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

**KHOA CƠ BẢN I**

**BỘ MÔN AN TOÀN MẠNG VIỄN THÔNG**



****

**AN TOÀN MẠNG VIỄN THÔNG**

**Xây dựng hệ thống HIDS phát hiện xâm nhập với Wazuh**

|  |  |
| --- | --- |
| **Giảng viên hướng dẫn** | **: Nguyễn Thanh Trà** |
| **Họ và tên sinh viên** | **: Ngô Trí Hoàng-B22DCVT207** |
|  | **: Đào Huy Hùng-B22DCVT223** |
|  | **: Bùi Quang Huy-B22DCVT231** |
|  | **: Phạm Huy Hoàng-B22DVT215** |
| **Lớp** | **: 07** |
| **Nhóm** | **: 05** |

***Hà Nội – 2025***

Mục lục

[Lời mở đầu 1](#_Toc212203327)

[Chương 1. Cơ sở lý thuyết 2](#_Toc212203328)

[1.1. Tổng quan về xâm nhập và kỹ thuật phát hiện xâm nhập. 2](#_Toc212203329)

[1.1.1 Xâm nhập 2](#_Toc212203330)

[1.1.2. Hệ thống phát hiện xâm nhập 4](#_Toc212203331)

[1.1.3. Phương pháp phát hiện xâm nhập: 6](#_Toc212203332)

[Chương 2. Thiết kế và Thực nghiệm 7](#_Toc212203333)

[2.1. Giới thiệu về  WAZUH 7](#_Toc212203334)

[2.2.1. Giới thiệu về wazuh 7](#_Toc212203335)

[2.2.2. Thành phần 7](#_Toc212203336)

[2.3. Thực hiện 9](#_Toc212203337)

[2.3.1. Phát hiện cuộc tấn công brute-force 9](#_Toc212203338)

[2.3.2. FIM 12](#_Toc212203339)

[2.3.3Ngăn chặn phần mềm độc hại với Wazuh 17](#_Toc212203340)

[2.3.4. Phát hiện các tiến trình ẩn 28](#_Toc212203341)

[Kết luận 32](#_Toc212203342)

**Thuật ngữ viết tắt**

|  |  |  |
| --- | --- | --- |
| **Từ viết tắt** | **Nghĩa tiếng Anh đầy đủ** | **Nghĩa tiếng Việt** |
| IDS | Intrusion Detection System | Hệ thống phát hiện xâm nhập |
| HIDS | Host-based Intrusion Detection System | Hệ thống phát hiện xâm nhập dựa trên máy chủ |
| NIDS | Network-based Intrusion Detection System | Hệ thống phát hiện xâm nhập dựa trên mạng |
| FIM | File Integrity Monitoring | Giám sát tính toàn vẹn tệp tin |
| SIEM | Security Information and Event Management | Quản lý thông tin và sự kiện bảo mật |
| XDR | Extended Detection and Response | Phát hiện và phản ứng mở rộng |
| API | Application Programming Interface | Giao diện lập trình ứng dụng |
| OVA | Open Virtual Appliance | Ảnh máy ảo đóng gói sẵn |
| LAN | Local Area Network | Mạng cục bộ |
| WAN | Wide Area Network | Mạng diện rộng |
| DNS | Domain Name System | Hệ thống phân giải tên miền |
| DoS | Denial of Service | Tấn công từ chối dịch vụ |
| GUI | Graphical User Interface | Giao diện đồ họa người dùng |
| SSH | Secure Shell | Giao thức kết nối bảo mật |
| EICAR | European Institute for Computer Antivirus Research | Viện nghiên cứu chống virus máy tính châu Âu |
| OSSEC | Open Source Security | Hệ thống bảo mật mã nguồn mở |
| SCAP | Security Content Automation Protocol | Giao thức tự động hóa nội dung bảo mật |
| XML | eXtensible Markup Language | Ngôn ngữ đánh dấu mở rộng |
| APIKEY | Application Programming Interface Key | Khóa truy cập API |
| IP | Internet Protocol | Giao thức Internet |

**Danh mục hình ảnh**

[Hình 1. Vị trí của hệ thống phát hiện xâm nhập IDS 4](#_Toc212237649)

[Hình 2. Mô hình hoạt động của wazuh 8](#_Toc212237650)

[Hình 3. Mô hinh lab tấn công brute-force 9](#_Toc212237651)

[Hình 4. Dùng Nmap tìm Port đang hoạt động 10](#_Toc212237652)

[Hình 5. Sử dụng hydra tấn công agent 11](#_Toc212237653)

[Hình 6. Cảnh báo ở wazuh events 11](#_Toc212237654)

[Hình 7. Nội dung cảnh báo brute-force 12](#_Toc212237655)

[Hình 8. Rules 5760 bắt cuộc tấn công 12](#_Toc212237656)

[Hình 9. Mô hình lab FIM 13](#_Toc212237657)

[Hình 10. Đặt thư mục theo dõi ở agent 14](#_Toc212237658)

[Hình 11. Khởi động lại agent 14](#_Toc212237659)

[Hình 12. Nội dung của file secret 14](#_Toc212237660)

[Hình 13. Thay đổi nội dung của file secret 15](#_Toc212237661)

[Hình 14. Thêm foder vào thư mục theo dõi 15](#_Toc212237662)

[Hình 15. Wazuh manager bắt được sự kiện FIM theo dõi 16](#_Toc212237663)

[Hình 16. Chi tiết về log Oct 18, 2025 17:17:03.452 File added to the system 16](#_Toc212237664)

[Hình 17. Chi tiết về Oct 18, 2025 17:16:57.572 Integrity checksum changed 17](#_Toc212237665)

[Hình 18. Rule 550 : dùng để phát hiện thay đổi nội dung tệp tin 17](#_Toc212237666)

[Hình 19. Rule 554 : dùng để phát hiện tệp tin mới được thêm vào hệ thống 17](#_Toc212237667)

[Hình 20. Mô hình lab ngăn chặn phần mềm độc hại 18](#_Toc212237668)

[Hình 21. Hình ảnh của wazuh group 19](#_Toc212237669)

[Hình 22. Thêm thư mục cần theo dõi trên manager 19](#_Toc212237670)

[Hình 23. Lấy apikey của virustotal 19](#_Toc212237671)

[Hình 24. Kích hoạt virustotal trên manager 20](#_Toc212237672)

[Hình 25. Khởi động lại wazuh manager 21](#_Toc212237673)

[Hình 26. Lệnh tải eicar về agent 21](#_Toc212237674)

[Hình 27. File Eicar đã được tải vào : C:\User\toila\Downloads 22](#_Toc212237675)

[Hình 28. Cảnh báo về file mã độc đã được gửi về manager 22](#_Toc212237676)

[Hình 29. Ảnh check được file mã độc eicar trên Virustotal.com 23](#_Toc212237677)

[Hình 30. Tạo file python đặt tập lệnh chủ động phản hồi 23](#_Toc212237678)

[Hình 31. Chuyển đổi file python thành ứng dụng thực thi 24](#_Toc212237679)

[Hình 32. File remove-threat.exe đã được tạo. 25](#_Toc212237680)

[Hình 33. Thêm phản hồi chủ động vào manager 25](#_Toc212237681)

[Hình 34. Lệnh vào local rule.xml 26](#_Toc212237682)

[Hình 35. Thêm quy tắc vào local rule.xml 26](#_Toc212237683)

[Hình 36. Tải eicar vào thư mục download 27](#_Toc212237684)

[Hình 37. File eicar đã bị xóa khỏi thư mục download 27](#_Toc212237685)

[Hình 38. Wazuh-manager đã hiện cảnh báo và phản ứng xóa file. 28](#_Toc212237686)

[Hình 39. Mô hình lab phát hiện tiến trình ẩn 29](#_Toc212237687)

[Hình 40. Chuyển vào chế độ root của agent 29](#_Toc212237688)

[Hình 41. Cấu hình quét root check mỗi 2 phút 30](#_Toc212237689)

[Hình 42. Tải module hạt nhân rookit 30](#_Toc212237690)

[Hình 43. Máy wazuh-manager đã nhận được cảnh báo rootcheck 31](#_Toc212237691)

# LỜI MỞ ĐẦU

Trong bối cảnh thế giới hiện nay, Internet đã trở thành nền tảng không thể thiếu trong mọi hoạt động của xã hội hiện đại, từ kinh tế, giáo dục đến quốc phòng và an ninh. Tuy nhiên, cùng với sự phát triển mạnh mẽ của công nghệ thông tin, các mối đe dọa về an toàn và bảo mật dữ liệu ngày càng gia tăng, với nhiều hình thức tấn công mạng tinh vi, khó phát hiện. Các giải pháp bảo vệ truyền thống như tường lửa hay phần mềm chống virus tuy cần thiết nhưng chưa đủ khả năng phát hiện sớm và ngăn chặn các hành vi xâm nhập bất thường. Do đó, việc xây dựng các hệ thống phát hiện xâm nhập (Intrusion Detection System – IDS), đặc biệt là hệ thống phát hiện xâm nhập dựa trên máy chủ (Host-based IDS – HIDS), đóng vai trò quan trọng trong công tác giám sát, cảnh báo và bảo vệ hệ thống trước các nguy cơ tấn công.

Xuất phát từ thực tế đó, nhóm chúng em lựa chọn đề tài “Xây dựng hệ thống HIDS phát hiện xâm nhập với Wazuh” với mong muốn tìm hiểu sâu hơn về cơ chế hoạt động, cách triển khai và đánh giá hiệu quả của một hệ thống phát hiện xâm nhập trong môi trường thực tế. Wazuh được chọn bởi đây là nền tảng mã nguồn mở mạnh mẽ, có khả năng giám sát toàn diện, dễ cài đặt, mở rộng linh hoạt và phù hợp cho cả mục đích học tập lẫn ứng dụng thực tế.

Đề tài tập trung vào việc tìm hiểu cơ sở lý thuyết về IDS và HIDS, nghiên cứu kiến trúc của Wazuh, xây dựng mô hình thử nghiệm giám sát – phát hiện xâm nhập trên môi trường giả lập, đồng thời mô phỏng một số tình huống tấn công để đánh giá khả năng phản ứng của hệ thống. Do giới hạn về thời gian và phạm vi nghiên cứu, đề tài chỉ triển khai ở quy mô nhỏ trong phạm vi mạng nội bộ và chưa kết hợp với các kỹ thuật phát hiện dựa trên học máy hay trí tuệ nhân tạo.

Với đề tài này, nhóm mong muốn góp phần củng cố kiến thức về an toàn mạng, nâng cao khả năng ứng dụng các công cụ mã nguồn mở vào thực tế, và hướng tới việc xây dựng các giải pháp phát hiện xâm nhập hiệu quả, góp phần đảm bảo an toàn thông tin trong kỷ nguyên số.

# Chương 1. Cơ sở lý thuyết

## 1.1. Tổng quan về xâm nhập và kỹ thuật phát hiện xâm nhập.

### 1.1.1 Xâm nhập

a, Khái niệm xâm nhập

Xâm nhập mạng là những hoạt động có chủ đích, lợi dụng các tổn thương của hệ thống thông tin nhằm phá vỡ tính sẵn sàng, tính toàn vẹn và tính bảo mật của hệ thống. Xâm nhập còn được hiểu là hành động trái phép vượt qua các cơ chế bảo mật của một hệ thống.

Có rất nhiều kiểu xâm nhập mạng khác nhau và thường được phân thành các loại chính: tấn công từ chối dịch vụ, kiểu thăm dò, tấn công chiếm quyền “root”, tấn công điều khiển từ xa.

Một trong những mối đe dọa chính đối với vấn đề an ninh là việc tin tặc (thường được gọi là hacker hoặc cracker) sử dụng một số hình thức xâm nhập. Có một số loại kẻ xâm nhập sau:

* Tội phạm mạng: Là các cá nhân hoặc tổ chức hoạt động vì mục đích tài chính. Họ thực hiện các hành vi như đánh cắp danh tính, chiếm đoạt thông tin tài chính, gián điệp doanh nghiệp hoặc tống tiền dữ liệu nhằm thu lợi bất chính.
* Kẻ hoạt động xã hội: Là những cá nhân hoặc nhóm bị thúc đẩy bởi lý do chính trị, xã hội hoặc ý thức hệ. Họ thường tiến hành các hành động như tấn công từ chối dịch vụ (DoS), thay đổi giao diện trang web (deface) hay công bố dữ liệu nhạy cảm nhằm gây chú ý và quảng bá thông điệp của mình.
* Các tổ chức do nhà nước bảo trợ: Là các nhóm tin tặc được các chính phủ bảo trợ để tiến hành các hoạt động gián điệp hoặc phá hoại.
* Các loại khác: Bao gồm những cá nhân có động cơ cá nhân như thử thách kỹ năng, tìm kiếm danh tiếng trong cộng đồng hoặc nghiên cứu kỹ thuật. Nhiều người trong số họ có thể là các hacker cổ điển, nhà nghiên cứu bảo mật hoặc người phát hiện lỗ hổng phần mềm mới.

b, Các dạng tấn công brute-force, port-scan, fim, mã độc

* Tấn công brute-force

Là kỹ thuật thử tất cả các khả năng của tên đăng nhập, mật khẩu hoặc khóa mã hóa cho đến khi tìm ra tổ hợp đúng.

Loại tấn công này thường được tự động hóa bằng các công cụ có khả năng thử hàng nghìn đến hàng triệu kết hợp mỗi giây. Mặc dù đơn giản, nhưng brute-force có thể thành công nếu hệ thống không giới hạn số lần đăng nhập hoặc sử dụng mật khẩu yếu.

* Tấn công port-scan

Là hành vi quét qua các cổng (port) trên máy chủ hoặc thiết bị mạng để xác định cổng nào đang mở và dịch vụ nào đang chạy.

Kẻ tấn công thường sử dụng công cụ như *Nmap* để thu thập thông tin cấu trúc mạng, qua đó tìm ra điểm yếu để khai thác.

* Tấn công fim

Kẻ tấn công thường khai thác lỗ hổng phần mềm, mật khẩu yếu hoặc quyền truy cập từ xa để đưa mã và thao tác trên hệ thống. Sau khi có quyền, họ sẽ chỉnh sửa tệp nhằm đạt được một trong các mục tiêu: ẩn mình (rootkit), khởi tạo kênh điều khiển (backdoor/webshell), hoặc làm phá hoại/tống tiền dữ liệu (ransomware – mã hóa file).

* Tấn công mã độc

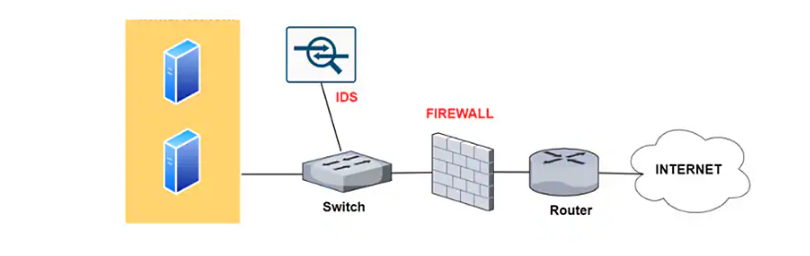
Là phần mềm được thiết kế nhằm xâm nhập, làm hỏng hoặc chiếm quyền điều khiển hệ thống. Có nhiều loại mã độc như: Virus, Worm (Sâu máy tính), Trojan, Rootkit, Botnet.

Mã độc là một trong những nguyên nhân chủ yếu gây xâm nhập hệ thống, làm rò rỉ dữ liệu và phá hoại tính toàn vẹn của thông tin.

### 1.1.2. Hệ thống phát hiện xâm nhập

a, Định nghĩa

Hệ thống phát hiện xâm nhập (IDS) là công nghệ bảo mật mạng ban đầu được xây dựng để phát hiện các lỗ hổng bảo mật nhằm vào ứng dụng hoặc máy tính mục tiêu. IDS cũng là một thiết bị chỉ nghe. IDS cũng là một thiết bị chỉ nghe. IDS giám sát lưu lượng và báo cáo kết quả cho quản trị viên. Nó không thể tự động thực hiện hành động để ngăn chặn việc khai thác được phát hiện chiếm quyền kiểm soát hệ thống. Kẻ tấn công có khả năng khai thác lỗ hổng nhanh chóng khi xâm nhập vào mạng. Do đó, IDS không đủ khả năng phòng ngừa. Hệ thống phát hiện xâm nhập và ngăn chặn xâm nhập đều thiết yếu đối với việc quản lý thông tin và sự kiện bảo mật



Hình 1. Vị trí của hệ thống phát hiện xâm nhập IDS

Hệ thống phát hiện xâm nhập (IDS) có nhiệm vụ chính là giám sát lưu lượng mạng hoặc các hành vi trên hệ thống nhằm nhận dạng các dấu hiệu của tấn công và xâm nhập. Khi phát hiện các hành vi đáng ngờ, IDS sẽ ghi lại log để phục vụ cho việc phân tích sau này, đồng thời gửi thông báo, cảnh báo cho người quản trị mạng. IDS chỉ tập trung phát hiện các mối đe dọa tiềm ẩn và thường được đặt ngoài băng tần của cơ sở hạ tầng mạng, không nằm trực tiếp trên đường truyền giao tiếp thời gian thực giữa người gửi và người nhận, nhờ đó không ảnh hưởng đến hiệu suất mạng nội tuyến. Các giải pháp IDS thường sử dụng cổng TAP hoặc SPAN để phân tích bản sao của luồng lưu lượng, đảm bảo quá trình giám sát hiệu quả mà không làm gián đoạn hoạt động mạng. Trước đây, khi IDS mới được phát triển, việc phân tích dữ liệu với độ sâu cần thiết để phát hiện xâm nhập còn chậm, chưa đáp ứng được tốc độ xử lý của các thành phần trong đường truyền mạng. Tuy nhiên, ngày nay, IDS được ứng dụng rộng rãi trong việc phát hiện các hoạt động bất thường để ngăn chặn tin tặc trước khi chúng gây hại cho hệ thống. IDS hoạt động bằng cách tìm kiếm các sai lệch so với hành vi bình thường hoặc đối chiếu với các mẫu tấn công đã biết, phân tích dữ liệu qua nhiều lớp giao thức và ứng dụng để phát hiện các sự kiện như đầu độc DNS, gói tin lỗi hay quét cổng. Ngoài ra, IDS có thể được triển khai dưới dạng thiết bị bảo mật vật lý, phần mềm hoặc trong môi trường đám mây nhằm bảo vệ dữ liệu và hệ thống một cách toàn diện.

b, Phân loại

Có hai loại IDS phổ biến là IDS dựa trên mạng (NIDS) — được cài đặt trực tiếp trong mạng, và IDS dựa trên máy chủ (HIDS) — được cài đặt trên từng máy khách.

* Hệ thống phát hiện xâm nhập HIDS

HIDS thêm một lớp phần mềm bảo mật chuyên biệt vào một hệ thống dễ bị tấn công hoặc các hệ thống nhạy cảm, chẳng hạn như máy chủ cơ sở dữ liệu và hệ thống quản trị.

HIDS giám sát hoạt động trên hệ thống theo nhiều cách khác nhau để phát hiện hành vi đáng ngờ. Lợi ích chính của HIDS là nó có thể phát hiện cả xâm nhập bên ngoài và bên trong, điều mà NIDS hoặc tường lửa không thể thực hiện được.

HIDS giám sát và ghi lại các sự kiện đáng ngờ, đồng thời gửi cảnh báo. Trong một số trường hợp, IDS có thể tạm dừng một cuộc tấn công trước khi bất kỳ thiệt hại nào được thực hiện, nhưng mục đích chính của nó là phát hiện.

HIDS có thể sử dụng các phương pháp tiếp cận bất thường hoặc các phương pháp tiếp cận dựa trên dấu hiệu xâm nhập/phỏng đoán để phát hiện hành vi trái phép trên thiết bị được giám sát.

HIDS thu thập dữ liệu từ các nguồn phổ biến sau: Dấu vết cuộc gọi hệ thống, Bản ghi tệp nhật ký (log files), Tổng kiểm tra tính toàn vẹn của tệp (File Integrity Checksums), Truy cập đăng ký (Registry Access).

* Hệ thống phát hiện xâm nhập NIDS

Định nghĩa và Mục đích: NIDS giám sát lưu lượng tại các điểm đã chọn trên mạng hoặc liên mạng để cố gắng phát hiện các mẫu xâm nhập.

NIDS kiểm tra gói lưu lượng theo gói trong thời gian thực (hoặc gần thời gian thực), phân tích các giao thức lớp mạng, lớp vận tải và/hoặc lớp ứng dụng để xác định hoạt động đáng ngờ. Không giống HIDS, NIDS kiểm tra lưu lượng gói hướng đến các hệ thống máy tính có khả năng bị tấn công trên mạng.

NIDS thường được bao gồm trong cơ sở hạ tầng bảo mật của một tổ chức, được kết hợp với hoặc liên kết với tường lửa. NIDS chủ yếu tập trung vào việc giám sát các nỗ lực xâm nhập từ bên ngoài bằng cách phân tích cả mẫu lưu lượng và nội dung lưu lượng.

Một hệ thống NIDS điển hình bao gồm một số cảm biến để giám sát lưu lượng gói, một hoặc nhiều máy chủ cho các chức năng quản lý NIDS và một hoặc nhiều cổng quản lý cho giao diện người dùng.

Việc xác định vị trí của các bộ cảm biến NIDS rất quan trọng. Các vị trí phổ biến bao gồm:

* Ngay bên trong tường lửa bên ngoài: Cho phép nhìn thấy các cuộc tấn công từ bên ngoài và làm nổi bật các vấn đề của tường lửa
* Giữa tường lửa bên ngoài và Internet (WAN): Giám sát tất cả lưu lượng mạng chưa được lọc, cung cấp dữ liệu về số lượng và kiểu tấn công.
* Trên các mạng đường trục chính hoặc mạng LAN quan trọng: Phát hiện hoạt động trái phép của người dùng được ủy quyền (tấn công bên trong và bên ngoài) và có thể được điều chỉnh theo các giao thức cụ thể.

### 1.1.3. Phương pháp phát hiện xâm nhập:

IDS thường sử dụng một trong các cách tiếp cận sau để phân tích dữ liệu cảm biến nhằm phát hiện các hành vi xâm nhập:

* Phát hiện bất thường: Liên quan đến việc thu thập dữ liệu liên quan đến hành vi của những người dùng hợp pháp trong một khoảng thời gian. Sau đó, hành vi quan sát hiện tại được phân tích để xác định với mức độ tin cậy cao liệu hành vi này có phải là dữ liệu của người dùng hợp pháp hay dữ liệu của kẻ xâm nhập.
* Phát hiện dựa trên dấu hiệu xâm nhập hoặc dựa trên phỏng đoán: Sử dụng một tập hợp các mẫu dữ liệu độc hại đã biết (dấu hiệu xâm nhập) hoặc các quy tắc tấn công (phỏng đoán) được so sánh với hành vi hiện tại để quyết định xem đó có phải là hành vi của kẻ xâm nhập hay không. Nó còn được gọi là phát hiện lạm dụng. Phương pháp tiếp cận này chỉ có thể xác định các cuộc tấn công đã biết dựa trên các mẫu hoặc quy tắc sẵn có.

# Chương 2. Thiết kế và Thực nghiệm

**2.1. Giới thiệu về  WAZUH**

**2.2.1. Giới thiệu về wazuh**

Wazuh là nền tảng an ninh mạng mã nguồn mở cung cấp năng lực SIEM/XDR: thu thập và phân tích log, phát hiện xâm nhập/malware, giám sát tính toàn vẹn tệp, đánh giá cấu hình và lỗ hổng, đáp ứng sự cố, và hỗ trợ tuân thủ. Kiến trúc gồm tác tử (agent) cài trên endpoint và các thành phần trung tâm để phân tích, lưu trữ, trực quan hóa dữ liệu.

Wazuh server (chứa Wazuh manager) chịu trách nhiệm phân tích và cảnh báo;

Wazuh indexer lưu trữ và lập chỉ mục dữ liệu;

Wazuh dashboard là giao diện web để tra cứu/giám sát.

**2.2.2. Thành phần**

A screenshot of a computer

AI-generated content may be incorrect.

Hình 2. Mô hình hoạt động của wazuh

Wazuh hoạt động dựa trên ba thành phần chính: Wazuh Agent, Wazuh Server (hoặc Wazuh Manager) và Wazuh Dashboard. Wazuh Agent được cài đặt trên các thiết bị cần giám sát như máy chủ, máy tính cá nhân hoặc thiết bị mạng. Agent có nhiệm vụ thu thập thông tin bảo mật từ hệ điều hành, tệp nhật ký và ứng dụng, đồng thời phát hiện các thay đổi cấu hình hoặc hoạt động bất thường. Dữ liệu này sau đó được gửi đến Wazuh Server để xử lý và phân tích.

Wazuh Server là thành phần trung tâm tiếp nhận và phân tích dữ liệu bảo mật từ các Agent. Dựa trên các quy tắc bảo mật được cấu hình sẵn, Server có thể phát hiện các sự kiện liên quan đến an ninh như xâm nhập, lỗ hổng bảo mật hoặc thay đổi không mong muốn trong cấu hình hệ thống. Ngoài ra, Wazuh Server có thể tích hợp với các công cụ bảo mật khác như VirusTotal, giúp nâng cao độ chính xác trong việc phát hiện mối đe dọa. Khi phát hiện sự kiện bảo mật, Server sẽ tạo cảnh báo và gửi đến Wazuh Dashboard.

Wazuh Dashboard là giao diện quản lý trên nền web, giúp người dùng giám sát và quản lý hệ thống bảo mật. Dashboard hiển thị báo cáo chi tiết, cảnh báo thời gian thực và biểu đồ trực quan, giúp quản trị viên theo dõi tình hình bảo mật dễ dàng. Ngoài ra, Dashboard còn hỗ trợ quản lý cấu hình cho cả Wazuh Agent và Server, giúp tối ưu hệ thống. Quy trình hoạt động của Wazuh bao gồm: Wazuh Agent thu thập dữ liệu → Wazuh Server phân tích và tạo cảnh báo → Wazuh Dashboard hiển thị thông tin, cung cấp giải pháp giám sát bảo mật hiệu quả và toàn diện.

## 2.3. Thực hiện

### 2.3.1. Phát hiện cuộc tấn công brute-force

* Môi trường thực hiện

- Chuẩn bị 2 máy Ubuntu 22.04 và Kali Linux trong cùng 1 mạng LAN.

* Ubuntu 22.04 dùng làm Wazuh Server
* Máy Ubuntu 22.04 thứ 2 là Wazuh Agent để thử nghiệm tấn công Brute force
* Máy Kali Linux để thực hiện tấn công Brute force

- Kịch bản: Sử dụng máy kali-linux thực hiện tấn công brute force vào máy

windows 7 có cài đặt wazuh agent. Sau đó tiến hành kiểm tra xem wazuh có

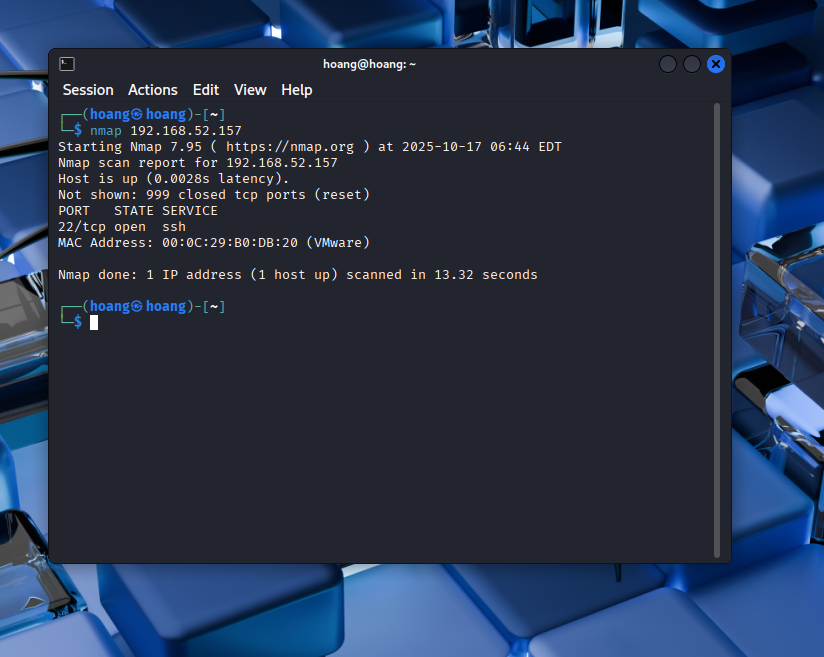
bắt được alert hay không.

A diagram of a computer network

AI-generated content may be incorrect.

Hình 3. Mô hinh lab tấn công brute-force

**Bước 1**: Trên kali-linux sử dụng công cụ nmap để tìm kiếm lỗ hổng trong máy ubuntu 22.04



Hình 4. Dùng Nmap tìm Port đang hoạt động

**Bước 2**: Phát hiện cổng 22 mở, thông qua cổng này, sử dụng công cụ hydra thực hiện tấn công brute force vào máy ubuntu 22.04 với file tài khoản, mật khẩu chuẩn bị trước.

A computer screen shot of a computer program

AI-generated content may be incorrect.

Hình 5. Sử dụng hydra tấn công agent

**Bước 3**: Mở wazuh trong events kiểm tra xem wazuh có bắt được alert không

A screenshot of a computer

AI-generated content may be incorrect.

Hình 6. Cảnh báo ở wazuh events

Ta thấy wazuh đã bắt được alert của một cuộc tấn công brute force. Ta thực

hiện xem nội dung cảnh báo.

A screenshot of a computer

AI-generated content may be incorrect.

Hình 7. Nội dung cảnh báo brute-force

Rules giúp ta bắt được alert của cuộc tấn công brute force này:

A close-up of a computer screen

AI-generated content may be incorrect.

Hình 8. Rules 5760 bắt cuộc tấn công

* Kết quả mong muốn

Phát hiện được cuộc tấn công Brute force và đưa ra được hướng xử lí ngăn chặn.

### 2.3.2. FIM

* Môi trường thực hiện

Chuẩn bị 1 máy Wazuh-Manager, 1 máy Windows (Wazuh Agent) trong cùng 1 mạng LAN .

* Máy Ubuntu 22.04 làm Wazuh-Manager.
* Máy Windows 10 dùng làm Wazuh Agent .
* Kịch bản

Kiểm tra chức năng Giám sát tính toàn vẹn tệp tin (FIM - Syscheck) của Wazuh. Bằng cách thêm và sửa file trong tệp mà mình cho FIM theo dõi, xem Wazuh có cảnh báo ko.

*A diagram of a computer system

AI-generated content may be incorrect.*

Hình 9. Mô hình lab FIM

**Bước 1**: Cấu hình file ossec.conf trên windows 10 agent, ở đây ta sẽ đặt thư mục cần theo dõi là C:\Administrator\TestFIM

A screenshot of a computer

AI-generated content may be incorrect.

Hình 10. Đặt thư mục theo dõi ở agent

**Bước 2**: Restart lại Wazuh-agent

A screenshot of a computer

AI-generated content may be incorrect.

Hình 11. Khởi động lại agent

A screenshot of a computer

AI-generated content may be incorrect.

Hình 12. Nội dung của file secret

A screenshot of a computer

AI-generated content may be incorrect.

Hình 13. Thay đổi nội dung của file secret

**Bước 4**: Thêm file: Test vào C:\Administrator\TestFIM

A computer screen with a white background

AI-generated content may be incorrect.

Hình 14. Thêm foder vào thư mục theo dõi

A screenshot of a computer

AI-generated content may be incorrect.

Hình 15. Wazuh manager bắt được sự kiện FIM theo dõi

Bên Security event bắt được sự kiện :

Oct 18, 2025 17:17:03.452 File added to the system

Oct 18, 2025 17:16:57.572 Integrity checksum changed.

🡺Wazuh-Server đã theo dõi được C:\Administrator\TestFIM

A screenshot of a computer

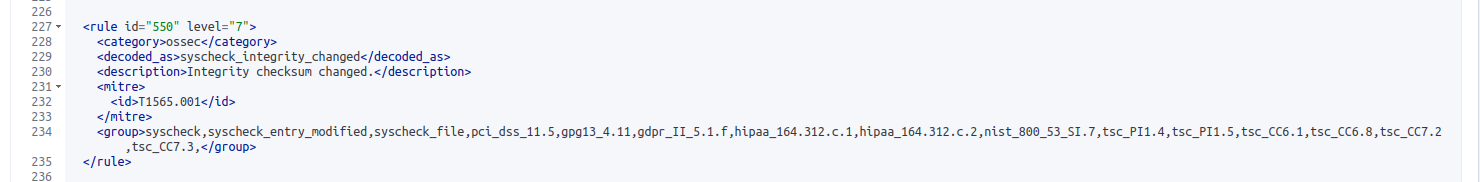
AI-generated content may be incorrect.

Hình 16. Chi tiết về log Oct 18, 2025 17:17:03.452 File added to the system

A screenshot of a computer

AI-generated content may be incorrect.

Hình 17. Chi tiết về Oct 18, 2025 17:16:57.572 Integrity checksum changed



Hình 18. Rule 550 : dùng để phát hiện thay đổi nội dung tệp tin



Hình 19. Rule 554 : dùng để phát hiện tệp tin mới được thêm vào hệ thống

### 2.3.3Ngăn chặn phần mềm độc hại với Wazuh

* Môi trường thực hiện

Chuẩn bị 1 máy Wazuh-Manager, 1 máy Windows (Wazuh Agent) trong cùng 1 mạng LAN .

* Máy Ubuntu 22.04 làm Wazuh-Manager.
* Máy Windows 10 dùng làm Wazuh Agent .
* Kịch bản:

Kịch bản này cấu hình FIM (Syscheck) của Wazuh để giám sát thư mục Downloads trên máy Agent. Khi một tệp thử nghiệm virus (EICAR) được tải về thư mục đó, Wazuh sẽ tự động gửi hash của tệp cho VirusTotal để quét. Ngay khi VirusTotal xác nhận tệp đó là độc hại, Wazuh sẽ kích hoạt cơ chế Active Response để tự động xóa tệp đó khỏi máy Agent. A computer virus and computer virus

AI-generated content may be incorrect.

Hình 20. Mô hình lab ngăn chặn phần mềm độc hại

**Bước 1**: Vào Wazuh-Manager để cài đặt theo dõi C:\User\toila\Downloads

A screenshot of a computer

AI-generated content may be incorrect.

Hình 21. Hình ảnh của wazuh group

A computer screen with a white box

AI-generated content may be incorrect.

Hình 22. Thêm thư mục cần theo dõi trên manager

**Bước 2**: Vào trang virustotal.com để lấy apikey.

A screenshot of a computer

AI-generated content may be incorrect.

Hình 23. Lấy apikey của virustotal

**Bước 4**: Thêm cấu hình sau vào /var/ossec/etc/ossec.conf tệp trên máy chủ Wazuh để kích hoạt tích hợp VirusTotal. Thao tác này cho phép kích hoạt truy vấn VirusTotal bất cứ khi nào bất kỳ quy tắc nào trong syschecknhóm FIM được kích hoạt.

A screenshot of a computer

AI-generated content may be incorrect.

Hình 24. Kích hoạt virustotal trên manager

**Bước 5**: Khởi động lại Wazuh-Manager.

A screenshot of a computer

AI-generated content may be incorrect.

Hình 25. Khởi động lại wazuh manager

**Bước 6**: Tải file mã độc EICAR về máy :

*Invoke-WebRequest -Uri "https://secure.eicar.com/eicar.com.txt" -OutFile "$env:USERPROFILE\Downloads\eicar.com"*

A computer screen shot of a blue screen

AI-generated content may be incorrect.

Hình 26. Lệnh tải eicar về agent

A screenshot of a computer

AI-generated content may be incorrect.

Hình 27. File Eicar đã được tải vào : C:\User\toila\Downloads

A screenshot of a computer

AI-generated content may be incorrect.

Hình 28. Cảnh báo về file mã độc đã được gửi về manager

A screenshot of a computer

AI-generated content may be incorrect.

Hình 29. Ảnh check được file mã độc eicar trên Virustotal.com

**Bước 7** : Tạo /var/ossec/active-response/bin/remove-threat.sh tập lệnh phản hồi chủ động để xóa các tệp độc hại khỏi máy agent.

A screenshot of a computer

AI-generated content may be incorrect.

Hình 30. Tạo file python đặt tập lệnh chủ động phản hồi

**Bước 8**: Chuyển đổi tập lệnh Python phản hồi đang hoạt động remove-threat.py thành ứng dụng thực thi Windows. Chạy lệnh PowerShell sau với tư cách quản trị viên để tạo tệp thực thi:

A screenshot of a computer program

AI-generated content may be incorrect.

Hình 31. Chuyển đổi file python thành ứng dụng thực thi

A screenshot of a computer

AI-generated content may be incorrect.

Hình 32. File remove-threat.exe đã được tạo.

**Bước 9**: Thêm các khối sau vào /var/ossec/etc/ossec.conf tệp máy chủ Wazuh. Thao tác này cho phép phản hồi chủ động và kích hoạt tệp remove-threat.exe thực thi khi truy vấn VirusTotal trả về kết quả trùng khớp với các mối đe dọa.

A screenshot of a computer

AI-generated content may be incorrect.

Hình 33. Thêm phản hồi chủ động vào manager

**Bước 10**: Thêm các quy tắc sau vào /var/ossec/etc/rules/local\_rules.xml tệp máy chủ Wazuh để cảnh báo về kết quả phản hồi đang hoạt động.

A screenshot of a computer

AI-generated content may be incorrect.

Hình 34. Lệnh vào local rule.xml

A screenshot of a computer

AI-generated content may be incorrect.

Hình 35. Thêm quy tắc vào local rule.xml

**Bước 11**: Tải file mã độc EICAR về .

A screenshot of a computer

AI-generated content may be incorrect.

Hình 36. Tải eicar vào thư mục download

Kết quả: File đã bị xóa

A screenshot of a computer

AI-generated content may be incorrect.

Hình 37. File eicar đã bị xóa khỏi thư mục download

A screenshot of a computer

AI-generated content may be incorrect.

Hình 38. Wazuh-manager đã hiện cảnh báo và phản ứng xóa file.

* **Kết quả và Phân tích kết quả:**

Kết quả thành công, xác nhận rằng cả Wazuh (trong việc giám sát tệp) và phần mềm diệt virus (trong việc bảo vệ) đều đang hoạt động như mong đợi.

### 2.3.4. Phát hiện các tiến trình ẩn

* Môi trường thực hiện

Chuẩn bị 1 máy Wazuh-Manager, 1 máy Windows (Wazuh Agent) trong cùng 1 mạng LAN .

* Máy Ubuntu 22.04 làm Wazuh-Manager.
* Máy Windows 10 dùng làm Wazuh Agent .
* Kịch bản

Sử dụng tính năng Rootcheck của Wazuh để phát hiện rootkit. Bạn sẽ cài một rootkit để che giấu một tiến trình; Rootcheck sẽ tự động quét, phát hiện ra sự bất thường này và gửi cảnh báo về máy chủ.

A computer and a computer switch

AI-generated content may be incorrect.

Hình 39. Mô hình lab phát hiện tiến trình ẩn

**Bước 1**: Chuyển sang người dùng root và cập nhật kernel của điểm cuối này

A screenshot of a computer

AI-generated content may be incorrect.

Hình 40. Chuyển vào chế độ root của agent

**Bước 2**: Cấu hình tác nhân Wazuh để chạy quét rootcheck mỗi 2 phút. Trong /var/ossec/etc/ossec.conftệp. Đặt frequency tùy chọn trong <rootcheck>phần thành 120:

A screenshot of a computer

AI-generated content may be incorrect.

Hình 41. Cấu hình quét root check mỗi 2 phút

**Bước 3**: Tải mô-đun hạt nhân rootkit

A computer screen shot of a code

AI-generated content may be incorrect.

Hình 42. Tải module hạt nhân rookit

**Bước 4**: Máy wazuh-manager đã nhận được cảnh báo rootcheck

A screenshot of a computer

AI-generated content may be incorrect.

Hình 43. Máy wazuh-manager đã nhận được cảnh báo rootcheck

* Kết quả và Phân tích kết quả:

Wazuh đã hoạt động chính xác—nó đã quét hệ thống và *phát hiện* ra một dấu hiệu bất thường về tiến trình chạy ẩn trong máy

# KẾT LUẬN

Wazuh là một nền tảng mã nguồn mở được phát triển dựa trên OSSEC HIDS, đồng thời tích hợp thêm Elastic Stack và OpenSCAP, giúp nâng cao khả năng phát hiện, giám sát và bảo vệ hệ thống trước sự gia tăng của các cuộc tấn công mạng hiện nay. Việc triển khai Wazuh thông qua Docker container tương đối thuận tiện, giúp việc cài đặt và quản lý trở nên nhanh chóng hơn. Giao diện Kibana tích hợp cùng Wazuh plugin thân thiện, dễ sử dụng và hỗ trợ người quản trị theo dõi hệ thống một cách trực quan.

Dữ liệu log từ các agent được cập nhật liên tục, thể hiện chi tiết từng sự kiện và cấp độ cảnh báo, giúp người quản trị dễ dàng đánh giá nguy cơ bị xâm nhập. Bộ quy tắc (rule set) mặc định của Wazuh được xây dựng khá toàn diện, có khả năng nhận diện nhiều hình thức tấn công phổ biến, qua đó giúp tăng cường khả năng phòng thủ của hệ thống.

* Ưu điểm
* Là dự án mã nguồn mở có cộng đồng người dùng và nhà phát triển rộng, thường xuyên cập nhật và cải tiến.
* Thích hợp triển khai cho mô hình nhỏ hoặc trung bình, dễ quản lý.
* Giao diện Kibana plugin cho phép cấu hình và giám sát các agent, cũng như theo dõi cảnh báo bảo mật một cách trực quan và hiệu quả.
* Cung cấp khả năng giám sát (monitoring) đáp ứng tốt các yêu cầu cơ bản, hỗ trợ đảm bảo an toàn cho hệ thống và các container.
* Hỗ trợ cài đặt nhanh với bản OVA có sẵn, giúp người dùng dễ dàng trải nghiệm hệ thống.
* Bộ rule mặc định bao phủ nhiều tình huống tấn công thông thường, cho phép phát hiện sớm các mối đe dọa.
* Nhược điểm
* Quá trình cài đặt phức tạp khi triển khai trong hệ thống quy mô lớn.
* Khi áp dụng mô hình phân tán (Distributed Deployment), khả năng mở rộng cao nhưng dễ gặp lỗi tương thích phiên bản giữa các thành phần, đặc biệt là Wazuh server.
* Triển khai bằng Ansible có thể phát sinh lỗi kết nối tới các máy chủ từ xa (remote host).
* Nếu cấu hình rule không chính xác, hệ thống có thể gửi nhiều cảnh báo sai hoặc không cần thiết.
* Hiện chưa hỗ trợ biểu đồ tương quan tài nguyên cho các container.
* Thời gian khởi động giao diện Wazuh và Kibana còn chậm, ảnh hưởng nhẹ đến trải nghiệm người dùng.

# Tài liệu tham khảo

[1] Nguyễn Chiến Trinh, Nguyễn Tiến Ban, Hoàng Trọng Minh, Nguyễn Thanh Trà, và Phạm Anh Thư, *Bài giảng An ninh mạng thông tin*. [Học viện công nghệ bưu chính viễn thông], [2021].

[2] Wazuh, "Wazuh Documentation". Có sẵn: <https://documentation.wazuh.com/>.