

Bộ Giáo Dục Và Đào Tạo
Trường Đại Học Ngoại Ngữ - Tin Học Thành Phố Hồ Chí Minh
Khoa Công Nghệ Thông Tin



**BÁO CÁO MÔN BẢO MẬT NGƯỜI DÙNG CUỐI
ĐỀ TÀI: XÂY DỰNG HỆ THỐNG BẢO MẬT ENDPOINT**
Giáo Viên Hướng Dẫn : Đỗ Phi Hưng

Phụ trách thực hiện :

Trần Quang Khải – 22DH114583
Vương Hồng Ngọc – 22DH112426

TP. Hồ Chí Minh, ngày 07 tháng 07 năm 2025

LỜI MỞ ĐẦU

Trong thời đại công nghệ số phát triển vượt bậc, thông tin và dữ liệu cá nhân trở thành những tài sản quý giá nhưng cũng đồng thời là mục tiêu hấp dẫn cho các cuộc tấn công mạng. Việc bảo vệ an toàn thông tin cá nhân và dữ liệu của người dùng cuối không chỉ là trách nhiệm của các tổ chức và doanh nghiệp mà còn là yêu cầu bức thiết đối với mỗi cá nhân trong xã hội.

Đề tài "Xây dựng hệ thống bảo mật người dùng cuối" nhằm mục đích nghiên cứu, phân tích và phát triển các biện pháp bảo mật hiệu quả để bảo vệ thông tin người dùng trước những nguy cơ tấn công ngày càng tinh vi và đa dạng. Hệ thống bảo mật không chỉ dừng lại ở việc ngăn chặn các cuộc tấn công từ bên ngoài mà còn bao gồm các biện pháp phát hiện, ứng phó và khắc phục hậu quả khi sự cố xảy ra.

Thông qua đề tài này, chúng tôi hy vọng sẽ mang đến những giải pháp tiên tiến và toàn diện, góp phần nâng cao nhận thức về an ninh mạng cũng như khả năng tự bảo vệ của người dùng cuối trong môi trường số. Đồng thời, nghiên cứu này cũng sẽ đưa ra những khuyến nghị thực tiễn giúp các tổ chức và doanh nghiệp xây dựng được hệ thống bảo mật mạnh mẽ và hiệu quả hơn.

Chúng tôi tin tưởng rằng, với sự kết hợp giữa kiến thức lý thuyết và ứng dụng thực tiễn, đề tài này sẽ đóng góp tích cực vào việc nâng cao mức độ an toàn thông tin, tạo ra một môi trường mạng an toàn và tin cậy cho mọi người.

LỜI CẢM ƠN

Kính gửi thầy Đỗ Phi Hưng

Đồ án này không thể hoàn thành nếu không có sự hướng dẫn tận tâm và sự hỗ trợ quý báu của thầy. Chúng em xin bày tỏ lòng biết ơn sâu sắc đến thầy vì đã luôn đồng hành, chỉ bảo và truyền cảm hứng cho chúng em trong suốt quá trình thực hiện đồ án.

Thầy không chỉ là người thầy tận tụy, mà còn là người bạn đồng hành đáng quý, luôn sẵn sàng lắng nghe, chia sẻ và giải đáp mọi thắc mắc của chúng em. Những lời khuyên, góp ý của thầy đã giúp chúng em vượt qua những khó khăn, hoàn thiện kiến thức và kỹ năng, từ đó đạt được kết quả tốt nhất trong đồ án này.

Chúng em xin trân trọng gửi lời cảm ơn chân thành nhất đến thầy Hưng. Hy vọng rằng trong tương lai, chúng em sẽ có thêm nhiều cơ hội được học hỏi và làm việc cùng thầy.

MỤC LỤC

I/ Giới thiệu đề tài	8
a/ Tổng quan về bảo mật EndPoint.....	8
a.1 Khái niệm.....	8
a.2 Tầm quan trọng	8
a.3 Các thành phần chính	8
b/ Mục tiêu của đề tài	8
b.1 Mục tiêu tổng quát	8
b.2 Mục tiêu cụ thể.....	8
II/ Cơ sở lý thuyết	10
a/EndPoint (Người Dùng Cuối).....	10
a.1 Khái niệm EndPoint	10
a.2 Vai trò của Endpoint trong hệ thống mạng	10
a.3 Mối đe dọa đối vs EndPoint.....	10
a.4 Khái niệm bảo mật EndPoint	10
b/ IDS/IPS	11
b.1 Khái niệm	11
b.2 Vai trò của IDS/IPD	11
b.3 Các giải pháp IDS/IPS.....	11
b.4 Giải pháp triển khai trong đề tài: Sử dụng Suricata trong pfSense	14
c/ System Endpoint	15
c.1 Khái niệm System Endpoint	15
c.2 Vai trò của System Endpoint	15
c.3 Các giải pháp System Endpoint	16
c.4 Giải pháp triển khai trong đề tài: Sử dụng Wazuh	19
III/ Triển khai các rules và demo tấn công	21
a/ Sơ đồ triển khai.....	21
b/ Cài đặt và triển khai.....	22
b.1 IDS/IPS.....	22
b.2 Winserver (Domain Server).....	25
b.3/ System Endpoint (Wazuh).....	26

c/ IDS/IPS Rule	28
c.1 SSH Brute Force.....	28
c.2 DDos.....	34
d/ Endpoint rule	37
d.1 Detecting and removing malware using VirusTotal integration.....	37
d.2 Detecting unauthorized processes	42
e/ Kịch bản tấn công	44
e.1 Tấn công DDOS	44
e.2 Tấn công gửi malware qua email	47
e.3 Tấn công Brute-Force SSH.....	51
f/ Tổng kết	54

DANH MỤC HÌNH ẢNH

Hình 1 Logo Snort.....	11
Hình 2 Logo Suricata	12
Hình 3 Logo Zeek	13
Hình 4 Logo pfSense.....	14
Hình 5 Logo Wazuh	16
Hình 6 Logo Ossec.....	17
Hình 7 Logo Security Onion	18
Hình 8 Sơ đồ vật lý	21
Hình 9 Sơ đồ logic	22
Hình 10 Cấu hình ip pfSense	23
Hình 11 Giao diện web của pfSense	23
Hình 12 Package manager	24
Hình 13 Service Suricata	24
Hình 14 Thêm interface Wan	29
Hình 15 Tab Wan Rules	29
Hình 16 Interface Wan đang off	30
Hình 17 Interface Wan đã bật	31
Hình 18 Lệnh tấn công brute-force ssh	31
Hình 19 Brute-force	32
Hình 20 Alert Suricata.....	33
Hình 21 Blocks tab.....	33
Hình 22 Kali attacker	34
Hình 23 DDos rule	34
Hình 24 Alert Ddos	36
Hình 25 Blocks tab.....	36
Hình 26 Deploy new agent trên Wazuh	37
Hình 27 PowerShell win10.....	37
Hình 28 Wazuh server.....	38
Hình 29 ossec.conf.....	38
Hình 30 Thư mục lưu remove-threat.exe	39
Hình 31 ossec.conf.....	39
Hình 32 ossec.conf.....	40
Hình 33 local_rules.xml	40
Hình 34 Threat Hunting	41
Hình 35 win10	41
Hình 36 Threat Hunting Virustotal	42
Hình 37 Download	42
Hình 38 ossec.conf.....	43
Hình 39 local_rules.xml	43
Hình 40 Ubuntu Agent	44
Hình 41 Threat Hunting	44

Hình 42 cmd kali.....	45
Hình 43 cmd Ubuntu	45
Hình 44 Alert suricata	46
Hình 45 Blocks tab.....	46
Hình 46 Mail.....	47
Hình 47 Tải malware.....	48
Hình 48 DownLoad.....	48
Hình 49 Cảnh báo	49
Hình 50 Chi tiết cảnh báo	49
Hình 51 Kết quả trên Virustotal.....	50
Hình 52 Threat Hunting	50
Hình 53 DownLoad empty	51
Hình 54 ssh brute force	51
Hình 55 Chi tiết tấn công	52
Hình 56 Alert	52
Hình 57 Blocks	53
Hình 58 CMD kali.....	53

I/ Giới thiệu đề tài

a/ Tổng quan về bảo mật Endpoint

a.1 Khái niệm

- **Endpoint:** Là các thiết bị đầu cuối kết nối vào hệ thống mạng (PC, laptop, điện thoại, máy in, thiết bị IoT...).
- **Bảo mật Endpoint:** Là việc bảo vệ các thiết bị đầu cuối khỏi phần mềm độc hại, tấn công mạng, truy cập trái phép...

a.2 Tầm quan trọng

- **Endpoint** là điểm yếu dễ bị tấn công nhất trong hệ thống.
- Là mục tiêu đầu tiên trong nhiều cuộc tấn công mạng như ransomware, phishing...
- Một endpoint bị xâm nhập có thể dẫn đến:
 - Rò rỉ dữ liệu.
 - Mất kiểm soát hệ thống.
 - Lây lan mã độc nội bộ.
- An toàn Endpoint giúp bảo vệ cả hệ thống và dữ liệu người dùng.

a.3 Các thành phần chính

- **Chống virus (Antivirus/Antimalware):** Phát hiện và ngăn chặn phần mềm độc hại, virus, trojan...
- **Tường lửa cá nhân (Firewall):** Kiểm soát dữ liệu ra vào thiết bị, ngăn chặn kết nối lạ.
- **Giám sát và phản ứng (EDR):** Theo dõi hoạt động trên thiết bị, phát hiện hành vi lạ và phản ứng kịp thời.
- **Cập nhật bảo mật (Patch Management):** Tự động cài đặt bản vá để vá lỗ hổng hệ thống.
- **Mã hóa dữ liệu (Encryption):** Bảo vệ dữ liệu trong thiết bị, tránh bị đọc nếu mất máy.
- **Kiểm soát thiết bị ngoại vi (Device Control):** Hạn chế sử dụng USB hoặc ổ cứng gắn ngoài để tránh lây nhiễm.

b/ Mục tiêu của đề tài

b.1 Mục tiêu tổng quát

- Xây dựng một hệ thống bảo mật cho các thiết bị đầu cuối (endpoint) nhằm phát hiện, ngăn chặn và phản ứng với các mối đe dọa an ninh mạng một cách hiệu quả.

b.2 Mục tiêu cụ thể

- **Phân tích các mối đe dọa phổ biến đối với endpoint,** như: phần mềm độc hại, tấn công từ xa, khai thác USB, v.v.
- **Thiết kế kiến trúc hệ thống bảo mật endpoint** với các chức năng chính như:
 - Giám sát hoạt động của thiết bị.

- Phát hiện phần mềm độc hại hoặc hành vi bất thường.
- Cảnh báo và tự động phản ứng với sự cố.
- **Xây dựng hoặc tích hợp các công cụ bảo mật**, bao gồm (tùy mục tiêu cụ thể của bạn):
 - Chống virus (Antivirus cơ bản).
 - Giám sát hành vi (hệ thống EDR đơn giản).
 - Kiểm soát thiết bị ngoại vi.
 - Ghi log và gửi cảnh báo về máy chủ trung tâm.
- **Thử nghiệm và đánh giá hiệu quả hệ thống** qua các kịch bản mô phỏng tấn công hoặc sử dụng thực tế.
- **Đảm bảo hệ thống dễ triển khai, sử dụng và phù hợp với mô hình tổ chức nhỏ hoặc cá nhân.**

II/ Cơ sở lý thuyết

a/EndPoint (Người Dùng Cuối)

a.1 Khái niệm EndPoint

Endpoint là thuật ngữ dùng để chỉ các thiết bị đầu cuối trong mạng, nơi người dùng trực tiếp tương tác với hệ thống. Các thiết bị này bao gồm:

- Máy tính để bàn (desktop), máy tính xách tay (laptop)
- Điện thoại thông minh (smartphone), máy tính bảng (tablet)
- Thiết bị IoT (Internet of Things)
- Máy in, máy quét, camera an ninh, v.v.

Các thiết bị endpoint thường kết nối với hệ thống mạng nội bộ hoặc Internet và là nơi diễn ra phần lớn các hoạt động của người dùng.

a.2 Vai trò của Endpoint trong hệ thống mạng

- Là **điểm giao tiếp chính giữa người dùng và hệ thống thông tin**.
- Là nơi **tiếp nhận, xử lý, truyền và lưu trữ thông tin**.
- Đồng thời, endpoint cũng là **điểm khởi đầu cho nhiều cuộc tấn công mạng** như:
 - Cài đặt phần mềm độc hại (malware)
 - Đánh cắp thông tin
 - Mở backdoor truy cập trái phép
 - Phát tán ransomware

a.3 Mối đe dọa đối vs EndPoint

Các endpoint thường đối mặt với nhiều nguy cơ an ninh như:

- **Phần mềm độc hại (Malware)**: virus, trojan, spyware, worm...
- **Tấn công phishing**: dụ người dùng tải mã độc hoặc cung cấp thông tin nhạy cảm.
- **Tấn công từ xa (Remote Access Trojan)**: kẻ tấn công chiếm quyền điều khiển thiết bị.
- **Tấn công qua thiết bị ngoại vi**: USB, ổ cứng di động có thể chứa mã độc.
- **Khai thác lỗ hổng hệ điều hành hoặc phần mềm chưa cập nhật**.

a.4 Khái niệm bảo mật EndPoint

Bảo mật endpoint là tập hợp các biện pháp, công nghệ và phần mềm nhằm bảo vệ các thiết bị đầu cuối khỏi các mối đe dọa kể trên.

Hệ thống bảo mật endpoint thường bao gồm:

- **Phát hiện và ngăn chặn phần mềm độc hại** (Antivirus, Antimalware)

- **Giám sát hành vi thiết bị**, ghi log và phát hiện bất thường (EDR – Endpoint Detection & Response)
- **Tường lửa cá nhân** để kiểm soát lưu lượng ra vào thiết bị
- **Cập nhật và vá lỗi hệ thống** (Patch Management)
- **Kiểm soát truy cập thiết bị ngoại vi**
- **Mã hóa dữ liệu** bảo vệ thông tin nhạy cảm

b/ IDS/IPS

b.1 Khái niệm

IDS (Intrusion Detection System): Hệ thống phát hiện xâm nhập – có nhiệm vụ giám sát lưu lượng mạng hoặc hệ thống để **phát hiện các hành vi đáng ngờ hoặc tấn công mạng**, nhưng **không ngăn chặn trực tiếp**, chỉ cảnh báo người quản trị.

IPS (Intrusion Prevention System): Hệ thống ngăn chặn xâm nhập – có chức năng tương tự IDS nhưng có thể **chủ động chặn hoặc ngắt kết nối độc hại**, bảo vệ hệ thống theo thời gian thực.

b.2 Vai trò của IDS/IPD

- Phát hiện các cuộc tấn công như:
 - Tấn công quét cổng (Port Scanning)
 - Tấn công từ chối dịch vụ (DoS/DDoS)
 - Tấn công khai thác lỗ hổng phần mềm (Exploit)
 - Mã độc lây lan trong mạng nội bộ
- Cung cấp **log chi tiết và cảnh báo sớm**, giúp người quản trị phân tích và ứng phó.
- **IPS có thể chặn gói tin độc hại**, hạn chế thiệt hại khi có tấn công xảy ra.

b.3 Các giải pháp IDS/IPS

❖ Snort



Hình 1 Logo Snort

Giới thiệu: Snort là một hệ thống IDS/IPS mã nguồn mở do công ty Sourcefire (nay thuộc Cisco) phát triển. Đây là một trong những công cụ phổ biến nhất hiện nay trong giám sát và phát hiện xâm nhập.

Tính năng chính:

- Phát hiện tấn công dựa trên chữ ký (signature-based).
- Phân tích gói tin theo thời gian thực (packet sniffer).
- Ghi log và cảnh báo khi phát hiện hành vi đáng ngờ.
- Có thể hoạt động ở các chế độ: sniffer, logger, IDS hoặc IPS (kết hợp với tường lửa như iptables).

Ưu điểm:

- Cộng đồng lớn, cập nhật chữ ký thường xuyên.
- Miễn phí và dễ triển khai trên Linux, Windows.
- Tài liệu và hỗ trợ kỹ thuật phong phú.

Hạn chế:

- Khó tùy biến trong môi trường phức tạp.
- Chưa tối ưu về hiệu suất khi chạy trên mạng tốc độ cao.
- Chủ yếu dựa trên chữ ký nên khó phát hiện tấn công mới (zero-day).

❖ **Suricata**



Hình 2 Logo Suricata

Giới thiệu: Suricata là một hệ thống IDS/IPS mã nguồn mở do Open Information Security Foundation (OISF) phát triển, được đánh giá là sự thay thế mạnh mẽ cho Snort trong nhiều môi trường hiện đại.

Tính năng chính:

- Hỗ trợ đa luồng (multi-threading), hiệu suất cao.
- Hỗ trợ cả IDS và IPS.
- Phân tích sâu vào các giao thức (deep packet inspection).
- Ghi log chi tiết, hỗ trợ chuẩn JSON, EVE.
- Có thể sử dụng các bộ quy tắc (ruleset) của Snort.

Ưu điểm:

- Hiệu suất cao hơn Snort nhờ sử dụng đa luồng.
- Giao diện log linh hoạt, dễ tích hợp với hệ thống SIEM.
- Dễ dàng mở rộng và tích hợp vào môi trường lớn.

Hạn chế:

- Cấu hình phức tạp hơn Snort với người mới.
- Cần phần cứng mạnh nếu xử lý lưu lượng lớn.
- Tập trung nhiều vào log nên có thể cần thêm công cụ phân tích.

❖ **Zeek**



Hình 3 Logo Zeek

Giới thiệu: Zeek là một hệ thống giám sát mạng mã nguồn mở thiên về phân tích hành vi và ghi log, thích hợp để phát hiện tấn công tinh vi. Khác với Snort hay Suricata, Zeek không tập trung vào chữ ký mà vào **phân tích lưu lượng**.

Tính năng chính:

- Phân tích hành vi dựa trên dòng dữ liệu thay vì gói đơn lẻ.
- Ghi log chi tiết toàn bộ hoạt động mạng (HTTP, DNS, SSL, SSH...).
- Có thể viết script tùy chỉnh để phát hiện hành vi đáng ngờ.
- Phù hợp cho phân tích forensic và điều tra sau tấn công.

Ưu điểm:

- Mạnh trong việc phát hiện tấn công tinh vi, khó nhận biết bằng chữ ký.
- Ghi log rất chi tiết, phục vụ tốt cho truy vết và phân tích.
- Có thể kết hợp với ELK stack, Splunk để trực quan hóa log.

Hạn chế:

- Không có khả năng ngăn chặn tấn công (chỉ phát hiện).
- Cần kỹ năng scripting nếu muốn tùy biến sâu.
- Dữ liệu log nhiều, cần hệ thống lưu trữ và phân tích tốt.

b.4 Giải pháp triển khai trong đề tài: Sử dụng Suricata trong pfSense

b.4.1 Lý do lựa chọn Suricata

Trong số các giải pháp IDS/IPS mã nguồn mở hiện nay, **Suricata** được đánh giá cao nhờ hiệu suất mạnh mẽ, hỗ trợ đa luồng, khả năng phát hiện tấn công tốt và dễ tích hợp vào các hệ thống hiện đại.

So với Snort và Zeek:

- Suricata hỗ trợ **vừa IDS vừa IPS**, có thể hoạt động ở chế độ phát hiện hoặc chặn.
- Có thể sử dụng chung bộ quy tắc của Snort nhưng **xử lý nhanh hơn**, hỗ trợ **phân tích sâu gói tin (Deep Packet Inspection)**.
- Hỗ trợ định dạng log chuẩn **EVE JSON**, dễ tích hợp với các hệ thống phân tích log như ELK Stack, Splunk.

b.4.2 Giới thiệu pfSense và khả năng tích hợp Suricata

pfSense là một firewall mã nguồn mở dựa trên FreeBSD, cung cấp giải pháp tường lửa, NAT, VPN và nhiều tính năng mạng mạnh mẽ. pfSense cho phép cài đặt các gói mở rộng (packages), trong đó **Suricata** là một trong những gói được hỗ trợ trực tiếp.



Hình 4 Logo pfSense

Việc triển khai **Suricata** trên **pfSense** mang lại nhiều lợi ích:

- **Giao diện cấu hình trực quan**, dễ sử dụng thông qua web GUI.
- Cho phép **cài đặt, quản lý quy tắc, cấu hình cảnh báo và hành vi IPS** ngay trong pfSense.

- Có thể áp dụng Suricata lên từng giao diện mạng cụ thể (WAN, LAN...).
- Tích hợp chặt chẽ với tường lửa của pfSense giúp chặn lưu lượng nghi ngờ theo thời gian thực.

b.4.3 Mục tiêu triển khai trong đề tài

Trong khuôn khổ đề tài, việc triển khai Suricata trong pfSense nhằm mục đích:

- **Phát hiện và ngăn chặn các cuộc tấn công mạng phổ biến** như: port scan, brute force, khai thác lỗ hổng, truy cập trái phép...
- **Giám sát lưu lượng mạng ra vào hệ thống nội bộ**, giúp quản trị viên nắm bắt tình hình an ninh.
- **Cảnh báo sớm và log chi tiết các sự kiện nghi ngờ**, phục vụ điều tra và cải thiện bảo mật.
- **Áp dụng các quy tắc phát hiện tấn công tiêu chuẩn (ET Open Rules, Snort Rules)** và tùy chỉnh theo môi trường thử nghiệm.

c/ System Endpoint

c.1 Khái niệm System Endpoint

System Endpoint (thiết bị đầu cuối trong hệ thống) là những thiết bị cá nhân hoặc thiết bị chuyên dụng có khả năng kết nối và giao tiếp với hệ thống mạng của tổ chức hoặc doanh nghiệp. Các endpoint phổ biến bao gồm máy tính để bàn, máy tính xách tay, thiết bị di động, máy chủ, máy in mạng, thiết bị IoT, v.v.

Trong bối cảnh an ninh mạng, endpoint được xem là một trong những điểm yếu quan trọng vì đây là nơi người dùng tương tác trực tiếp với tài nguyên hệ thống, đồng thời cũng là mục tiêu hàng đầu của các cuộc tấn công như malware, phishing, ransomware hoặc truy cập trái phép.

c.2 Vai trò của System Endpoint

Hệ thống bảo mật endpoint đóng vai trò then chốt trong việc bảo vệ dữ liệu và duy trì tính toàn vẹn của hệ thống thông tin. Các vai trò chính bao gồm:

- **Bảo vệ thiết bị khỏi phần mềm độc hại:** Endpoint là nơi đầu tiên tiếp nhận các tập tin và dữ liệu từ bên ngoài, do đó cần có cơ chế phát hiện và ngăn chặn malware như virus, trojan, spyware, ransomware...
- **Giám sát hành vi và hoạt động hệ thống:** Theo dõi các tiến trình, hoạt động đăng nhập, thay đổi tệp tin và hành vi người dùng để phát hiện các hành vi đáng ngờ hoặc nguy cơ tiềm ẩn.
- **Quản lý và kiểm soát thiết bị ngoại vi:** Ngăn chặn việc sử dụng trái phép USB, ổ cứng ngoài hoặc thiết bị không rõ nguồn gốc nhằm hạn chế nguy cơ rò rỉ dữ liệu.

- **Tăng cường an ninh mạng tổng thể:** Endpoint là điểm khởi đầu trong chuỗi phòng thủ đa lớp. Nếu endpoint bị xâm nhập, toàn bộ hệ thống có thể bị ảnh hưởng. Do đó, bảo mật endpoint là bước đầu quan trọng trong chiến lược bảo vệ tổng thể.
- **Tích hợp với các hệ thống giám sát tập trung:** Dữ liệu từ endpoint có thể được gửi về hệ thống SIEM để phục vụ phân tích, phát hiện mối đe dọa và điều tra bảo mật.

c.3 Các giải pháp System Endpoint

❖ Wazuh



Hình 5 Logo Wazuh

Giới thiệu: Wazuh là một nền tảng bảo mật mã nguồn mở mạnh mẽ, kế thừa và mở rộng từ hệ thống OSSEC. Wazuh hoạt động như một hệ thống HIDS (Host-based Intrusion Detection System) kết hợp khả năng SIEM cơ bản.

Tính năng chính:

- Phát hiện rootkit và hành vi tấn công trên thiết bị đầu cuối.
- Kiểm tra tính toàn vẹn tệp tin (file integrity monitoring).
- Giám sát log hệ thống (event logs, syslog...).
- Theo dõi người dùng, tiến trình, kết nối mạng.
- Cảnh báo thời gian thực, tích hợp giao diện Kibana để hiển thị dữ liệu.

Cấu trúc hệ thống:

- **Agent** cài trên endpoint (Windows/Linux/macOS).
- **Manager/Server** nhận log, phân tích và đưa ra cảnh báo.
- Có thể tích hợp với **Elastic Stack (ELK)** để trực quan hóa dữ liệu.

Ưu điểm:

- Miễn phí, mã nguồn mở, cộng đồng hỗ trợ tốt.

- Tích hợp dễ dàng vào hệ thống giám sát tập trung.
- Phù hợp với cả giám sát endpoint và hệ thống mạng.

Hạn chế:

- Cần cấu hình nhiều bước ban đầu.
- Khó sử dụng nếu không quen với log và phân tích sự kiện.

❖ Ossec



Hình 6 Logo Ossec

Giới thiệu: OSSEC (Open Source Security) là một hệ thống HIDS mã nguồn mở lâu đời, dùng để giám sát các endpoint về thay đổi file, log, rootkit và hành vi nghi ngờ.

Tính năng chính:

- Theo dõi các thay đổi tệp và thư mục quan trọng.
- Giám sát log hệ điều hành, web server, cơ sở dữ liệu...
- Hỗ trợ nhiều nền tảng: Windows, Linux, macOS, BSD.
- Phản ứng tự động với các sự kiện bảo mật qua cảnh báo hoặc kịch bản tùy chỉnh.

Cấu trúc hệ thống:

- Mô hình client-server: agent cài trên endpoint, gửi dữ liệu về server phân tích.
- Quản trị viên có thể thiết lập chính sách phát hiện cho từng loại thiết bị.

Ưu điểm:

- Nhẹ, dễ triển khai trong môi trường nhỏ.
- Có thể chạy độc lập hoặc kết hợp với các công cụ SIEM.
- Hỗ trợ alert qua email, syslog.

Hạn chế:

- Giao diện người dùng hạn chế (CLI).
- Không có khả năng hiển thị trực quan nếu không tích hợp ELK hoặc Graylog.

❖ Security Onion



Hình 7 Logo Security Onion

Giới thiệu: Security Onion là một bản phân phối Linux chuyên về giám sát an ninh mạng và phân tích sự kiện. Nó tích hợp nhiều công cụ mã nguồn mở mạnh mẽ như Suricata, Zeek, Wazuh, Elastic Stack...

Tính năng chính:

- Giám sát mạng và endpoint từ một hệ thống tập trung.
- Cung cấp khả năng phát hiện tấn công theo thời gian thực.
- Cho phép thu thập log, phân tích sự kiện, điều tra sự cố (forensics).
- Giao diện web quản lý tập trung.

Thành phần tích hợp:

- **Wazuh** (giám sát host).
- **Suricata** (IDS/IPS).
- **Zeek** (phân tích hành vi mạng).
- **TheHive, Kibana, Elasticsearch...**

Ưu điểm:

- Mạnh mẽ, all-in-one, phù hợp với phân tích sự cố toàn diện.
- Giao diện trực quan, dữ liệu chi tiết.
- Dễ mở rộng và hỗ trợ hệ thống mạng lớn.

Hạn chế:

- Cần phần cứng mạnh để vận hành đầy đủ.
- Không phù hợp cho hệ thống nhỏ hoặc người dùng cá nhân.

❖ Auditbeat (Elastic Agent)

Giới thiệu: Auditbeat là một thành phần thuộc Elastic Stack, dùng để thu thập thông tin từ các thiết bị đầu cuối và gửi về Elasticsearch để phân tích.

Tính năng chính:

- Giám sát sự kiện audit trên Linux: lệnh chạy, thay đổi file, thay đổi quyền.
- Theo dõi tiến trình, người dùng đăng nhập, mạng, socket...
- Gửi dữ liệu dưới dạng JSON về hệ thống ELK để phân tích và cảnh báo.

Ưu điểm:

- Nhẹ, dễ triển khai.
- Ghi lại chi tiết hoạt động trên hệ thống endpoint.
- Tích hợp mạnh mẽ với Kibana để hiển thị biểu đồ, thống kê.

Hạn chế:

- Chỉ hoạt động tốt khi kết hợp với ELK Stack.
- Không có khả năng tự động chặn tấn công (chỉ giám sát và ghi log).

c.4 Giải pháp triển khai trong đề tài: Sử dụng Wazuh

c.4.1 Lý do lựa chọn Wazuh

Wazuh được lựa chọn là giải pháp bảo mật endpoint trong đề tài vì các lý do sau:

- Là giải pháp mã nguồn mở, hoàn toàn miễn phí, phù hợp với nghiên cứu và triển khai thực tế.
- Có khả năng giám sát chuyên sâu hành vi trên thiết bị đầu cuối: theo dõi tiến trình, truy cập tệp tin, người dùng, log hệ thống, v.v.
- Hỗ trợ đa nền tảng: Windows, Linux, macOS.
- Tích hợp với Elastic Stack (ELK) giúp trực quan hóa dữ liệu và dễ dàng điều tra sự kiện bảo mật.
- Cho phép mở rộng quy mô và kết hợp với các hệ thống mạng, SIEM, IDS khác như Suricata, Zeek.

c.4.2 Mục tiêu triển khai Wazuh trong đề tài

Việc triển khai Wazuh trong đề tài hướng đến các mục tiêu cụ thể sau:

- **Tăng cường bảo mật cho thiết bị đầu cuối**

Wazuh sẽ được cài đặt trên các thiết bị người dùng nhằm giám sát hoạt động hệ thống, phát hiện sớm các hành vi bất thường hoặc nguy cơ tấn công.

- **Thu thập và phân tích log tập trung**

Dữ liệu log từ các thiết bị sẽ được gửi về máy chủ Wazuh để xử lý và phân tích theo thời gian thực, giúp phát hiện sớm các sự cố an ninh.

- **Cảnh báo các mối đe dọa kịp thời**

Khi phát hiện hành vi bất thường, hệ thống sẽ sinh cảnh báo, hỗ trợ người quản trị đưa ra quyết định nhanh chóng nhằm ngăn chặn rủi ro.

- **Xây dựng mô hình giám sát an ninh chủ động**

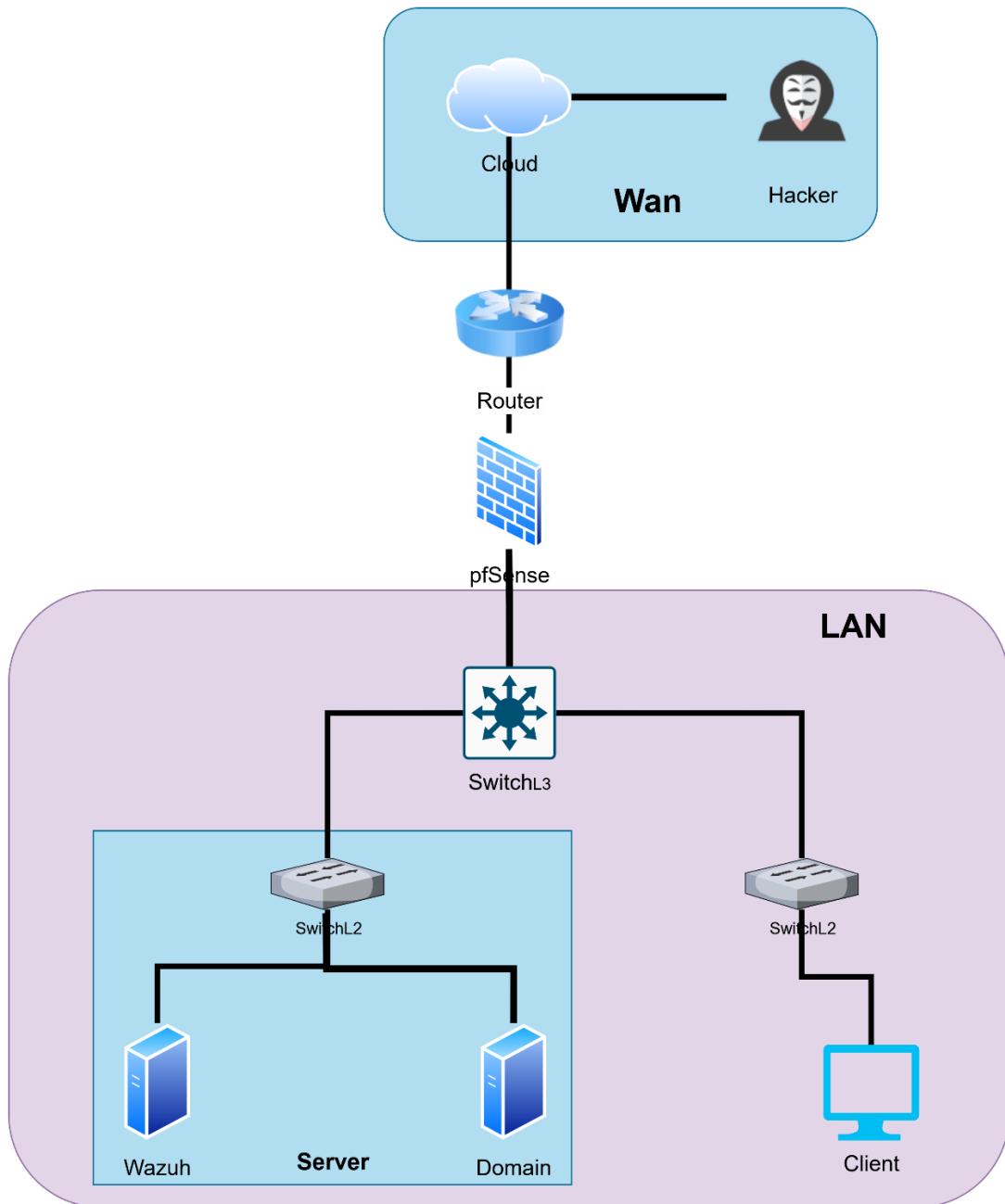
Để tài sử dụng Wazuh để xây dựng mô hình giám sát an ninh tập trung, có khả năng mở rộng và tích hợp trong tương lai với các giải pháp khác.

- **Phục vụ thử nghiệm và đánh giá hiệu quả bảo mật**

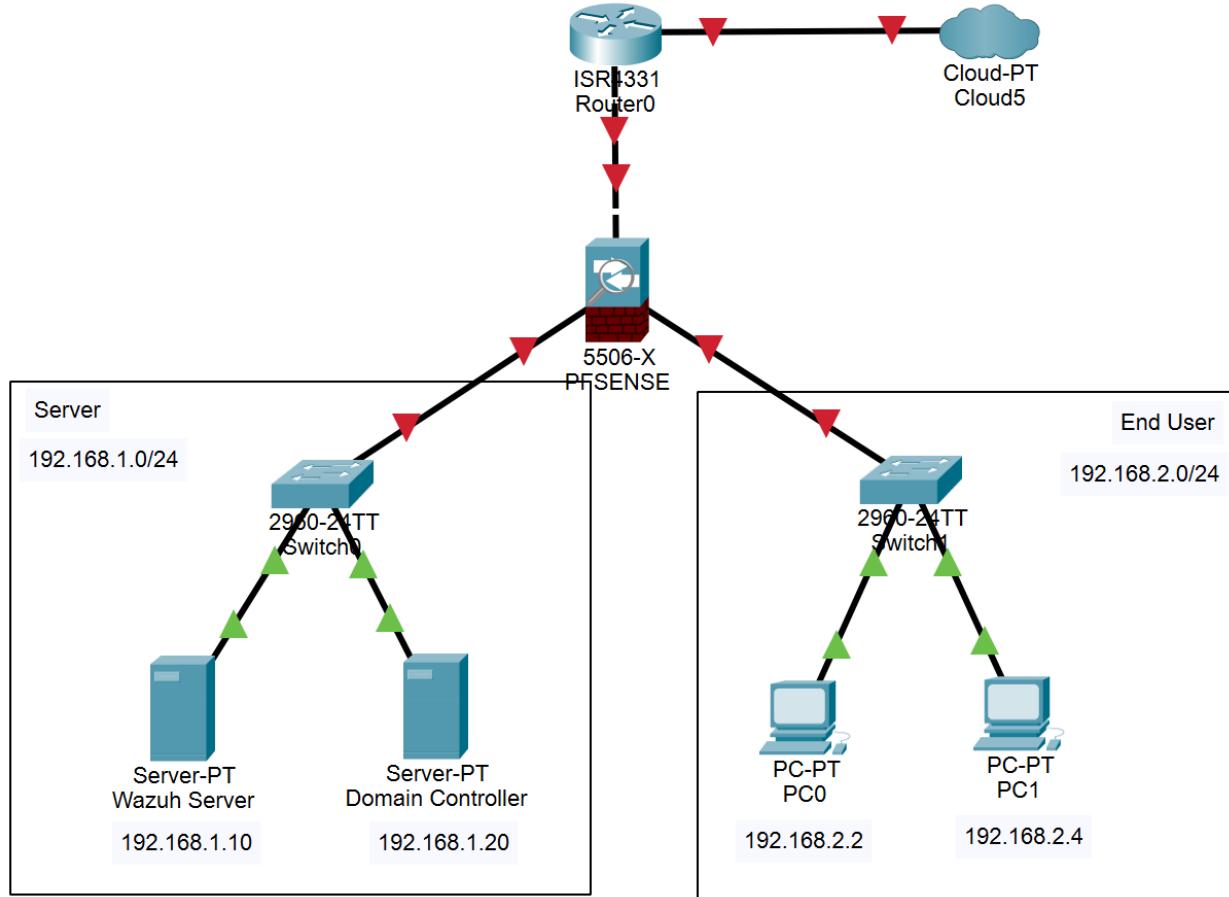
Wazuh sẽ là công cụ hỗ trợ trong quá trình thực nghiệm, cho phép kiểm tra, đánh giá các kịch bản tấn công giả lập và khả năng phản ứng của hệ thống.

III/ Triển khai các rules và demo tấn công

a/ Sơ đồ triển khai



Hình 8 Sơ đồ vật lý



Hình 9 Sơ đồ logic

Tổng quan thiết bị:

- 1 Firewall Pfsense (Suricata sẽ được tích hợp trong pfSense)
- 3 máy PC (2 máy Client và một máy attacker)
- 2 máy Server (một máy Wazuh Server, một máy Domain)

b/ Cài đặt và triển khai

b.1 IDS/IPS

Cài đặt pfSense: Tải và boot từ ISO pfSense

Cấu hình địa chỉ IP tĩnh cho các interface (LAN, OPT1).

```
Starting package snort...done.
pfSense 2.7.1-RELEASE amd64 20231115-1706
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 6c5e0070dbfef5827d02

*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.1.128/24
LAN (lan)      -> em1          -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2          -> v4: 192.168.2.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: ■
```

Hình 10 Cấu hình ip pfSense

Truy cập giao diện web tại: http://192.168.1.1, đăng nhập:

- **Username:** admin
- **Password:** pfsense

The screenshot shows the pfSense web interface. At the top, there's a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the main dashboard has two main sections: "System Information" on the left and "Netgate Services And Support" on the right. The "System Information" section contains details like Name (pfSense.home.arpa), User (admin@192.168.1.2), System (VMware Virtual Machine, Netgate Device ID: 6c5e0070dbfef5827d02), BIOS (Vendor: Phoenix Technologies LTD, Version: 6.00, Release Date: Thu Nov 12 2020), Version (2.7.1-RELEASE (amd64) built on Wed Nov 15 17:06:00 UTC 2023 FreeBSD 14.0-CURRENT), and CPU Type (13th Gen Intel(R) Core(TM) i5-13500H, 2 CPUs: 1 package(s) x 2 core(s), AES-NI CPU Crypto: Yes (inactive), QAT Crypto: No). The "Netgate Services And Support" section includes a "Community Support" contract type, a "NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES" section with links to upgrade support, community support resources, official pfSense training, and professional services, and a note about purchasing TAC support. At the bottom, there's a search bar and a toolbar.

Hình 11 Giao diện web của pfSense

Cài đặt thêm service Suricata để quản lý IDS/IPS:

Trong phần Packages Manager tìm suricata và cài đặt.

Name	Category	Version	Description	Actions
✓ suricata	security	7.0.8_1	High Performance Network IDS, IPS and Security Monitoring engine by OISF. Package Dependencies: suricata-7.0.8	

Legend: = Update = Current
 = Remove = Information = Reinstall
Newer version available
Package is configured but not (fully) installed or deprecated

Hình 12 Package manager

Sau khi cài đặt thành công suricata, Tiến hành truy cập Suricata trong tab Service

Add interface WAN (em0) để giám sát mọi lưu lượng truy cập từ ngoài vào mạng nội bộ.

Bloking Mode: LEGACY MODE để kết hợp thêm IPS.

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> WAN (em0)		AUTO	LEGACY MODE	WAN	

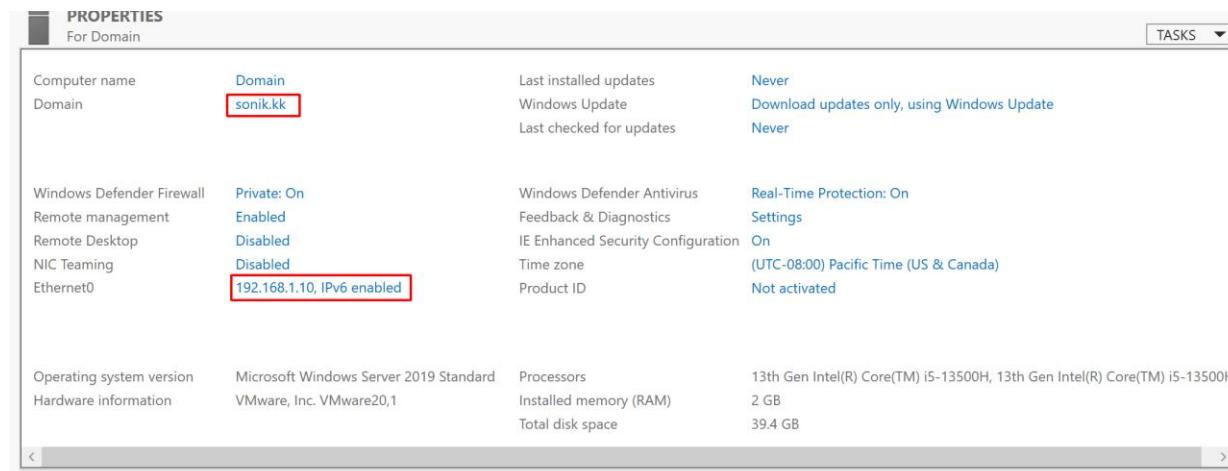
Hình 13 Service Suricata

Cấu hình file suricata.yaml để sử dụng rule-file: custom.rules

```
suricata.yaml * suricata.yaml
312 # IDS output about what its doing, errors, etc.
313 logging:
314
315     # This value is overriden by the SC_LOG_LEVEL env var.
316     default-log-level: info
317     default-log-format: "%t - <%d> -- "
318
319     # Define your logging outputs.
320     outputs:
321         - console:
322             enabled: yes
323         - file:
324             enabled: yes
325             filename: /var/log/suricata/suricata_em028498/suricata.log
326         - syslog:
327             enabled: no
328             facility: local1
329             level: notice
330             format: "[%i] <%d> -- "
331
332 # IPS Mode Configuration
333 # PCAP
334 pcap:
335     - interface: em0
336         checksum-checks: auto
337         promisc: yes
338         snaplen: 1518
339
340 legacy:
341     uricontent: enabled
342
343 default-rule-path: /usr/local/etc/suricata/suricata_28498_em0/rules
344 rule-files:
345     - custom.rules
346
347 classification-file: /usr/local/etc/suricata/suricata_28498_em0/classification.config
348 reference-config-file: /usr/local/etc/suricata/suricata_28498_em0/reference.config
349
350 # Holds variables that would be used by the engine.
351 vars:
352
353     # Holds the address group vars that would be passed in a Signature.
354     address-groups:
355         HOME_NET: "192.168.1.1/32, 8.8.8.8/32, 127.0.0.1/32, 192.168.1.0/24, 192.168.2.0/24, 192.168.150.2/32, 192.168.150.128/32, ::1/128, fe80::20c:29ff:fe60:3c48/128"
356         EXTERNAL_NET: "[!$HOME_NET]"
357         DNS_SERVERS: "$HOME_NET"
358         SMTP_SERVERS: "$HOME_NET"
359         HTTP_SERVERS: "$HOME_NET"
360         SQL_SERVERS: "$HOME_NET"
```

b.2/ Winserver (Domain Server)

Tiến hành nâng cấp winserver lên domain: sonik.kk, ip: 192.168.1.10



Cấu hình DNS cho server

The DNS Manager interface shows the configuration of the 'sonik.kk' zone. The left pane displays the tree structure under 'DOMAIN'. The right pane lists the zone's records:

Name	Type	Data	Timestamp
_msdcs	Start of Authority (SOA)	[19] domain.sonik.kk., host...	static
_sites	Name Server (NS)	domain.sonik.kk.	static
_tcp	Host (A)	192.168.1.10	7/11/2025
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)			
(same as parent folder)			
(same as parent folder)			
domain	Host (A)	192.168.1.10	static

Cấu hình DHCP trên server để cấp ip tự động cho các máy client:

The DHCP Manager interface shows the configuration of the 'Scope [192.168.2.0] dhcp-lan'. The left pane displays the tree structure under 'domain.sonik.kk'. The right pane shows the scope's properties:

Contents of DHCP Server	Status	Description	Failover Relationship
Scope [192.168.2.0] dhcp-lan	** Active **		
Server Options			
Policies			
Filters			

b.3/ System Endpoint (Wazuh)

Thực hiện chạy các câu lệnh để cài đặt Wazuh trên Ubuntu

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

```
See 'snap info curl' for additional versions.  
sonik@sonik:~$ sudo apt install curl -y  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following NEW packages will be installed:  
  curl  
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.  
Need to get 226 kB of archives.  
After this operation, 534 kB of additional disk space will be used.  
Get:1 http://vn.archive.ubuntu.com/ubuntu noble-updates/main amd64 curl amd64 8.  
5.0-2ubuntu10.6 [226 kB]  
Fetched 226 kB in 0s (2,672 kB/s)  
Selecting previously unselected package curl.  
(Reading database ... 149613 files and directories currently installed.)  
Preparing to unpack .../curl_8.5.0-2ubuntu10.6_amd64.deb ...  
Unpacking curl (8.5.0-2ubuntu10.6) ...  
Setting up curl (8.5.0-2ubuntu10.6) ...  
Processing triggers for man-db (2.12.0-4build2) ...  
sonik@sonik:~$ curl -s0 https://packages.wazuh.com/4.12/wazuh-install.sh && sudo  
bash ./wazuh-install.sh -a
```

Đây là các thông tin bạn nhận được sau khi cài đặt thành công Wazuh trên Ubuntu

```
30/06/2025 21:13:03 INFO: Starting service filebeat.  
30/06/2025 21:13:05 INFO: filebeat service started.  
30/06/2025 21:13:05 INFO: --- Wazuh dashboard ---  
30/06/2025 21:13:05 INFO: Starting Wazuh dashboard installation.  
30/06/2025 21:14:23 INFO: Wazuh dashboard installation finished.  
30/06/2025 21:14:23 INFO: Wazuh dashboard post-install configuration finished.  
30/06/2025 21:14:23 INFO: Starting service wazuh-dashboard.  
30/06/2025 21:14:25 INFO: wazuh-dashboard service started.  
30/06/2025 21:14:27 INFO: Updating the internal users.  
30/06/2025 21:14:37 INFO: A backup of the internal users has been saved in the /  
etc/wazuh-indexer/internalusers-backup folder.  
30/06/2025 21:15:01 INFO: The filebeat.yml file has been updated to use the File  
beat Keystore username and password.  
30/06/2025 21:15:38 INFO: Initializing Wazuh dashboard web application.  
30/06/2025 21:15:38 INFO: Wazuh dashboard web application initialized.  
30/06/2025 21:15:38 INFO: --- Summary ---  
30/06/2025 21:15:38 INFO: You can access the web interface https://<wazuh-dashbo  
ard-ip>:443  
  User: admin  
    Password: NFyn?aWg5KwpZWS.8HKuu.2ckg1?yTa6  
30/06/2025 21:15:38 INFO: --- Dependencies ----  
30/06/2025 21:15:38 INFO: Removing gawk.  
30/06/2025 21:15:44 INFO: Installation finished.  
sonik@sonik:~$
```

Sau khi cài đặt thành công tiến hành kiểm tra tài khoản trên Wazuh bằng câu lệnh:\

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

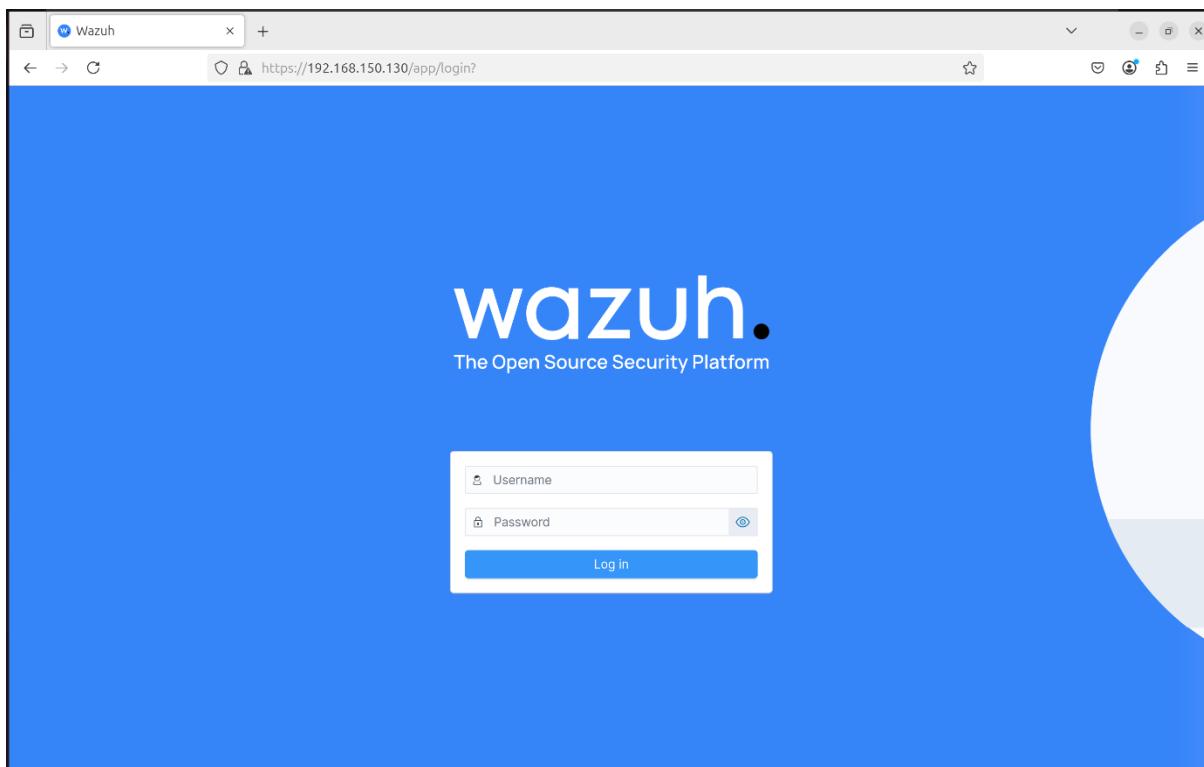
```
sudo: command not found
sonik@sonik:~$ sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazu
h-passwords.txt
wazuh-install-files/wazuh-passwords.txt
# Admin user for the web user interface and Wazuh indexer. Use this user to log
in to Wazuh dashboard
indexer_username: 'admin'
indexer_password: 'NFyn?aWg5KWPZWS.8HKuu.2ckg1?yTa6'

# Anomaly detection user for the web user interface
indexer_username: 'anomalyadmin'
indexer_password: '8cqA96X87hADkBXm?uC7jvZ*?uxWkyZa'

# Wazuh dashboard user for establishing the connection with Wazuh indexer
indexer_username: 'kibanaserver'
indexer_password: 'XN1tYWZDX0iWN8u5RL50qcUtVG1qkgA*'

# Regular Dashboard user, only has read permissions to all indices and all permis
sions on the .kibana index
```

Sau đó tiến hành truy cập vào giao diện web của Wazuh bằng ip của máy Ubuntu cài Wazuh và sử dụng tài khoản mật khẩu ở trên để đăng nhập vào Wazuh



c/ IDS/IPS Rule

c.1 SSH Brute Force

Tiến hành thêm interface Wan để giám sát lưu lượng từ ngoài vào mạng

Báo Cáo Học Tập

The screenshot shows the Suricata interface settings page at the URL 192.168.150.128/suricata/suricata_interfaces_edit.php?id=0. A yellow warning box at the top states: "WARNING! Suricata now requires that Hardware Checksum Offloading, Hardware TCP Segmentation Offloading and Hardware Large Receive Offloading all be disabled for proper operation. This firewall currently has one or more of these Offloading settings NOT disabled. Visit the System > Advanced > Networking tab and ensure all three of these Offloading settings are disabled." Below the warning, there are tabs for Interfaces, Global Settings, Updates, Alerts, Blocks, Files, Pass Lists, Suppress, Logs View, Logs Mgmt, and SID Mgmt. Under the Interfaces tab, there are sub-tabs for Sync and IP Lists. The main content area is titled "General Settings". It includes an "Enable" checkbox (checked) and a note: "Checking this box enables Suricata inspection on the interface." A dropdown menu for "Interface" is set to "WAN (em0)", which is highlighted with a red box. A note below says: "Choose which interface this Suricata instance applies to. In most cases, you will want to choose LAN here if this is the first Suricata-configured interface." There is also a "Description" field set to "WAN". The "Logging Settings" section is visible at the bottom.

Hình 14 Thêm interface Wan

Tại tab Wan Rules, mục Category lựa chọn custom.rules để tiến hành tự custom rule

The screenshot shows the Wan Rules tab under the Services / Suricata / Interface Settings section. The tabs at the top are Interfaces, Global Settings, Updates, Alerts, Blocks, Files, Pass Lists, Suppress, Logs View, Logs Mgmt, and SID Mgmt. The sub-tabs are Sync and IP Lists. The main content area is titled "Available Rule Categories". A dropdown menu for "Category" is set to "custom.rules", which is highlighted with a red box. A note below says: "Select the rule category to view and manage." The "Defined Custom Rules" section shows a single rule entry: "alert tcp any any -> any 22 (msg:"SSH Brute Force Attack Detected"; flow:to_server; content:"SSH-"; depth:4; threshold:type threshold, track by_src, count 5, seconds 60; classtype:attempted-dos; sid:1000004; rev:1; flowbits:set,ssh.attempt;)".

Hình 15 Tab Wan Rules

Rule custom để giám sát SSH brute force:

```
alert tcp any any -> any 22 (msg:"SSH Brute Force Attack Detected"; flow:to_server; content:"SSH-"; depth:4; threshold:type threshold, track by_src, count 5, seconds 60; classtype:attempted-dos; sid:1000004; rev:1; flowbits:set,ssh.attempt;)
```

Phân tích cấu hình rule:

Thành phần	Mô tả
alert	Hành động của rule – tạo cảnh báo khi điều kiện khớp
tcp	Giao thức TCP
any any	Mọi địa chỉ IP nguồn, mọi cổng nguồn
->	Dòng dữ liệu đi từ client → server
any 22	Bất kỳ IP đích nào, nhưng cổng đích là 22 (SSH)

Thành phần	Mô tả
msg:"SSH Brute Force Attack Detected"	Tin nhắn cảnh báo sẽ xuất hiện khi rule kích hoạt
flow:to_server	Rule chỉ áp dụng với lưu lượng gửi tới server
content:"SSH-"	Tìm chuỗi " SSH- " trong payload – dấu hiệu khởi đầu phiên SSH
depth:4	Chỉ tìm chuỗi "SSH-" trong 4 byte đầu tiên của payload (tối ưu hiệu suất)
threshold:type threshold, track by_src, count 5, seconds 60	Nếu 1 địa chỉ IP gửi 5 gói SSH trong vòng 60 giây → cảnh báo
classtype:attempted-dos	Phân loại mối đe dọa là tấn công từ chối dịch vụ
sid:1000004	ID của rule – duy nhất trong bộ rule
rev:1	Phiên bản của rule (dùng để cập nhật sau này)
flowbits:set,ssh.attempt;	Đặt cờ ssh.attempt để sử dụng lại trong các rule khác (ghi nhận hành vi tấn công SSH trước đó)

Sau khi cấu hình sau trạng thái mặc định của interface Wan sẽ là off.

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
WAN (em0)	OFF	AUTO	DISABLED	WAN	

Hình 16 Interface Wan đang off

Tiến hành bật interface Wan để giám sát mạng Wan bằng suricata

The screenshot shows the 'Interface Settings Overview' section of the Suricata configuration interface. It lists a single interface, 'WAN (em0)', with the following details:

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
WAN (em0)	<input checked="" type="checkbox"/>	AUTO	DISABLED	WAN	

At the bottom right of the interface, there are buttons for '+ Add' and 'Delete'.

Hình 17 Interface Wan đã bật

Tiến hành bật Block Offenders để block với chế độ IPS Mode “Legacy Mode”

The screenshot shows the 'Alert and Block Settings' page. Under the 'IPS Mode' section, the dropdown is set to 'Legacy Mode'. A detailed description explains that Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface, while Inline Mode inserts the Suricata inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Other settings shown include:

- Block Offenders:** Checked checkbox indicating automatic blocking of hosts generating alerts.
- Kill States:** Checked checkbox indicating killing firewall states for blocked IP.
- Which IP to Block:** Set to 'BOTH'.
- Block On DROP Only:** Unchecked checkbox indicating inserting blocks only when rule signatures have the DROP action.
- IP Pass List:** Set to 'default' with a 'View List' button.
- Enable Passlist Debugging Log:** Unchecked checkbox indicating enabling detailed passlist operations logging.

Test Rule

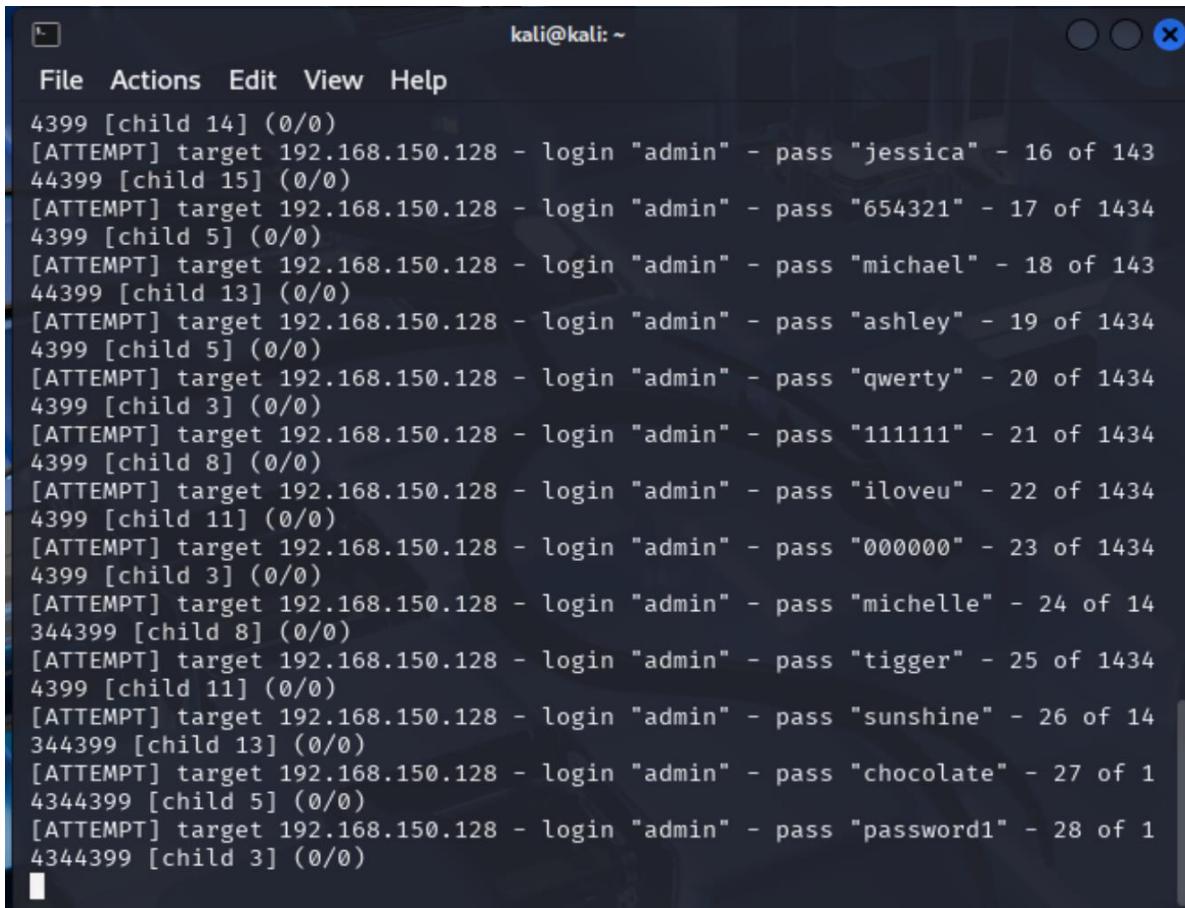
Trên máy attacker kali:

Dùng công cụ brute-force hydra để tấn công đến ip 192.168.1.128 với username là admin dùng danh sách mật khẩu phổ biến rockyou.txt với giao thức SSH.

```
(kali㉿kali)-[~]
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.128 ssh -vV
```

Hình 18 Lệnh tấn công brute-force ssh

Tiến hành brute-force:



A screenshot of a terminal window titled "kali@kali: ~". The window displays a log of a brute-force attack against a target at 192.168.150.128. The log shows multiple login attempts for the "admin" user, each with a different password. The progress is tracked by a counter from 16 to 28 of 1434 attempts. The password list includes "jessica", "654321", "michael", "ashley", "qwerty", "111111", "iloveu", "000000", "michelle", "tigger", "sunshine", "chocolate", and "password1". The terminal has a dark theme with light-colored text.

```
kali@kali: ~
File Actions Edit View Help
4399 [child 14] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "jessica" - 16 of 143
44399 [child 15] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "654321" - 17 of 1434
4399 [child 5] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "michael" - 18 of 143
44399 [child 13] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "ashley" - 19 of 1434
4399 [child 5] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "qwerty" - 20 of 1434
4399 [child 3] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "111111" - 21 of 1434
4399 [child 8] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "iloveu" - 22 of 1434
4399 [child 11] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "000000" - 23 of 1434
4399 [child 3] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "michelle" - 24 of 14
344399 [child 8] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "tigger" - 25 of 1434
4399 [child 11] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "sunshine" - 26 of 14
344399 [child 13] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "chocolate" - 27 of 1
4344399 [child 5] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "password1" - 28 of 1
4344399 [child 3] (0/0)
```

Hình 19 Brute-force

Trên Alert của pfSense đã nhận được cảnh báo SSH Brute-force

Báo Cáo Học Tập

The screenshot shows the Suricata interface under the 'Alerts' tab. In the 'Alert Log View Settings' section, the 'Instance to View' dropdown is set to '(WAN) WAN'. Below it, there are buttons for 'Download' and 'Clear'. The 'Save Settings' section includes a 'Save' button, a checked 'Refresh' checkbox, and a dropdown for 'Number of alerts to display' set to 250. The 'Alert Log View Filter' section shows 'Last 250 Alert Entries'. A table lists five entries, each with a red box highlighting the source IP (192.168.150.129), destination port (22), and description ('SSH Brute Force Attack Detected').

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
07/23/2025 14:05:04	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	56582	192.168.150.128	22	1:1000004	SSH Brute Force Attack Detected
07/23/2025 14:05:04	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	56610	192.168.150.128	22	1:1000004	SSH Brute Force Attack Detected
07/23/2025 14:05:04	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	56682	192.168.150.128	22	1:1000004	SSH Brute Force Attack Detected
07/23/2025 14:05:04	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	56674	192.168.150.128	22	1:1000004	SSH Brute Force Attack Detected
07/23/2025 14:05:04	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	56610	192.168.150.128	22	1:1000004	SSH Brute Force Attack Detected

Hình 20 Alert Suricata

Do đã phát hiện tấn công SSH Brute-force nên Suricata đã tiến hành block máy attacker.

The screenshot shows the Suricata interface under the 'Blocks' tab. In the 'Blocked Hosts Log View Settings' section, there are buttons for 'Save or Remove Hosts' and 'Clear'. The 'Save Settings' section includes a 'Save' button, a checked 'Refresh' checkbox, and a dropdown for 'Number of blocked entries to view' set to 500. The 'Last 500 Hosts Blocked by Suricata' section shows a table with one entry. A note at the top states: 'Note: Only blocked IP addresses from Legacy Mode interfaces are shown! For inline IPS mode interfaces, dropped IP addresses are highlighted on the ALERTS tab.' The table has columns: Blocked IP, Block Date/Time, Block Alert Description, Block Rule GID:SID, and Remove Block. The entry shows '192.168.150.129' as the blocked IP, '07/23/2025 14:10:57' as the date/time, 'SSH Brute Force Attack Detected' as the description, '1:1000004' as the rule, and a red 'X' icon in the Remove Block column.

Blocked IP	Block Date/Time	Block Alert Description	Block Rule GID:SID	Remove Block
192.168.150.129	07/23/2025 14:10:57	SSH Brute Force Attack Detected	1:1000004	X

Hình 21 Blocks tab

Trên máy attacker đã ko thể tiếp tục tấn công.

```

File Actions Edit View Help
4403 [child 15] (0/4)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "anthony" - 30 of 143
44403 [child 6] (0/4)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "friends" - 31 of 143
44403 [child 1] (0/4)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "butterfly" - 32 of 1
4344403 [child 3] (0/4)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "purple" - 33 of 1434
4403 [child 4] (0/4)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "angel" - 34 of 14344
403 [child 9] (0/4)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "jordan" - 35 of 1434
4403 [child 0] (0/4)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "liverpool" - 36 of 1
4344403 [child 10] (0/4)
[ERROR] could not connect to target port 22: Timeout connecting to 192.168.15
0.128
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 14
[ERROR] could not connect to target port 22: Timeout connecting to 192.168.15
0.128
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 13
[RE-ATTEMPT] target 192.168.150.128 - login "admin" - pass "lovely" - 36 of 1
4344403 [child 14] (0/4)
[RE-ATTEMPT] target 192.168.150.128 - login "admin" - pass "monkey" - 36 of 1
4344403 [child 13] (0/4)

```

Hình 22 Kali attacker

c.2 DDos

Các cách cấu hình Ddos rule sẽ giống cấu hình SSH rule. Chỉ khác nội dung của rule

```
alert tcp any any -> $HOME_NET 80 (msg:"[DOS] Possible SYN Flood attack"; flags:S;
threshold:type threshold, track by_src, count 20, seconds 10; classtype:attempted-dos;
sid:7000001; rev:1);
```

Available Rule Categories	
Category	custom.rules
Select the rule category to view and manage.	

Defined Custom Rules	
<pre>alert tcp any any -> any 22 (msg:"SSH Brute Force Attack Detected"; flow:to_server; content:"SSH-"; depth:4; threshold:type threshold, track by_src, count 20, seconds 10; classtype:attempted-dos; sid:7000001; rev:1); alert tcp any any -> \$HOME_NET 80 (msg:"[DOS] Possible SYN Flood attack"; flags:S; threshold:type threshold, track by_src, count 20, seconds 10; classtype:attempted-dos; sid:7000002; rev:1);</pre>	

Hình 23 DDos rule

Thành phần	Mô tả
alert	Hành động của rule – tạo cảnh báo khi điều kiện khớp
tcp	Giao thức TCP
any any	Mọi địa chỉ IP nguồn, mọi cổng nguồn
->	Dòng dữ liệu đi từ client → server
\$HOME_NET 80	Đích: cổng 80 (HTTP) trên hệ thống nội bộ (\$HOME_NET)

Thành phần	Mô tả
msg:"[DOS] Possible SYN Flood attack"	Tin nhắn cảnh báo sẽ xuất hiện khi rule kích hoạt
flags:S;	Kiểm tra cờ SYN – tức là chỉ bắt các gói TCP SYN dùng để khởi tạo kết nối
threshold:type threshold, track by_src, count 20, seconds 10;	Nếu 1 địa chỉ IP nguồn gửi 20 gói SYN trong 10 giây → kích hoạt cảnh báo
classtype:attempted-dos	Phân loại mối đe dọa: tấn công từ chối dịch vụ
sid:7000001	ID của rule (unique Suricata rule identifier)
rev:1	Phiên bản rule (revision)

Test Rule

Trên máy attacker kali:

```
sudo hping3 -S -p 80 --flood 192.168.150.128
```

Lệnh này dùng để **tấn công SYN Flood** bằng cách gửi liên tục gói TCP SYN đến port 80 của IP 192.168.150.128 với tốc độ cực nhanh (flood), nhằm làm quá tải dịch vụ.

Trên suricata đã nhận được cảnh báo và tiến hành block máy attacker.

Báo Cáo Học Tập

Alert Log View Settings

Instance to View: (WAN) WAN
Choose which instance alerts you want to inspect.

Save or Remove Logs: Download Clear
All alert log files for selected interface will be downloaded
Clear the currently active Alerts log file

Save Settings: Save Refresh Default is ON
Save auto-refresh and view settings
Number of alerts to display. Default is 250

Alert Log View Filter

Last 250 Alert Entries. (Most recent entries are listed first)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
07/23/2025 14:21:43	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	39185	192.168.150.128	80	1:7000001	[DOS] Possible SYN Flood attack
07/23/2025 14:21:43	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	14164	192.168.150.128	80	1:7000001	[DOS] Possible SYN Flood attack
07/23/2025 14:21:43	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	14069	192.168.150.128	80	1:7000001	[DOS] Possible SYN Flood attack
07/23/2025 14:21:43	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	14049	192.168.150.128	80	1:7000001	[DOS] Possible SYN Flood attack
07/23/2025 14:21:43	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	14029	192.168.150.128	80	1:7000001	[DOS] Possible SYN Flood attack
07/23/2025 14:21:43	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	14008	192.168.150.128	80	1:7000001	[DOS] Possible SYN Flood attack

Hình 24 Alert Ddos

Services / Suricata / Blocked Hosts

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Interfaces Global Settings Updates Alerts **Blocks** Files Pass Lists Suppress Logs View Logs Mgmt SID Mgmt

Sync IP Lists

Blocked Hosts Log View Settings

Save or Remove Hosts: Download Clear
All blocked hosts will be saved
All blocked hosts will be cleared

Save Settings: Save Refresh Default is ON
Save auto-refresh and view settings
Number of blocked entries to view.
Default is 500

Last 500 Hosts Blocked by Suricata

Note: Only blocked IP addresses from Legacy Mode interfaces are shown! For inline IPS mode interfaces, dropped IP addresses are highlighted on the ALERTS tab.

Blocked IP	Block Date/Time	Block Alert Description	Block Rule GID:SID	Remove Block
192.168.150.129	07/23/2025 14:21:09 07/23/2025 14:10:57	[DOS] Possible SYN Flood attack SSH Brute Force Attack Detected	1:7000001 1:1000004	X

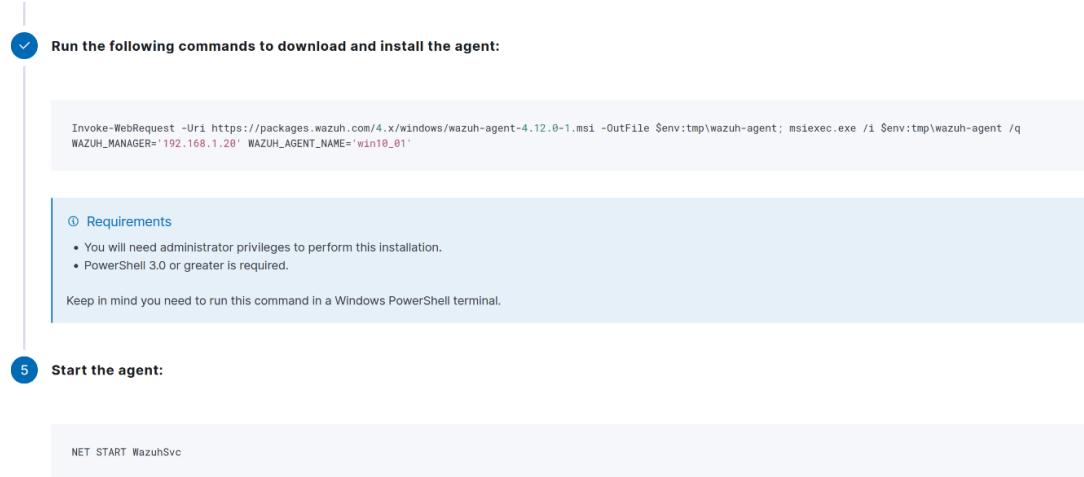
1 host IP address is currently being blocked.

Hình 25 Blocks tab

d/ Endpoint rule

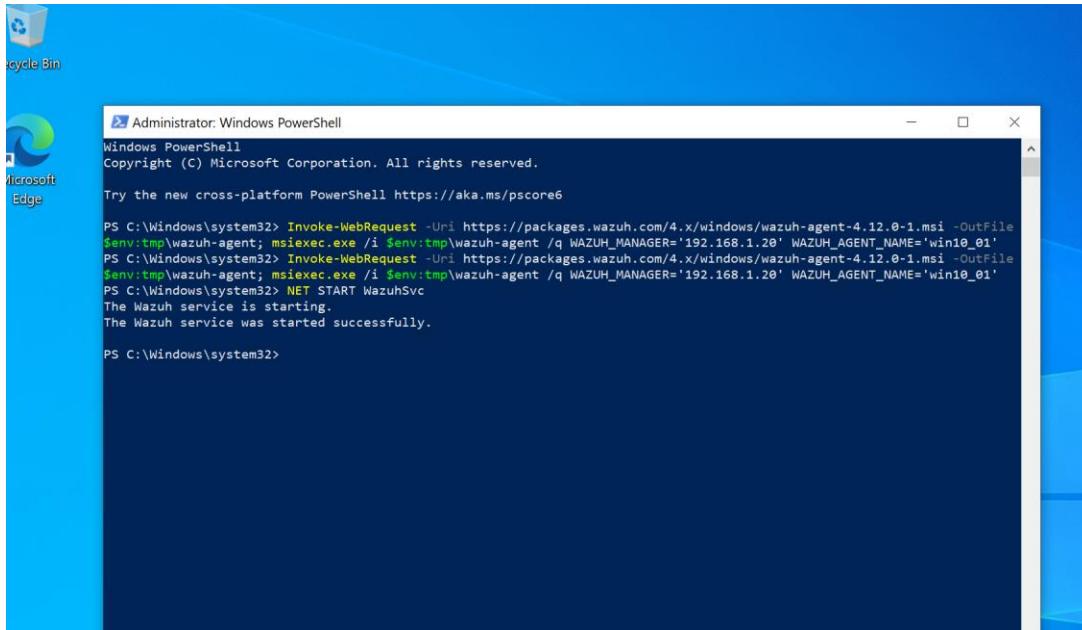
d.1 Detecting and removing malware using VirusTotal integration

Tiến hành nhập các thông tin cần thiết để Wazuh khởi tạo lệnh Deploy agent



Hình 26 Deploy new agent trên Wazuh

Tiến hành copy và chạy các lệnh trên máy Agent.



Hình 27 PowerShell win10

Danh sách các Agent đã kết nối thành công đến Wazuh server

Agents (3)									
Show only outdated									
Deploy new agent Refresh Export formatted More									
Search WQL									
ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions	
001	win10_01	192.168.2.11	default	Microsoft Windows 10 Home 10.0.19045.6093	node01	v4.12.0	disconnected	Reconnect	...
002	win10_2	192.168.2.12	default	Microsoft Windows 10 Home 10.0.19045.2965	node01	v4.12.0	disconnected	Reconnect	...
003	ubuntu_01	192.168.2.10	default	Ubuntu 24.04.2 LTS	node01	v4.12.0	disconnected	Reconnect	...

Hình 28 Wazuh server

Cấu hình trong file C:\Program Files (x86)\ossec-agent\ossec.conf

Chắc chắn <disable> là no

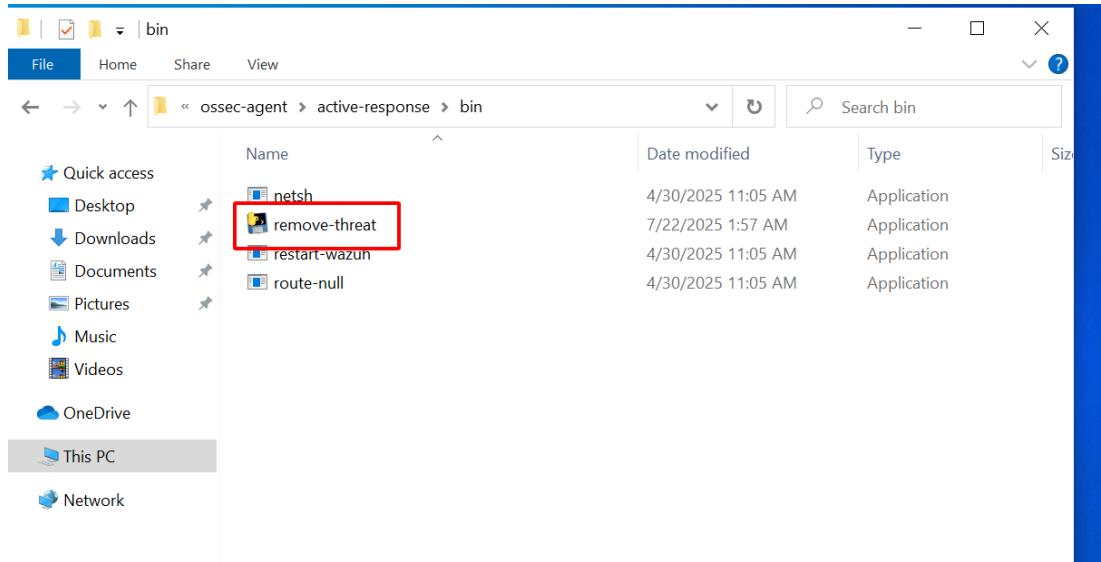
Thêm <directories realtime="yes">C:\Users<USER_NAME>\Downloads</directories> vào ossec.conf

```
<!-- Agent buffer options -->
<client_buffer>
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
</client_buffer>

<!-- Log analysis -->
```

Hình 29 ossec.conf

Tiến hành viết một file remove-threat.py để xóa malware. Sử dụng pyinstaller để khởi tạo thành file remove-threat.exe và copy file .exe vào thư mục C:\Program Files (x86)\ossec-agent\active-response\bin



Hình 30 Thư mục lưu remove-threat.exe

Cuối cùng reset Wazuh agent.

Trên Wazuh server tiến hành sửa file /var/ossec/etc/ossec.conf

Cấu hình này giúp Wazuh tự động gửi hash file bị thay đổi lên VirusTotal để kiểm tra mã độc thông qua API.

```
<ossec_config>
  <integration>
    <name>virustotal</name>
    <api_key><YOUR_VIRUS_TOTAL_API_KEY></api_key> <!-- Replace with your own API key -->
    <group>syscheck</group>
    <alert_format>json</alert_format>
  </integration>
</ossec_config>
```

Hình 31 ossec.conf

Cấu hình này cho phép Wazuh **tự động chạy file remove-threat.exe trên máy cục bộ** khi có cảnh báo với **ID rule 87105**, để xử lý hoặc gỡ bỏ mối đe dọa.

```
<ossec_config>
  <command>
    <name>remove-threat</name>
    <executable>remove-threat.exe</executable>
    <timeout_allowed>no</timeout_allowed>
  </command>

  <active-response>
    <disabled>no</disabled>
    <command>remove-threat</command>
    <location>local</location>
    <rules_id>87105</rules_id>
  </active-response>
</ossec_config>
```

Hình 32 ossec.conf

Sau đó chỉnh sửa trên file /var/ossec/etc/rules/local_rules.xml

Rule 100092 phát hiện khi Wazuh **đã loại bỏ mã độc thành công**, hiển thị tên chương trình và vị trí file.

Rule 100093 phát hiện khi **xóa thất bại**, ghi lại lỗi và đường dẫn file nghỉ ngò.

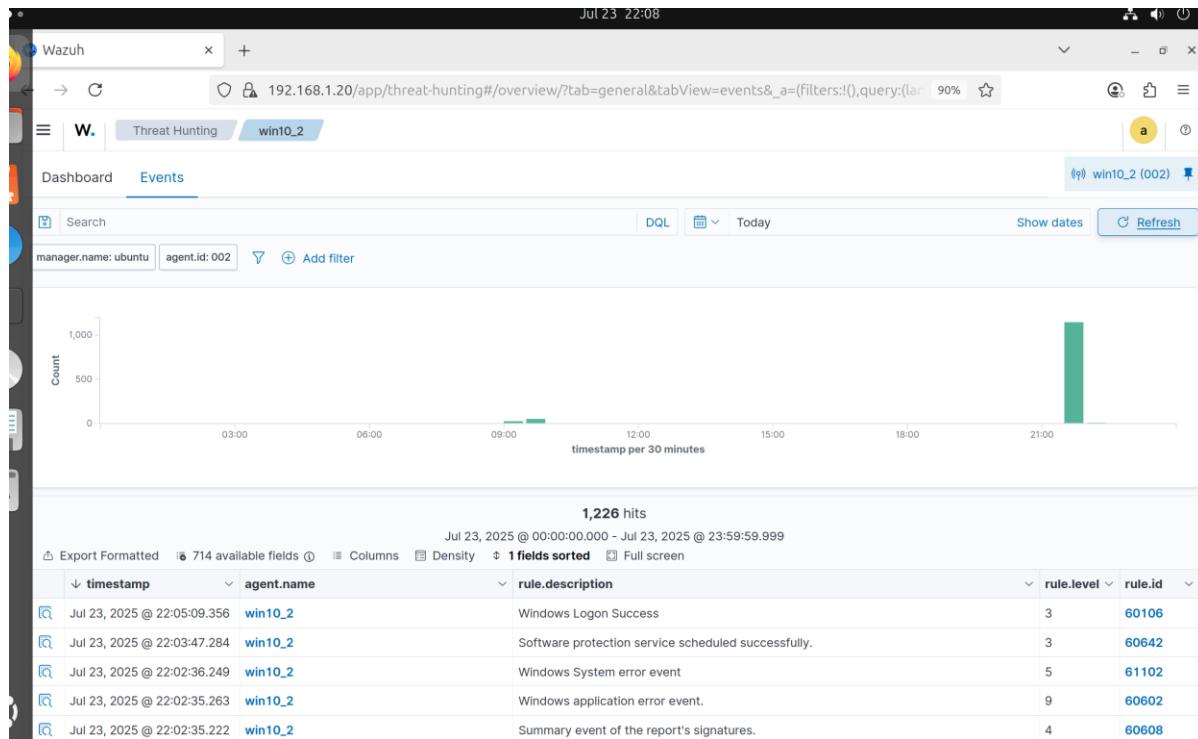
```
<group name="virustotal,">
  <rule id="100092" level="12">
    <if_sid>657</if_sid>
    <match>Successfully removed threat</match>
    <description>$(parameters.program) removed threat located at $(|</description>
  </rule>

  <rule id="100093" level="12">
    <if_sid>657</if_sid>
    <match>Error removing threat</match>
    <description>Error removing threat located at $(parameters.alert.|</description>
  </rule>
</group>
```

Hình 33 local_rules.xml

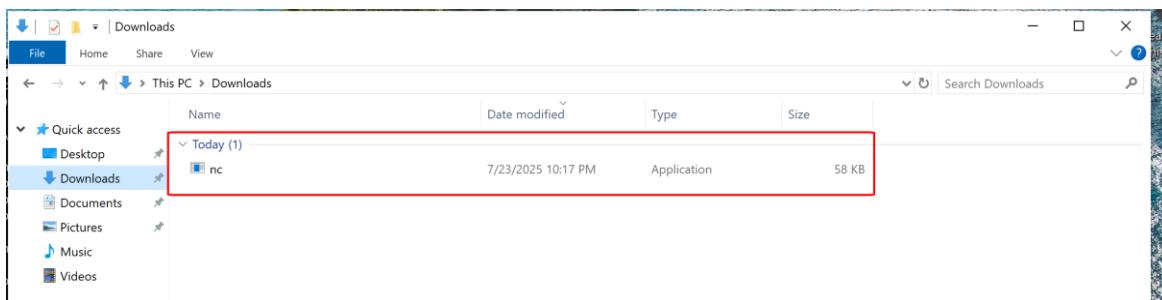
Cuối cùng reset lại Wazuh server

Mở tab Threat Hunting để theo dõi cảnh báo



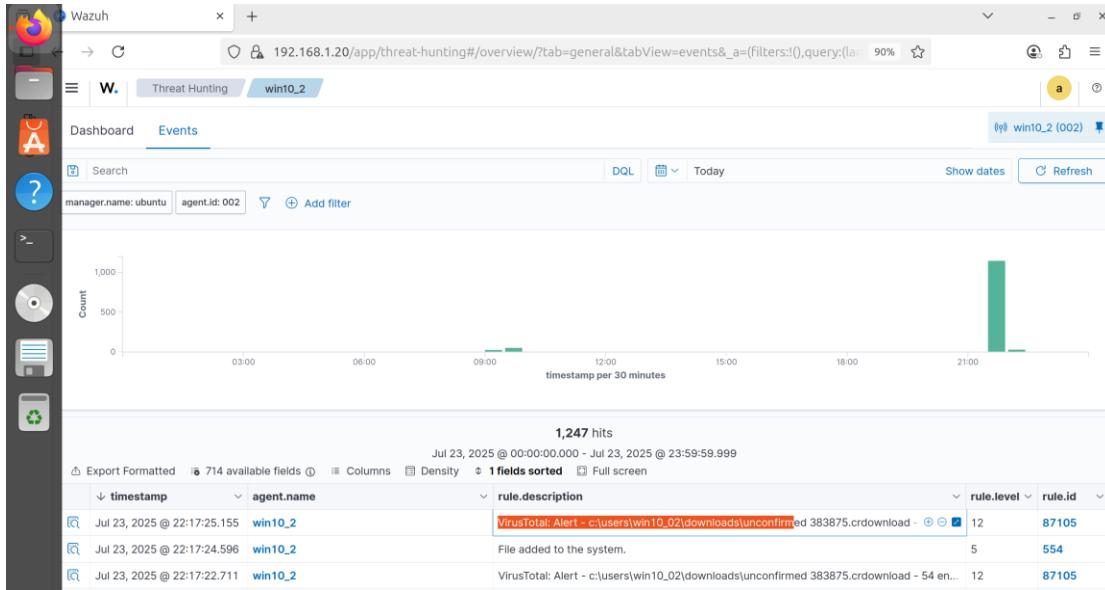
Hình 34 Threat Hunting

Trên máy agent tải file lạ



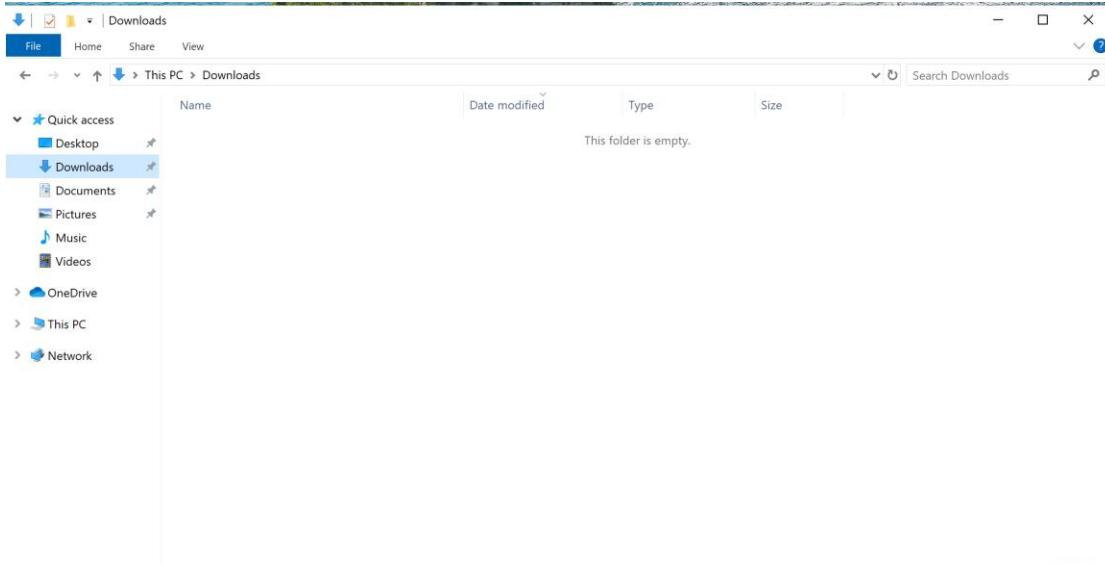
Hình 35 win10

Trên wazuh đã nhận được cảnh báo.



Hình 36 Threat Hunting Virustotal

Và file lạ sau khi xác nhận là malware đã bị xóa

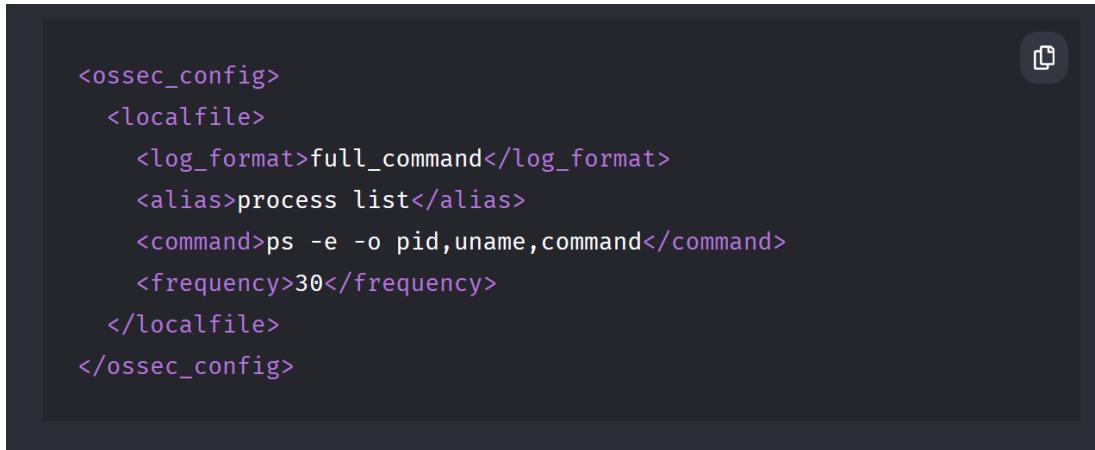


Hình 37 Download

d.2 Detecting unauthorized processes

Trên ubuntu endpoint tiến hành sửa cấu hình file /var/ossec/etc/ossec.conf

Cấu hình này giúp Wazuh thu thập danh sách tiến trình đang chạy (process list) trên hệ thống mỗi 30 giây bằng lệnh ps.



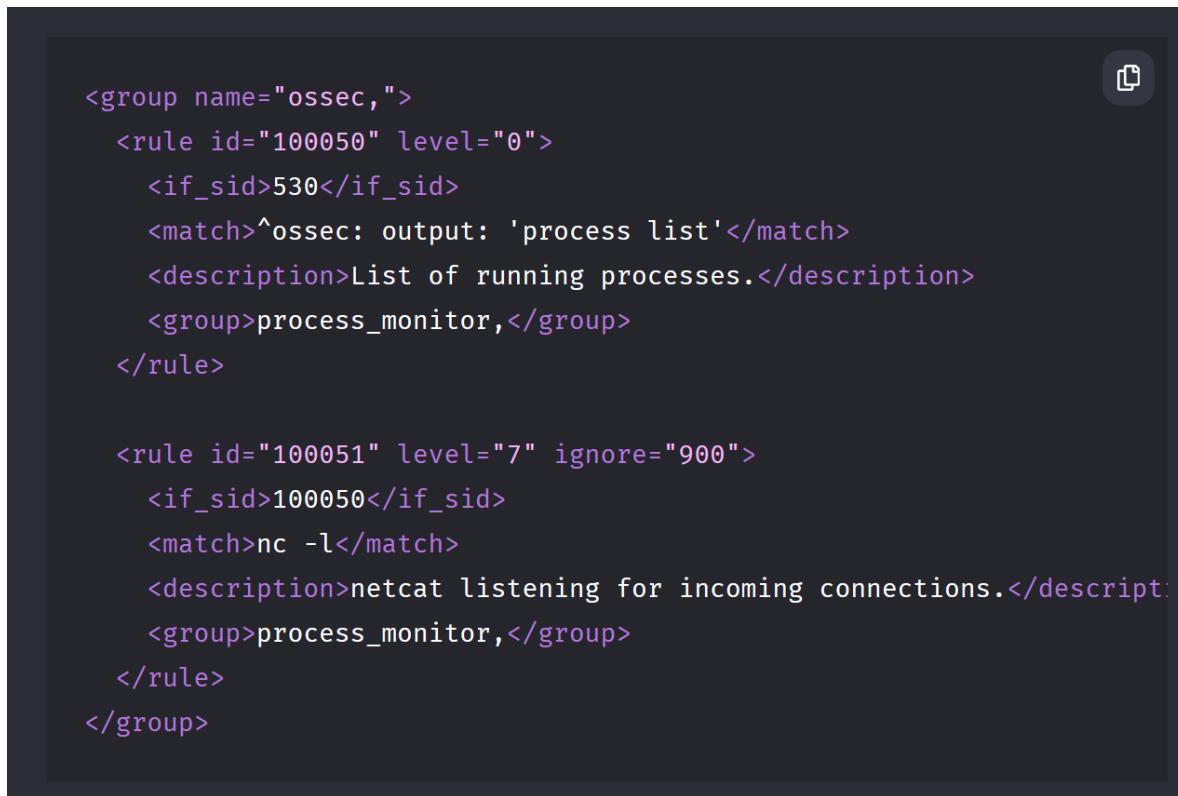
```
<ossec_config>
  <localfile>
    <log_format>full_command</log_format>
    <alias>process list</alias>
    <command>ps -e -o pid,uname,command</command>
    <frequency>30</frequency>
  </localfile>
</ossec_config>
```

Hình 38 ossec.conf

Sau đó tiến hành reset agent

Trên Wazuh servser tiến hành cấu hình file /var/ossec/etc/rules/local_rules.xml

Cấu hình này tạo rule cho Wazuh để **giám sát tiến trình**, cảnh báo nếu phát hiện lệnh nguy hiểm như nc -l (netcat đang nghe kết nối).



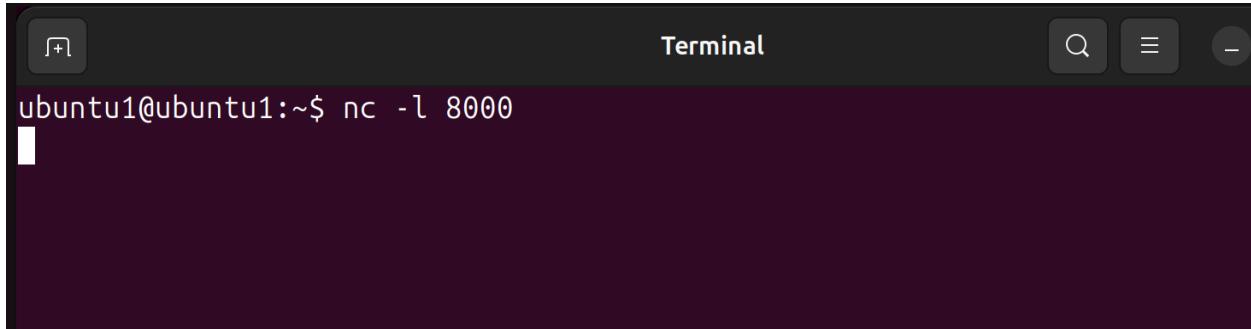
```
<group name="ossec,">
  <rule id="100050" level="0">
    <if_sid>530</if_sid>
    <match>^ossec: output: 'process list'</match>
    <description>List of running processes.</description>
    <group>process_monitor,</group>
  </rule>

  <rule id="100051" level="7" ignore="900">
    <if_sid>100050</if_sid>
    <match>nc -l</match>
    <description>netcat listening for incoming connections.</description>
    <group>process_monitor,</group>
  </rule>
</group>
```

Hình 39 local_rules.xml

Trên máy agent dùng lệnh nc -l 8000

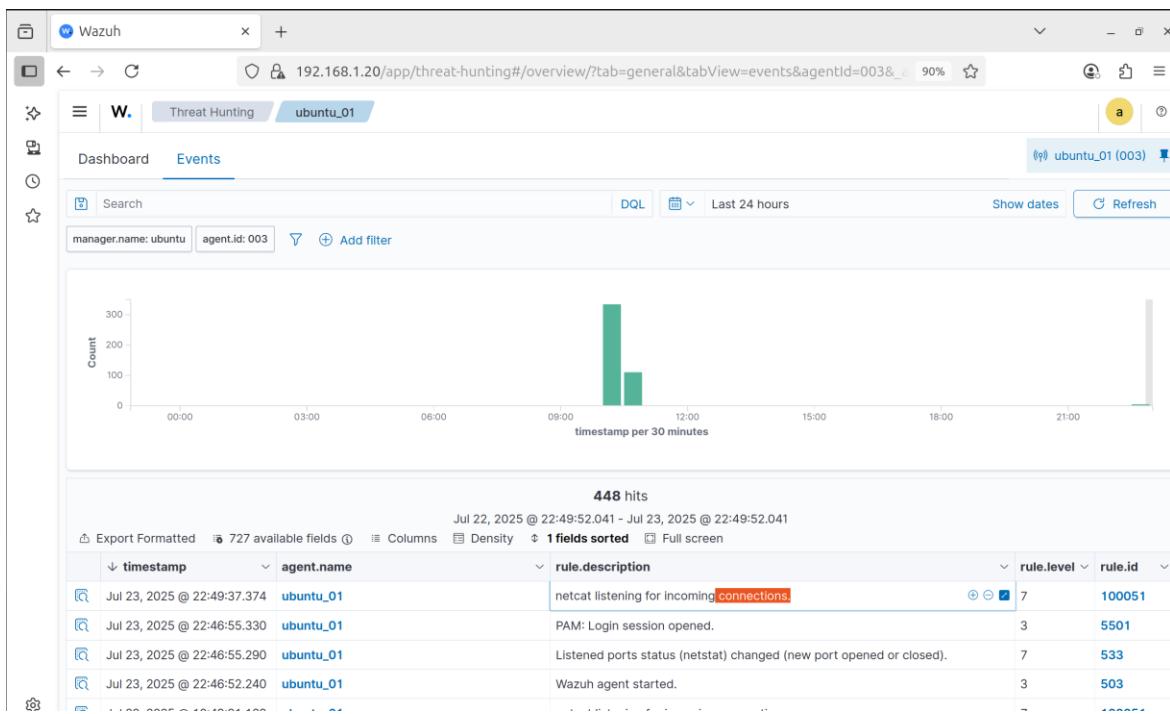
Lệnh nc -l 8000 dùng để **mở một cổng lắng nghe kết nối đến** bằng công cụ nc (Netcat), một công cụ dòng lệnh mạnh mẽ dùng cho việc gửi và nhận dữ liệu qua mạng.



```
ubuntu1@ubuntu1:~$ nc -l 8000
```

Hình 40 Ubuntu Agent

Trên máy Wazuh server mở Threat Hunting để giám sát Event và đã thấy sự kiện netcat.



Hình 41 Threat Hunting

e/ Kịch bản tấn công

e.1 Tấn công DDOS

Giới thiệu:

Tấn công từ chối dịch vụ phân tán (**DDoS – Distributed Denial of Service**) là hình thức tấn công mạng nhằm **làm gián đoạn hoặc khiến dịch vụ không thể truy cập được** bằng cách **tạo ra lượng lớn lưu lượng truy cập giả mạo** đến hệ thống mục tiêu.

Do trong hệ thống này mọi đường mạng đều thông qua firewall để kết nối đến với nhau. Nên em sẽ tiến hành tấn công ddos vào firewall pfsense để làm gián đoạn hệ thống mạng.

Các bước tấn công:

B1: Attacker sử dụng kali để và công cụ hping3 để gửi hàng ngàn gói TCP SYN đến cổng WAN của pfsense

```
kali㉿kali:~
```

File Actions Edit View Help

```
[kali㉿kali:~] ~
```

```
sudo hping3 -S -p 80 --flood 192.168.150.128
```

Hình 42 cmd kali

B2: Sau đó hệ thống mạng sẽ bị gián đoạn gây lag trên toàn hệ thống. Thủ kết nối từ máy Ubutu từ opt1 ra Internet thì thấy kết nối không ổn định

```
ubuntu1@ubuntu1:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=1252 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=208 ms
^C
--- 8.8.8.8 ping statistics ---
16 packets transmitted, 2 received, 87.5% packet loss, time 15444ms
rtt min/avg/max/mdev = 207.691/729.643/1251.595/521.952 ms, pipe 2
ubuntu1@ubuntu1:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
```

Hình 43 cmd Ubuntu

B3: Suricata nhận được alert và tiến hành block máy attacker

Báo Cáo Học Tập

The screenshot shows the 'Alert Log View Settings' section of the Suricata interface. It includes fields for selecting the instance to view (WAN WAN), saving or removing logs, and setting the number of alerts to display (250). Below this is the 'Alert Log View Filter' section, which displays a table of 'Last 250 Alert Entries'. The table columns include Date, Action, Pri, Proto, Class, Src, SPort, Dst, DPort, GID:SID, and Description. All entries show a SYN Flood attack from 192.168.150.129 to 192.168.150.128 on port 80.

Last 250 Alert Entries. (Most recent entries are listed first)										
Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
07/23/2025 19:39:34	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	37589	192.168.150.128	80	1:7000001	[DOS] Possible SYN Flood attack
07/23/2025 19:39:34	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	37569	192.168.150.128	80	1:7000001	[DOS] Possible SYN Flood attack
07/23/2025 19:39:34	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	37549	192.168.150.128	80	1:7000001	[DOS] Possible SYN Flood attack
07/23/2025 19:39:34	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	37529	192.168.150.128	80	1:7000001	[DOS] Possible SYN Flood attack
07/23/2025 19:39:34	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	37509	192.168.150.128	80	1:7000001	[DOS] Possible SYN Flood attack
07/23/2025 19:39:34	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	37489	192.168.150.128	80	1:7000001	[DOS] Possible SYN Flood attack

Hình 44 Alert suricata

The screenshot shows the 'Blocked Hosts Log View Settings' section of the Suricata interface. It includes fields for saving or removing hosts, and setting the number of blocked entries to view (500). Below this is the 'Last 500 Hosts Blocked by Suricata' section, which displays a table of blocked IP addresses. The table columns include Blocked IP, Block Date/Time, Block Alert Description, Block Rule GID:SID, and Remove Block. The table shows multiple entries for 192.168.150.129, mostly related to SYN Flood attacks and SSH Brute Force attacks.

Last 500 Hosts Blocked by Suricata				
Blocked IP	Block Date/Time	Block Alert Description	Block Rule GID:SID	Remove Block
192.168.150.129	07/23/2025 19:46:06	[DOS] Possible SYN Flood attack	1:7000001	X
	07/23/2025 19:24:33	SSH Brute Force Attack Detected	1:1000004	
	07/23/2025 19:03:35	[DOS] Possible SYN Flood attack	1:7000001	
	07/23/2025 14:21:09	[DOS] Possible SYN Flood attack	1:7000001	
	07/23/2025 14:10:57	SSH Brute Force Attack Detected	1:1000004	

Hình 45 Blocks tab

Kết quả: Suricata đã phát hiện được hành vi tấn công DDOS vào hệ thống mạng làm hệ thống mạng bị trì trệ. Khi đó suricata đã tiến hành block máy tấn công.

e.2 Tấn công gửi malware qua email

Giới thiệu:

Tấn công gửi malware qua email là hình thức lừa nạn nhân mở file đính kèm nháp vào liên kết độc hại trong email giả mạo. Khi thực hiện, mã độc sẽ được cài lên máy nạn nhân, giúp kẻ tấn công kiểm soát thiết bị, đánh cắp dữ liệu hoặc lan rộng trong hệ thống. Đây là hình thức tấn công phổ biến vì tận dụng yếu tố con người – thường là mắt xích yếu nhất trong bảo mật.

B1: Attacker sẽ gửi một email gắn link hoặc tập tin chứa virus đến máy tính nạn nhân



Khải Trần <quangkhaiktwor@gmail.com>

đến tôi ▾

Chào bạn,

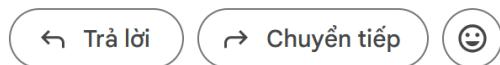
Bộ phận IT cần bạn tải và chạy công cụ kiểm tra kết nối mạng để đảm bảo hệ thống hoạt động ổn định.

Vui lòng tải tại đây: <http://192.168.150.129:8000>

Sau khi tải, bấm đúp để chạy.

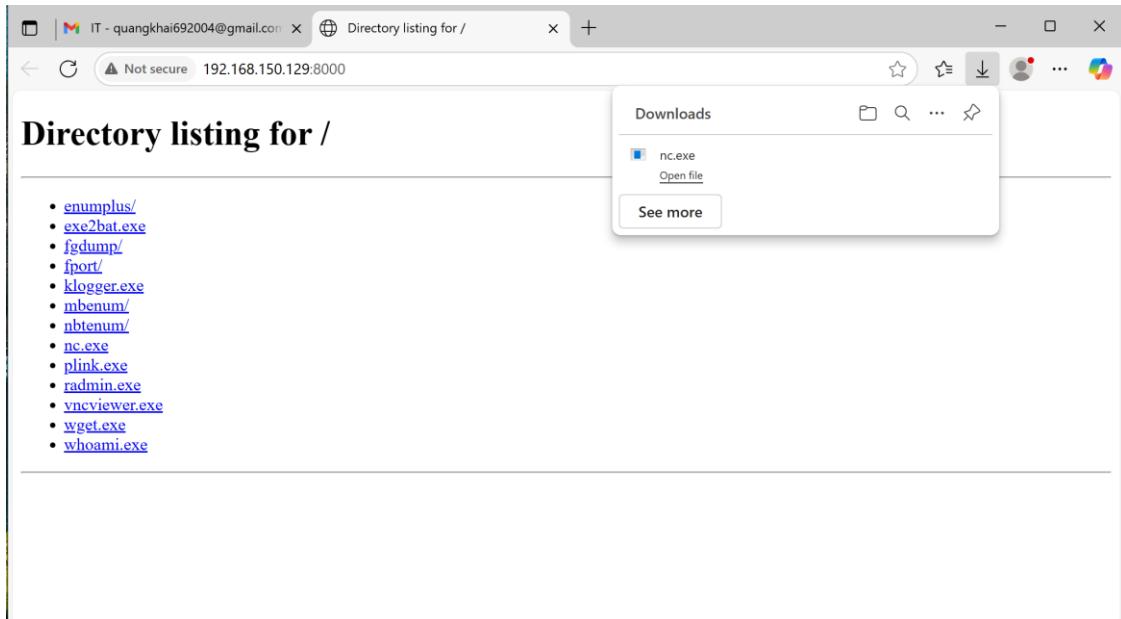
Cảm ơn bạn đã hợp tác!

IT Support



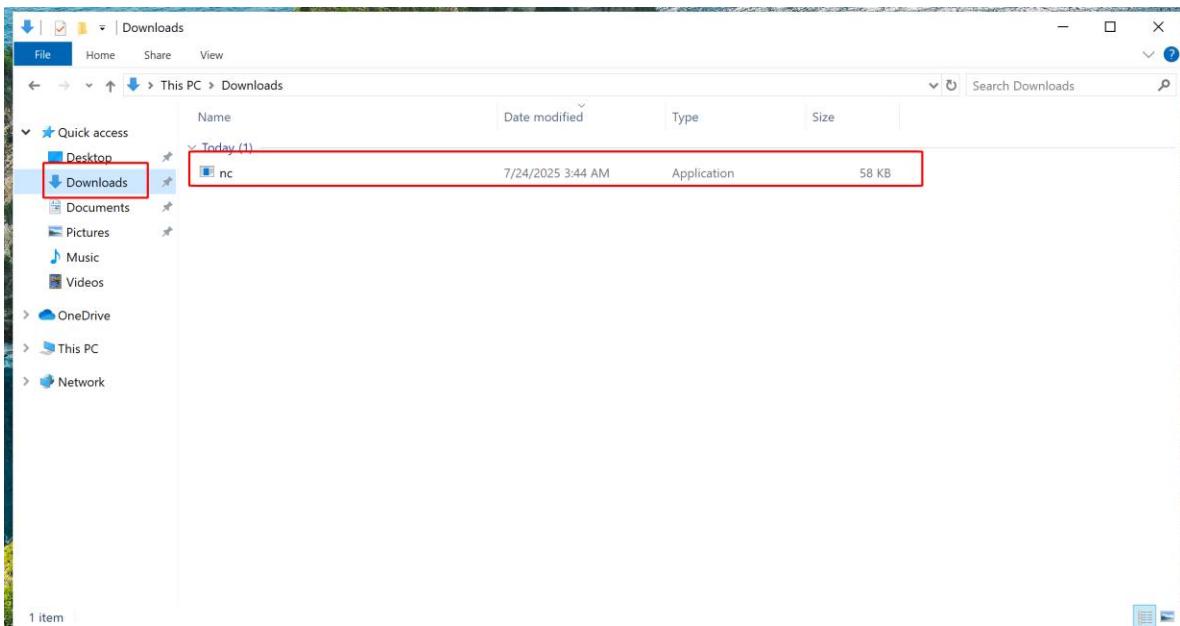
Hình 46 Mail

B2: Đối với những người không có kinh nghiệm thì họ sẽ tin đó là thật liền truy cập link và tiến hành tải các file mà ko biết đó là virus.



Hình 47 Tải malware

Và malware thường sẽ được lưu ở Download



Hình 48 DownLoad

B3: Lúc này Wazuh sẽ gửi file lên Virustotal để phân tích và phát hiện đây là file độc hại

Báo Cáo Học Tập

The screenshot shows a threat hunting interface with the following details:

- Timestamp:** Jul 23, 2025 @ 03:51:06.979 - Jul 24, 2025 @ 03:51:06.979
- Agent:** win10_2
- Hits:** 1,381
- Fields:** timestamp, agent.name, rule.description, rule.level, rule.id
- Row 1 (highlighted):** Jul 24, 2025 @ 03:48:31.685 win10_2. Rule description: VirusTotal: Alert - c:\users\win10_02\downloads\nc.exe - 54 engines detected ... Rule level: 12, Rule ID: 87105.
- Row 2:** Jul 24, 2025 @ 03:48:31.693 win10_2. Rule description: Integrity checksum changed. Rule level: 7, Rule ID: 550.
- Row 3:** Jul 24, 2025 @ 03:48:55.286 win10_2. Rule description: VirusTotal: Alert - c:\users\win10_02\downloads\nc.exe - 54 engines detected ... Rule level: 12, Rule ID: 87105.
- Row 4:** Jul 24, 2025 @ 03:48:49.065 win10_2. Rule description: Windows Logon Success. Rule level: 3, Rule ID: 60106.
- Row 5:** Jul 24, 2025 @ 03:48:20.807 win10_2. Rule description: Service startup type was changed. Rule level: 3, Rule ID: 61104.
- Row 6:** Jul 24, 2025 @ 03:45:53.524 win10_2. Rule description: Windows application error event. Rule level: 9, Rule ID: 60602.
- Row 7:** Jul 24, 2025 @ 03:45:53.069 win10_2. Rule description: Summary event of the report's signatures. Rule level: 4, Rule ID: 60608.
- Row 8:** Jul 24, 2025 @ 03:45:44.274 win10_2. Rule description: Windows Logon Success. Rule level: 3, Rule ID: 60106.
- Row 9:** Jul 24, 2025 @ 03:44:49.810 win10_2. Rule description: Software protection service scheduled successfully. Rule level: 3, Rule ID: 60642.
- Row 10:** Jul 24, 2025 @ 03:44:06.850 win10_2. Rule description: VirusTotal: Alert - c:\users\win10_02\downloads\nc.exe - 54 engines detected ... Rule level: 12, Rule ID: 87105.
- Row 11:** Jul 24, 2025 @ 03:44:03.171 win10_2. Rule description: Integrity checksum changed. Rule level: 7, Rule ID: 550.
- Row 12:** Jul 24, 2025 @ 03:44:01.406 win10_2. Rule description: VirusTotal: Alert - c:\users\win10_02\downloads\nc.exe - 54 engines detected ... Rule level: 12, Rule ID: 87105.
- Row 13:** Jul 24, 2025 @ 03:43:58.985 win10_2. Rule description: File added to the system. Rule level: 5, Rule ID: 554.
- Row 14:** Jul 24, 2025 @ 03:43:08.320 win10_2. Rule description: Software protection service scheduled successfully. Rule level: 3, Rule ID: 60642.
- Row 15:** Jul 24, 2025 @ 03:43:02.115 win10_2. Rule description: Windows Logon Success. Rule level: 3, Rule ID: 60106.

Hình 49 Cảnh báo

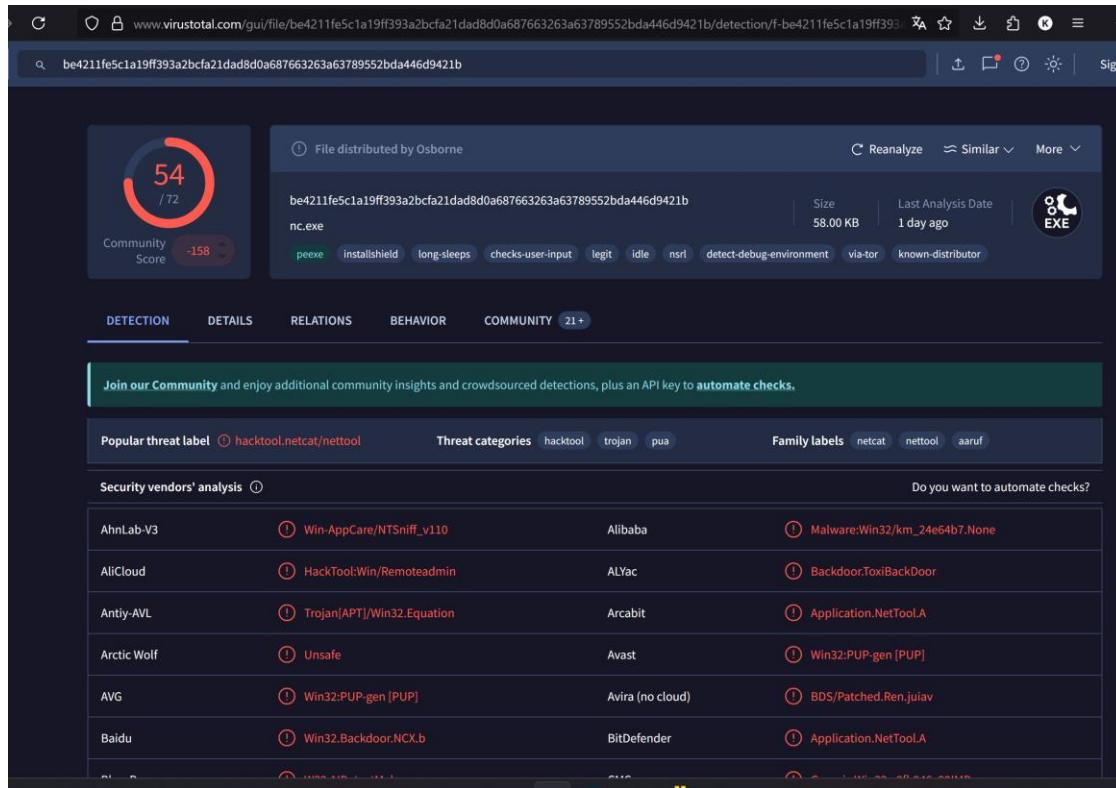
The screenshot shows a detailed view of a specific alert from the previous list:

Document Details

Table	JSON
t _index	wazuh-alerts-4.x-2025.07.23
t agent.id	002
t agent.ip	192.168.2.12
t agent.name	win10_2
t data.integration	virustotal
t data.virustotal.found	1
t data.virustotal.malicious	1
t data.virustotalpermalink	https://www.virustotal.com/gui/file/bcd211fe5ca10ff393a2bcfa21dada80a687663263a63789552bd946d9421fb/detection/f-bc4211fe5ca10ff393a2bcfa21dada80a687663263a63789552bd946d9421b-1753167763
t data.virustotal.positives	54
t data.virustotal.scan_date	2025-07-22 07:02:43
t data.virustotal.sha1	57f0839433234285cc9df96198a6ca58248a4707
t data.virustotal.source.alert	1753380438.567678
t data.virustotal._id	
t data.virustotal.source.file	c:\users\win10_02\downloads\nc.exe
t data.virustotal.source.md5	e0fb946cb0b140693e3cf5de258c22a1
t data.virustotal.source.sha1	57f0839433234285cc9df96198a6ca58248a4707

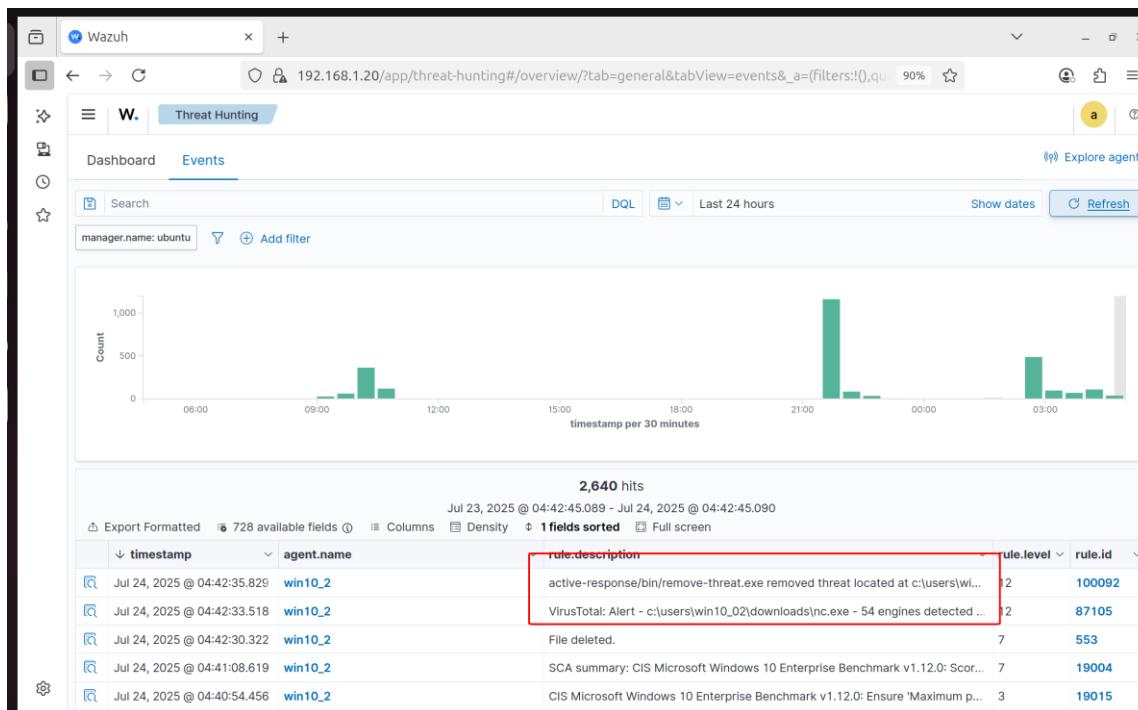
Hình 50 Chi tiết cảnh báo

Báo Cáo Học Tập

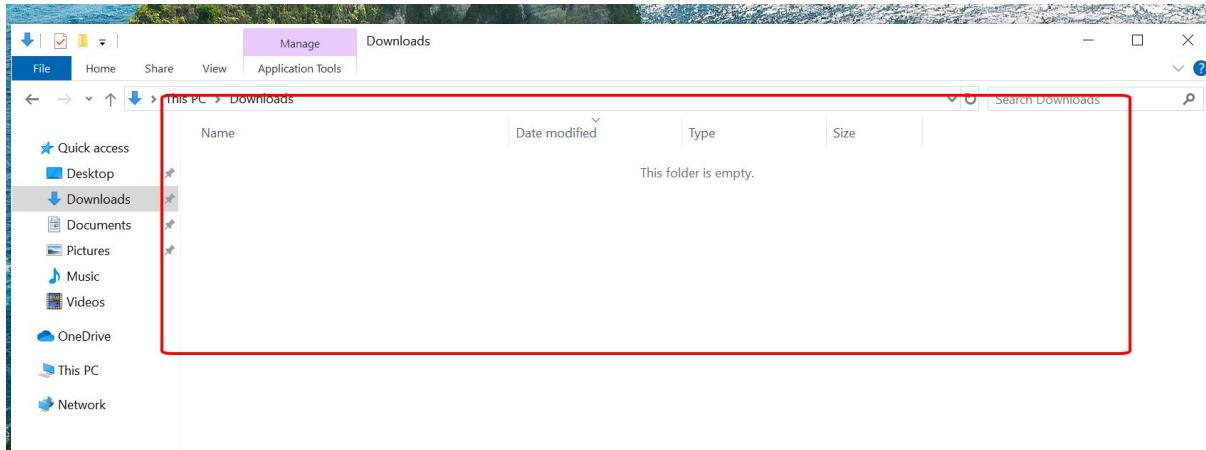


Hình 51 Kết quả trên VirusTotal

B4: Wazuh liên remove threat



Hình 52 Threat Hunting



Hình 53 DownLoad empty

Kết quả : Nhanh trong phát hiện và xóa bỏ virus trước khi nó có thể thực thi và lây lên trong hệ thống mạng.

e.3 Tấn công Brute-Force SSH

Giới thiệu:

Brute-force SSH là hình thức tấn công mạng trong đó kẻ tấn công **thử hàng loạt tên đăng nhập và mật khẩu** để đăng nhập trái phép vào hệ thống qua giao thức **SSH (Secure Shell)**.

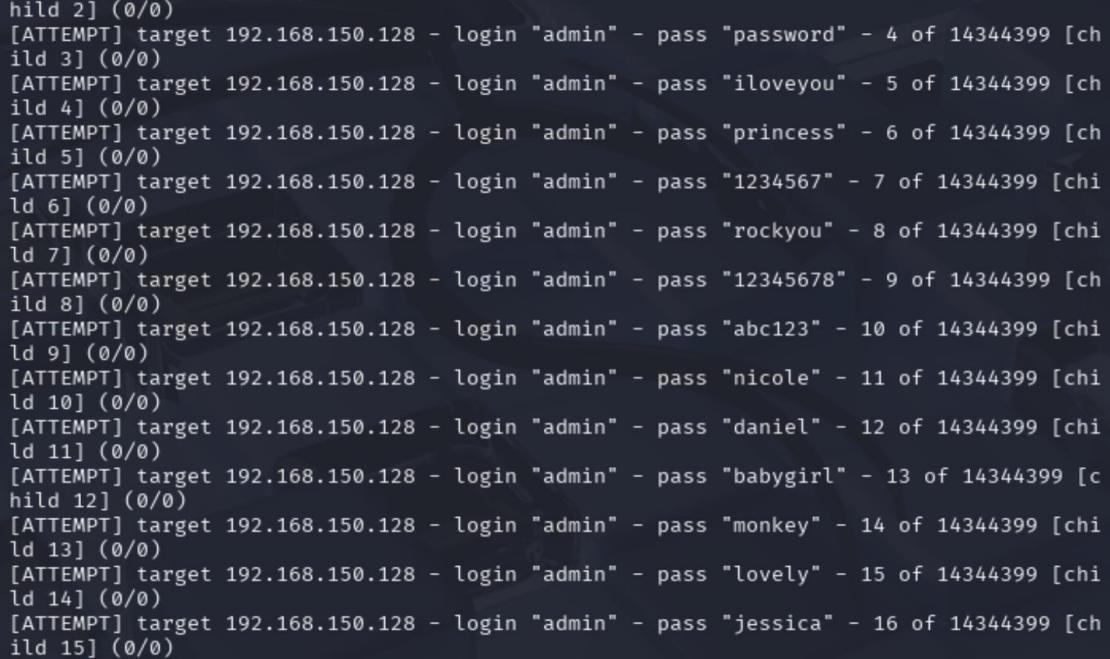
Giao thức SSH thường được dùng để quản lý từ xa các máy chủ Linux.

B1: Kẻ tấn công sử dụng **tool tự động** để:

- Thủ túng kết hợp username + password (hoặc từ danh sách có sẵn).
- Nhắm đến cổng **22/TCP** (cổng mặc định của SSH).
- Lặp lại hàng trăm hoặc hàng nghìn lần trong thời gian ngắn.

```
kali㉿kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.150.128 ssh -v
```

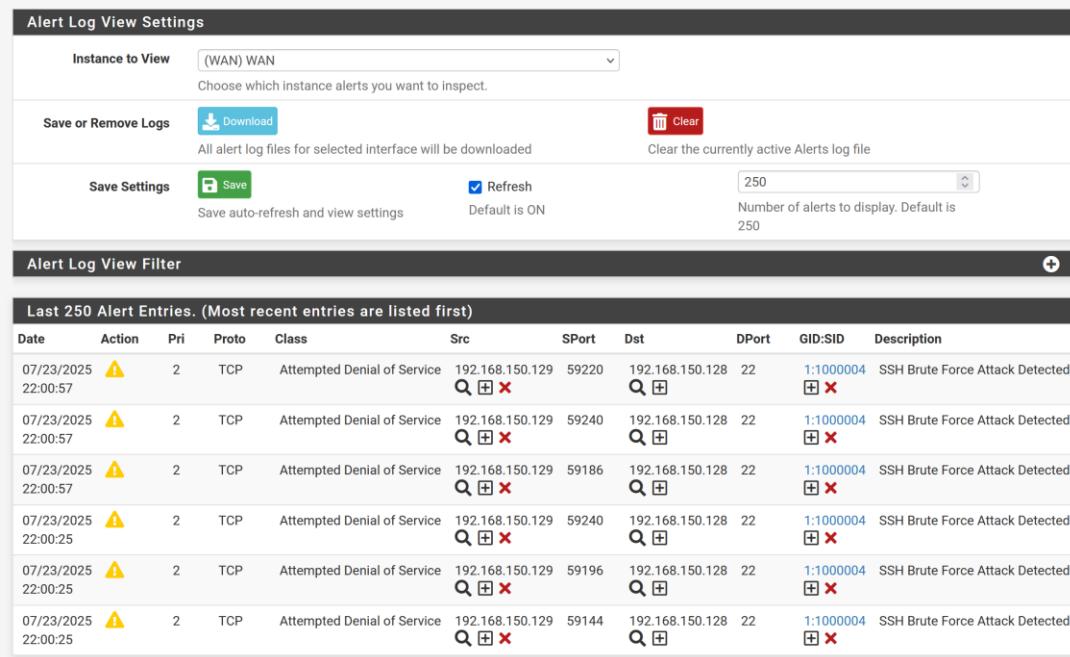
Hình 54 ssh brute force



```
kali@kali: ~
File Actions Edit View Help
hild 2] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.150.128 - login "admin" - pass "jessica" - 16 of 14344399 [child 15] (0/0)
```

Hình 55 Chi tiết tấn công

B2: Sau đó suricata sẽ có thể phát hiện và cảnh báo có tấn công SSH Brute Force.



Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
07/23/2025 22:00:57	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	59220	192.168.150.128	22	1:1000004	SSH Brute Force Attack Detected
07/23/2025 22:00:57	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	59240	192.168.150.128	22	1:1000004	SSH Brute Force Attack Detected
07/23/2025 22:00:57	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	59186	192.168.150.128	22	1:1000004	SSH Brute Force Attack Detected
07/23/2025 22:00:25	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	59240	192.168.150.128	22	1:1000004	SSH Brute Force Attack Detected
07/23/2025 22:00:25	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	59196	192.168.150.128	22	1:1000004	SSH Brute Force Attack Detected
07/23/2025 22:00:25	⚠️	2	TCP	Attempted Denial of Service	192.168.150.129	59144	192.168.150.128	22	1:1000004	SSH Brute Force Attack Detected

Hình 56 Alert

B3: Suricata tiến hành block máy attacker

The screenshot shows the Suricata interface with the 'Blocks' tab selected. At the top, there are tabs for Interfaces, Global Settings, Updates, Alerts, Blocks, Files, Pass Lists, Suppress, Logs View, Logs Mgmt, and SID Mgmt. Below these are Sync and IP Lists buttons. The main area is titled 'Blocked Hosts Log View Settings'. It includes buttons for Save or Remove Hosts (with Download and Clear options), Save Settings (with Save and Refresh checkboxes), and a dropdown for the number of blocked entries to view (set to 500). A note states: 'Note: Only blocked IP addresses from Legacy Mode interfaces are shown! For inline IPS mode interfaces, dropped IP addresses are highlighted on the ALERTS tab.' Below this is a table titled 'Last 500 Hosts Blocked by Suricata' showing a list of blocked IP addresses with their block dates, alert descriptions, and rule GID:SID. One entry is highlighted in red. A note at the bottom says '1 host IP address is currently being blocked.'

Hình 57 Blocks

B4: Từ đó phía bên Attacker không thể tiếp tục tấn công vào hệ thống nữa

The terminal window shows Hydra attack logs. A red box highlights several error messages related to SSH protocol errors and disabled child processes. The logs indicate that the target system is blocking connections due to errors. The final message shows the attack completed with no valid password found.

```
[VERBOSE] Disabled child 12 because of too many errors
[VERBOSE] Disabled child 13 because of too many errors
[VERBOSE] Disabled child 15 because of too many errors
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Timeout connecting to 192.168.150.128
[ERROR] could not connect to target port 22: Timeout connecting to 192.168.150.128
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Timeout connecting to 192.168.150.128
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Timeout connecting to 192.168.150.128
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Timeout connecting to 192.168.150.128
[ERROR] ssh protocol error
[VERBOSE] Disabled child 1 because of too many errors
[VERBOSE] Disabled child 6 because of too many errors
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Timeout connecting to 192.168.150.128
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Timeout connecting to 192.168.150.128
[VERBOSE] Disabled child 9 because of too many errors
[VERBOSE] Disabled child 10 because of too many errors
[ERROR] ssh protocol error
[VERBOSE] Disabled child 3 because of too many errors
[VERBOSE] Disabled child 11 because of too many errors
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-23 18:00:57
```

Hình 58 CMD kali

Kết quả: Phát hiện và ngăn chặn kịp thời hành vi tấn công ssh nhằm quản lý các máy nạn nhân từ xa.

IV/ Tổng kết

Hệ thống đã triển khai đạt được các chức năng chính như sau:

- **Giám sát lưu lượng mạng** và phát hiện các cuộc tấn công như SSH Brute Force, DDoS (SYN Flood) thông qua Suricata trên pfSense.
- **Giám sát máy trạm và máy chủ** với Wazuh, bao gồm:
 - Phát hiện tiến trình bất thường.
 - Phát hiện và xử lý phần mềm độc hại bằng tích hợp VirusTotal.
- **Phối hợp giữa Suricata và Wazuh** để phát hiện tấn công từ cả mạng và thiết bị đầu cuối, nâng cao khả năng bảo vệ hệ thống.