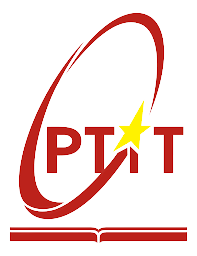
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA CÔNG NGHỆ THÔNG TIN 2**

--🙢🕮🙠--



**BÁO CÁO CHƯƠNG 3**

**THỰC NGHIỆM**

**Môn:**

**Kỹ Thuật Theo Dõi, Giám Sát An Toàn Mạng**

**GIẢNG VIÊN HƯỚNG DẪN : TS HUỲNH THANH TÂM**

Thực hiện đề tài :

* Nguyễn Hoàng Đại Nghĩa – N19DCAT054 – D19CQAT01-N

**TP.HCM, tháng 04/2023**

## CHƯƠNG 3:

# KẾT QUẢ THỰC NGHIỆM

Contents

[CHƯƠNG 3: 2](#_Toc133617188)

[KẾT QUẢ THỰC NGHIỆM 2](#_Toc133617189)

[**3.1** **Kịch bản 1: Phát hiện một cuộc tấn công SQL injection** 2](#_Toc133617190)

[**a)** **Nội dung lí thuyết:** 2](#_Toc133617191)

[**b)** **Triển khai:** 2](#_Toc133617192)

[**3.2** **Kịch bản 2:** **Giám sát các sự kiện Docker** 3](#_Toc133617193)

[**a)** **Nội dung lí thuyết:** 3](#_Toc133617194)

[**b)** **Triển khai:** 4](#_Toc133617195)

[**3.3** **Kịch bản 3:** **Giám sát tính toàn vẹn của tệp** 6](#_Toc133617196)

[**a)** **Nội dung lí thuyết :** 6](#_Toc133617197)

[**b)** **Triển khai:** 7](#_Toc133617198)

1. **Kịch bản 1: Phát hiện một cuộc tấn công SQL injection**
2. **Nội dung lí thuyết:**

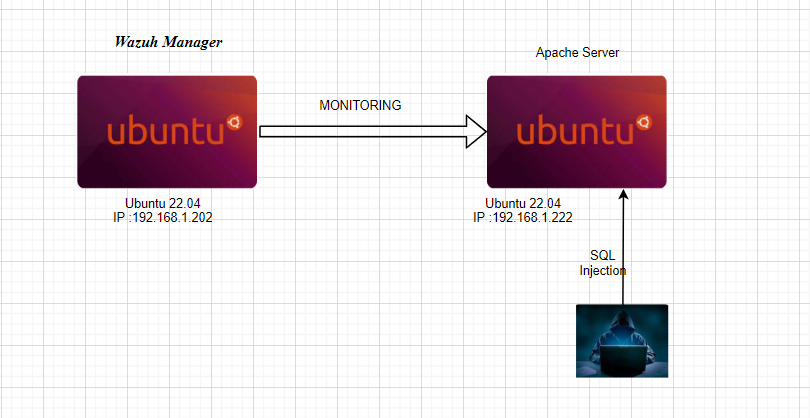
* SQL injection là một cuộc tấn công trong đó kẻ đe dọa chèn mã độc hại vào các chuỗi được truyền đến máy chủ cơ sở dữ liệu để phân tích cú pháp và thực thi. Một cuộc tấn công SQL injection thành công cho phép truy cập trái phép vào thông tin bí mật có trong cơ sở dữ liệu.
* Bạn có thể sử dụng Wazuh để phát hiện các cuộc tấn công tiêm nhiễm SQL từ nhật ký máy chủ web có chứa các mẫu như **select, union** và các mẫu tiêm nhiễm SQL phổ biến khác.

1. **Triển khai:**

* **Chuẩn bị môi trường:**

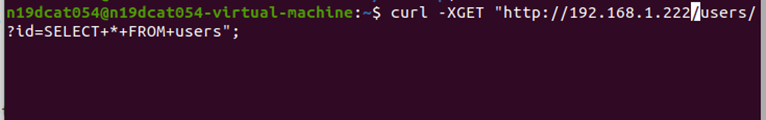
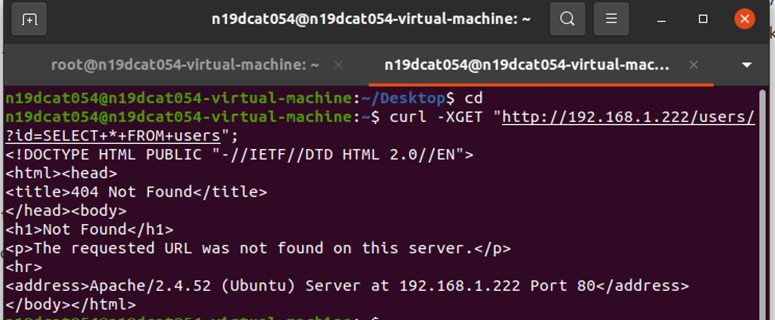
***Wazuh manager:***Ubuntu 22.04 – IP:192.168.1.202

***Apache Server:*** Ubuntu 22.04 – IP:192.168.1.222

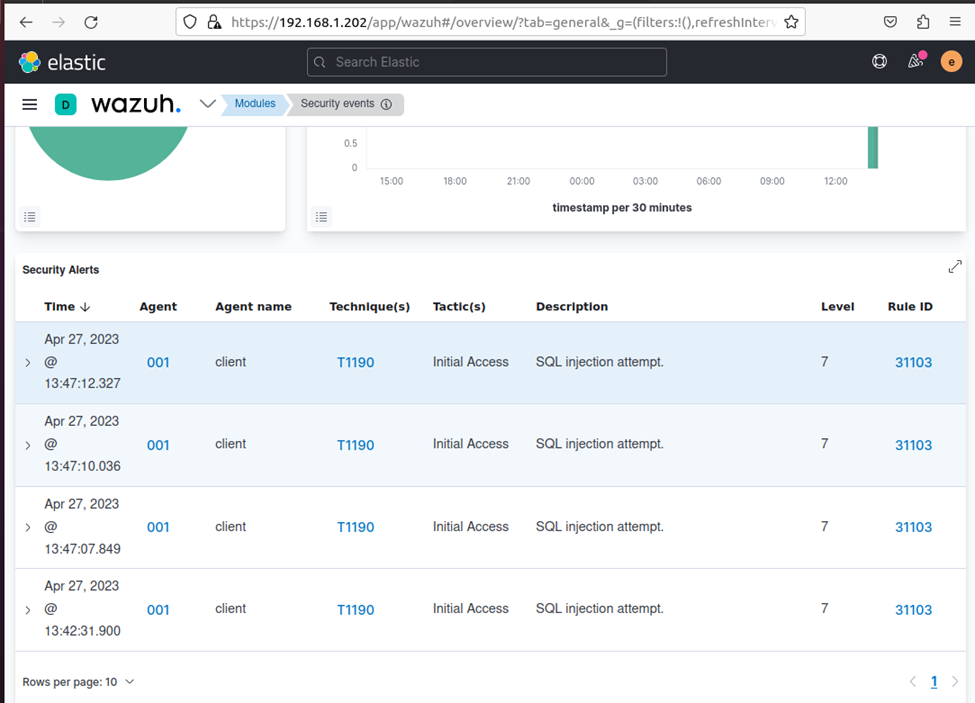
****

* **Demo:**

Hacker thực hiện câu lệnh tấn công SQL Injection đến máy chủ Apache Server



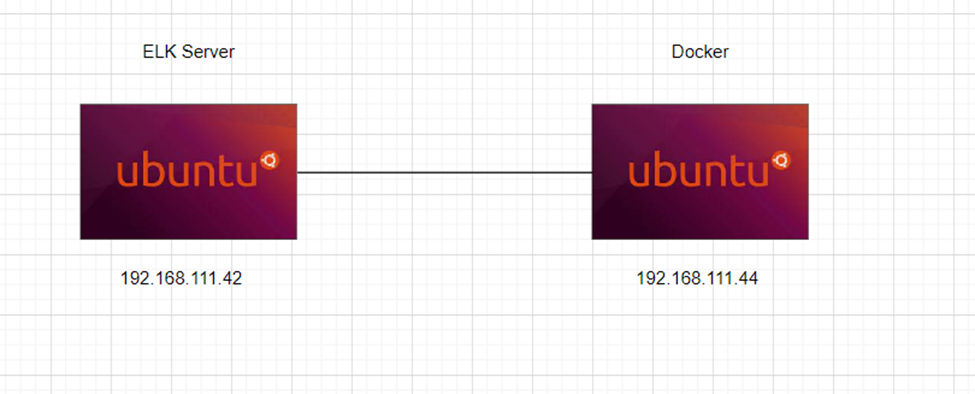
Tại trình duyệt của Wazuh manager , Ta thấy Agent alert rằng đã phát hiện được Tấn công SQL injection attempt vào máy chủ apache.



1. **Kịch bản 2:** **Giám sát các sự kiện Docker**
2. **Nội dung lí thuyết:**

* Giám sát sự kiện trong Docker ( hay Monitoring Docker events) là quá trình giám sát và thu thập thông tin về hoạt động của các container và hệ thống Docker. Khi triển khai các ứng dụng trong môi trường Docker, việc giám sát sự kiện là một phần quan trọng để theo dõi và phân tích hiệu suất, sự ổn định và tài nguyên sử dụng của các container và hệ thống Docker.
* Ý nghĩa của việc giám sát các sự kiện của Docker:
* Phát hiện lỗ hổng bảo mật: Wazuh giúp phát hiện các hoạt động xâm nhập và các vấn đề bảo mật có thể xảy ra trong môi trường Docker, bảo vệ hệ thống khỏi các cuộc tấn công và lỗ hổng bảo mật.
* Giám sát hiệu suất: Wazuh cho phép bạn theo dõi tài nguyên sử dụng của Docker, bao gồm CPU, bộ nhớ

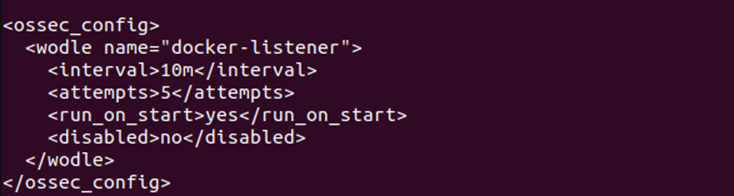
1. **Triển khai:**

****

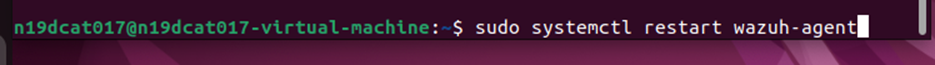
**Chuẩn bị môi trường:**

* *Cài đặt Wazuh Manager:* Tạo một máy chủ hoặc máy ảo để cài đặt Wazuh Manager. Có thể sử dụng phiên bản OS Linux phổ biến như CentOS hoặc Ubuntu.
* *Cài đặt Docker:* Cài đặt Docker trên máy chủ hoặc máy ảo Docker host.
* Cài đặt Wazuh Agent trên Docker host:
* *Cài đặt Wazuh Agent*: Trên Docker host, cài đặt Wazuh Agent và cấu hình nó để kết nối với Wazuh Manager. Agent sẽ thu thập thông tin sự kiện từ Docker host và các container chạy trên nó.
* *Cấu hình Wazuh Agent:* Thiết lập cấu hình Wazuh Agent để đảm bảo rằng nó sẽ thu thập nhật ký và thông tin sự kiện từ Docker Daemon và các container Docker.
* **Cấu hình Wazuh Manager:**
* Quy tắc giám sát Docker: Tạo và cấu hình quy tắc giám sát cho Docker trong Wazuh Manager. Quy tắc này sẽ xác định các hoạt động không bình thường và các vấn đề bảo mật có thể xảy ra trong môi trường Docker.
* Phát hiện xâm nhập: Cấu hình các quy tắc an ninh trong Wazuh Manager để phát hiện các hành vi xâm nhập trong Docker.
* **Xem và quản lý sự kiện:**
* Giao diện Wazuh Manager: Truy cập vào giao diện người dùng của Wazuh Manager để xem và quản lý các sự kiện, cảnh báo và báo cáo từ Docker.
* Cảnh báo và thông báo: Cấu hình cảnh báo và thông báo trong Wazuh Manager để nhận thông báo về các sự kiện bất thường trong Docker qua email, tin nhắn hoặc tích hợp với các hệ thống giám sát khác.
* **Demo:**

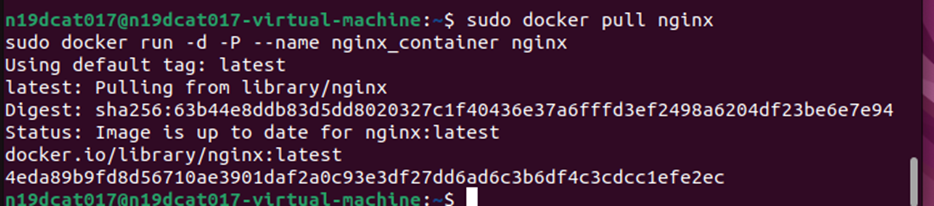
Sau khi cấu hình wazuh manager và wazuh agent ta vào file /var/ossec/etc/ossec.conf và thêm khối sau để kích hoạt mô-đun docker-listener:



Tiếp theo ta khỏi động lại wazuh-agent bằng lệnh sau :



Bây giờ, ta sẽ thử pull một image bất kì về và run nó lên thành container ở Docker host.

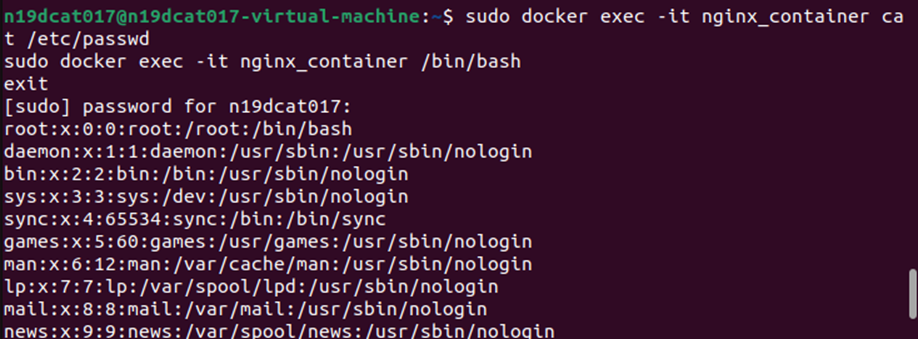


Qua ELKServer , mở wazuh manager, vào event của agent tương ứng với Docker host

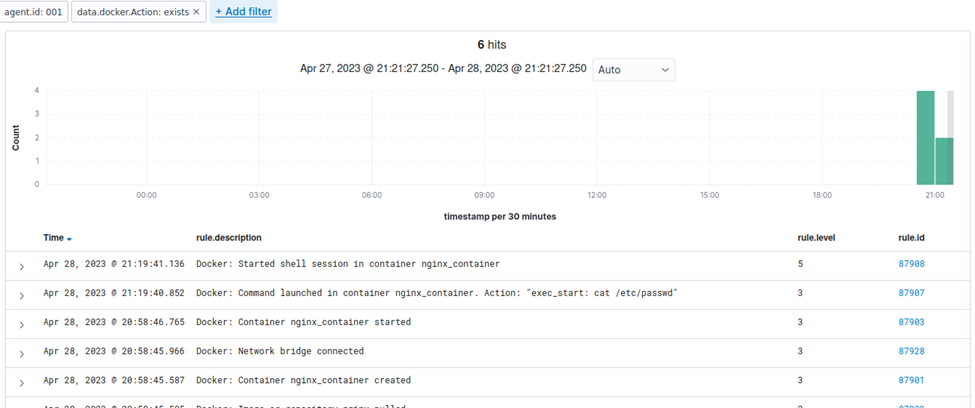


Ta thấy Agent alert rằng đã có một image được pull về và có một container được tạo và chạy với tên ngixn\_container

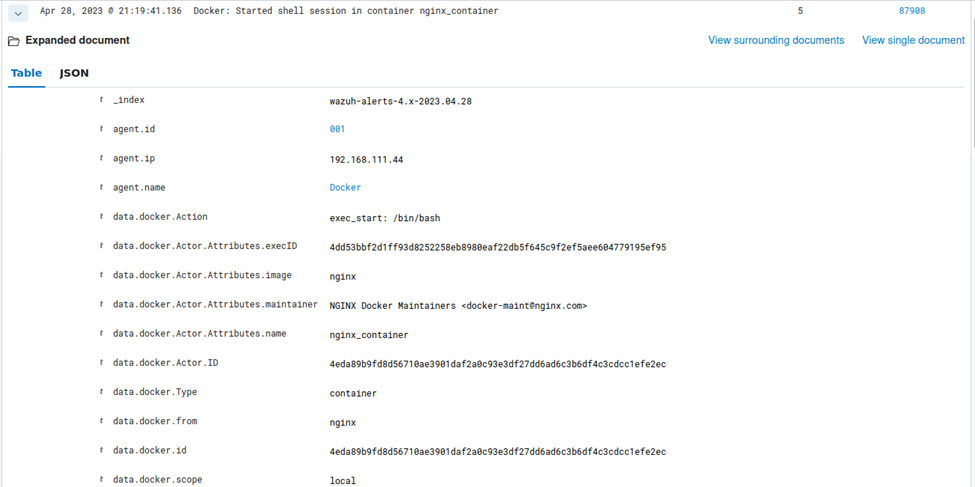
Qua Docker host ta chạy thử một số lệnh trên container



Ta qua Wazuh manager để xem thông báo Agent alert. Ta có thể filter data.Docker.Action để có thể filter các alert liên quan đến Docker



Ta có thể click vào dấu mũi tên nằm ngang ( > ) để có thể xem chi tiết về alert



Ở đây ta có thể thấy các thông tin về Agent.ip , Action, Type,….

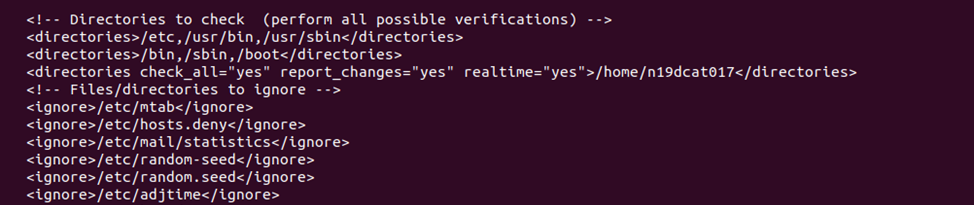
* 1. **Kịch bản 3:** **Giám sát tính toàn vẹn của tệp**

1. **Nội dung lí thuyết :**

* Giám sát tính toàn vẹn của tệp (File Integrity Monitoring - FIM) là quá trình giám sát và theo dõi sự thay đổi và thay đổi không mong muốn trong tệp tin hệ thống. Nó bao gồm việc kiểm tra tính toàn vẹn của các tệp tin bằng cách so sánh chúng với các giá trị băm (hash) hoặc thông qua quy tắc và mẫu được định nghĩa trước.
* Quan trọng nhất, FIM cung cấp khả năng phát hiện sự thay đổi bất thường trong tệp tin, như các tệp tin bị sửa đổi, xóa, thêm mới hoặc di chuyển. Điều này có thể xảy ra do các hành động không mong muốn, lỗ hổng bảo mật, tấn công xâm nhập hoặc các sự kiện không được ủy quyền.
* **Các tính năng và lợi ích của việc giám sát tính toàn vẹn của tệp tin bao gồm:**
* Phát hiện sớm các sự thay đổi bất thường: FIM giúp phát hiện sớm các hành vi xâm nhập, tấn công hoặc các hoạt động không mong muốn bằng cách cung cấp cảnh báo khi có sự thay đổi không được phép trong tệp tin.
* Bảo vệ dữ liệu và hệ thống: Bằng cách giám sát tính toàn vẹn của tệp, FIM giúp bảo vệ dữ liệu quan trọng và ngăn chặn các hành vi phá hoại hoặc lỗ hổng bảo mật trên hệ thống.
* Tuân thủ quy định và tiêu chuẩn bảo mật: FIM giúp đáp ứng các yêu cầu tuân thủ quy định và tiêu chuẩn bảo mật như PCI-DSS, HIPAA, GDPR và CIS benchmarks bằng cách cung cấp khả năng theo dõi và báo cáo sự thay đổi trong tệp tin.
* Điều tra và phân tích sự cố: Khi xảy ra sự cố hoặc vi phạm bảo mật, FIM cung cấp thông tin chi tiết về các sự thay đổi trong tệp tin, giúp điều tra nguyên nhân và phân tích hậu quả.

1. **Triển khai:**

* Tương tự như giám sát các sự kiện Docker, sau khi cấu hình wazuh manager và wazuh agent ta chỉnh sửa tệp cấu hình tác nhân Wazuh /var/ossec/etc/ossec.conf. Thêm các thư mục để theo dõi trong <syscheck> khối. Đối với trường hợp sử dụng này, bạn định cấu hình Wazuh để giám sát thư mục /home/n19dcat017. Để có thêm thông tin về người dùng và quy trình đã thực hiện các thay đổi.



Sau đó ta sẽ restart wazuh-agent với lệnh sau:



Sau khi restart ta sẽ thử tạo một file trên thư muc /home/n19dcat017

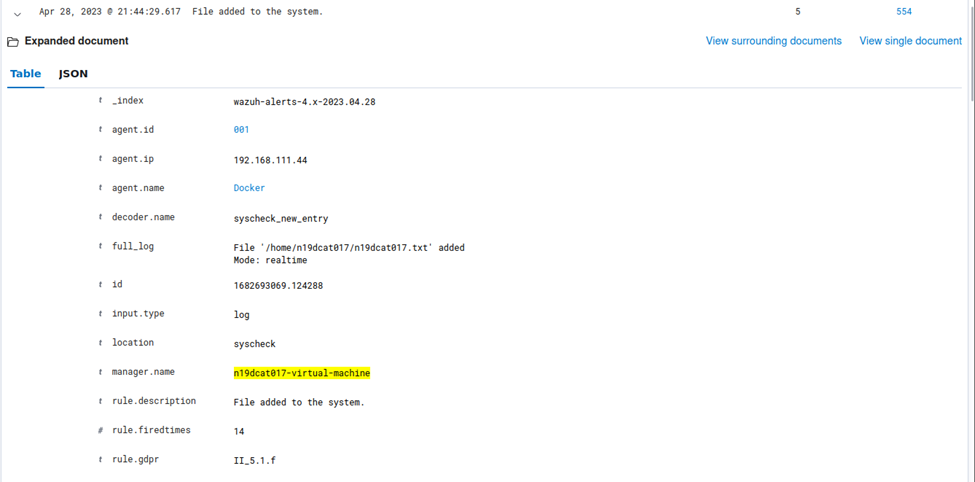


Ta có thể qua wazuh manaegr để kiểm tra agent alert



Ta thấy alert thông báo về việc có file được tạo ở tính toàn vẹn của tệp đã thay đổi

Ta có thể click vào dấu mũi tên để xem chi tiết thông tin của alert



Ta có thể thấy chi tiết alert hiển thị về path, về agent.name, description,…

# 