**** TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

VÀ TRUYỀN THÔNG VIỆT - HÀN

**KHOA KỸ THUẬT MÁY TÍNH VÀ ĐIỆN TỬ**

**🙠🙠🕮🙢🙢**

**BÁO CÁO**

**BẢO MẬT VÀ AN TOÀN HỆ THỐNG THÔNG TIN**

**TÊN ĐỀ TÀI**

**Tìm hiểu và triển khai công cụ Network monitoring system trên Pandora FSM**

**Sinh viên thực hiện : Trần Thị Phương  
 Nguyễn An Phúc**

**Võ Mạnh Quân**

**Nguyễn Thanh Phúc**

**Lớp học phần : Inforsec 7**

**Giảng viên hướng dẫn : TS. Hoàng Hữu Đức**

***Đà Nẵng, tháng 5 năm 2024***

**** TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

VÀ TRUYỀN THÔNG VIỆT - HÀN

**KHOA KỸ THUẬT MÁY TÍNH VÀ ĐIỆN TỬ**

**🙠🙠🕮🙢🙢**

**BÁO CÁO**

**BẢO MẬT VÀ AN TOÀN HỆ THỐNG THÔNG TIN**

**TÊN ĐỀ TÀI**

**Tìm hiểu và triển khai công cụ Network monitoring system trên Pandora FSM**

**Sinh viên thực hiện : Trần Thị Phương**

**Nguyễn An Phúc**

**Võ Mạnh Quân**

**Nguyễn Thanh Phúc**

**Lớp học phần : Inforsec 7**

**Giảng viên hướng dẫn :** **TS. Hoàng Hữu Đức**

***Đà Nẵng, tháng 5 năm 2024***

**NHẬN XÉT**

***Đà Nẵng, tháng 05 năm 2024***

***Giảng viên hướng dẫn***

*(Ký, ghi rõ họ tên)*

**LỜI CẢM ƠN**

Chúng em xin chân thành cảm ơn quý thầy cô giáo của trường Đại học Công nghệ thông tin và truyền thông Việt-Hàn, đặc biệt là thầy TS.Hoàng Hữu Đức, giảng viên hướng dẫn của tôi, đã tận tình hướng dẫn, chỉ bảo và động viên chúng em trong suốt quá trình thực hiện báo cáo môn học này.

Những bài giảng của thầy không chỉ là nguồn kiến thức chất lượng mà còn là nguồn động viên và truyền cảm hứng lớn lao. Thầy luôn tạo điều kiện cho học viên có cơ hội phát triển và thể hiện bản thân mình, từ đó giúp chúng tôi tự tin hơn trong học tập và cuộc sống.

Sự nhiệt tình và tận tâm của thầy không bao giờ làm chúng tôi thất vọng. Thầy luôn sẵn lòng chia sẻ kiến thức và kinh nghiệm, giúp chúng tôi hiểu rõ hơn về chủ đề và phương pháp học tập.

Đến nay, chúng tôi rất may mắn khi có cơ hội được học hỏi dưới sự dẫn dắt của thầy/cô. Sự đóng góp của quý thầy/cô không chỉ là niềm tự hào của trường học mà còn là nguồn động viên lớn lao cho tất cả học viên.

Một lần nữa, tôi xin chân thành cảm ơn quý thầy về sự tận tâm và hiệu quả trong việc dạy dỗ chúng tôi.

**Sinh viên thực hiện**

**Trần Thị Phương**

**Nguyễn An Phúc**

**Võ Mạnh Quân**

**Nguyễn Thanh Phúc**

MỤC LỤC

DANH MỤC HÌNH ẢNH

[Hình 1. 1 Các thuộc tính cần bảo vệ của tài sản thông tin 1](#_Toc166694286)

[Hình 1. 2 Các thành phần chính của An toàn thông tin 2](#_Toc166694287)

[Hình 1. 3 Mô hình hệ thống thông tin của cơ quan, tổ chức 3](#_Toc166694288)

[Hình 1. 4 Các thành phần của hệ thống thông tin và an toàn 4](#_Toc166694289)

[Hình 1. 5Một văn bản được đóng dấu Confidential 4](#_Toc166694290)

[Hình 1. 6 Đảm bảo tính bí mật bằng đường hầm VPN 5](#_Toc166694291)

[Hình 1. 7Minh họa tính sẵn dùng 6](#_Toc166694292)

[Hình 1. 8 Phân bố lỗ hổng bảo mật trong các thành phần của hệ thống 6](#_Toc166694293)

[Hình 1. 9 Hệ thống rà quét, kiểm tra, đánh giá lỗ hổng 8](#_Toc166694294)

[Hình 1. 10 Kết quả quét của Microsoft Baseline Security Analyzer 9](#_Toc166694295)

[Hình 1. 11 Giao diện của công cụ Zenmap 9](#_Toc166694296)

[Hình 1. 12 Sử dụng Wireshark để bắt gói tin 10](#_Toc166694297)

[Hình 1. 13 Mô đun Keylogger phần cứng 11](#_Toc166694298)

[Hình 1. 14 Tấn công nghe lén 13](#_Toc166694299)

[Hình 1. 15 Tấn công pharming thông qua máy chủ DNS 13](#_Toc166694300)

[Hình 1. 16 Mô hình tấn công kiểu người đứng giữa 14](#_Toc166694301)

[Hình 1. 17 Minh họa virus máy tính 15](#_Toc166694302)

[Hình 2. 1 Phần mềm giám sát Pandora FMS 17](#_Toc167376877)

[Hình 2. 2 Giao diện bắt đầu của Pandora FMS 21](#_Toc167376878)

[Hình 2. 3 Các điều khoản cấp phép 21](#_Toc167376879)

[Hình 2. 4 Các phụ thuộc phần mềm 22](#_Toc167376880)

[Hình 2. 5 Tạo cơ sở dữ liệu mới 22](#_Toc167376881)

[Hình 2. 6 Cấu hình cơ sở dữ liệu thành công 23](#_Toc167376882)

[Hình 2. 7 Bảng điều khiển Pandora 23](#_Toc167376883)

[Hình 2. 8 Màn hình sau khi đăng nhập 24](#_Toc167376884)

[Hình 2. 9 Máy chủ Pandora FMS 24](#_Toc167376885)

DANH MỤC TỪ VIẾT TẮT

|  |  |
| --- | --- |
| CNTT | Công nghệ thông tin |
| SQL | Structured Query Language |
| SMTP | Simple Mail Transfer Protocol |
| DNS | Domain Name System |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| SNMP | Simple Network Management Protocol |
| ICMP | Internet Control Message Protocol |
| UDP | User Datagram Protocol |

PHẦN MỞ ĐẦU

Trong thời đại công nghệ thông tin phát triển như hiện nay, việc truy cập internet là một nhu cầu thiết yếu của con người. Để đáp ứng nhu cầu này, việc xây dựng một hệ thống wifi ổn định, an toàn và hiệu quả là rất quan trọng. Trong số các thiết bị wifi hiện có trên thị trường, AP unifi và controller bằng phần mềm là một giải pháp tiên tiến và được nhiều doanh nghiệp lựa chọn. Để tìm hiểu và triển khai hệ thống wifi với AP unifi và controller bằng phần mềm, em đã được thực tập tại Trung tâm CNTT VKU trong vòng 2 tháng. Qua quá trình thực tập, em đã được học hỏi và trải nghiệm rất nhiều kiến thức và kỹ năng liên quan đến lĩnh vực này. Em xin trình bày kết quả của quá trình thực tập trong báo cáo này với đề tài: “Tìm hiểu và triển khai hệ thống wifi với AP unifi và controller bằng phần mềm”.

Báo cáo gồm có 3 phần chính như sau:

Chương 1: Tổng quan về bảo mật hệ thống thông tin

Chương 2: Giới thiệu phần mềm Pandora FMS

Chương 3: Ứng dụng thực nghiệm

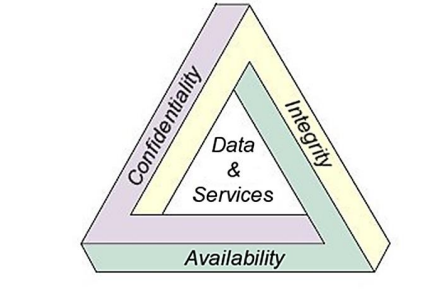
Chúng em xin gửi lời cảm ơn chân thành đến thầy giáo TS.Hoàng Hữu Đức trong quá trình thực hiện nghiên cứu, thực hiện đề tài đã định hướng và hướng dẫn nhiệt tình để chúng em có thể hoàn thành báo cáo thực tập này được đầy đủ nhất. Mong thầy luôn luôn hạnh phúc và gặt hái được nhiều thành công trong sự nghiệp giảng dạy của thầy.

Trong quá trình thực hiện và hoàn thành báo cáo có nhiều sai sót, mong sự đóng góp ý kiến của thầy cô để báo cáo thực tập doanh nghiệp đầu tiên của em hoàn thiện hơn và có kinh nghiệp hơn cho những lần thực tập tiếp theo.

CHƯƠNG 1: TỔNG QUAN VỀ BẢO MẬT HỆ THỐNG

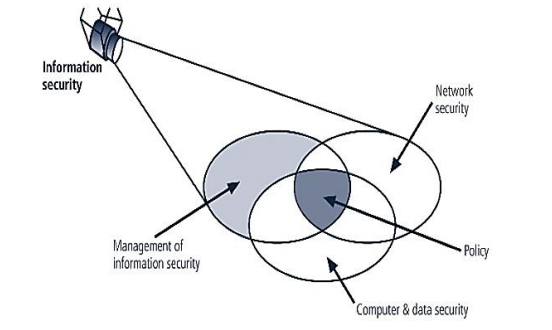
THÔNG TIN

* 1. Khái quát về an toàn thông tin
     1. An toàn thông tin là gì?
* An toàn thông tin (Information security) là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép.
* Theo cuốn Principles of Information Security, An toàn thông tin là việc bảo vệ các thuộc tính bí mật (confidentiality), tính toàn vẹn (integrity) và tính sẵn dùng (availability) của các tài sản thông tin trong quá trình chúng được lưu trữ, xử lý, hoặc truyền tải.



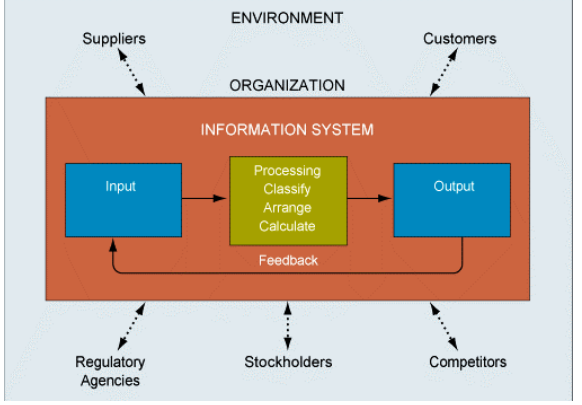
Hình 1. 1 Các thuộc tính cần bảo vệ của tài sản thông tin

* An toàn thông tin gồm hai lĩnh vực chính là An toàn công nghệ thông tin (Information technology security, hay IT security) và Đảm bảo thông tin (Information assurance). An toàn công nghệ thông tin, hay còn gọi là An toàn máy tính (Computer security) là việc đảm bảo an toàn cho các hệ thống công nghệ thông tin, bao gồm các hệ thống máy tính và mạng, chống lại các cuộc tấn công phá hoại. Đảm bảo thông tin là việc đảm bảo thông tin không bị mất khi xảy ra các sự cố, như thiên tai, hỏng hóc, trộm cắp, phá hoại,… Đảm bảo thông tin thường được thực hiện sử dụng các kỹ thuật sao lưu ngoại vi (offsite 13 backup), trong đó dữ liệu thông tin từ hệ thống gốc được sao lưu ra các thiết bị lưu trữ vật lý đặt ở một vị trí khác.
* Một số khái niệm khác trong an toàn thông tin:
  + Truy nhập (Access) là việc một chủ thể, người dùng hoặc một đối tượng có khả năng sử dụng, xử lý, sửa đổi, hoặc gây ảnh hưởng đến một chủ thể, người dùng hoặc một đối tượng khác. Trong khi người dùng hợp pháp có quyền truy nhập hợp pháp đến một hệ thống thì tin tặc truy nhập bất hợp pháp đến hệ thống.
  + Tài sản (Asset) là tài nguyên của các tổ chức, cá nhân được bảo vệ. Tài sản có thể là tài sản lô gíc, như một trang web, thông tin, hoặc dữ liệu. Tài sản có thể là tài sản vật lý, như hệ thống máy tính, thiết bị mạng, hoặc các tài sản khác.
  + Tấn công (Attack) là hành động có chủ ý hoặc không có chủ ý có khả năng gây hại, hoặc làm thỏa hiệp các thông tin, hệ thống và các tài sản được bảo vệ. Tấn công có thể chủ động hoặc thụ động, trực tiếp hoặc gián tiếp.
    1. Các thành phần của an toàn thông tin
* An toàn thông tin có thể được chia thành ba thành phần chính: an toàn máy tính và dữ liệu (Computer & data security), an ninh mạng (Network security) và quản lý an toàn thông tin (Management of information security)



Hình 1. 2 Các thành phần chính của An toàn thông tin

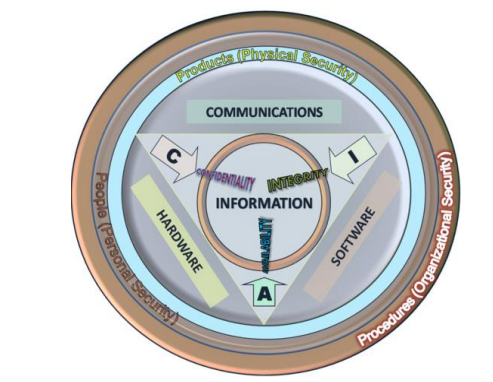
* **An ninh mạng** là việc đảm bảo an toàn cho hệ thống mạng và các thông tin truyền tải trên mạng, chống lại các tấn công, xâm nhập trái phép.
* **Quản lý an toàn thông tin** là việc quản lý và giám sát việc thực thi các biện pháp đảm bảo an toàn thông tin, giúp nâng cao hiệu quả của chúng.
* **Chính sách an toàn thông tin** các nội quy, quy định của cơ quan, tổ chức, nhằm đảm bảo các biện pháp đảm bảo an toàn thông tin được thực thi và tuân thủ
* An toàn máy tính và dữ liệu việc đảm bảo an toàn cho hệ thống phần cứng, phần mềm và dữ liệu trên máy tính đảm bảo cho máy tính có thể vận hành an toàn, đáp ứng các yêu cầu của người sử dụng.
  1. Khái quát về an toàn hệ thống thông tin
     1. Các thành phần của hệ thống thông tin
* Hệ thống thông tin (Information system), theo cuốn sách Fundamentals of Information Systems Security [2] là một hệ thống tích hợp các thành phần nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin và chuyển giao thông tin, tri thức và các sản phẩm số. Trong nền kinh tế số, hệ thống thông tin đóng vai trò rất quan trọng trong hoạt động của các tổ chức, cơ quan và doanh nghiệp (gọi chung là tổ chức). Có thể nói, hầu hết các tổ chức đều sử dụng các hệ thống thông tin với các quy mô khác nhau để quản lý các hoạt động của mình.
* Hệ thống thông tin được sử dụng để tương tác với khách hàng (Customers), với nhà cung cấp (Suppliers), với cơ quan chính quyền (Regulatory Agencies), với cổ đông và với đối thủ cạnh tranh (Competitors). Có thể nêu là một số hệ thống thông tin điển hình như các hệ lập kế hoạch nguồn lực doanh nghiệp, các máy tìm kiếm và các hệ thống thông tin.



Hình 1. 3 Mô hình hệ thống thông tin của cơ quan, tổ chức

* Trong lớp các hệ thống thông tin, hệ thống thông tin dựa trên máy tính (Computerbased information system), hay sử dụng công nghệ máy tính để thực thi các nhiệm vụ là lớp hệ thống thông tin được sử dụng rộng rãi nhất. Hệ thống thông tin dựa trên máy tính thường gồm các thành phần:
* Phần cứng (Hardware) để thu thập, lưu trữ, xử lý và biểu diễn dữ liệu phần mềm (Software) chạy trên
* Phần cứng để xử lý dữ liệu, cơ sở dữ liệu (Databases) để lưu trữ dữ liệu
* Mạng (Networks) là hệ thống truyền dẫn thông tin/dữ liệu
* Các thủ tục (Procedures) là tập hợp các lệnh kết hợp các bộ phận nêu trên để xử lý dữ liệu, đưa ra kết quả mong muốn.
  + 1. An toàn hệ thống thông tin là gì?

An toàn hệ thống thông tin (Information systems security) là việc đảm bảo các thuộc tính an ninh, an toàn của hệ thống thông tin, bao gồm tính bí mật (confidentiality), tính toàn vẹn (integrity) và tính sẵn dùng (availability).



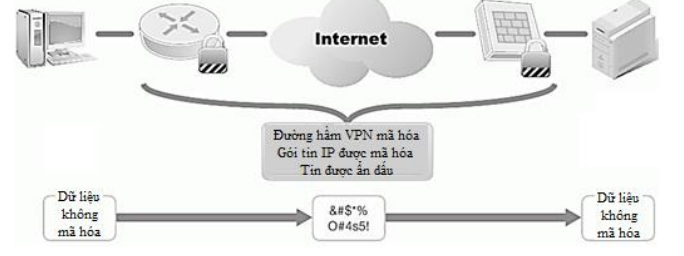
Hình 1. 4 Các thành phần của hệ thống thông tin và an toàn

* 1. Các yêu cầu đảm bảo an toàn hệ thống thông tin
     1. Bí mật
* Tính bí mật đảm bảo rằng chỉ người dùng có thẩm quyền mới được truy nhập thông tin, hệ thống. Các thông tin bí mật có thể bao gồm: (i) dữ liệu riêng của cá nhân, (ii) các thông tin thuộc quyền sở hữu trí tuệ của các doanh nghiệp hay các cơ quan, tổ chức và (iii) các thông tin có liên quan đến an ninh của các quốc gia và các chính phủ.



Hình 1. 5Một văn bản được đóng dấu Confidential

* Thông tin bí mật lưu trữ hoặc trong quá trình truyền tải cần được bảo vệ bằng các biện pháp phù hợp, tránh bị lộ lọt hoặc bị đánh cắp. Các biện pháp có thể sử dụng để đảm bảo tính bí mật của thông tin như bảo vệ vật lý, hoặc sử dụng mật mã (cryptography).



Hình 1. 6 Đảm bảo tính bí mật bằng đường hầm VPN

* + 1. Toàn vẹn

Tính toàn vẹn đảm bảo rằng thông tin và dữ liệu chỉ có thể được sửa đổi bởi những người dùng có thẩm quyền. Tính toàn vẹn liên quan đến tính hợp lệ (validity) và chính xác (accuracy) của dữ liệu. Trong nhiều tổ chức, thông tin và dữ liệu có giá trị rất lớn, như bản quyền phần mềm, bản quyền âm nhạc, bản quyền phát minh, sáng chế. Mọi thay đổi không có thẩm quyền có thể ảnh hưởng rất nhiều đến giá trị của thông tin. Thông tin hoặc dữ liệu là toàn vẹn nếu nó thỏa mãn ba điều kiện: không bị thay đổi, hợp lệ và (chính xác.

* + 1. Sẵn dùng

Tính sẵn dùng, hoặc khả dụng đảm bảo rằng thông tin, hoặc hệ thống có thể truy nhập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu. Tính sẵn dùng có thể được đo bằng các yếu tố:

- Thời gian cung cấp dịch vụ (Uptime).

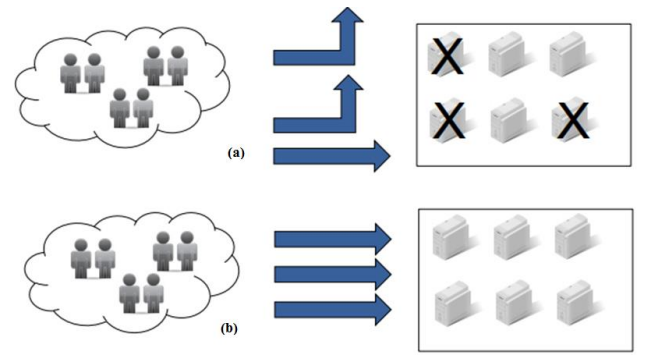
- Thời gian ngừng cung cấp dịch vụ (Downtime).

- Tỷ lệ phục vụ: A = (Uptime) / (Uptime + Downtime).

- Thời gian trung bình giữa các sự cố.

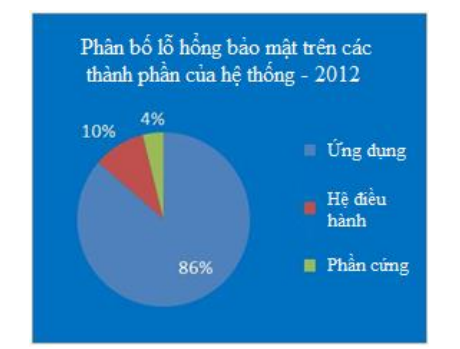
- Thời gian trung bình ngừng để sửa chữa.

- Thời gian khôi phục sau sự cố.



Hình 1. 7Minh họa tính sẵn dùng

* 1. Các dạng tấn cồn và phần mềm độc hại
     1. Khái niệm về mối đe dọa, điểm yếu, lỗ hổng và tấn công
* Mối đe dọa (Threat) là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống. Các tài nguyên hệ thống bao gồm phần cứng, phần mềm, cơ sở dữ liệu, các file, dữ liệu, hoặc hạ tầng mạng vật lý,…



Hình 1. 8 Phân bố lỗ hổng bảo mật trong các thành phần của hệ thống

* Các điểm yếu hệ thống (System weaknesses) là các lỗi hay các khiếm khuyết tồn tại trong hệ thống. Nguyên nhân của sự tồn tại các điểm yếu có thể do lỗi thiết kế, lỗi cài đặt, lỗi lập trình, hoặc lỗi quản trị, cấu hình hoạt động. Các điểm yếu có thể tồn tại trong cả các mô đun phần cứng và các mô đun phần mềm.
* Lỗ hổng bảo mật (Security vulnerability) là một điểm yếu tồn tại trong một hệ thống cho phép tin tặc khai thác gây tổn hại đến các thuộc tính an ninh của hệ thống đó, bao gồm tính toàn vẹn, tính bí mật, tính sẵn dùng. Nói chung, lỗ hổng bảo mật tồn tại trong tất cả các thành phần của hệ thống, bao gồm phần cứng, hệ điều hành và các phần mềm ứng dụng.
* Tấn công (Attack) là một, hoặc một chuỗi các hành động vi phạm các chính sách an ninh an toàn của cơ quan, tổ chức, gây tổn hại đến các thuộc tính bí mật, toàn vẹn và sẵn dùng của thông tin, hệ thống và mạng. Một cuộc tấn công vào hệ thống máy tính hoặc các tài nguyên mạng thường được thực hiện bằng cách khai thác các lỗ hổng tồn tại trong hệ thống.
  + 1. Các dạng mối đe dọa thường gặp

Không phải tất cả các mối đe dọa đều là ác tính hay độc hại (malicious). Một số mối đe dọa là chủ động, cố ý, nhưng một số khác chỉ là ngẫu nhiên, hoặc vô tình. Các mối đe dọa thường gặp đối với thông tin, hệ thống và mạng:

- Phần mềm độc hại

- Kẻ tấn công ở bên trong

- Kẻ tấn công ở bên ngoài

- Hư hỏng phần cứng hoặc phần mềm

- Mất trộm các thiết bị

- Tai họa thiên nhiên

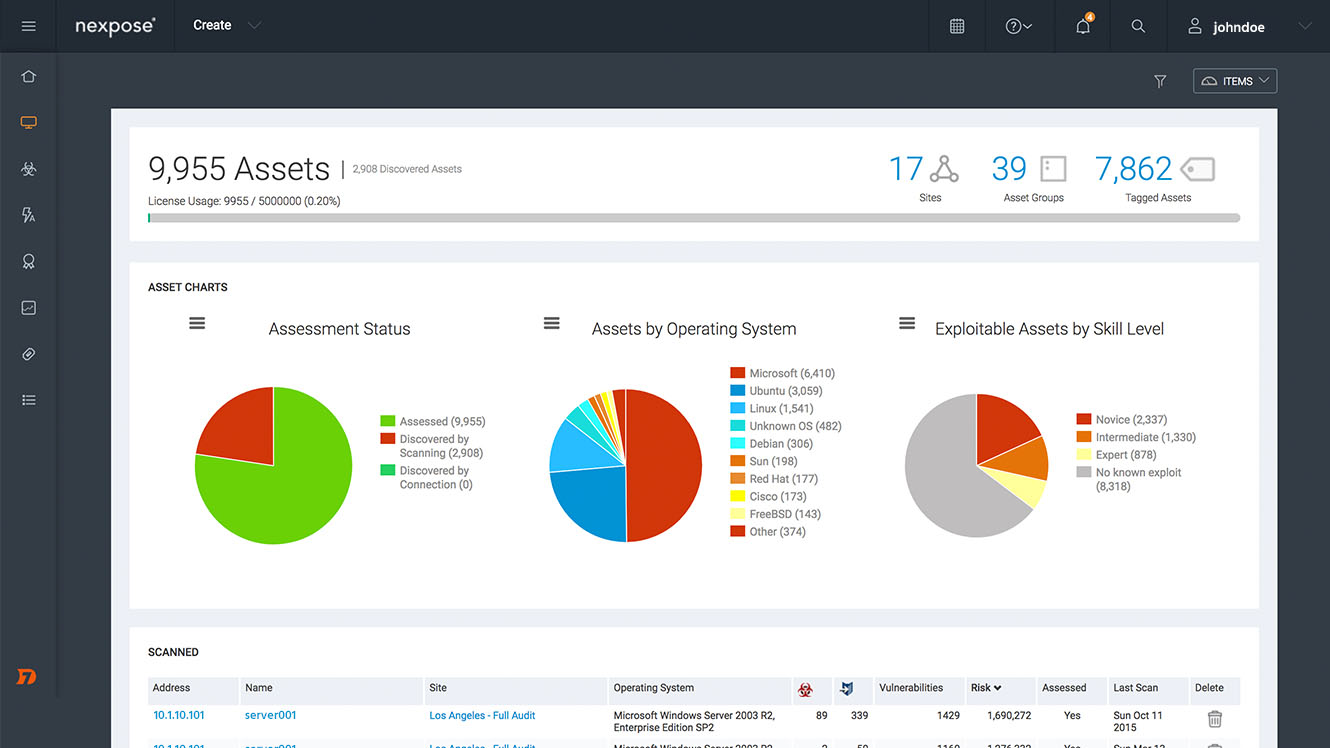
- Gián điệp công nghiệp

- Khủng bố phá hoại.

* + 1. Các loại tấn công
* Có thể chia tấn công theo mục đích thực hiện thành 4 loại chính như sau:
  + - Giả mạo (Fabrications): Tấn công giả mạo thông tin thường được sử dụng để đánh lừa người dùng thông thường.
    - Chặn bắt (Interceptions): Tấn công chặn bắt thường liên quan đến việc nghe lén trên đường truyền và chuyển hướng thông tin để sử dụng trái phép.
    - Gây ngắt quãng (Interruptions): Tấn công gây ngắt quãng làm ngắt, hoặc chậm kênh truyền thông, hoặc làm quá tải hệ thống, ngăn cản việc truy nhập dịch vụ của người dùng hợp pháp.
    - Sửa đổi (Modifications): Tấn công sửa đổi liên quan đến việc sửa đổi thông tin trên đường truyền hoặc sửa đổi dữ liệu file.
* Theo hình thức thực hiện, có thể chia các loại tấn công thành 2 kiểu chính như sau:
* Tấn công chủ động (Active attacks): Tấn công chủ động là một đột nhập, xâm nhập (intrusion) về mặt vật lý vào hệ thống, hoặc mạng. Các tấn công chủ động thực hiện sửa đổi dữ liệu trên đường truyền, sửa đổi dữ liệu trong file, hoặc giành quyền truy nhập trái phép vào máy tính hoặc hệ thống mạng.
* Tấn công thụ động (Passive attacks): Tấn công thụ động thường không gây ra thay đổi trên hệ thống. Các tấn công thụ động điển hình là nghe trộm và giám sát lưu lượng trên đường truyền.
* Trên thực tế, tấn công thụ động thường là giai đoạn đầu của tấn công chủ động, trong đó tin tặc sử dụng các kỹ thuật tấn công thụ động để thu thập các thông tin về hệ thống, mạng, và trên cơ sở thông tin có được sẽ lựa chọn kỹ thuật tấn công chủ động có xác suất thành công cao nhất.
  1. Các công cụ hỗ trợ tấn công
     1. Công cụ rà quét lỗ hổng, điểm yếu hệ thống

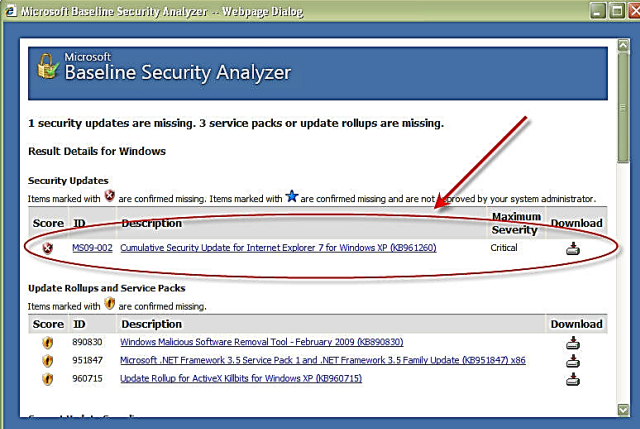
Các công cụ rà quét các điểm yếu hệ thống và lỗ hổng bảo mật có thể được người quản trị sử dụng để chủ động rà quét các hệ thống, nhằm tìm ra các điểm yếu và lỗ hổng bảo mật tồn tại trong hệ thống. Trên cơ sở kết quả rà quét, phân tích và đề xuất áp dụng các biện pháp khắc phục phù hợp. Mặt khác, các công cụ này cũng có thể được kẻ tấn công sử dụng để rà quét hệ thống và dựa trên kết quả rà quét điểm yếu, lỗ hổng để quyết định dạng tấn công có khả năng thành công cao nhất. Các công cụ bao gồm, các công cụ rà quét lỗ hổng bảo mật hệ thống, và các công cụ rà quét lỗ hổng ứng dụng web, hay các trang web.

* Công cụ rà quét lỗ hổng ứng dụng web: cho phép rà quét, phân tích các trang web, tìm các lỗi và lỗ hổng bảo mật. Chúng cũng hỗ trợ phân tích tình trạng các lỗi tìm được, như các lỗi XSS, lỗi chèn mã SQL, lỗi CSRF, lỗi bảo mật phiên,…



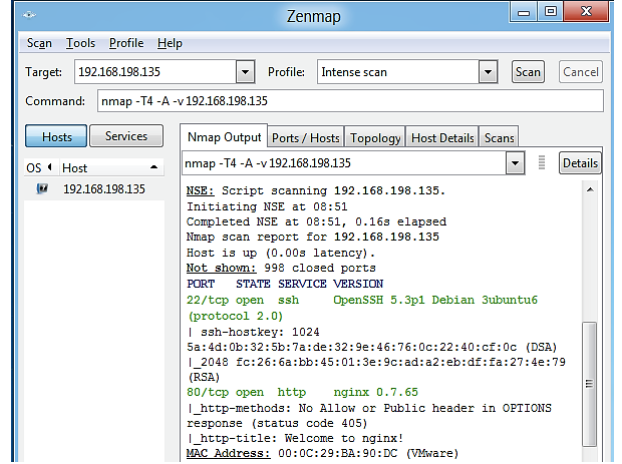
Hình 1. 9 Hệ thống rà quét, kiểm tra, đánh giá lỗ hổng

* Công cụ rà quét lỗ hổng bảo mật hệ thống cho phép rà quét hệ thống, tìm các điểm yếu và các lỗ hổng bảo mật. Đồng thời, chúng cũng cung cấp phần phân tích chi tiết từng điểm yếu, lỗ hổng, kèm theo là hướng dẫn khắc phục, sửa chữa.



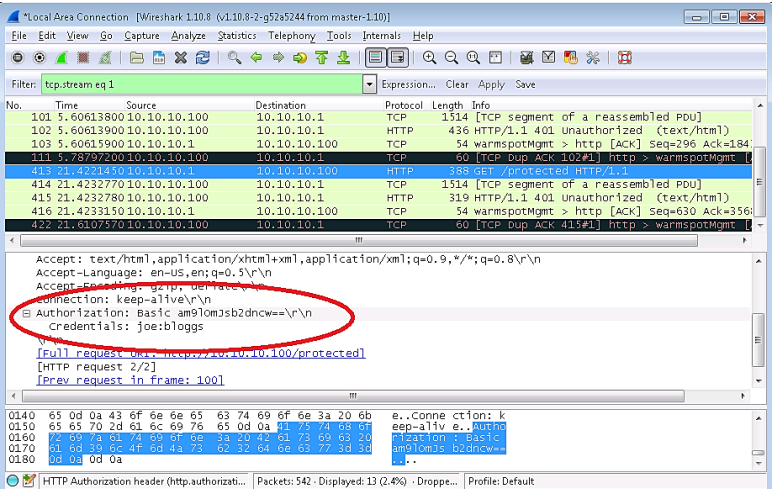
Hình 1. 10 Kết quả quét của Microsoft Baseline Security Analyzer

* + 1. Công cụ quét cổng dịch vụ



Hình 1. 11 Giao diện của công cụ Zenmap

* Các công cụ quét cổng dịch vụ (Port scanners) cho phép quét các cổng, tìm các cổng đang mở, đang hoạt động, đồng thời tìm các thông tin về ứng dụng, dịch vụ và hệ điều hành đang hoạt động trên hệ thống. Dựa trên thông tin quét cổng dịch vụ, có thể xác định được dịch vụ, ứng dụng nào đang chạy trên hệ thống:
* Cổng 80/443 mở có nghĩa là dịch vụ web đang hoạt động.
* Cổng 25 mở có nghĩa là dịch vụ gửi/nhận email SMTP đang hoạt động.
* Cổng 1433 mở có nghĩa là máy chủ Microsoft SQL Server đang hoạt động.
* Cổng 53 mở có nghĩa là dịch vụ tên miền DNS đang hoạt động,...
* Các công cụ quét cổng dịch vụ được sử dụng phổ biến bao gồm: Nmap, Zenmap, Portsweep, Advanced Port Scanner, Angry IP Scanner, SuperScan và NetScanTools.
  + 1. Công cụ nghe trộm
* Công cụ nghe trộm hay nghe lén (Sniffers) cho phép bắt các gói tin khi chúng được truyền trên mạng. Công cụ nghe lén có thể là mô đun phần cứng, phần mềm hoặc kết hợp.
* Các thông tin nhạy cảm như thông tin tài khoản, thẻ tín dụng, hoặc mật khẩu nếu không được mã hóa thì có thể bị kẻ tấn công nghe lén khi được truyền từ máy trạm đến máy chủ và bị lạm dụng. Một số công cụ phần mềm cho phép bắt gói tin truyền trên mạng:
* Tcpdump
* Wireshark
* Pcap / Wincap / Libcap (Packet capture)
* IP Tools (<http://www.softpedia.com>).



Hình 1. 12 Sử dụng Wireshark để bắt gói tin

* + 1. Công cụ ghi phím gõ

Công cụ ghi phím gõ (Keyloggers) là một dạng công cụ giám sát bằng phần cứng hoặc phần mềm có khả năng ghi lại mọi phím người dùng gõ và lưu vào một file. File đã ghi sau đó có thể được gửi cho kẻ tấn công theo địa chỉ chỉ định trước hoặc sao chép trực tiếp. Ngoài kẻ tấn công, người quản lý cũng có thể cài đặt Keylogger vào máy tính của nhân viên để theo dõi hoạt động của các nhân viên.

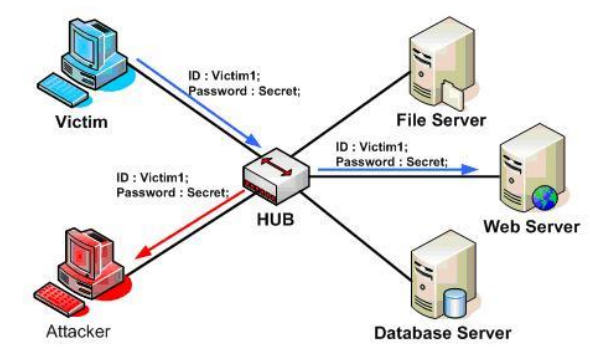


Hình 1. 13 Mô đun Keylogger phần cứng

* 1. Các dạng tấn công thường gặp
     1. Tấn công vào mật khẩu
* Tấn công vào mật khẩu (Password attack) là dạng tấn công nhằm đánh cắp mật khẩu và thông tin tài khoản của người dùng để lạm dụng. Tên người dùng và mật khẩu không 33 được mã hóa có thể bị đánh cắp trên đường truyền từ máy khách đến máy chủ, hoặc các thông tin này có thể bị đánh cắp thông qua các dạng tấn công XSS, hoặc lừa đảo, bẫy người dùng cung cấp thông tin.
* Có thể chia tấn công vào mật khẩu thành 2 dạng: -
* Tấn công dựa trên từ điển (Dictionary attacks): Dạng tấn công này khai thác vấn đề người dùng có xu hướng chọn mật khẩu là các từ đơn giản cho dễ nhớ. Kẻ tấn công thử các từ có tần suất sử dụng cao làm mật khẩu trong từ điển, nhờ vậy tăng khả năng thành công.
* Tấn công vét cạn (Brute force attacks): Dạng vét cạn sử dụng tổ hợp các ký tự và thử tự động. Phương pháp này thường được sử dụng với các mật khẩu đã được mã hóa. Kẻ tấn công sinh tổ hợp ký tự, sau đó mã hóa với cùng thuật toán mà hệ thống sử dụng, tiếp theo so sánh chuỗi mã hóa từ tổ hợp ký tự với chuỗi mật khẩu mã hóa thu thập được. Nếu hai bản mã trùng nhau thì tổ hợp ký tự là mật khẩu
* Để đảm bảo an toàn cho mật khẩu, cần thực hiện kết hợp các biện pháp sau:
* Chọn mật khẩu đủ mạnh: Mật khẩu mạnh cho người dùng thông thường cần có độ dài lớn hơn hoặc bằng 8 ký tự, gồm tổ hợp của 4 loại ký tự: chữ cái hoa, chữ cái thường, chữ số và ký tự đặc biệt (?#$...). Mật khẩu cho người quản trị hệ thống cần có độ dài lớn hơn hoặc bằng 10 ký tự cũng với các loại ký tự như mật khẩu cho người dùng thông thường.
* Định kỳ thay đổi mật khẩu. Thời hạn đổi mật khẩu tùy thuộc vào chính sách an ninh của cơ quan, tổ chức, có thể là 3 tháng, hoặc 6 tháng.
* Mật khẩu không nên lưu ở dạng rõ (plaintext). Nên lưu mật khẩu ở dạng đã mã hóa (thường dùng hàm băm).
* Hạn chế trao đổi tên người dùng và mật khẩu trên kênh truyền không được mã hóa.
  + 1. Tấn công bằng mã độc

Tấn công bằng mã độc (Malicious code attacks) là dạng tấn công sử dụng các mã độc (Malicious code) làm công cụ để tấn công hệ thống nạn nhân. Tấn công bằng mã độc có thể chia thành 2 loại:

* Khai thác các lỗ hổng về lập trình, lỗ hổng cấu hình hệ thống để chèn và thực hiện mã độc trên hệ thống nạn nhân. Loại tấn công này lại gồm 2 dạng:
  + Tấn công khai thác lỗi tràn bộ đệm (Buffer Overflow)
  + Tấn công khai thác lỗi không kiểm tra đầu vào, gồm tấn công chèn mã SQL (SQL Injection) và tấn công sử dụng mã script, kiểu XSS, CSRF.
* Lừa người sử dụng tải, cài đặt và thực hiện các phần mềm độc hại, như:
  + Các phần mềm quảng cáo (Adware), gián điệp (Spyware)
  + Vi rút
  + Zombie/Bot
  + Trojan
    1. Tấn công nghe lén
* Tấn công nghe lén (Sniffing/Eavesdropping), dạng tấn công sử dụng thiết bị phần cứng hoặc phần mềm, lắng nghe trên card mạng, hub, switch, router, hoặc môi trường truyền dẫn để bắt các gói tin dùng cho phân tích, hoặc lạm dụng về sau. Đây là kiểu tấn công thụ động nhằm thu thập các thông tin nhạy cảm, hoặc giám sát lưu lượng mạng. Các thông tin nhạy cảm như tên người dùng, mật khẩu, thông tin thanh toán nếu không được mã hóa có thể bị nghe lén và lạm dụng. Các thông tin truyền trong mạng WiFi, hoặc các mạng không dây cũng có thể bị nghe lén dễ dàng do môi trường truyền dẫn vô tuyến và nếu không sử dụng các cơ chế bảo mật đủ mạnh.
* Để phòng chống tấn công nghe lén, có thể áp dụng các biện pháp sau:
* Có cơ chế bảo vệ các thiết bị mạng và hệ thống truyền dẫn ở mức vật lý
* Sử dụng các biện pháp, cơ chế xác thực người dùng đủ mạnh
* Sử dụng các biện pháp bảo mật thông tin truyền dựa trên các kỹ thuật mã hóa.



Hình 1. 14 Tấn công nghe lén

* + 1. Tấn công pharming
* Pharming là kiểu tấn công vào trình duyệt của người dùng, trong đó người dùng gõ địa chỉ 1 website, trình duyệt lại yêu cầu và tải 1 website khác, thường là website độc hại.
* Có 2 dạng tấn công pharming:
  + Kẻ tấn công thường sử dụng sâu, vi rút hoặc các phần mềm độc hại cài vào hệ thống để điều khiển trình duyệt của người dùng
  + Kẻ tấn công có thể tấn công vào hệ thống tên miền (DNS) để thay đổi kết quả truy vấn: thay địa chỉ IP của website hợp pháp thành IP của website độc hại.



Hình 1. 15 Tấn công pharming thông qua máy chủ DNS

* + 1. Tấn công kiểu người đứng giữa
* Tấn công kiểu người đứng giữa (Man in the middle) là dạng tấn công dụng quá trình chuyển gói tin đi qua nhiều trạm (hop) thuộc các mạng khác nhau, trong đó kẻ tấn công chặn bắt các thông điệp giữa 2 bên tham gia truyền thông và chuyển thông điệp lại cho bên kia. Mục đích chính của dạng tấn công này là đánh cắp thông tin.



Hình 1. 16 Mô hình tấn công kiểu người đứng giữa

* Một trong các biện pháp hiệu quả để phòng chống tấn công kiểu người đứng giữa là hai bên tham gia truyền thông phải có cơ chế xác thực thông tin nhận dạng của nhau và xác thực tính toàn vẹn của các thông điệp trao đổi. Chẳng hạn, các bên có thể sử dụng chứng chỉ số khóa công khai (Public key certificate) để xác thực thông tin nhận dạng của nhau và sử dụng chữ ký số để đảm bảo tính toàn vẹn của các thông điệp trao đổi.
  1. Các phần mềm độc hại
     1. Giới thiệu
* Các phần mềm độc hại (Malware hay Malicious software) là các chương trình, phần mềm được viết ra nhằm các mục đích xấu, như đánh cắp thông tin nhạy cảm, hoặc phá hoại các hệ thống. Có nhiều phương pháp phân loại các phần mềm độc hại, trong đó một phương pháp được thừa nhận rộng rãi là chia các phần mềm độc hại thành 2 nhóm chính:
* Các phần mềm độc hại cần chương trình chủ, vật chủ (host) để ký sinh và lây nhiễm. Các phần mềm độc hại thuộc nhóm này gồm Logic bomb (Bom logic), Back door (Cửa hậu), Trojan horse (Con ngựa thành Tơ roa), Virus (Vi rút), Rootkit, Adware (Phần mềm quảng cáo) và Spyware (Phần mềm gián điệp).
* Các phần mềm độc hại không cần chương trình chủ, vật chủ để lây nhiễm. Các phần mềm độc hại thuộc nhóm này gồm Worm (Sâu) và Zombie hay Bot (Phần mềm máy tính ma).
* Trong số các phần mềm độc hại, các phần mềm độc hại có khả năng tự lây nhiễm (self-infection), hay tự nhân bản (self-replicate) gồm Vi rút, Sâu và Phần mềm máy tính ma. Các dạng còn lại không có khả năng tự lây nhiễm. Việc phân loại các phần mềm độc hại kể trên mang tính chất tương đối do hiện nay, có một số phần mềm độc hại có các đặc tính của cả Vi rút, Sâu và Phần mềm gián điệp.
  + 1. Logic bomb
* Logic bomb (Bom lô gíc) là các đoạn mã độc thường được “nhúng” vào các chương trình bình thường và thường hẹn giờ để “phát nổ” trong một số điều kiện cụ thể. Điều kiện để bom “phát nổ” có thể là sự xuất hiện hoặc biến mất của các file cụ thể, một thời điểm cụ thể, hoặc một ngày trong tuần. Khi “phát nổ” bom logic có thể xoá dữ liệu, file, tắt cả hệ thống...
* Thực tế đã ghi nhận quả bom logic do Tim Lloyd cài lại đã “phát nổ” tại công ty Omega Engineering vào ngày 30/7/1996, 20 ngày sau khi Tim Lloyd bị sa thải. Bom lô gíc này đã xoá sạch các bản thiết kế và các chương trình, gây thiệt hại 10 triệu USD cho công ty. Bản thân Tim Lloyd bị phạt 2 triệu USD và 41 tháng tù.
  + 1. Virus
* Vi rút (Virus) là một chương trình có thể “nhiễm” vào các chương trình khác, bằng cách sửa đổi các chương trình này. Nếu các chương trình đã bị sửa đổi chứa vi rút được kích hoạt thì vi rút sẽ tiếp tục “lây nhiễm” sang các chương trình khác. Tương tự như vi rút sinh học, vi rút máy tính cũng có khả năng tự nhân bản, tự lây nhiễm sang các chương trình khác mà nó tiếp xúc. Có nhiều con đường lây nhiễm vi rút, như sao chép file, gọi các ứng dụng và dịch vụ qua mạng, email...
* Vi rút có thể thực hiện được mọi việc mà một chương trình thông thường có thể thực hiện. Khi đã lây nhiễm vào một chương trình, vi rút tự động được thực hiện khi chương trình này chạy.



Hình 1. 17 Minh họa virus máy tính

* Các loại vi rút thường gặp bao gồm file vi rút, boot vi rút, macro vi rút và email vi rút. Boot vi rút là dạng vi rút lây nhiễm vào cung khởi động (boot sector) của đĩa hoặc phần hệ thống của đĩa như cung khởi động chủ của đĩa cứng (master boot record). Do boot vi rút lây nhiễm vào cung khởi động nên nó luôn được nạp vào bộ nhớ mỗi khi hệ thống máy khởi động. Boot vi rút có thể gây hỏng phần khởi động của đĩa, thậm chí có thể làm cho đĩa không thể truy nhập được.

CHƯƠNG 2: GIỚI THIỆU PHẦN MỀM PANDORA FMS

* 1. Giới thiệu phần mềm Pandora FMS
     1. Khái niệm
* Pandora FMS là giải pháp giám sát dành cho doanh nghiệp, cung cấp tính linh hoạt tuyệt vời cho CNTT để giải quyết các vấn đề vận hành trước mắt và không lường trước được, bao gồm cơ sở hạ tầng và quy trình CNTT. Nó đặc biệt cho phép doanh nghiệp và CNTT thích ứng với nhu cầu thay đổi thông qua cách tiếp cận linh hoạt và nhanh chóng để triển khai CNTT và kinh doanh.
* Kiến trúc Pandora FMS được tạo thành từ các dịch vụ khác nhau:
* Máy chủ cơ sở dữ liệu
* Bảng điều khiển web
* Máy chủ PandoraFMS



Hình 2. 1 Phần mềm giám sát Pandora FMS

* Pandora FMS hợp nhất tất cả các nhu cầu giám sát hiện đại (ITOM, APM, BAM) và cung cấp các số liệu trạng thái và hiệu suất từ ​​các hệ điều hành, đám mây, cơ sở hạ tầng ảo (VMware, Hyper-V, XEN), bộ chứa Docker, ứng dụng, thiết bị lưu trữ và phần cứng khác nhau chẳng hạn như tường lửa, proxy, cơ sở dữ liệu, máy chủ web hoặc bộ định tuyến.
* Pandora FMS có một số máy chủ xử lý và lấy thông tin từ các nguồn khác nhau, sử dụng WMI để thu thập thông tin Windows từ xa, máy chủ dự đoán, máy chủ plug-in giúp thực hiện các thử nghiệm mạng phức tạp do người dùng xác định, máy chủ xuất nâng cao để sao chép dữ liệu giữa các trang web khác nhau của Pandora FMS, máy chủ khám phá mạng và bảng điều khiển SNMP Trap.
* Pandora FMS hiện có đại lý cho tất cả các hệ điều hành trên thị trường. Nó có thể được sử dụng thành công không chỉ để giám sát các hệ thống mà còn cho tất cả các loại thiết bị mạng, sử dụng SNMP, thông qua các đầu dò giao thức TCP, ICMP, UDP hoặc đại lý phần mềm.
  + 1. Tính năng của Pandora FMS
* Tự giám sát: theo mặc định, nó cho phép phát hiện các thiết bị lưu trữ hoặc cơ sở dữ liệu trong máy chủ, trong số những thứ khác.
* Tự động phát hiện: từ xa bằng mạng, bạn có thể phát hiện tất cả các thành phần của nó, lập danh mục chúng theo hệ điều hành (OS) và giám sát bằng cấu hình chỉ định.
* Tác nhân: họ có thể lấy thông tin từ việc thực thi lệnh đến gọi cấp thấp nhất của API MS Windows.
* Cảnh báo và thông báo: việc thông báo lỗi cũng quan trọng như việc phát lỗi. Với Pandora FMS có một số cách và định dạng thông báo có sẵn.
* Xem và phân tích: mặc dù việc giám sát đang nhận bẫy SNMP hoặc xem dịch vụ bị gián đoạn, nhưng nó cũng trình bày các báo cáo xu hướng, biểu đồ tóm tắt dữ liệu được thu thập qua nhiều tháng, tạo cổng thông tin người dùng, ủy quyền báo cáo cho bên thứ ba hoặc xác định biểu đồ và bảng của riêng bạn.
* Đa năng: Pandora FMS không chỉ giám sát các máy chủ, mạng và ứng dụng, mà còn hỗ trợ giám sát các môi trường ảo hóa, điện toán đám mây và thiết bị di động, tạo ra một bức tranh tổng thể về tình trạng hoạt động của hệ thống.
* Tính linh hoạt: Phần mềm này cho phép tùy chỉnh linh hoạt để phù hợp với nhu cầu cụ thể của từng tổ chức. Bạn có thể tạo các bản báo cáo tùy chỉnh, cấu hình cảnh báo và quản lý người dùng một cách dễ dàng.
* Giao diện sử dụng dễ dàng: Giao diện người dùng trực quan và dễ sử dụng giúp người dùng dễ dàng theo dõi và quản lý tất cả các hoạt động giám sát một cách hiệu quả.
* Kiến thức mở rộng: Pandora FMS cho phép tích hợp với nhiều công nghệ và dịch vụ khác nhau như SNMP, WMI, SSH, và nhiều giao thức khác, giúp mở rộng khả năng giám sát của nó trên nhiều nền tảng.
* Tính năng tự động hóa: Phần mềm này cung cấp các tính năng tự động hóa cho việc cấu hình và quản lý, giúp giảm thiểu thời gian và công sức cần thiết cho việc duy trì hệ thống.
* Hỗ trợ đa nền tảng: Pandora FMS hỗ trợ đa nền tảng, bao gồm Windows, Linux, Unix, MacOS, và các nền tảng ảo hóa như VMware và Hyper-V.
* Tính hiệu quả: Với khả năng giám sát thời gian thực và cảnh báo sớm về sự cố, Pandora FMS giúp tổ chức tiết kiệm thời gian và tài nguyên trong việc xử lý vấn đề và đảm bảo sự ổn định của hệ thống.
  + 1. Kiến trúc của hệ thống giám sát Pandora FMS
* Trong kiến ​​trúc Pandora FMS, máy chủ là cốt lõi của hệ thống vì chúng là nơi nhận các gói thông tin. Họ cũng tạo ra các cảnh báo giám sát. Có thể có các cấu hình mô-đun khác nhau cho các máy chủ: một số máy chủ cho các hệ thống rất lớn hoặc chỉ một máy chủ. Máy chủ cũng chịu trách nhiệm chèn dữ liệu đã thu thập vào cơ sở dữ liệu của Pandora.
* Có thể có một số Máy chủ Pandora được kết nối với một Cơ sở dữ liệu. Các máy chủ khác nhau được sử dụng cho các loại giám sát khác nhau: giám sát từ xa, giám sát WMI, SNMP và giám sát mạng khác, thu hồi hàng tồn kho, v.v. Khả năng mở rộng cao (lên tới 2000 nút với một máy chủ), hoàn toàn dựa trên web và giao diện nhiều bên thuê.
* Có hệ thống ACL rất linh hoạt và nhiều báo cáo đồ họa cũng như màn hình điều khiển do người dùng xác định.
* Web console: Giao diện người dùng của Pandora cho phép mọi người vận hành và quản lý hệ thống giám sát. Nó được phát triển bằng PHP và phụ thuộc vào cơ sở dữ liệu và máy chủ web. Nó có thể hoạt động trên nhiều nền tảng: Linux , Solaris , Windows , AIX và các nền tảng khác. Một số bảng điều khiển web có thể được triển khai trong cùng một hệ thống nếu được yêu cầu. Bảng điều khiển Web có nhiều lựa chọn, chẳng hạn như giám sát SNMP .
* Agents: Tác nhân là các daemon hoặc dịch vụ có thể giám sát bất kỳ tham số số, trạng thái Boolean, chuỗi hoặc dữ liệu gia tăng số và/hoặc điều kiện nào.
* Database Mô-đun cơ sở dữ liệu là mô-đun cốt lõi của Pandora. Tất cả thông tin của hệ thống đều nằm ở đây. Ví dụ: tất cả dữ liệu được thu thập bởi các tác nhân, cấu hình do quản trị viên xác định, sự kiện, sự cố, thông tin kiểm tra, v.v. đều được lưu trữ trong cơ sở dữ liệu. Hiện tại, cơ sở dữ liệu MySQL và cơ sở dữ liệu MariaDB được hỗ trợ. Hỗ trợ của Oracle đã được thêm vào trong phiên bản 6.0.
  + 1. Thủ tục giám sát

Trước khi bắt đầu giai đoạn triển khai, điều quan trọng là phải xem xét đâu là điểm quan trọng và quan trọng nhất của nền tảng công nghệ được giám sát. Bằng cách này, trước khi có thông tin dữ liệu cụ thể và hệ thống, có thể biết phải làm gì với chúng và cách khai thác toàn bộ tiện ích mà không lãng phí thời gian điều tra hoặc các chi tiết tầm thường.

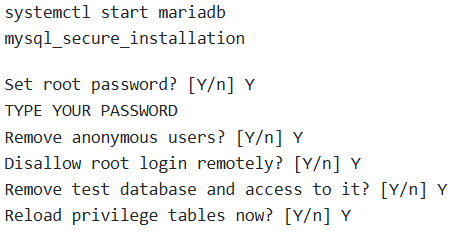
* Tính sẵn có: giám sát dựa trên sự kiện được quan tâm hơn hết và giám sát từ xa có lẽ là đủ, nó được triển khai nhanh hơn và có thể thu được kết quả trong thời gian ngắn. Báo cáo SLA sẽ hữu ích nhất trong trường hợp này.
* Hiệu suất: là đồ thị và các con số, bạn có thể lấy thông tin đó bằng cả tác nhân và triển khai từ xa, nhưng có thể cần có tác nhân để lấy thông tin chi tiết từ hệ thống. Các báo cáo được nhóm và biểu đồ kết hợp ưu tiên.
* Lập kế hoạch năng lực: chuyên biệt hơn, cần phải thu thập dữ liệu. Việc thiết lập các cảnh báo sớm sẽ rất hữu ích và bạn sẽ cần phải biết rõ các khái niệm về trạng thái cảnh báo và tiêu chuẩn, ngoài việc phát triển một loạt chính sách quản lý sự kiện cho phép bạn lường trước sự cố trước khi nó xảy ra, chắc chắn là phức tạp nhất.
  1. Cài đặt phần mềm Pandora FMS

1. Chuẩn bị môi trường cài đặt

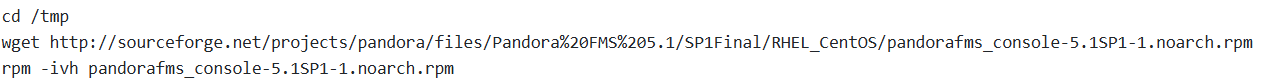
* Cần một máy chạy CentOS 7 -64bit cho máy chủ Pandora
* Tên miền hợp lệ được chỉ định bằng IP máy chủ của bạn
* Mật khẩu gốc được định cấu hình máy chủ

1. Cài đặt các gói điều kiện tiên quyết cho Pandora FMS
2. Cài đặt Pandora FMS trên CentOS 7

* Bước 1: Định cấu hình MariDB/MySQL



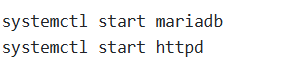
* Bước 2: Cài đặt bảng điều khiển Pandora
* Tải xuống và cài đặt bảng điều khiển Pandora.



* Cấp quyền 777 cho tệp cấu hình máy chủ Pandora

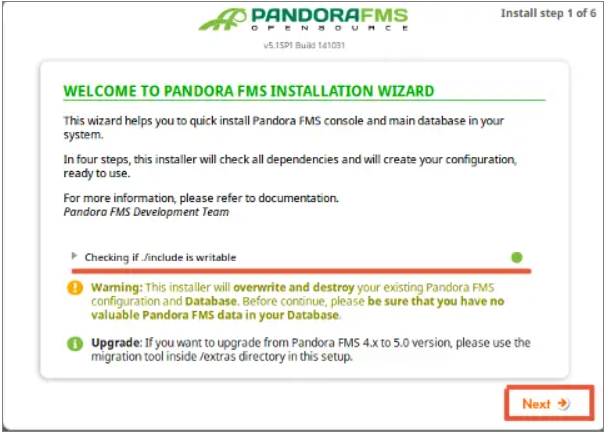


* Bắt đầu MariaDB và httpd



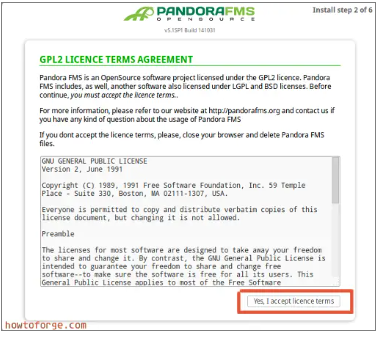
* Mở máy chủ Pandora từ trình duyệt của bạn:

http://yourip/pandora\_console/.



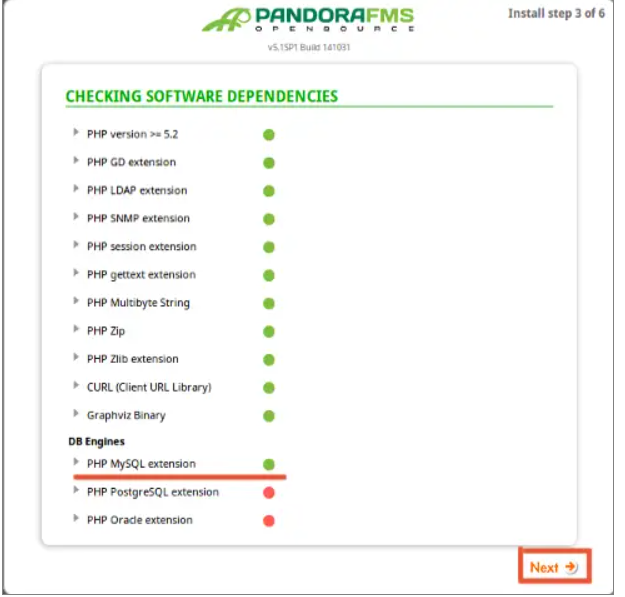
Hình 2. 2 Giao diện bắt đầu của Pandora FMS

* Nhấp vào có, tôi chấp nhận các điều khoản cấp phép



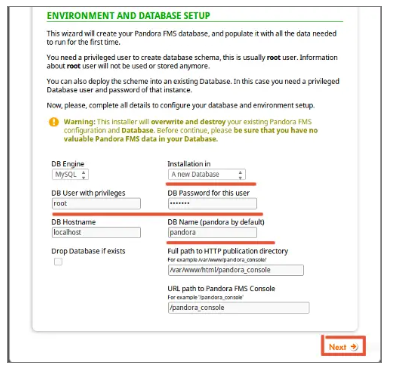
Hình 2. 3 Các điều khoản cấp phép

* Tất cả các phần mềm phục thuộc đã được cài đặt, chọn cơ sở dữ liệu MySQL cho hướng dẫn này và nhấp vào tiếp theo.



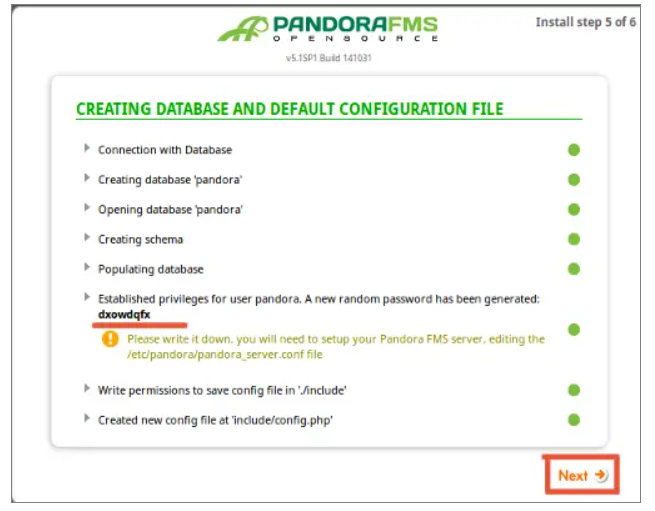
Hình 2. 4 Các phụ thuộc phần mềm

* Tạo một cơ sở dữ liệu mới với tên Pandora với quyền root. Nhấp vào tiếp theo



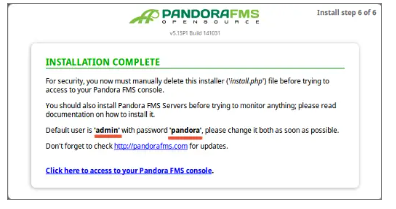
Hình 2. 5 Tạo cơ sở dữ liệu mới

* Cấu hình cơ sở dữ liệu đã hoàn tất. Lưu mật khẩu ngẫu nhiên được tạo và nhấp vào tiếp theo.



Hình 2. 6 Cấu hình cơ sở dữ liệu thành công

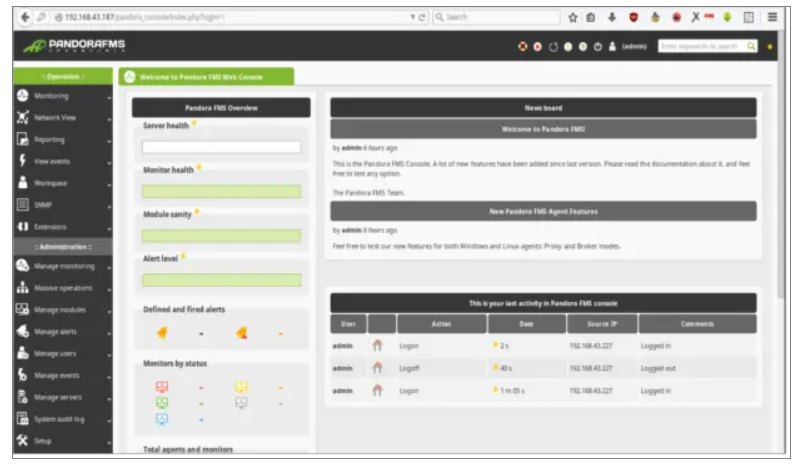
* Bảng điều khiển Pandora đã được cài đặt, bây giờ có thể đăng nhập bằng thông thông tin đăng nhập mặc định.



Hình 2. 7 Bảng điều khiển Pandora

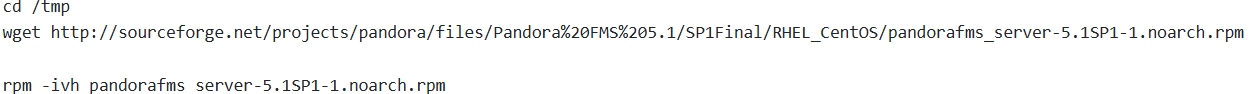
* Trước khi đăng nhập vào Pandora FMS, cần đổi tên tệp install.php trong thư mục: /var/www/html/pandora\_console.





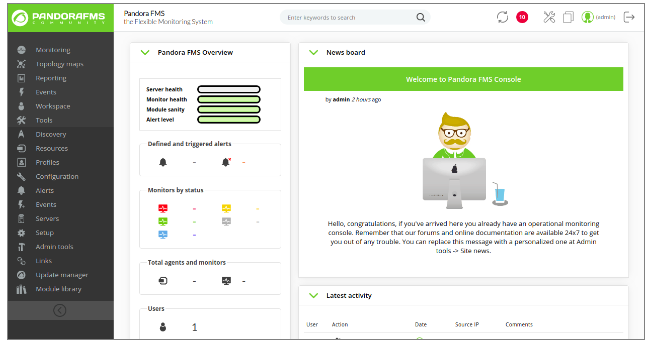
Hình 2. 8 Màn hình sau khi đăng nhập

* Bước 3: Cài đặt máy chủ Pandora
* Tải xuống và cài đặt máy chủ Pandora



* Chỉnh sửa tệp cấu hình tác nhân Pandora



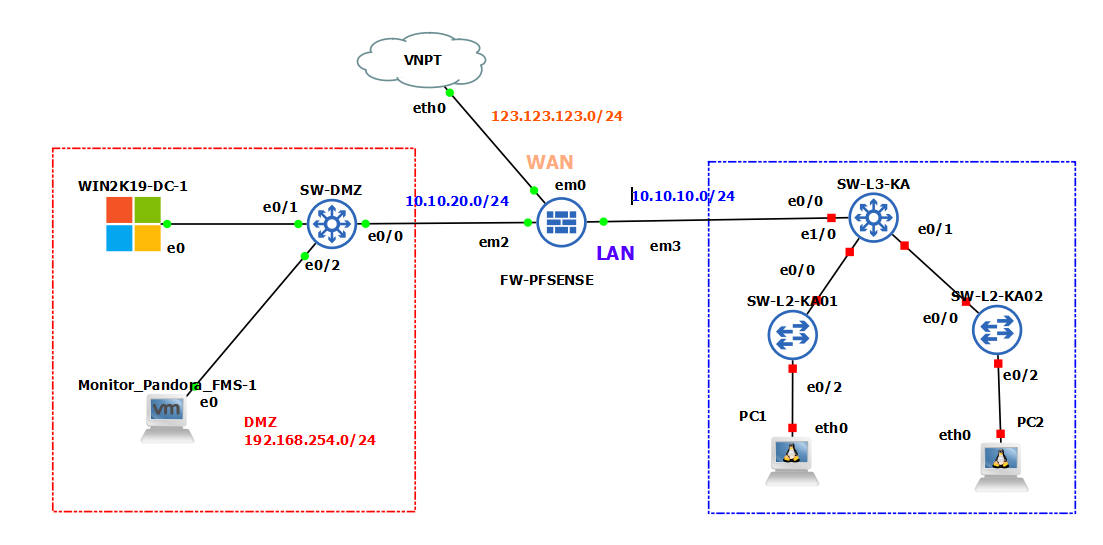


Hình 2. 9 Máy chủ Pandora FMS

CHƯƠNG 3: XÂY DỰNG LAB MÔ PHỎNG

1. TỔNG QUAN VỀ MÔ HÌNH THỰC HÀNH

## Giới thiệu mô hình.



Hình : Mô hình thực nghiệm.

Trong sơ đồ này sẽ xác định 3 vùng riêng biệt bao gồm: DMZ, LAN và Internet

* Vùng DMZ : vùng chứa các Server , Domain Controller của công ty như FTP Server, Web Server...Ngoài ra để giám sát các máy Server trong vùng DMZ sử dụng một hệ thống giám sát Pandora FMS
* Vùng Internet: là vùng bên ngoài cung ty, cung cấp dịch vụ Internet cho công ty- Ngoài ra để kết nối 3 vùng này với nhau thì sử dụng Firewall pfSense
* Vùng LAN: là vùng chứa các Switch và các thiết bị Linux của máy nhân viên.

## Giải thích mô hình.

Trong vùng LAN: ở trong vùng LAN chứa các máy Client sẽ Join vào Domain để lấy User sử dụng trong công ty cũng như sẽ chấp hành theo những chính sách người quản trị đưa xuống để làm việc)

Trong vùng DMZ: đặt luôn Domain Controller (vì lí do Domain Controller là nơi xây dựng các User – Group được sử dụng trong công ty, hơn thế nữa nơi đây cũng là nơi triển khai toàn bộ các chính sách của công ty xuống các phòng ban, các User và Group, và các máy Client sẽ phải chứa toàn bộ những server sử dụng cho công ty như Web Server (Website của công ty), FTP Server (lưu giữ các file tài liệu), hay MailServer (mail riêng của nội bộ công ty)… Vùng này cũng sẽ là nơi được public các dịch vụ ra ngoài internet để người sử dụng cũng có thể làm việc, như việc public Website của công ty để người sử dụng truy cập bằng tên miền vào website . . .

Trong vùng DMZ sẽ có một hệ thống giám sát hoạt động của các Server, để người quản trị có thể kịp thời phát hiện sự cố - hỏng thiết bị và khắc phục dễ dàng hơn, ở đây sẽ sử dụng giám sát hệ thống bằng Pandora FMS. Với phần mềm Pandora FMS giúp giải quyết được toàn bộ những khó khăn của doanh nghiệp trong việc quản lý tài nguyên, cho phép quản lý toàn sự cố, quản lý topo mạng và cấu hình thiết bị mạng. Tạo nên một hệ thống mạng chủ động.

Vùng internet: là nơi cung cấp dịch vụ Internet cho người sử dụng internet trong công ty.

Firewall pfSense: Trước khi Internet từ nhà mạng qua router đến công ty sẽ đi qua một hệ thống Firewall. Là nơi kết nối các khu vực với nhau bằng các Rule sao cho hệ thống có thể hoạt động tốt nhưng cũng đảm bảo độ an toàn cho các khu vực riêng biệt, tránh sự tấn công xâm nhập từ bên ngoài thông qua các Rule quản lý

## Triển khai hệ thống.

Triển khai hệ thống theo mô hình tập trung, cài đặt các thành phần của Pandora FMS trên cùng một sever phục vụ cho việc giám sát hệ thống mạng. Thực hiện cài đặt theo hướng dẫn “Mục 2.2. Cài đặt phần mềm Pandora FMS”.

Các thành phần của hệ thống mạng bao gồm:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | Host name | IP | OS | Description |
| 1 | SW-DMZ | 192.168.254.1 | Switch Cisco | Switch layer 2 sử dụng kết nối mạng nội bộ của vùng DNZ |
| 2 | WIN2K19-DC | 192.168.254.254 | Windown Server 2019 | Máy chủ quản lý domain, OU và các dịch vụ IIS, DHCP, DNS,.. cho mạng nội bộ |
| 3 | WIN2K19-ADC | 192.168.254.253 | Windown Server 2019 | Máy chủ dự phòng của WIN2K19-DC nhằm tang mức dự phòng của hệ thống mạng |
| 4 | FW-PFSENSE | 10.10.10.1 | Router | Route sử dụng để cấp internet từ phía bên ngoài vào và nhằm bảo vệ các thiết bị bên trong thông qua các chính sách. |
| 5 | Pandora-FMS-Server | 192.168.254.100 | Linux (Redhat 8.9 Enterprise) | Máy chủ giám sát thiết bị mạng, chương trình ứng dụng, tài nguyên của các thiết bị mạng nội bộ. |

### Kịch bản giám sát hệ thống mạng.

Xây dựng kịch bản giám sát phần hệ thống (hosts, end devices) trong hệ thống mạngbao gồm: 03 máy chủ chạy hệ điều hành windows server 2012, 02 máy chủ chạy hệ điều hành linux server (Centos 7.2 và Redhat 7.2).

Xây dựng kịch bản giám sát phần hệ thống (hosts, end devices) trong hệ thống mạng bao gồm: 02 máy chủ chạy hệ điều hành windows server 2019, 01 máy chủ chạy hệ điều hành linux server (Redhat 8.9). 02 switch cisco, 01 firewall Pfsense và 02 hệ điều hành Linux của phía client.

a. Giám sát trạng thái trên host

* Trạng thái hoạt động của hosts.
* Độ trễ của thiết bị.
* Kiểm tra và update địa chỉ IP của thiết bị.
* Trạng thái hoạt động của services.
* Trạng thái của các interfaces trên host.

b. Giám sát việc sử dụng các tài nguyên

* CPU số lượng processes trong hàng đợi hay theo % sử dụng CPU của hosts
* Ram: Cho biết dung lượng tổng, số lượng dung lượng sử dụng hay còn trống
* Disk: Cho biết dung lượng tổng, còn trống, và đã sử dụng.

c. Giám sát lưu lượng mạng vào ra trên các host

* Giám sát lưu lượng vào ra trên các interface của host: tổng lưu lượng vào ra.
* Giám sát tổng băng thông trên từng cổng.

d. Thông tin, quản lý dữ liệu giám sát của các host.

* Lưu trữ các thông số trong 7->30 ngày có thể xem lại và phục vụ cho việc phân tích và nâng cấp hệ thống sau này sau này
* Biển diễn theo danh sách hoặc biểu đồ trực quan về tình hình sử dụng tài nguyên và thông số trên các host.
* In ra các bản báo cáo chi tiết về thời gian hoạt động của thiết bị, mô hình biểu đồ trực quan.

e. Cảnh báo

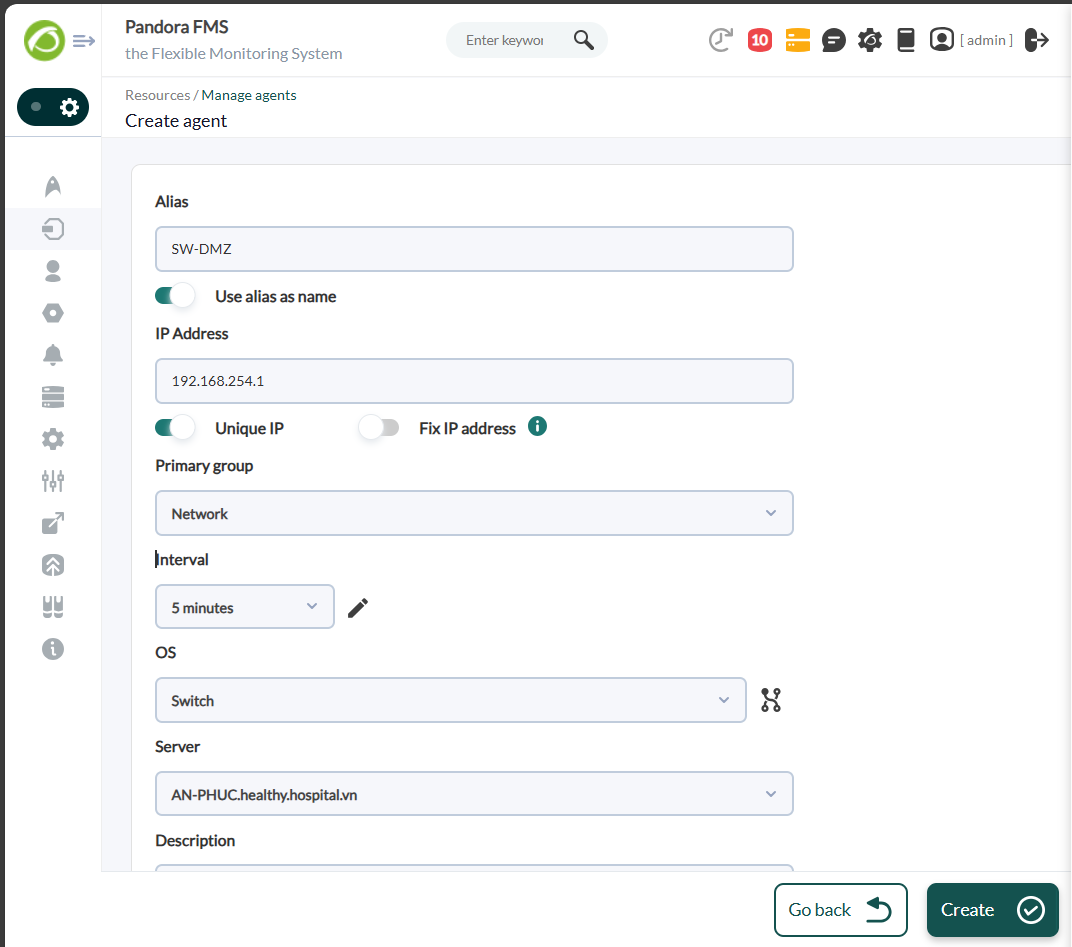
* Cảnh báo trạng thái: ví dụ host bị down bất thường, hay sự cố ngoài ý muốn
* Cảnh báo dịch vụ: Services bị tắt hay thay đổi trạng thái
* Ví dụ: Máy chủ bất ngờ shutdown
* Cảnh báo thời gian máy chủ shutdow

### Cấu hình giám sát hệ thống mạng.

Khi hệ thống hoạt động, việc theo dõi trạng thái các máy chủ đang trong tình trạng như thế nào, các dịch vụ quan trọng có được chạy hay không? Hay trạng thái các interfaces cần thiết trên các thiết bị đầu cuối ấy là 1 điều bắt buộc cần giám sát. Thiếp lập từng bước giám sát hệ thống mạng: tạo agent, cấu hình IP và sử dụng SNMP để kết nối tới cho các host windows server và linux server trong hệ thống.

#### Các bước để tạo và giám sát Agent:

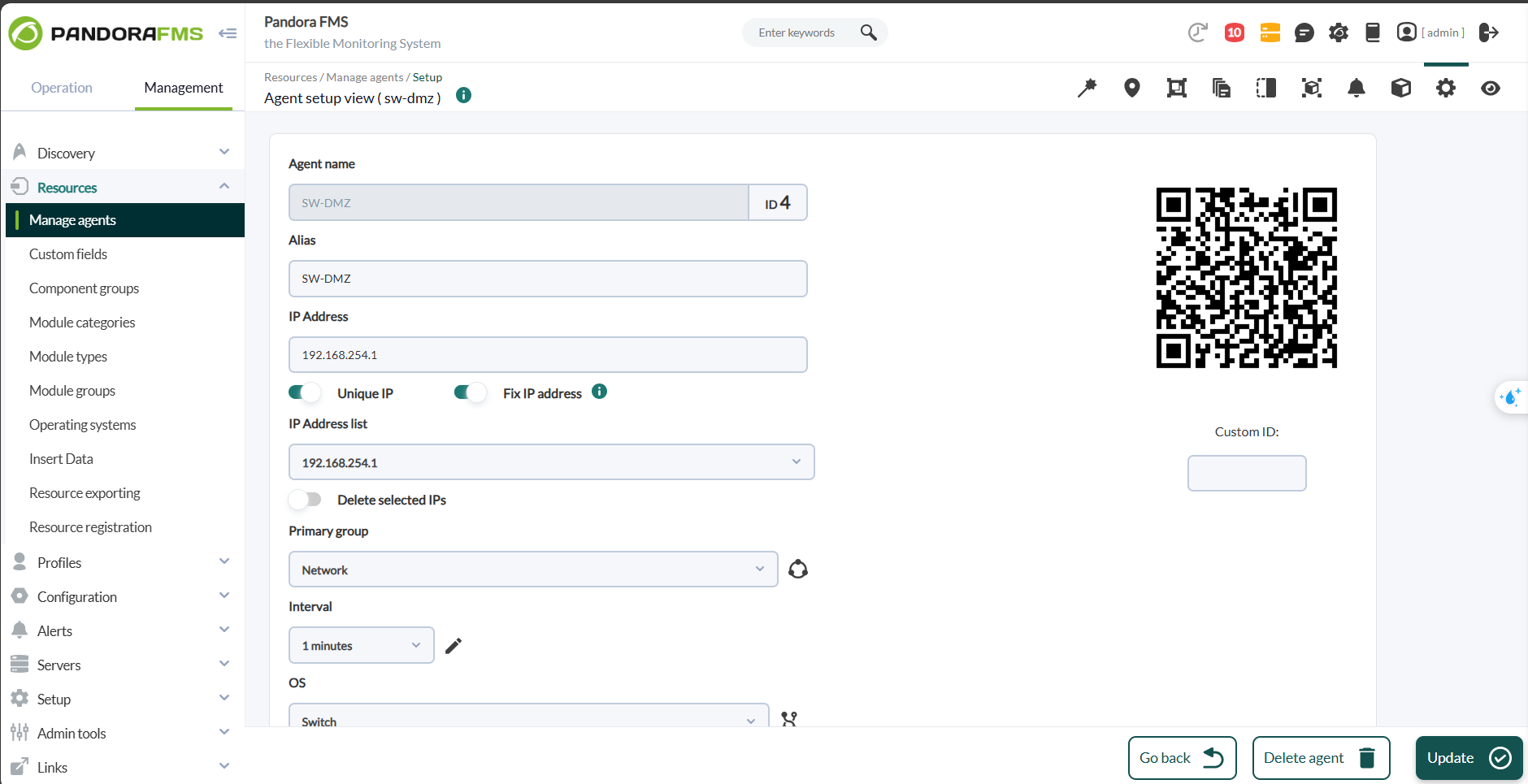
* + Bước 1 : Tạo Agent và thêm thông tin về thiết bị. Sau đó lưu lại.



Hình : Tạo Agent và điền thông tin về thiết bị

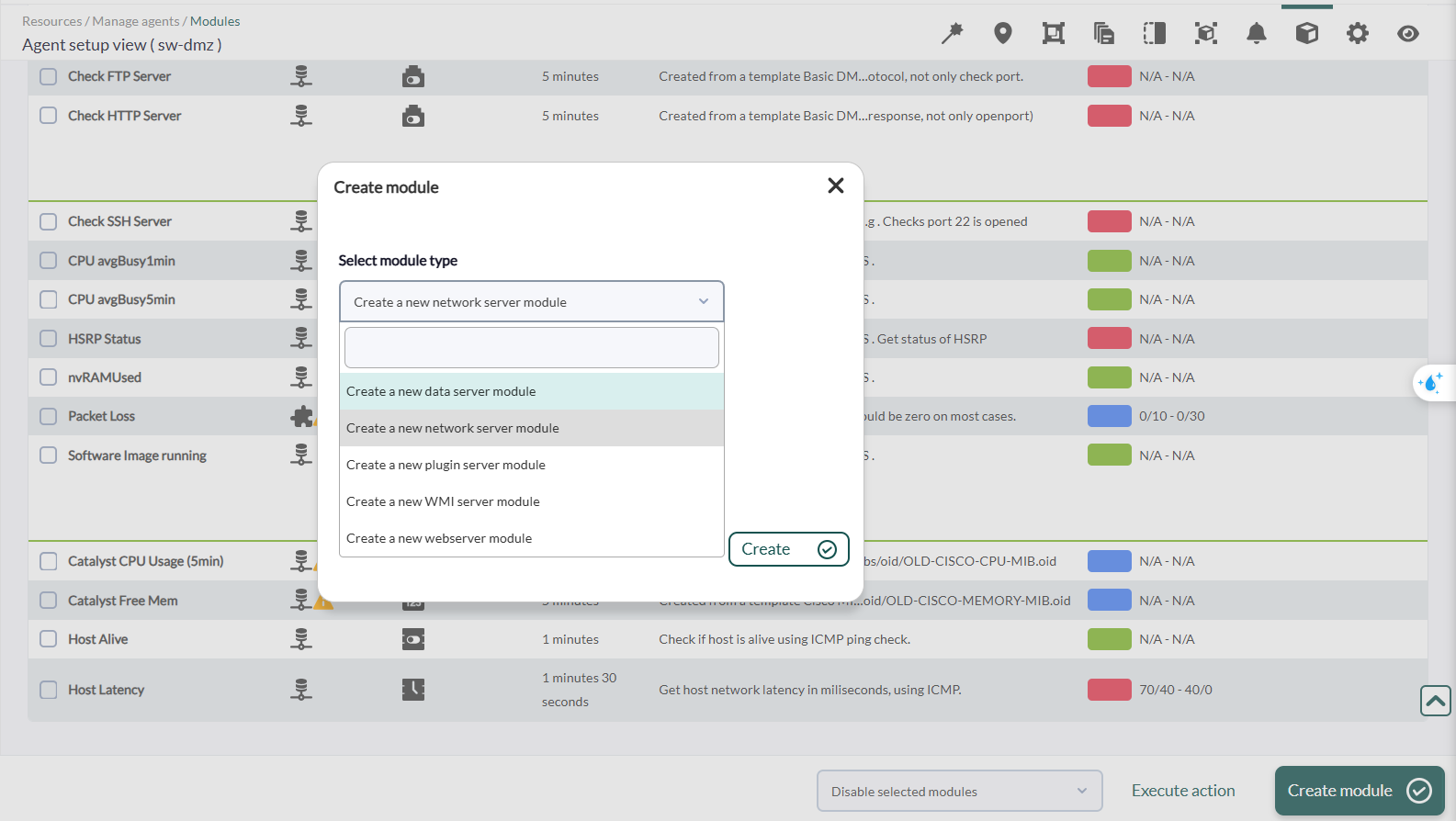
Điền các thông tin cấu hình về thiết bị:

* + - Alias: SW-DMZ.
    - IP Address: 192.168.254.1
    - Check Unique IP và Fix IP address.
    - Primary group: Network.
    - Interval (khoảng thời gian cập nhật thiết bị): 5 minutes.
    - OS (Hệ điều hành): Switch.
    - Server: AN-PHUC.healthy.hospital.vn
    - Description: Connect to switch cisco agent to monitoring.

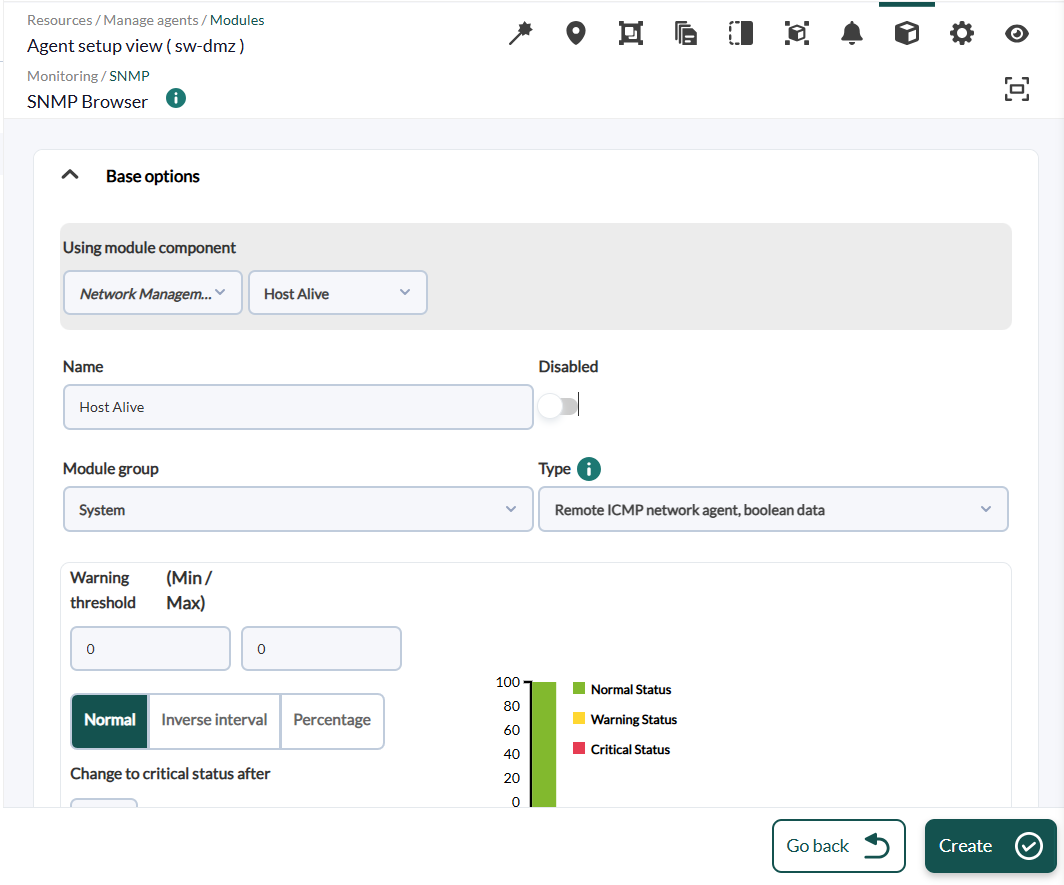


Hình : Điền các thông tin về agent

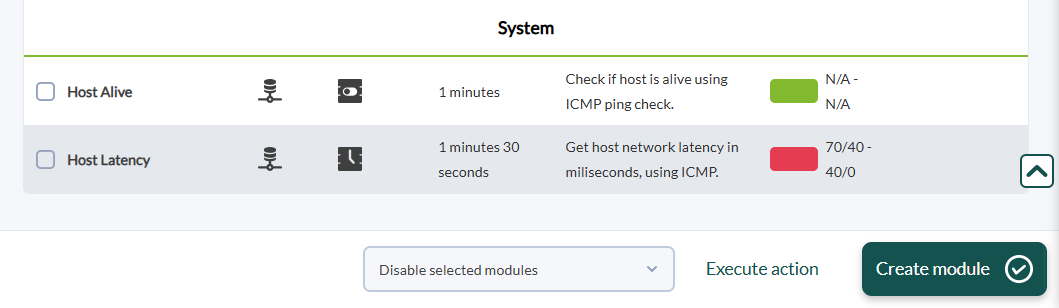
* Bước 2: Tạo các modules có sẵn để thực hiện việc giám sát thông qua giao thức SNMP
* Nhấn vào Create module, sau đó chọn Create a new network server module.



* Tạo modules Host Alive và Host Latency ở group System để kiểm tra tình trạng hoạt động và độ trễ của thiết bị thông qua phương thức ICMP trả về kết quả Boolean data và latency.



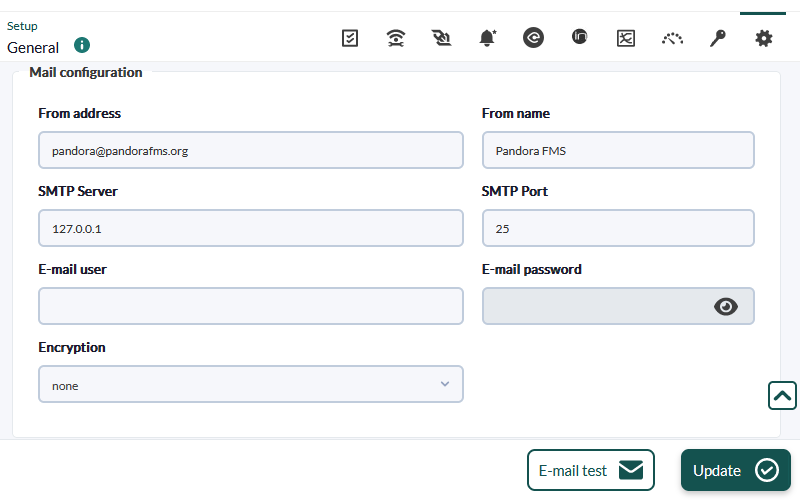
* Bước 3: Kiểm tra modules.
* Ở bước này ta sẽ đợi thời gian phản hồi và xem thông tin chi tiết về modules đã tạo.



#### Thiết lập cảnh báo

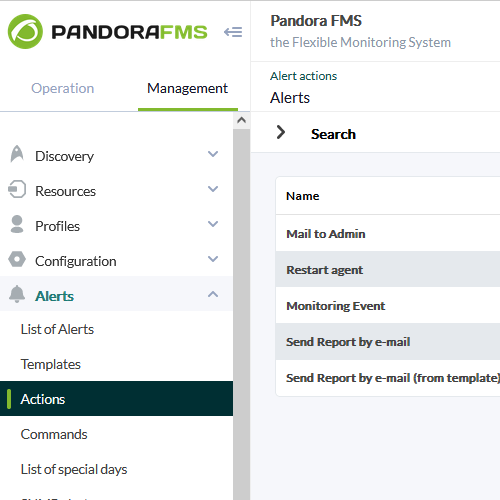
1. Cảnh báo gửi về email.

Pandora FMS đã chứa trong cài đặt của nó một máy chủ để gửi email, có người gửi mặc định là pandora@pandorafms.org .Mặc dù nói chung chúng được phân loại là SPAM bởi bất kỳ người nhận nào. Trong trường hợp bạn muốn thay đổi địa chỉ email phụ trách gửi thông báo và máy chủ xử lý chúng, hãy chuyển đến bảng điều khiển, đến phần Thiết lập > Thiết lập > Thiết lập chung. Ở cuối trang cấu hình, bạn sẽ tìm thấy phần cấu hình thư.



Hình : Thiết lập cảnh báo về email

* Để có thể định cấu hình người nhận cảnh báo, hãy sửa đổi hành động. Hành động là "Thư đến XXX" trong Cảnh báo > Hành động.
* Nhấp vào tên hành động để thêm cấu hình. Thực hiện theo menu "Cảnh báo -> Hành động".



1. Cảnh báo gửi về Telegram

**KẾT LUẬN**

**TÀI LIỆU THAM KHẢO**

[1] [[PDF]Giáo trình An toàn bảo mật thông tin.pdf (tailieumienphi.vn)](https://tailieumienphi.vn/doc/giao-trinh-an-toan-bao-mat-thong-tin-8b3guq.html)

[2] [Hướng dẫn cài đặt CentOS 7 trên VMware đầy đủ nhất (kdata.vn)](https://kdata.vn/tin-tuc/huong-dan-cai-dat-centos7-tren-vmware-day-du-nhat)

[3] [How To Install pandorafms-agent on Ubuntu 22.04 | Installati.one](https://installati.one/install-pandorafms-agent-ubuntu-22-04/)

[4] [Installation [current] (pandorafms.com)](https://pandorafms.com/manual/!current/en/documentation/pandorafms/installation/01_installing)

[5] [Giáo trình an toàn và bảo mật thông tin (haui.edu.vn)](https://lic.haui.edu.vn/vn/gioi-thieu-sach-moi/giao-trinh-an-toan-va-bao-mat-thong-tin/78159)

[6] [Giáo trình an toàn và bảo mật thông tin (tmu.edu.vn)](https://dlib.tmu.edu.vn/entities/publication/b5522f94-6988-479e-8515-39e00706ab61)

*.*