

TP Hồ Chí Minh, năm 2022

The logo of the University of Transport and Communications (UTC) is a circular emblem. It features a yellow outer ring with the text "TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI" in Vietnamese and "UNIVERSITY OF TRANSPORT AND COMMUNICATIONS" in English. The center is a dark blue circle containing a stylized yellow graphic of a ship or a bridge structure.

TP Hồ Chí Minh, năm 2022

NHIỆM VỤ BÁO CÁO
MÔN: AN NINH MẠNG

-----***-----

Họ và tên: Hoàng Minh Tài	MSSV: 6051071102
Họ và tên: Nguyễn Hoàng Hiệp	MSSV: 6051071147
Họ và tên: Cao Lâm Bảo Khanh	MSSV: 6051071056
Họ và tên: Nguyễn Hữu Đại	MSSV: 6051071023
Họ và tên: Trương Được	MSSV: 6051071033
Khóa: 60	Lớp: CQ.60.CNTT

1. Tên đề tài

Wazuh

2. Mục tiêu

HIDS/ giám sát hệ thống

3. Các kết quả chính dự kiến sẽ đạt được

Hiểu mô hình giám sát/phát hiện tấn công với Wazuh, thực hiện một cuộc tấn công. Thực hiện: Detect an SSH brute-force attack. Detect an RDP brute force attack

4. Giảng viên và cán bộ hướng dẫn

- Giảng viên: Phan Thanh Hy.
- Đơn vị công tác: Trường đại học Giao thông Vận tải Phân hiệu tại Thành phố Hồ Chí Minh.

LỜI CẢM ƠN

Lời đầu tiên, em xin gửi lời cảm ơn chân thành đến Trường Đại học Giao Thông Vận Tải - Phân hiệu tại thành phố Hồ Chí Minh đã đưa ngành Công nghệ thông tin vào chương trình đào tạo. Đặc biệt là quý thầy, cô giáo trong Bộ môn Công nghệ thông tin – những người đã dành cả tâm huyết để chỉ dạy và truyền đạt những kiến thức, kinh nghiệm của mình cho chúng em.

Trong những năm học tập tại trường, với những gì thầy cô truyền đạt, bản thân em đã tiếp thu được những kiến thức cơ bản các môn học và ngày càng hiểu rõ về ngành mà em đã lựa chọn. Không những thế, dưới mái trường này, em còn được học những kỹ năng mà có lẽ nó sẽ giúp em không ít trong sự nghiệp tương lai. Để hoàn thành được báo cáo này, em xin bày tỏ lòng biết ơn chân thành và sâu sắc đến thầy Phan Thanh Hy, giảng viên dạy bộ môn An ninh mạng, người đã trực tiếp hướng dẫn, dìu dắt, giúp đỡ chúng em với những chỉ dẫn khoa học quý giá trong suốt quá trình triển khai, nghiên cứu và hoàn thành báo cáo. Như người ta thường nói, người thầy như một nhà làm vườn, đêm ngày ươm trồng chăm sóc cho hạt giống của mình mong sao chúng có thể lớn nhanh để có ích cho đời. Hạt giống mà thầy cô gieo trồng chính là hạt giống tâm hồn – sự nghiệp trồng người. Cảm ơn thầy đã cho chúng em thứ tài sản vô giá, là hành trang vững chắc để chúng em có thể bước từng bước vào cuộc sống đầy chông gai và thử thách của cuộc sống.

Do kiến thức còn hạn chế và khả năng tiếp thu chưa được hoàn hảo nên chúng em khó tránh được những sai sót trong quá trình làm bài. Mong thầy/cô thông cảm và góp ý thêm cho bài báo cáo nhóm em.

Sau cùng, em xin kính chúc quý thầy cô trong Bộ môn Công nghệ thông tin và toàn thể quý thầy cô đang giảng dạy tại Trường Đại học Giao Thông Vận Tải - Phân hiệu tại thành phố Hồ Chí Minh lời chúc sức khỏe, luôn hạnh phúc và thành công hơn nữa trong công việc cũng như cuộc sống.

Em xin chân thành cảm ơn!

NHẬN XÉT CỦA GIÁO VIÊN

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Tp. Hồ Chí Minh, ngày ... tháng ... năm ...
Giảng viên hướng dẫn

Phan Thanh Hy

MỤC LỤC

Contents

CHƯƠNG I: KHÁI NIỆM VỀ WAZUH.....	1
1. Giới thiệu về Wazuh.....	1
2. Các thành phần.....	1
CHƯƠNG II: HỆ THỐNG PHÁT HIỆN XÂM NHẬP OSSEC.....	4
1. Tổng quan về IDS	4
2. Tổng quan về hệ thống phát hiện xâm nhập OSSEC.....	5
CHƯƠNG III: CÀI ĐẶT WAZUH	8
1. Cài đặt Wazuh.....	8
2. Cài đặt CentOS	10
CHƯƠNG IV: TẤN CÔNG.....	11
1. Thực hiện tấn công.....	11
2. Detect an SSH brute-force attack	16
CHƯƠNG V: TỔNG KẾT	20
1. Kết quả đạt được.....	20

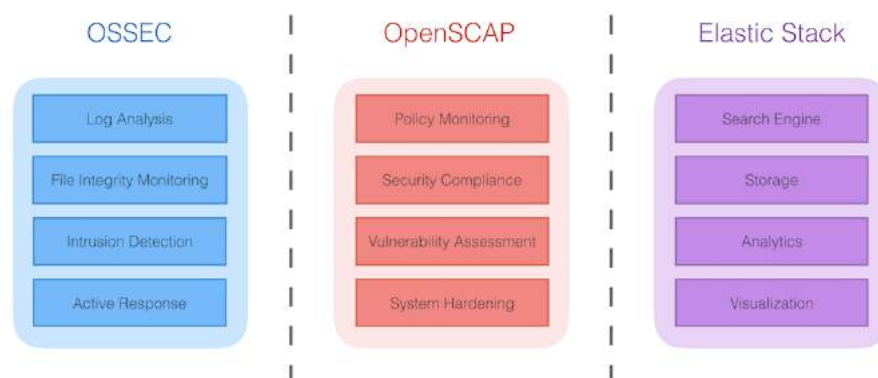
DANH MỤC HÌNH ẢNH

Hình 1. Trang chủ Wazuh	8
Hình 2. IP address.....	9
Hình 3. Login Wazuh	9
Hình 4. Add agent	9
Hình 5. Add agent guide.....	10
Hình 6. Add command	10
Hình 7. Add command	11
Hình 8. Add command	11
Hình 9. Kết quả	11
Hình 10. Tấn công SSH.....	12
Hình 11. SSH btute-force attack.....	16

CHƯƠNG I: KHÁI NIỆM VỀ WAZUH

1. Giới thiệu về Wazuh

Wazuh là 1 project mã nguồn dùng cho việc bảo vệ an ninh. Được xây dựng từ các thành phần : OSSEC HIDS, OpenSCAP và Elastic Stack.



- **OSSEC HIDS:** host-based Intrusion Detection System (HIDS) được dùng cho việc phát hiện xâm nhập, hiển thị và giám sát. Nó dựa vào một multi-platform agent cho việc đẩy dữ liệu hệ thống (log message, file hash và phát hiện bất thường) tới một máy quản lý trung tâm, nơi sẽ phân tích và xử lý, dựa trên các cảnh báo an ninh. Các agent truyền event data tới máy quản lý trung tâm thông qua kênh được bảo mật và xác thực. OSSEC HIDS cung cấp syslog server trung tâm và hệ thống giám sát không cần agent, cung cấp việc giám sát tới các event và thay đổi trên các thiết bị không cài được agent như firewall, switch, router, access point, thiết bị mạng...
- **OpenSCAP:** OpenSCAP là một OVAL (Open Vulnerability Assessment Language) và XCCDF (Extensible Configuration Checklist Description Format) được dùng để kiểm tra cấu hình hệ thống và phát hiện các ứng dụng dễ bị tấn công. Nó được biết đến như là một công cụ được thiết kế để kiểm tra việc tuân thủ an ninh của hệ thống sử dụng các tiêu chuẩn an ninh dùng cho môi trường doanh nghiệp.
- **ELK Stack:** Sử dụng cho việc thu thập, phân tích, index, store, search và hiển thị dữ liệu log.

2. Các thành phần

2.1 Wazuh agent

Chạy trên: Windows, Linux, Solaris, BSD hoặc MAC OS. Dùng thu thập các dạng khác nhau của dữ liệu hệ thống và ứng dụng. Dữ liệu được chuyển tới Wazuh

server thông qua một kênh được mã hóa và xác thực. Để thiết lập kênh này, một quá trình đăng ký bao gồm pre-shared key duy nhất được thiết lập.

Các agent có thể dùng để giám sát server vật lý, máy ảo, cloud instance (AWS, Azure hoặc Google cloud). Các cài đặt pre-compile agent có sẵn cho các OS : Linux, AIX, Solaris, Windows và Darwin (Mac OS X).

Trên các OS Unix-based, agent chạy trên multiple process, các process này liên lạc với nhau thông qua local Unix domain socket. 1 trong các process này phụ trách việc liên lạc và gửi dữ liệu tới Wazuh server. Trên Windows, chỉ có 1 agent process chạy trên multiple task sử dụng mutexes.

Các agent task hoặc process khác nhau được dùng để giám sát hệ thống theo các cách khác nhau (giám sát sự thay đổi về file, đọc log, quét các thay đổi hệ thống). Tất cả các process agent có mục tiêu và thiết lập khác nhau.

- Rootcheck: Thực hiện các task liên quan đến phát hiện về Rootkits, malware và các bất thường của hệ thống. Nó chạy 1 số công cụ kiểm tra an ninh cơ bản dựa vào các file cấu hình hệ thống.
- Log Collector: Dùng để đọc và thu thập các log message, bao gồm các file flat log như Windows event log và thậm chí là Windows Event Channel. Nó cũng được cấu hình để chạy định kỳ và bắt 1 số output của các câu lệnh cụ thể.
- Syscheck: Process này thực hiện file integrity monitoring (FIM) (Giám sát tính toàn vẹn của file). Nó cũng có thể giám sát registry key trên Windows. Nó sẽ bắt các thay đổi về nội dung file, quyền và các thuộc tính khác, cũng như phát hiện việc tạo và xóa file.
- OpenSCAP: Được dùng để publish OVAL và XCCDF dựa vào các hồ sơ bảo mật cơ bản, định kỳ quét hệ thống, nó sẽ phát hiện được các ứng dụng và cấu hình sẽ bị tấn công, không tuân theo các chuẩn được xác định theo CIS (Center of Internet Security).
- Agent Daemon : Process nhận dữ liệu được tạo hoặc được thu thập bởi tất cả các thành phần agent khác. Nó nén, mã hóa và phân phối dữ liệu tới server thông qua kênh được xác thực. Process này chạy trên "chroot" environment được cô lập, có nghĩa rằng nó sẽ hạn chế truy cập tới các hệ thống được giám sát. Điều này cải thiện được an toàn cho agent vì process đó là process duy nhất kết nối tới mạng.

Chú giải:

- Rootkits: Phần mềm hoặc công cụ phần mềm che giấu sự tồn tại của 1 phần mềm khác, thường là virus xâm nhập vào hệ thống.

- Malware: Mọi loại mã gây hại trên máy tính người dùng : spyware, trojan, virus...

2.2 Wazuh server

Thành phần server phụ trách việc phân tích dữ liệu nhận từ agent, tạo các ngưỡng cảnh báo khi 1 event ánh xạ với rule (phát hiện xâm nhập, thay đổi file, cấu hình không tương thích với policy, rootkit...).

Server thông thường chạy các thành phần agent với mục tiêu giám sát chính nó. Một số thành phần server chính là :

- Registration service : Được dùng để register agent mới được việc cung cấp và phân phối các key xác thực pre-shared, các key này là độc nhất với mỗi agent. Process này chạy như 1 network service và hỗ trợ việc xác thực qua TLS/SSL với 1 fixed password.
- Remote daemon service : Service này nhận dữ liệu từ agent. Nó sử dụng pre-shared key để xác thực định danh của mỗi agent và mã hóa giao tiếp với chúng.
- Analysis daemon : Process này thực hiện việc phân tích dữ liệu. Nó sử dụng các bộ giải mã để nhận dạng thông tin được xử lý (các Windows event, SSHD logs...) và sau đó giải nén các yếu tố dữ liệu thích hợp từ log message (source ip, event id, user...) Sau đó, bằng cách sử dụng các rule được định nghĩa bằng cách pattern đặc biệt trên bộ giải mã, nó sẽ tạo các ngưỡng cảnh báo thậm chí ra lệnh để thực hiện các biện pháp đối phó như chặn IP trên firewall.
- RESTful API : Cung cấp interface để quản lý và giám sát cấu hình và trạng thái triển khai của các agent. Nó cũng được dùng bởi Wazuh web interface (Kibana).

Wazuh tích hợp với Elastic stack để cung cấp các log message đã được giải mã và đánh index bởi Elasticsearch, cũng như là 1 web console real-time cho việc cảnh báo và phân tích log. Wazuh web interface (chạy trên Kibana) có thể dùng để quản lý và giám sát hạ tầng Wazuh.

Một Elasticsearch index là một tập hợp các document có một chút các đặc trưng tương tự nhau (như các trường chung hoặc các yêu cầu về data retention được chia sẻ). Wazuh sử dụng 3 index khác nhau, được tạo hàng ngày và lưu trữ các dạng event khác nhau :

- Wazuh-alert : Index cho các cảnh báo được sinh ra bởi Wazuh server mỗi khi một event ứng với rule tạo ra.
- Wazuh-events : Index cho tất cả các event (archive data) được nhận từ các agent, bất kể có ứng với rule hay không.
- Wazuh- monitoring: Index cho dữ liệu liên quan đến trạng thái agent. Nó được dùng bởi web interface cho việc hiển thị agent đã hoặc đang "Active", "Disconnect" hoặc "Never connected".

Với các index trên, document là các cảnh báo, archived event hoặc status event riêng lẻ.

Một Elasticsearch index được chia tới 1 hoặc nhiều shard, và mỗi shard có thể có 1 hoặc nhiều replica. Mỗi primary và replica shard là 1 Lucene index đơn lẻ. Vì vậy 1 Elasticsearch index được tạo bởi nhiều Lucene index. Khi 1 tìm kiếm chạy trên 1 Elasticsearch index, search đó được xử lý trên các shard song song, và kết quả được merge lại. Việc chia nhỏ các Elasticsearch tới nhiều shard và replica cũng được dùng với Elasticsearch cluster với mục tiêu là mở rộng việc tìm kiếm và HA. Một Elasticsearch cluster single-node thường chỉ có 1 shard mỗi index và không có replica.

CHƯƠNG II: HỆ THỐNG PHÁT HIỆN XÂM NHẬP OSSEC

1. Tổng quan về IDS

1.1 Hệ thống phát hiện xâm nhập IDS

IDS là hệ thống phát hiện các dấu hiệu của tấn công xâm nhập, đồng thời có thể khởi tạo các hành động trên thiết bị khác để ngăn chặn tấn công. Khác với tường lửa, IDS không thực hiện các thao tác ngăn chặn truy nhập mà chỉ theo dõi các hoạt động trên mạng để tìm ra các dấu hiệu của tấn công và cảnh báo cho người quản trị mạng. Một điểm khác biệt khác đó là mặc dù cả hai đều liên quan đến bảo mật mạng, nhưng tường lửa theo dõi sự xâm nhập từ bên ngoài và ngăn chặn chúng xảy ra, nó giới hạn truy nhập giữa các mạng để ngăn chặn sự xâm nhập nhưng không phát hiện được cuộc tấn công từ bên trong mạng. Bên cạnh đó IDS sẽ đánh giá sự xâm nhập đáng ngờ khi nó đã diễn ra đồng thời phát ra cảnh báo, nó theo dõi được các cuộc tấn công có nguồn gốc từ bên trong một hệ thống. Chức năng ban đầu của IDS chỉ là phát hiện các dấu hiệu xâm nhập, do đó IDS chỉ có thể tạo ra các cảnh báo tấn công khi tấn công đang diễn ra hoặc thậm chí sau khi tấn công đã hoàn tất. Càng về sau, nhiều kỹ thuật mới được tích hợp vào IDS, giúp nó có khả năng dự đoán được tấn công (prediction) và thậm chí phản ứng chủ động các tấn công đang diễn ra (Active response).

1.2 Phân loại

Dựa trên phạm vi giám sát, IDS được chia thành 2 loại:

- Network-based IDS (NIDS): Là những IDS giám sát trên toàn bộ mạng. Nguồn thông tin chủ yếu của NIDS là các gói dữ liệu đang lưu thông trên mạng. NIDS thường được lắp đặt tại ngõ vào của mạng, có thể đứng trước hoặc sau tường lửa.
- Host-based IDS (HIDS): Là những IDS giám sát hoạt động của từng máy tính riêng biệt. Do vậy, nguồn thông tin chủ yếu của HIDS ngoài lưu lượng

dữ liệu đến và đi từ máy chủ còn có hệ thống dữ liệu nhật ký hệ thống (system log) và kiểm tra hệ thống (system audit).

Dựa trên kỹ thuật phát hiện, IDS cũng được chia thành 2 loại:

- Signature-based IDS: Signature-based IDS phát hiện xâm nhập dựa trên dấu hiệu của hành vi xâm nhập, thông qua phân tích lưu lượng mạng và log hệ thống. Kỹ thuật này đòi hỏi phải duy trì một cơ sở dữ liệu về các dấu hiệu xâm nhập (signature database), và cơ sở dữ liệu này phải được cập nhật thường xuyên mỗi khi có một hình thức hoặc kỹ thuật xâm nhập mới.
- Anomaly-based IDS: phát hiện xâm nhập bằng cách so sánh (mang tính thống kê) các hành vi hiện tại với hoạt động bình thường của hệ thống để phát hiện các bất thường (anomaly) có thể là dấu hiệu của xâm nhập. Ví dụ, trong điều kiện bình thường, lưu lượng trên một giao tiếp mạng của server là vào khoảng 25% băng thông cực đại của giao tiếp. Nếu tại một thời điểm nào đó, lưu lượng này đột ngột tăng lên đến 50% hoặc hơn nữa, thì có thể giả định rằng server đang bị tấn công DoS. Để hoạt động chính xác, các IDS loại này phải thực hiện một quá trình học, tức là giám sát hoạt động của hệ thống trong điều kiện bình thường để ghi nhận các thông số hoạt động, đây là cơ sở để phát hiện các bất thường về sau.

2. Tổng quan về hệ thống phát hiện xâm nhập OSSEC

2.1 Giới thiệu

OSSEC là hệ thống phát hiện xâm nhập dựa trên host (HIDS) dựa trên log mã nguồn mở, miễn phí, đa nền tảng có thể mở rộng và có nhiều cơ chế bảo mật khác nhau. OSSEC có thể phát hiện xâm nhập bằng cả chữ ký hoặc dấu hiệu bất thường. Các dấu hiệu bình thường và bất thường được mô tả trong bộ luật của OSSEC. OSSEC có một công cụ phân tích và tương quan mạnh mẽ, tích hợp giám sát và phân tích log, kiểm tra tính toàn vẹn của file, kiểm tra registry của Windows, thực thi chính sách tập trung, giám sát chính sách, phát hiện rootkit, cảnh báo thời gian thực và phản ứng một cách chủ động cuộc tấn công đang diễn ra. Các hành động này cũng có thể được định nghĩa trước bằng luật trong OSSEC để OSSEC hoạt động theo ý muốn của người quản trị. Ngoài việc được triển khai như một HIDS, nó thường được sử dụng như một công cụ phân tích log, theo dõi và phân tích các bản ghi lại, IDS, các máy chủ Web và các bản ghi xác thực. OSSEC chạy trên hầu hết các hệ điều hành, bao gồm Linux, OpenBSD, FreeBSD, Mac OS X, Sun Solaris và Microsoft Windows. OSSEC còn có thể được tích hợp trong các hệ thống bảo mật lớn hơn là SIEM (Security information and event management). OSSEC chỉ có thể cài đặt trên Windows với tư cách là một agent.

*Ưu điểm của HIDS: HIDS có một số điểm cải tiến hơn so với NIDS

- Phù hợp với môi trường dữ liệu mã hóa ngày càng phổ biến. HIDS có khả năng đọc được các dữ liệu (log) được mã hóa tại server nhận.
 - Thích hợp trong các mạng được chuyển đổi nơi mà chỉ có máy chủ lưu trữ cuối cùng mới có thể nhìn thấy lưu lượng truy cập.
 - Theo dõi được các tiến trình sử dụng của người dùng tại máy chủ.
 - Có khả năng phát hiện và phản ứng với thời gian thực.
 - Xác minh khả năng của một cuộc tấn công. NIDS thường đưa ra một cảnh báo sớm, còn HIDS có khả năng xác minh xem một cuộc tấn công hay xâm nhập trái phép có khả năng thành công hay thất bại.
 - Khắc phục các cuộc tấn công mà NIDS không thể cảnh báo được như tấn công phân mảnh hay ghép nối phiên.
- ➔ Vì những lý do như vậy mà OSSEC được phát triển theo HIDS chứ không phải NIDS.

*Các tính năng nổi bật của OSSEC là:

- Theo dõi và phân tích các log: OSSEC thu thập log theo thời gian thực từ nhiều nguồn khác nhau để phân tích (giải mã, lọc và phân loại) và đưa ra cảnh báo dựa trên bộ luật được xây dựng trước. OSSEC phát hiện các cuộc tấn công trên mạng, hệ thống hoặc ứng dụng cụ thể bằng cách sử dụng log làm nguồn thông tin chính. Log cũng rất hữu ích để phát hiện việc khai thác lỗ hổng phần mềm, vi phạm chính sách và các hình thức hoạt động không phù hợp khác. Một số loại log mà OSSEC có thể phân tích là log proxy, log web, log ghi lại xác thực, system log.
- Kiểm tra tính toàn vẹn của file: Sử dụng hàm băm mật mã, có thể tính toán giá trị băm của mỗi file trong hệ điều hành dựa trên tên file, nội dung file và giá trị băm này là duy nhất. OSSEC có thể giám sát các ổ đĩa để phát hiện các thay đổi của giá trị băm này khi có ai đó, hoặc điều gì đó, sửa đổi nội dung của file hoặc thay thế phiên bản file này bằng một phiên bản file khác.
- Giám sát Registry: Hệ thống Registry là danh sách thư mục tất cả các cài đặt phần cứng và phần mềm, các cấu hình hệ điều hành, người dùng, nhóm người dùng, và các preference trên một hệ thống Microsoft Windows. Các thay đổi được thực hiện bởi người dùng và quản trị viên đối với hệ thống được ghi lại trong các khóa registry để các thay đổi được lưu khi người dùng đăng xuất hoặc hệ thống được khởi động lại. Registry cũng cho thấy kernel của hệ điều hành tương tác với phần cứng và phần mềm máy tính như thế nào. HIDS có thể giám sát những thay đổi này đối với các khóa registry quan trọng để đảm

đảm bảo rằng người dùng hoặc ứng dụng không cài đặt một chương trình mới hoặc sửa đổi chương trình hiện có với mục đích xấu.

- **Phát hiện Rootkit:** OSSEC phát hiện Rootkit dựa trên chữ ký, rootkit là công cụ cho phép kẻ đột nhập khả năng xâm nhập trở máy tính bị cài rootkit và xóa dấu vết về sự tồn tại của nó. Kẻ xâm nhập có thể sử dụng rootkit để ăn cắp thông tin và tài nguyên từ máy tính nạn nhân. OSSEC có khả năng phát hiện rootkit bằng cách đọc file cơ sở dữ liệu về rootkit và tiến hành quét hệ thống định kỳ, thực hiện các lời gọi hệ thống để phát hiện các file không bình thường, các tiến trình ẩn, các dấu hiệu vượt quyền, các cổng ẩn và so sánh chúng với cơ sở dữ liệu để phát hiện rootkit.
- **Phản ứng chủ động:** Phản ứng chủ động cho phép các IDS nói chung và OSSEC nói riêng tự động thực thi các lệnh hoặc phản ứng khi một sự kiện hoặc tập hợp sự kiện cụ thể được kích hoạt. Phản ứng chủ động có thể được xác định bằng luật. Các lợi ích của phản ứng chủ động là rất lớn, nhưng cũng rất nguy hiểm, có thể ngăn chặn kết nối hợp pháp hoặc là lỗ hổng để kẻ tấn công khai thác. Ví dụ: quản trị viên hợp pháp có thể tạo ra báo động sai và chặn người dùng/máy chủ hợp pháp truy cập nếu các luật được thiết kế kém.

2.2 Kiến trúc và quy trình hoạt động của OSSEC

a. Kiến trúc

OSSEC được thiết kế theo mô hình client server, gồm 2 thành phần chính là OSSEC server và OSSEC agent

OSSEC server:

- Đây là phần trung tâm và quan trọng nhất của OSSEC. Server là nơi lưu trữ dữ liệu. Tất cả các luật, bộ giải mã (decoder) cũng được lưu trữ trên server.
- Server còn đảm nhận nhiệm vụ quản lý các agent. Các agent kết nối với máy chủ trên cổng 1514 hoặc 514, giao thức UDP. Kết nối với cổng này phải được cho phép để các agent kết nối với manager.
- Nhiệm vụ quan trọng nhất của server là phân tích các log nhận được từ các agent hay agentless (gọi chung là client) và xuất ra các cảnh báo. Các cảnh báo này có thể xuất ra cho các công cụ xử lý log như Logstash, Elastic Search để hiển thị cho người quản trị bằng Kibana, lưu trữ trong cơ sở dữ liệu.

OSSEC Agent:

- Agent (đầy đủ là installable agent) là một chương trình nhỏ, hoặc tập hợp các chương trình, được cài đặt trên các hệ thống được giám sát.

- Agent sẽ thu thập thông tin và gửi cho manager để phân tích và so sánh. Một số thông tin được thu thập trong thời gian thực, những thông tin khác theo định kỳ.
- Agent có một bộ nhớ rất nhỏ và sử dụng rất ít CPU, không ảnh hưởng đến việc sử dụng của hệ thống. Server cấu hình cho các agent. Các agent được cài đặt trên các host và chúng gửi lại các log cho server thông qua giao thức thông điệp được mã hóa OSSEC.
- Các modul chức năng của agent là: giám sát host, kiểm tra tính toàn vẹn file trên máy host mà nó được cài, phát hiện rootkit trên máy host, đọc các log và gửi các log cho server.

Quy trình hoạt động

OSSEC hoạt động theo mô hình Client Server:

- Các agent có trách nhiệm theo dõi và thu thập log từ các máy host được cài đặt, mã hóa chúng và gửi cho server theo giao thức UDP, cổng 1514.
- Server chịu trách nhiệm nhận log từ agent và phân tích chúng, so sánh với các luật.
- Log đã được xử lý sẽ được server chuyển về hệ thống được tích hợp ELK để lưu trữ và hiển thị cảnh báo cho admin theo giao diện web.

CHƯƠNG III: CÀI ĐẶT WAZUH

1. Cài đặt Wazuh

Truy cập vào trang web wazuh.com

- Document → Deployment → Virtual Machine (OVA) → Download virtual appliance (OVA) phiên bản 4.2 (current)



Hình 1. Trang chủ Wazuh

Chú ý : Network Adapter chọn Bridged (Automatic)

- Wazuh-manager login: root

- Password: wazuh
- # ip add

```

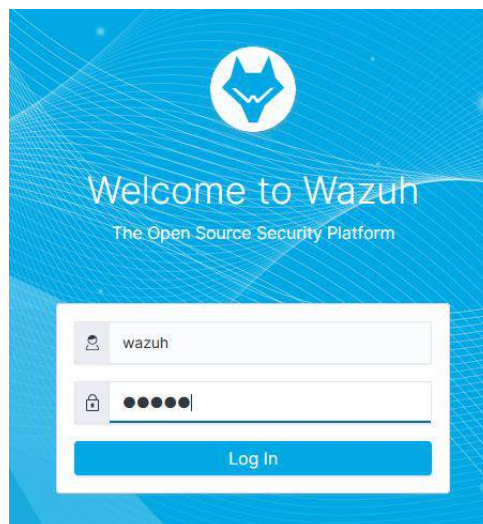
[root@wazuh-manager ~]# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:c6:48:43 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.7/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 3416sec preferred_lft 3416sec
    inet6 2402:800:6347:d907:20c:29ff:fec6:4843/64 scope global mngtmpaddr dynamic
        valid_lft 74660sec preferred_lft 74660sec
    inet6 fe80::20c:29ff:fec6:4843/64 scope link
        valid_lft forever preferred_lft forever
[root@wazuh-manager ~]#

```

Hình 2. IP address

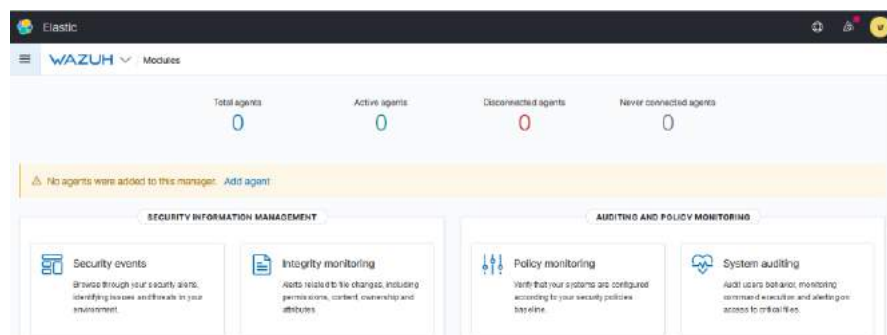
- <https://192.168.1.7> → Advanced... → Accept the Risk and Continue
- Login Wazuh, password: wazuh

Chú ý: khuyến khích dùng trình duyệt firefox



Hình 3. Login Wazuh

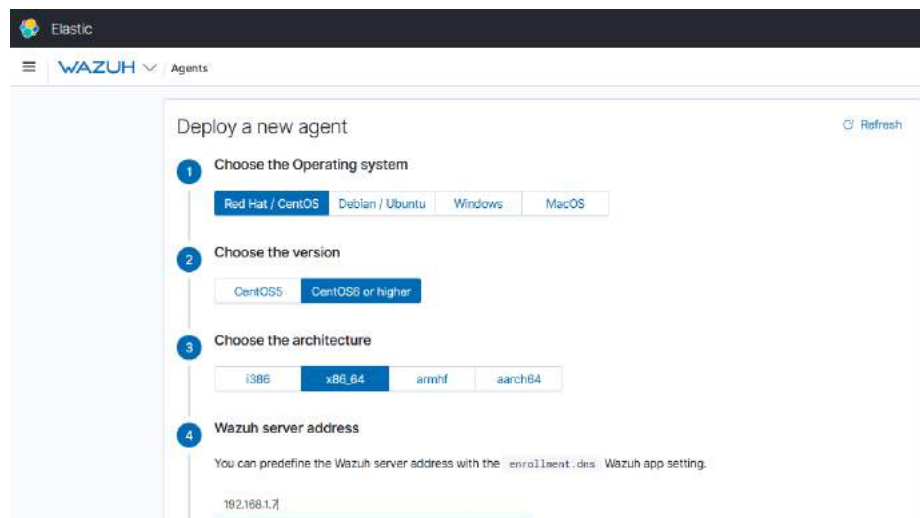
- Add Agent



Hình 4. Add agent

- Choose the Operating System: Red Hat / CentOS
- Choose the version: CentOS6 or higher
- Choose the Architecture: x86_64

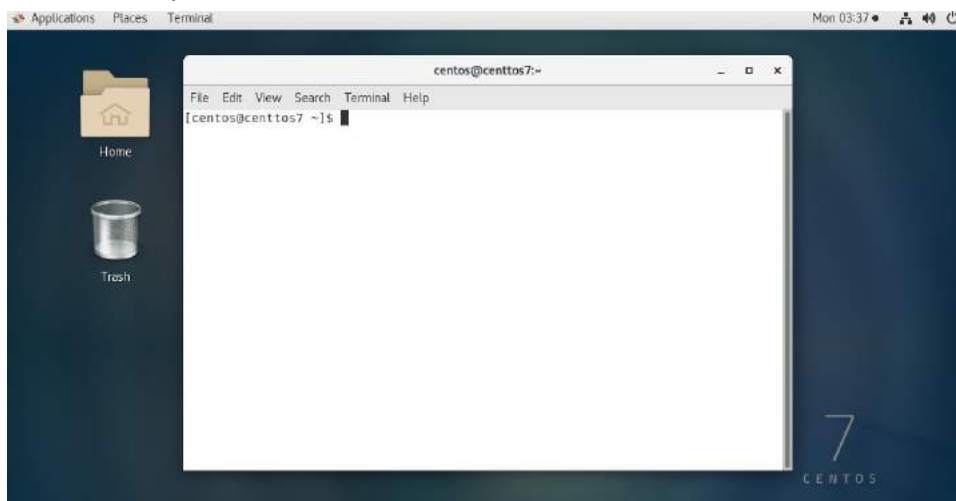
- Wazuh server address: 192.168.1.7
- Assign the agent to a group: default



Hình 5. Add agent guide

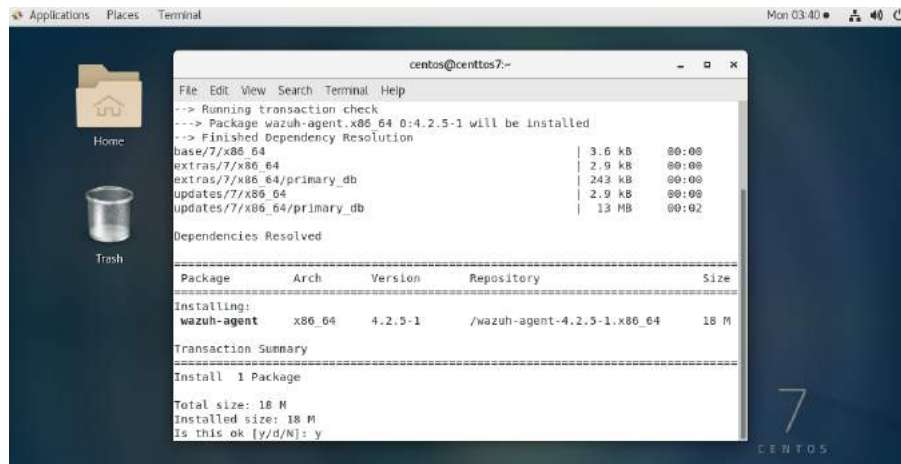
2. Cài đặt CentOS

- Download CentOS
- Import Virtual Machine
- Login CentOS
- Application → System tools → Terminal



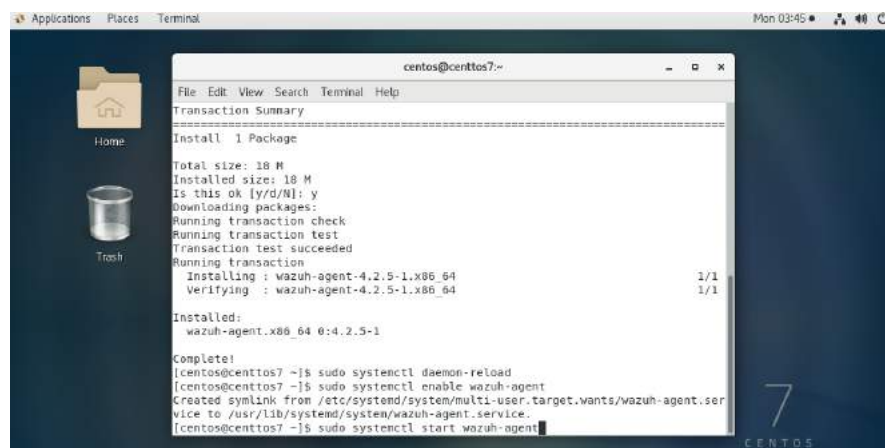
Hình 6. Add command

- Vào wazuh copy command trong Install and enroll the agent
- Vào lại CentOS dán command vào terminal rồi chọn y



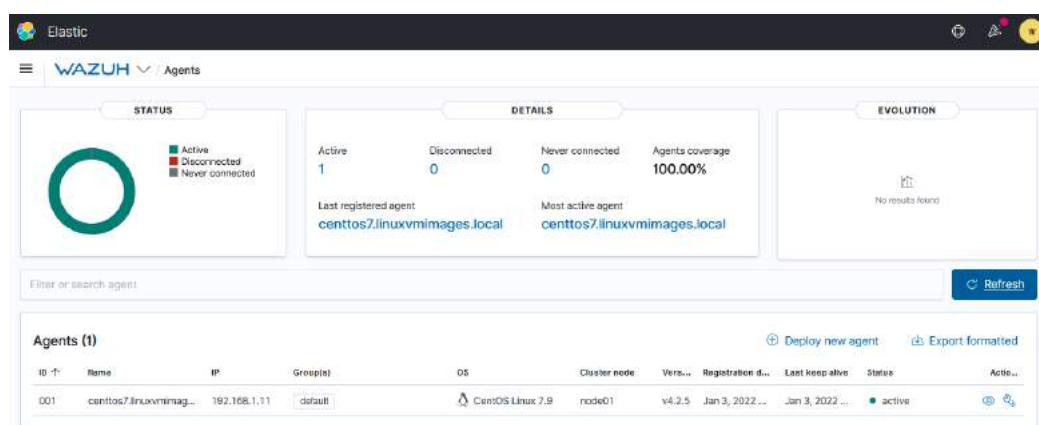
Hình 7. Add command

- Vào wazuh copy command trong Start the agent
- Vào CentOS dán command vào terminal



Hình 8. Add command

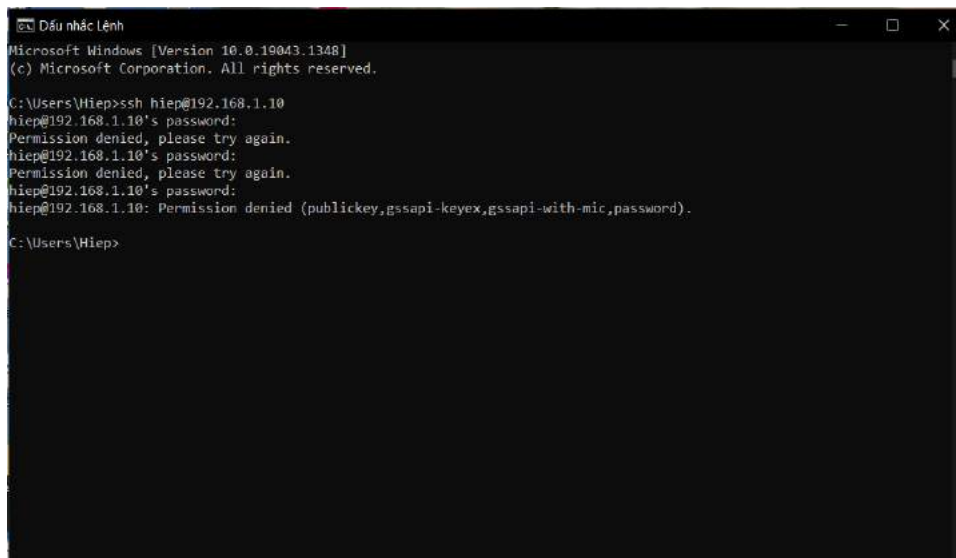
- Vào lại wazuh và F5



Hình 9. Kết quả

CHƯƠNG IV: TẤN CÔNG

1. Thực hiện tấn công



```
Dấu nhắc Lệnh
Microsoft Windows [Version 10.0.19043.1348]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Hiep>ssh hiep@192.168.1.10
hiep@192.168.1.10's password:
Permission denied, please try again.
hiep@192.168.1.10's password:
Permission denied, please try again.
hiep@192.168.1.10's password:
hiep@192.168.1.10: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).

C:\Users\Hiep>
```

Hình 10. Tấn công SSH

- JSON tấn công SSh

```
{
  "_index": "wazuh-alerts-4.x-2022.01.03",
  "_type": "_doc",
  "_id": "nR1DIH4Bp-PB1vUssaHt",
  "_version": 1,
  "_score": null,
  "_source": {
    "predecoder": {
      "hostname": "wazuh-manager",
      "program_name": "sshd",
      "timestamp": "Jan 3 14:06:48"
    },
    "input": {
      "type": "log"
    },
    "agent": {
      "name": "wazuh-manager",
      "id": "000"
```

```
},
"data": {
  "srcuser": "hiep",
  "srcip": "192.168.1.7"
},
"manager": {
  "name": "wazuh-manager"
},
"rule": {
  "mail": false,
  "level": 5,
  "pci_dss": [
    "10.2.4",
    "10.2.5",
    "10.6.1"
  ],
  "hipaa": [
    "164.312.b"
  ],
  "tsc": [
    "CC6.1",
    "CC6.8",
    "CC7.2",
    "CC7.3"
  ],
  "description": "sshd: Attempt to login using a non-existent user",
  "groups": [
    "syslog",
    "sshd",
```

```
"invalid_login",
"authentication_failed"
],
"nist_800_53": [
  "AU.14",
  "AC.7",
  "AU.6"
],
"gdpr": [
  "IV_35.7.d",
  "IV_32.2"
],
"firedtimes": 30,
"mitre": {
  "technique": [
    "Brute Force"
  ],
  "id": [
    "T1110"
  ],
  "tactic": [
    "Credential Access"
  ]
},
"id": "5710",
"gpg13": [
  "7.1"
]
},
```

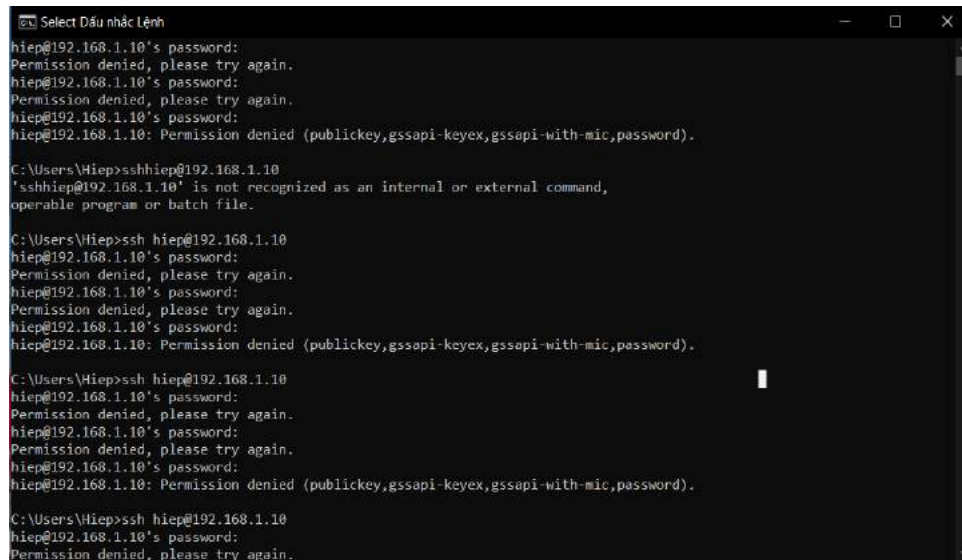
```

"location": "/var/log/secure",
"id": "1641218809.581120",
"decoder": {
  "parent": "sshd",
  "name": "sshd"
},
"full_log": "Jan  3 14:06:48 wazuh-manager sshd[3154]: Failed password for
invalid user hiep from 192.168.1.7 port 54040 ssh2",
"timestamp": "2022-01-03T14:06:49.837+0000"
},
"fields": {
  "timestamp": [
    "2022-01-03T14:06:49.837Z"
  ]
},
"highlight": {
  "manager.name": [
    "@kibana-highlighted-field@wazuh-manager@/kibana-highlighted-field@"
  ],
  "data.srcuser": [
    "@kibana-highlighted-field@hiep@/kibana-highlighted-field@"
  ],
  "full_log": [
    "Jan  3 14:06:48 wazuh-manager sshd[3154]: Failed password for invalid user
    @kibana-highlighted-field@hiep@/kibana-highlighted-field@ from 192.168.1.7 port
    54040 ssh2"
  ]
},
"sort": [
  1641218809837

```

```
]
}
```

2. Detect an SSH brute-force attack



```
Select Dấu nhắc Lệnh
hiep@192.168.1.10's password:
Permission denied, please try again.
hiep@192.168.1.10's password:
Permission denied, please try again.
hiep@192.168.1.10's password:
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).

C:\Users\Hiep>ssh hiep@192.168.1.10
'ssh hiep@192.168.1.10' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Hiep>ssh hiep@192.168.1.10
hiep@192.168.1.10's password:
Permission denied, please try again.
hiep@192.168.1.10's password:
Permission denied, please try again.
hiep@192.168.1.10's password:
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).

C:\Users\Hiep>ssh hiep@192.168.1.10
hiep@192.168.1.10's password:
Permission denied, please try again.
hiep@192.168.1.10's password:
Permission denied, please try again.
hiep@192.168.1.10's password:
Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).

C:\Users\Hiep>ssh hiep@192.168.1.10
hiep@192.168.1.10's password:
Permission denied, please try again.
```

Hình 11. SSH btute-force attack

- JSON SSH brute-force attack

```
{
  "_index": "wazuh-alerts-4.x-2022.01.03",
  "_type": "_doc",
  "_id": "hx1CIH4Bp-PBbvUsBKEa",
  "_version": 1,
  "_score": null,
  "_source": {
    "predecoder": {
      "hostname": "wazuh-manager",
      "program_name": "sshd",
      "timestamp": "Jan  3 14:05:01"
    },
    "input": {
      "type": "log"
    },
    "agent": {
```

```

    "name": "wazuh-manager",
    "id": "000"
  },
  "previous_output": "Jan 3 14:04:46 wazuh-manager sshd[3138]: Failed password for
invalid user hiep from 192.168.1.7 port 56184 ssh2\nJan 3 14:04:45 wazuh-manager
sshd[3138]: Failed password for invalid user hiep from 192.168.1.7 port 56184
ssh2\nJan 3 14:04:45 wazuh-manager sshd[3138]: Failed none for invalid user hiep
from 192.168.1.7 port 56184 ssh2\nJan 3 14:04:43 wazuh-manager sshd[3138]:
Invalid user hiep from 192.168.1.7 port 56184\nJan 3 14:04:28 wazuh-manager
sshd[3136]: Failed password for invalid user hiep from 192.168.1.7 port 54542
ssh2\nJan 3 14:04:26 wazuh-manager sshd[3136]: Failed none for invalid user hiep
from 192.168.1.7 port 54542 ssh2\nJan 3 14:04:27 wazuh-manager sshd[3136]: Failed
password for invalid user hiep from 192.168.1.7 port 54542 ssh2",
  "data": {
    "srcuser": "hiep",
    "srcip": "192.168.1.7"
  },
  "manager": {
    "name": "wazuh-manager"
  },
  "rule": {
    "mail": false,
    "level": 10,
    "pci_dss": [
      "11.4",
      "10.2.4",
      "10.2.5"
    ],
    "hipaa": [
      "164.312.b"
    ],
    "tsc": [
      "CC6.1",

```



```
"CC6.8",
"CC7.2",
"CC7.3"
],
"description": "sshd: brute force trying to get access to the system.",
"groups": [
  "syslog",
  "sshd",
  "authentication_failures"
],
"nist_800_53": [
  "SI.4",
  "AU.14",
  "AC.7"
],
"frequency": 8,
"gdpr": [
  "IV_35.7.d",
  "IV_32.2"
],
"fioredtimes": 1,
"mitre": {
  "technique": [
    "Brute Force"
  ],
  "id": [
    "T1110"
  ],
  "tactic": [
    "Credential Access"
```

```

    ]
  },
  "id": "5712"
},
"location": "/var/log/secure",
"decoder": {
  "parent": "sshd",
  "name": "sshd"
},
"id": "1641218701.568036",
"full_log": "Jan 3 14:05:01 wazuh-manager sshd[3140]: Failed none for invalid user
hiep from 192.168.1.7 port 56185 ssh2",
"timestamp": "2022-01-03T14:05:01.692+0000"
},
"fields": {
  "timestamp": [
    "2022-01-03T14:05:01.692Z"
  ]
},
"highlight": {
  "manager.name": [
    "@kibana-highlighted-field@wazuh-manager@/kibana-highlighted-field@"
  ],
  "data.srcuser": [
    "@kibana-highlighted-field@hiep@/kibana-highlighted-field@"
  ],
  "full_log": [
    "Jan 3 14:05:01 wazuh-manager sshd[3140]: Failed none for invalid user @kibana-
highlighted-field@hiep@/kibana-highlighted-field@ from 192.168.1.7 port 56185
ssh2"
  ]
}

```

```

},
"sort": [
  1641218701692
]
}

```

CHƯƠNG V: TỔNG KẾT

1. Kết quả đạt được

Hiểu mô hình giám sát/phát hiện tấn công với Wazuh, thực hiện một cuộc tấn công.

Thực hiện: Detect an SSH brute-force attack.

Tài liệu tham khảo

- Wazuh.com
- CentOS.com
- <https://www.youtube.com/watch?v=kd5THDYTarM>

Bảng phân công nhiệm vụ

Họ và tên	Nhiệm vụ	Hoàn thành
Hoàng Minh Tài	Cài đặt máy ảo VMWare + Wazuh-Manager + Add Agent + Detect SSH brute-force attack	100%
Nguyễn Hoàng Hiệp	Cài đặt VMWare, CentOS 7.9	100%
Cao Lâm Bảo Khanh	Tìm hiểu lý thuyết + Làm báo cáo + PowerPoint	100%
Nguyễn Hữu Đại	Cài đặt VMWare, CentOS 7.9	100%
Trương Được	Tìm hiểu lý thuyết + Làm báo cáo + PowerPoint	100%