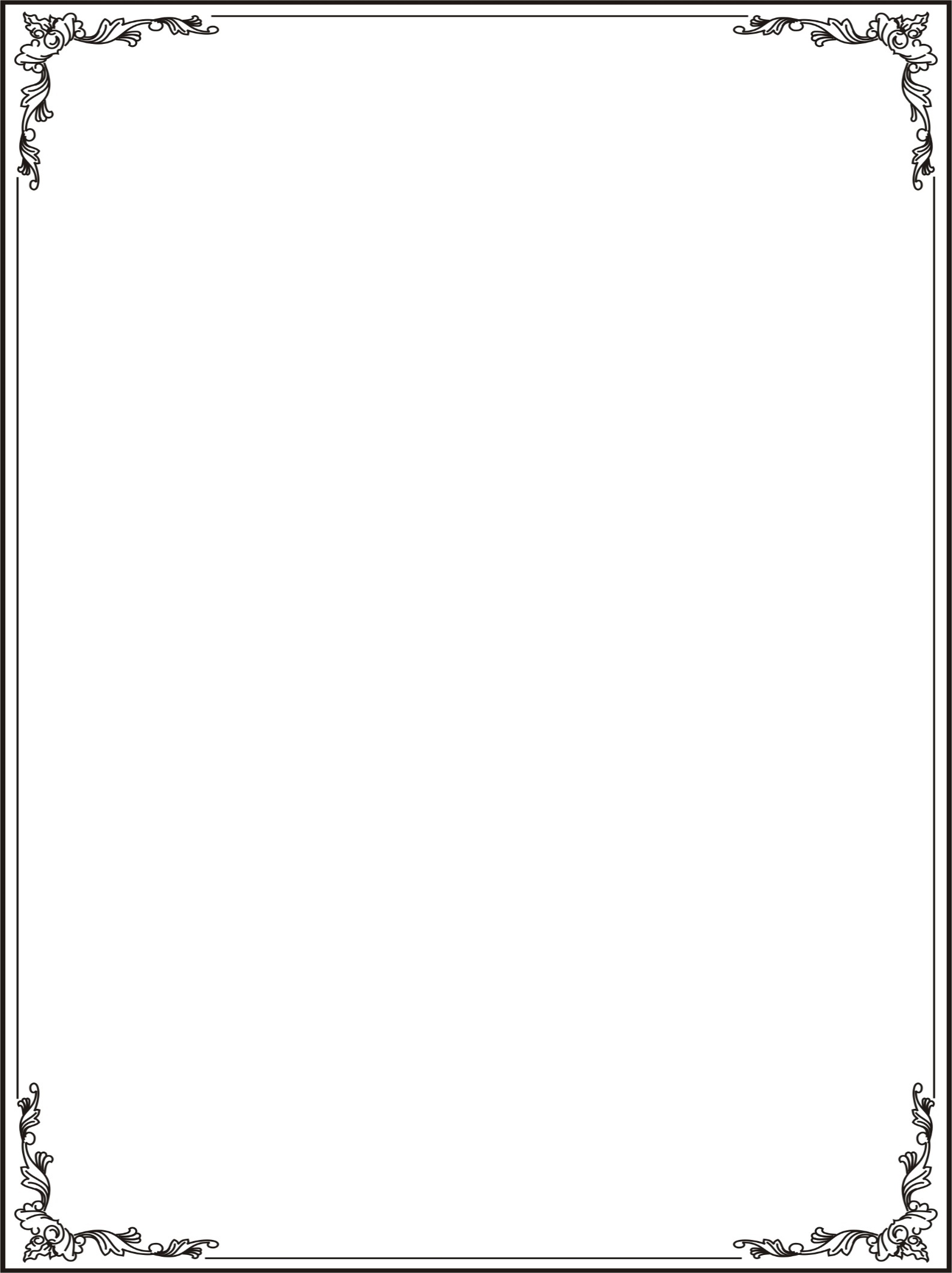
**

**HỌC VIỆN KỸ THUẬT MẬT MÃ**

**KHOA AN TOÀN THÔNG TIN**

---🙤🙤🕮🙤🙤---



**BÁO CÁO MÔN HỌC**

**QUẢN LÝ AN TOÀN THÔNG TIN**

**ĐỀ TÀI:**

**TÌM HIỂU PHƯƠNG PHÁP ĐÁNH GIÁ RỦI RO TRONG QUẢN LÝ AN TOÀN THÔNG TIN**

**TRÌNH BÀY CÁC CÔNG CỤ TỰ ĐỘNG ĐÁNH GIÁ RỦI RO**

***Nhóm sinh viên thực hiện:*** Vũ Tiến Đạt AT170609

Vũ Phú Hòa AT170121

Lê Sỹ Thành AT170547

Nhóm 10

Hà Nội, tháng 4 năm 2024

MỤC LỤC

[DANH MỤC HÌNH ẢNH 1](#_Toc163744250)

[DANH MỤC VIẾT TẮT 3](#_Toc163744251)

[LỜI MỞ ĐẦU 4](#_Toc163744252)

[CHƯƠNG 1. TỔNG QUAN VỀ ĐÁNH GIÁ RỦI RO TRONG LĨNH VỰC QUẢN LÝ AN TOÀN THÔNG TIN 5](#_Toc163744253)

[1.1 Khái niệm 5](#_Toc163744254)

[1.2 Tầm quan trọng 5](#_Toc163744255)

[1.3 Vai trò chính 5](#_Toc163744256)

[1.4 Các tiêu chuẩn tham chiếu 5](#_Toc163744257)

[CHƯƠNG 2. CÁC PHƯƠNG PHÁP ĐÁNH GIÁ VÀ CÔNG CỤ TỰ ĐỘNG ĐÁNH GIÁ RỦI RO 6](#_Toc163744258)

[2.1 Các phương pháp đánh giá rủi ro 6](#_Toc163744259)

[2.1.1 Phương pháp nhận diện rủi ro 6](#_Toc163744260)

[2.1.1.1 Khái niệm 6](#_Toc163744261)

[2.1.1.2 Nhận biết về tài sản 7](#_Toc163744262)

[2.1.1.3 Nhận biết về mối đe doạ 11](#_Toc163744263)

[2.1.1.4 Nhận biết về điểm yếu 11](#_Toc163744264)

[2.1.2 Phương pháp phân tích rủi ro 12](#_Toc163744265)

[2.1.3 Phương pháp ước lượng rủi ro 16](#_Toc163744266)

[2.2 Các công cụ tự động đánh giá rủi ro 18](#_Toc163744267)

[2.2.1 Qualys 18](#_Toc163744268)

[2.2.2 Nessus 19](#_Toc163744269)

[2.2.3 OpenVAS 21](#_Toc163744270)

[2.2.4 Rapid7 Nexpose 22](#_Toc163744271)

[CHƯƠNG 3. THỰC NGHIỆM 23](#_Toc163744272)

[3.1 Mục đích 23](#_Toc163744273)

[3.2 Mô hình 23](#_Toc163744274)

[3.3 Các kịch bản thực nghiệm 23](#_Toc163744275)

[KẾT LUẬN 33](#_Toc163744276)

[TÀI LIỆU THAM KHẢO 34](#_Toc163744277)

[PHỤ LỤC 35](#_Toc163744278)

# DANH MỤC HÌNH ẢNH

[Hình 2.1 Định lượng rủi ro 16](#_Toc163756307)

[Hình 2.2 Dashboard của Qualys 19](#_Toc163756308)

[Hình 2.3 Dashboard của Nessus 20](#_Toc163756309)

[Hình 2.4 Assets Dashboard của OpenVAS 22](#_Toc163756310)

[Hình 3.1 Mô hình thực nghiệm 23](#_Toc163756311)

[Hình 3.2 Tạo bản quét mới 24](#_Toc163756312)

[Hình 3.3 Thiết lập cài đặt 24](#_Toc163756313)

[Hình 3.4 Cài đặt tự động rò quét 25](#_Toc163756314)

[Hình 3.5 Chạy bản quét 25](#_Toc163756315)

[Hình 3.6 Kết quả sau khi hoàn thành quét 26](#_Toc163756316)

[Hình 3.7 Kết quả dò quét trên Windows Server 2012 26](#_Toc163756317)

[Hình 3.8 Các lỗ hổng của Microsoft Windows 27](#_Toc163756318)

[Hình 3.9 Lỗ hổng MS16-047 27](#_Toc163756319)

[Hình 3.10 Đánh giá về MS16-047 của Nessus 28](#_Toc163756320)

[Hình 3.11 Lỗ hổng MSB 28](#_Toc163756321)

[Hình 3.12 Đánh giá về lỗ hổng MSB 29](#_Toc163756322)

[Hình 3.13 Kết quả dò quét trên Windows 7 29](#_Toc163756323)

[Hình 3.14 Lỗ hổng của Windows 7 30](#_Toc163756324)

[Hình 3.15 Unsupported Windows OS 30](#_Toc163756325)

[Hình 3.16 Lỗ hổng MS17-010 31](#_Toc163756326)

[Hình 3.17 Thông tin thêm về lỗ hổng MS17-010 31](#_Toc163756327)

[Hình 3.18 Đánh giá về lỗ hổng MS17-010 32](#_Toc163756328)

# DANH MỤC VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| **Viết tắt** | **Viết đầy đủ** | **Nghĩa tiếng Việt** |
| ATTT | An toàn thông tin |  |
| TT | Thông tin |  |
| HT | Hệ thống |  |
| HTTT | Hệ thống thông tin |  |

# DANH MỤC BẢNG BIỂU

[Table 1 Thang điểm giá trị 9](#_Toc163756144)

[Table 2 Gán trọng số cho mỗi nhân tố 10](#_Toc163756145)

[Table 3 Bảng tiêu chí đánh giá hậu quả 14](#_Toc163756146)

[Table 4 Khả năng xảy ra sự cố 15](#_Toc163756147)

[Table 5 Năm mức rủi ro 16](#_Toc163756148)

[Table 6 Tiêu chí xác định mức rủi ro 17](#_Toc163756149)

[Table 7 Gán giá trị hoặc mức điểm rủi ro 18](#_Toc163756150)

[Table 8 Nhận biết về mối đe dọa 36](#_Toc163756151)

[Table 9 Nhận biết về điểm yếu 42](#_Toc163756152)

[Table 10 Xác định điểm yếu và mối đe dọa 43](#_Toc163756153)

# LỜI MỞ ĐẦU

**1. Tính cấp thiết của đề tài.**

Trong thời đại số hóa ngày nay, bảo vệ thông tin trở thành một ưu tiên hàng đầu đối với mọi tổ chức và doanh nghiệp. Việc quản lý an toàn thông tin không chỉ là một nhiệm vụ cần thiết mà còn là một thách thức không ngừng trong môi trường kinh doanh đầy biến động. Một phần quan trọng của quản lý an toàn thông tin là việc đánh giá rủi ro, giúp tổ chức nhận biết, đánh giá và quản lý các nguy cơ tiềm ẩn đối với thông tin.

Nội dung báo cáo gồm 3 chương với các nội dung sau:

***Chương 1: Tổng quan về đánh giá rủi ro trong quản lý an toàn thông tin.***

Nội dung chương 1 là đi tìm hiểu định nghĩa, vai trò và tầm quan trọng của việc đánh giá rủi ro.

***Chương 2: Các phương pháp và công cụ đánh giá rủi ro.***

Nội dung chương 2 là tìm hiểu các phương pháp trong đánh giá rủi ro và các công cụ đánh giá hiện nay.

***Chương 3: Thực nghiệm*.**

Chương cuối sẽ đi vào thực nghiệm để minh hoạ cách hoạt động của việc đánh giá rủi ro trong thực tiễn.

**2. Mục tiêu nghiên cứu của đề tài**

Tìm hiểu các phương pháp đánh giá rủi ro và các công cụ tự động đánh giá rủi ro trong quản lý an toàn thông tin**.**

**3. Đối tượng và phạm vi nghiên cứu**

Đối tượng: Cơ quan, tổ chức liên quan đến hoạt động đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin trong cơ quan, tổ chức nhà nước.

Phạm vi: Nghiên cứu đánh giá rủi ro an toàn thông tin, bao gồm các nội dung liên quan đến xác định mức rủi ro, quy trình đánh giá, các công cụ tự động

# TỔNG QUAN VỀ ĐÁNH GIÁ RỦI RO TRONG LĨNH VỰC QUẢN LÝ AN TOÀN THÔNG TIN

## Khái niệm

**Đánh giá rủi ro trong an toàn thông tin** là việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin, hệ thống thông tin.

## Tầm quan trọng

Rủi ro mà một tổ chức gặp phải xuất hiện ở bất cứ đâu, bất cứ phần nào trong hệ thống thông tin, từ việc nhỏ như vô tình lộ mật khẩu tài khoản công ty hay vô tình xoá mất dữ liệu.

Để hạn chế tối đa các tác động của rủi ro cần có một phương pháp đánh giá rủi ro trong HTTT một cách hiệu quả.

Người đứng đầu đơn vị tổ chức phải đảm bảo rằng tổ chức có mức hỗ trợ mong muốn khi đối mặt với các mối đe dọa trong thực tế.

## Vai trò chính

Xác định khả năng mà hệ thống có thể bị tấn công với từng mối đe doạ

Đánh giá tương đối các rủi ro có thể xảy tới với tài sản thông tin của hệ thống, từ đó có thể biết các tài sản nào cần tập trung kiểm soát và bảo vệ.

Tính toán rủi ro mà tài sản bị mất đối với các thiết lập hiện tại

Nhìn tổng thể các phần có thể bị tấn công để xác định lỗ hổng và cách kiểm soát các rủi ro với tài sản

Viết tài liệu và báo cáo về việc xác định và đánh giá rủi ro

## Các tiêu chuẩn tham chiếu

TCVN 10295:2014- Công nghệ thông tin – Các kỹ thuật an toàn – Quản lý rủi ro ATTT.

ISO/IEC 27005:2011, Informatinon Technology Security Techniques Informatinon Security Risk management system.

NIST SP 800-30r1, Guide for Conducting Risk Assessments.

ISO 31010:2019

# CÁC PHƯƠNG PHÁP ĐÁNH GIÁ VÀ CÔNG CỤ TỰ ĐỘNG ĐÁNH GIÁ RỦI RO

## Các phương pháp đánh giá rủi ro

### Phương pháp nhận diện rủi ro

#### Khái niệm

* Nhận diện rủi ro là quá trình tìm kiếm, thừa nhận và ghi lại các rủi ro.

Bao gồm:

* + **Nhận biết về tài sản:** để xác định danh mục các tài sản của tổ chức cần bảo vệ bao gồm TT, HTTT.
  + **Nhận biết về mối đe dọa:** để xác định các mối đe dọa đối với mỗi tài sản.
  + **Nhận biết về điểm yếu:** để xác định các điểm yếu có thể tồn tại đối với mỗi tài sản.

**Kết quả**: danh mục các mối đe dọa và điểm yếu đối với các tài sản được xác định.

* Phương pháp nhận diện rủi ro
  1. Thiết lập bảng kê
  2. Phân tích tài chính
  3. Phương pháp lưu đồ
  4. Phân tích công nghệ
  5. Kiểm tra hiện trường
  6. Tham khảo các chuyên gia khác trong tổ chức
  7. Phương pháp thông qua tư vấn
  8. Phương pháp phân tích hợp đồng
  9. Nghiên cứu các số liệu tổn thất trong quá khứ
  10. Nhận diện những mối nguy tiềm năng.

#### Nhận biết về tài sản

* Cần xác định và thu thập TT đầy đủ về tài sản đang được quản lý, đặc biệt là các TT liên quan đến đặc điểm, nơi lưu trữ, mức độ quan trọng và giá trị, đặc thù của tài sản.
* Các kỹ thuật thu thập thông tin về hệ thống:

**Bảng câu hỏi**: Để thu thập thông tin liên quan, nhân viên đánh giá rủi ro có thể phát triển một bảng câu hỏi liên quan đến quản lý và kiểm soát hoạt động được lập kế hoạch hoặc sử dụng cho hệ thống CNTT. Bảng câu hỏi này nên được phân phối cho các nhân viên quản lý kỹ thuật và kỹ thuật hiện hành đang thiết kế hoặc hỗ trợ hệ thống CNTT.

**Phỏng vấn tại chỗ**: Phỏng vấn với nhân viên quản lý và hỗ trợ hệ thống CNTT có thể cho phép nhân viên đánh giá rủi ro thu thập thông tin hữu ích về CNTT hệ thống (ví dụ: hệ thống được vận hành và quản lý như thế nào). Các chuyến thăm tại nơi cũng cho phép nhân viên đánh giá rủi ro quan sát và thu thập thông tin về tình trạng vật lý, môi trường và bảo mật hoạt động của hệ thống CNTT. Đối với các hệ thống vẫn đang trong giai đoạn thiết kế, chuyến thăm tại nơi sẽ là các bài tập thu thập dữ liệu trực tiếp và có thể tạo cơ hội để đánh giá môi trường vật lý mà hệ thống CNTT sẽ hoạt động.

**Xem xét tài liệu**: Tài liệu chính sách (ví dụ: tài liệu lập pháp, chỉ thị), tài liệu hệ thống (ví dụ: hướng dẫn sử dụng hệ thống, sổ tay quản trị hệ thống, tài liệu yêu cầu và thiết kế hệ thống, tài liệu mua lại) và tài liệu liên quan đến bảo mật (ví dụ: báo cáo đánh giá trước đây, báo cáo đánh giá rủi ro, kết quả kiểm tra hệ thống, kế hoạch bảo mật hệ thống, chính sách bảo mật) có thể cung cấp thông tin tốt về các biện pháp kiểm soát bảo mật được sử dụng và lập kế hoạch cho hệ thống CNTT. Phân tích các tác động nhiệm vụ của tổ chức hoặc đánh giá mức độ nghiêm trọng của nguồn cung cấp thông tin liên quan đến độ nhạy và độ nhạy của hệ thống và dữ liệu.

**Sử dụng Công cụ quét tự động**: Các phương pháp kỹ thuật chủ động có thể được sử dụng để thu thập thông tin hệ thống một cách hiệu quả. Ví dụ: một công cụ lập bản đồ mạng có thể xác định các dịch vụ chạy trên một nhóm lớn các máy chủ và cung cấp một cách nhanh chóng để xây dựng các cấu hình riêng lẻ của hệ thống CNTT.

* Chú ý:
  + Coi TT là đơn vị tài sản thành phần của HTTT.
  + HT có nhiều loại TT khác nhau, các TT có cùng mức độ quan trọng, có thể tồn tại những điểm yếu và mối đe dọa giống nhau thì có thể đưa vào thành một nhóm để thực hiện đánh giá và quản lý rủi ro.
  + Một HTTT lớn có thể được chia thành nhiều HTTT thành phần tương đối độc lập nhau về chức năng, mục đích sử dụng. Việc áp dụng biện pháp đánh giá và quản lý rủi ro được áp dụng cho từng HT thành phần theo mức rủi ro xác định được.
  + TT bao gồm : TT công khai, TT riêng, TT cá nhân và TT bí mật nhà nước. TT bí mật nhà nước được chia làm 03 mức: Mật, Tối Mật và Tuyệt Mật. Để xác định đầy đủ các tài sản TT có trong HT, ta có thể xác định các loại thông tin có cùng loại ở trên. Ví dụ TT công khai: TT lịch họp, TT thông cáo báo trí…; TT riêng: TT về quy trình nghiệp vụ…
  + HTTT bao gồm: HTTT phục vụ hoạt động nội bộ của cơ quan, tổ chức; HTTT phục vụ người dân, doanh nghiệp; HT cơ sở hạ tầng TT; HTTT Điều khiển công nghiệp.
* Tạo bảng đánh giá với các câu hỏi dựa trên các tiêu chí xác định
  + Các tiêu chí:
    - Tài sản nào đóng vai trò then chốt nhất đối với việc thành công của tổ chức?
    - Tài sản nào tạo ra thu nhập lớn nhất?
    - Tài sản nào tạo ra lợi nhuận lớn nhất?
    - Tài sản nào đắt nhất nếu phải thay thế?
    - Tài sản nào tốn kém chi phí bảo vệ nhất?
    - Tài sản nào sẽ làm tổ chức gặp rắc rối nhất nếu bị lộ?
* Có thể thêm các tiêu chí sau:
  + Giá trị còn lại sau khi tạo ra tài sản
  + Giá trị còn lại sau khi đã duy trì tài sản
  + Giá trị ứng với chi phí thay thế tài sản
  + Giá trị từ việc cung cấp thông tin của tài sản
  + Giá trị ứng với chi phí cho việc bảo vệ tài sản
  + Giá trị của tài sản đối với những người sở hữu
  + Giá trị của tài sản đối với việc sở hữu trí tuệ
  + Giá trị của tài sản đối với những kẻ tấn công
* **Ví dụ xác định giá trị tài sản bằng phương pháp 1**

Cần phân tích kĩ lưỡng → Thiết lập thứ tự sắp xếp mức độ quan trọng của các tài sản → hỗ trợ đưa ra chiến lược bảo vệ chính xác

Giá trị của tài sản sẽ được chia làm 05 mức theo thang điểm được tính từ tích của các giá trị C, I, A như ví dụ dưới đây:



Table 1 Thang điểm giá trị

- Đối với thuộc tính bí mật (C) thì giá trị được xác định vào loại thông tin hoặc loại thông tin hệ thống đó xử lý. Ví dụ: thông tin công khai thang điểm 1; thông tin riêng, thông tin cá nhân thang điểm 2; thông tin Mật thang điểm 3; thông tin Tối Mật thang điểm 4; thông tin Tuyệt Mật thang điểm 5.

- Đối với thuộc tính nguyên vẹn (I) thì giá trị được xác định vào yêu cầu đối với mức độ nguyên vẹn của thông tin hoặc loại thông tin mà hệ thống đó xử lý. Ví dụ: tính nguyên vẹn thấp thang điểm 1; tính nguyên vẹn trung bình thang điểm 2; tính nguyên vẹn cao thang điểm 3; tính nguyên vẹn rất cao điểm 4; tính nguyên vẹn tuyệt đối thang điểm 5.

- Đối với thuộc tính sẵn sàng (A) thì giá trị được xác định vào yêu cầu đối với mức sẵn sàng của thông tin hoặc hệ thống thông tin đó. Ví dụ: tính sẵn sàng thấp thang điểm 1; tính tính sẵn sàng trung bình thang điểm 2; tính tính sẵn sàng cao thang điểm 3; tính tính sẵn sàng rất cao điểm 4; tính tính sẵn sàng tuyệt đối thang điểm 5.

Theo đó, giá trị tài sản sẽ được xác định theo giá trị của các thuộc tính C, A, I như sau:

Căn cứ vào giá trị tài sản, ta có thể xác định loại tài sản nào là quan trọng cần ưu tiên bảo vệ. Căn cứ vào mỗi thuộc tính C, A, I của tài sản ta có thể xác định được những điểm yếu, mối đe dọa làm cơ sở để xác định hậu quả, mức ảnh hưởng tới cơ quan, tổ chức khi xảy ra rủi ro đối với tài sản đó.

* **Ví dụ xác định giá trị của tài sản bằng phương pháp 2**
* Sử dụng phương pháp phân tích nhân tố có trọng số
  + Nhân tố chính là tiêu chí đánh giá của tổ chức
  + Trọng số là thang điểm do tổ chức quy định
* Mỗi nhân tố được gán một trọng số trên tổng trọng số cho trước
  + Ví dụ: tổng trọng số là 100, từng nhân tố được gán trọng số từ 1–100 để tổng luôn là 100
* Ứng với mỗi nhân tố, gán một điểm số cho tài sản
  + Ví dụ: theo tài liệu NIST SP800-30 của Mỹ: 0.1 – 1.0

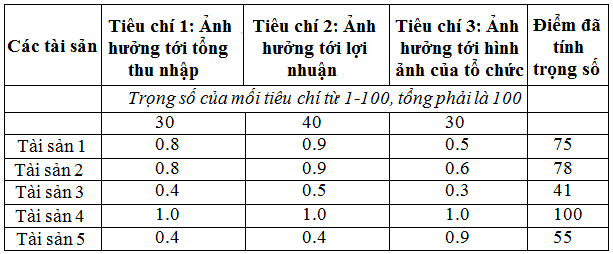


Table 2 Gán trọng số cho mỗi nhân tố

#### Nhận biết về mối đe doạ

* Mối đe dọa có thể được xác định dựa vào các điểm yếu của TT, HTTT nên xác định các mối đe dọa có thể dựa vào việc phân nhóm các điểm yếu.
* Thiết lập bảng đánh giá với một số câu hỏi cơ bản như:
  + Mối đe dọa nào nguy hiểm với tài sản của tổ chức trong môi trường hoạt động đã biết?
  + Mối đe dọa nào gây nguy hiểm nhất đối với thông tin của tổ chức?
  + Nếu tấn công xảy ra thì phải mất chi phí bao nhiêu để phục hồi?
  + Mối đe dọa nào yêu cầu chi phí phòng tránh lớn nhất?
* Mối đe dọa có thể được phân, nhưng không giới hạn các nhóm như sau:

1. Nhóm các mối đe dọa từ việc tồn tại điểm yếu, lỗ hổng trong HT

2. Nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp quản lý

3. Nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp kỹ thuật.

#### Nhận biết về điểm yếu

* Các điểm yếu có thể có nhiều tiêu chí xác định và được phân làm các nhóm khác nhau.
* Xem xét lại đối với mỗi mối đe dọa có thể ảnh hưởng tới tài sản → Lập danh sách các điểm yếu
  + - Đôi khi mang tính chủ quan, phụ thuộc nhiều vào kinh nghiệm và kiến thức của người thực hiện

Nên được thực hiện bởi một nhóm hiểu thực sự về tổ chức.

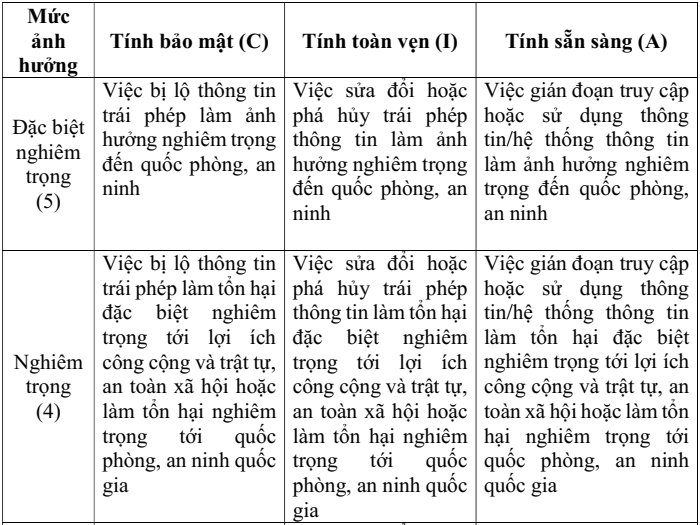
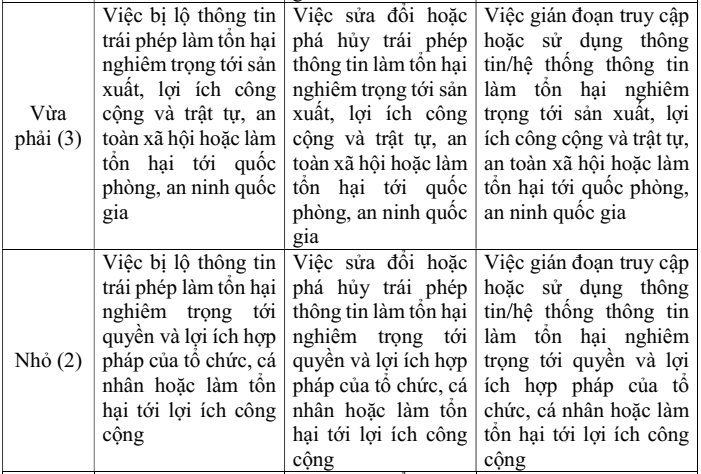
* Các điểm yếu có thể được phân thành các nhóm sau:
  + Nhóm các điểm yếu liên quan đến tồn tại lỗ hổng, điểm yếu ATTT trong HT
  + Nhóm các điểm yếu liên quan đến thiếu hoặc không đáp ứng các biện pháp quản lý: không có quy định về sử dụng mật khẩu an toàn, không có quy định về lưu trữ có mã hóa, không có quy định về quy trình xử lý sự cố .v.v.
  + Nhóm các điểm yếu liên quan đến thiếu hoặc không đáp ứng các biện pháp kỹ thuật: không có biện pháp phòng chống xâm nhập, không có biện pháp phòng chống mã độc, không có biện pháp phòng chống tấn công .v.v.

### Phương pháp phân tích rủi ro

* Phân tích rủi ro là tạo dựng hiểu biết về rủi ro.
* Gồm:
  + **Đánh giá các hậu quả** để xác định mức ảnh hưởng đối với cơ quan, tổ chức khi tài sản bị khai thác điểm yếu gây ra các mối nguy.
  + **Đánh giá khả năng** xảy ra đối với từng loại sự cố.

**Kết quả**: xác định được các hậu quả, mức ảnh hưởng mà cơ quan, tổ chức phải xử lý

* Các phương pháp:
  + Định tính: xác định hệ quả, xác suất và mức rủi ro bằng các mức như “cao”, “trung bình” và “thấp”, có thể kết hợp hệ quả và xác suất, và đánh giá mức rủi ro theo các tiêu chí định tính
  + Bán định lượng: sử dụng thang chia bằng số đối với hệ quả và xác suất kết hợp chúng để đưa ra một mức rủi ro bằng cách sử dụng công thức. Thang đo có thể là tuyến tính hoặc theo logarit, hay có mối quan hệ khác nào đó, công thức được sử dụng cũng có thể khác nhau.
  + Định lượng: ước tính giá trị thực tế đối với hệ quả và xác suất của chúng, và đưa ra giá trị về mức rủi ro theo các đơn vị cụ thể được xác định khi xây dựng bối cảnh.
* Mức độ chi tiết cần thiết phụ thuộc vào ứng dụng cụ thể, sự sẵn có của dữ liệu đáng tin cậy và các nhu cầu ra quyết định của tổ chức. Một số phương pháp và mức độ chi tiết của phân tích có thể do luật pháp quy định.
* Tiêu chí đánh giá hậu quả:



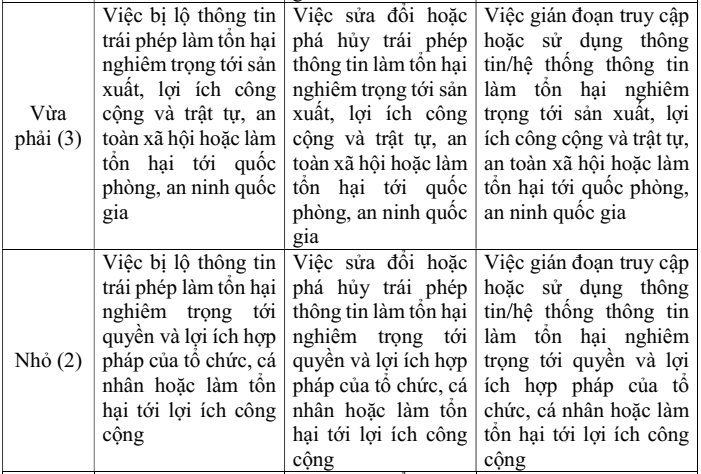
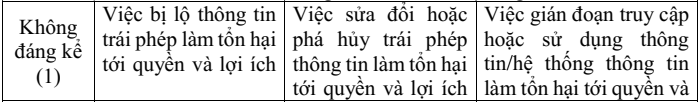
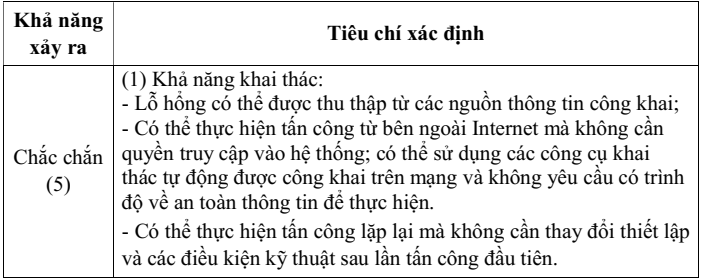
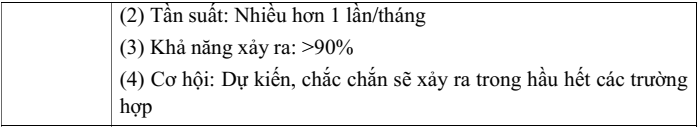
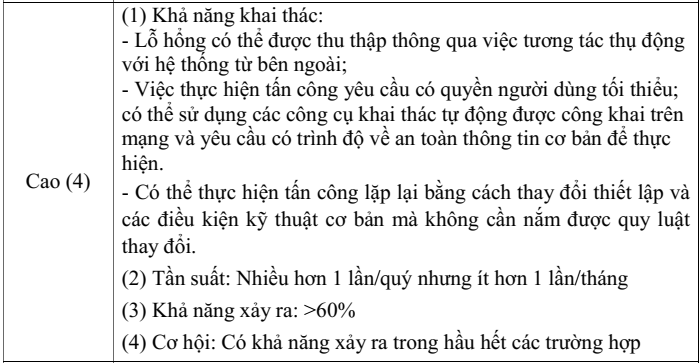
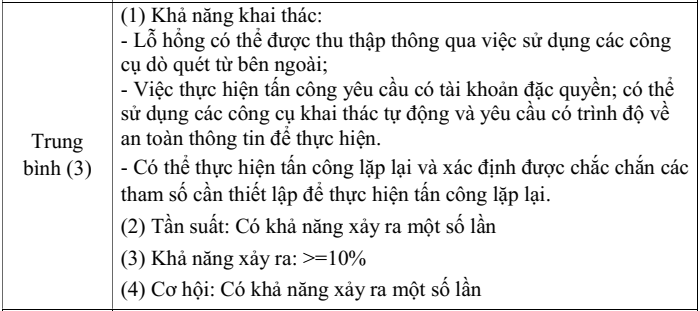




Table 3 Bảng tiêu chí đánh giá hậu quả

* Khả năng xảy ra sự cố:





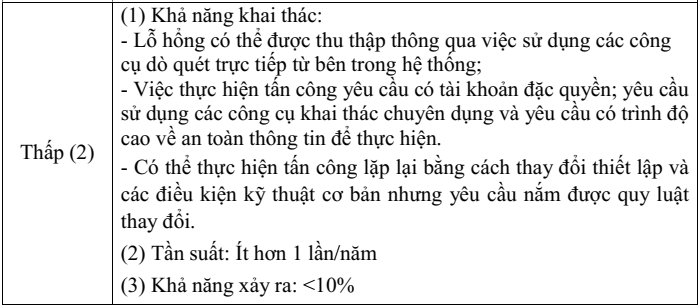




Table 4 Khả năng xảy ra sự cố

### Phương pháp ước lượng rủi ro

* Ước lượng rủi ro là quá trình đánh giá rủi ro như những đe dọa và

cơ hội tiềm năng.



Hình 2.1 Định lượng rủi ro

* Rủi ro được tính giá trị bằng công thức: **Mức rủi ro = f(hệ quả rủi ro, khả năng xảy ra)**
* Rủi ro được xếp hạng ưu tiên từ cao đến thấp theo các giá trị  
  mức rủi ro tính toán được
* Tùy theo tổ chức và đặc thù từng quá trình/dự án, chủ quá trình/trưởng dự án sẽ xác định những rủi ro nào cần đưa vào kiểm soát theo mức ưu tiên.
* **Ví dụ ước lượng rủi ro theo phương pháp 1**

Chia rủi ro chia thành 05 mức:

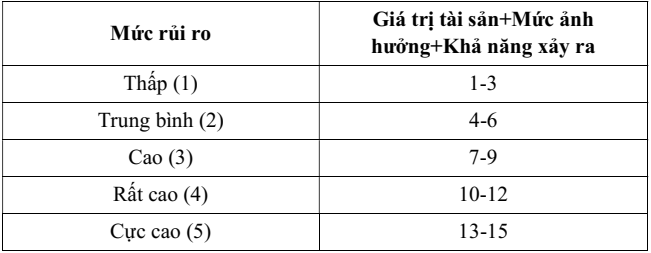


Table 5 Năm mức rủi ro

Việc xác định khả năng xảy ra sự cố cần dựa Giá trị tái sản, Mức ảnh hưởng, Khả năng xảy ra. Trên cơ sở đó, Mức rủi ro đối với danh sách tài sản được xác định như Bảng dưới đây:

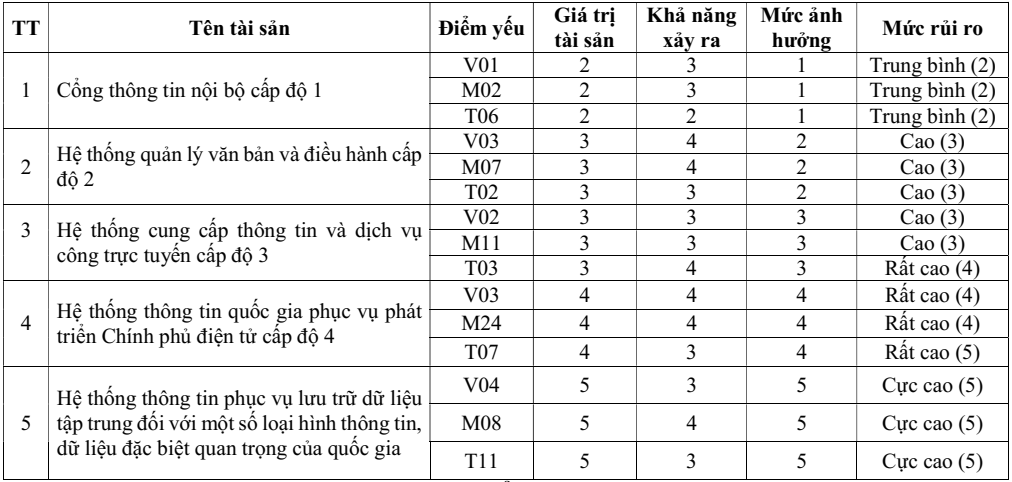


Table 6 Tiêu chí xác định mức rủi ro

* **Ví dụ ước lượng rủi ro theo phương pháp 2**

- Gán tỉ lệ hoặc mức điểm số rủi ro cho mỗi tài sản

- Công thức tính rủi ro:

* + **RR= V x P –R + U**:
    - RR: rủi ro
    - P: khả năng xuất hiện một điểm yếu
    - V: giá trị của tài sản
    - R: mức độ rủi ro được giảm thiểu do có các kiểm soát an toàn
    - U: mức độ rủi do do sự không chắc chắn của các tri thức hiện tại về điểm yếu

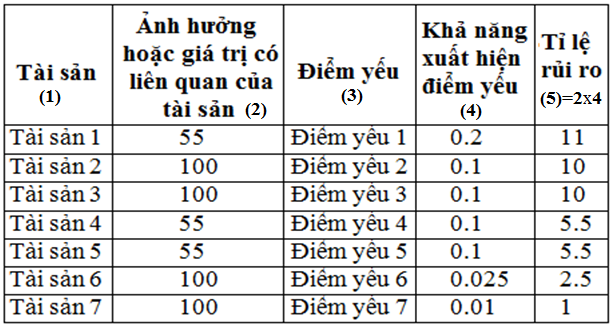


Table 7 Gán giá trị hoặc mức điểm rủi ro

- Tài sản A có giá trị là 50 và có 01 điểm yếu (điểm yếu 1). Điểm yếu 1 có khả năng xuất hiện là 1.0 và hiện tại không có sự kiểm soát nào.

- Các giả thiết và dữ liệu có độ chính xác là 90%.

## Các công cụ tự động đánh giá rủi ro

### Qualys

a) Khái niệm

Qualys là một nền tảng bảo mật thông tin chuyên nghiệp, cung cấp nhiều chức năng hữu ích.

b) Chức năng

**-Vulnerability Management (Quản lý lỗ hổng):**

**+Quét lỗ hổng**: Qualys cho phép quét các lỗ hổng trên hệ thống và ứng dụng web để xác định các điểm yếu.

**+Báo cáo và phân tích**: Tạo báo cáo chi tiết về lỗ hổng và phân tích dữ liệu để đưa ra quyết định bảo mật.

+**Quản lý lỗ hổng**: Hỗ trợ việc triển khai các biện pháp khắc phục lỗ hổng.

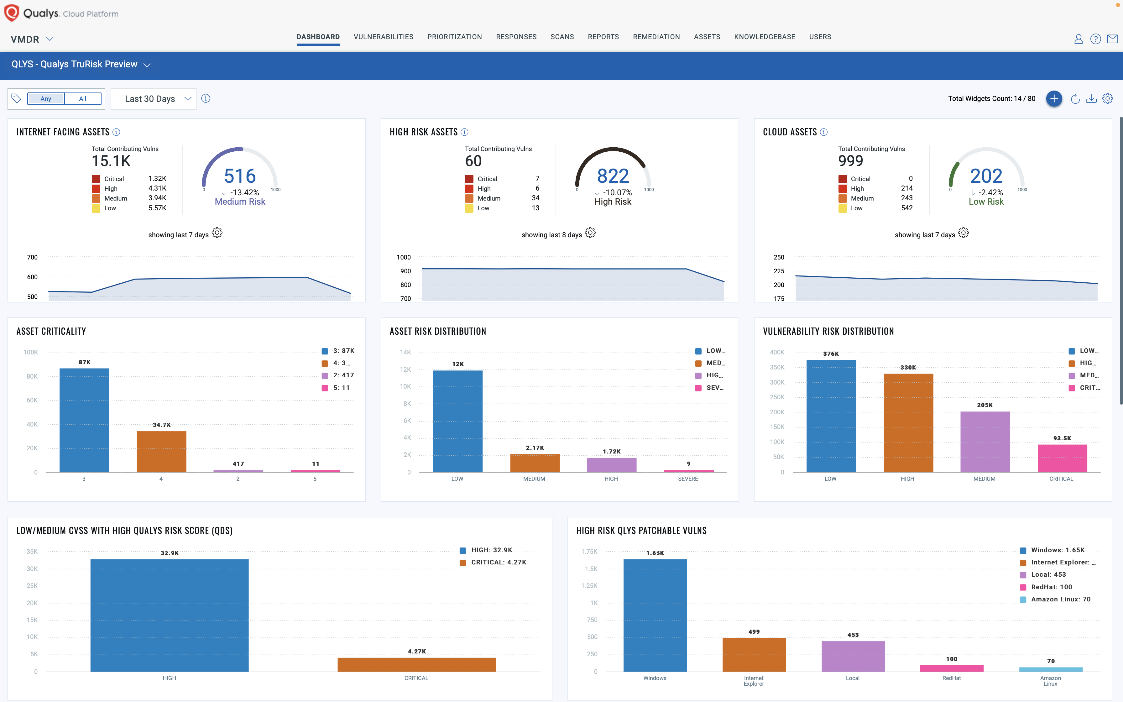
**-Policy Compliance (Tuân thủ chính sách):**

**+Kiểm tra tuân thủ chính sách**: Xác minh cấu hình cơ bản của các tài sản máy chủ.

**+PCI Compliance (Tuân thủ PCI)**: Quét tài sản để đảm bảo tuân thủ các yêu cầu PCI DSS.

**-Endpoint Detection and Response (Phát hiện và phản ứng trên thiết bị cuối):**

**+Bảo mật thiết bị cuối**: Bảo vệ các thiết bị cuối và tìm kiếm mã độc với Qualys EDR.



Hình 2.2 Dashboard của Qualys

### Nessus

a) Khái niệm

Nessus là một công cụ quét lỗ hổng mạng phổ biến và mạnh mẽ, độc quyền được phát triển bởi công ty anh ninh mạng Tenable. Nessus giúp các tổ chức xác định và đánh giá các lỗ hổng bảo mật trong hệ thống, ứng dụng và thiết bị mạng của họ.

A screenshot of a computer

Description automatically generated

Hình 2.3 Dashboard của Nessus

b) Cách hoạt động

Nessus quét các cổng và dịch vụ trên mạng để xác định các lỗ hổng bảo mật bằng cách kiểm tra các điểm yếu tiềm năng.

Công cụ này sử dụng cơ sở dữ liệu lỗ hổng rộng rãi để so sánh thông tin quét với các lỗ hổng đã biết.

Nessus cung cấp báo cáo chi tiết về các lỗ hổng, đánh giá mức độ nghiêm trọng và cung cấp hướng dẫn về cách vá chúng.

c) Các chức năng chính

**Quét mạng**: Nessus có thể quét các địa chỉ IP hoặc phạm vi địa chỉ IP cụ thể để phát hiện các lỗ hổng bảo mật trên hệ thống mạng.

**Phát hiện lỗ hổng**: Nessus phân tích các dịch vụ và ứng dụng đang chạy trên hệ thống mạng để phát hiện các lỗ hổng bảo mật như các lỗ hổng của phần mềm và các cấu hình không an toàn.

**Tự động cập nhật**: Nessus có khả năng tự động cập nhật để đảm bảo rằng nó có thể phát hiện các lỗ hổng mới nhất.

**Thực hiện kiểm tra nhanh**: Nessus có thể thực hiện các kiểm tra nhanh để phát hiện các lỗ hổng bảo mật một cách nhanh chóng.

**Tạo báo cáo**: Nessus cho phép tạo các báo cáo về các lỗ hổng bảo mật được phát hiện trên hệ thống mạng. Báo cáo này có thể được lưu trữ hoặc xuất ra dưới dạng các định dạng khác nhau như PDF, HTML hoặc CSV.

**Điều chỉnh phạm vi quét**: Nessus cung cấp các tùy chọn để điều chỉnh phạm vi quét để giảm thiểu số lỗi giả mạo hoặc tăng độ chính xác.

**Tự động xác định thiết bị**: Nessus có thể tự động xác định các thiết bị đang chạy trên hệ thống mạng và quét chúng để phát hiện các lỗ hổng bảo mật.

**Các cấu hình đa dạng**: Nessus có thể được cấu hình để thực hiện các kiểm tra đa dạng, bao gồm các kiểm tra lỗ hổng của phần mềm, kiểm tra cấu hình và kiểm tra tích hợp.

### OpenVAS

a) Khái niệm

**OpenVAS (Open Vulnerability Assessment System)** là một hệ thống đánh giá lỗ hổng bảo mật mã nguồn mở. Nó cung cấp một bộ công cụ để phát hiện, phân tích và giải quyết các lỗ hổng bảo mật trong hệ thống và ứng dụng.

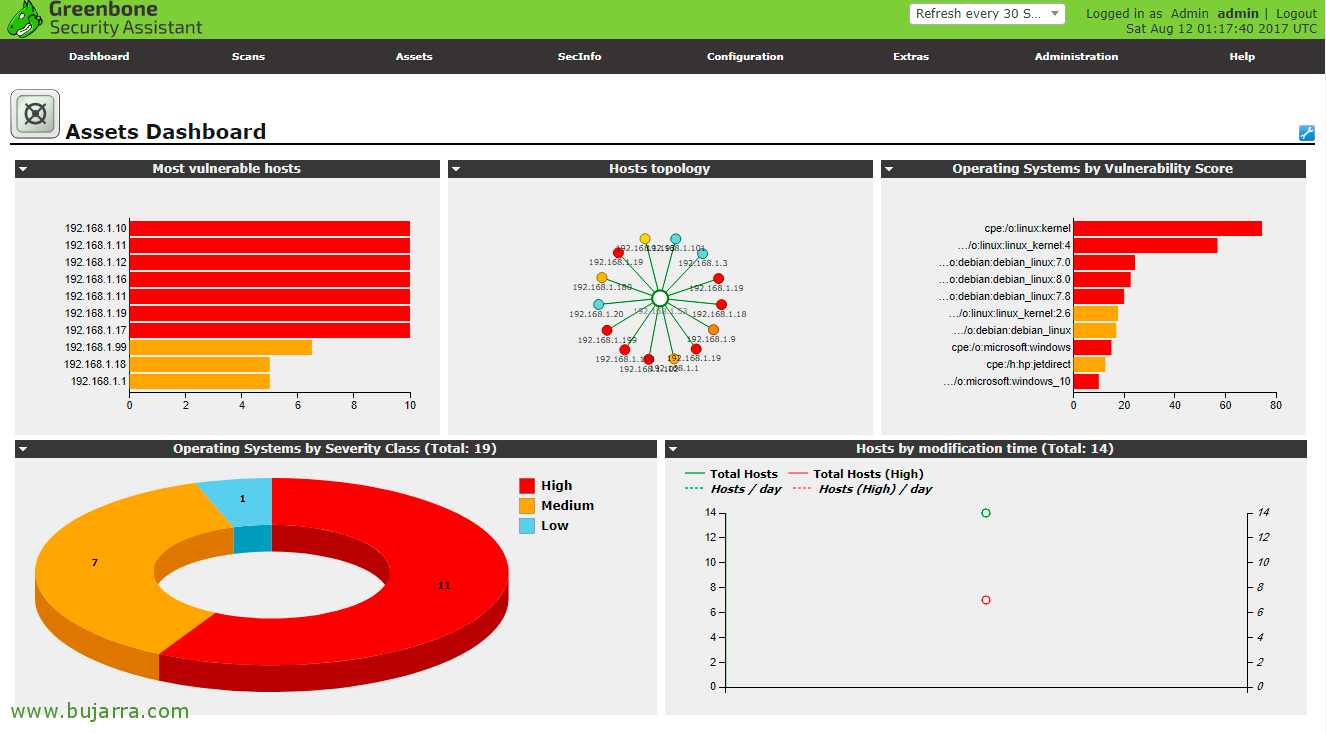
b) Chức năng

**OpenVAS Scanner**: một công cụ quét mạnh mẽ để phát hiện các lỗ hổng bảo mật trong các hệ thống và ứng dụng.

**OpenVAS Manager**: quản lý các công cụ quét và báo cáo các kết quả quét.

**OpenVAS CLI**: một giao diện dòng lệnh để điều khiển và kiểm soát OpenVAS.

**Greenbone Security Assistant**: một giao diện web cho phép quản trị viên tạo, quản lý và xem các báo cáo về các lỗ hổng bảo mật.



Hình 2.4 Assets Dashboard của OpenVAS

### Rapid7 Nexpose

a) Khái niệm

Nexpose là phần mềm quét lỗ hổng bảo mật chuyên nghiệp. Được sử dụng để đánh giá các lỗ hỗng an ninh thông tin cho hệ thống mạng hiện đại

b) Chức năng:

**Khám phá và phát hiện lỗ hổng**: Nexpose giúp xác định các lỗ hổng trong hệ thống, từ việc phát hiện các thiết bị mới đến xác minh các lỗ hổng tồn tại.

**Xác minh và phân loại mức độ rủi ro**: Nexpose không chỉ tìm ra lỗ hổng, mà còn đánh giá mức độ rủi ro của chúng, có thể biết được lỗ hổng nào cần được ưu tiên xử lý trước.

**Báo cáo phân tích ảnh hưởng của các rủi ro**: Nexpose cung cấp báo cáo chi tiết về tác động của các lỗ hổng khi bị tấn công, giúp đưa ra quyết định hợp lý về biện pháp kiểm soát.

**Liên kết với các giải pháp khác**: Nexpose tích hợp với nhiều sản phẩm khác nhau, bao gồm các hệ thống SIEM, giải pháp quản lý vé, tường lửa thế hệ mới và quản lý chứng chỉ.

Nexpose giúp bạn giảm nguy cơ bị đe dọa bằng cách cung cấp thông tin thời gian thực và ưu tiên rủi ro trên các lỗ hổng, cấu hình và biện pháp kiểm soát.

# THỰC NGHIỆM

## Mục đích

Tìm hiểu về công cụ Nessus, nghiên cứu triển khai các kịch bản thực nghiệm, phân tích đánh giá rủi ro dựa trên kết quả của phần mềm.

## Mô hình

A diagram of a computer network

Description automatically generated

Hình 3.1 Mô hình thực nghiệm

* Một máy ảo windows server 2012
* Một máy ảo Kali Linux đã cài đặt Nessus
* Một máy ảo windows 7

## Các kịch bản thực nghiệm

Kịch bản: Dò quét kiểm tra các thiết bị thuộc cùng dải mạng

Bước 1: Tạo bản quét mới

A screenshot of a computer

Description automatically generated

Hình 3.2 Tạo bản quét mới

- Chọn New Scan ở góc bên phải để tạo bản quét mới

- Tiếp tục chọn Advanced Scan để thiết lập cài đặt các thông số

A screenshot of a computer

Description automatically generated

Hình 3.3 Thiết lập cài đặt

Trong mục Settings/Basic/General, phần “Targets” để dải IP cần quét (trong bài này là 192.168.146.2/24)

A screenshot of a computer

Description automatically generated

Hình 3.4 Cài đặt tự động rò quét

Trong phần Schedule (lịch trình), có thể tích “Enabled” để thực hiện dò quét tự động, Như trong bài, bản quét này sẽ tự động chạy vào lúc 9 giờ hàng ngày. Tuy nhiên, phiên bản Nessus này chỉ giới hạn cho một bản quét được tự động chạy.

Các phần còn lại, có thể để mặc định hoặc hiệu chỉnh tùy mục đích người dùng. Chọn Save để lưu bản quét.

**Bước 2: Chạy bản quét**

A screenshot of a computer

Description automatically generated

Hình 3.5 Chạy bản quét

Chọn “Launch” (là phần gạch đỏ trong hình) để chạy bản quét

**Bước 3: Phân tích kết quả**

A blue and white text box

Description automatically generated

Hình 3.6 Kết quả sau khi hoàn thành quét

Sau khi hoàn thành dò quét các thiết bị thuộc cùng dải mạng, thu được một số kết quả như sau:

Phát hiện hơn 59 lỗ hổng trên toàn bộ các thiết bị thuộc dải mạng.

Trên windows server 2012 (IP: 192.168.146.132) phát hiện 21 lỗ hổng với 10% các lỗ hổng có độ nghiêm trọng trung bình.

Trên windows 7 (IP: 192.168.146.133) phát hiện 19 lỗ hổng với 5% các lỗ hổng có độ nghiêm trọng ở mức trung bình và 5% lỗ hổng có mức độ nghiêm trọng rất cao.

a) Đánh giá trên windows server 2012

A screenshot of a computer

Description automatically generated

Hình 3.7 Kết quả dò quét trên Windows Server 2012

Kết quả cho thấy có các lỗ hổng liên quan các vấn đề của Microsoft Windows, SMB.

Trong phần lỗ hổng của Microsoft Windows, có lỗ hổng mang tên MS16-047 được đánh giá ở mức độ trung bình (medium)

A screenshot of a computer

Description automatically generated

Hình 3.8 Các lỗ hổng của Microsoft Windows

A screenshot of a computer

Description automatically generated

Hình 3.9 Lỗ hổng MS16-047

MS16-047 là lỗ hổng liên quan đến xác thực và cơ sở dữ liệu. Kẻ tấn công lợi dụng lỗ hổng của SAM và chính sách miền (LSAD) để chặn liên lạc giữa máy khách và máy chủ lưu trữ cơ sở liệu SAM, khai thác điều này để hạ cấp xác thức, cho phép kẻ tấn công mạo danh người dùng.



Hình 3.10 Đánh giá về MS16-047 của Nessus

A screenshot of a computer

Description automatically generated

Hình 3.11 Lỗ hổng MSB

Lỗ hổng SMB giúp kẻ tấn công không cần đăng nhập trên máy chủ SMB từ xa, kẻ tấn công có thể khai thác và tiến hành tấn công “man in the middle” chống lại máy chủ SMB.

A screenshot of a computer

Description automatically generated

Hình 3.12 Đánh giá về lỗ hổng MSB

b) Đánh giá trên windows 7

A screenshot of a computer

Description automatically generated

Hình 3.13 Kết quả dò quét trên Windows 7

Có thể thấy, các lỗ hổng trên Windows 7 khá đa dạng. Tuy nhiên giống với Windows Server 2012, các lỗ hổng nguy hiểm nhất liên qua đến Microsoft và SMB.

A screenshot of a computer

Description automatically generated

Hình 3.14 Lỗ hổng của Windows 7

Với 1 lỗi ở múc độ rất nghiêm trọng (critical), 1 lỗi ở mức độ cao (high) và 1 lỗi ở mức độ medium, phiên bản Windows 7 đang tiềm tàng rất nhiều rủi ro và cơ hội cho các kẻ tấn công là rất cao. Lỗ hổng MS16-047 một lần nữa lại xuất hiện tại phiên bản Windows này.

A close-up of a computer screen

Description automatically generated

Hình 3.15 Unsupported Windows OS

Như hình 3.14, điểm đánh giá đạt mức độ tuyệt đối (10.0). Lỗ hổng này tồn tại vì phiên bản Windows này không còn được nhà phát triển hỗ trợ.

A screenshot of a computer

Description automatically generated

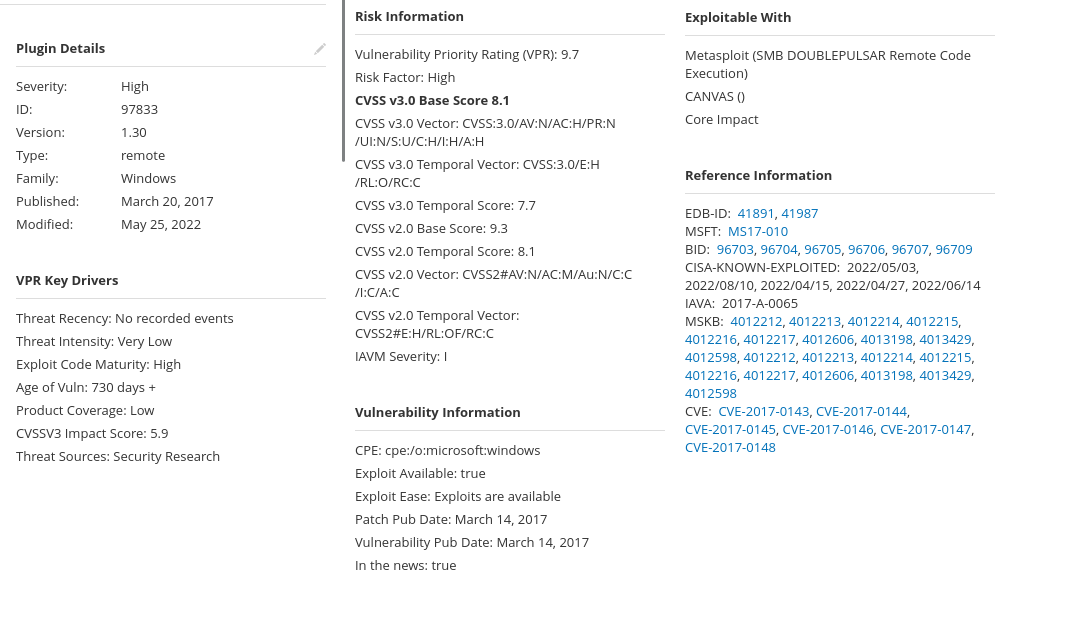
Hình 3.16 Lỗ hổng MS17-010

Lỗ hổng MS17-010 được đánh giá ở mức độ nghiêm trong cao. Đây là một lỗ hổng phức tạp gây ảnh hưởng tới máy chủ Windows. Liên quan đến lỗ hổng thực thi mã từ xa tồn tại trong Microsoft Server Message Block 1.0 (SMBv1) do xử lí không đúng các yêu cầu nhất định. Kẻ tấn công có thể lợi dụng điểm này để tiến hành các cuộc tấn công và khai thác.

A screenshot of a computer

Description automatically generated

Hình 3.17 Thông tin thêm về lỗ hổng MS17-010



Hình 3.18 Đánh giá về lỗ hổng MS17-010

# KẾT LUẬN

Bài báo cáo này đã xem xét về phương pháp đánh giá rủi ro trong lĩnh vực quản lý an toàn thông tin và các công cụ tự động đánh giá rủi ro. Các phần được trình bày bao gồm một tổng quan về vấn đề, khảo sát về các phương pháp và công cụ đánh giá rủi ro, và cuối cùng là phần thực nghiệm.

Trong Chương 1 là tổng quan về đánh giá rủi ro trong lĩnh vực quản lý an toàn thông tin. Cho thấy rằng đánh giá rủi ro đóng vai trò quan trọng trong việc bảo vệ thông tin của tổ chức, từ việc xác định và đánh giá các nguy cơ đến việc phát triển các biện pháp bảo vệ phù hợp. Quá trình này không chỉ giúp cải thiện mức độ an toàn của hệ thống thông tin mà còn tạo ra lợi ích kinh tế và tăng cường uy tín của tổ chức.

Trong Chương 2, khảo sát về các phương pháp và công cụ đánh giá rủi ro. Qua đó thấy được các phương pháp và tiêu chí đánh giá rủi ro cùng với các công cụ tự động đánh giá rủi ro như Qualys, OpenVAS, Rapid7 Nexpose và Nessus đã mang lại nhiều lợi ích cho tổ chức trong việc quản lý rủi ro.

Trong Chương 3, đã tiến hành một số thử nghiệm để xác định hiệu suất của các công cụ tự động đánh giá rủi ro. Kết quả từ các thử nghiệm này đã minh hoạ dễ hiểu mô hình đánh giá rủi ro trong thực tế.

Tóm lại, việc áp dụng phương pháp đánh giá rủi ro và sử dụng các công cụ tự động đánh giá rủi ro là một phần không thể thiếu trong quản lý an toàn thông tin của tổ chức.

# TÀI LIỆU THAM KHẢO

[1] Giáo trình Quản lý an toàn thông tin

[2] [TÌM HIỂU NESSUS CÔNG CỤ QUÉT LỖ HỔNG - Vacif.com](https://vacif.com/blog/tim-hieu-nessus-cong-cu-quet-lo-hong/)

[3] [Đánh giá rủi ro an toàn thông tin mạng là gì? Việc đánh giá rủi ro an toàn thông tin mạng phải do ai thực hiện? (thuvienphapluat.vn)](https://thuvienphapluat.vn/phap-luat/danh-gia-rui-ro-an-toan-thong-tin-mang-la-gi-viec-danh-gia-rui-ro-an-toan-thong-tin-mang-phai-do-ai-124583-119043.html)

[4] [OpenVAS công cụ đánh giá lỗ hổng bảo mật mã nguồn mở - Cú Đêm Solutions (cudem.info)](https://cudem.info/openvas/)

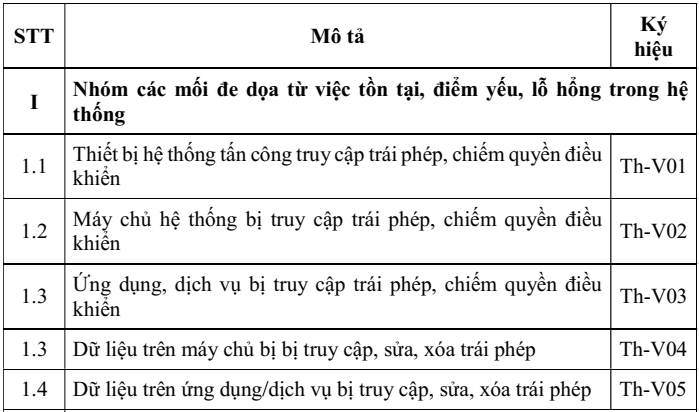
[5] [Qualys Documentation: Release Notes, User Guides & more | Qualys](https://www.qualys.com/documentation/#vulnerability-management)

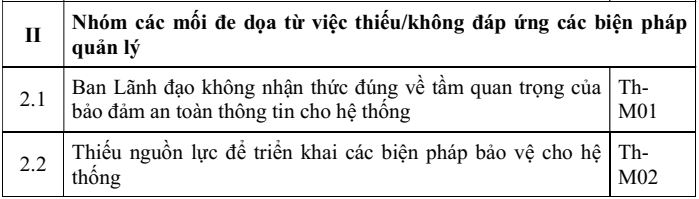
[6] [Các chức năng của công cụ quét bảo mật mạng Nessus và cách cài đặt - Cú Đêm Solutions (cudem.info)](https://cudem.info/cac-chuc-nang-cua-cong-cu-quet-bao-mat-mang-nessus-va-cach-cai-dat/)

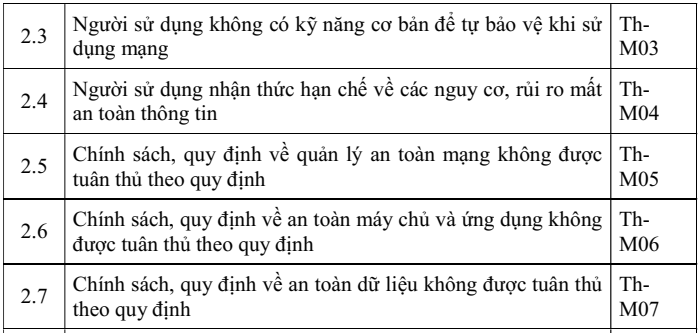
[7] [Welcome to Tenable Nessus 10.3.x (Tenable Nessus 10.3)](https://docs.tenable.com/nessus/10_3/Content/GettingStarted.htm)

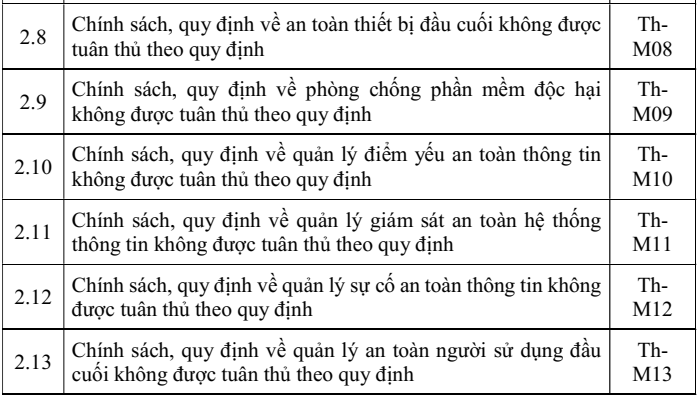
# PHỤ LỤC

* Các mối đe doạ phổ biến trong mục **nhận biết về mối đe doạ:**









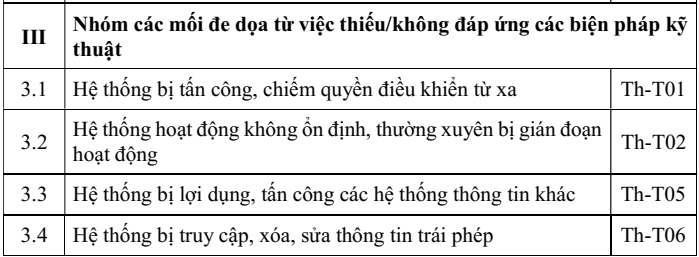
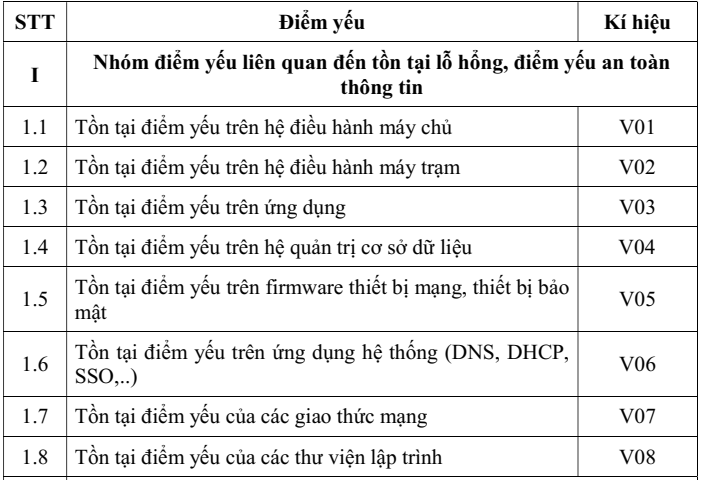
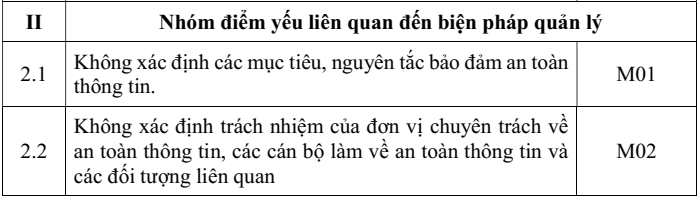
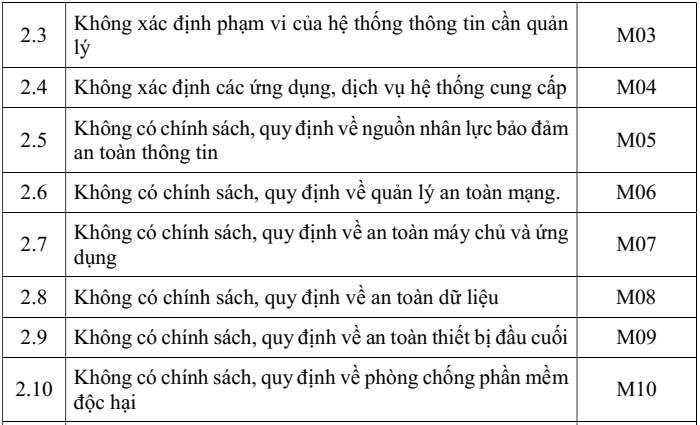


Table 8 Nhận biết về mối đe dọa

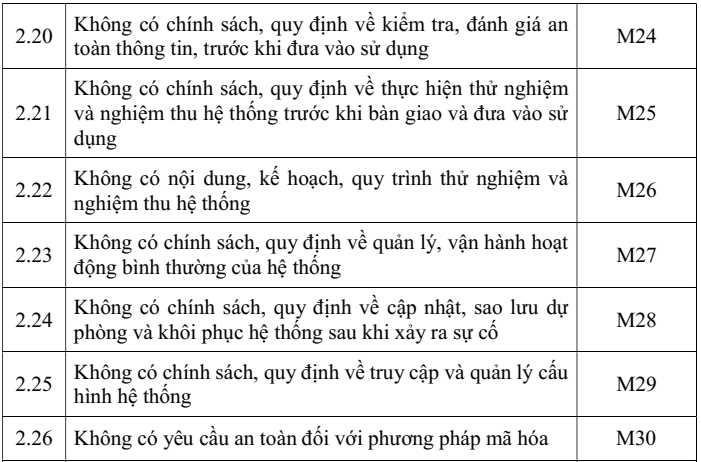
* Các điểm yếu phổ biến trong mục **nhận biết về điểm yếu:**

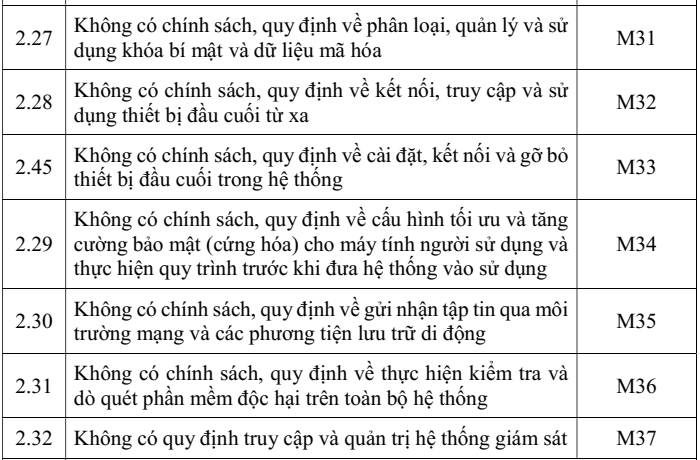


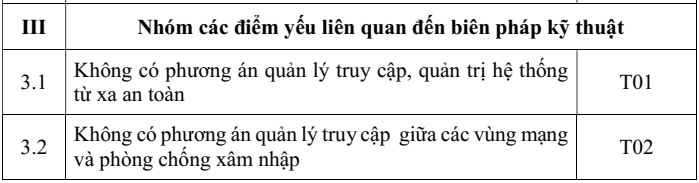


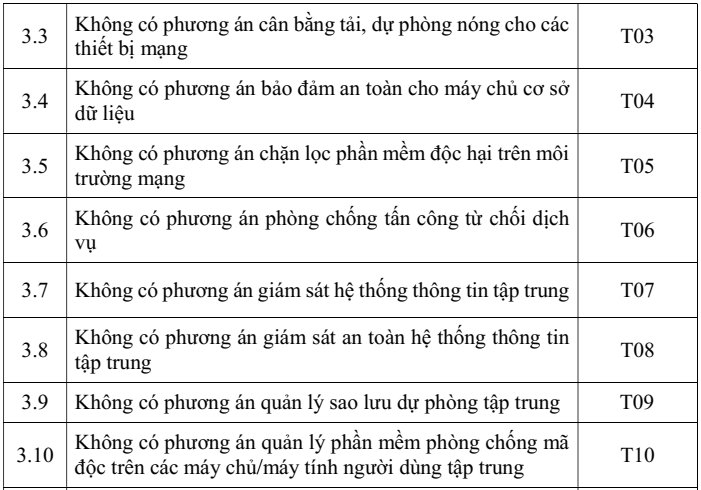


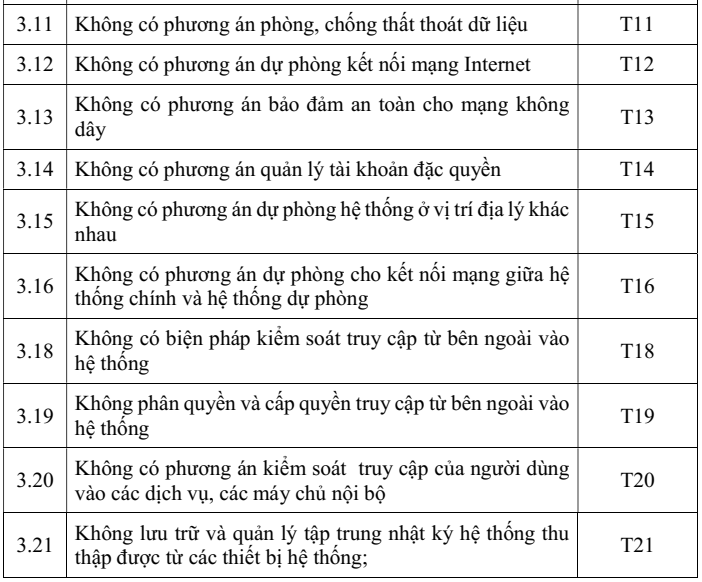


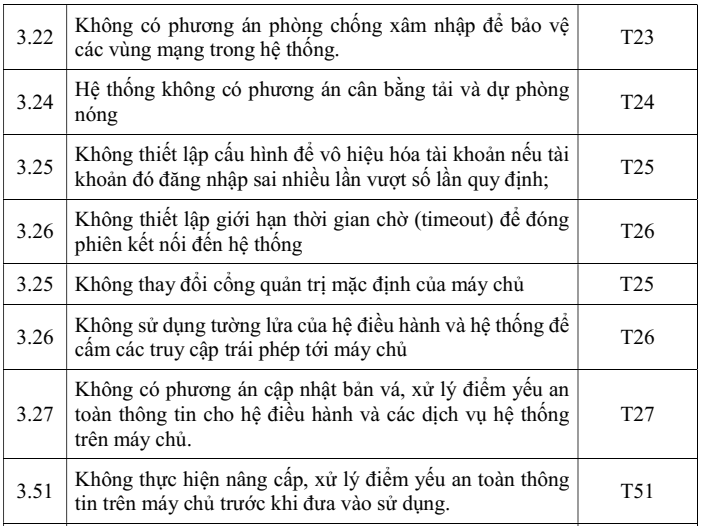


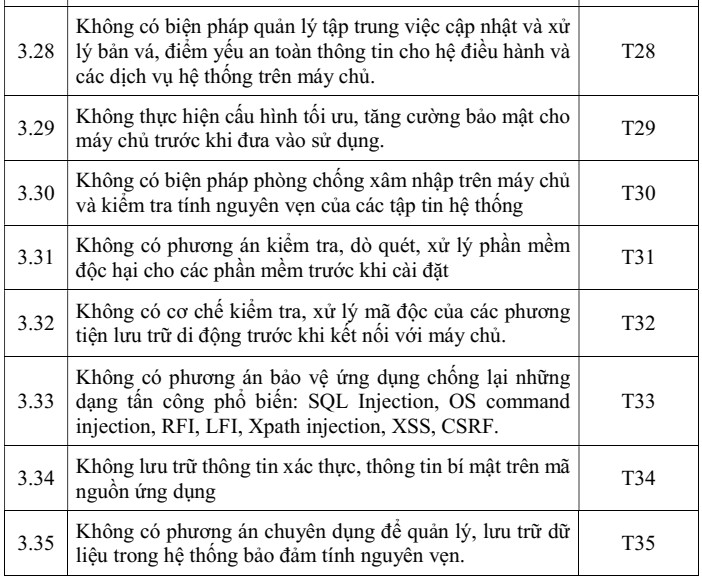












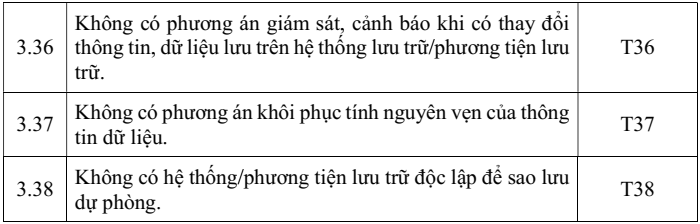
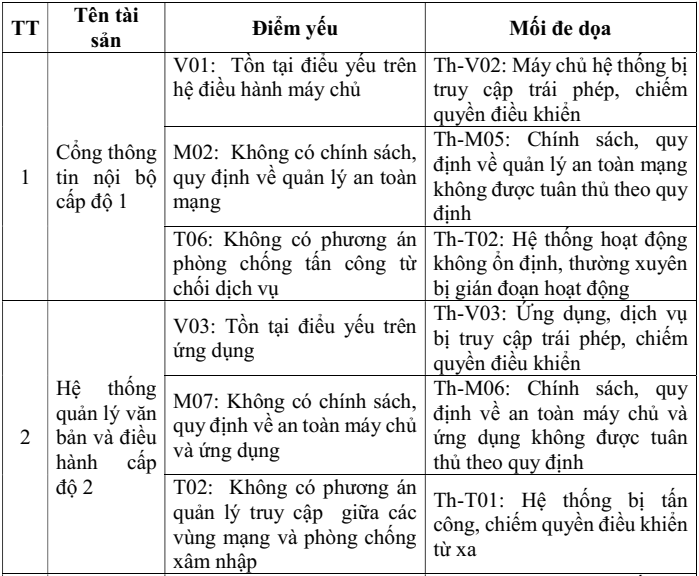


Table 9 Nhận biết về điểm yếu

* **Ví dụ Xác định Điểm yếu và Mối đe dọa:**



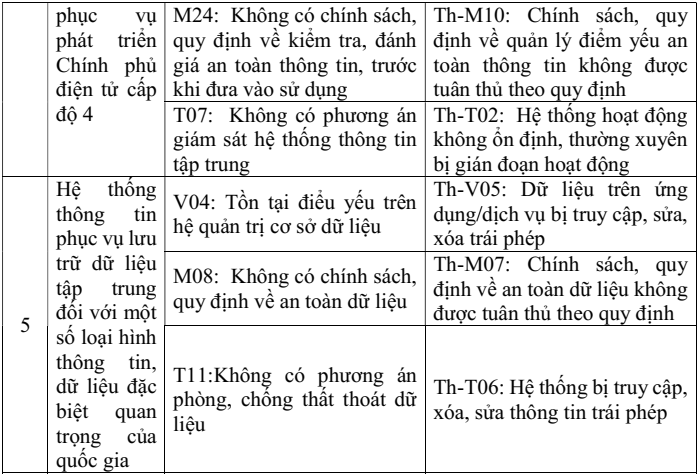


Table 10 Xác định điểm yếu và mối đe dọa