OFDM | DSSS hay CCK hay OFDM |
| **Dải tần số trung tần (RF)** | 5GHZ | 2,4GHz | 2,4GHz | 2,4GHz hay 5GHz |
| **Spatial Stream** | 1 | 1 | 1 | 1.2,3 hay 4 |
| **Độ rộng băng thông** | 20MHz | 20MHz | 20MHz | 20MHz hay 40 MHz |

- **Các chuẩn bảo mật**:

+ WEP ( Wired Equiva WEP (Wired Equivalency Privacy)

+ WPA (WiFi Protected Access)

+ WPA 2 (WiFi Protected Access 2)

* WPA

- Điểm yếu của WPA

+ Không chống được tấn công từ chối dịch vụ

+ Thuật toán RC4 có thể dễ dàng bị bẻ vỡ bởi tấn công FMS và một số tấn công khác

* WPA 2

- Sử dụng thuật toán mã hóa AES kích thước 128, 192 hoặc 256 bit

- Cho độ an toàn bảo mật cao

- Có thể bị khai thác lợi dụng WPS

-Mục tiêu:

+ Xác định những điểm yếu để giảm thiểu những rủi ro công nghệ không dây gây ra

- Một số lưu ý khi đánh giá an toàn mạng không dây:

+ Vị trí các thiết bị được quét

+ Mức độ bảo mật của dữ liệu được truyền khi sử dụng công nghệ không dây.

+ Tần số kết nối và ngắt kết nối với môi trường

+ Hệ thống phát hiện và ngăn chặn xâm nhập không dây (WIDPS) có thể có những thông tin cần thiết cho quá trình kiểm tra.

- Cách thức thực hiện dò quét:

+ Theo kiểu bị động

+ Theo kiểu chủ động

- Sử dụng công cụ dò quét mạng không dây

* Dò quét mạng không dây bị động

- Sử dụng công cụ nghe ngóng các tín hiệu phát ra từ mạng không dây

+ Bắt những lưu lượng mạng không dây được truyền đi trong phạm vi ăng-ten

* Phát hiện SSID
* Loại thiết bị
  + - * Kênh phát song
      * Địa chỉ MAC
      * Cường độ tín hiệu
      * Số lượng gói tin truyền
* Dò quét mạng không dây chủ động:

- Gửi trực tiếp các gói tin tới hệ thống mạng không dây

* Kiểm tra SSID
* Kiểm tra cơ chế xác thực, mã hóa dữ liệu
* Kiểm tra quyền truy cập quản trị

- Tập trung vào việc nhận dạng và định vị các thiết bị giả mạo

- Kiểm tra khả năng giám sát của hệ thống IDS/IPS không dây

# Câu 9 : 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 loại bẻ mật khẩu:

+ Dictionary Attack: Một từ điển được đưa vào ứng dụng crack để xác định tài khoản

+ Brute Forcing Attacks: 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 điểm và tấn công brute force

+ Rule- based Attack: Được sử dụng khi đã có 1 số thông tin về mật khẩu

# Câu 10: Kiểm thử xâm nhập

- Kiểm thử xâm nhập

+ Là kiểm tra độ an toàn của hệ thống thông tin

+ Người đánh giá bắt chước các tấn công thực tế để phá vỡ các tính năng bảo mật của ứng dụng, hệ thống hoặc mạng

- Kiểm thử xâm 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 lạc 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

- Kiểm thử xâm nhập có thể được thực hiện công khai hoặc bí mật

+ Kiểm thử công khai (Kiểm thử hộp trắng):

* Được sự hỗ trợ của nhân viên công nghệ thông tin của tổ chức để cung cấp các thông tin liên quan tới hệ thống mạng kiểm thử:
* Bản đồ mạng
* Tài khoản và mật khẩu đăng nhập
* Các nguy cơ thường xảy đến đối với hệ thống
* Mã nguồn ứng dụng và một số vấn đề khác liên quan
* Ưu điểm:
* Cho phép đánh giá toàn bộ mạng hoặc tình hình an toàn hệ thống
* Có thể hạn chế một số ảnh hưởng có thể xảy ra từ kiểm thử
* Nhược điểm:
* Thời gian thực hiện lâu
* Tốn kém
* Đòi hỏi người kiểm thử phải có trình độ chuyên môn sâu

+ Kiểm thử bí mật ( Kiểm thử hộp đen)

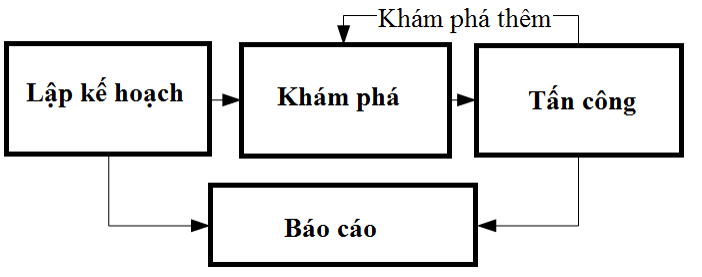
* Không cần có sự tham gia của nhân viên công nghệ thông tin của tổ chức nhưng được sự cho phép của quản lí cấp trên:
* Các thông tin có được:
* Tên công ty
* Mục tiêu đánh giá
* Địa chỉ thực hiện đánh giá
* Người kiểm thử đóng vai trò như 1 kẻ tấn công, thực hiện các bước kiểm thử để tìm ra các điểm yếu tồn tại trong hệ thống
* Ưu điểm:
* Hữu ích trong việc kiểm tra các biện pháp kiểm soát an toàn về mặt kĩ thuật, nhân viên công nghệ thông tin ứng phó với các sự cố an toàn nhận thấy được, tri thức của nhân viên và sự thực thi của chính sách an toàn của tổ chức
* Tính thực tế cao
* Nhược điểm:
* Không xác định được toàn bộ lỗ hổng trong hệ thống
* Mang lại nhiều rủi ro cho hệ thống mạng
* Các tấn công có thể bị hạn chế do tường lửa hoặc các hệ thống phòng thủ mạng

- Phương thức thực hiện:

+ Bên trong: thực hiện trong hệ thống mạng nội bộ

+ Bên ngoài: thực hiện từ mạng Internet

- Các pha kiểm thử:



* **Khám phá:**

- Thu thập thông tin:

+ Thông tin địa chỉ IP và tên máy chủTên nhân viên và thông tin liên hệ.

+ Thông tin hệ thống như tên và các chia sẻ

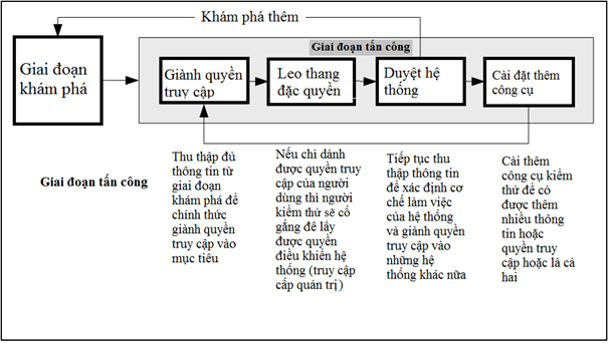
+ Thông tin dịch vụ và ứng dụng

- Xác định điểm yếu:

+Dò quét cổng và dịch vụ

+ Dò quét lỗ hổng

* Tấn công:



- Một số điểm yếu thường gặp:

+ Lỗi cấu hình (misconfiguration)

+ Các lỗ hổng nhân (kernel flaw)

+ Tràn bộ đệm (buffer overflow)

+ Thông qua đầu vào không đầy đủ (insufficient input validation)

+ Các liên kết tượng trưng (symbolic link)

+ Tấn công mô tả tệp tin (file descriptor attack).

+ Các điều kiện tranh đua (race conditions

+ Lỗi phân quyền thư mục và tệp tin (incorrect file and directory permissions)

# Câu 11: Kỹ nghệ xã hội

- Tấn công Kỹ nghệ xã hội:

+ 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:

+ Để 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 e-mail, 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 12: 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, và các lỗ hổng hệ thống

* Thu thập dữ liệu

- Thông tin liên quan đến kiến trúc, cấu hình của mạng được đánh 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.

* 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, và các thiết bị di động cũng phải có những biện pháp bảo vệ về mặt logic và vật lý tại nơi hoạt động

* Truyền dữ liệu

- Phương pháp truyền dữ liệu nhạy cảm bảo gồm việc mã hóa các tệp trên chứa dữ liệu nhạy cảm, mã hóa kênh thông tin tuân theo FIPS (VPN, SSL) và truyền các thông tin thông qua việc giao nhận các bản copy

* 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
* Thường 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 tấn công dựa 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 sạch:**

* 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 Erase (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,…

Các chú 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 vào 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 13: Các rủi ro mức cao, mức trung bình, mức thấp

- Rủi ro phát sinh từ:

+ Hệ điều hành

+ Webserver

+ CSDL

+ Ứng dụng

+ Thiết bị

+ Thu thập rò quét ban đầu

* **Rủi ro mức cao:**

- Ảnh hưởng nghiêm trọng tới hệ thống

- Cho phép chiếm quyền điều khiển hệ thống

- 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

**- Ví dụ về rủi ro mức cao**

+ Mức độ nguy hại: Cao

+ Công cụ: Firefox, Internet Explorer, …

+ Cách kiểm tra:

* Gõ một từ khóa bất kỳ, ví dụ "a" vào trang login email tại địa chỉ: <http://test.edu.vn/Email/web/default.asp>
* Xuất hiện thông báo lỗi tại URL của IE: <http://test.edu.vn/Email/web/default.asp?error_code=213&values=a@test.edu.vn||a||210.245.84.7||210.245.84.7||110||25||0&mode=standard_login>
* Thử thay ký tự "a" ở trên bằng 1 đoạn script: http://test.edu.vn/Email/web/default.asp?error\_code=213&values=>"''><script src="javascript:alert(document.cookie)">@test.edu.vn||>"''><script src="javascript:alert(document.cookie)">||210.245.123.12||210.245.123.12||110||25||0&mode=standard\_login
* Xuất hiện thông báo lỗi của Internet Explorer ASPSESSIONIDQCADAQBS=JCFBFJIAEMALMLKEEOAKCFLL

+ Kết quả: Trang Web bị lỗi Cross Site Scripting tại địa chỉ: http://test.edu.vn/email/web/default.asp

+ Mô tả + Rủi ro có thể gặp phải: Khi đã phát hiện được lỗi Cross Site Scripting, Hacker có thể thực thi một đoạn Script bằng cách liên kết đến một trang web nào đó, hoặc có thể xây dựng file script rồi cho URL trỏ đến file đó để thực thi file, hoặc đánh cắp account khi thực hiện tấn công hijacking, thay đổi các thiệt đặt của người sử dụng, đánh cắp cookie, …

+ Khuyến cáo: Để fix lỗi này thì khi GET data từ url phải lọc các ký tự như < hoặc > và các từ đặc biệt như script chẳng hạn

* **Rủi ro mức trung bình:**

- Ảnh hưởng tới hệ thống nhưng không trực tiếp

- Liên quan đến quyền sử dụng của người dùng bình thường, có thể thực hiện một số thao tác lên hệ thống nhưng không thể thực hiện các hành động của người quản trị

* **Rủi ro mức thấp:**

- Ảnh hưởng ở mức thấp

- Lộ thông tin, lộ tài khoản email, hoặc sử dụng các thư mục ẩn trong hệ thống

# Câu 14: Khái niệm kiểm định an toàn hệ thống 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.

- Kiểm định an toàn thông tin nhằm:

+ Nâng cao mức độ an toàn thông tin, tránh những sai sót trong thiết kế bảo mật thông tin

+ Tối ưu hóa hiệu quả của các biện pháp bảo vệ an ninh và các quy trình bảo mật

+ Tạo niềm tin đối với khách hàng, cũng như thể hiện sự tuân thủ các qui định trong việc đảm bảo an toàn thông tin của cơ quan tổ chức.

- Kết quả của một quá trình kiểm định an toàn thông tin:

+ Các báo cáo kiểm định

* Về tình hình an toàn thông tin hiện tại
* Các đề xuất nâng cao hiệu quả trong việc đảm bảo an toàn thông tin

+ Chứng nhận kiểm định (nếu đủ điều kiện)

# Câu 15: Các dạng kiểm định an toàn thông tin

- 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 an toàn thông tin toàn bộ:

- Kiểm tra toàn bộ các vấn đề về an toàn trong tổ chức

- Ưu điểm:

+ Tiếp cận toàn diện hệ thống

+ Có một cái nhìn toàn diện về tình trạng an ninh thông tin của tổ chức

- Nhược điểm:

+ Đòi hỏi nhiều thời gian

+ Việc kiểm tra có thể không được thực hiện một cách kỹ lưỡng

* Kiểm tra an toàn thông tin 1 phần:

- Kiểm định giới hạn trong một phần nhất định của tổ chức

- Ưu điểm:

+ Các kiểm tra diễn ra nghiêm ngặt hơn so với kiểm định toàn bộ

- Nhược điểm:

+ Chỉ có một số hạn chế các đối tượng được kiểm tra

# Câu 16: Các tiêu chuẩn kiểm định an toàn thông tin

- TCSEC

+ Ra đời tháng 8/1983

+ Đề cập đến nhiều vấn đề của an toàn máy tính (Trusted Network Interpretation)

+ Bảo vệ bằng mật mã

+ Đảm bảo tính bí mật và tính toàn vẹn của thông tin

+ Cách tiếp cận hệ thống đối với vấn đề truy cập và sự hình thành các nguyên lý cấu trúc hệ thống

- Các tiêu chí Liên bang đánh giá an toàn công nghệ thông tin (Mỹ)

+ Ra đời vào cuối những năm 80

+ Cốt lõi của là Hồ sơ bảo vệ (PP - Proctection Profile)

- Tiêu chí hài hòa của các nước châu Âu (Pháp, Anh, Đức, Hà Lan)

+ Công bố năm 1991

+ Tổ chức yêu cầu kiểm định và cấp chứng nhận cho sản phẩm CNTT cần tự xây dựng mục tiêu kiểm định, mô tả các mối đe dọa tiềm ẩn về ATTT và đề xuất các chức năng bảo vệ

+ Cơ quan cấp chứng nhận kiểm định mức độ đạt được mục tiêu thông qua các các chức năng đã đề ra

- Tiêu chí chung kiểm định an toàn công nghệ thông tin (CC - Common Criteria) (Canada, Mỹ, Anh, Đức, Hà Lan và Pháp)

+ Phát triển năm 1993

+ Kết hợp và phát triển ba tiêu chuẩn “Tiêu chuẩn hài hòa” của các nước Châu Âu”, “Tiêu chí kiểm định các hệ thống máy tính tin cậy” của Canada và “Tiêu chuẩn Liên bang an toàn công nghệ thông tin”.

+ Bao quát về nhiều khía cạnh của ATTT

- Tiêu chí chung (CC)

+ Các phương án:

* Phương án 1: 1996
* Phương án 2: 1998
* Phương án 2.1: 1999
* Ban hành trên cơ sở góp ý của nhóm công tác chuyên ngành thuộc tổ chức ISO
* Phương án 3.0: 2005
* Ra đời trên cơ sở xem xét lại nhiều nội dung của các phương án trước đó
* Phương án CC 3.1: 2006
* Bản chính thức của CC

+ Đối tượng đánh giá là sản phẩm và hệ thống thông tin (TOE - Target of Evaluation)

+ Môi trường an toàn

* Môi trường pháp lý
* Môi trường hành chính
* Môi trường vật lý
* Môi trường kỹ thuật

+ Mục tiêu an toàn (ST)

* Xây dựng trên cơ sở các giả thiết về an toàn
* Nhằm đảm bảo chống lại các mối đe dọa và thực hiện đầy đủ các chính sách về an toàn

+ Các mức đánh giá đảm bảo an toàn (7 mức):

* Mức 1 (EAL- 1): thấp nhất
* Áp dụng cho các mối đe dọa an toàn không được coi là nghiêm trọng và đạt được với chi phí tối thiểu thông qua việc phân tích các đặc tả chức năng, giao diện, tài liệu khai thác kết hợp với phép kiểm tra độc lập
* Mức 7 (EAL- 7): cao nhất
* Áp dụng cho những đối tượng đánh giá được sử dụng trong những trường hợp có rủi ro cao hoặc là những nơi mà giá trị của tài nguyên thông tin đòi hỏi chi phí lớn

- Tiêu chuẩn ISO

+ ISO 27002: Tiêu chuẩn hướng dẫn thực hiện an toàn hệ thống thông tin

* Giúp các cơ quan, tổ chức đưa ra mô hình cho hệ thống quản lý an toàn thông tin cùng với các quy tắc cần thiết phải áp dụng trong công tác đảm bảo an toàn cho hệ thống thông tin
* Là tài liệu biên soạn TCQG Việt Nam tương đương là TCVN 27002:2011

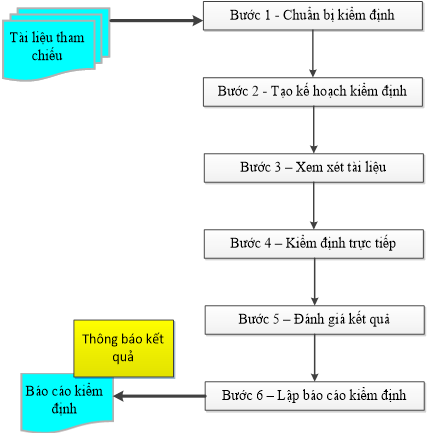
+ ISO 27001: Tiêu chuẩn chứng nhận

* Kiểm định lại vấn đề đảm bảo an toàn thông tin trong cơ quan, tổ chức

+ Tiêu chuẩn ISO 27001:2013

* Được biên soạn bởi ủy ban kỹ thuật chung về công nghệ thông tin - ISO/IEC JTC 1 thuộc tiểu ban các kỹ thuật an toàn thông tin - SC 27 thuộc tổ chức ISO
* Ban hành vào 01/10/2013, thay thế tiêu chuẩn ISO 27001:2005
* Thiết lập, triển khai, điều hành, giám sát, soán xét, bảo trì và nâng cấp hệ thống quản lý an toàn thông tin

# Câu 17: Quy trình kiểm định an toàn hệ thống thông tin



- 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

- 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 các 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 tra trực tiếp | 35% |
| Bước 5 | Đánh giá kết quả | 5% |
| Bước 6 | Lập báo cáo kiểm định | 20% |

- 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

- 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:

* Hỏi trực tiếp bằng lời (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

- 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

- 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