

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

| | | |
|----------------------------------|-------------|----------|
| <u>Nhóm sinh viên thực hiện:</u> | Vũ Tiên 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 |
| DANH MỤC VIẾT TẮT | 2 |
| LỜI MỞ ĐẦU | 4 |
| CHƯƠNG 1. TỔNG QUAN VỀ ĐÁNH GIÁ RỦI RO TRONG LĨNH VỰC QUẢN LÝ AN TOÀN THÔNG TIN | 5 |
| 1.1 Khái niệm | 5 |
| 1.2 Tầm quan trọng..... | 5 |
| 1.3 Vai trò chính | 5 |
| 1.4 Các tiêu chuẩn tham chiếu..... | 5 |
| CHƯƠNG 2. CÁC PHƯƠNG PHÁP ĐÁNH GIÁ VÀ CÔNG CỤ TỰ ĐỘNG ĐÁNH GIÁ RỦI RO..... | 6 |
| 2.1 Các phương pháp đánh giá rủi ro | 6 |
| 2.1.1 <i>Phương pháp nhận diện rủi ro</i> | 6 |
| 2.1.1.1 Khái niệm..... | 6 |
| 2.1.1.2 Nhận biết về tài sản..... | 7 |
| 2.1.1.3 Nhận biết về mối đe doạ | 11 |
| 2.1.1.4 Nhận biết về điểm yếu | 11 |
| 2.1.2 <i>Phương pháp phân tích rủi ro</i> | 12 |
| 2.1.3 <i>Phương pháp ước lượng rủi ro</i> | 16 |
| 2.2 Các công cụ tự động đánh giá rủi ro..... | 18 |
| 2.2.1 <i>Qualys</i> | 18 |
| 2.2.2 <i>Nessus</i> | 19 |
| 2.2.3 <i>OpenVAS</i> | 21 |
| 2.2.4 <i>Rapid7 Nexpose</i> | 22 |
| CHƯƠNG 3. THỰC NGHIỆM | 23 |
| 3.1 Mục đích | 23 |
| 3.2 Mô hình..... | 23 |
| 3.3 Các kịch bản thực nghiệm | 23 |

| | |
|-------------------------|----|
| KẾT LUẬN | 33 |
| TÀI LIỆU THAM KHẢO..... | 34 |
| PHỤ LỤC | 35 |

DANH MỤC HÌNH ẢNH

| | |
|---|----|
| Hình 2.1 Định lượng rủi ro..... | 16 |
| Hình 2.2 Dashboard của Qualys..... | 19 |
| Hình 2.3 Dashboard của Nessus..... | 20 |
| Hình 2.4 Assets Dashboard của OpenVAS..... | 22 |
| Hình 3.1 Mô hình thực nghiệm | 23 |
| Hình 3.2 Tạo bản quét mới..... | 24 |
| Hình 3.3 Thiết lập cài đặt..... | 24 |
| Hình 3.4 Cài đặt tự động rò quét..... | 25 |
| Hình 3.5 Chạy bản quét..... | 25 |
| Hình 3.6 Kết quả sau khi hoàn thành quét | 26 |
| Hình 3.7 Kết quả dò quét trên Windows Server 2012 | 26 |
| Hình 3.8 Các lỗ hổng của Microsoft Windows..... | 27 |
| Hình 3.9 Lỗ hổng MS16-047 | 27 |
| Hình 3.10 Đánh giá về MS16-047 của Nessus | 28 |
| Hình 3.11 Lỗ hổng MSB | 28 |
| Hình 3.12 Đánh giá về lỗ hổng MSB | 29 |
| Hình 3.13 Kết quả dò quét trên Windows 7..... | 29 |
| Hình 3.14 Lỗ hổng của Windows 7 | 30 |
| Hình 3.15 Unsupported Windows OS..... | 30 |
| Hình 3.16 Lỗ hổng MS17-010 | 31 |
| Hình 3.17 Thông tin thêm về lỗ hổng MS17-010..... | 31 |
| Hình 3.18 Đánh giá về lỗ hổng MS17-010 | 32 |

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

| | |
|---|----|
| Bảng 2.1. Thang điểm giá trị..... | 9 |
| Bảng 2.2. Gán trọng số cho mỗi nhân tố..... | 10 |
| Bảng 2.3. Tiêu chí đánh giá hậu quả..... | 14 |
| Bảng 2.4. Khả năng xảy ra sự cố..... | 15 |
| Bảng 2.5. Năm mức rủi ro..... | 16 |
| Bảng 2.6. Tiêu chí xác định mức rủi ro..... | 17 |
| Bảng 2.7. Gán giá trị hoặc mức điểm rủi ro..... | 18 |

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 họa 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

CHƯƠNG 1. TỔNG QUAN VỀ ĐÁNH GIÁ RỦI RO TRONG LĨNH VỰC QUẢN LÝ AN TOÀN THÔNG TIN

1.1 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.

1.2 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.

1.3 Vai trò chính

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

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

1.4 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

CHƯƠNG 2. CÁC PHƯƠNG PHÁP ĐÁNH GIÁ VÀ CÔNG CỤ TỰ ĐỘNG ĐÁNH GIÁ RỦI RO

2.1 Các phương pháp đánh giá rủi ro

2.1.1 Phương pháp nhận diện rủi ro

2.1.1.1 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.

2.1.1.2 Nhận biết về tài sản

- ❖ Cân 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 chí...; 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**

Cân 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:

| Giá trị tài sản | Giá trị C+I+A |
|-----------------|---------------|
| Thấp (1) | 1-3 |
| Trung bình (2) | 4-6 |
| Cao (3) | 7-9 |
| Rất cao (4) | 10-12 |
| Cực cao (5) | 13-15 |

Bảng 2.1. 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 thang 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 sẵn sàng trung bình thang điểm 2; tính sẵn sàng

cao thang điểm 3; tính tính săn sàng rất cao điểm 4; tính tính săn 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

| Các tài sản | Tiêu chí 1: Ảnh hưởng tới tổng thu nhập | Tiêu chí 2: Ảnh hưởng tới lợi nhuận | Tiêu chí 3: Ảnh hưởng tới hình ảnh của tổ chức | Điểm đã tính trọng số |
|---|---|-------------------------------------|--|-----------------------|
| <i>Trọng số của mỗi tiêu chí từ 1-100, tổng phải là 100</i> | | | | |
| | 30 | 40 | 30 | |
| Tài sản 1 | 0.8 | 0.9 | 0.5 | 75 |
| Tài sản 2 | 0.8 | 0.9 | 0.6 | 78 |
| Tài sản 3 | 0.4 | 0.5 | 0.3 | 41 |
| Tài sản 4 | 1.0 | 1.0 | 1.0 | 100 |
| Tài sản 5 | 0.4 | 0.4 | 0.9 | 55 |

Bảng 2.2. Gán trọng số cho mỗi nhân tố

2.1.1.3 Nhận biết về mối đe dọa

- ❖ 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.

2.1.1.4 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 hiệnNên 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.

2.1.2 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:

| Mức ảnh hưởng | Tính bảo mật (C) | Tính toàn vẹn (I) | Tính sẵn sàng (A) |
|---------------------------|--|---|---|
| Đặc biệt nghiêm trọng (5) | Việc bị lộ thông tin trái phép làm ảnh hưởng nghiêm trọng đến quốc phòng, an ninh | Việc sửa đổi hoặc phá hủy trái phép thông tin làm ảnh hưởng nghiêm trọng đến quốc phòng, an ninh | Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm ảnh hưởng nghiêm trọng đến quốc phòng, an ninh |
| Nghiêm trọng (4) | Việc bị lộ thông tin trái phép làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia | Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia | Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia |
| Vừa phải (3) | Việc bị lộ thông tin trái phép làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia | Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia | Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia |

| | | | |
|-------------------------|---|--|--|
| Nhỏ (2) | Việc bị lộ thông tin trái phép làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng | Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng | Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng |
| Không đáng kể (1) | Việc bị lộ thông tin trái phép làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân | Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân | Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân |
| | | | |

Bảng 2.3. Tiêu chí đánh giá hậu quả

❖ Khả năng xảy ra sự cố:

| Khả năng xảy ra | Tiêu chí xác định |
|-----------------|---|
| Chắc chắn (5) | <p>(1) Khả năng khai thác:</p> <ul style="list-style-type: none"> - Lỗi hỏng có thể được thu thập từ các nguồn thông tin công khai; - Có thể thực hiện tấn công từ bên ngoài Internet mà không cần quyền truy cập vào hệ thống; có thể sử dụng các công cụ khai thác tự động được công khai trên mạng và không yêu cầu có trình độ về an toàn thông tin để thực hiện. - Có thể thực hiện tấn công lặp lại mà không cần thay đổi thiết lập và các điều kiện kỹ thuật sau lần tấn công đầu tiên. |
| | <p>(2) Tần suất: Nhiều hơn 1 lần/tháng</p> <p>(3) Khả năng xảy ra: >90%</p> <p>(4) Cơ hội: Dự kiến, chắc chắn sẽ xảy ra trong hầu hết các trường hợp</p> |

| | |
|----------------|---|
| Cao (4) | <p>(1) Khả năng khai thác:</p> <ul style="list-style-type: none"> - Lỗi hỏng có thể được thu thập thông qua việc tương tác thụ động với hệ thống từ bên ngoài; - Việc thực hiện tấn công yêu cầu có quyền người dùng tối thiểu; có thể sử dụng các công cụ khai thác tự động được công khai trên mạng và yêu cầu có trình độ về an toàn thông tin cơ bản để thực hiện. - Có thể thực hiện tấn công lặp lại bằng cách thay đổi thiết lập và các điều kiện kỹ thuật cơ bản mà không cần nắm được quy luật thay đổi. <p>(2) Tần suất: Nhiều hơn 1 lần/quý nhưng ít hơn 1 lần/tháng</p> <p>(3) Khả năng xảy ra: >60%</p> <p>(4) Cơ hội: Có khả năng xảy ra trong hầu hết các trường hợp</p> |
| Trung bình (3) | <p>(1) Khả năng khai thác:</p> <ul style="list-style-type: none"> - Lỗi hỏng có thể được thu thập thông qua việc sử dụng các công cụ dò quét từ bên ngoài; - Việc thực hiện tấn công yêu cầu có tài khoản đặc quyền; có thể sử dụng các công cụ khai thác tự động và yêu cầu có trình độ về an toàn thông tin để thực hiện. - Có thể thực hiện tấn công lặp lại và xác định được chắc chắn các tham số cần thiết lập để thực hiện tấn công lặp lại. <p>(2) Tần suất: Có khả năng xảy ra một số lần</p> <p>(3) Khả năng xảy ra: >=10%</p> <p>(4) Cơ hội: Có khả năng xảy ra một số lần</p> |
| Thấp (2) | <p>(1) Khả năng khai thác:</p> <ul style="list-style-type: none"> - Lỗi hỏng có thể được thu thập thông qua việc sử dụng các công cụ dò quét trực tiếp từ bên trong hệ thống; - Việc thực hiện tấn công yêu cầu có tài khoản đặc quyền; yêu cầu sử dụng các công cụ khai thác chuyên dụng và yêu cầu có trình độ cao về an toàn thông tin để thực hiện. - Có thể thực hiện tấn công lặp lại bằng cách thay đổi thiết lập và các điều kiện kỹ thuật cơ bản nhưng yêu cầu nắm được quy luật thay đổi. <p>(2) Tần suất: Ít hơn 1 lần/năm</p> <p>(3) Khả năng xảy ra: <10%</p> <p>(4) Cơ hội: Chỉ xảy ra trong một số trường hợp</p> |

Bảng 2.4. Khả năng xảy ra sự cố

2.1.3 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(đe dọa 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:

| Mức rủi ro | Giá trị tài sản+Mức ảnh hưởng+Khả năng xảy ra |
|----------------|---|
| Thấp (1) | 1-3 |
| Trung bình (2) | 4-6 |
| Cao (3) | 7-9 |
| Rất cao (4) | 10-12 |
| Cực cao (5) | 13-15 |

Bảng 2.5. Năm mức rủi ro

Việc xác định khả năng xảy ra sự cố cần dựa Giá trị tài 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:

| TT | Tên tài sản | Điểm yếu | Giá trị tài sản | Khả năng xảy ra | Mức ảnh hưởng | Mức rủi ro |
|----|---|----------|-----------------|-----------------|---------------|----------------|
| 1 | Công thông tin nội bộ cấp độ 1 | V01 | 2 | 3 | 1 | Trung bình (2) |
| | | M02 | 2 | 3 | 1 | Trung bình (2) |
| | | T06 | 2 | 2 | 1 | Trung bình (2) |
| 2 | Hệ thống quản lý văn bản và điều hành cấp độ 2 | V03 | 3 | 4 | 2 | Cao (3) |
| | | M07 | 3 | 4 | 2 | Cao (3) |
| | | T02 | 3 | 3 | 2 | Cao (3) |
| 3 | Hệ thống cung cấp thông tin và dịch vụ công trực tuyến cấp độ 3 | V02 | 3 | 3 | 3 | Cao (3) |
| | | M11 | 3 | 3 | 3 | Cao (3) |
| | | T03 | 3 | 4 | 3 | Rất cao (4) |
| 4 | Hệ thống thông tin quốc gia phục vụ phát triển Chính phủ điện tử cấp độ 4 | V03 | 4 | 4 | 4 | Rất cao (4) |
| | | M24 | 4 | 4 | 4 | Rất cao (4) |
| | | T07 | 4 | 3 | 4 | Rất cao (5) |
| 5 | Hệ thống thông tin phục vụ lưu trữ dữ liệu tập trung đối với một số loại hình thông tin, dữ liệu đặc biệt quan trọng của quốc gia | V04 | 5 | 3 | 5 | Cực cao (5) |
| | | M08 | 5 | 4 | 5 | Cực cao (5) |
| | | T11 | 5 | 3 | 5 | Cực cao (5) |

Bảng 2.6. 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:

$$\circ \quad RR = V \times P - R + U:$$

- 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 ro do do sự không chắc chắn của các tri thức hiện tại về điểm yếu

| Tài sản (1) | Ảnh hưởng hoặc giá trị có liên quan của tài sản (2) | Điểm yếu (3) | Khả năng xuất hiện điểm yếu (4) | Tỉ lệ rủi ro (5)=2x4 |
|----------------|--|-----------------|--|----------------------------|
| Tài sản 1 | 55 | Điểm yếu 1 | 0.2 | 11 |
| Tài sản 2 | 100 | Điểm yếu 2 | 0.1 | 10 |
| Tài sản 3 | 100 | Điểm yếu 3 | 0.1 | 10 |
| Tài sản 4 | 55 | Điểm yếu 4 | 0.1 | 5.5 |
| Tài sản 5 | 55 | Điểm yếu 5 | 0.1 | 5.5 |
| Tài sản 6 | 100 | Điểm yếu 6 | 0.025 | 2.5 |
| Tài sản 7 | 100 | Điểm yếu 7 | 0.01 | 1 |

Bảng 2.7. 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%.

$$U = 100\% - 90\% = 10\%$$

$$RR_{Điểm\ yếu\ 1} = 50 * (1.0 - 0\% + 10\%) = 55$$

2.2 Các công cụ tự động đánh giá rủi ro

2.2.1 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.

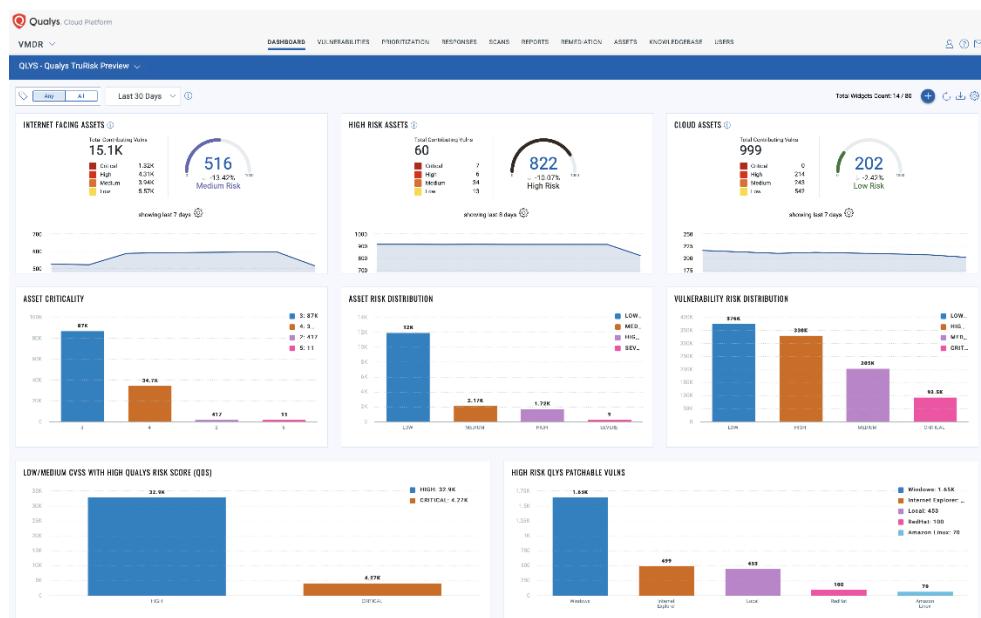
-Policy Compliance (Tuân thủ chính sách):

+**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.

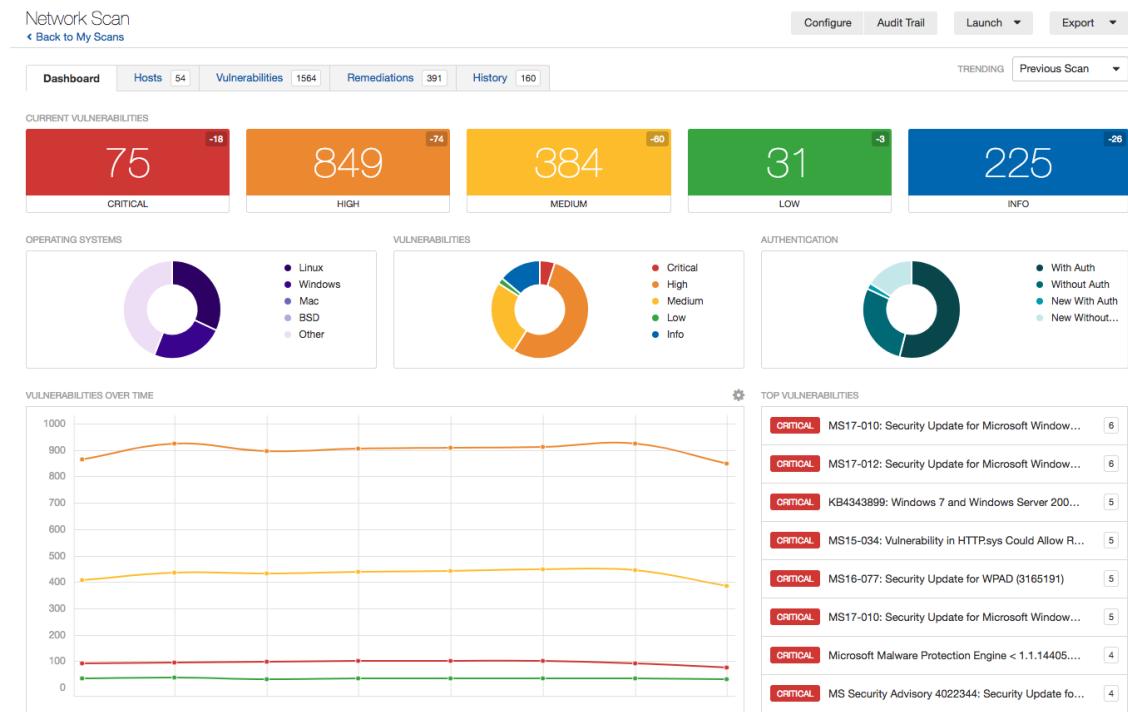


Hình 2.2 Dashboard của Qualys

2.2.2 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 an 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.



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.

2.2.3 *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.

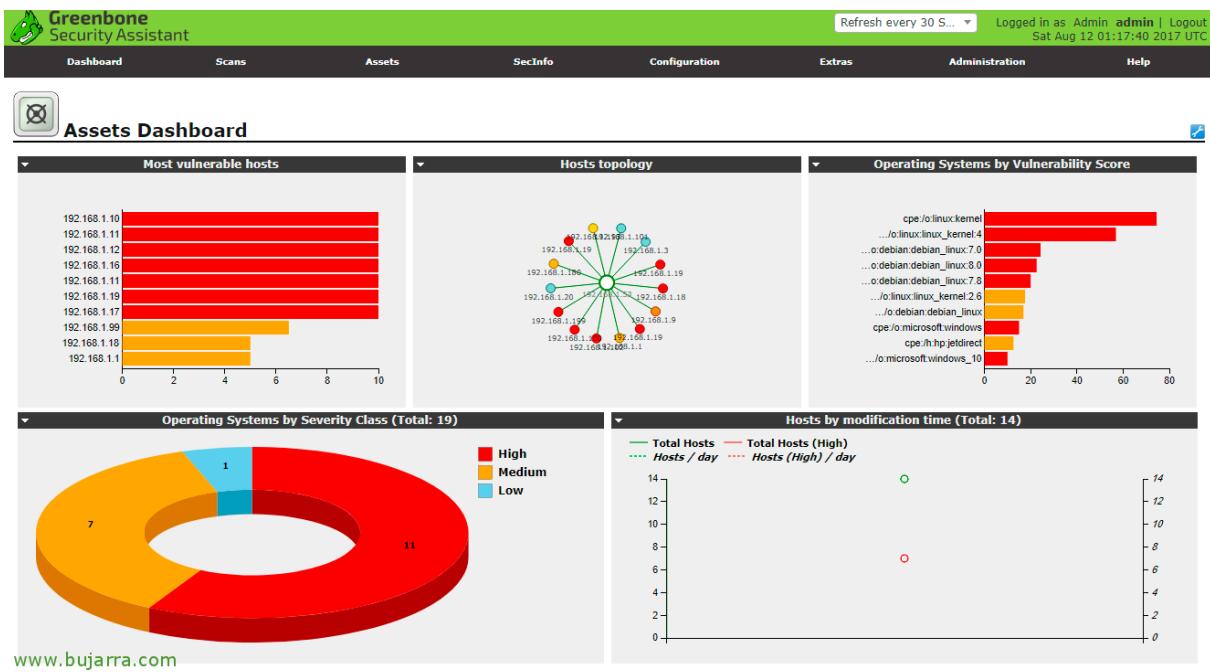
b) Chức năng

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

2.2.4 Rapid7 Nmap

a) Khái niệm

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

b) Chức năng:

Khám phá và phát hiện lỗ hổng: Nmap 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: Nmap 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: Nmap 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: Nmap 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.

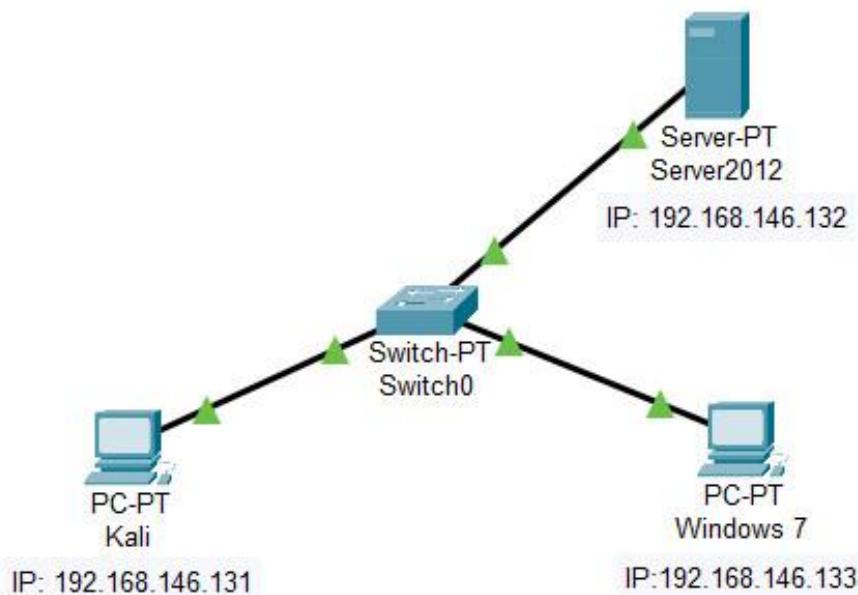
Nmap giúp bạn giảm nguy cơ bị đe dọa bằng cách cung cấp thông tin thời gian thực và ưu tiên rủi ro trên các lỗ hổng, cấu hình và biện pháp kiểm soát.

CHƯƠNG 3. THỰC NGHIỆM

3.1 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.

3.2 Mô hình



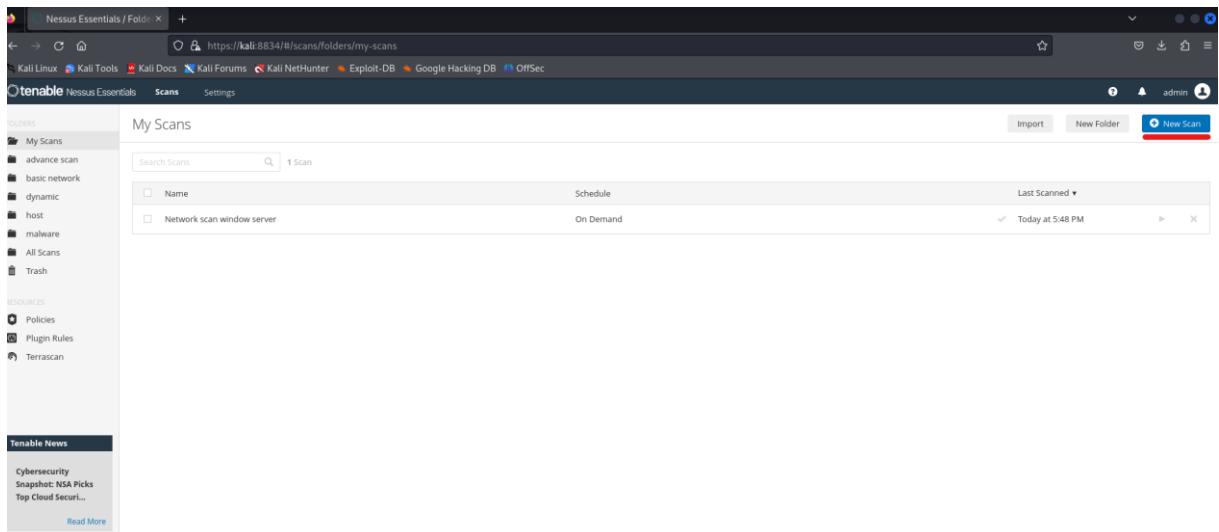
Hình 3.1 Mô hình thực nghiệm

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

3.3 Các kịch bản thực nghiệm

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

Bước 1: Tạo bản quét mới



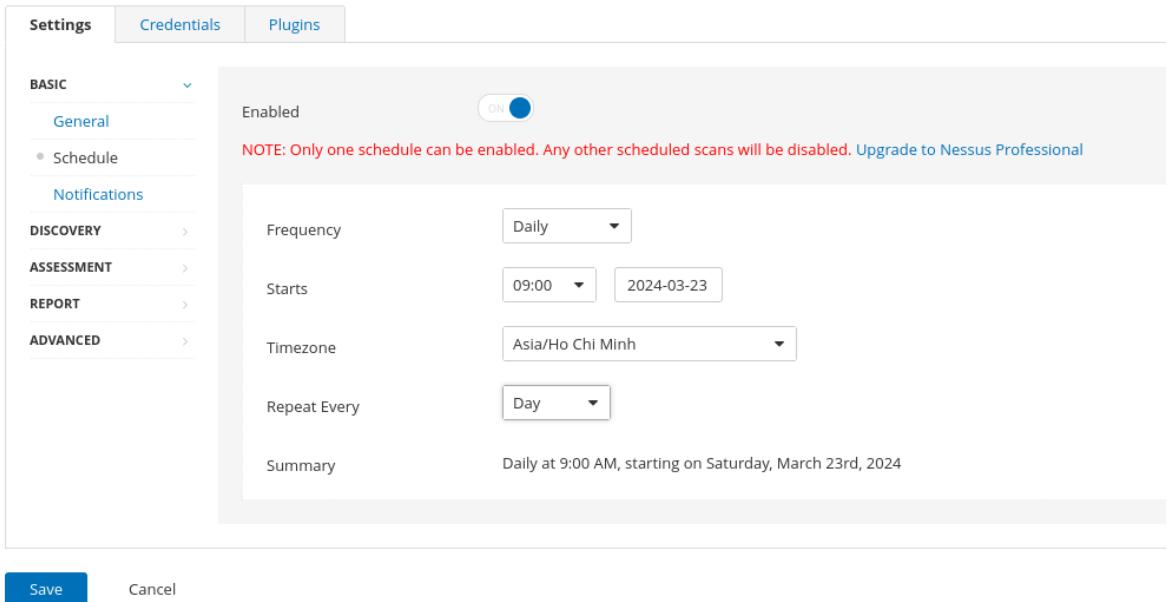
Hình 3.2 Tạo bản quét mới

- 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

| | |
|-------------------|--|
| BASIC | <input type="text" value="all"/> Description <input type="text" value="scan all LAN's devices"/> |
| DISCOVERY | Folder <input type="text" value="advance scan"/> |
| ASSESSMENT | |
| REPORT | |
| ADVANCED | Targets <input type="text" value="192.168.146.2/24"/> <input type="button" value="Upload Targets"/> <input type="button" value="Add File"/> |

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)



Hình 3.4 Cài đặt tự động rò quét

Trong phần Schedule (lịch trình), có thẻ 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.

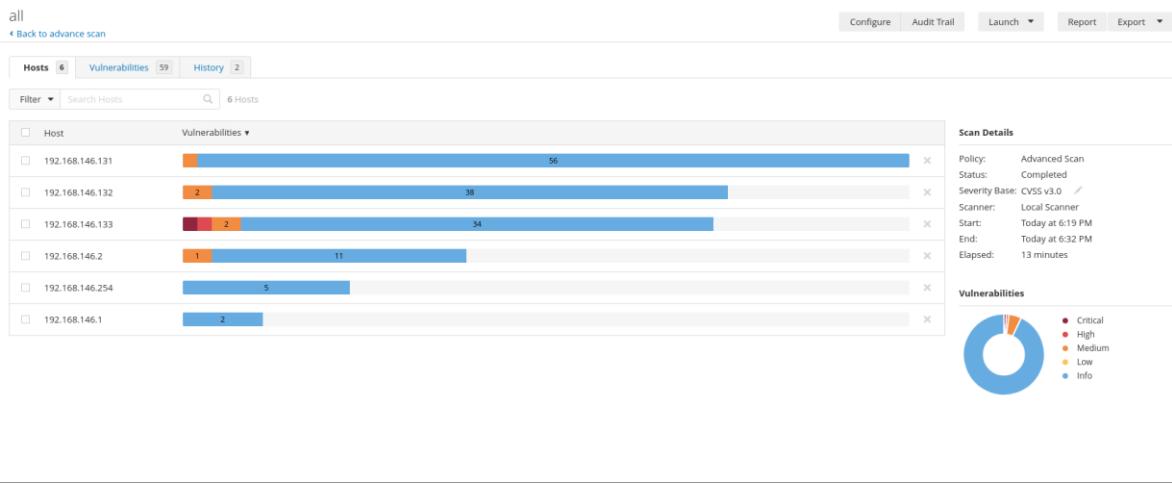
Các phần còn lại, có thể để mặc định hoặc hiệu chỉnh tùy mục đích người dùng. Chọn Save để lưu bản quét.

Bước 2: Chạy bản quét

Hình 3.5 Chạy bản quét

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

Bước 3: Phân tích kết quả



Hình 3.6 Kết quả sau khi hoàn thành quét

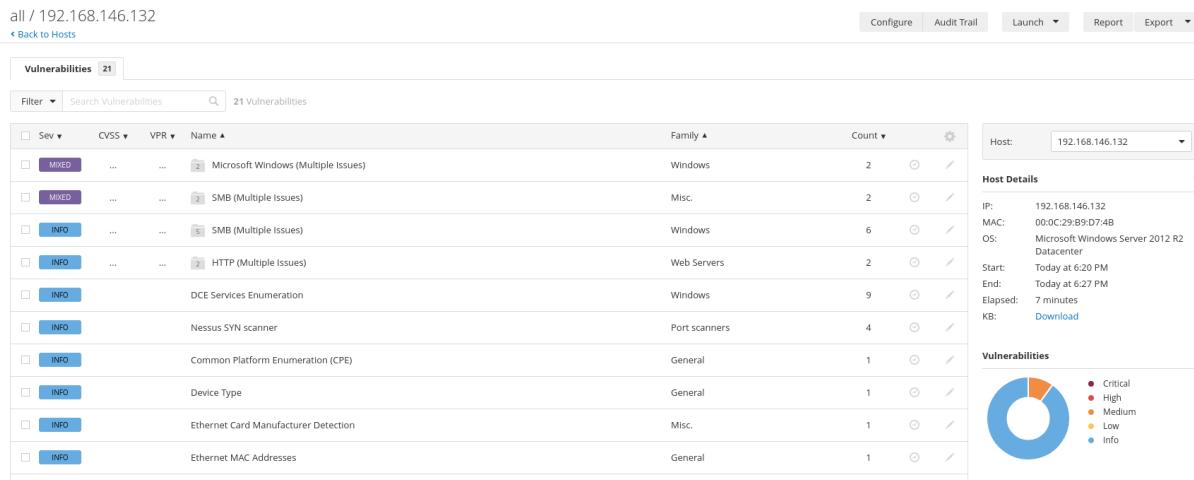
Sau khi hoàn thành dò quét các thiết bị thuộc cùng dải mạng, thu được một số kết quả như sau:

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.

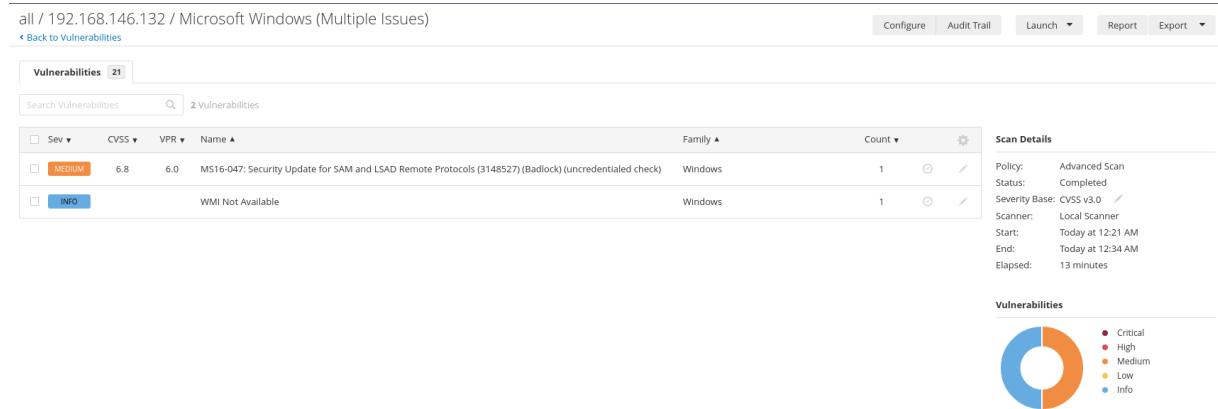
a) Đánh giá trên windows server 2012



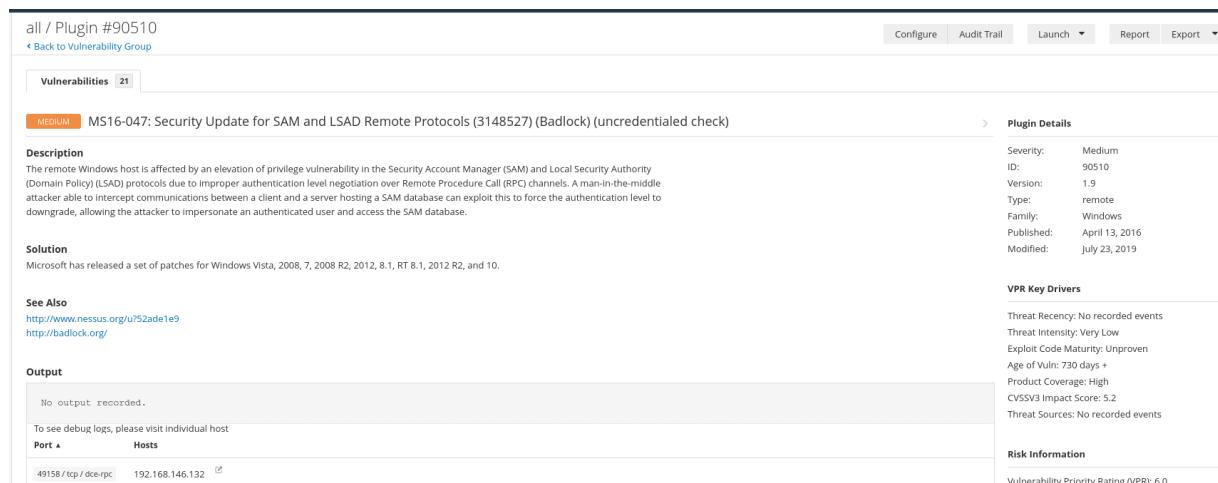
Hình 3.7 Kết quả dò quét trên Windows Server 2012

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)



Hình 3.8 Các lỗ hổng của Microsoft Windows



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 dữ liệu SAM, khai thác điều này để hạ cấp xác thực, cho phép kẻ tấn công mạo danh người dùng.

| Plugin Details | | Risk Information |
|--|----------------|--|
| Severity: | Medium | Vulnerability Priority Rating (VPR): 6.0 |
| ID: | 90510 | Risk Factor: Medium |
| Version: | 1.9 | CVSS v3.0 Base Score 6.8 |
| Type: | remote | CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N /UI:R/S:U/C:H/I:H/A:N |
| Family: | Windows | CVSS v3.0 Temporal Vector: CVSS:3.0/E:U /RL:O/RC:C |
| Published: | April 13, 2016 | CVSS v3.0 Temporal Score: 5.9 |
| Modified: | July 23, 2019 | CVSS v2.0 Base Score: 5.8 |
| VPR Key Drivers | | CVSS v2.0 Temporal Score: 4.3 |
| Threat Recency: No recorded events | | CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P /I:P/A:N |
| Threat Intensity: Very Low | | CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C |
| Exploit Code Maturity: Unproven | | IAVM Severity: I |
| Age of Vuln: 730 days + | | |
| Product Coverage: High | | |
| CVSSV3 Impact Score: 5.2 | | |
| Threat Sources: No recorded events | | |
| Reference Information | | Vulnerability Information |
| CERT: 813296 | | CPE: cpe:/o:microsoft:windows |
| MSFT: MS16-047 | | Exploit Available: false |
| BID: 86002 | | Exploit Ease: No known exploits are available |
| IAVA: 2016-A-0093 | | Patch Pub Date: April 12, 2016 |
| MSKB: 3148527 , 3149090 , 3147461 , 3147458 , 3148527 , 3149090 , 3147461 , 3147458 | | Vulnerability Pub Date: March 23, 2016 |
| CVE: CVE-2016-0128 | | In the news: true |

Hình 3.10 Đánh giá về MS16-047 của Nessus

The screenshot shows the Nessus interface with the following details:

- Vulnerabilities**: 21
- MEDIUM** SMB Signing not required
- Description**: Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.
- Solution**: Enforce message signing in the host's configuration. On Windows, this is found in the policy setting "Microsoft network server: Digitally sign communications (always)". On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
- See Also**: <http://www.nessus.org/ndf39b8b3>, <http://technet.microsoft.com/en-us/library/cc731957.aspx>, <http://www.nessus.org/t74b80723>, <https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>, <http://www.nessus.org/ura:sc4e6a>
- Output**: No output recorded.
- Port × Hosts**: Port 445 / tcp / nfss, 192.168.146.132
- Plugin Details** (right side):
 - Severity: Medium
 - ID: 57608
 - Version: 1.20
 - Type: remote
 - Family: Misc.
 - Published: January 19, 2012
 - Modified: October 5, 2022
- Risk Information** (right side):
 - Risk Factor: Medium
 - CVSS v3.0 Base Score 5.3**
 - CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N
/UI:N/S:U/C:H/I:A:N
 - CVSS v3.0 Temporal Vector: CVSS:3.0/E:U
/RL:O/RC:C
 - CVSS v3.0 Temporal Score: 4.6
 - CVSS v2.0 Base Score: 5.0
 - CVSS v2.0 Temporal Score: 3.7
 - CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N
/I:P/A:N
 - CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

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.

Plugin Details

| | |
|------------|------------------|
| Severity: | Medium |
| ID: | 57608 |
| Version: | 1.20 |
| Type: | remote |
| Family: | Misc. |
| Published: | January 19, 2012 |
| Modified: | October 5, 2022 |

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score 5.3

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N
/UI:N/S:U/C:N/I:L/A:N

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U
/RL:O/RC:C

CVSS v3.0 Temporal Score: 4.6

CVSS v2.0 Base Score: 5.0

CVSS v2.0 Temporal Score: 3.7

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N
/I:P/A:N

CVSS v2.0 Temporal Vector:
CVSS2#E:U/RL:OF/RC:C

Hình 3.12 Đánh giá về lỗ hổng MSB

b) Đánh giá trên windows 7

all / 192.168.146.133

Configure Audit Trail Launch Report Export

Back to Hosts

Vulnerabilities 19

Filter Search Vulnerabilities 19 Vulnerabilities

| Sev | CVSS | VPR | Name | Family | Count | Actions |
|-------|---|-----|-------------------------------------|---------------|-------|---------|
| MIXED | ... | ... | Microsoft Windows (Multiple Issues) | Windows | 4 | ○/○/○/○ |
| MIXED | ... | ... | SMB (Multiple Issues) | Misc. | 2 | ○/○/○/○ |
| INFO | ... | ... | SMB (Multiple Issues) | Windows | 7 | ○/○/○/○ |
| INFO | DCE Services Enumeration | | | Windows | 8 | ○/○/○/○ |
| INFO | Nessus SYN scanner | | | Port scanners | 3 | ○/○/○/○ |
| INFO | Common Platform Enumeration (CPE) | | | General | 1 | ○/○/○/○ |
| INFO | Device Type | | | General | 1 | ○/○/○/○ |
| INFO | Ethernet Card Manufacturer Detection | | | Misc. | 1 | ○/○/○/○ |
| INFO | Ethernet MAC Addresses | | | General | 1 | ○/○/○/○ |
| INFO | ICMP Timestamp Request Remote Date Disclosure | | | General | 1 | ○/○/○/○ |

Host: 192.168.146.133

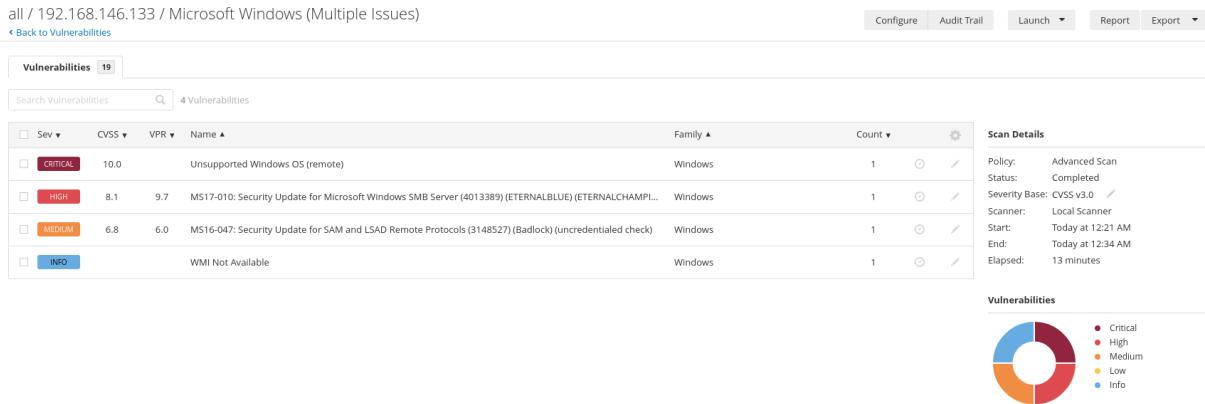
Host Details

- IP: 192.168.146.133
- MAC: 00:0C:29:A6:AC:A7
- OS: Microsoft Windows 7 Ultimate
- Start: Today at 12:22 AM
- End: Today at 12:25 AM
- Elapsed: 3 minutes
- KB: Download

Vulnerabilities

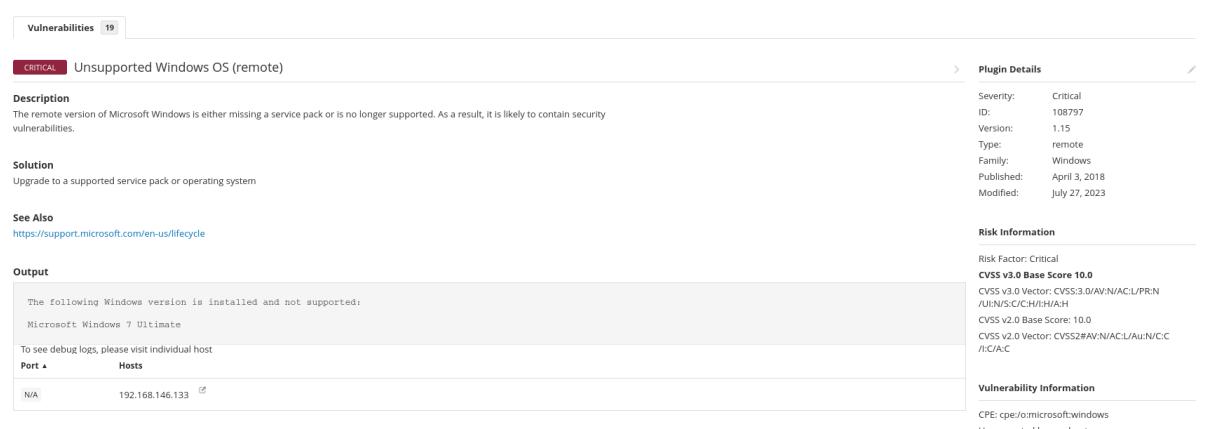
Hình 3.13 Kết quả quét trên Windows 7

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.



Hình 3.14 Lỗ hổng của Windows 7

Với 1 lỗi ở mức 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 xuất hiện tại phiên bản Windows này.



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.

| Vulnerabilities | 19 |
|--|--|
| MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNTERGY) | |
| Description | |
| The remote Windows host is affected by the following vulnerabilities: | |
| - Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) | Severity: High ID: 97833 Version: 1.30 Type: remote Family: Windows Published: March 20, 2017 Modified: May 25, 2022 |
| - An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147) | |
| ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNTERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE. | VRP Key Drivers Threat Recency: No recorded events Threat Intensity: Very Low Exploit Code Maturity: High Age of Vuln: 730 days + Product Coverage: Low CVSSv3 Impact Score: 5.9 Threat Sources: Security Research |
| Solution | |
| Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8. | Risk Information Vulnerability Priority Rating (VPR): 9.7 Risk Factor: High |

Hình 3.16 Lỗ hổng MS17-010

Lỗ hổng MS17-010 được đánh giá ở mức độ nghiêm trọng 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.

Hình 3.17 Thông tin thêm về lô hồng MS17-010

| Plugin Details | | Risk Information | Exploitable With |
|----------------------------------|---|---|---|
| Severity: | High | Vulnerability Priority Rating (VPR): 9.7 | Metasploit (SMB DOUBLEPULSAR Remote Code Execution) |
| ID: | 97833 | Risk Factor: High | CANVAS () |
| Version: | 1.30 | CVSS v3.0 Base Score 8.1 | Core Impact |
| Type: | remote | CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/U:U/S:U/C:H/I:H/A:H | |
| Family: | Windows | CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C | |
| Published: | March 20, 2017 | CVSS v3.0 Temporal Score: 7.7 | |
| Modified: | May 25, 2022 | CVSS v2.0 Base Score: 9.3 | |
| VPR Key Drivers | | CVSS v2.0 Temporal Score: 8.1 | |
| Threat Recency: | No recorded events | CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:I/C:A:C | |
| Threat Intensity: | Very Low | CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C | |
| Exploit Code Maturity: | High | IAVM Severity: I | |
| Age of Vuln: | 730 days + | | |
| Product Coverage: | Low | | |
| CVSSV3 Impact Score: | 5.9 | | |
| Threat Sources: | Security Research | | |
| Vulnerability Information | | | |
| CPE: | cpe:/o:microsoft:windows | | |
| Exploit Available: | true | | |
| Exploit Ease: | Exploits are available | | |
| Patch Pub Date: | March 14, 2017 | | |
| Vulnerability Pub Date: | March 14, 2017 | | |
| In the news: | true | | |
| Reference Information | | | |
| EDB-ID: | 41891 , 41987 | | |
| MSFT: | MS17-010 | | |
| BID: | 96703 , 96704 , 96705 , 96706 , 96707 , 96709 | | |
| CISA-KNOWN-EXPLOITED: | 2022/05/03, 2022/08/10, 2022/04/15, 2022/04/27, 2022/06/14 | | |
| IAVA: | 2017-A-0065 | | |
| MSKB: | 4012212 , 4012213 , 4012214 , 4012215 , 4012216 , 4012217 , 4012606 , 4013198 , 4013429 , 4012598 , 4012212 , 4012213 , 4012214 , 4012215 , 4012216 , 4012217 , 4012606 , 4013198 , 4013429 , 4012598 | | |
| CVE: | CVE-2017-0143 , CVE-2017-0144 , CVE-2017-0145 , CVE-2017-0146 , CVE-2017-0147 , CVE-2017-0148 | | |

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 họa 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 HỒNG - Vacif.com](#)
- [3] [Dánh 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? \(thuvienphapluat.vn\)](#)
- [4] [OpenVAS công cụ đánh giá lỗ hổng bảo mật mã nguồn mở - Cú Đêm Solutions \(cudem.info\)](#)
- [5] [Qualys Documentation: Release Notes, User Guides & more | Qualys](#)
- [6] [Các chức năng của công cụ quét bảo mật mạng Nessus và cách cài đặt - Cú Đêm Solutions \(cudem.info\)](#)
- [7] [Welcome to Tenable Nessus 10.3.x \(Tenable Nessus 10.3\)](#)

PHỤ LỤC

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

| STT | Mô tả | Ký hiệu |
|-----------|--|---------|
| I | Nhóm các mối đe dọa từ việc tồn tại, điểm yếu, lỗ hổng trong hệ thống | |
| 1.1 | Thiết bị hệ thống tấn công truy cập trái phép, chiếm quyền điều khiển | Th-V01 |
| 1.2 | Máy chủ hệ thống bị truy cập trái phép, chiếm quyền điều khiển | Th-V02 |
| 1.3 | Ứng dụng, dịch vụ bị truy cập trái phép, chiếm quyền điều khiển | Th-V03 |
| 1.3 | Dữ liệu trên máy chủ bị bị truy cập, sửa, xóa trái phép | Th-V04 |
| 1.4 | Dữ liệu trên ứng dụng/dịch vụ bị truy cập, sửa, xóa trái phép | Th-V05 |
| II | Nhóm các mối đe dọa từ việc thiếu/không đáp ứng các biện pháp quản lý | |
| 2.1 | Ban Lãnh đạo không nhận thức đúng về tầm quan trọng của bảo đảm an toàn thông tin cho hệ thống | Th-M01 |
| 2.2 | Thiếu nguồn lực để triển khai các biện pháp bảo vệ cho hệ thống | Th-M02 |
| 2.3 | Người sử dụng không có kỹ năng cơ bản để tự bảo vệ khi sử dụng mạng | Th-M03 |
| 2.4 | Người sử dụng nhận thức hạn chế về các nguy cơ, rủi ro mất an toàn thông tin | Th-M04 |
| 2.5 | Chính sách, quy định về quản lý an toàn mạng không được tuân thủ theo quy định | Th-M05 |
| 2.6 | Chính sách, quy định về an toàn máy chủ và ứng dụng không được tuân thủ theo quy định | Th-M06 |
| 2.7 | Chính sách, quy định về an toàn dữ liệu không được tuân thủ theo quy định | Th-M07 |

| | | |
|------|---|--------|
| 2.8 | Chính sách, quy định về an toàn thiết bị đầu cuối không được tuân thủ theo quy định | Th-M08 |
| 2.9 | Chính sách, quy định về phòng chống phần mềm độc hại không được tuân thủ theo quy định | Th-M09 |
| 2.10 | Chính sách, quy định về quản lý điểm yếu an toàn thông tin không được tuân thủ theo quy định | Th-M10 |
| 2.11 | Chính sách, quy định về quản lý giám sát an toàn hệ thống thông tin không được tuân thủ theo quy định | Th-M11 |
| 2.12 | Chính sách, quy định về quản lý sự cố an toàn thông tin không được tuân thủ theo quy định | Th-M12 |
| 2.13 | Chính sách, quy định về quản lý an toàn người sử dụng đầu cuối không được tuân thủ theo quy định | Th-M13 |

| | | |
|------------|---|--------|
| III | Nhóm các mối đe dọa từ việc thiếu/không đáp ứng các biện pháp kỹ thuật | |
| 3.1 | Hệ thống bị tấn công, chiếm quyền điều khiển từ xa | Th-T01 |
| 3.2 | Hệ thống hoạt động không ổn định, thường xuyên bị gián đoạn hoạt động | Th-T02 |
| 3.3 | Hệ thống bị lợi dụng, tấn công các hệ thống thông tin khác | Th-T05 |
| 3.4 | Hệ thống bị truy cập, xóa, sửa thông tin trái phép | Th-T06 |

Nhận biết về mối đe dọa

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

| STT | Điểm yếu | Kí hiệu |
|------|---|---------|
| I | Nhóm điểm yếu liên quan đến tồn tại lỗ hổng, điểm yếu an toàn thông tin | |
| 1.1 | Tồn tại điểm yếu trên hệ điều hành máy chủ | V01 |
| 1.2 | Tồn tại điểm yếu trên hệ điều hành máy trạm | V02 |
| 1.3 | Tồn tại điểm yếu trên ứng dụng | V03 |
| 1.4 | Tồn tại điểm yếu trên hệ quản trị cơ sở dữ liệu | V04 |
| 1.5 | Tồn tại điểm yếu trên firmware thiết bị mạng, thiết bị bảo mật | V05 |
| 1.6 | Tồn tại điểm yếu trên ứng dụng hệ thống (DNS, DHCP, SSO,..) | V06 |
| 1.7 | Tồn tại điểm yếu của các giao thức mạng | V07 |
| 1.8 | Tồn tại điểm yếu của các thư viện lập trình | V08 |
| II | Nhóm điểm yếu liên quan đến biện pháp quản lý | |
| 2.1 | Không xác định các mục tiêu, nguyên tắc bảo đảm an toàn thông tin. | M01 |
| 2.2 | Không xác định trách nhiệm của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về an toàn thông tin và các đối tượng liên quan | M02 |
| 2.3 | Không xác định phạm vi của hệ thống thông tin cần quản lý | M03 |
| 2.4 | Không xác định các ứng dụng, dịch vụ hệ thống cung cấp | M04 |
| 2.5 | Không có chính sách, quy định về nguồn nhân lực bảo đảm an toàn thông tin | M05 |
| 2.6 | Không có chính sách, quy định về quản lý an toàn mạng. | M06 |
| 2.7 | Không có chính sách, quy định về an toàn máy chủ và ứng dụng | M07 |
| 2.8 | Không có chính sách, quy định về an toàn dữ liệu | M08 |
| 2.9 | Không có chính sách, quy định về an toàn thiết bị đầu cuối | M09 |
| 2.10 | Không có chính sách, quy định về phòng chống phần mềm độc hại | M10 |

| | | |
|------|--|-----|
| 2.11 | Không có chính sách, quy định về quản lý điểm yếu an toàn thông tin | M11 |
| 2.12 | Không có chính sách, quy định về quản lý giám sát an toàn hệ thống thông tin | M12 |
| 2.13 | Không có chính sách, quy định về quản lý sự cố an toàn thông tin | M13 |
| 2.14 | Không có chính sách, quy định về quản lý an toàn người sử dụng đầu cuối | M14 |
| 2.15 | Không có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng | M19 |
| 2.16 | Không có chính sách, quy định về tổ chức đào tạo về an toàn thông tin cho người sử dụng | M20 |
| 2.17 | Không có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc | M21 |
| 2.18 | Không có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin | M22 |
| 2.19 | Không có chính sách, quy định về kiểm thử phần mềm trên môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng | M23 |

| | | |
|------|--|-----|
| 2.20 | Không có chính sách, quy định về kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng | M24 |
| 2.21 | Không có chính sách, quy định về thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng | M25 |
| 2.22 | Không có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống | M26 |
| 2.23 | Không có chính sách, quy định về quản lý, vận hành hoạt động bình thường của hệ thống | M27 |
| 2.24 | Không có chính sách, quy định về cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố | M28 |
| 2.25 | Không có chính sách, quy định về truy cập và quản lý cấu hình hệ thống | M29 |
| 2.26 | Không có yêu cầu an toàn đối với phương pháp mã hóa | M30 |

| | | |
|------|--|-----|
| 2.27 | Không có chính sách, quy định về phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa | M31 |
| 2.28 | Không có chính sách, quy định về kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa | M32 |
| 2.45 | Không có chính sách, quy định về cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống | M33 |
| 2.29 | Không có chính sách, quy định về cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng | M34 |
| 2.30 | Không có chính sách, quy định về gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động | M35 |
| 2.31 | Không có chính sách, quy định về thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống | M36 |
| 2.32 | Không có quy định truy cập và quản trị hệ thống giám sát | M37 |

| III | Nhóm các điểm yếu liên quan đến biên pháp kỹ thuật | |
|------------|--|-----|
| 3.1 | Không có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn | T01 |
| 3.2 | Không có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập | T02 |

| | | |
|------|---|-----|
| 3.3 | Không có phương án cân bằng tải, dự phòng nóng cho các thiết bị mạng | T03 |
| 3.4 | Không có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu | T04 |
| 3.5 | Không có phương án chặn lọc phần mềm độc hại trên môi trường mạng | T05 |
| 3.6 | Không có phương án phòng chống tấn công từ chối dịch vụ | T06 |
| 3.7 | Không có phương án giám sát hệ thống thông tin tập trung | T07 |
| 3.8 | Không có phương án giám sát an toàn hệ thống thông tin tập trung | T08 |
| 3.9 | Không có phương án quản lý sao lưu dự phòng tập trung | T09 |
| 3.10 | Không có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung | T10 |
| 3.11 | Không có phương án phòng, chống thất thoát dữ liệu | T11 |
| 3.12 | Không có phương án dự phòng kết nối mạng Internet | T12 |
| 3.13 | Không có phương án bảo đảm an toàn cho mạng không dây | T13 |
| 3.14 | Không có phương án quản lý tài khoản đặc quyền | T14 |
| 3.15 | Không có phương án dự phòng hệ thống ở vị trí địa lý khác nhau | T15 |
| 3.16 | Không có phương án dự phòng cho kết nối mạng giữa hệ thống chính và hệ thống dự phòng | T16 |
| 3.18 | Không có biện pháp kiểm soát truy cập từ bên ngoài vào hệ thống | T18 |
| 3.19 | Không phân quyền và cấp quyền truy cập từ bên ngoài vào hệ thống | T19 |
| 3.20 | Không có phương án kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ | T20 |
| 3.21 | Không lưu trữ và quản lý tập trung nhật ký hệ thống thu thập được từ các thiết bị hệ thống; | T21 |

| | | |
|------|---|-----|
| 3.22 | Không có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống. | T23 |
| 3.24 | Hệ thống không có phương án cân bằng tải và dự phòng nóng | T24 |
| 3.25 | Không thiết lập cấu hình để vô hiệu hóa tài khoản nếu tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định; | T25 |
| 3.26 | Không thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối đến hệ thống | T26 |
| 3.25 | Không thay đổi cổng quản trị mặc định của máy chủ | T25 |
| 3.26 | Không sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ | T26 |
| 3.27 | Không có phương án cập nhật bản vá, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ. | T27 |
| 3.51 | Không thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng. | T51 |
| 3.28 | Không có biện pháp quản lý tập trung việc cập nhật và xử lý bản vá, điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ. | T28 |
| 3.29 | Không thực hiện cấu hình tối ưu, tăng cường bảo mật cho máy chủ trước khi đưa vào sử dụng. | T29 |
| 3.30 | Không có biện pháp phòng chống xâm nhập trên máy chủ và kiểm tra tính nguyên vẹn của các tập tin hệ thống | T30 |
| 3.31 | Không có phương án kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt | T31 |
| 3.32 | Không có cơ chế kiểm tra, xử lý mã độc của các phương tiện lưu trữ di động trước khi kết nối với máy chủ. | T32 |
| 3.33 | Không có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF. | T33 |
| 3.34 | Không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng | T34 |
| 3.35 | Không có phương án chuyên dụng để quản lý, lưu trữ dữ liệu trong hệ thống bảo đảm tính nguyên vẹn. | T35 |

| | | |
|------|---|-----|
| 3.36 | Không có phương án giám sát, cảnh báo khi có thay đổi thông tin, dữ liệu lưu trên hệ thống lưu trữ/phương tiện lưu trữ. | T36 |
| 3.37 | Không có phương án khôi phục tính nguyên vẹn của thông tin dữ liệu. | T37 |
| 3.38 | Không có hệ thống/phương tiện lưu trữ độc lập để sao lưu dự phòng. | T38 |

Nhận biết về điểm yếu

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

| TT | Tên tài sản | Điểm yếu | Mối đe dọa |
|-----------|---|---|--|
| 1 | Cổng thông tin nội bộ cấp độ 1 | V01: Tồn tại điều yếu trên hệ điều hành máy chủ | Th-V02: Máy chủ hệ thống bị truy cập trái phép, chiếm quyền điều khiển |
| | | M02: Không có chính sách, quy định về quản lý an toàn mạng | Th-M05: Chính sách, quy định về quản lý an toàn mạng không được tuân thủ theo quy định |
| | | T06: Không có phương án phòng chống tấn công từ chối dịch vụ | Th-T02: Hệ thống hoạt động không ổn định, thường xuyên bị gián đoạn hoạt động |
| 2 | Hệ thống quản lý văn bản và điều hành cấp độ 2 | V03: Tồn tại điều yếu trên ứng dụng | Th-V03: Ứng dụng, dịch vụ bị truy cập trái phép, chiếm quyền điều khiển |
| | | M07: Không có chính sách, quy định về an toàn máy chủ và ứng dụng | Th-M06: Chính sách, quy định về an toàn máy chủ và ứng dụng không được tuân thủ theo quy định |
| | | T02: Không có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập | Th-T01: Hệ thống bị tấn công, chiếm quyền điều khiển từ xa |
| 4 | phục vụ phát triển Chính phủ điện tử cấp độ 4 | M24: Không có chính sách, quy định về kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng | Th-M10: Chính sách, quy định về quản lý điểm yếu an toàn thông tin không được tuân thủ theo quy định |
| | | T07: Không có phương án giám sát hệ thống thông tin tập trung | Th-T02: Hệ thống hoạt động không ổn định, thường xuyên bị gián đoạn hoạt động |
| 5 | Hệ thống thông tin phục vụ lưu trữ dữ liệu tập trung đối với một số loại hình thông tin, dữ liệu đặc biệt quan trọng của quốc gia | V04: Tồn tại điều yếu trên hệ quản trị cơ sở dữ liệu | Th-V05: Dữ liệu trên ứng dụng/dịch vụ bị truy cập, sửa, xóa trái phép |
| | | M08: Không có chính sách, quy định về an toàn dữ liệu | Th-M07: Chính sách, quy định về an toàn dữ liệu không được tuân thủ theo quy định |
| | | T11: Không có phương án phòng, chống thất thoát dữ liệu | Th-T06: Hệ thống bị truy cập, xóa, sửa thông tin trái phép |

Xác định điểm yếu và mối đe dọa