

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC NGOẠI NGỮ – TIN HỌC TP.HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN



Chuyên ngành: An ninh mạng
MÔN HỌC : Bảo Mật Người Dùng Cuối
Đề Tài: Bảo Mật Người Dùng Cuối

GIÁO VIÊN HƯỚNG DẪN: Đỗ Phi Hưng

THÀNH VIÊN NHÓM: Nhóm 1

Vũ Bình An – 22DH110065

Phạm Đức Vĩ – 22DH114289

Bùi Phạm Anh Tuấn – 22DH114799

TP.HỒ CHÍ MINH, THÁNG 07 NĂM 2025

 Điểm phần trình bày – Điểm hệ 10

	CBCT1	CBCT2
Họ tên CBCT Chữ ký: Chữ ký:
Điểm Băng chẽ: Băng chẽ:
Nhận xét Báo cáo: 2đ	Quyết báo cáo: (...) điểm..... Vân đáp: (...) điểm.....	Quyết báo cáo: (...) điểm..... Vân đáp: (...) điểm.....
Ván đáp: 2đ	Chức năng: (...) điểm.....	Chức năng: (...) điểm.....
Chức năng và demo: 5đ	Mở rộng: (...) điểm.....	Mở rộng: (...) điểm.....
Mở rộng và ứng dụng thực tiễn: 1đ

 Điểm quá trình – Điểm hệ 10

Họ tên CBCT:

 Điểm tổng kết:(Băng chẽ:.....)

LỜI NÓI ĐẦU

Trong bối cảnh chuyển đổi số đang diễn ra mạnh mẽ, bảo mật thông tin cá nhân và dữ liệu người dùng trở thành một trong những yếu tố then chốt để đảm bảo sự an toàn và tin cậy trong các hệ thống công nghệ thông tin. Các vụ tấn công mạng, rò rỉ dữ liệu và hành vi xâm phạm quyền riêng tư ngày càng diễn ra phổ biến, đòi hỏi mỗi cá nhân và tổ chức cần nâng cao nhận thức cũng như năng lực bảo vệ người dùng trước các mối đe dọa ngày càng tinh vi.

Môn học **Bảo mật người dùng** nhằm trang bị cho sinh viên kiến thức nền tảng về các rủi ro bảo mật thường gặp, kỹ thuật tấn công nhắm vào người dùng, cùng các biện pháp phòng chống hiệu quả. Thông qua các nội dung lý thuyết kết hợp với bài thực hành, sinh viên sẽ được tiếp cận các công cụ, phương pháp giám sát và tăng cường bảo vệ người dùng khỏi các nguy cơ đánh cắp thông tin, giả mạo danh tính và lừa đảo trực tuyến.

Môn học được giảng dạy bởi **Thầy Đỗ Phi Hưng**, người có nhiều năm kinh nghiệm trong lĩnh vực an toàn thông tin, sẽ giúp sinh viên có cái nhìn thực tế và ứng dụng được kiến thức vào bảo vệ người dùng trong môi trường số hiện nay.

Hy vọng rằng với tinh thần học tập nghiêm túc, chủ động tìm tòi và thực hành, các bạn sinh viên sẽ tiếp thu hiệu quả và vận dụng tốt kiến thức đã học vào thực tiễn.

LỜI CẢM ƠN

Nhóm 1 xin gửi lời cảm ơn chân thành đến Thầy Đỗ Phi Hưng – giảng viên phụ trách môn học Bảo mật người dùng đã tận tình giảng dạy, hướng dẫn và truyền đạt những kiến thức quý báu, giúp nhóm em hiểu rõ hơn về tầm quan trọng của bảo mật thông tin trong môi trường công nghệ hiện đại.

Đặc biệt, chúng em trân trọng sự kiên nhẫn, nhiệt huyết và phản hồi mang tính xây dựng từ thầy trong suốt quá trình làm báo cáo. Những nhận xét và góp ý của thầy đã giúp chúng em hoàn thiện nội dung một cách rõ ràng, khoa học và có chiều sâu hơn.

Cuối cùng, em xin chân thành cảm ơn các bạn học cùng lớp đã hỗ trợ, chia sẻ tài liệu và cùng nhau trao đổi trong suốt quá trình thực hiện môn học.

KẾ HOẠCH - PHÂN CÔNG NHÓM

Họ tên	Công việc	Mức độ hoàn thành
Phạm Đức Vĩ	Nghiên cứu lý thuyết nền tảng về bảo mật người dùng cuối, phân tích các mối đe dọa và xây dựng kịch bản tấn công mô phỏng.	100%
Vũ Bình An	Cài đặt, cấu hình hệ thống Wazuh và Suricata; thực hiện mô phỏng các cuộc tấn công thực tế.	100%
Bùi Phạm Anh Tuấn	Cài đặt, cấu hình hệ thống Wazuh và Suricata; thực hiện mô phỏng các cuộc tấn công thực tế.	100%

NHẬN XÉT CỦA GIẢNG VIÊN

MỤC LỤC

LỜI NÓI ĐẦU	3
LỜI CẢM ƠN	4
KẾ HOẠCH - PHÂN CÔNG NHÓM.....	5
NHẬN XÉT CỦA GIẢNG VIÊN	6
MỤC LỤC	7
MỤC LỤC HÌNH ẢNH.....	10
CHƯƠNG I. GIỚI THIỆU ĐỀ TÀI.....	13
CHƯƠNG II. TỔNG QUAN LÝ THUYẾT.....	14
 1. BẢO MẬT CƠ BẢN.....	14
 1.1. CIA (Confidentiality, Integrity, and Availability).....	14
 1.2. Non-repudiation.....	15
 1.3. AAA (Authentication, Authorization, and Accounting)	15
 1.4. Gap Analysis	15
 1.5. Zero Trust	17
 1.6. Physical Security (Bảo mật vật lý)	17
 1.7. Deception and Disruption Technology (Công nghệ lừa đảo và phá hoại)	18
 2. CÁC QUY TRÌNH CHANGE MANAGEMENT VÀ TÁC ĐỘNG ĐẾN BẢO MẬT.....	19
 2.1. Business Processes Impacting Security Operation (Quy trình kinh doanh ảnh hưởng đến hoạt động bảo mật)	19
 2.2. Technical Implications (Hệ quả kỹ thuật)	20
 3. SỬ DỤNG CÁC GIẢI PHÁP CRYPTOGRAPHIC SOLUTIONS PHÙ HỢP	22
 3.1. Public Key Infrastructure (PKI) (Cơ sở hạ tầng khóa công khai).....	22

3.2. Encryption (Mã hóa)	23
3.3. Tools (Công cụ)	24
3.4. Obfuscation (Che giấu)	25
3.5. Hashing.....	26
3.6. Salting.....	26
3.7. Digital Signatures	27
3.8. Key Stretching	27
3.9. Blockchain	28
3.10. Open Public Ledger.....	29
4. Các Tác Nhân Đe Dọa Phổ Biến và Động Cơ	29
 4.2. Thuộc Tính của Tác Nhân (Attributes of Actors).....	31
 4.3. Động Cơ (Motivations).....	31
5. CÁC TÁC NHÂN ĐE DỌA PHỔ BIẾN VÀ ĐỘNG CƠ.....	33
 5.1. Các Tác Nhân Đe Dọa (Threat Actors).....	33
 5.2. Thuộc Tính của Tác Nhân (Attributes of Actors).....	34
 5.3. Động Cơ (Motivations).....	35
 5.4. So Sánh và Phân Biệt	37
6. CÁC VECTOR ĐE DỌA VÀ BỀ MẶT TẤN CÔNG PHỔ BIẾN	38
7. CÁC LOẠI LỖ HỒNG BẢO MẬT	42
8. DỰA TRÊN KỊCH BẢN, PHÂN TÍCH CÁC CHỈ BÁO HOẠT ĐỘNG ĐỘC HẠI.....	45
CHƯƠNG III. SẢN PHẨM THỰC NGHIỆM	48
 1. Cài đặt Wazuh.....	48
a. Cài đặt Wazuh Server.....	48
b. Cài đặt Wazuh Agent	51
 2. Cấu hình và triển khai.....	56
2.1 . Tích hợp Suricata IDS phát hiện xâm nhập mạng.....	56

2.2. Phát hiện và loại bỏ phần mềm độc hại bằng cách tích hợp VirusTotal	
65	
KẾT LUẬN	77
TÀI LIỆU THAM KHẢO.....	78

MỤC LỤC HÌNH ẢNH

Hình 1. Tam giác bảo mật CIA.....	14
Hình 2. AAA	15
Hình 3. Gap Analysis	16
Hình 4. Zero Trust.....	17
Hình 5. Deception and Disruption Technology.....	18
Hình 6. Business Processes Impacting Security Operation	19
Hình 7. Technical Implications	20
Hình 8. PKI	22
Hình 9. Encryption	23
Hình 10. Obfuscation.....	25
Hình 11. Hashing	26
Hình 12. Salting	26
Hình 13. Digital Signatures.....	27
Hình 14. Key Stretching.....	27
Hình 15. Blockchain	28
Hình 16. Open Public Ledger.....	29
Hình 17. Threat Actors.....	30
Hình 18. Attributes of Actors.....	31
Hình 19. Motivation.....	31
Hình 20. Threat Actors.....	33
Hình 21. Attributes of Actors.....	34
Hình 22. Motivations	35
Hình 23. So sánh và phân biệt	37
Hình 24. Các Vector và bề mặt tấn công phổ biến.....	38
Hình 25. Các loại lỗ hổng bảo mật	42
Hình 26. Sơ đồ thiết kế hệ thống mạng lan	47
Hình 27. Cài đặt Wazuh.....	48
Hình 28. Cài đặt hoàn thành	49
Hình 29. IP máy Wazuh Server	49
Hình 30. Wazuh Dashboard.....	50
Hình 31. Danh sách password	51

Hình 32. Thêm khóa GPG	52
Hình 33. Thêm repository	53
Hình 34. Deloy Wazuh Agent.....	54
Hình 35. Khởi động lại các dịch vụ	55
Hình 36. IP máy Agent	55
Hình 37. Agent hiện bên Dashboard	56
Hình 38. Suricata setup	57
Hình 39. suricata setup.....	57
Hình 40. Tạo rule cảnh báo ICMP	58
Hình 41. rule cảnh báo policy.....	58
Hình 42. rule cảnh báo scan.....	58
Hình 43. Sửa đổi cài đặt Suricata trong tệp	59
Hình 44. Sửa đổi cài đặt Suricata trong tệp	60
Hình 45. Sửa đổi cài đặt Suricata trong tệp	60
Hình 46. Sửa đổi cài đặt Suricata trong tệp	61
Hình 47. Mô phỏng tấn công	62
Hình 48. Check log trên wazuh	63
Hình 49. Nmap	63
Hình 50. Check log trên Wazuh	64
Hình 51. cấu hình thư mục được giám sát	65
Hình 52. Cài đặt jq	66
Hình 53. để xóa các tệp độc hại khỏi endpoint	66
Hình 54. Thay đổi quyền sở hữu và quyền hạn của tệp	67
Hình 55. Thay đổi quyền sở hữu và quyền hạn của tệp	67
Hình 56. Khởi động lại Wazuh-agent để áp dụng các thay đổi	67
Hình 57. Thêm các quy tắc	68
Hình 58. Đăng nhập VirusTotal lấy API KEY	68
Hình 59. Kích hoạt Phản hồi Chủ động và kích hoạt tập lệnh remove-threat.sh	69
Hình 60. Khởi động lại Wazuh-manager.....	69
Hình 61. Mô phỏng tấn công	70
Hình 62. Check log trên Wazuh	70
Hình 63. Cập nhật các gói cục bộ và cài đặt máy chủ web Apache	71
Hình 64. Kiểm tra trạng thái của dịch vụ Apache.....	71
Hình 65. Check trang đích Apache và xác minh cài đặt	72
Hình 66. Wazuh agent theo dõi nhật ký truy cập của máy chủ Apache.....	72

Hình 67. Khởi động lại Wazuh-agent để áp dụng các thay đổi cấu hình	73
Hình 68. Mô phỏng tấn công	73
Hình 69. Mô phỏng tấn công	74
Hình 70. Phát hiện tấn công ShellShock.....	74
Hình 71. Mô phỏng tấn công	75
Hình 72. Mô phỏng tấn công	75
Hình 73. Mô phỏng tấn công	76

CHƯƠNG I. GIỚI THIỆU ĐỀ TÀI

A. Lý do chọn đề tài

Trong thời đại công nghệ số bùng nổ, con người ngày càng phụ thuộc nhiều hơn vào các thiết bị công nghệ và mạng Internet để phục vụ nhu cầu học tập, làm việc và giải trí. Tuy nhiên, cùng với sự phát triển đó là sự gia tăng của các mối đe dọa về an toàn thông tin, đặc biệt là đối với người dùng cuối – những cá nhân trực tiếp tương tác với hệ thống thông tin, nhưng lại thường thiếu kiến thức hoặc kỹ năng để tự bảo vệ bản thân khỏi các nguy cơ mạng.

Người dùng cuối chính là mắt xích yếu nhất trong chuỗi bảo mật. Dù các hệ thống có được trang bị các công nghệ bảo mật tiên tiến như firewall, antivirus, mã hóa hay xác thực đa yếu tố, nhưng chỉ một hành vi bất cẩn như click vào liên kết độc hại, sử dụng mật khẩu yếu hoặc chia sẻ thông tin nhạy cảm cũng có thể khiến toàn bộ hệ thống bị xâm phạm. Thực tế đã chứng minh rằng phần lớn các cuộc tấn công mạng thành công là do lỗi từ phía người dùng cuối.

Chính vì vậy, việc nghiên cứu và nâng cao nhận thức, kỹ năng bảo mật cho người dùng cuối là hết sức cấp thiết. Đây không chỉ là trách nhiệm của các chuyên gia bảo mật mà còn là nhiệm vụ chung của toàn bộ cộng đồng sử dụng công nghệ thông tin.

B. Mục tiêu nghiên cứu

- Làm rõ vai trò và tầm quan trọng của bảo mật người dùng cuối trong hệ thống thông tin.
- Phân tích các mối đe dọa thường gặp đối với người dùng cuối như phishing, malware, social engineering,...
- Đề xuất các giải pháp và biện pháp nâng cao nhận thức, kỹ năng phòng tránh rủi ro cho người dùng cuối.

C. Đối tượng và phạm vi nghiên cứu

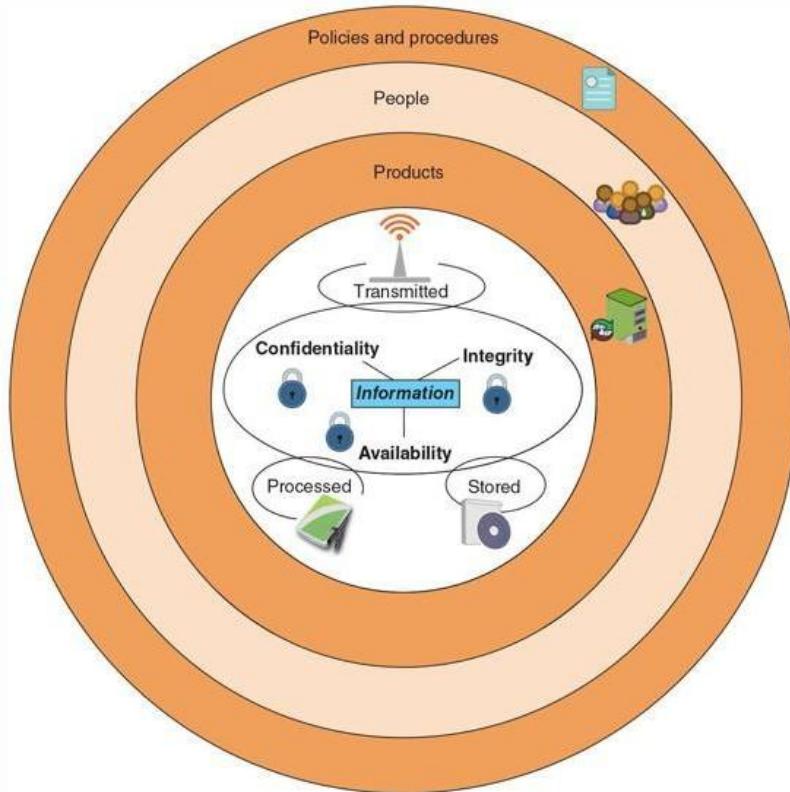
- Đối tượng nghiên cứu: Người dùng cuối sử dụng thiết bị công nghệ và Internet trong môi trường cá nhân hoặc tổ chức.
- Phạm vi nghiên cứu: Tập trung vào các rủi ro bảo mật từ phía người dùng cuối, bao gồm hành vi sử dụng, nhận thức về an toàn thông tin, và các biện pháp phòng tránh đơn giản – không đi sâu vào các kỹ thuật bảo mật nâng cao hoặc hệ thống mạng phức tạp.

CHƯƠNG II. TỔNG QUAN LÝ THUYẾT

1. BẢO MẬT CƠ BẢN

1.1. CIA (Confidentiality, Integrity, and Availability)

- Confidentiality (Tính bảo mật): Đảm bảo rằng dữ liệu chỉ được truy cập bởi những người được ủy quyền.
- Integrity (Tính toàn vẹn): Đảm bảo dữ liệu chính xác và không bị sửa đổi bởi các thực thể không được phép.
- Availability (Tính sẵn sàng): Đảm bảo dữ liệu và hệ thống có thể truy cập khi cần thiết.



Hình 1. Tam giác bảo mật CIA

1.2. Non-repudiation

Đảm bảo người gửi thông tin không thể từ chối đã gửi thông tin và người nhận không thể từ chối đã nhận thông tin.

1.3. AAA (Authentication, Authorization, and Accounting)



Hình 2. AAA

Authentication (Xác thực): Xác minh danh tính người dùng, hệ thống hoặc thực thể.

Authenticating People: Sử dụng mật khẩu, sinh trắc học hoặc token.

Authenticating Systems: Sử dụng chứng chỉ hoặc khóa.

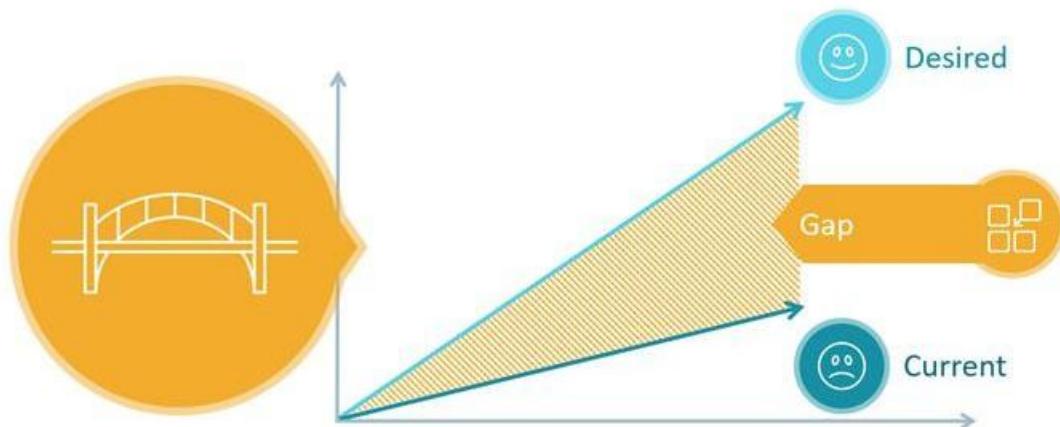
Authorization (Phân quyền): Xác định quyền truy cập, xác định người dùng hoặc hệ thống được xác thực có thể làm gì.

Authorization Models: Ví dụ bao gồm Role-Based Access Control (RBAC - Kiểm soát truy cập theo vai trò) và Mandatory Access Control (MAC - Kiểm soát truy cập bắt buộc).

Accounting (Kiểm toán): Theo dõi hoạt động của người dùng để đảm bảo họ đang hoạt động trong phạm vi quyền hạn cho phép.

1.4. Gap Analysis

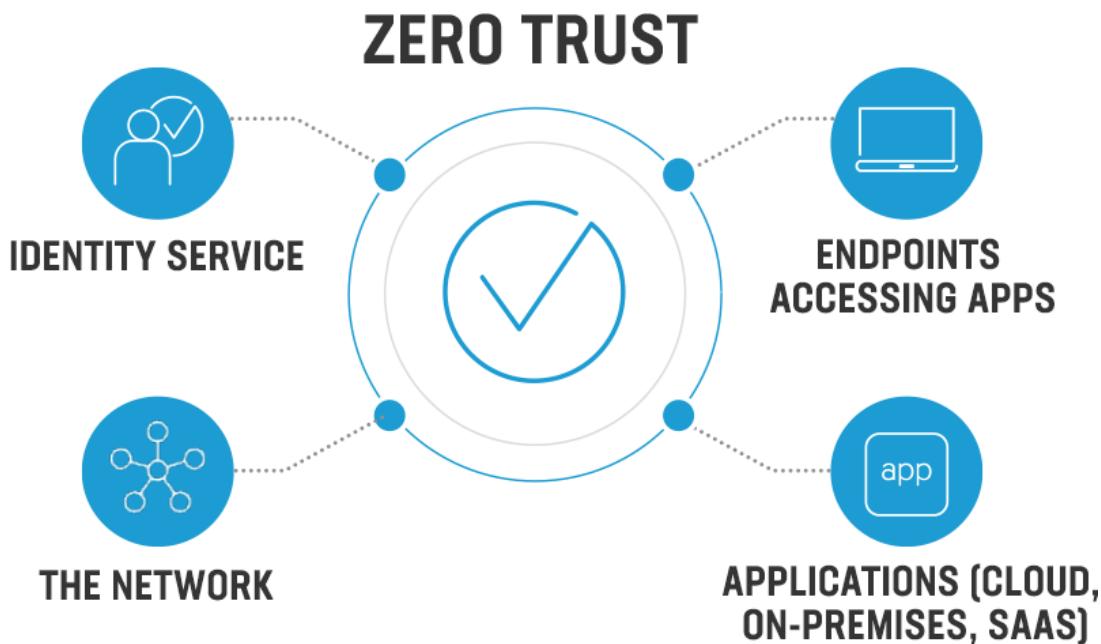
Gap Analysis Types and Tools



Hình 3. Gap Analysis

Quá trình xác định sự khác biệt giữa các thực tiễn bảo mật hiện tại và kết quả hoặc tiêu chuẩn mong muốn.

1.5. Zero Trust



Hình 4. Zero Trust

- Control Plane (Mặt kiểm soát):
 - Adaptive Identity: Xác minh danh tính người dùng/hệ thống một cách linh hoạt theo ngữ cảnh.
 - Threat Scope Reduction: Giảm thiểu bề mặt tấn công.
 - Policy-driven Access Control: Truy cập dựa trên chính sách thay vì quyền tĩnh.
 - Policy Administrator: Quản lý và cập nhật chính sách truy cập.
 - Policy Engine: Xử lý và đánh giá các yêu cầu truy cập theo chính sách.
 - Data Plane (Mặt dữ liệu):
 - Implicit Trust Zones: Khu vực mặc định được tin tưởng.
 - Subject/System: Các thực thể hoặc hệ thống được cấp quyền truy cập.
- Policy Enforcement Point:** Điểm thực thi chính sách, nơi các quyết định truy cập được thực hiện dựa trên các chính sách.

1.6. Physical Security (Bảo mật vật lý)

Access Control Vestibule: Không gian vào được bảo mật, thường có hai bộ cửa để kiểm soát truy cập.

Fencing: Rào cản để ngăn chặn các lối vào không được phép.

Video Surveillance: Máy quay giám sát và ghi lại các hoạt động.

Security Guard: Nhân viên bảo vệ giám sát cơ sở.

Access Badge: Thẻ ID cấp quyền truy cập vào các tòa nhà hoặc khu vực.

Lighting: Đảm bảo khả năng quan sát, thường ngăn chặn các hoạt động không được phép.

Infrared: Phát hiện phát xạ nhiệt, thường từ con người.

Pressure: Phát hiện trọng lượng hoặc thay đổi áp suất, chẳng hạn như bước chân.

Microwave: Sử dụng tín hiệu vi sóng để phát hiện chuyển động.

Ultrasonic: Sử dụng sóng âm để phát hiện sự hiện diện hoặc chuyển động.

1.7. Deception and Disruption Technology (Công nghệ lừa đảo và phá hoại)

EVOLUTION OF DECEPTION TECHNOLOGY



Hình 5. Deception and Disruption Technology

Honeypot: Hệ thống hoặc bộ dữ liệu mồi để thu hút kẻ tấn công.

Honeynet: Mạng lưới các honeypot.

Honeyfile: Tệp mồi được đặt để phát hiện truy cập không được phép.

Honeytoken: Một mẫu dữ liệu được sử dụng để cảnh báo khi bị truy cập, nó không có giá trị thực tế ngoài việc là bẫy.

2. CÁC QUY TRÌNH CHANGE MANAGEMENT VÀ TÁC ĐỘNG ĐẾN BẢO MẬT

2.1. Business Processes Impacting Security Operation (Quy trình kinh doanh ảnh hưởng đến hoạt động bảo mật)



Hình 6. Business Processes Impacting Security Operation

- **Approval Process:** Đảm bảo chỉ những thay đổi đã được kiểm tra và cần thiết mới được triển khai, giảm thiểu rủi ro giới thiệu lỗ hổng.
- **Ownership:** Xác định rõ chủ sở hữu và trách nhiệm, đảm bảo tính trách nhiệm và an toàn trong việc thực hiện thay đổi.
- **Stakeholders:** Đảm bảo các bên liên quan được thông báo về thay đổi và có thể cung cấp phản hồi có giá trị, giảm thiểu các khoảng trống bảo mật tiềm ẩn.

- **Impact Analysis:** Đánh giá hậu quả tiềm tàng của một thay đổi có thể tiết lộ các rủi ro bảo mật và khu vực dễ bị tổn thương.
- **Test Results:** Kiểm tra thay đổi trước khi triển khai có thể phát hiện và xác nhận các lỗi bảo mật hoặc vấn đề tương thích.
- **Backout Plan:** Nếu một thay đổi gây ra lỗ hổng không lường trước, có kế hoạch khôi phục thay đổi là điều cần thiết để duy trì bảo mật.
- **Maintenance Window:** Xác định thời gian cụ thể cho các thay đổi giúp giảm thiểu gián đoạn và đảm bảo tài nguyên sẵn có khi có sự cố xảy ra.
- **Standard Operating Procedure:** Tuân thủ các quy trình đã thiết lập đảm bảo tính nhất quán, khả năng dự đoán và bảo mật trong quá trình thay đổi.

2.2. Technical Implications (Hệ quả kỹ thuật)



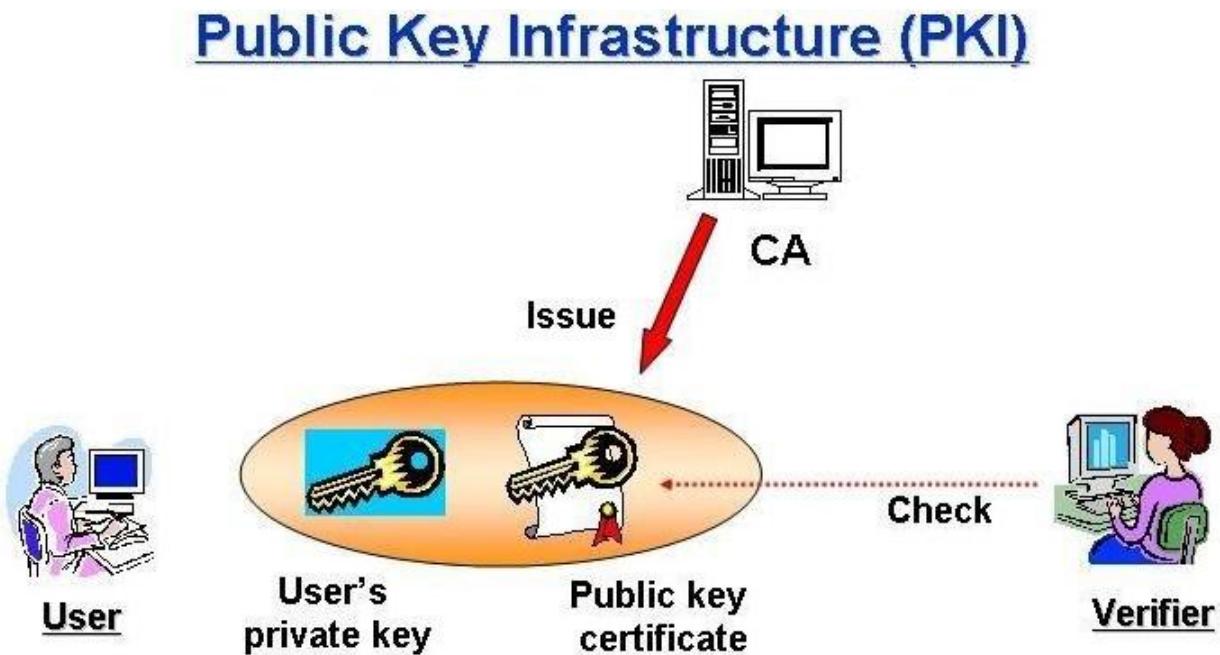
Hình 7. Technical Implications

- **Allow lists/Deny lists:** Các thay đổi có thể yêu cầu cập nhật danh sách cho phép hoặc cấm, xác định rõ các hoạt động hoặc thực thể được phép hoặc bị cấm, ảnh hưởng trực tiếp đến tư thế bảo mật.

- **Restricted Activities:** Một số thay đổi có thể giới hạn các hoạt động kinh doanh hoặc giám sát bảo mật.
- **Downtime:** Thời gian ngừng hoạt động không được lên kế hoạch hoặc kéo dài có thể khiến doanh nghiệp đối mặt với rủi ro, đặc biệt nếu các biện pháp bảo mật bị gián đoạn.
- **Service Restart:** Khởi động lại dịch vụ có thể giới thiệu lỗ hổng nếu không được thực hiện an toàn.
- **Application Restart:** Tương tự như khởi động lại dịch vụ, việc khởi động lại ứng dụng cần được thực hiện an toàn để tránh các rủi ro tiềm ẩn.
- **Legacy Applications:** Phần mềm cũ có thể không tương thích với các thay đổi mới và có thể chứa các lỗ hổng chưa được giải quyết.

3. SỬ DỤNG CÁC GIẢI PHÁP CRYPTOGRAPHIC SOLUTIONS PHÙ HỢP

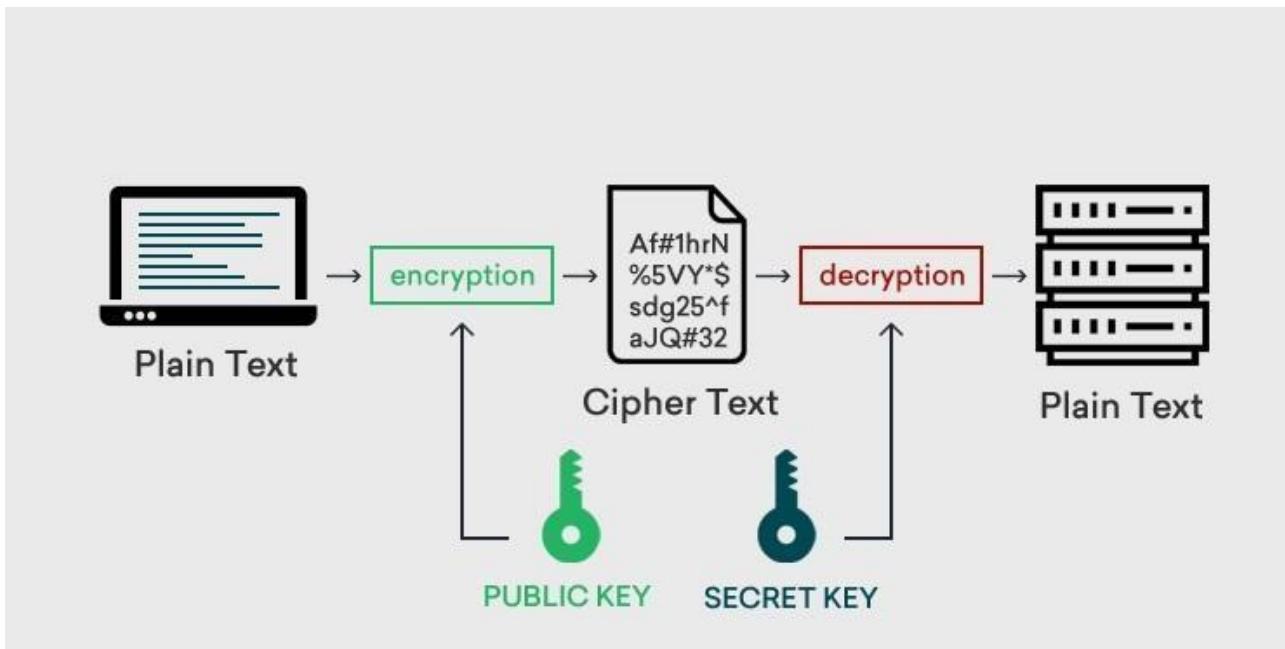
3.1. Public Key Infrastructure (PKI) (Cơ sở hạ tầng khóa công khai)



Hình 8. PKI

- **Public/Private Key:** Đảm bảo giao tiếp bảo mật, nơi chỉ người giữ khóa riêng có thể giải mã thông điệp.
- **Key Escrow:** Lưu trữ khóa của bên thứ ba đáng tin cậy để hỗ trợ **cryptographic keys**, đảm bảo chúng sẵn sàng nếu người sở hữu mất quyền truy cập hoặc trong các tình huống pháp lý.

3.2. Encryption (Mã hóa)



Hình 9. Encryption

- **Level:**
 - **Full-disk:** Mã hóa toàn bộ thiết bị lưu trữ, bảo vệ dữ liệu nếu thiết bị bị mất hoặc bị đánh cắp.
 - **Partition, Volume:** Mã hóa các phân cụ thể của thiết bị lưu trữ.
 - **File, Database, Record:** Mã hóa các tệp tin riêng lẻ, cơ sở dữ liệu hoặc bản ghi trong đó.
- **Transport/Communication:** Bảo vệ dữ liệu khi truyền qua mạng, ví dụ như với HTTPS.
- **Asymmetric/Symmetric:** Sử dụng các phương pháp mã hóa bất đối xứng và đối xứng, trong đó cả hai phương pháp sử dụng cùng một khóa cho mã hóa và giải mã.
- **Key Exchange:** Quá trình bảo mật để trao đổi khóa **cryptographic**.

- **Algorithms:** Các quy trình bảo mật cho mã hóa và giải mã dữ liệu (ví dụ: AES, RSA).
- **Key Length:** Độ dài khóa càng lớn, việc bẻ khóa càng khó, nhưng cũng có thể làm chậm hoạt động.

3.3. Tools (Công cụ)

- **TPM:** Một bộ điều khiển vi mô chuyên dụng lưu trữ khóa, mật khẩu và chứng chỉ số một cách an toàn.
- **HSM:** Thiết bị phần cứng bảo mật quản lý khóa số và cung cấp cấp độ bảo mật phần cứng.
- **Key Management System:** Hệ thống được thiết kế để quản lý khóa cryptographic xuyên suốt vòng đời của chúng.
- **Secure Enclave:** Một khu vực lưu trữ bảo mật dựa trên phần cứng trong bộ xử lý, cô lập nó khỏi bộ xử lý chính để bảo vệ dữ liệu nhạy cảm.

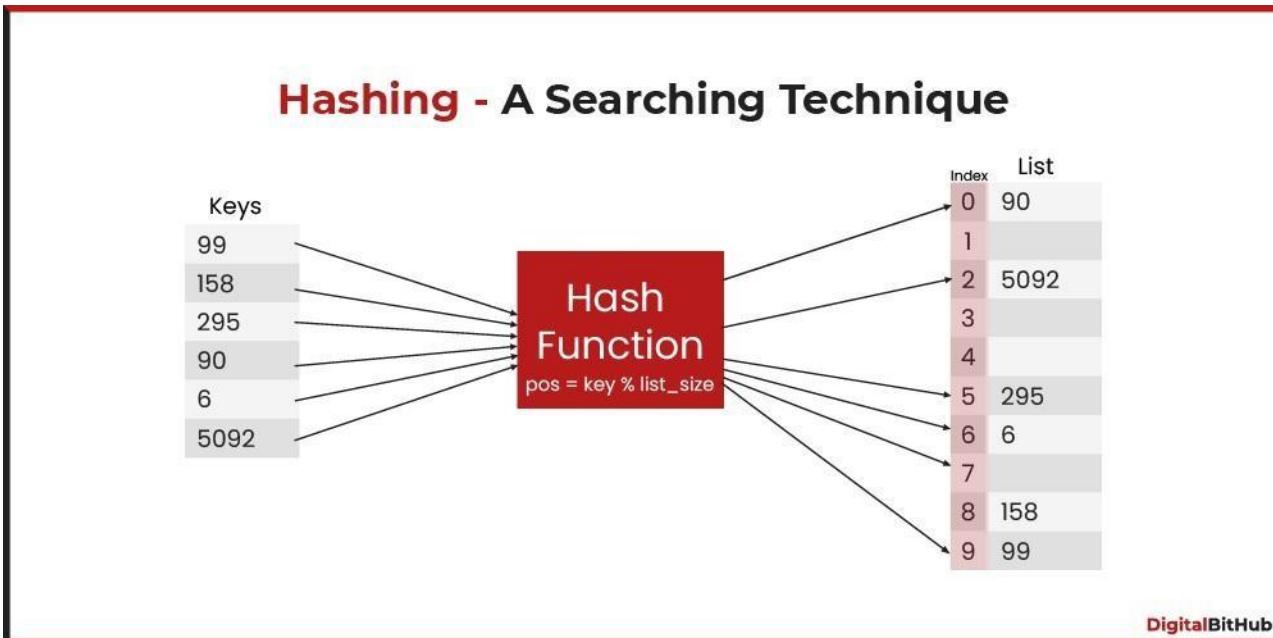
3.4. Obfuscation (Che giấu)



Hình 10. Obfuscation

- **Steganography**: Ấn dấu liệu trong dữ liệu khác (ví dụ: nhúng thông điệp bí mật vào hình ảnh).
- **Tokenization**: Thay thế dữ liệu nhạy cảm bằng các giá trị không nhạy cảm.
- **Data Masking**: Che giấu dữ liệu cụ thể trong cơ sở dữ liệu, làm cho dữ liệu không thể truy cập được đối với người dùng không được phép.

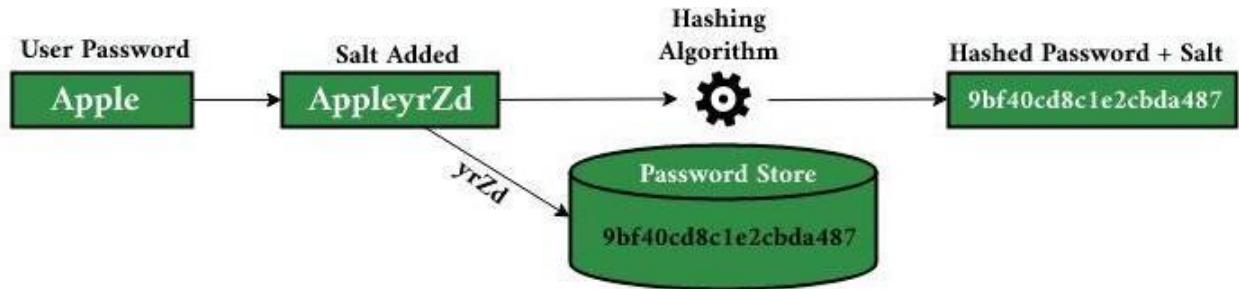
3.5. Hashing



Hình 11. Hashing

Chuyển đổi dữ liệu thành chuỗi có độ dài cố định, đảm bảo tính toàn vẹn dữ liệu.

3.6. Salting

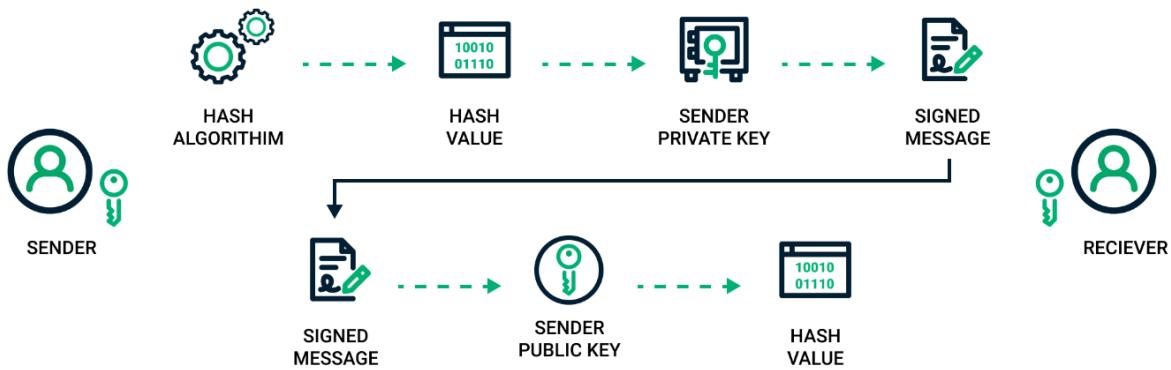


Hình 12. Salting

Dữ liệu ngẫu nhiên được thêm vào trước khi hash để đảm bảo cùng một đầu vào tạo ra các đầu ra khác nhau.

3.7. Digital Signatures

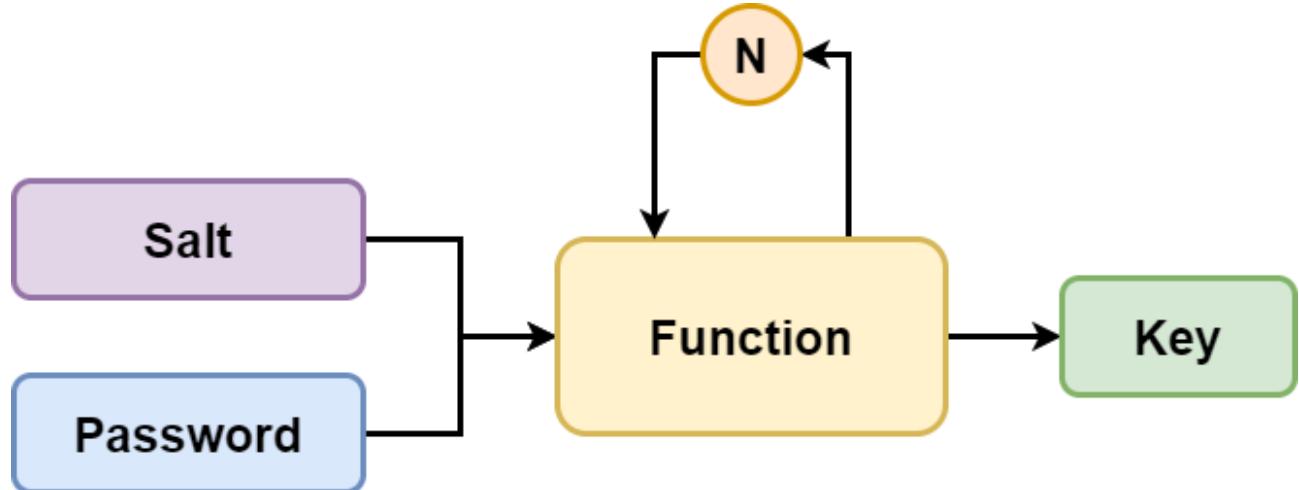
How Does a Digital Signature Work?



Hình 13. Digital Signatures

Xác nhận tính xác thực của tài liệu hoặc tin nhắn kỹ thuật số.

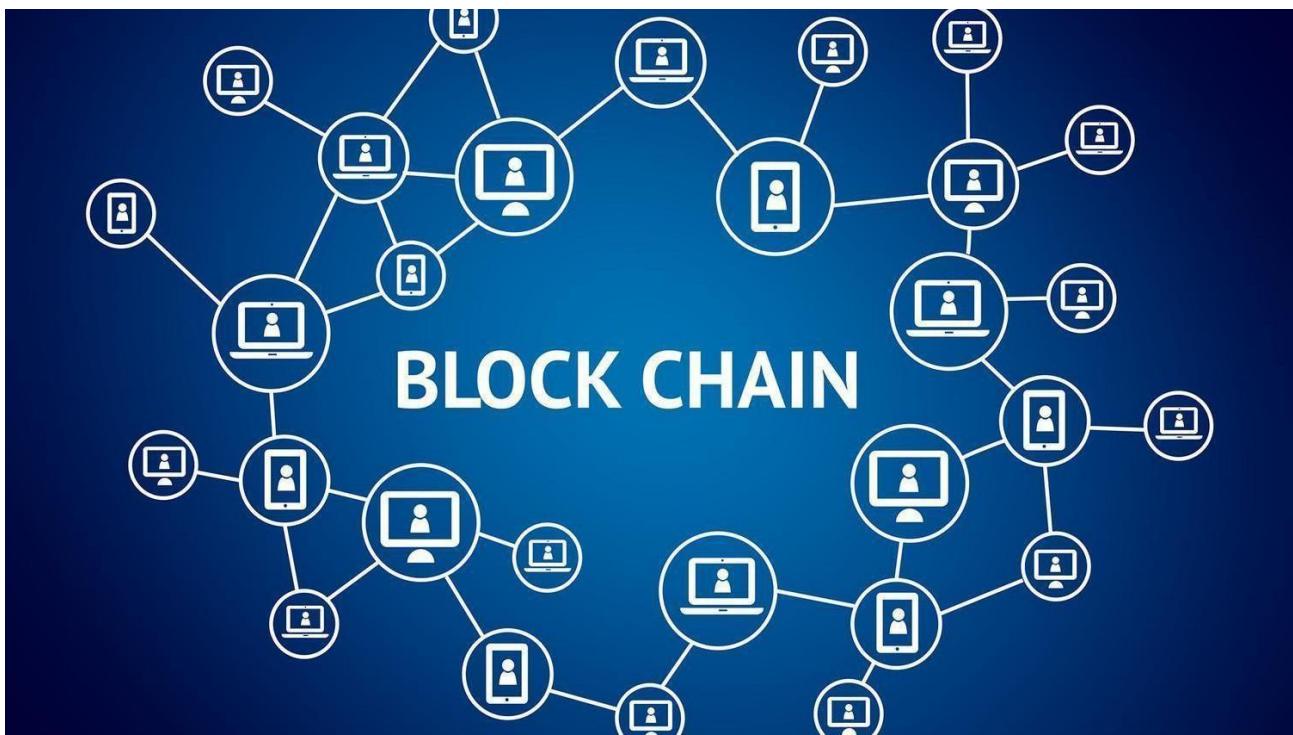
3.8. Key Stretching



Hình 14. Key Stretching

Làm cho khóa có khả năng chống lại các cuộc tấn công brute force bằng cách làm cho quá trình tạo khóa tốn nhiều tính toán hơn.

3.9. Blockchain

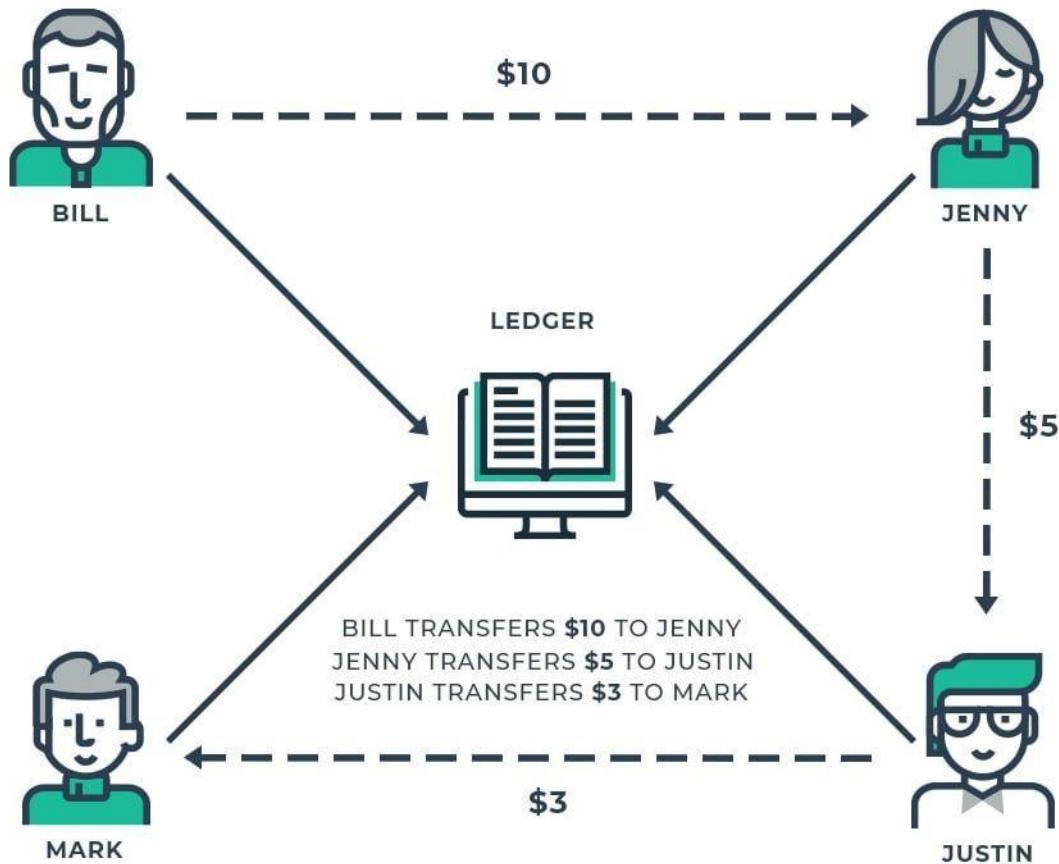


Hình 15. Blockchain

Số cái phân tán, phi tập trung sử dụng các giải pháp mật mã để đảm bảo tính toàn vẹn dữ liệu.

3.10. Open Public Ledger

OPEN “CENTRALIZED” LEDGER



Hình 16. Open Public Ledger

Sổ cái minh bạch, có thể truy cập công khai nơi tất cả các giao dịch đều có thể nhìn thấy.

4. Các Tác Nhân Đe Dọa Phổ Biến và Động Cơ

4.1. Các Tác Nhân Đe Dọa (Threat Actors)

4.1 CÁC TÁC NHÂN ĐE DOẠ (THREAT ACTORS)



Hình 17. Threat Actors

- a. **Nation-State**: Các chính phủ hoặc tổ chức được chính phủ hậu thuẫn tham gia vào các hoạt động mạng, thường nhằm mục đích gián điệp, phá hoại hoặc chiến tranh.
- b. **Unskilled Attacker**: Cá nhân có kỹ năng kỹ thuật hạn chế, thường sử dụng các công cụ hoặc script có sẵn để phát động tấn công. Đôi khi được gọi là "script kiddies."
- c. **Hacktivist**: Hacker được thúc đẩy bởi các nguyên nhân chính trị hoặc xã hội, nhằm mục đích thúc đẩy thông điệp hoặc phản đối các thực thể cụ thể.
- d. **Insider Threat**: Các cá nhân trong tổ chức, chẳng hạn như nhân viên hoặc nhà thầu, có thể lạm dụng quyền truy cập của họ để làm hại tổ chức.
- e. **Organized Crime**: Các nhóm tham gia vào tội phạm mạng vì lợi ích tài chính.
- f. **Shadow IT**: Các ứng dụng, công cụ hoặc hệ thống không được phép sử dụng trong tổ chức, không được phòng IT chính thức phê duyệt.

4.2. Thuộc Tính của Tác Nhân (Attributes of Actors)



Hình 18. Attributes of Actors

- Internal/External:** Tác nhân đe dọa có xuất phát từ bên trong (ví dụ: Insider Threat) hay bên ngoài (ví dụ: Nation-State) tổ chức.
- Resources/Funding:** Số tiền và nguồn lực có sẵn cho tác nhân đe dọa. Ví dụ, Nation-States thường có nguồn lực đáng kể, trong khi Unskilled Attackers ở mức thấp hơn.
- Level of Sophistication/Capability:** Mức độ kỹ năng kỹ thuật của tác nhân đe dọa. Nation-States và Organized Crime groups thường có mức độ tinh vi cao, trong khi Unskilled Attackers ở mức thấp hơn.

4.3. Động Cơ (Motivations)



Hình 19. Motivation

- Data Exfiltration:** Đánh cắp dữ liệu từ mục tiêu, thường để bán hoặc tận dụng.

- b. Espionage:** Gián điệp các thực thể để thu thập thông tin nhạy cảm, phô biến với Nation-States.
- c. Service Disruption:** Vô hiệu hóa hoặc làm gián đoạn dịch vụ, thường thấy với hacktivist phản đối các dịch vụ hoặc công ty cụ thể.
- d. Blackmail:** Đe dọa tiết lộ dữ liệu nhạy cảm trừ khi có yêu cầu (thường là tiền) được đáp ứng.
- e. Financial Gain:** Đánh cắp dữ liệu hoặc trực tiếp lấy cắp tiền, động cơ phô biến cho organized crime.
- f. Philosophical/Political Beliefs:** Hành động dựa trên niềm tin cá nhân hoặc nhóm, thường thấy với hacktivist.
- g. Ethical:** Hành động theo nghĩa vụ đạo đức được cảm nhận, đôi khi thấy với whistleblower hoặc "white hat" hackers xác định các lỗ hổng.

5. CÁC TÁC NHÂN ĐE DỌA PHỔ BIẾN VÀ ĐỘNG CƠ

5.1. Các Tác Nhân Đe Dọa (Threat Actors)



Hình 20. Threat Actors

- a. **Nation-State**: Các chính phủ hoặc tổ chức được chính phủ hậu thuẫn tham gia vào các hoạt động mạng, thường nhằm mục đích gián điệp, phá hoại hoặc chiến tranh.
- b. **Unskilled Attacker**: Cá nhân có kỹ năng kỹ thuật hạn chế, thường sử dụng các công cụ hoặc script có sẵn để phát động tấn công. Đôi khi được gọi là "script kiddies."
- c. **Hacktivist**: Hacker được thúc đẩy bởi các nguyên nhân chính trị hoặc xã hội, nhằm mục đích thúc đẩy thông điệp hoặc phản đối các thực thể cụ thể.

- d. **Insider Threat:** Các cá nhân trong tổ chức, chẳng hạn như nhân viên hoặc nhà thầu, có thể lạm dụng quyền truy cập của họ để làm hại tổ chức.
- e. **Organized Crime:** Các nhóm tham gia vào tội phạm mạng vì lợi ích tài chính.
- f. **Shadow IT:** Các ứng dụng, công cụ hoặc hệ thống không được phép sử dụng trong tổ chức, không được phòng IT chính thức phê duyệt.

5.2. Thuộc Tính của Tác Nhân (Attributes of Actors)



Hình 21. Attributes of Actors

- a. **Internal/External:** Tác nhân đe dọa có xuất phát từ bên trong (ví dụ: Insider Threat) hay bên ngoài (ví dụ: Nation-State) tổ chức.
- b. **Resources/Funding:** Số tiền và nguồn lực có sẵn cho tác nhân đe dọa. Ví dụ, Nation-States thường có nguồn lực đáng kể, trong khi Unskilled Attackers ở mức thấp hơn.

c. **Level of Sophistication/Capability:** Mức độ kỹ năng kỹ thuật của tác nhân đe dọa. Nation-States và Organized Crime groups thường có mức độ tinh vi cao, trong khi Unskilled Attackers ở mức thấp hơn.

5.3. Động Cơ (Motivations)

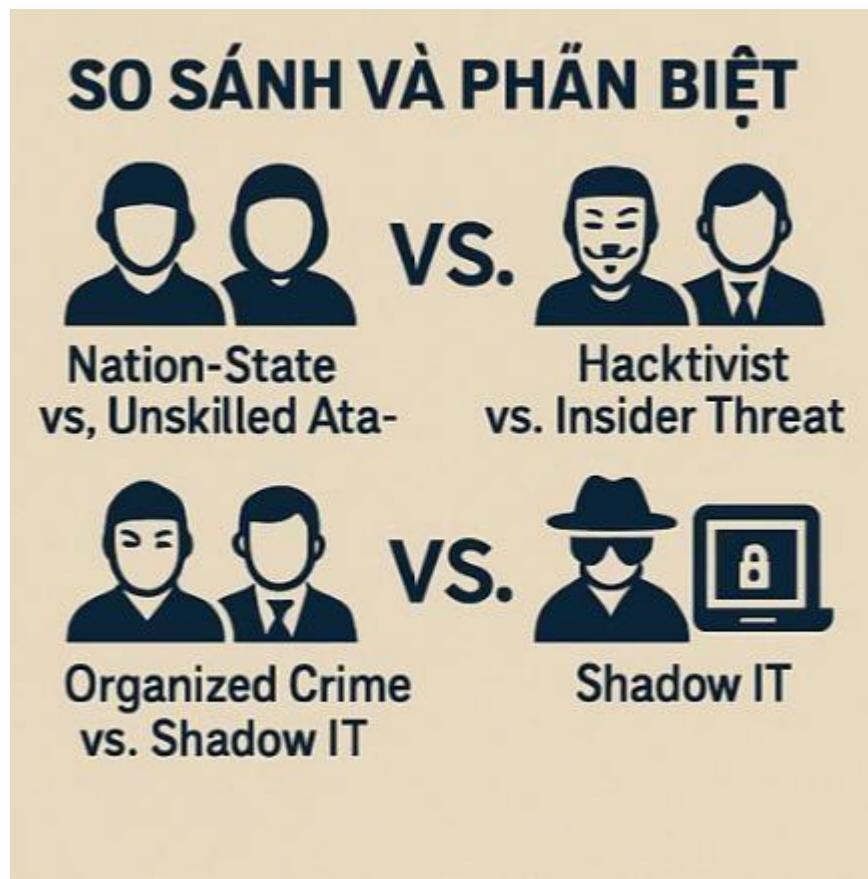


Hình 22. Motivations

- a. **Data Exfiltration:** Đánh cắp dữ liệu từ mục tiêu, thường để bán hoặc tận dụng.
- b. **Espionage:** Gián điệp các thực thể để thu thập thông tin nhạy cảm, phổ biến với Nation-States.
- c. **Service Disruption:** Vô hiệu hóa hoặc làm gián đoạn dịch vụ, thường thấy với hacktivist phản đối các dịch vụ hoặc công ty cụ thể.
- d. **Blackmail:** Đe dọa tiết lộ dữ liệu nhạy cảm trừ khi có yêu cầu (thường là tiền) được đáp ứng.

- e. **Financial Gain:** Đánh cắp dữ liệu hoặc trực tiếp lấy cắp tiền, động cơ phổ biến cho organized crime.
- f. **Philosophical/Political Beliefs:** Hành động dựa trên niềm tin cá nhân hoặc nhóm, thường thấy với hacktivist.
- g. **Ethical:** Hành động theo nghĩa vụ đạo đức được cảm nhận, đôi khi thấy với whistleblower hoặc "white hat" hackers xác định các lỗ hổng.
- h. **Revenge:** Nhắm mục tiêu một thực thể để trả thù cho một sự sai trái được cảm nhận.
- i. **Disruption/Chaos:** Được thúc đẩy hoàn toàn bởi mong muốn tạo ra sự hỗn loạn, đôi khi không có mục tiêu chính trị hoặc lợi nhuận cụ thể.
- j. **War:** Các hoạt động mang là một thành phần của chiến tranh lớn hơn, thường được thúc đẩy bởi Nation-States.

5.4. So Sánh và Phân Biệt



Hình 23. So sánh và phân biệt

- **Nation-State vs. Unskilled Attacker:** Trong khi nation-states có nguồn lực cao và khả năng tinh vi, thường có động cơ chính trị, unskilled attackers ít tinh vi hơn, thường được thúc đẩy bởi sự hỗn loạn, trả thù, hoặc đơn giản là cảm giác hồi hộp của việc hacking.
- **Hacktivist vs. Insider Threat:** Trong khi cả hai đều có thể được thúc đẩy bởi niềm tin triết học hoặc chính trị, nhằm mục đích gửi thông điệp. Ngược lại, insider threats có thể có các lý do khác nhau, bao gồm sự bất mãn cá nhân hoặc lợi ích tài chính.
- **Organized Crime vs. Shadow IT:** Organized crime groups là bên ngoài, có nguồn lực tốt và tinh vi, thường được thúc đẩy bởi lợi ích tài chính. Shadow IT, tuy nhiên, đại

diện cho mối đe dọa nội bộ "vô tình" từ nhân viên cố gắng cải thiện năng suất nhưng vô tình tạo ra rủi ro bảo mật.

6. CÁC VECTOR ĐE DỌA VÀ BỀ MẶT TẤN CÔNG PHỐ BIẾN

CÁC VECTOR DE DOA VÀ BỀ MẶT TẤN CÔNG PHỐ BIẾN



Message-based

Email-Phương diện poba ién
for dnithűic hrinhu co linc



Image-based

Harmoful payloads coube



Voice Call

Vôce-based phishing



Voitee Call



Removable Device

- Client-based
- Agentless



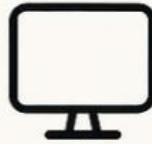
Vulnerable Software

Outdated software may pose a significant risk



Insecure Networks

- Wireless
- Wired
- Bluetooth



Insecure Networks

Hình 24. Các Vector và bề mặt tấn công phổ biến

Threat Vectors và **Attack Surfaces** đề cập đến các phương pháp và con đường khác nhau mà thông qua đó những kẻ tấn công mạng có thể nhắm mục tiêu vào cá nhân và

tổ chức. Bằng cách hiểu rõ những điều này, các tổ chức có thể chuẩn bị, bảo vệ và giảm thiểu các rủi ro tiềm ẩn.

a. Message-based

- **Email:** Phương tiện phổ biến để phân phối nội dung độc hại hoặc liên kết. Các nỗ lực phishing, malware, ransomware và social engineering thường sử dụng phương pháp này.
- **SMS:** Tin nhắn văn bản di động có thể chứa các liên kết phishing (Smishing) hoặc nội dung độc hại nhắm mục tiêu vào smartphone.
- **Instant Messaging (IM):** Các dịch vụ nhắn tin thời gian thực có thể được khai thác để phân phối malware hoặc nội dung phishing.

b. Image-based

Các payload độc hại có thể được nhúng trong hình ảnh, khi được xem có thể khai thác các lỗ hổng.

c. File-based

Phần mềm độc hại có thể được nhúng trong các tệp tin, khi mở hoặc thực thi có thể làm tổn hại hệ thống.

d. Voice Call

Vishing (voice-based phishing) liên quan đến tội phạm sử dụng cuộc gọi điện thoại để lừa nạn nhân tiết lộ thông tin cá nhân hoặc tuân theo các hướng dẫn độc hại.

e. Removable Device

Các thiết bị như USB có thể được sử dụng để đưa malware vào hoặc khai thác các lỗ hổng phần mềm khi kết nối với hệ thống.

f. Vulnerable Software

- **Client-based:** Phần mềm yêu cầu cài đặt trên hệ thống của người dùng có thể được nhắm mục tiêu cho các lỗ hổng.

- **Agentless:** Phần mềm chạy mà không cần cài đặt hoặc agent, khiến chúng khó giám sát và có thể dễ bị tấn công.

g. Unsupported Systems and Applications

Phần mềm lỗi thời không còn nhận được cập nhật bảo mật có thể là rủi ro đáng kể.

h. Insecure Networks

- **Wireless:** Các mạng Wi-Fi không bảo mật có thể bị chặn hoặc khai thác.
- **Wired:** Truy cập vật lý vào mạng có dây có thể dẫn đến xâm nhập.
- **Bluetooth:** Các lỗ hổng trong Bluetooth có thể được khai thác để theo dõi hoặc kiểm soát thiết bị.

i. Open Service Ports

Các cổng mở không được bảo mật có thể cho phép truy cập trái phép hoặc tấn công vào các dịch vụ đang chạy trên những cổng đó.

j. Default Credentials

Các thiết bị hoặc hệ thống có mật khẩu mặc định không thay đổi có thể dễ dàng được kẻ tấn công truy cập.

k. Supply Chain

- **Managed Service Providers (MSPs):** Nếu bị tổn hại, có thể cung cấp quyền truy cập vào cơ sở hạ tầng của khách hàng.
- **Vendors:** Các hệ thống của họ, nếu bị vi phạm, có thể hoạt động như một cửa ngõ vào cơ sở hạ tầng của tổ chức.
- **Suppliers:** Sự tổn hại trong bảo mật của nhà cung cấp có thể có tác động lan rộng đến khách hàng của họ.

l. Human Vectors/Social Engineering

- **Phishing:** Email lừa đảo nhằm đánh cắp thông tin nhạy cảm.

- **Vishing:** Cuộc gọi thoại cố gắng lừa đảo nạn nhân.
- **Smishing:** Các nỗ lực phishing dựa trên SMS.
- **Misinformation/Disinformation:** Truyền bá thông tin sai lệch để lừa đảo hoặc thao túng.
- **Impersonation:** Giả mạo là người khác để lừa đảo nạn nhân.
- **Business Email Compromise:** Các chiến thuật lừa đảo để thao túng nhân viên chuyên tiền hoặc tiết lộ dữ liệu nhạy cảm.
- **Pretexting:** Sử dụng các kịch bản bịa đặt để có được thông tin cá nhân.
- **Watering Hole:** Tốn hại một website thường được sử dụng để nhắm mục tiêu vào khách truy cập của nó.
- **Brand Impersonation:** Bắt chước các thương hiệu nổi tiếng để lừa đảo nạn nhân.
- **Typosquatting:** Đăng ký các domain tương tự như những domain phổ biến để lừa đảo người dùng.

7. CÁC LOẠI LỖ HỒNG BẢO MẬT



Hình 25. Các loại lỗ hổng bảo mật

Vulnerabilities đề cập đến các điểm yếu trong hệ thống hoặc quy trình có thể được các tác nhân đe dọa khai thác để có được quyền truy cập trái phép hoặc thực hiện các hành động trái phép. Dưới đây là phân tích các loại lỗ hổng khác nhau:

a. Application Vulnerabilities

- **Memory Injection:** Việc đưa mã độc hại vào bộ nhớ của mục tiêu.
- **Buffer Overflow:** Xảy ra khi dữ liệu vượt quá khả năng của buffer, dẫn đến ghi đè lên các vị trí bộ nhớ liền kề.
- **Race Conditions:** Các tình huống mà hành vi của hệ thống phụ thuộc vào chuỗi hoặc thời gian của các sự kiện không thể kiểm soát.
 - **Time-of-check (TOC) / Time-of-use (TOU)**: Lỗ hổng này có thể xảy ra nếu trạng thái của hệ thống thay đổi giữa thời điểm kiểm tra và thời điểm sử dụng kết quả từ việc kiểm tra.

- **Malicious Update:** Các cập nhật chứa mã độc hại hoặc làm suy yếu các cơ chế bảo mật.

b. Operating System (OS)-based Vulnerabilities:

Các điểm yếu trong hệ điều hành có thể được khai thác để có được quyền truy cập trái phép, nâng cao đặc quyền, v.v.

c. Web-based Vulnerabilities:

- **Structured Query Language Injection (SQL):** Kẻ tấn công chèn mã SQL độc hại vào các trường input để thao túng với cơ sở dữ liệu, dẫn đến truy cập trái phép hoặc rò rỉ dữ liệu.
- **Cross-site Scripting (XSS):** Kẻ tấn công chèn các script độc hại vào website, sau đó được thực thi bởi trình duyệt của nạn nhân.

d. Hardware Vulnerabilities:

- **Firmware Vulnerabilities:** Các điểm yếu trong phần mềm cấp thấp chạy trên các thiết bị phần cứng.
- **End-of-life Hardware:** Các thiết bị không còn được nhà sản xuất hỗ trợ, dẫn đến các lỗ hổng không được vá.
- **Legacy Hardware:** Phần cứng cũ có thể không tương thích với các biện pháp bảo mật hiện tại.

e. Virtualization Vulnerabilities:

- **Virtual Machine (VM) Escape:** Kẻ tấn công chạy mã trên VM cho phép họ thoát ra và tương tác với hệ thống host.
- **Resource Reuse:** Dữ liệu nhạy cảm có thể vẫn còn trong tài nguyên hệ thống và được truy cập bởi các quy trình khác.

f. Cloud-specific Vulnerabilities:

Các điểm yếu cụ thể của dịch vụ cloud, bao gồm cấu hình sai, API không bảo mật và vi phạm dữ liệu.

g. Supply Chain Vulnerabilities:

- **Service Provider:** Lỗ hổng được đưa vào bởi các nhà cung cấp dịch vụ bên thứ ba.
- **Hardware Provider:** Các điểm yếu hoặc backdoor trong phần cứng được cung cấp bởi bên thứ ba.
- **Software Provider:** Lỗ hổng trong các sản phẩm phần mềm hoặc thư viện của bên thứ ba.

h. Cryptographic Vulnerabilities:

Các điểm yếu trong thuật toán mã hóa hoặc việc triển khai của chúng có thể được khai thác để giải mã dữ liệu nhạy cảm.

i. Misconfiguration:

Phần mềm hoặc phần cứng được cấu hình không chính xác, khiến các port bảo mật bị lỗ hổng.

j. Mobile Device Vulnerabilities:

- **Side Loading:** Cài đặt ứng dụng từ các nguồn không chính thức có thể đưa vào các ứng dụng độc hại.
- **Jailbreaking:** Bỏ qua các cơ chế bảo mật tích hợp của iOS, khiến thiết bị dễ bị tấn công.

k. Zero-day Vulnerabilities:

Các lỗ hổng chưa được biết đến trước đó mà chưa được các nhà cung cấp vá lỗi. Vì những lỗ hổng này chưa được công chúng biết đến, không có biện pháp phòng thủ nào cho đến khi chúng được phát hiện.

8. DỰA TRÊN KỊCH BẢN, PHÂN TÍCH CÁC CHỈ BÁO HOẠT ĐỘNG ĐỘC HẠI

Phân tích các chỉ báo hoạt động độc hại có nghĩa là tìm kiếm các dấu hiệu hoặc bằng chứng cho thấy một cuộc tấn công hoặc sự xâm phạm đã xảy ra hoặc đang diễn ra. Dưới đây là cách bạn có thể phân tích các chỉ báo được đưa ra trong các kịch bản hoạt động độc hại khác nhau:

a. Malware Attacks

- **Các Chỉ Báo Chung:** Hành vi hệ thống bất thường, vấn đề về hiệu suất, mất dữ liệu, truy cập dữ liệu trái phép hoặc truyền tải.
 - Ransomware: Mã hóa tệp đột ngột, hiển thị thông báo tiền chuộc, thay đổi phần mở rộng tệp.
 - Trojan: Các ứng dụng không mong muốn đang chạy, thay đổi hệ thống trái phép.
 - Worm: Lây lan nhanh chóng qua các thiết bị mạng, hành vi tự sao chép.
 - Spyware: Truyền tải dữ liệu trái phép, quảng cáo popup, thay đổi cài đặt trình duyệt.
 - Bloatware: Cài đặt phần mềm không mong muốn, giảm hiệu suất hệ thống.
 - Virus: Tệp bị hỏng, hành vi chương trình bị thay đổi, vấn đề khởi động.
 - Keylogger: Truy cập dữ liệu trái phép, đầu vào bất ngờ được ghi lại.

- Logic Bomb: Các sự kiện được kích hoạt tại các điều kiện hoặc ngày cụ thể.
- Rootki: Sự hiện diện malware không thể phát hiện, kiểm soát hệ thống sâu bởi các thực thể không rõ.

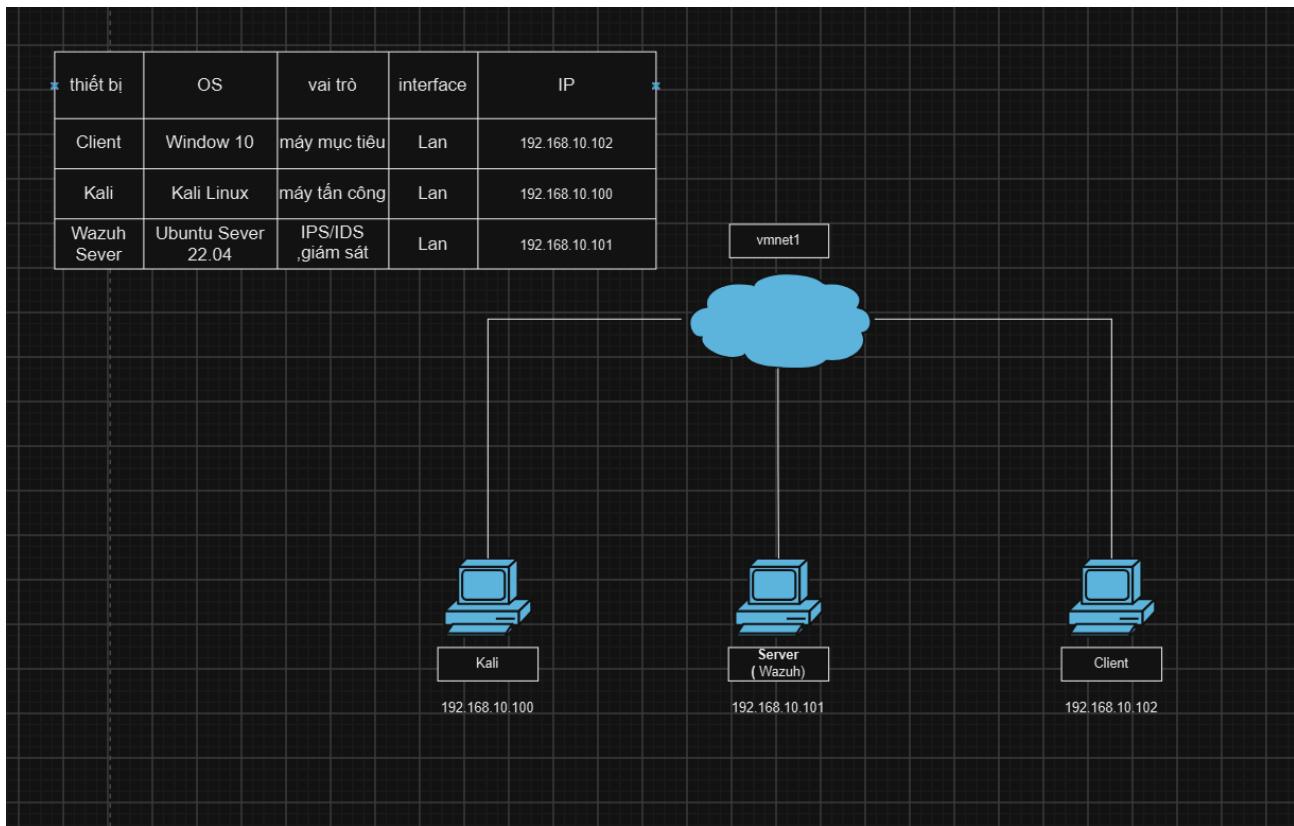
b. Physical Attacks

- **Brute Force:** Thiệt hại có thể nhìn thấy đối với khóa hoặc điểm vào, việc xâm nhập trái phép.
- **RFID Cloning:** Truy cập trái phép bằng cách sử dụng thẻ RFID nhân bản.
- **Environmental:** Thao tác các điều khiển môi trường như sưởi ấm hoặc làm mát.

c. Network Attacks

- **Distributed Denial-of-Service (DDoS):**
 - **Amplified/Reflected**: Lượng lớn lưu lượng từ nhiều nguồn.
- **DNS Attacks:** Lưu lượng được chuyển hướng, domain trái phép.
- **Wireless Attacks:** Các thiết bị trái phép trên mạng, SSID không rõ.
- **On-path (Man-in-the-Middle):** Dữ liệu bị chặn, giao tiếp bị thay đổi.
- **Credential Replay:** Nhiều nỗ lực đăng nhập từ cùng một thông tin đăng nhập.

9. Sơ đồ thiết kế hệ thống mạng lan



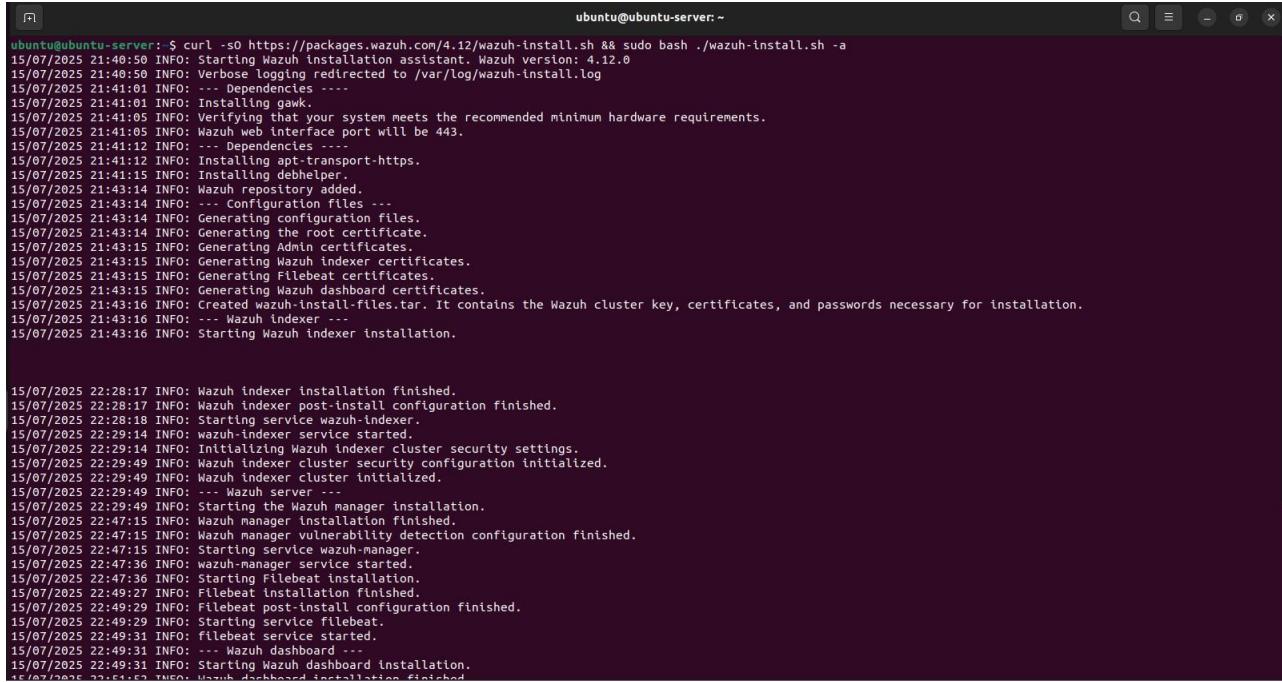
Hình 26. Sơ đồ thiết kế hệ thống mạng lan

CHƯƠNG III. SẢN PHẨM THỰC NGHIỆM

1. Cài đặt Wazuh

a. Cài đặt Wazuh Server

```
curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```



The screenshot shows a terminal window titled "ubuntu@ubuntu-server:~". The log output is as follows:

```
ubuntu@ubuntu-server:~$ curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
15/07/2025 21:40:50 INFO: Starting Wazuh installation assistant. Wazuh version: 4.12.0
15/07/2025 21:40:50 INFO: Verbose logging redirected to /var/log/wazuh-install.log
15/07/2025 21:41:01 INFO: Dependencies ***
15/07/2025 21:41:01 INFO: Installing gawk.
15/07/2025 21:41:05 INFO: Verifying that your system meets the recommended minimum hardware requirements.
15/07/2025 21:41:05 INFO: Wazuh web interface port will be 443.
15/07/2025 21:41:12 INFO: --- Dependencies ***
15/07/2025 21:41:12 INFO: Installing apt-transport-https.
15/07/2025 21:41:15 INFO: Installing debhelper.
15/07/2025 21:43:14 INFO: Wazuh repository added.
15/07/2025 21:43:14 INFO: --- Configuration files ***
15/07/2025 21:43:14 INFO: Generating configuration files.
15/07/2025 21:43:14 INFO: Generating the root certificate.
15/07/2025 21:43:15 INFO: Generating Admin certificates.
15/07/2025 21:43:15 INFO: Generating Wazuh Indexer certificates.
15/07/2025 21:43:15 INFO: Generating Filebeat certificates.
15/07/2025 21:43:16 INFO: Generating Wazuh dashboard certificates.
15/07/2025 21:43:16 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
15/07/2025 21:43:16 INFO: --- Wazuh indexer ***
15/07/2025 21:43:16 INFO: Starting Wazuh indexer installation.

15/07/2025 22:28:17 INFO: Wazuh indexer installation finished.
15/07/2025 22:28:17 INFO: Wazuh indexer post-install configuration finished.
15/07/2025 22:28:18 INFO: Starting service wazuh-indexer.
15/07/2025 22:29:14 INFO: wazuh-indexer service started.
15/07/2025 22:29:14 INFO: Initializing Wazuh indexer cluster security settings.
15/07/2025 22:29:49 INFO: Wazuh indexer cluster security configuration initialized.
15/07/2025 22:29:49 INFO: Wazuh indexer cluster initialized.
15/07/2025 22:29:49 INFO: --- Wazuh server ***
15/07/2025 22:29:49 INFO: Starting the Wazuh manager installation.
15/07/2025 22:47:11 INFO: Wazuh manager installation finished.
15/07/2025 22:47:11 INFO: Wazuh manager vulnerability detection configuration finished.
15/07/2025 22:47:11 INFO: Starting service wazuh-manager.
15/07/2025 22:47:33 INFO: wazuh-manager service started.
15/07/2025 22:47:36 INFO: Starting Filebeat installation.
15/07/2025 22:49:27 INFO: Filebeat installation finished.
15/07/2025 22:49:27 INFO: Filebeat post-install configuration finished.
15/07/2025 22:49:29 INFO: Starting service filebeat.
15/07/2025 22:49:31 INFO: filebeat service started.
15/07/2025 22:49:31 INFO: --- Wazuh dashboard ***
15/07/2025 22:49:31 INFO: Starting Wazuh dashboard installation.
15/07/2025 22:49:31 INFO: Wazuh dashboard installation finished.
```

Hình 27. Cài đặt Wazuh

```

ubuntu@ubuntu-server:~ 
15/07/2025 21:43:15 INFO: Generating Wazuh dashboard certificates.
15/07/2025 21:43:16 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
15/07/2025 21:43:16 INFO: --- Wazuh Indexer ---
15/07/2025 21:43:16 INFO: Starting Wazuh indexer installation.

15/07/2025 22:28:17 INFO: Wazuh indexer installation finished.
15/07/2025 22:28:17 INFO: Wazuh indexer post-install configuration finished.
15/07/2025 22:28:18 INFO: Starting service wazuh-indexer.
15/07/2025 22:29:14 INFO: wazuh-indexer service started.
15/07/2025 22:29:14 INFO: Initializing Wazuh indexer cluster security settings.
15/07/2025 22:29:49 INFO: Wazuh indexer cluster security configuration initialized.
15/07/2025 22:29:49 INFO: Wazuh indexer cluster initialized.
15/07/2025 22:29:49 INFO: Wazuh server
15/07/2025 22:29:49 INFO: Starting the Wazuh manager installation.
15/07/2025 22:47:15 INFO: Wazuh Manager Installation finished.
15/07/2025 22:47:15 INFO: Wazuh manager vulnerability detection configuration finished.
15/07/2025 22:47:15 INFO: Starting service wazuh-manager.
15/07/2025 22:47:36 INFO: wazuh-manager service started.
15/07/2025 22:47:36 INFO: Starting Filebeat installation.
15/07/2025 22:49:27 INFO: Filebeat installation finished.
15/07/2025 22:49:29 INFO: Filebeat post-install configuration finished.
15/07/2025 22:49:29 INFO: Starting service filebeat.
15/07/2025 22:49:31 INFO: filebeat service started.
15/07/2025 22:49:31 INFO: --- Wazuh dashboard ---
15/07/2025 22:49:31 INFO: Starting Wazuh dashboard installation.
15/07/2025 22:51:52 INFO: Wazuh dashboard installation finished.
15/07/2025 22:51:52 INFO: Wazuh dashboard post-install configuration finished.
15/07/2025 22:51:52 INFO: Starting service wazuh-dashboard.
15/07/2025 22:51:53 INFO: wazuh-dashboard service started.
15/07/2025 22:51:57 INFO: Updating the internal users.
15/07/2025 22:52:18 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
15/07/2025 22:54:34 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
15/07/2025 22:56:01 INFO: Initializing Wazuh dashboard web application.
15/07/2025 22:56:04 INFO: Wazuh dashboard web application initialized.
15/07/2025 22:56:04 INFO: --- Summary ---
15/07/2025 22:56:04 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: 5T7v*ltPdeaBLISH.khynphrkX0VpUp
15/07/2025 22:56:04 INFO: --- Dependencies ---
15/07/2025 22:56:04 INFO: Removing gawk.
15/07/2025 22:56:11 INFO: Installation finished.
ubuntu@ubuntu-server: ~
```

Hình 28. Cài đặt hoàn thành

Tra IP của máy server

Ifconfig

```

ubuntu@ubuntu-server:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.36.145  netmask 255.255.255.0  broadcast 192.168.36.255
        inet6 fe80::906:725f:1f0e:9b22  prefixlen 64  scopeid 0x20<link>
          ether 00:0c:29:72:01:e5  txqueuelen 1000  (Ethernet)
            RX packets 1235  bytes 1329152 (1.3 MB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 353  bytes 36040 (36.0 KB)
            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 144  bytes 13225 (13.2 KB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 144  bytes 13225 (13.2 KB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

ubuntu@ubuntu-server:~$
```

Hình 29. IP máy Wazuh Server

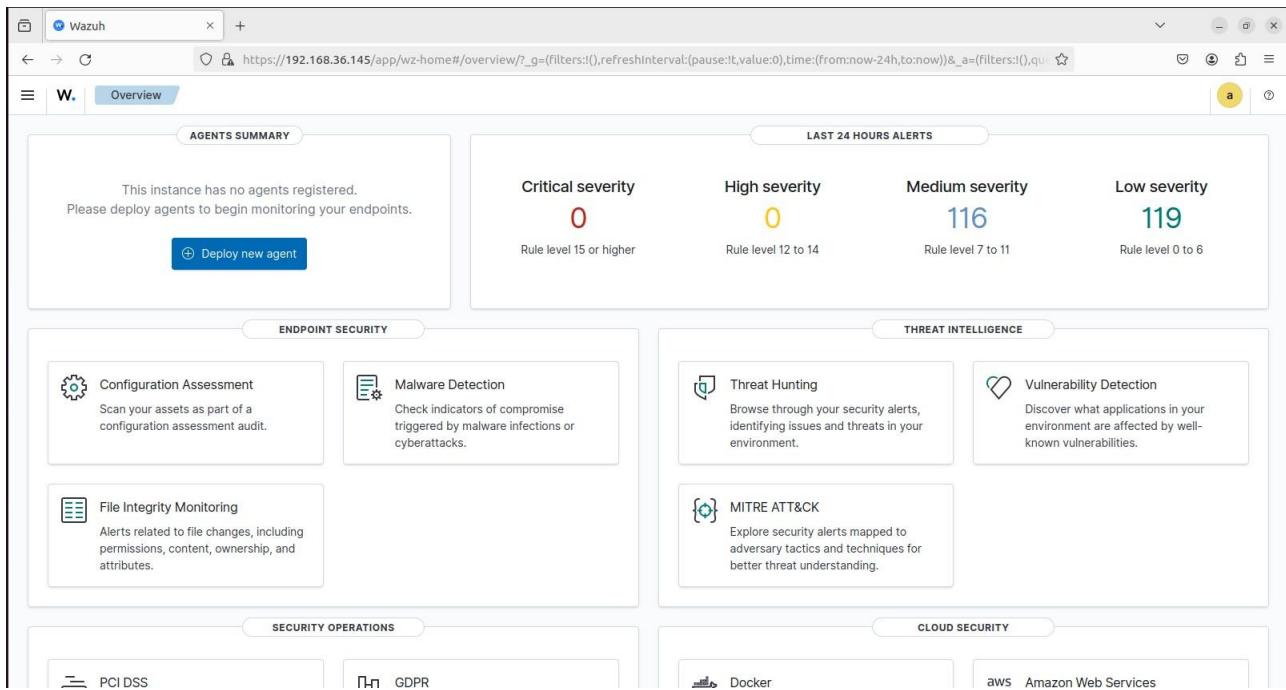
Truy cập giao diện web Wazuh bằng

https://<WAZUH_DASHBOARD_IP_ADDRESS>

<https://192.168.36.145>

User: admin

Password: 5T?v*!TpPdea8LISH.khynphrkX0VpUp



Hình 30. Wazuh Dashboard

Trong trường hợp quên password, ta có thể truy cập

sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt

```

ubuntu@ubuntu-server: $ sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
[sudo] password for ubuntu:
wazuh-install-files/wazuh-passwords.txt
# Admin user for the web user interface and Wazuh indexer. Use this user to log in to Wazuh dashboard
indexer_username: 'admin'
indexer_password: '5T?v*lTpPdea8LISH.khynphrkX0VpUp'

# Anomaly detection user for the web user interface
indexer_username: 'anomalyadmin'
indexer_password: '3ZlUQAJPyAjk12JG?34Gye1ARW72Kx?.'

# Wazuh dashboard user for establishing the connection with Wazuh indexer
indexer_username: 'kibanaserver'
indexer_password: 'Jl2h+Hl37FR69sQed?XLE1*f92.0EYKH'

# Regular Dashboard user, only has read permissions to all indices and all permissions on the .kibana index
indexer_username: 'kibanaro'
indexer_password: 'Mx0Sk1bSs48+V?UZDoahGhjlN.JnDzXk'

# Filebeat user for CRUD operations on Wazuh indices
indexer_username: 'logstash'
indexer_password: '+mc9i0ragN*yXU8J0C3*?*laQ6mBV2+p'

# User with READ access to all indices
indexer_username: 'readall'
indexer_password: 'etr?+Lemp30p4?CZ*q1?*qQyZerD9Xp5'

# User with permissions to perform snapshot and restore operations
indexer_username: 'snapshotrestore'
indexer_password: 'LfMUinQKs+p6U2MdAJ?gjcJEMDyWMjYA'

# Password for wazuh API user
api_username: 'wazuh'
api_password: 'glCcfP2uniBSw9JVT5UUUvgz?9*OLxCTE'

# Password for wazuh-wui API user
api_username: 'wazuh-wui'
api_password: 'chADKDbV0cewyayOkT1zQ6hkYf?kXY2t'

ubuntu@ubuntu-server: $

```

Hình 31. Danh sách password

b. Cài đặt Wazuh Agent

Cài đặt Wazuh Agent trên máy khách (Ubuntu):

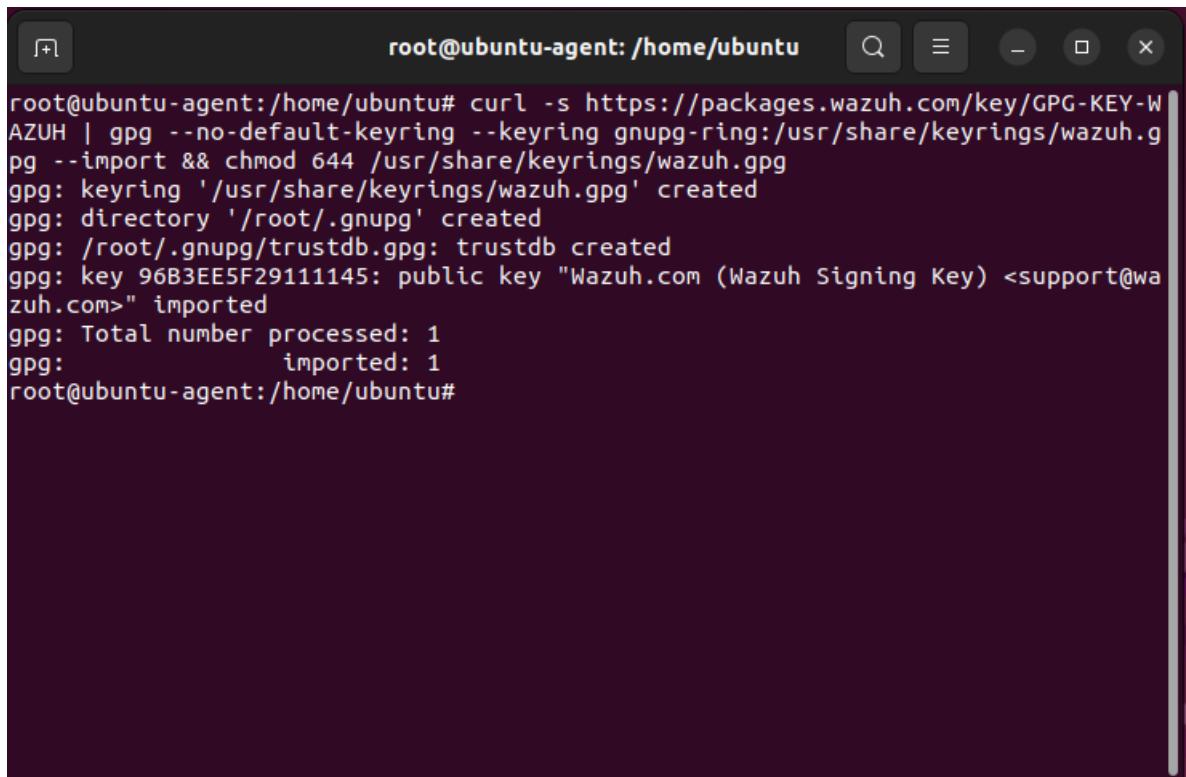
Thêm khóa GPG của Wazuh:

sudo su

```

curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg

```

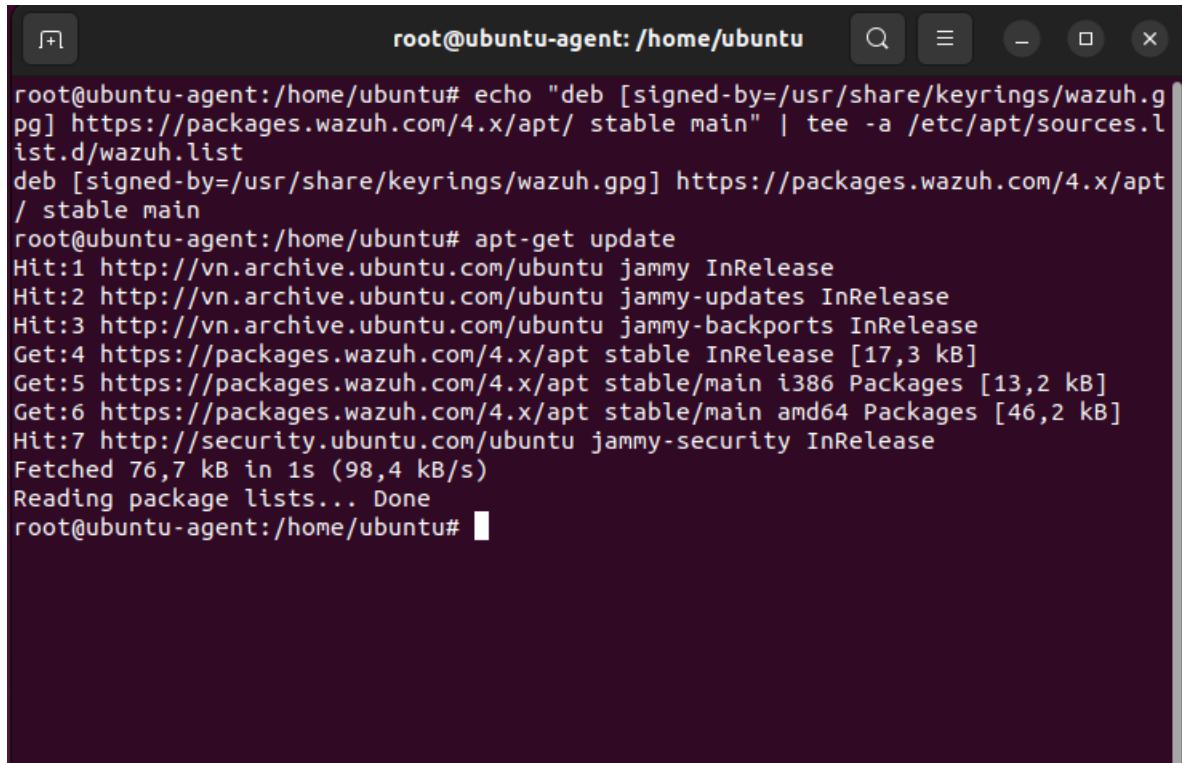


```
root@ubuntu-agent:/home/ubuntu# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
gpg: keyring '/usr/share/keyrings/wazuh.gpg' created
gpg: directory '/root/.gnupg' created
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 96B3EE5F29111145: public key "Wazuh.com (Wazuh Signing Key) <support@wazuh.com>" imported
gpg: Total number processed: 1
gpg:              imported: 1
root@ubuntu-agent:/home/ubuntu#
```

Hình 32. Thêm khóa GPG

Thêm repository:

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg]
https://packages.wazuh.com/4.x/apt/
/stable main" | tee -a
/etc/apt/sources.list.d/wazuh.list
apt-get update
```



The screenshot shows a terminal window titled "root@ubuntu-agent: /home/ubuntu". The user has run the command "echo 'deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main' | tee -a /etc/apt/sources.list.d/wazuh.list" to add the Wazuh repository. Subsequent commands "apt-get update" and "apt-get upgrade" are shown, along with their output, indicating successful repository addition and package updates.

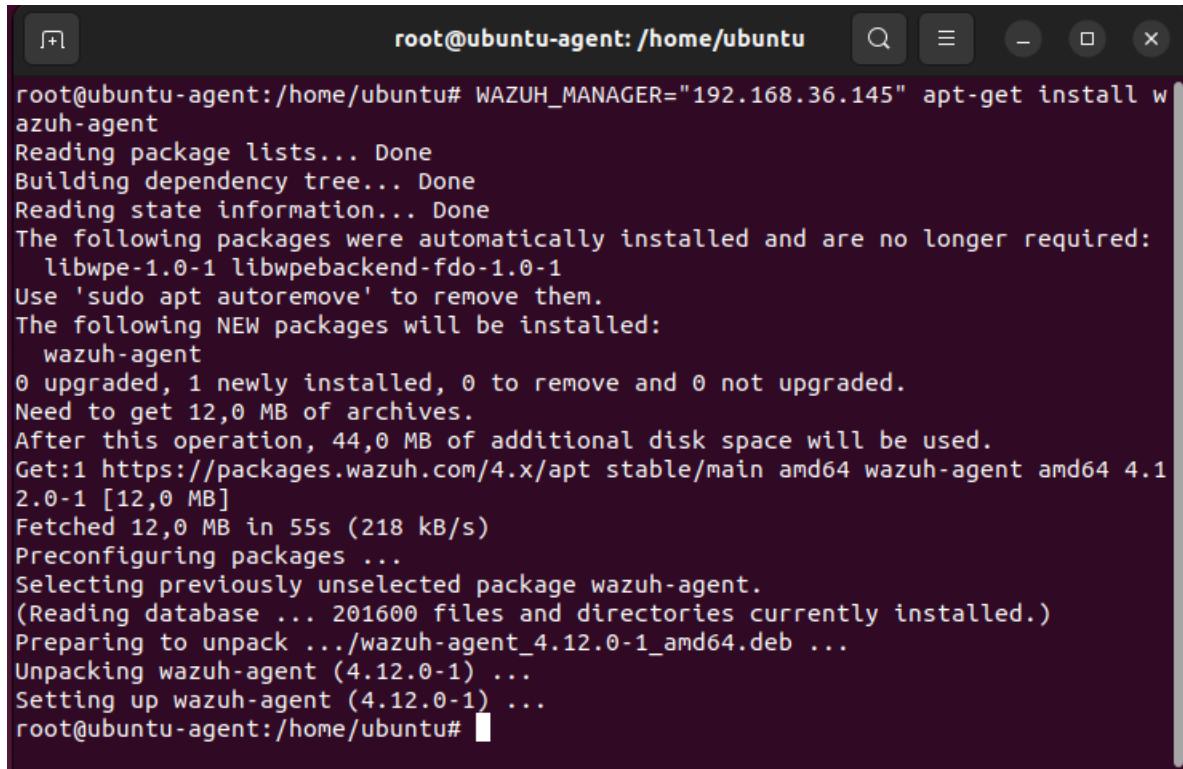
```
root@ubuntu-agent:/home/ubuntu# echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main
root@ubuntu-agent:/home/ubuntu# apt-get update
Hit:1 http://vn.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://vn.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://vn.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:4 https://packages.wazuh.com/4.x/apt stable InRelease [17,3 kB]
Get:5 https://packages.wazuh.com/4.x/apt stable/main i386 Packages [13,2 kB]
Get:6 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [46,2 kB]
Hit:7 http://security.ubuntu.com/ubuntu jammy-security InRelease
Fetched 76,7 kB in 1s (98,4 kB/s)
Reading package lists... Done
root@ubuntu-agent:/home/ubuntu# apt-get upgrade
```

Hình 33. Thêm repository

Deploy a Wazuh agent

WAZUH_MANAGER="IP_SERVER" apt-get install wazuh-agent

WAZUH_MANAGER="192.168.36.145" apt-get install wazuh-agent



```
root@ubuntu-agent:/home/ubuntu# WAZUH_MANAGER="192.168.36.145" apt-get install wazuh-agent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  wazuh-agent
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 12,0 MB of archives.
After this operation, 44,0 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-agent amd64 4.1.2.0-1 [12,0 MB]
Fetched 12,0 MB in 55s (218 kB/s)
Preconfiguring packages ...
Selecting previously unselected package wazuh-agent.
(Reading database ... 201600 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.12.0-1_amd64.deb ...
Unpacking wazuh-agent (4.12.0-1) ...
Setting up wazuh-agent (4.12.0-1) ...
root@ubuntu-agent:/home/ubuntu#
```

Hình 34. Deploy Wazuh Agent

Enable and start the Wazuh agent service

systemctl daemon-reload

systemctl enable wazuh-agent

systemctl start wazuh-agent

systemctl status wazuh-agent

```

root@ubuntu-agent:/home/ubuntu# systemctl daemon-reload
root@ubuntu-agent:/home/ubuntu# systemctl enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/system/wazuh-agent.service.
root@ubuntu-agent:/home/ubuntu# systemctl start wazuh-agent
root@ubuntu-agent:/home/ubuntu# 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 Tue 2025-07-15 23:14:48 +07; 2s ago
     Process: 4734 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/成功)
       Tasks: 31 (limit: 2207)
      Memory: 25.7M
        CPU: 3.816s
      CGroup: /system.slice/wazuh-agent.service
              ├─4756 /var/ossec/bin/wazuh-execd
              ├─4767 /var/ossec/bin/wazuh-agentd
              ├─4781 /var/ossec/bin/wazuh-syscheckd
              ├─4794 /var/ossec/bin/wazuh-logcollector
              ├─4812 /var/ossec/bin/wazuh-modulesd
              └─5122 sudo -V

Thg 7 15 23:14:40 ubuntu-agent systemd[1]: Starting Wazuh agent...
Thg 7 15 23:14:40 ubuntu-agent env[4734]: Starting Wazuh v4.12.0...
Thg 7 15 23:14:42 ubuntu-agent env[4734]: Started wazuh-execd...
Thg 7 15 23:14:43 ubuntu-agent env[4734]: Started wazuh-agentd...
Thg 7 15 23:14:44 ubuntu-agent env[4734]: Started wazuh-syscheckd...
Thg 7 15 23:14:45 ubuntu-agent env[4734]: Started wazuh-logcollector...
Thg 7 15 23:14:46 ubuntu-agent env[4734]: Started wazuh-modulesd...
Thg 7 15 23:14:48 ubuntu-agent env[4734]: Completed.
lines 1-23...skipping...

```

Hình 35. Khởi động lại các dịch vụ

IP máy Agent

```

ubuntu@ubuntu-agent: ~
ubuntu@ubuntu-agent: $ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.36.146 netmask 255.255.255.0 broadcast 192.168.36.255
        inet6 fe80::1b0a:4954:40e6:648e prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:80:dc:36 txqueuelen 1000 (Ethernet)
                RX packets 1161 bytes 522385 (522.3 KB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 220 bytes 21670 (21.6 KB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

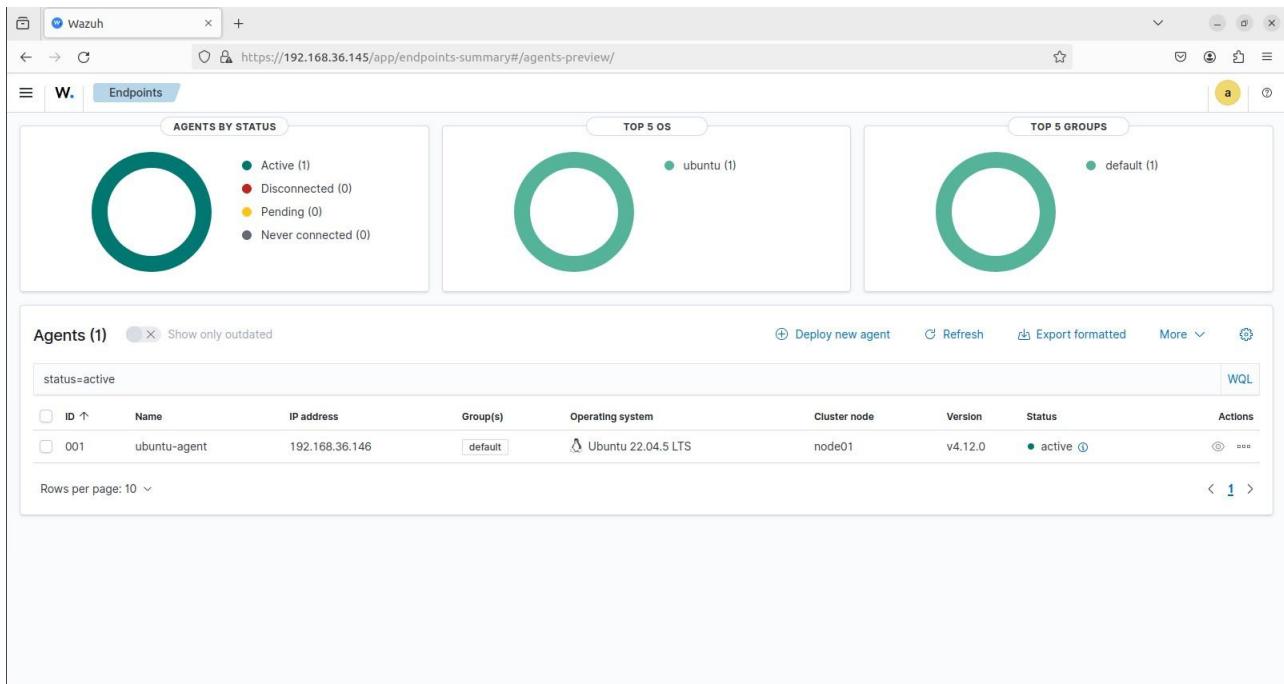
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 149 bytes 13539 (13.5 KB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 149 bytes 13539 (13.5 KB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ubuntu@ubuntu-agent: $

```

Hình 36. IP máy Agent

Kiểm tra bên Wazuh Dashboard



Hình 37. Agent hiện bên Dashboard

2. Cấu hình và triển khai

2.1. Tích hợp Suricata IDS phát hiện xâm nhập mạng

Cài đặt Suricata

```
sudo add-apt-repository ppa:oisf/suricata-stable
```

```
sudo apt-get update
```

```
sudo apt-get install suricata -y
```

```

root@ubuntu-agent:/home/ubuntu# sudo add-apt-repository ppa:oisf/suricata-stable
Repository: 'deb https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/ jammy main'
Description: Suricata IDS/IPS/NSM stable packages
https://suricata.io/
https://oisf.net/
Suricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevention System and Network Security Monitoring engine.
Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF, its supporting vendors and the community.
This Engine supports:
- Multi-Threading - provides for extremely fast and flexible operation on multicore systems.
- Multi Tenancy - Per vlan/Per interface
- Uses Rust for most protocol detection/parsing
- TLS support - certificate matching/logging
- JA3 TLS client fingerprinting
- JA3S TLS server fingerprinting
- IEEE 802.1ad (QInQ) and IEEE 802.1Q (VLAN) support
- VXLAN support
- All JSON output/logging capability
- IDS runmode
- IPS runmode
- IDPS runmode
- NSM runmode
- ebPF/XDP
- Automatic Protocol Detection and logging - IPv4/6, TCP, UDP, ICMP, HTTP, SMTP, TLS, SSH, SMB, DNS, NFS, TFTP, KRBS, DHCP, IKEV2, SNMP, SIP, RDP
SCADA automatic protocol detection - ENIP/DNP3/MODBUS
- File MD5/SHA1/SHA256 matching
- Gzip Decompression
- Fast IP Matching
- Datasets matching
- Rustlang enabled protocol detection
- Lua scripting
and many more great features -
https://suricata.io/features/all-features/
More info: https://launchpad.net/~oisf/+archive/ubuntu/suricata-stable
Adding repository...
Press [ENTER] to continue or Ctrl-c to cancel.
Adding deb entry to /etc/apt/sources.list.d/oisf-ubuntu-suricata-stable-jammy.list

```

Hình 38. Suricata setup

```

root@ubuntu-agent:/home/ubuntu# sudo apt-get update
Hit:1 http://vn.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://vn.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://vn.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:5 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu jammy InRelease
Reading package lists... Done
root@ubuntu-agent:/home/ubuntu# sudo apt-get install suricata -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  liblwepe-1.0-1 liblwepebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libevent-core-2.1-7 libevent-pthreads-2.1-7 libbiredis0.14 libhyperscan5 libluajit-5.1-common libnet1 libnetfilter-queue1
The following NEW packages will be installed:
  libevent-core-2.1-7 libevent-pthreads-2.1-7 libbiredis0.14 libhyperscan5 libluajit-5.1-common libnet1 libnetfilter-queue1 suricata
0 upgraded, 8 newly installed, 0 to remove and 16 not upgraded.
Need to get 2,293 kB of archives.
After this operation, 33,940 kB of additional disk space will be used.
Get:1 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 libhyperscan5 amd64 5.4.0-2 [2,485 kB]
Get:2 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu jammy/main amd64 suricata amd64 1:8.0.0-0ubuntu0 [4,567 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu jammy/main amd64 libevent-core-2.1-7 amd64 2.1.12-stable-1build3 [93.9 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu jammy/main amd64 libevent-pthreads-2.1-7 amd64 2.1.12-stable-1build3 [7,642 B]
Get:5 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 libbiredis0.14 amd64 0.14.1-2 [32.8 kB]
Get:6 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 libluajit-5.1-common all 2.1.0-beta3+dfsg-6 [44.3 kB]
Get:7 http://vn.archive.ubuntu.com/ubuntu jammy/main amd64 libnet1 amd64 1.1.6+dfsg-3.1build3 [46.9 kB]
Get:8 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 libnetfilter-queue1 amd64 1.0.5-2 [14.4 kB]
Fetched 7,293 kB in 48s (152 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libhyperscan5.
(Reading database ... 202040 files and directories currently installed.)
Preparing to unpack .../0-libhyperscan5_5.4.0-2_amd64.deb ...
Unpacking libhyperscan5 (5.4.0-2) ...
Selecting previously unselected package libevent-core-2.1-7:amd64.
Preparing to unpack .../1-libevent-core-2.1-7_2.1.12-stable-1build3_amd64.deb ...
Unpacking libevent-core-2.1-7:amd64 (2.1.12-stable-1build3) ...
Selecting previously unselected package libevent-pthreads-2.1-7:amd64.
Preparing to unpack .../2-libevent-pthreads-2.1-7_2.1.12-stable-1build3_amd64.deb ...
Unpacking libevent-pthreads-2.1-7:amd64 (2.1.12-stable-1build3) ...
Selecting previously unselected package libbiredis0.14:amd64.
Preparing to unpack .../3-libbiredis0.14_0.14.1-2_amd64.deb ...
Unpacking libbiredis0.14:amd64 (0.14.1-2) ...

```

Hình 39. suricata setup

sudo mkdir /etc/suricata/rules

cd /etc/suricata/rules

Tạo rule cảnh báo ICMP

Nano emerging-icmp_info.rules

```
root@ubuntu-agent: /etc/suricata/rules
GNU nano 6.2                                     emerging-icmp_info.rules

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP_INFO PING BS0type"; itype:8; content:"|08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17|"; depth:32; reference:arachni,157);
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP_INFO PING BayRS Router"; itype:8; content:"|01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F|"; depth:32; reference:arachni,157);
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP_INFO PING Be054.x"; itype:8; content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"; depth:32; reference:arachni,157);
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP_INFO PING Cisco Type.x"; itype:8; content:"|AB CD AB CD AB CD AB CD AB CD AB CD AB CD|"; depth:32; reference:arachni,157);
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP_INFO PING Flowpoint2200 or Network Management Software"; itype:8; content:"|01 02 03 04 05 06 07 08 09 0A 0B 0C 0D|"; depth:32; reference:arachni,157);
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP_INFO PING IP NetMonitor Macintosh"; itype:8; content:"|A9| Sustainable So|"; depth:32; reference:arachni,157); class:info
```

Hình 40. Tạo rule cảnh báo ICMP

Tạo rule cảnh báo policy

Nano emerging-policy.rules

```
root@ubuntu-agent: /etc/suricata/rules
GNU nano 6.2
alert tcp $HOME_NET 21 -> $EXTERNAL_NET any (msg:"ET POLICY External FTP Connection TO Local HP JetDirect Printer"; flow:to_client,established; content:"Hewlett-Packard FTP Pr
alert ip $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY Protocol 41 IPv6 encapsulation potential 6in4 IPv6 tunnel active"; ip_proto:41; threshold:type both,track_by_dst, cb
#alert ip [0.0.0.8,192.0.0.8/24,192.0.2.0/24,198.18.0.0/15,198.51.100.0/24,203.0.111.0/24] any -> $HOME_NET any (msg:"ET POLICY Unallocated IP Space Traffic - Bogon Nets"; t
alert udp $HOME_NET 17500 -> any 17500 (msg:"ET POLICY Dropbox Client Broadcasting"; content:"[|22|host_int[22 3a] |"; depth:13; content:"|22|version[22 3a] |"; distance:0; co
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY Windows-Based OpenSSL Tunnel Outbound"; flow:established; content:"|16 03 00||"; content:"|00 5c|"; distance:0; co
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY WIndows-Based OpenSSL Tunnel Connection Outbound 1"; flow:established; content:"|16 03 00||"; content:"|00 26|"; di
alert tcp $HOME_NET any -> $EXTERNAL_NET any 443 (msg:"ET POLICY WIndows-Based OpenSSL Tunnel Connection Outbound 3"; flow:established; content:"|16 03 00||"; content:"|00 34|"; di
#alert tcp $HOME_NET any -> $EXTERNAL_NET 13389 (msg:"ET POLICY Remote Desktop Connection via non RDP Port"; flow:established,to_server; content:"|03|"; depth:1; content:"|e0|>
#alert tcp $EXTERNAL_NET any -> $HOME_NET 3389 (msg:"GPL POLICY MS Remote Desktop Request RDP"; flow:to_server,established; content:"|03 00 00|"; depth:3; content:"|e0 00 00 00
alert tcp $EXTERNAL_NET any -> $HOME_NET 3389 (msg:"ET POLICY MS Terminal Server Root login"; flow:established,to_server; content:"|03 00 00||"; depth:3; content:"|e0 00 00 00
alert tcp $EXTERNAL_NET any -> $HOME_NET 3389 (msg:"ET POLICY MS Remote Desktop Service User Login Request"; flow:to_server,established; content:"|03 00 00||"; depth:3; content:"|e0 00 00 00
alert tcp $EXTERNAL_NET any -> $HOME_NET 3389 (msg:"ET POLICY MS Remote Desktop POS User Login Request"; flow:to_server,established; content:"|03 00 00||"; depth:3; content:"|e0 00 00 00
```

Hình 41. rule cảnh báo policy

Tạo rule cảnh báo scan

Nano emerging-scan.rules

Hình 42. rule cảnh báo scan

Cấp quyền cho các file *.rules

```
sudo chmod 640 /etc/suricata/rules/*.rules
```

Sửa đổi cài đặt Suricata trong tệp /etc/suricata/suricata.yaml và đặt các biến sau:

HOME_NET: "<UBUNTU_IP>"

EXTERNAL_NET: "any"

default-rule-path: /etc/suricata/rules

rule-files:

- "*.rules"

Global stats configuration

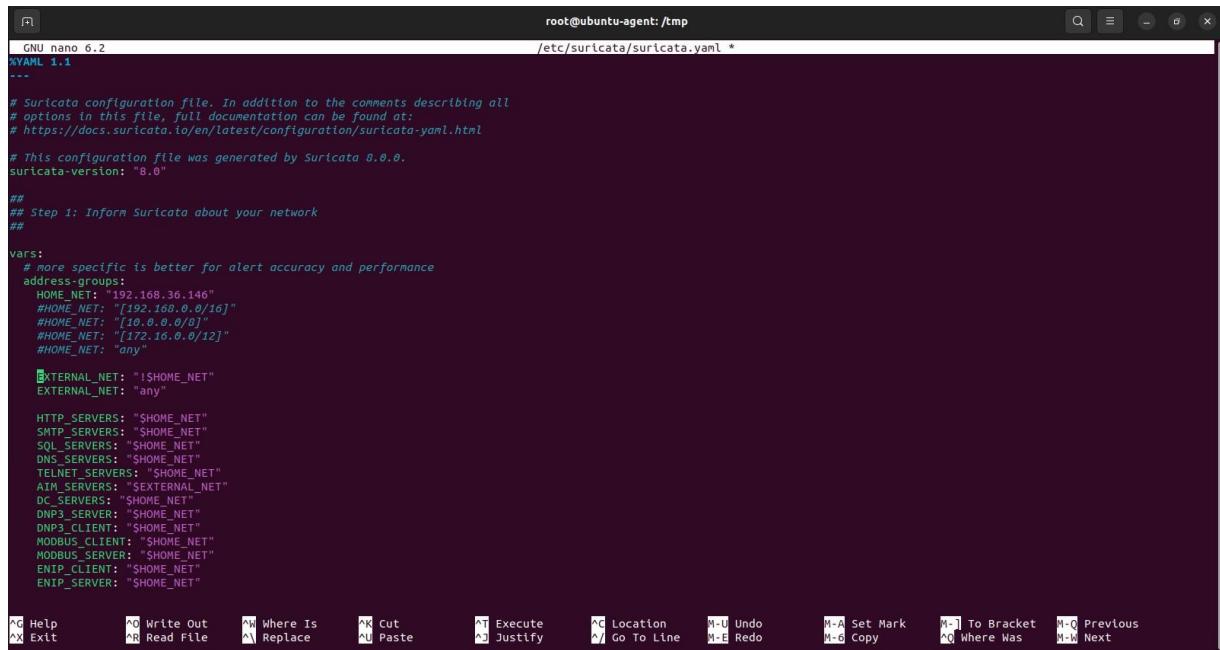
stats:

enabled: yes

Linux high speed capture support

af-packet:

- interface: ens33



```
GNU nano 6.2                                     root@ubuntu-agent:/tmp
---                                                 /etc/suricata/suricata.yaml *
# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html
# This configuration file was generated by Suricata 8.0.0.
suricata-version: "8.0"

##
## Step 1: Inform Suricata about your network
##

vars:
    # more specific is better for alert accuracy and performance
    address-groups:
        HOME_NET: "192.168.36.146"
        #HOME_NET: "[192.168.0.0/16]"
        #HOME_NET: "[10.0.0.0/8]"
        #HOME_NET: "[172.16.0.0/12]"
        #HOME_NET: "any"

        EXTERNAL_NET: "!$HOME_NET"
        EXTERNAL_NET: "any"

        HTTP_SERVERS: "$HOME_NET"
        SMTP_SERVERS: "$HOME_NET"
        SQL_SERVERS: "$HOME_NET"
        DNS_SERVERS: "$HOME_NET"
        TELNET_SERVERS: "$HOME_NET"
        AIM_SERVERS: "$EXTERNAL_NET"
        DC_SERVERS: "$HOME_NET"
        DNP3_SERVER: "$HOME_NET"
        DNP3_CLIENT: "$HOME_NET"
        MODBUS_CLIENT: "$HOME_NET"
        MODBUS_SERVER: "$HOME_NET"
        ENIP_CLIENT: "$HOME_NET"
        ENIP_SERVER: "$HOME_NET"

^G Help      ^Q Write Out   ^W Where Is   ^X Cut          ^T Execute   ^C Location   ^U Undo       ^A Set Mark   ^I To Bracket  ^O Previous
^X Exit      ^R Read File   ^R Replace    ^U Paste        ^D Justify   ^F Go To Line  ^E Redo       ^M-C Copy     ^P Where Was   ^W Next
```

Hình 43. Sửa đổi cài đặt Suricata trong tệp

```

GNU nano 6.2                                     root@ubuntu-agent:/tmp
# ports: [0-1,2-3]
#
# When auto-config is enabled the hashmode specifies the algorithm for
# determining to which stream a given packet is to be delivered.
# This can be any valid Nopatech NTPL hashmode command.
#
# The most common hashmode commands are: hash2tuple, hash2tuplesorted,
# hashStuple, hashStuplesorted and roundRobin.
#
# See Nopatech NTPL documentation other hashmodes and details on their use.
#
# This parameter has no effect if auto-config is disabled.
#
hashmode: hashStuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##

default-rule-path: /etc/suricata/rules

rule-files:
- "*.*rules"
#
## Auxiliary configuration files.
##

classification-file: /etc/suricata/classification.config
reference-config-file: /etc/suricata/reference.config
# threshold-file: /etc/suricata/threshold.config

##
## Suricata as a Firewall options (experimental)
##
firewall:
# toggle to enable firewall mode
enabled: no

GN Help      W Write Out   W Where Is    C Cut          E Execute     L Location   U Undo       A Set Mark   T To Bracket   P Previous
X Exit       R Read File   R Replace    U Paste        J Justify    G Go To Line M-E Redo     M-A Copy     M-Q Where Was  M-W Next

```

Hình 44. Sửa đổi cài đặt Suricata trong tệp

```

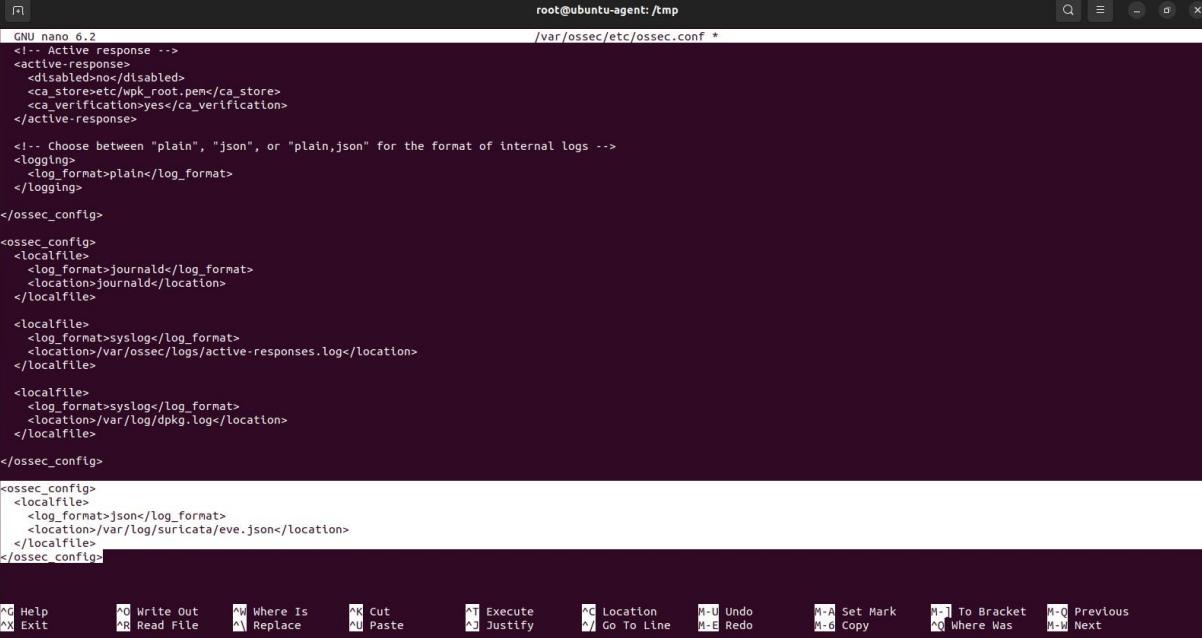
GNU nano 6.2                                     root@ubuntu-agent:/tmp
file:
- file:
  enabled: yes
  level: info
  filename: suricata.log
  # format: "[%l - %m] %z %d: %S: %M"
  # type: json
-syslog:
  enabled: no
  facility: locals
  format: "[%i] <%d> -- "
  # type: json

##
## Step 3: Configure common capture settings
##
## See "Advanced Capture Options" below for more options, including Netmap
## and PF_RING.
##
# Linux high speed capture support
af-packet:
- interface: ens33
  # Number of receive threads. "auto" uses the number of cores
  #threads: auto
  # Default clusterid. AF_PACKET will load balance packets based on flow.
  cluster-id: 99
  # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per hash.
  # This is only supported for Linux kernel > 3.1
  # possible value are:
  # * cluster_flow: all packets of a given flow are sent to the same socket
  # * cluster_cpu: all packets treated in kernel by a CPU are sent to the same socket
  # * cluster_qm: all packets linked by network card to a RSS queue are sent to the same
  #   socket. Requires at least Linux 3.14.
  # * cluster_ebpf: eBPF file load balancing. See doc/ugruidge/capture-hardware/ebpf-xdp.rst for
  #   more info.
  # Recommended modes are cluster_flow on most boxes and cluster_cpu or cluster_qm on system
  # with capture card using RSS (requires cpu affinity tuning and system IRQ tuning)
  # cluster_rollover has been deprecated; if used, it'll be replaced with cluster_flow.
  cluster-type: cluster_flow

GN Help      W Write Out   W Where Is    C Cut          E Execute     L Location   U Undo       A Set Mark   T To Bracket   P Previous
X Exit       R Read File   R Replace    U Paste        J Justify    G Go To Line M-E Redo     M-A Copy     M-Q Where Was  M-W Next

```

Hình 45. Sửa đổi cài đặt Suricata trong tệp



```
GNU nano 6.2                                     root@ubuntu-agent:/tmp
/var/ossec/etc/ossec.conf *

<!-- Active response -->
<active-response>
  <disabled>no</disabled>
  <ca_store>/etc/wpk_root.pem</ca_store>
  <ca_verification>yes</ca_verification>
</active-response>

<!-- Choose between "plain", "json", or "plain,json" for the format of internal logs -->
<logging>
  <log_format>plain</log_format>
</logging>

</ossec_config>

<ossec_config>
  <localfile>
    <log_format>journald</log_format>
    <location>journald</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/ossec/logs/active-responses.log</location>
  </localfile>

  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/dpkg.log</location>
  </localfile>
</ossec_config>

<ossec_config>
  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>
</ossec_config>

^G Help      ^O Write Out   ^W Where Is   ^K Cut        ^T Execute   ^C Location   M-U Undo   M-A Set Mark   M-[ To Bracket   M-Q Previous
^X Exit      ^R Read File   ^H Replace   ^U Paste     ^D Justify   ^V Go To Line M-E Redo   M-C Copy      M-Q Where Was   M-W Next
```

Hình 46. Sửa đổi cài đặt Suricata trong tệp

Mô phỏng tấn công

ping -c 20 192.168.36.146

```
(kali㉿kali)-[~]
$ ping -c 20 192.168.36.146
PING 192.168.36.146 (192.168.36.146) 56(84) bytes of data.
64 bytes from 192.168.36.146: icmp_seq=1 ttl=64 time=2.03 ms
64 bytes from 192.168.36.146: icmp_seq=2 ttl=64 time=0.869 ms
64 bytes from 192.168.36.146: icmp_seq=3 ttl=64 time=0.440 ms
64 bytes from 192.168.36.146: icmp_seq=4 ttl=64 time=0.388 ms
64 bytes from 192.168.36.146: icmp_seq=5 ttl=64 time=0.789 ms
64 bytes from 192.168.36.146: icmp_seq=6 ttl=64 time=0.805 ms
64 bytes from 192.168.36.146: icmp_seq=7 ttl=64 time=0.426 ms
64 bytes from 192.168.36.146: icmp_seq=8 ttl=64 time=0.656 ms
64 bytes from 192.168.36.146: icmp_seq=9 ttl=64 time=0.419 ms
64 bytes from 192.168.36.146: icmp_seq=10 ttl=64 time=0.650 ms
64 bytes from 192.168.36.146: icmp_seq=11 ttl=64 time=0.410 ms
64 bytes from 192.168.36.146: icmp_seq=12 ttl=64 time=0.513 ms
64 bytes from 192.168.36.146: icmp_seq=13 ttl=64 time=0.554 ms
64 bytes from 192.168.36.146: icmp_seq=14 ttl=64 time=0.559 ms
64 bytes from 192.168.36.146: icmp_seq=15 ttl=64 time=0.531 ms
64 bytes from 192.168.36.146: icmp_seq=16 ttl=64 time=0.450 ms
64 bytes from 192.168.36.146: icmp_seq=17 ttl=64 time=0.459 ms
64 bytes from 192.168.36.146: icmp_seq=18 ttl=64 time=0.349 ms
64 bytes from 192.168.36.146: icmp_seq=19 ttl=64 time=0.948 ms
64 bytes from 192.168.36.146: icmp_seq=20 ttl=64 time=0.404 ms

--- 192.168.36.146 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19147ms
rtt min/avg/max/mdev = 0.349/0.632/2.027/0.362 ms
```

Hình 47. Mô phỏng tấn công

Check log trên wazuh

192 hits				
Jul 22, 2025 @ 01:45:52.437 - Jul 23, 2025 @ 01:45:52.438				
Export Formatted	641 available fields	Columns	Density	1 fields sorted
↓ timestamp	↑ agent.name	rule.description	rule.level	rule.id
Jul 23, 2025 @ 01:45:47.843	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:47.840	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:45.841	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:45.841	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:43.841	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:43.838	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:41.878	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:41.835	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:21.815	ubuntu-agent	Suricata: Alert - ET POLICY Possible Kali Linux hostname in DHCP Request Packet	3	86601
Jul 23, 2025 @ 01:43:37.983	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:43:37.699	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:43:35.966	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:43:35.693	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:43:33.950	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:43:33.692	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601

Rows per page: 15 < 1 2 3 4 5 ... 13 >

Hình 48. Check log trên wazuh

Nmap 192.168.36.146

```
(kali㉿kali)-[~]
└─$ nmap 192.168.36.146
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-22 14:47 EDT
Nmap scan report for 192.168.36.146
Host is up (0.00027s latency).
All 1000 scanned ports on 192.168.36.146 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:80:DC:36 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds

(kali㉿kali)-[~]
└─$
```

Hình 49. Nmap

Check log trên Wazuh

Wazuh Threat Hunting

209 hits
Jul 22, 2025 @ 01:47:29.173 - Jul 23, 2025 @ 01:47:29.175

Export Formatted | 641 available fields | Columns | Density | 1 fields sorted | Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Jul 23, 2025 @ 01:47:23.993	ubuntu-agent	Suricata: Alert - ET SCAN Suspicious inbound to PostgreSQL port 5432	3	86601
Jul 23, 2025 @ 01:47:23.992	ubuntu-agent	Suricata: Alert - ET SCAN Potential VNC Scan 5800-5820	3	86601
Jul 23, 2025 @ 01:47:23.951	ubuntu-agent	Suricata: Alert - ET SCAN Suspicious inbound to mySQL port 3306	3	86601
Jul 23, 2025 @ 01:47:23.951	ubuntu-agent	Suricata: Alert - ET SCAN Suspicious inbound to Oracle SQL port 1521	3	86601
Jul 23, 2025 @ 01:47:23.951	ubuntu-agent	Suricata: Alert - ET SCAN Suspicious inbound to MSSQL port 1433	3	86601
Jul 23, 2025 @ 01:45:59.860	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:59.855	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:57.857	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:57.853	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:55.855	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:55.850	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:53.890	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:53.848	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:51.847	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601
Jul 23, 2025 @ 01:45:51.846	ubuntu-agent	Suricata: Alert - GPL ICMP_INFO PING +NIX	3	86601

Rows per page: 15 | < 1 2 3 4 ... 14 >

Hình 50. Check log trên Wazuh

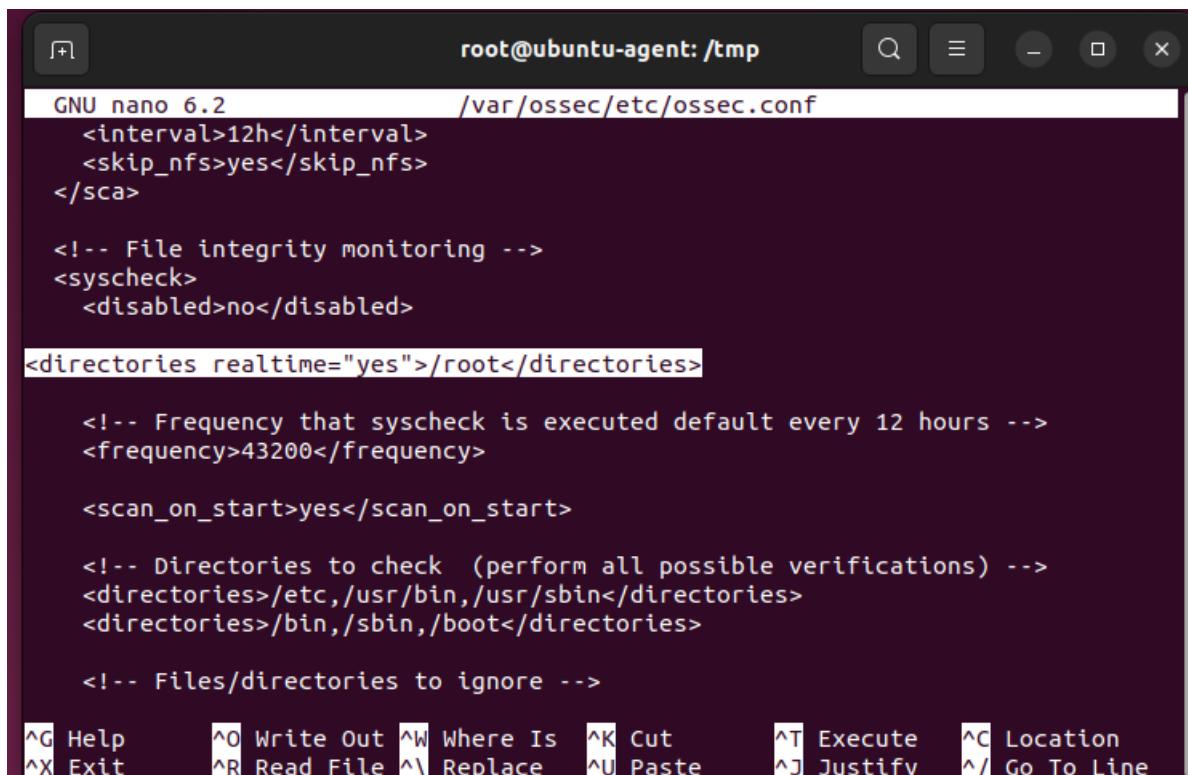
2.2. Phát hiện và loại bỏ phần mềm độc hại bằng cách tích hợp VirusTotal

a. Ubuntu endpoint

Sudo nano /var/ossec/etc/ossec.conf

Thêm một mục trong <syscheck> để cấu hình thư mục được giám sát gần như theo thời gian thực. Trong trường hợp này, bạn đang giám sát thư mục /root:

```
<directories realtime="yes">/root</directories>
```



```
GNU nano 6.2          /var/ossec/etc/ossec.conf
<interval>12h</interval>
<skip_nfs>yes</skip_nfs>
</sca>

<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

<directories realtime="yes">/root</directories>

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

  <scan_on_start>yes</scan_on_start>

  <!-- Directories to check (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>

  <!-- Files/directories to ignore -->
```

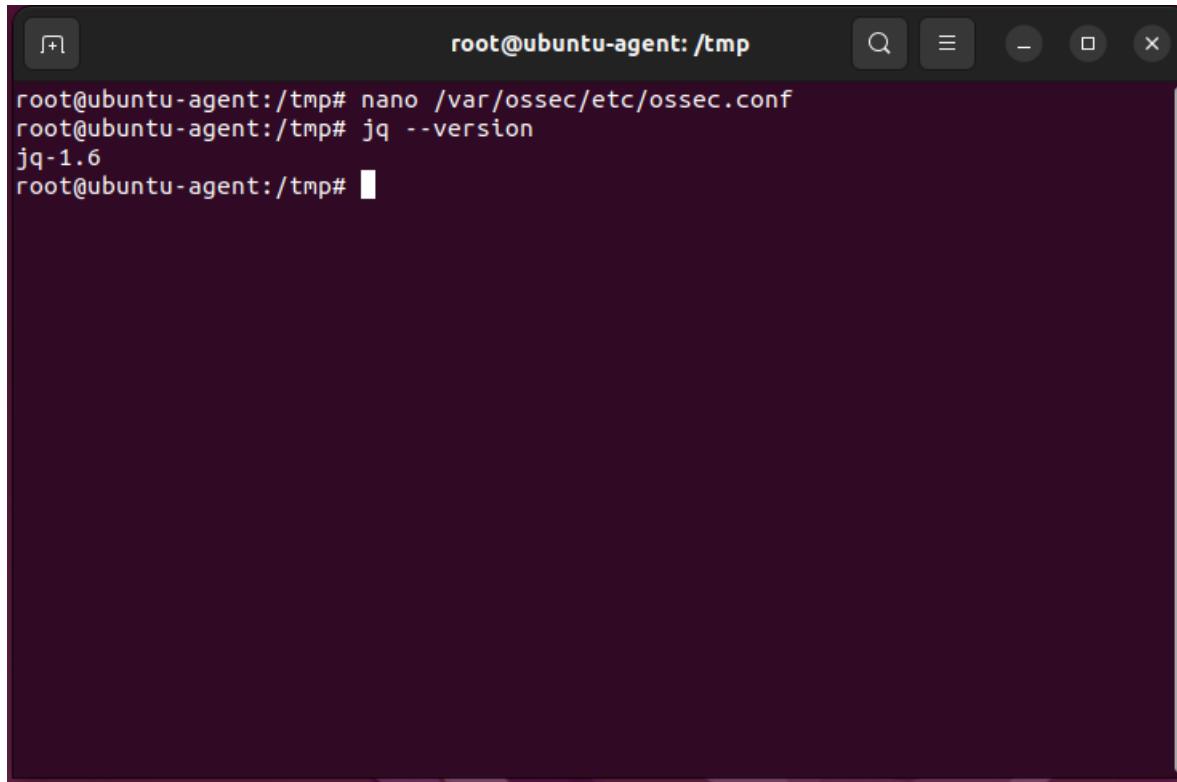
The terminal window shows the command "root@ubuntu-agent: /tmp" at the top. The bottom of the window displays a menu bar with various keyboard shortcuts for nano editor commands.

Hình 51. cấu hình thư mục được giám sát

Cài đặt jq, một tiện ích xử lý dữ liệu đầu vào JSON từ tập lệnh phản hồi đang hoạt động.

```
sudo apt update
```

```
sudo apt -y install jq
```

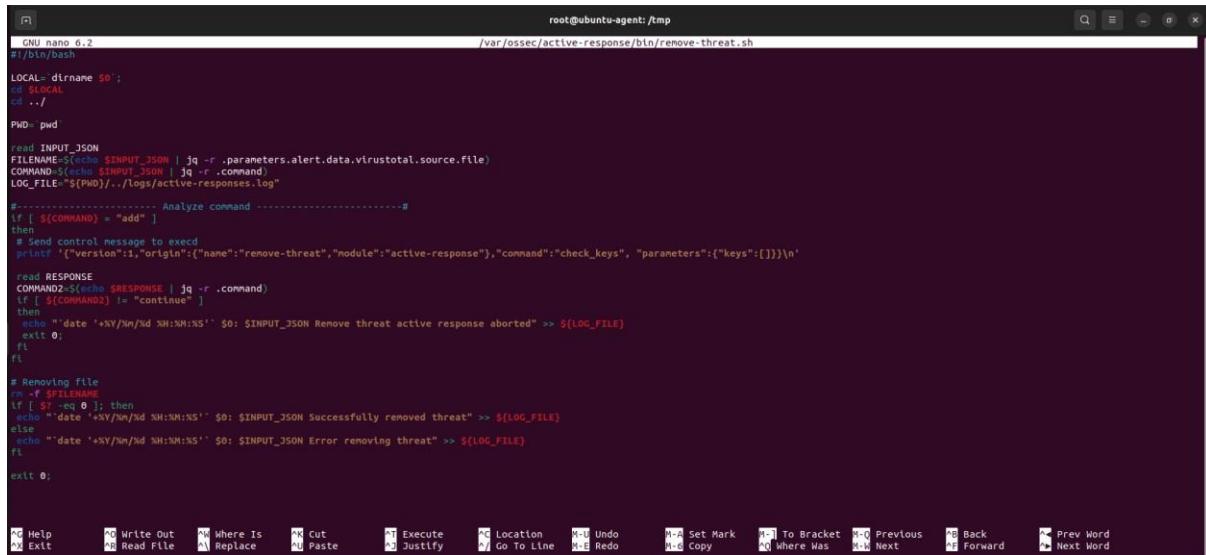


```
root@ubuntu-agent:/tmp# nano /var/ossec/etc/ossec.conf
root@ubuntu-agent:/tmp# jq --version
jq-1.6
root@ubuntu-agent:/tmp#
```

Hình 52. Cài đặt jq

Tạo tập lệnh /var/ossec/active-response/bin/remove-threat.sh để xóa các tệp độc hại khỏi endpoint

Sudo nano /var/ossec/active-response/bin/remove-threat.sh



```
GNU nano 6.2
#!/bin/bash

LOCAL=$(dirname $0);
cd $LOCAL
cd ..
PWD=$(pwd)

read INPUT_JSON
FILENAME=$(echo $INPUT_JSON | jq -r .parameters.alert.data.virustotal.source.file)
COMMAND=$(echo $INPUT_JSON | jq -r .command)
LOG_FILE="${PWD}/../logs/active-responses.log"

#----- Analyze command -----
if [ ${COMMAND} = "add" ]
then
    # Send control message to execd
    printf '{"version":1,"origin":{"name":"remove-threat","module":"active-response"},"command":"check_keys", "parameters":{"keys":[]}}\n'

    read INPUT_RESPONSE
    COMMAND2=$(echo $INPUT_RESPONSE | jq -r .command)
    if [ ${COMMAND2} != "continue" ]
    then
        echo "date '+%Y/%m/%d %H:%M:%S'" $0: $INPUT_JSON Remove threat active response aborted" >> ${LOG_FILE}
        exit 0;
    fi
fi

# Removing File
rm -f $FILENAME
if [ $? -eq 0 ]; then
    echo "date '+%Y/%m/%d %H:%M:%S'" $0: $INPUT_JSON Successfully removed threat" >> ${LOG_FILE}
else
    echo "date '+%Y/%m/%d %H:%M:%S'" $0: $INPUT_JSON Error removing threat" >> ${LOG_FILE}
fi
exit 0;
```

Hình 53. để xóa các tệp độc hại khỏi endpoint

Thay đổi quyền sở hữu và quyền hạn của tệp /var/ossec/active-response/bin/remove-threat.sh

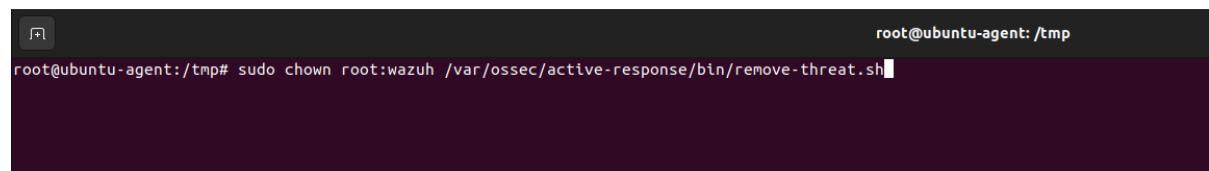
```
sudo chmod 750 /var/ossec/active-response/bin/remove-threat.sh
```

```
sudo chown root:wazuh /var/ossec/active-response/bin/remove-threat.sh
```



```
root@ubuntu-agent:/tmp# sudo chmod 750 /var/ossec/active-response/bin/remove-threat.sh
```

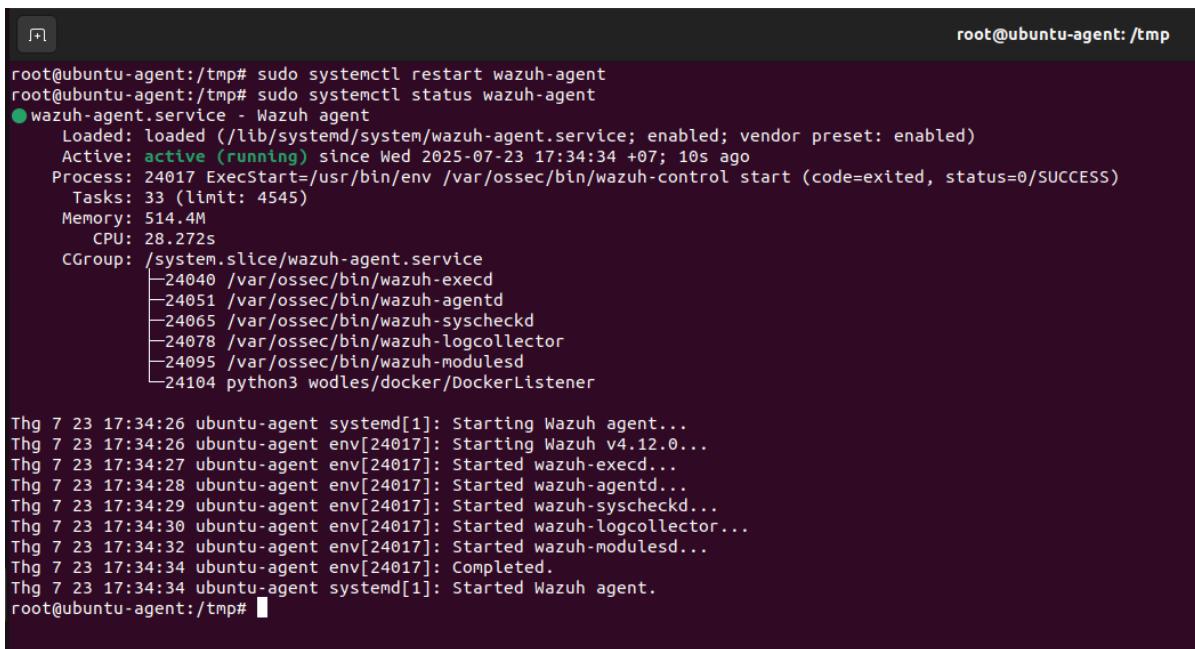
Hình 54. Thay đổi quyền sở hữu và quyền hạn của tệp



```
root@ubuntu-agent:/tmp# sudo chown root:wazuh /var/ossec/active-response/bin/remove-threat.sh
```

Hình 55. Thay đổi quyền sở hữu và quyền hạn của tệp

Khởi động lại Wazuh-agent để áp dụng các thay đổi
sudo systemctl restart wazuh-agent



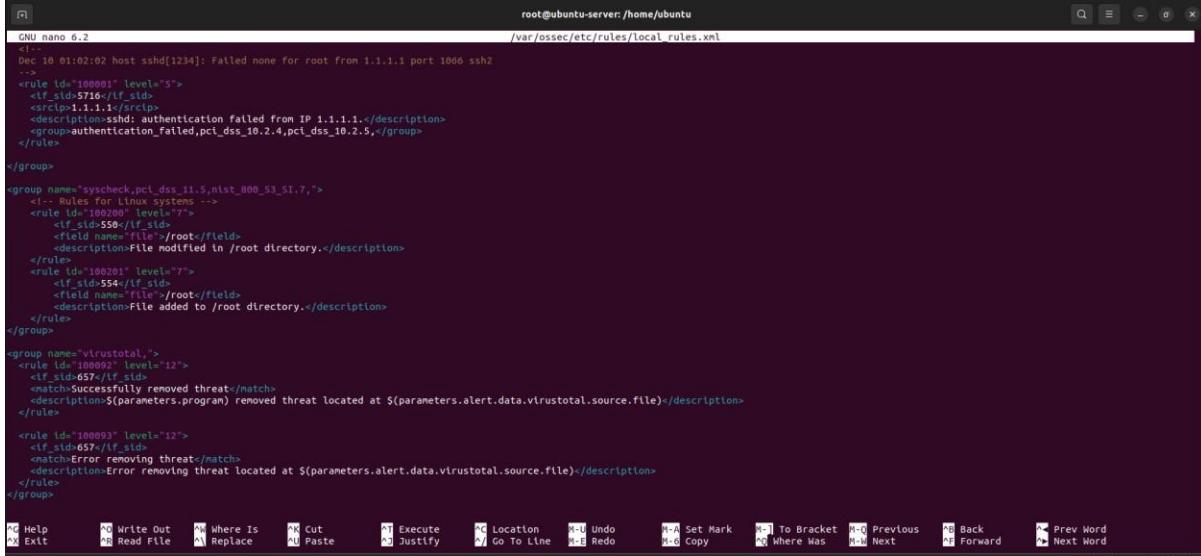
```
root@ubuntu-agent:/tmp# sudo systemctl restart wazuh-agent
root@ubuntu-agent:/tmp# sudo systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
   Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2025-07-23 17:34:34 +07; 10s ago
     Process: 24017 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
       Tasks: 33 (limit: 4545)
      Memory: 514.4M
        CPU: 28.272s
      CGroup: /system.slice/wazuh-agent.service
              ├─24040 /var/ossec/bin/wazuh-execd
              ├─24051 /var/ossec/bin/wazuh-agentd
              ├─24065 /var/ossec/bin/wazuh-syscheckd
              ├─24078 /var/ossec/bin/wazuh-logcollector
              ├─24095 /var/ossec/bin/wazuh-modulesd
              └─24104 python3 wodles/docker/DockerListener

Thg 7 23 17:34:26 ubuntu-agent systemd[1]: Starting Wazuh agent...
Thg 7 23 17:34:26 ubuntu-agent env[24017]: Starting Wazuh v4.12.0...
Thg 7 23 17:34:27 ubuntu-agent env[24017]: Started wazuh-execd...
Thg 7 23 17:34:28 ubuntu-agent env[24017]: Started wazuh-agentd...
Thg 7 23 17:34:29 ubuntu-agent env[24017]: Started wazuh-syscheckd...
Thg 7 23 17:34:30 ubuntu-agent env[24017]: Started wazuh-logcollector...
Thg 7 23 17:34:32 ubuntu-agent env[24017]: Started wazuh-modulesd...
Thg 7 23 17:34:34 ubuntu-agent env[24017]: Completed.
Thg 7 23 17:34:34 ubuntu-agent systemd[1]: Started Wazuh agent.
root@ubuntu-agent:/tmp#
```

Hình 56. Khởi động lại Wazuh-agent để áp dụng các thay đổi

b. Phát hiện tấn công Cài mã độc

Thêm các quy tắc sau vào /var/ossec/etc/rules/local_rules.xml

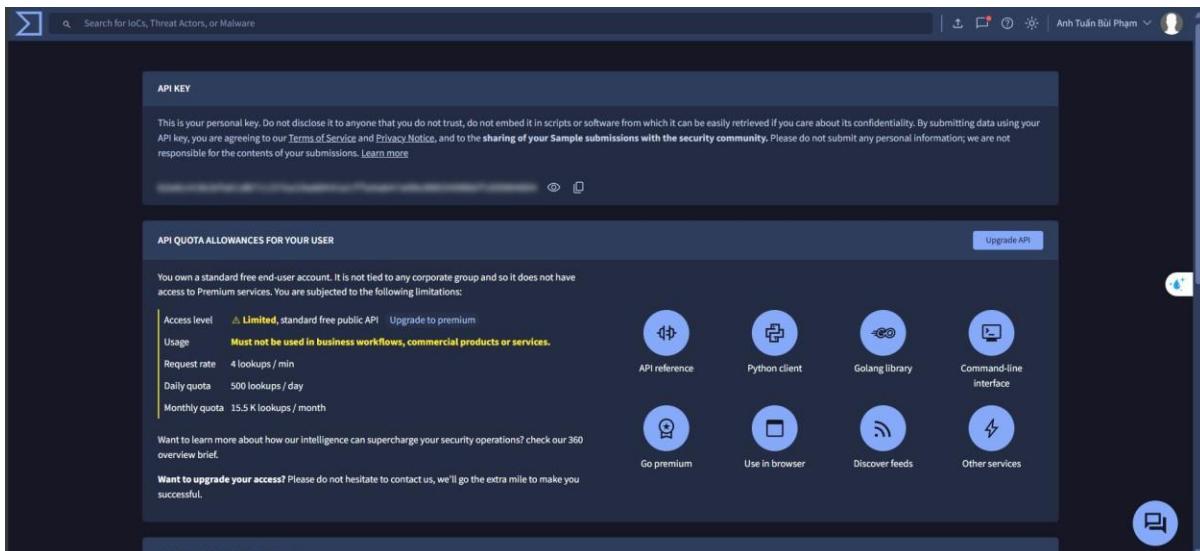


```
GNU nano 6.2                                     /var/ossec/etc/rules/local_rules.xml
<!--
Dec 10 01:02:02 host sshd[1234]: Failed none for root From 1.1.1.1 port 1066 ssh2
-->
<rule id="510001" level="5">
<if_sid>5716</if_sid>
<rclip>1.1.1.1</rclip>
<description>sshd: authentication failed from IP 1.1.1.1.</description>
<group>authentication_failed,pct_dss_10.2.4,pct_dss_10.2.5,</group>
</rule>
</group>
<group name="syscheck,pct_dss_11.5,nist_800_53_S1.7,">
<!-- Rules for Linux systems -->
<rule id="100009" level="7">
<if_sid>550</if_sid>
<field name="file">/root</field>
<description>File modified in /root directory.</description>
</rule>
<rule id="100001" level="7">
<if_sid>554</if_sid>
<field name="file">/root</field>
<description>File added to /root directory.</description>
</rule>
</group>
<group name="virustotal,">
<rule id="510002" level="12">
<if_sid>657</if_sid>
<match>Successfully removed threat</match>
<description>$parameters.program removed threat located at $parameters.alert.data.virustotal.source.file</description>
</rule>
<rule id="510003" level="12">
<if_sid>657</if_sid>
<match>Error removing threat</match>
<description>Error removing threat located at $parameters.alert.data.virustotal.source.file</description>
</rule>
</group>

```

Hình 57. Thêm các quy tắc

Đăng nhập VirusTotal lấy API KEY



Hình 58. Đăng nhập VirusTotal lấy API KEY

Thêm các khối sau vào tệp /var/ossec/etc/ossec.conf của Wazuh Server. Thao tác này sẽ kích hoạt Phản hồi Chủ động và kích hoạt tập lệnh remove-threat.sh khi VirusTotal đánh dấu một tệp là độc hại, kích hoạt tích hợp Virustotal:

```

GNU nano 6.2
<location>/var/log/dpkg.log</location>
</localfile>
</ossec_config>
<ossec_config>
<command>
<name>remove-threat</name>
<executable>remove-threat.sh</executable>
<timeout_allowed>no</timeout_allowed>
</command>
<active-response>
<disabled>no</disabled>
<command>remove-threat</command>
<location>/local</location>
<rule_id>#10105</rule_id>
</active-response>
</ossec_config>
<ossec_config>
<integration>
<name>virustotal</name>
<api_key>b2edc410cbfe61d8711375a19add441e1ffa4ab47a98c0893490b6f169904894</api_key> <!-- Replace with your VirusTotal API key -->
<rule_id>100200,100201</rule_id>
<alert_format>json</alert_format>
</integration>
</ossec_config>

```

Hình 59. Kích hoạt Phản hồi Chủ động và kích hoạt tập lệnh remove-threat.sh

Khởi động lại Wazuh-manager

```

root@ubuntu-server:/home/ubuntu# sudo systemctl restart wazuh-manager
root@ubuntu-server:/home/ubuntu# sudo systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2025-07-23 16:26:15 +07; 10s ago
     Process: 78224 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
       Tasks: 154 (limit: 4545)
      Memory: 584.8M
        CPU: 33.864s
      CGroup: /system.slice/wazuh-manager.service
              ├─78286 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
              ├─78287 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
              ├─78288 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
              ├─78291 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
              ├─78294 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
              ├─78317 /var/ossec/bin/wazuh-integratord
              ├─78339 /var/ossec/bin/wazuh-authd
              ├─78355 /var/ossec/bin/wazuh-db
              ├─78380 /var/ossec/bin/wazuh-execd
              ├─78394 /var/ossec/bin/wazuh-analysisd
              ├─78411 /var/ossec/bin/wazuh-syscheckd
              ├─78430 /var/ossec/bin/wazuh-remoted
              ├─78464 /var/ossec/bin/wazuh-logcollector
              ├─78483 /var/ossec/bin/wazuh-monitord
              ├─78492 /var/ossec/bin/wazuh-modulesd

```

Hình 60. Khởi động lại Wazuh-manager

Mô phỏng tấn công

sudo curl -Lo /root/eicar.com https://secure.eicar.org/eicar.com && sudo ls -lah /root/eicar.com

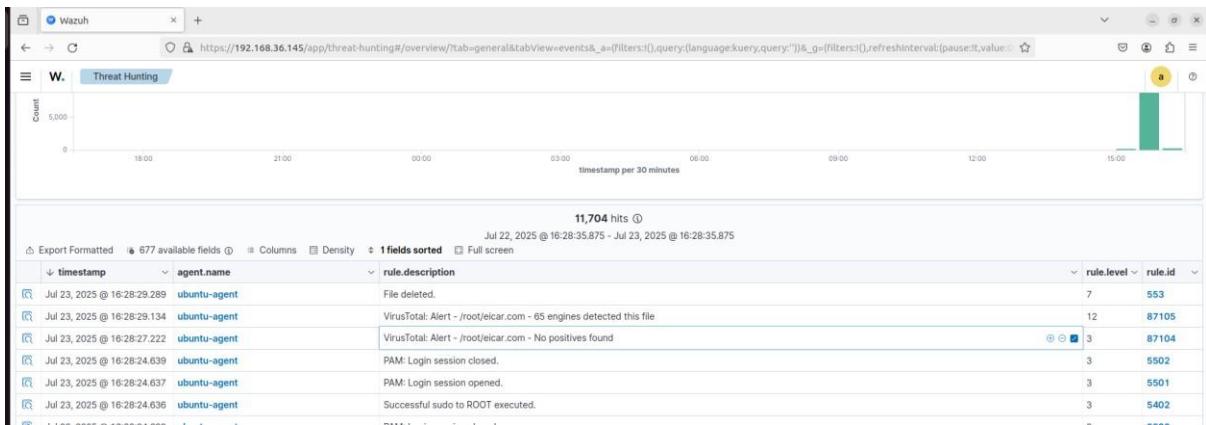
```

root@ubuntu-agent:/tmp# sudo curl -Lo /root/eicar.com https://secure.eicar.org/eicar.com && sudo ls -lah /root/eicar.com
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload  Upload   Total Spent   Left  Speed
100  68  100  68    0     0      66      0  0:00:01  0:00:01 --:--:--   66
-rw-r--r-- 1 root root 68 Thg 7 23 16:30 /root/eicar.com
root@ubuntu-agent:/tmp#

```

Hình 61. Mô phỏng tấn công

Check log trên Wazuh



Hình 62. Check log trên Wazuh

c. Phát hiện tấn công SQL Injection

Cập nhật các gói cục bộ và cài đặt máy chủ web Apache:

sudo apt update

sudo apt install apache2

```

root@ubuntu-agent:/tmp#
Selecting previously unselected package apache2.
Preparing to unpack .../apache2_2.4.52-1ubuntu0.22.04.15_amd64.deb ...
Unpacking apache2 (2.4.52-1ubuntu0.22.04.15) ...
Setting up libapr1:amd64 (1.7.0-8ubuntu0.22.04.2) ...
Setting up libaprutil1:amd64 (1.6.1-Subuntu0.22.04.2) ...
Setting up libaprutil1-dbd-pgsql (1.6.1-Subuntu0.22.04.2) ...
Setting up libaprutil1-ldap (1.6.1-Subuntu0.22.04.2) ...
Setting up libcurl3:amd64 (1.36.1-Subuntu0.22.04.2) ...
Setting up apache2-utils (2.4.52-1ubuntu0.15) ...
Setting up apache2-bin (2.4.52-1ubuntu0.15) ...
Setting up apache2 (2.4.52-1ubuntu0.15) ...
Enabling module mpm_event.
Enabling module authn_core.
Enabling module authn_file.
Enabling module authz_host.
Enabling module authn_core.
Enabling module authn_file.
Enabling module authz_user.
Enabling module authn_core.
Enabling module dir.
Enabling module autoindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module envif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling module headers.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Creating symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
Processing triggers for ufw (0.36.1-0ubuntu0.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.10) ...
root@ubuntu-agent:/tmp# 
```

Hình 63. Cập nhật các gói cục bộ và cài đặt máy chủ web Apache

Kiểm tra trạng thái của dịch vụ Apache để xác minh rằng web server đang chạy
sudo systemctl status apache2

```

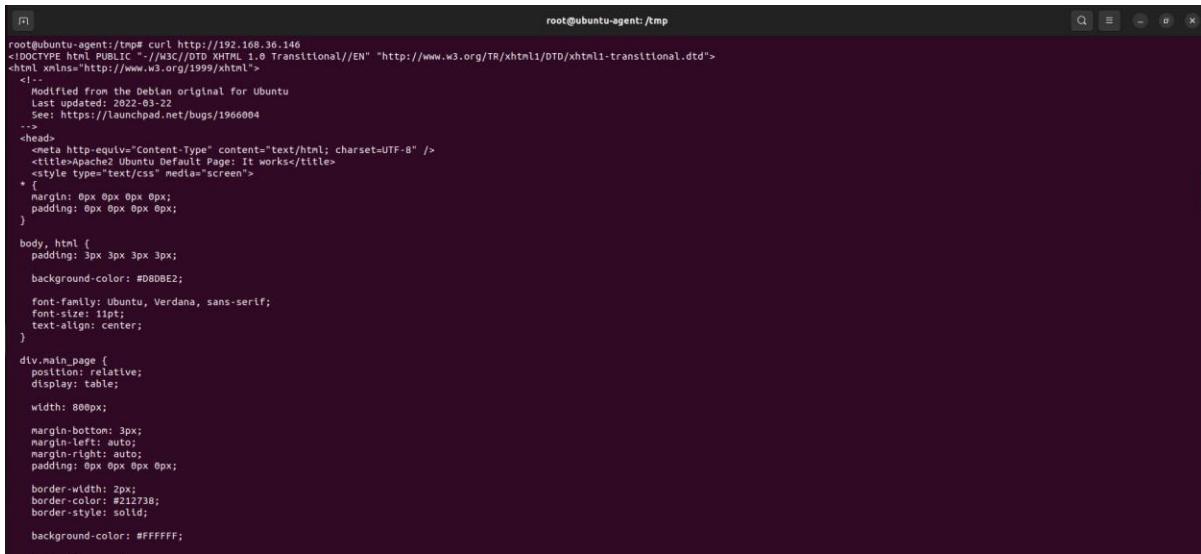
root@ubuntu-agent:/tmp# sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2025-07-23 17:44:54 +07; 1min 21s ago
     Docs: https://httpd.apache.org/docs/2.4/
 Main PID: 26778 (apache2)
   Tasks: 55 (limit: 4545)
   Memory: 155M
      CPU: 155ms
     CGroup: /system.slice/apache2.service
             └─26778 /usr/sbin/apache2 -k start
                  ├─26780 /usr/sbin/apache2 -k start
                  ├─26781 /usr/sbin/apache2 -k start
                  └─26781 /usr/sbin/apache2 -k start

Thg 7 23 17:44:54 ubuntu-agent[1]: Starting The Apache HTTP Server...
Thg 7 23 17:44:54 ubuntu-agent apachectl[26777]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to support
Thg 7 23 17:44:54 ubuntu-agent systemd[1]: Started The Apache HTTP Server.
lines 1-16 (END) 
```

Hình 64. Kiểm tra trạng thái của dịch vụ Apache

Sử dụng lệnh curl hoặc mở http://<UBUNTU_IP> trong trình duyệt để xem trang đích Apache và xác minh cài đặt

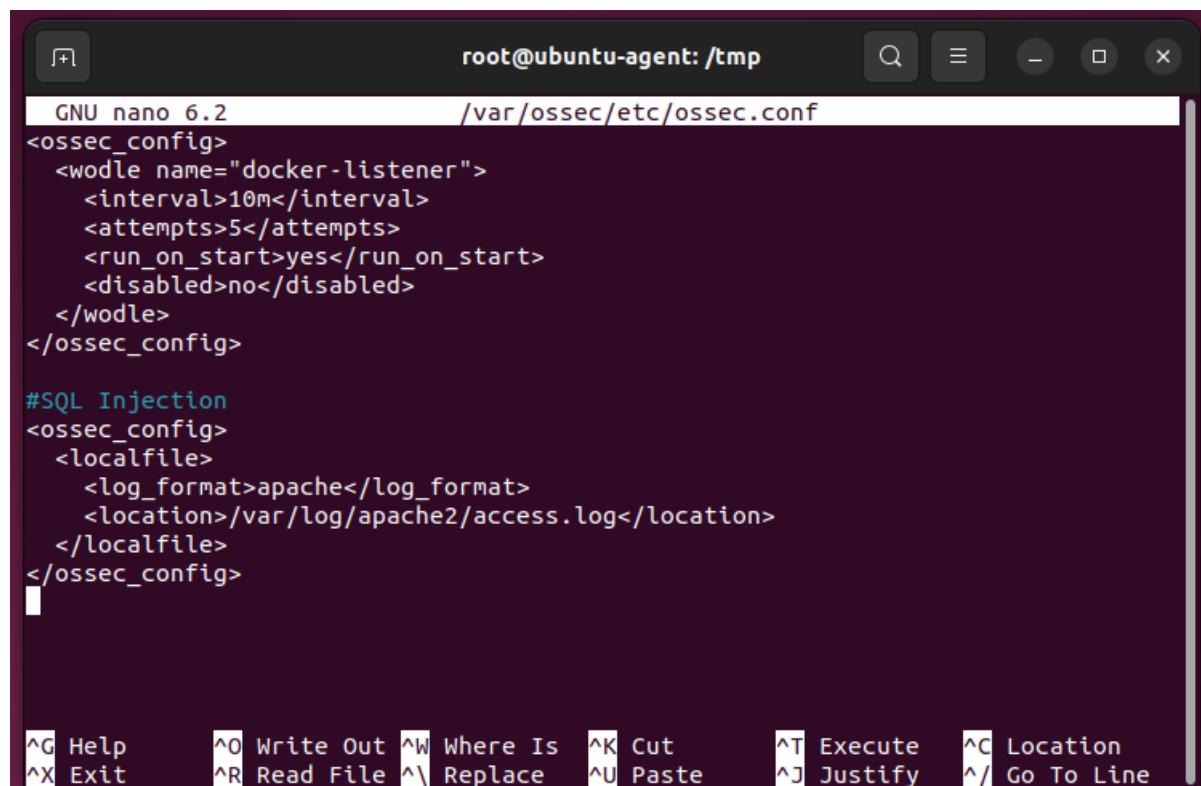
curl http://192.168.36.146



```
root@ubuntu-agent:/tmp# curl -v http://192.168.36.146
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<!--
    Modified from the Debian original for Ubuntu
    Last updated: 2022-03-22
    See: https://launchpad.net/bugs/1966004
-->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Ubuntu Default Page: It works</title>
<style type="text/css" media="screen">
<{
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
}
body, html {
    padding: 3px 3px 3px 3px;
    background-color: #D9E1F2;
    font-family: ubuntu, Verdana, sans-serif;
    font-size: 1em;
    text-align: center;
}
div.main_page {
    position: relative;
    display: table;
    width: 800px;
    margin-bottom: 3px;
    margin-left: auto;
    margin-right: auto;
    padding: 0px 0px 0px 0px;
    border-width: 2px;
    border-color: #21273B;
    border-style: solid;
    background-color: #FFFFFF;
}
```

Hình 65. Check trang đích Apache và xác minh cài đặt

Thêm các dòng sau vào tệp /var/ossec/etc/ossec.conf của Wazuh agent. Điều này cho phép Wazuh agent theo dõi nhật ký truy cập của máy chủ Apache của bạn.



```
GNU nano 6.2                               /var/ossec/etc/ossec.conf
<ossec_config>
  <wodle name="docker-listener">
    <interval>10m</interval>
    <attempts>5</attempts>
    <run_on_start>yes</run_on_start>
    <disabled>no</disabled>
  </wodle>
</ossec_config>

#SQL Injection
<ossec_config>
  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>
</ossec_config>
```

Hình 66. Wazuh agent theo dõi nhật ký truy cập của máy chủ Apache

Khởi động lại Wazuh-agent để áp dụng các thay đổi cấu hình:
sudo systemctl restart wazuh-agent

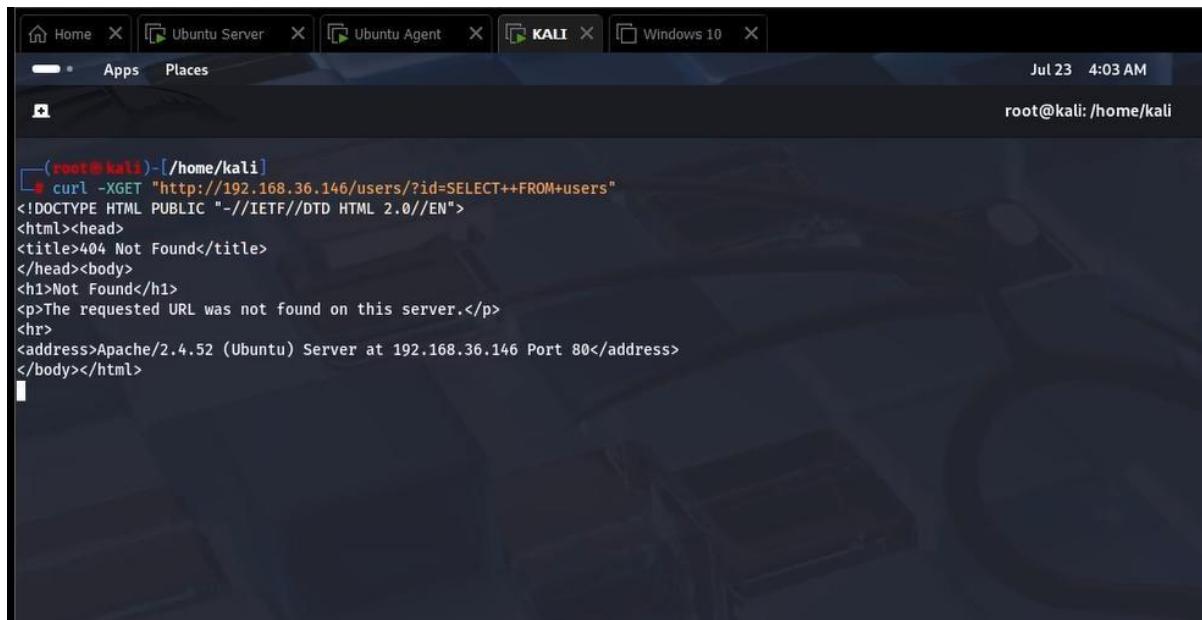
```
root@ubuntu-agent:/tmp# sudo systemctl restart wazuh-agent
root@ubuntu-agent:/tmp# sudo systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
   Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2023-07-23 17:50:43 +07; 12s ago
     Process: 27644 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
       Tasks: 36 (limit: 4545)
      Memory: 729.8M
        CPU: 24.643s
      CGroup: /system.slice/wazuh-agent.service
              ├─27667 /var/ossec/bin/wazuh-execd
              ├─27678 /var/ossec/bin/wazuh-agentd
              ├─27691 /var/ossec/bin/wazuh-syscheckd
              ├─27705 /var/ossec/bin/wazuh-logcollector
              ├─27722 /var/ossec/bin/wazuh-modulesd
              └─27733 python3 wodles/docker/DockerListener

Thg 7 23 17:50:35 ubuntu-agent systemd[1]: Starting Wazuh agent...
Thg 7 23 17:50:35 ubuntu-agent env[27644]: Starting Wazuh v4.12.0...
Thg 7 23 17:50:36 ubuntu-agent env[27644]: Started wazuh-execd...
Thg 7 23 17:50:38 ubuntu-agent env[27644]: Started wazuh-agentd...
Thg 7 23 17:50:39 ubuntu-agent env[27644]: Started wazuh-syscheckd...
Thg 7 23 17:50:40 ubuntu-agent env[27644]: Started wazuh-logcollector...
Thg 7 23 17:50:41 ubuntu-agent env[27644]: Started wazuh-modulesd...
Thg 7 23 17:50:43 ubuntu-agent env[27644]: Completed.
Thg 7 23 17:50:43 ubuntu-agent systemd[1]: Started Wazuh agent.
root@ubuntu-agent:/tmp#
```

Hình 67. Khởi động lại Wazuh-agent để áp dụng các thay đổi cấu hình

Mô phỏng tấn công

```
curl -XGET "http://192.168.36.146/users/?id=SELECT++*+FROM+users";
```



Hình 68. Mô phỏng tấn công

The screenshot shows the Wazuh Threat Hunting interface in a Firefox browser. The URL is [https://192.168.36.145/app/threat-hunting#/overview/tab=general&tabView=events_a_=\({filters:\[\]},query:\(language:kuery,query:''\)\)&_g=\({filters:\[\],refreshInterval:\(pause:0,value:0\)}\)](https://192.168.36.145/app/threat-hunting#/overview/tab=general&tabView=events_a_=({filters:[]},query:(language:kuery,query:''))&_g=({filters:[],refreshInterval:(pause:0,value:0)})). The left sidebar has a 'Threat Hunting' tab selected. The main area displays a table of log entries. One specific log entry is highlighted in the table:

Document Details	
# decoder.name	web-accesslog
# full.log	192.168.36.131 - [23/Jul/2025:15:03:54 +0700] "GET /users/?id=SELECT+*+FROM+users+HTTP/1.1" 404 437 "-" "curl/8.12.1"
# id	1752287834.777218
# input.type	log
# location	/var/log/apache2/access.log
# manager.name	ubuntu-server
# rule.description	SQL injection attempt.
# rule.firedtimes	1
# rule.gidr	IV_05.7.d
# rule.groups	web, accesslog, attack, sql_injection
# rule.id	31103
# rule.level	7
# rule.mail	false
# rule.mitre.id	T1198
# rule.mitre.tactic	Initial Access
# rule.mitre.technique	Exploit Public-Facing Application
# rule.nist_800_53	SA.11, SI.4
# rule.pci_dss	6.5, 11.4, 6.5.1
# rule.tsc	CC6.6, CC7.1, CC8.1, CC9.8, CC7.2, CC7.3
# timestamp	Jul 23, 2025 0 15:03:54.783

Hình 69. Mô phỏng tấn công

d. Phát hiện tấn công ShellShock

Thêm các dòng sau vào tệp /var/ossec/etc/ossec.conf của Wazuh agent. Điều này cho phép Wazuh agent theo dõi nhật ký truy cập của máy chủ Apache của bạn.

```

root@ubuntu-agent: /tmp
GNU nano 6.2
</ossec_config>

#SQL Injection
<ossec_config>
  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>
</ossec_config>

#ShellShock
<ossec_config>
  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>
</ossec_config>

Save modified buffer?
Y Yes
N No
^C Cancel

```

Hình 70. Phát hiện tấn công ShellShock

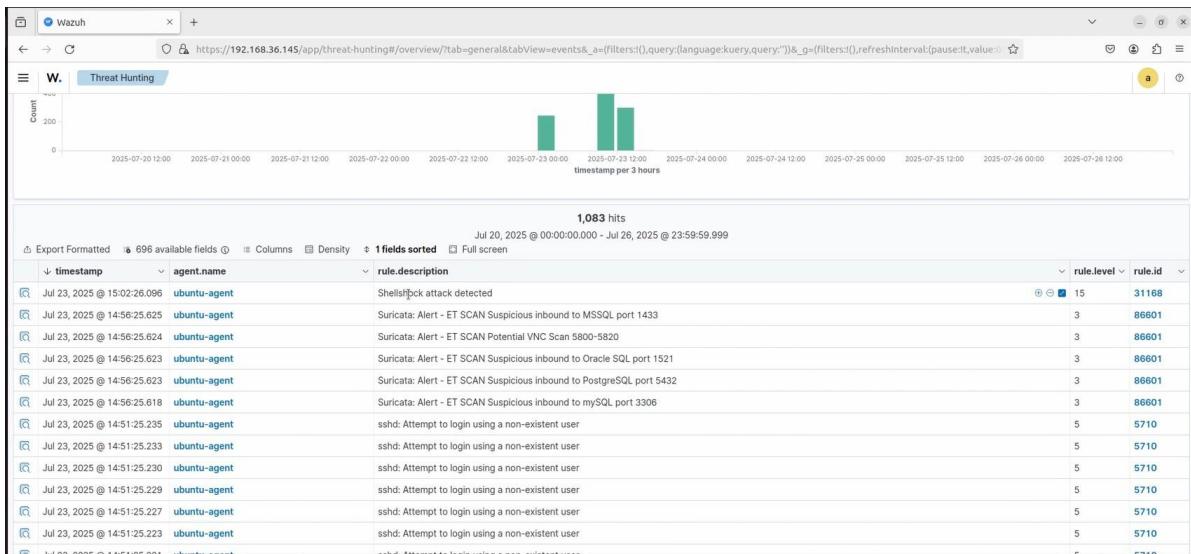
Mô phỏng tấn công



```
(root@kali)-[~/home/kali]
# sudo curl -H "User-Agent: () { :; }; /bin/cat /etc/passwd" 192.168.36.146|
```

Hình 71. Mô phỏng tấn công

Hiển thị log cảnh báo trên wazuh



Hình 72. Mô phỏng tấn công

The screenshot shows the Wazuh Threat Hunting interface. On the left, a timeline displays event counts over time, with a specific event selected on July 20, 2025, at 00:00:00.000. The event details are shown on the right, including:

Document Details

Table	JSON
t _index	wazuh-alerts-4.x-2025.07.23
t agent.id	001
t agent.ip	192.168.36.146
t agent.name	ubuntu-agent
t data.id	200
t data.protocol	GET
t data.scpip	192.168.36.131
t data.url	/
t decoder.name	web-accesslog
t full_log	192.168.36.131 - - [29/Jul/2025:15:02:25 +0700] "GET / HTTP/1.1" 200 10926 "-" "() { :; }; /bin/cat /etc/passwd"
t id	175257746.776806
t input.type	log
t location	/var/log/apache2/access.log
t manager.name	ubuntu-server
t rule.description	Shellshock attack detected
# rule.firetimes	1
t rule.gdpr	IV_35.7.d
t rule.groups	web, accesslog, attack

Hình 73. Mô phỏng tấn công

KẾT LUẬN

Trong thời kỳ mà công nghệ thông tin phát triển mạnh mẽ và len lỏi vào mọi lĩnh vực của đời sống, vấn đề bảo mật thông tin, đặc biệt là đối với người dùng cuối, trở thành mối quan tâm hàng đầu. Người dùng cuối không chỉ là mục tiêu tấn công của tin tặc mà còn là mắt xích yếu nhất trong chuỗi an toàn thông tin. Do đó, việc nâng cao nhận thức, trang bị kiến thức và áp dụng các giải pháp bảo vệ phù hợp là điều hết sức cần thiết.

Qua quá trình tìm hiểu lý thuyết và thực hành triển khai hệ thống giám sát bảo mật với Wazuh và Suricata, nhóm đã có cái nhìn sâu sắc hơn về các loại mối đe dọa thực tế như tấn công mạng, mã độc, lỗ hổng hệ thống, cũng như các kỹ thuật phòng thủ và phát hiện xâm nhập hiệu quả. Việc cấu hình hệ thống cảnh báo, giám sát hoạt động và phản hồi chủ động giúp chúng ta hiểu rõ hơn về cách vận hành của một hệ thống bảo mật hiện đại trong doanh nghiệp.

Đặc biệt, bài thực nghiệm không chỉ cung cấp kiến thức lý thuyết mà còn giúp nhóm rèn luyện kỹ năng làm việc nhóm, phân công công việc và giải quyết vấn đề kỹ thuật trong môi trường mô phỏng thực tế. Đây là trải nghiệm quý báu, chuẩn bị hành trang vững chắc cho sinh viên trong quá trình học tập và làm việc sau này trong lĩnh vực An toàn thông tin.

TÀI LIỆU THAM KHẢO

1. CompTIA Security+ SY0-601 Official Study Guide – CompTIA.
2. <https://documentation.wazuh.com>
3. <https://suricata.io>
4. OWASP Top 10 – <https://owasp.org>
5. Sách "An toàn thông tin mạng" – NXB Thông Tin & Truyền Thông.
6. Các bài viết từ VietNamCERT, Cục An toàn thông tin – <https://ais.gov.vn>