

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 KẾT THÚC HỌC PHẦN
QUẢN TRỊ HỆ THỐNG BẢO MẬT
ĐỀ TÀI : CHÍNH SÁCH BẢO MẬT DOANH NGHIỆP**

Giảng Viên Hướng Dẫn : ThS. Đỗ Phi Hưng
Sinh viên thực hiện:

- | | | |
|----|----------------------|------------|
| 1. | Nguyễn Vũ Anh Khoa | 22DH111684 |
| 2. | Lê Nguyễn Quốc Thanh | 22DH113286 |
| 3. | Phạm Đức Long | 22DH114617 |

Tp. Hồ Chí Minh - Ngày tháng năm 2025

LỜI CẢM ƠN

Lời nói đầu tiên, chúng em xin gửi lời cảm ơn chân thành nhất đến các thầy bộ môn **Bảo mật người dùng cuối** đã dành thời gian để truyền đạt những kiến thức quý báu cho chúng em trong quá trình học và làm đồ án. Bài đồ án cuối kỳ là cơ hội để chúng em áp dụng những kiến thức đã được thầy truyền dạy, giúp chúng em hiểu rõ hơn về môn học **Bảo mật người dùng cuối** cũng như các Chính sách bảo mật và có thêm kỹ năng làm việc nhóm.

Trong quá trình học tập và nghiên cứu, do bản thân em vẫn còn chưa vững kiến thức về chuyên ngành và kinh nghiệm thực tế nên có nhiều khi em còn thiếu sót nhưng nhờ có những lời chỉ dẫn, góp ý của các thầy đã giúp chúng em hoàn thành sản phẩm của mình một cách tốt nhất. Chúng em rất biết ơn các thầy vì đã dành thời gian để hướng dẫn chúng em trong quá trình thực hiện đồ án.

Chúng em xin gửi lời cảm ơn đặc biệt đến **Thầy Đỗ Phi Hưng** vì đã dành thời gian tận tình hướng dẫn và chia sẻ những kiến thức quý báu giúp chúng em từng bước một thực hiện đồ án, cảm ơn thầy suốt thời gian qua đã luôn góp ý cho chúng em từng chi tiết nhỏ trong đồ án cuối kỳ lần này, giúp đồ án của chúng em có thể hoàn chỉnh nhất.

Cuối cùng, chúng em xin gửi lời cảm ơn sâu sắc đến tất cả các thầy và các bạn đã đồng hành và hỗ trợ chúng em trong suốt quá trình thực hiện đồ án. Chúng em cảm thấy rất may mắn và tự hào khi có cơ hội được học cùng với những người thầy tận tâm như vậy.

Chúng em xin chân thành cảm ơn!

NHẬN XÉT CỦA GIẢNG VIÊN

(Của ThS Đỗ Phi Hưng)

Điểm: _____ (bằng chữ: _____)

,ngày tháng

năm 2025

GIÁO VIÊN

HƯỚNG DẪN

(ky, ho ten)

BẢNG CHỮ KÝ

Tác giả:

Tên: _____

Chữ ký: _____

Vị trí: _____

Ngày: _____

Tên: _____

Chữ ký: _____

Vị trí: _____

Ngày: _____

Tên: _____

Chữ ký: _____

Vị trí: _____

Ngày: _____

Người điều chỉnh:

Tên: _____

Chữ ký: _____

Vị trí: _____

Ngày: _____

Người duyệt:

Tên: _____

Chữ ký: _____

Vị trí: _____

Ngày: _____

Mục lục

LỜI CẢM ƠN.....	2
NHẬN XÉT CỦA GIÁNG VIÊN	3
BẢNG CHỮ KÝ.....	5
CHƯƠNG I: TỔNG QUAN VỀ BẢO MẬT NGƯỜI DÙNG CUỐI (ENDPOINT SECURITY)	11
1.1 Giới thiệu về Bảo mật người dùng cuối (Endpoint Security)	11
1.1.1. Khái niệm và vai trò	11
1.1.2. Tầm quan trọng của việc bảo vệ Endpoint trong môi trường hiện đại	12
1.1.3. Các thành phần chính của một hệ thống Endpoint	14
1.2. Các mối đe dọa chính đối với người dùng cuối	16
1.2.1. Phân loại các kiểu tấn công nhắm vào Endpoint	16
1.2.2. Xu hướng và thống kê về các cuộc tấn công Endpoint	19
1.3. Các chính sách và tiêu chuẩn bảo mật liên quan đến Endpoint.....	21
1.3.1. Giới thiệu tổng quan về các chính sách bảo mật	21
1.3.2. Vai trò của chính sách trong việc quản lý và bảo vệ Endpoint	22
CHƯƠNG II: CƠ SỞ LÝ THUYẾT	24
2.2.Sơ đồ vật lý , logic.....	24
2.2.1 Sơ đồ vật lý	24
2.2.2 Sơ đồ logic	24
2.3 Các bước triển khai IPS/IDS.....	25
2.3.1 Setup suricata trong pfsense	25
2.3.2. Video Demo	29
2.4 Các bước triển khai System Endpiont	29
2.4.1 Setup System Endpoint.....	29
2.4.2 Demo :	33
2.5. Kịch bản 1 : Tân Công DDOS	33
2.5.1 : Kịch bản tấn công Ddos :	33
2.5.2 : Các bước tấn công :	35
2.5.3 Tân công khi không phòng chống	37
2.5.4 : Video demo :	43
2.6 Kịch bản 2 : Tân công Fishing	44
2.6.1 Kịch bản mô phỏng Tân công Phishing và Phòng thủ với Wazuh/ClamAV :	44
2.6.2 Các bước tấn công :	45
2.6.3 Kết quả :	54

2.6.4 : Video Demo :.....	55
2.7 Kịch bản 3 : Tấn Brute Force	55
2.7.1 Kịch bản mô phỏng tấn công Brute Force :.....	55
2.7.2 Các bước tấn công :	57
2.7.3 Kết quả :.....	57
2.7.4 Video Demo	58
Chương III : Kết luận	59
3.1 : Các phương án bảo mật	59
3.1.1 : Khái niệm về Honeypot.....	59
3.1.2 : Cài và cấu hình Honeypot	59
3.1.3 : Kết quả.....	63
3.1.4 Video Demo :	66
TÀI LIỆU THAM KHẢO	67

DANH MỤC HÌNH ẢNH

Hình 1. Định nghĩa bảo Mật Người Dùng Cuối	11
Hình 2. Tầm quan trọng của việc bảo vệ ENDPOINT	12
Hình 3. Các thành phần chính của ENDPOINT	14
Hình 4. Các loại tấn công phổ biến	17
Hình 5. các loại VIRUS phổ biến	19
Hình 6. Tổng quan về chính sách bảo mật	21
Hình 7. Vai trò của ENDPOINT PROTECTION	22
Hình 8. Sơ đồ vật lý	24
Hình 9. Sơ đồ logic	24
Hình 10. Giao diện quản lý gói Suricata đã cài đặt trên pfSense.	25
Hình 11. Cấu hình kích hoạt và tùy chọn ghi nhật ký cho giao diện giám sát WAN của Suricata.	26
Hình 12. Cấu hình chế độ IPS và tùy chọn chặn tự động trong Suricata.	26
Hình 13. Định nghĩa các luật chặn tùy chỉnh (Custom Rules) trong Suricata.	27
Hình 14. Thực hiện quét cổng Nmap và Ddos từ máy tấn công.	27
Hình 15. Nhật ký các cảnh báo được ghi nhận bởi Suricata.	28
Hình 16. Danh sách các địa chỉ IP bị chặn bởi Suricata.	28
Hình 17. Kết quả ping từ máy người dùng bị chặn sau khi IPS hoạt động.	29
Hình 18. Thiết lập rule chống Brute Force trên Wazuh Manager	30
Hình 19. Định nghĩa lệnh Firewall-drop chống Brute Force	30
Hình 20. Cấu hình giám sát thư mục máy Agent trên Wazuh Manager	31
Hình 21. Tích hợp API của VirusTotal vào Wazuh Manager	31
Hình 22. Định nghĩa ID để báo Log về cho Wazuh Manager	32
Hình 23. Thiết lập rule xóa file chứa Virus	32
Hình 24. Thực thi cho lệnh remove-theat	33
Hình 25. Kết quả xóa Virus và báo Log lên Dashboard của Wazuh Manager	33
Hình 26. Cài đặt và xem trạng thái hoạt động của Nginx	35
Hình 27. Cấu hình Nginx và IP máy chủ Nginx được thiết lập để phục vụ trang web.	36
Hình 28. Truy xuất trang web từ máy Client	36
Hình 29. Các lệnh tấn công Ddos ở Layer 3, 4 & 7 trên Kali	37

Hình 30. Giám sát hệ thống khi bị Ddos	38
Hình 31. Kiểm tra SYN Flood bằng Netstat	39
Hình 32. Kết quả tấn công DDoS: Trang web không phản hồi	39
Hình 33. Cài đặt và khởi động nftables trên Ubuntu	40
Hình 34. Thiết lập rule cho nftables	40
Hình 35. Cấu hình rule anti Ddos Layer 7 trên Nginx	41
Hình 36. Cấu hình rule lọc các yêu cầu HTTP bất thường	41
Hình 37. Danh sách IP bị chặn (Blacklist DDoS - nftables)	42
Hình 38. Giám sát kết nối SYN_RECV – Kiểm tra tấn công DDoS TCP SYN	42
Hình 39. Phản hồi Log của Nginx khi bị Ddos ở Layer 7	43
Hình 40. Cài đặt Gophish trên máy Kali	45
Hình 41. Thực thi gophish để có thể truy cập vào giao diện	46
Hình 42. Giao diện chính của Gophish	46
Hình 43. Tạo 1 hồ sơ gửi chứa thông tin về máy Chủ SMTP trên Gophish	47
Hình 44. Tạo 1 trang giao diện có nút tải xuống trên Gophish	47
Hình 45. Tạo 1 mẫu Email để gửi đến nạn nhân	48
Hình 46. Tạo Users & Groups để thực hiện chiến dịch gửi email	48
Hình 47. Tạo 1 chiến dịch trên Campaigns	49
Hình 48. Email đã được gửi đến nạn nhân	49
Hình 49. File mã độc đã được tải về máy nạn nhân	50
Hình 50. Cấu hình giám sát thư mục Downloads trên máy Wazuh Agent	50
Hình 51. Rule cảnh báo phishing wazuh manager	51
Hình 52. Cài đặt ClamAV và Freshclam	51
Hình 53. Tạo 1 tệp quét Virus ClamAV theo thời gian thực	52
Hình 54. Kiểm tra hoạt động của ClamAV	52
Hình 55. File cấu hình dịch vụ clamav-realtime.service dùng cho systemd.	53
Hình 56. Wazuh manager báo log level 12 khi Agent tải file phishing	54
Hình 57. Kết quả quét virus khi nạn nhân tải về và ClamAV xóa	55
Hình 58. Tấn công brutce-force trên máy kali	57

Hình 59. Khi chưa triển khai bảo mật chống Brute Force	57
Hình 60. Thiết lập rule chống Brute Force	58
Hình 61. Cài đặt thư viện Python cần thiết	59
Hình 62. Clown Crowrie	60
Hình 63. Cài đặt môi trường cần thiết cho HoneyPot	60
Hình 64. Thực thi Crowrie	61
Hình 65. Cấu hình cowrie	61
Hình 66. Thiết lập rules agent báo log	62
Hình 67. Thiết lập rules báo log HoneyPot trên Wazuh-manager	62
Hình 68. Cổng lắng nghe trên HoneyPot	63
Hình 69. Tân công nmap trên kali đến HoneyPot	64
Hình 70. Kết quả tấn công Brute Force	64
Hình 71. Lệnh tấn công SSH trên Kali	65
Hình 72. Ghi lại log bên máy HoneyPot	66
Hình 73. Wazuh manager báo log	66

CHƯƠNG I: TỔNG QUAN VỀ BẢO MẬT NGƯỜI DÙNG CUỐI (ENDPOINT SECURITY)

1.1 Giới thiệu về Bảo mật người dùng cuối (Endpoint Security)

1.1.1. Khái niệm và vai trò



Hình 1. Định nghĩa bảo Mật Người Dùng Cuối

- Endpoint Security (Bảo mật người dùng cuối) hay Endpoint Protection là một phương pháp tiếp cận toàn diện để bảo vệ các thiết bị cuối (endpoints) như máy tính để bàn, máy tính xách tay, máy chủ, máy ảo, điện thoại thông minh và các thiết bị IoT khác khỏi các mối đe dọa mạng. Các thiết bị này thường là điểm truy cập của người dùng vào mạng của tổ chức, tạo ra các "điểm vào" tiềm năng cho kẻ tấn công.
- Vai trò: Mục tiêu chính của Endpoint Security là ngăn chặn, phát hiện và phản ứng trước các mối đe dọa tại cấp độ thiết bị, trước khi chúng có thể lan rộng vào mạng hoặc gây hại cho dữ liệu. Nó đi xa hơn các giải pháp chống virus truyền thống bằng cách tích hợp nhiều công nghệ bảo vệ nâng cao.

1.1.2. Tầm quan trọng của việc bảo vệ Endpoint trong môi trường hiện đại



Hình 2. Tầm quan trọng của việc bảo vệ ENDPOINT

Tầm quan trọng của việc bảo vệ Endpoint trong môi trường hiện đại:

1. Điểm yếu dễ bị tấn công nhất:

- Endpoint (máy tính, laptop, điện thoại, máy chủ, IoT devices) là điểm cuối mà người dùng tương tác trực tiếp với dữ liệu và hệ thống. Chúng thường là điểm yếu đầu tiên mà kẻ tấn công nhắm đến để xâm nhập vào mạng lưới.
- Sự đa dạng của các loại thiết bị và hệ điều hành trên endpoint tạo ra nhiều lỗ hổng tiềm ẩn.

2. Ngăn chặn sự lây lan của các mối đe dọa:

- Các cuộc tấn công hiện đại thường bắt đầu từ một endpoint đơn lẻ (ví dụ: qua email lừa đảo, tải xuống phần mềm độc hại).
- Bảo mật endpoint hiệu quả giúp phát hiện và ngăn chặn các mối đe dọa ngay tại nguồn, không cho phép chúng lây lan sang các hệ thống khác trong mạng.
- Giảm thiểu rủi ro từ các cuộc tấn công ransomware, mã độc, phần mềm gián điệp.

3. Bảo vệ dữ liệu nhạy cảm:

- Dữ liệu quan trọng và nhạy cảm (thông tin khách hàng, tài chính, sở hữu trí tuệ) thường được lưu trữ hoặc truy cập từ các endpoint.
- Việc mất mát hoặc rò rỉ dữ liệu từ endpoint có thể gây ra thiệt hại nghiêm trọng về tài chính, uy tín và pháp lý cho tổ chức.

4. Tuân thủ quy định và tiêu chuẩn:

- Nhiều quy định về bảo mật dữ liệu (như GDPR, HIPAA, PCI DSS) yêu cầu các tổ

chức phải có biện pháp bảo vệ mạnh mẽ cho dữ liệu trên endpoint.

- Việc tuân thủ không chỉ tránh được các khoản phạt mà còn xây dựng lòng tin với khách hàng và đối tác.

5. Hỗ trợ làm việc từ xa và mô hình Hybrid Work:

- Với sự gia tăng của làm việc từ xa và mô hình làm việc kết hợp (hybrid work), các endpoint không còn chỉ nằm trong phạm vi an toàn của văn phòng.
- Người dùng truy cập tài nguyên công ty từ nhiều địa điểm và mạng khác nhau, tăng cường bè mặt tấn công. Bảo mật endpoint trở nên cực kỳ quan trọng để đảm bảo an toàn cho dữ liệu khi truy cập từ xa.

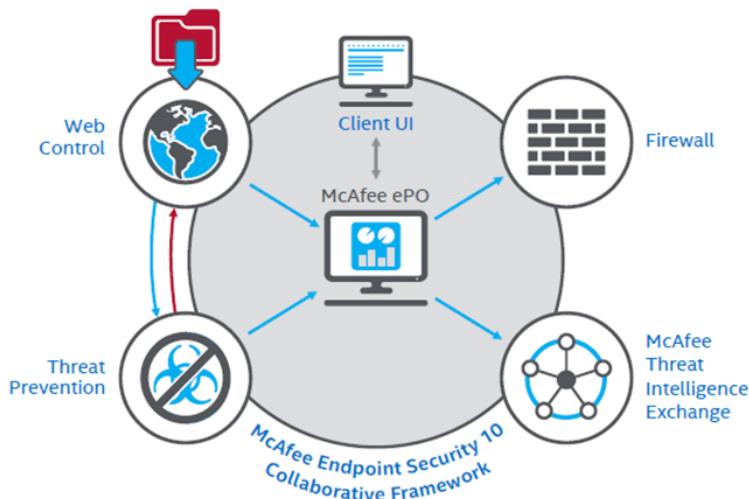
6. Tác động đến năng suất và hoạt động kinh doanh:

- Một cuộc tấn công thành công vào endpoint có thể làm gián đoạn hoạt động kinh doanh, gây mất năng suất của nhân viên.
- Phục hồi sau một cuộc tấn công có thể tốn kém và mất thời gian, ảnh hưởng đến lợi nhuận và sự liên tục của doanh nghiệp.

7. Sự phát triển của các mối đe dọa:

- Các mối đe dọa ngày càng tinh vi và đa dạng (tấn công không cần tệp, tấn công dựa trên kỹ thuật xã hội, APT).
- Bảo mật endpoint cần phải liên tục phát triển để đối phó với những thách thức mới này, sử dụng các công nghệ tiên tiến như AI/ML để phát hiện các mối đe dọa chưa từng biết đến.

1.1.3. Các thành phần chính của một hệ thống Endpoint Security



Hình 3. Các thành phần chính của ENDPOINT

Một hệ thống bảo mật Endpoint hiện đại thường tích hợp nhiều thành phần để tạo ra một lớp bảo vệ toàn diện, từ phòng ngừa đến phát hiện và phản ứng. Các thành phần chính bao gồm:

- **Chống Virus/Phần mềm độc hại (Antivirus/Anti-malware):**

- Mục đích: Phát hiện, ngăn chặn và loại bỏ các loại phần mềm độc hại phổ biến như virus, worm, trojan, spyware, adware, ransomware.
- Cách hoạt động: Sử dụng cơ sở dữ liệu chữ ký (signature-based), phân tích hành vi (heuristic/behavioral analysis), và gần đây là trí tuệ nhân tạo/học máy (AI/ML) để nhận diện các mối đe dọa.
- Tầm quan trọng: Là lớp bảo vệ cơ bản và không thể thiếu cho mọi endpoint.

- **Tường lửa Endpoint (Endpoint Firewall):**

- Mục đích: Kiểm soát lưu lượng mạng vào và ra khỏi endpoint, ngăn chặn truy cập trái phép và các kết nối độc hại.
- Cách hoạt động: Dựa trên các quy tắc được định nghĩa (ports, protocols, IP addresses) để cho phép hoặc chặn các kết nối.

- Tầm quan trọng: Giúp bảo vệ endpoint khỏi các cuộc tấn công từ mạng và kiểm soát dữ liệu đi ra ngoài.

- **Phát hiện và Phản hồi Endpoint (Endpoint Detection and Response - EDR):**

- Mục đích: Giám sát liên tục các hoạt động trên endpoint, phát hiện các hoạt động đáng ngờ hoặc tấn công phức tạp, và cung cấp khả năng phản ứng nhanh chóng.
- Cách hoạt động: Thu thập dữ liệu hoạt động (tiến trình, kết nối mạng, thay đổi hệ thống), sử dụng AI/ML để phân tích, phát hiện mối đe dọa, và cung cấp khả năng điều tra, cách ly, khắc phục từ xa.
- Tầm quan trọng: Nâng cao khả năng nhìn thấy (visibility) và phản ứng với các mối đe dọa tiên tiến (APTs, zero-day).

- **Bảo vệ Dựa trên Hành vi và Học máy (Behavioral & Machine Learning Protection):**

- Mục đích: Phát hiện các mối đe dọa mới, chưa từng được biết đến (zero-day exploits) và các cuộc tấn công không cần tệp (fileless attacks) bằng cách phân tích hành vi bất thường.
- Cách hoạt động: Học hỏi từ hành vi bình thường của hệ thống và người dùng, sau đó cảnh báo hoặc ngăn chặn bất kỳ hành vi nào lệch chuẩn.
- Tầm quan trọng: Bổ sung cho phương pháp dựa trên chữ ký, giúp đối phó với các cuộc tấn công tinh vi hơn.

- **Kiểm soát ứng dụng (Application Control):**

- Mục đích: Hạn chế các ứng dụng được phép chạy trên endpoint, ngăn chặn việc thực thi phần mềm trái phép hoặc độc hại.
- Cách hoạt động: Cho phép chỉ các ứng dụng trong danh sách trắng (whitelist) được chạy, hoặc chặn các ứng dụng trong danh sách đen (blacklist).
- Tầm quan trọng: Giảm thiểu bừa bãi tấn công và ngăn chặn việc cài đặt phần mềm độc hại hoặc không được ủy quyền.

- **Mã hóa dữ liệu (Data Encryption):**

- Mục đích: Bảo vệ dữ liệu nhạy cảm được lưu trữ trên endpoint (mã hóa ổ đĩa toàn bộ) hoặc dữ liệu đang truyền tải.

- Cách hoạt động: Chuyển đổi dữ liệu thành định dạng không thể đọc được nếu không có khóa giải mã.
- Tầm quan trọng: Đảm bảo an toàn dữ liệu ngay cả khi thiết bị bị mất cắp hoặc truy cập trái phép.

- **Kiểm soát thiết bị (Device Control):**

- Mục đích: Quản lý và hạn chế việc sử dụng các thiết bị ngoại vi (USB drives, ổ cứng ngoài, điện thoại) kết nối với endpoint.
- Cách hoạt động: Cho phép, chặn hoặc chỉ cho phép đọc/ghi đối với các loại thiết bị cụ thể.
- Tầm quan trọng: Ngăn chặn rò rỉ dữ liệu qua các thiết bị lưu trữ di động và ngăn chặn mã độc lây nhiễm qua USB.

- **Quản lý lỗ hổng (Vulnerability Management):**

- Mục đích: Phát hiện, đánh giá và ưu tiên khắc phục các lỗ hổng bảo mật trên endpoint (hệ điều hành, ứng dụng).
- Cách hoạt động: Quét các endpoint để tìm các bản vá lỗi còn thiếu, cấu hình sai hoặc các lỗ hổng đã biết.
- Tầm quan trọng: Giảm thiểu các điểm yếu có thể bị tấn công khai thác.

1.2. Các mối đe dọa chính đối với người dùng cuối

1.2.1. Phân loại các kiểu tấn công nhắm vào Endpoint



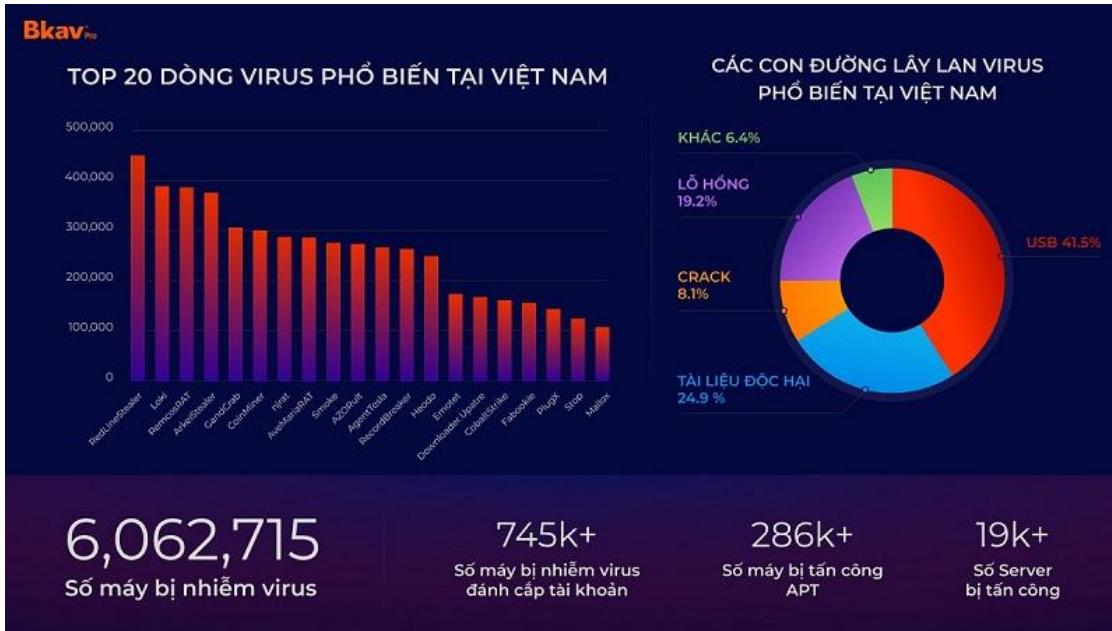
Hình 4. Các loại tấn công phổ biến

Các thiết bị đầu cuối (Endpoint) như máy tính, điện thoại, máy chủ là mục tiêu chính của nhiều loại tấn công mạng. Việc hiểu rõ các mối đe dọa này là rất quan trọng để bảo vệ hệ thống. Dưới đây là các kiểu tấn công phổ biến:

- **Phần mềm độc hại (Malware):** Là thuật ngữ chung cho mọi phần mềm được tạo ra với ý đồ xấu nhằm gây hại cho hệ thống, đánh cắp thông tin, hoặc kiểm soát thiết bị.
 - **Virus:** Chương trình tự nhân bản và lây lan bằng cách gắn vào các tệp hợp pháp, kích hoạt khi tệp bị mở.
 - **Ransomware (Mã độc tống tiền):** Mã hóa dữ liệu của nạn nhân và đòi tiền chuộc để giải mã.
 - **Trojan Horse (Ngựa thành Troy):** Ngụy trang thành phần mềm hữu ích để lừa người dùng cài đặt, sau đó thực hiện các hành vi độc hại ẩn giấu.
 - **Spyware (Phần mềm gián điệp):** Bí mật thu thập thông tin cá nhân và hoạt động của người dùng mà không được sự cho phép.
 - **Fileless Malware:** Hoạt động trực tiếp trong bộ nhớ của hệ thống mà không ghi tệp lên ổ đĩa, gây khó khăn cho việc phát hiện.
- **Tấn công dựa trên kỹ thuật xã hội (Social Engineering Attacks):** Các cuộc tấn công này lợi dụng tâm lý, sự thiếu cảnh giác của con người để lừa họ tiết lộ thông tin nhạy cảm hoặc thực hiện hành động có hại.

- **Phishing (Tấn công giả mạo):** Gửi email, tin nhắn hoặc tạo trang web giả mạo các tổ chức uy tín để lừa người dùng cung cấp thông tin đăng nhập hoặc dữ liệu cá nhân.
 - **Spear Phishing:** Một dạng phishing nhắm mục tiêu cụ thể vào cá nhân hoặc nhóm nhỏ, sử dụng thông tin riêng để tăng độ tin cậy.
 - **Vishing/Smishing:** Sử dụng cuộc gọi điện thoại (vishing) hoặc tin nhắn SMS (smishing) để thực hiện lừa đảo, thường yêu cầu nhấp vào liên kết độc hại hoặc cung cấp thông tin.
 - **Baiting (Tấn công bằng mồi nhử):** Dụ dỗ nạn nhân sử dụng các thiết bị hoặc tệp tin chứa mã độc (ví dụ: USB bị bỏ quên).
- **Khai thác lỗ hổng phần mềm (Exploiting Software Vulnerabilities):** Tận dụng các điểm yếu bảo mật trong hệ điều hành, trình duyệt hoặc ứng dụng để thực thi mã độc hoặc giành quyền truy cập trái phép.
- **Zero-day Exploits:** Khai thác các lỗ hổng bảo mật hoàn toàn mới, chưa được biết đến công khai và chưa có bản vá, khiến chúng cực kỳ nguy hiểm.
 - **Buffer Overflow/SQL Injection/XSS:** Các kỹ thuật khai thác lỗi lập trình phổ biến để chèn mã độc vào hệ thống hoặc ứng dụng.
- **Tấn công vật lý (Physical Attacks):** Liên quan đến việc tiếp cận trực tiếp thiết bị để đánh cắp dữ liệu, cài đặt mã độc hoặc gây thiệt hại.
- **Trộm cắp thiết bị:** Đánh cắp các thiết bị chứa dữ liệu quan trọng như laptop, điện thoại.
 - **Evil Maid Attack:** Kẻ tấn công lợi dụng việc có quyền truy cập vật lý ngắn ngủi vào thiết bị để cài đặt phần mềm độc hại.

1.2.2. Xu hướng và thống kê về các cuộc tấn công Endpoint



Hình 5. các loại VIRUS phổ biến

- Endpoint đang trở thành tâm điểm của các cuộc tấn công mạng, phản ánh sự thay đổi trong chiến thuật của tội phạm mạng và sự mở rộng của bề mặt tấn công. Việc phân tích xu hướng và thống kê là tối quan trọng để hiểu rõ bối cảnh đe dọa và định hình chiến lược phòng thủ hiệu quả.

1. Xu hướng Tăng cường và Đa dạng hóa Tấn công:

- **Sự gia tăng đáng kể về số lượng:** Các báo cáo an ninh mạng liên tục chỉ ra sự tăng vọt về số lượng các cuộc tấn công nhắm vào endpoint. Điều này đặc biệt đúng trong bối cảnh làm việc từ xa (remote work) và làm việc kết hợp (hybrid work) trở thành bình thường mới, làm mờ đi ranh giới bảo mật truyền thống.
- **Tính tinh vi và phức tạp:** Các cuộc tấn công ngày càng trở nên phức tạp hơn, sử dụng nhiều kỹ thuật kết hợp như kỹ thuật xã hội, khai thác lỗ hổng zero-day, và mã độc không tệp (fileless malware) để né tránh các giải pháp bảo mật truyền thống.
 - *Ví dụ minh họa:* Tấn công chuỗi cung ứng (supply chain attacks) nhắm vào phần mềm, hoặc các chiến dịch tấn công dai dẳng nâng cao (APT) thường bắt đầu từ một endpoint yếu kém.
- **Nhắm mục tiêu cụ thể (Targeted Attacks):** Thay vì các cuộc tấn công diện rộng, tội phạm mạng đang chuyển sang các cuộc tấn công nhắm mục tiêu vào các cá nhân hoặc bộ phận cụ thể trong tổ chức để tối đa hóa khả năng thành công và giá trị thu được.

- **Ví dụ minh họa:** Các cuộc tấn công Spear Phishing nhắm vào nhân sự cấp cao (Whaling) để lấy cắp thông tin nhạy cảm hoặc chiếm quyền điều khiển tài khoản.

2. Thông kê nổi bật về các Mối đe dọa chính:

- **Ransomware vẫn là mối đe dọa hàng đầu:** Dù có nhiều nỗ lực phòng chống, ransomware vẫn là một trong những mối đe dọa tồn kém và gây gián đoạn nhất cho các tổ chức.
- **Phishing và Kỹ thuật xã hội:** Đây là điểm khởi đầu cho phần lớn các cuộc tấn công endpoint thành công. Kẻ tấn công liên tục sáng tạo các chiêu trò lừa đảo để dụ dỗ người dùng click vào liên kết độc hại hoặc tải xuống phần mềm nguy hiểm.
- **Tăng cường tấn công Fileless và Zero-day:** Do các giải pháp bảo mật truyền thống tập trung vào tệp, kẻ tấn công ngày càng khai thác các kỹ thuật tấn công không cần tệp hoặc lợi dụng lỗ hổng chưa được biết (zero-day) để khó bị phát hiện hơn.

3. Tác động kinh tế và vận hành:

- **Chi phí thiệt hại khổng lồ:** Các cuộc tấn công endpoint gây ra thiệt hại đáng kể không chỉ về mặt tài chính (tiền chuộc, chi phí khắc phục, phạt vi phạm quy định) mà còn về uy tín, gián đoạn kinh doanh và mất mát dữ liệu.
- **Ảnh hưởng đến lòng tin và năng suất:** Sự cố an ninh làm suy giảm niềm tin của khách hàng và đối tác, đồng thời gây gián đoạn hoạt động, giảm năng suất làm việc của nhân viên.

4. Xu hướng bảo mật phản ứng:

- Để đối phó với các mối đe dọa ngày càng tinh vi, các giải pháp bảo mật endpoint đang dịch chuyển từ việc chỉ tập trung vào phòng ngừa sang khả năng **phát hiện và phản hồi nhanh cao (EDR/XDR)**, kết hợp trí tuệ nhân tạo (AI) và học máy (ML) để phân tích hành vi bất thường.
- Việc **đào tạo nhận thức an ninh mạng** cho người dùng cuối trở thành yếu tố then chốt, giúp họ trở thành tuyến phòng thủ đầu tiên chống lại các cuộc tấn công kỹ thuật xã hội.

1.3. Các chính sách và tiêu chuẩn bảo mật liên quan đến Endpoint

1.3.1. Giới thiệu tổng quan về các chính sách bảo mật



Hình 6. Tổng quan về chính sách bảo mật

- Chính sách bảo mật là tập hợp các quy tắc và hướng dẫn mà một tổ chức thiết lập để bảo vệ thông tin, hệ thống và tài sản công nghệ thông tin. Đối với Endpoint, chính sách này quy định cách người dùng và thiết bị tương tác với dữ liệu và mạng lưới để đảm bảo an toàn.

Mục đích chính của chính sách bảo mật Endpoint:

- **Định hướng và Chuẩn hóa:**
 - Cung cấp khuôn khổ rõ ràng cho việc sử dụng, cấu hình và bảo vệ Endpoint.
 - Giúp chuẩn hóa quy trình bảo mật, tránh lỗ hổng do quản lý không đồng nhất.
- **Giảm thiểu Rủi ro:**
 - Xác định các mối đe dọa tiềm ẩn.
 - Đề ra biện pháp kiểm soát để giảm thiểu sự cố như mất dữ liệu, xâm nhập.
- **Đảm bảo Tuân thủ:**
 - Giúp tổ chức đáp ứng các yêu cầu pháp lý (GDPR, HIPAA) và tiêu chuẩn ngành.
 - Tránh các khoản phạt tài chính và tổn hại danh tiếng.
- **Nâng cao Nhận thức Người dùng:**
 - Tuyên truyền về trách nhiệm của người dùng trong việc bảo vệ dữ liệu.
 - Hướng dẫn tuân thủ các quy tắc an toàn khi sử dụng thiết bị và truy cập tài nguyên.
- **Phản ứng và Khắc phục sự cố:**
 - Thiết lập quy trình rõ ràng cho việc phát hiện, phản ứng và khắc phục sự cố bảo mật trên Endpoint.
 - Giúp giảm thiểu thiệt hại và phục hồi hệ thống nhanh chóng.

Tầm quan trọng đối với Bảo mật Endpoint:

- Chính sách bảo mật là nền tảng cốt lõi cho mọi chiến lược bảo vệ Endpoint. Chúng đóng vai trò là "kim chỉ nam", giúp các giải pháp công nghệ phát huy hiệu quả tối đa. Một chính sách bảo mật rõ ràng, được thực thi tốt sẽ biến người dùng cuối thành tuyến phòng thủ chủ động, góp phần vào an ninh tổng thể của tổ chức.

1.3.2. Vai trò của chính sách trong việc quản lý và bảo vệ Endpoint



Hình 7. Vai trò của ENDPOINT PROTECTION

- Chính sách bảo mật đóng vai trò trung tâm và không thể thiếu trong việc quản lý hiệu quả và bảo vệ mạnh mẽ các thiết bị Endpoint trong một tổ chức. Chúng không chỉ là tài liệu hướng dẫn mà còn là công cụ chiến lược để xây dựng một môi trường an ninh vững chắc.
- **Thiết lập Ranh giới Sử dụng Rõ ràng:**

Chính sách quy định chi tiết những gì người dùng được phép và không được phép thực hiện trên các thiết bị Endpoint. Điều này bao gồm các quy tắc về việc sử dụng thiết bị lưu trữ di động (như USB), cài đặt phần mềm từ các nguồn không đáng tin cậy, hoặc các giới hạn về truy cập mạng. Mục đích là để người dùng hiểu rõ giới hạn và trách nhiệm của mình, từ đó hạn chế các hành vi tiềm ẩn rủi ro.

- **Chuẩn hóa và Đảm bảo Cấu hình An toàn:**

Một vai trò quan trọng của chính sách là đảm bảo rằng tất cả các Endpoint trong tổ chức đều được cấu hình theo cùng một tiêu chuẩn bảo mật nhất quán. Các chính sách này sẽ yêu cầu việc thiết lập mật khẩu mạnh, thực hiện cập nhật hệ điều hành và các

ứng dụng định kỳ, cũng như kích hoạt tường lửa. Điều này giúp loại bỏ các lỗ hổng phát sinh từ cấu hình sai sót hoặc thiếu sự đồng bộ.

- **Kiểm soát Chặt chẽ Truy cập và Bảo vệ Dữ liệu:**

Chính sách bảo mật định ra các quy định cụ thể về quyền truy cập của người dùng đối với các tài nguyên và dữ liệu nhạy cảm trên Endpoint. Các chính sách về phân quyền người dùng và yêu cầu mã hóa dữ liệu là những ví dụ điển hình, nhằm mục đích ngăn chặn hiệu quả việc truy cập trái phép và giảm thiểu nguy cơ rò rỉ thông tin quan trọng của tổ chức.

- **Phòng ngừa và Giảm thiểu Rủi ro Tấn công:**

Bằng cách thiết lập các quy tắc về hành vi an toàn khi duyệt web, cách nhận diện và đối phó với email lừa đảo (phishing), hoặc các quy định về việc không mở các tệp đính kèm đáng ngờ, chính sách bảo mật giúp người dùng tránh xa các mối đe dọa phổ biến. Điều này trực tiếp làm giảm bớt mối đe dọa và nguy cơ bị lây nhiễm mã độc vào hệ thống.

- **Hỗ trợ Phát hiện và Phản hồi Sự cố Nhanh chóng:**

Chính sách còn hướng dẫn việc ghi lại các hoạt động trên Endpoint (logging) và xác định các quy trình cụ thể để báo cáo, cũng như xử lý khi phát hiện các hành vi bất thường hoặc sự cố bảo mật. Điều này cải thiện đáng kể khả năng giám sát, cho phép tổ chức phản ứng nhanh chóng và hiệu quả hơn khi một mối đe dọa xuất hiện, giảm thiểu thiệt hại tiềm ẩn.

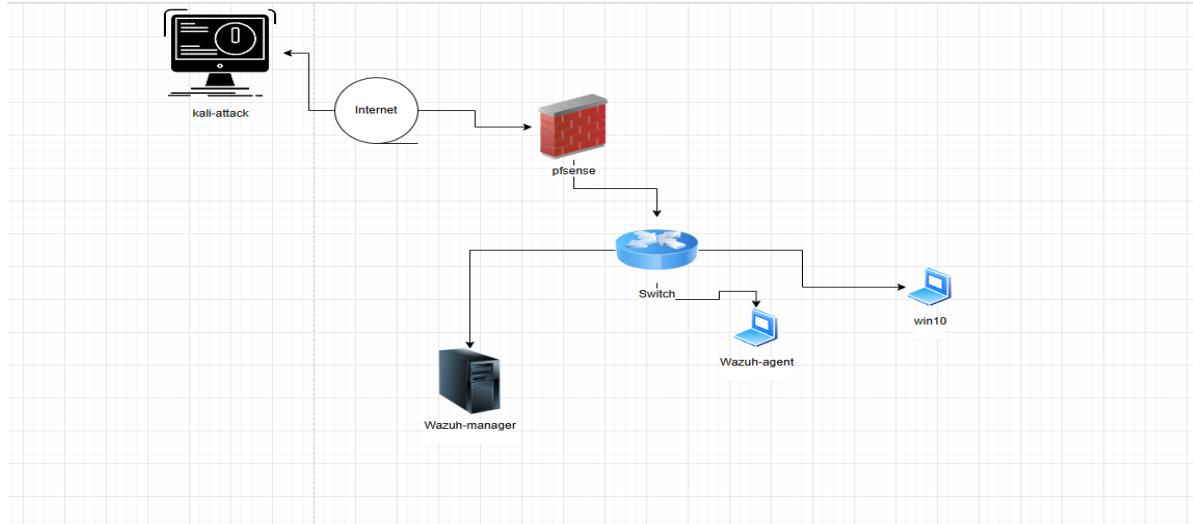
- **Xây dựng và Thúc đẩy Văn hóa An ninh:**

Cuối cùng, chính sách bảo mật đóng vai trò quan trọng trong việc nâng cao nhận thức và ý thức trách nhiệm về an ninh mạng cho toàn bộ nhân viên. Khi mỗi cá nhân hiểu và tuân thủ các quy tắc, họ trở thành một tuyến phòng thủ chủ động và hiệu quả, giúp xây dựng một môi trường làm việc an toàn và có trách nhiệm hơn cho cả tổ chức.

CHƯƠNG II: CƠ SỞ LÝ THUYẾT

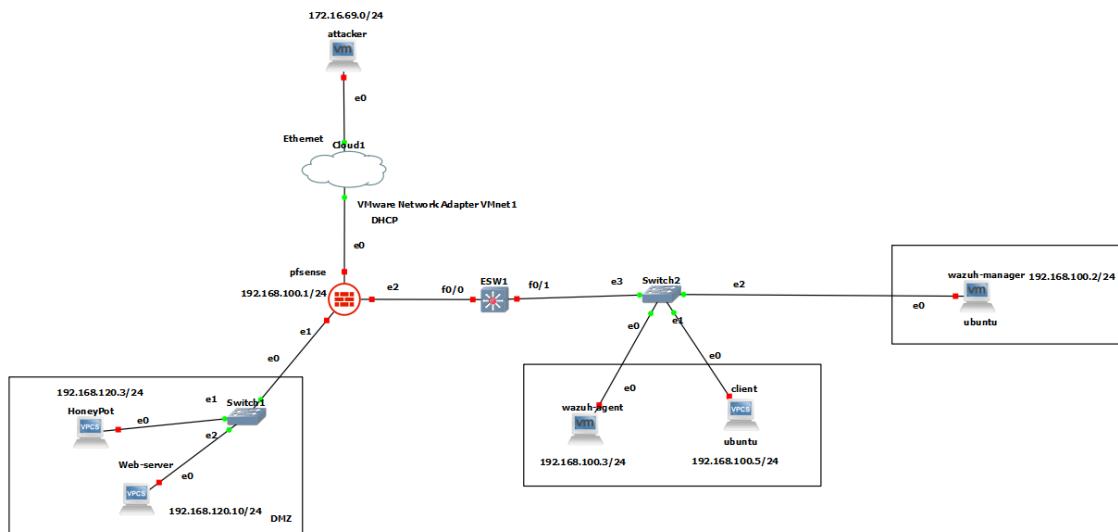
2.2. Sơ đồ vật lý, logic

2.2.1 Sơ đồ vật lý



Hình 8. Sơ đồ vật lý

2.2.2 Sơ đồ logic



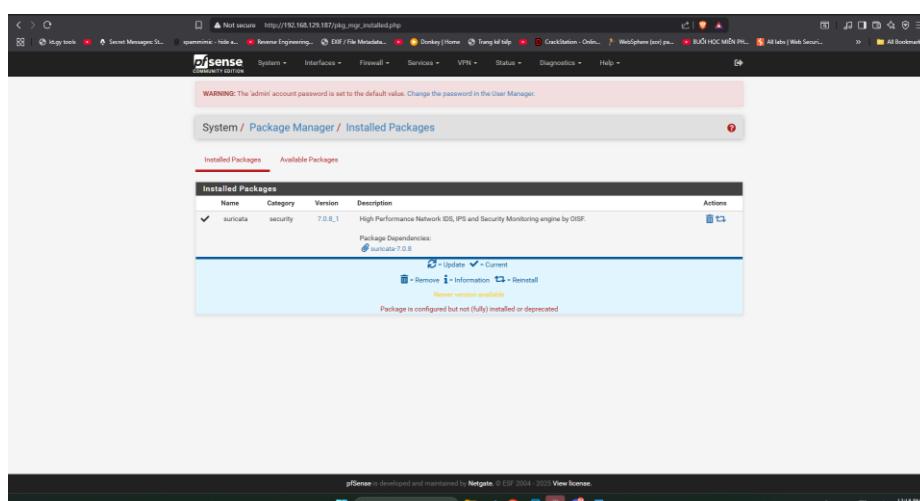
Hình 9. Sơ đồ logic

2.3 Các bước triển khai IPS/IDS

2.3.1 Setup suricata trong pfSense

Để thiết lập hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS) sử dụng Suricata trên pfSense, chúng ta cần thực hiện các bước cấu hình chi tiết như sau:

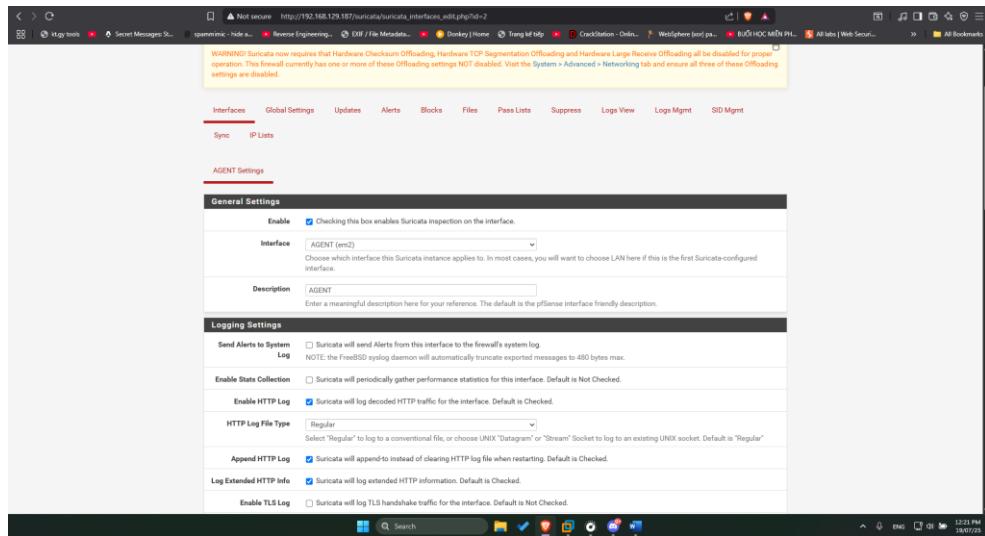
Bước 1 Cài gói Suricata



Hình 10. Giao diện quản lý gói Suricata đã cài đặt trên pfSense.

- Truy cập vào giao diện quản lý pfSense, điều hướng đến mục System -> Package Manager và chọn Available Packages. Tìm kiếm "Suricata" và tiến hành cài đặt.

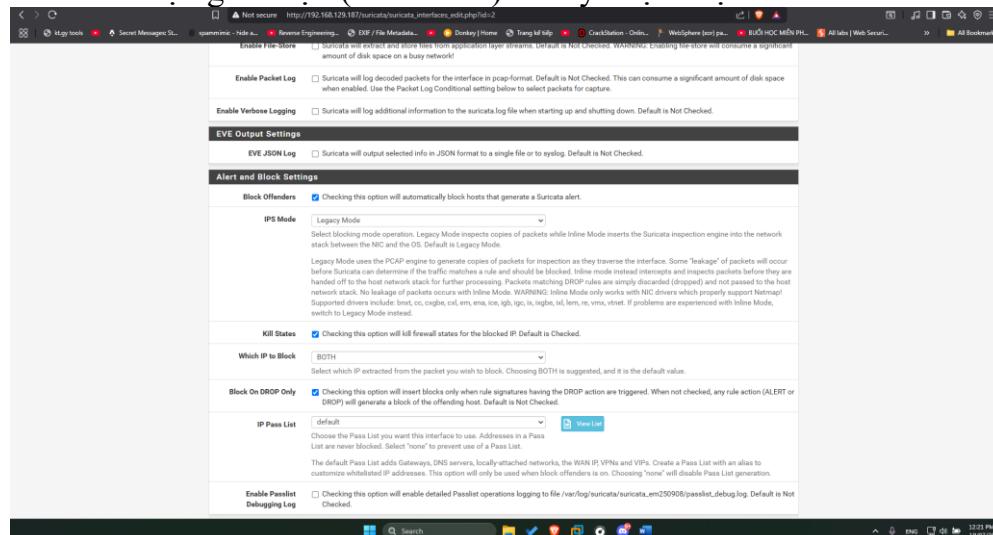
Bước 2 : Cấu hình Interface (Giao diện mạng) cho Suricata



Hình 11. Cấu hình kích hoạt và tùy chọn ghi nhật ký cho giao diện giám sát WAN của Suricata.

- Diều hướng đến Services -> Suricata -> Interfaces.Chọn giao diện mạng cho Suricata giám sát. Cấu hình các tùy chọn logging phù hợp để ghi lại các cảnh báo và hoạt động. Đặc biệt chú ý đến phần Alert Log View Settings và Logging Settings.

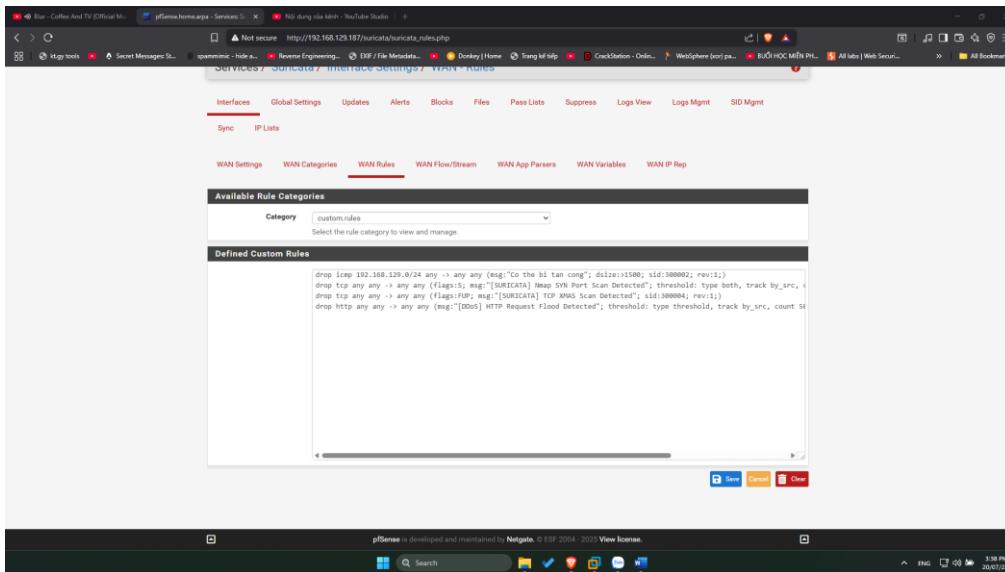
Bước 3 : Cấu hình chế độ ngăn chặn (IPS Mode) và tùy chọn chặn



Hình 12. Cấu hình chế độ IPS và tùy chọn chặn tự động trong Suricata.

- Alert and Block Settings trong cấu hình Interface, nơi bạn có thể chọn Block Offenders để kích hoạt chức năng IPS

Bước 4 : Định nghĩa các luật tùy chỉnh (Custom Rules)

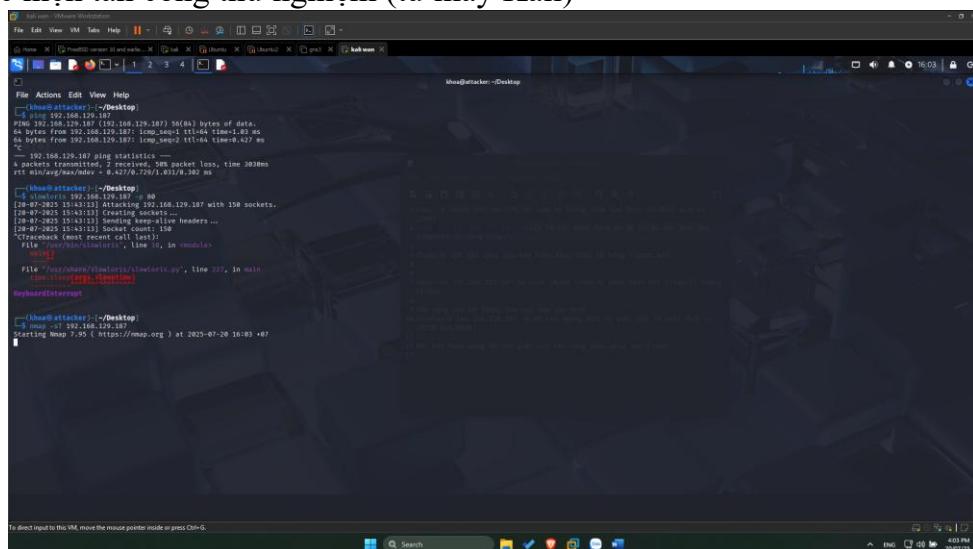


Hình 13. Định nghĩa các luật chặn tùy chỉnh (Custom Rules) trong Suricata.

Trong giao diện Suricata, điều hướng đến tab WAN Rules thêm các luật tùy chỉnh. Các luật này sẽ xác định hành vi mạng độc hại và hành động tương ứng để cảnh báo và chặn các lưu lượng vượt quá mức cho phép.

- drop icmp 192.168.129.0/24 any -> any any (msg:"Co the bi tan cong"; sid:3000002; rev:1;)
- drop tcp any any -> any any (flags:S; msg:"[SURICATA] Nmap SYN Port Scan Detected"; type: threshold, track by_src, (,
- drop tcp any any -> any any (flags:FUP; msg:"[SURICATA] TCP XMAS Scan Detected"; sid:3000004; rev:1;)
- drop http any any -> any any (msg:"[DNS] HTTP Request Flood Detected"; type: threshold, track by_src, count SI

Bước 5 : Thực hiện tấn công thử nghiệm (từ máy Kali)



Hình 14. Thực hiện quét cổng Nmap và Ddos từ máy tấn công.

- Để kiểm tra hoạt động, bạn có thể thực hiện một cuộc tấn công mô phỏng như quét cổng

bằng Nmap từ một máy tính khác vào địa chỉ IP của pfSense hoặc một máy trong mạng (được bảo vệ) và quan sát xem Suricata có phát hiện và chặn hay không.

Dùng lệnh

- nmap -sT 192.168.129.187
- slowloris 192.168.129.87 -p 80

Bước 6 : Xem nhật ký cảnh báo (Alert Log View)

The screenshot shows the 'Alert Log View' interface on a Kali Linux VM. The top navigation bar includes tabs for Home, File, Edit, View, VM, Tabs, Help, and several open windows like 'Suricata Alerts.php'. The main window has a title 'pfSense.home.apa - Seri'. It displays 'Alert Log View Settings' with 'Instance to View' set to '(WAN) WAN'. Below this is the 'Alert Log View Filter' section with a note about viewing the last 250 alert entries. The main table lists alerts from July 20, 2025, with columns for Date, Action, Pci, Proto, Class, Src, SPort, Dst, DPort, GID/SID, and Description. Most entries are UDP SYN Port Scan Detected or UDPv4 invalid checksum errors. A status bar at the bottom indicates 'Sync' and shows the date and time as 20/07/25 16:03.

Hình 15. Nhật ký các cảnh báo được ghi nhận bởi Suricata.

- **Xem cảnh báo:** Truy cập tab Alerts để xem các cảnh báo được Suricata tạo ra. Các mục được đánh dấu sẽ là các gói tin bị chặn (IPS mode).

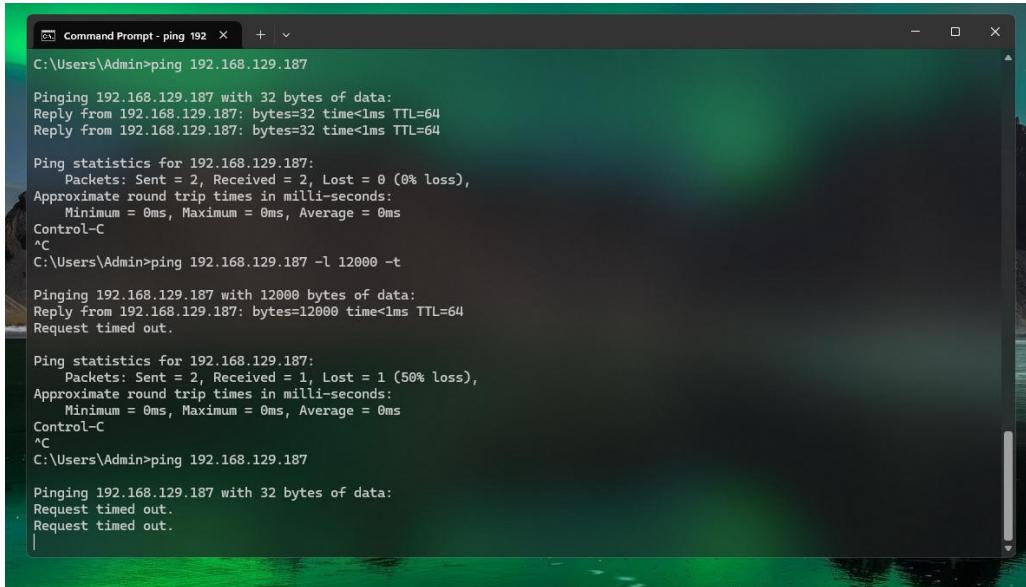
Bước 7 : Xem danh sách IP bị chặn (Blocked Hosts)

The screenshot shows the 'Blocked Hosts Log View' interface on a Kali Linux VM. The top navigation bar includes tabs for Wazuh, Interfaces, Global Settings, Updates, Alerts, Blocks, Files, Pass Lists, Suppress, Logs View, Logs Mgmt, and SID Mgmt. The main window has a title 'pfSense.home.apa - Seri'. It displays 'Blocked Hosts Log View Settings' with 'Save or Remove Hosts' and 'Save Settings' buttons. Below this is the 'Last 500 Hosts Blocked by Suricata' section with a note about legacy mode interfaces. The main table lists blocked hosts with columns for Blocked IP, Block Date/Time, Block Alert Description, Block Rule GID/SID, and Remove Block. Most descriptions are related to SYN Port Scan Detected or UDPv4 invalid checksum errors. A status bar at the bottom indicates 'Sync' and shows the date and time as 20/07/25 16:03.

Hình 16. Danh sách các địa chỉ IP bị chặn bởi Suricata.

- **Xem các IP bị chặn:** Truy cập tab Blocks để xem danh sách các địa chỉ IP đã bị Suricata chặn do vi phạm luật.

Bước 8 : Kiểm tra kết quả sau khi Suricata chặn (từ máy người dùng/nạn nhân)



```
C:\Users\Admin>ping 192.168.129.187

Pinging 192.168.129.187 with 32 bytes of data:
Reply from 192.168.129.187: bytes=32 time<1ms TTL=64
Reply from 192.168.129.187: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.129.187:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Admin>ping 192.168.129.187 -l 12000 -t

Pinging 192.168.129.187 with 12000 bytes of data:
Reply from 192.168.129.187: bytes=12000 time<1ms TTL=64
Request timed out.

Ping statistics for 192.168.129.187:
    Packets: Sent = 2, Received = 1, Lost = 1 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Admin>ping 192.168.129.187

Pinging 192.168.129.187 with 32 bytes of data:
Request timed out.
Request timed out.
```

Hình 17. Kết quả ping từ máy người dùng bị chặn sau khi IPS hoạt động.

- Lệnh ping 192.168.129.187 ban đầu thành công.
- Sau đó, lệnh ping 192.168.129.187 -l 12000 -t (ping với gói tin lớn và liên tục) cho thấy "Request timed out", nghĩa là gói tin bị chặn.
- Lệnh ping thông thường sau đó cũng bị "Request timed out".

2.3.2. Video Demo

Rule chống gói tin lớn và nmap : <https://youtu.be/L7d34fKjYQo>

Rule chống DDOS và nmap xmas : <https://youtu.be/WcNbLLDEnzI>

2.4 Các bước triển khai System Endpoint

2.4.1 Setup System Endpoint

Rule 1 : Cấu hình chống Brute force

```

root@khoa-VMware-Virtual-Platform:/var/ossec/ruleset/rules
GNU nano 7.2                               /var/ossec/etc/ossec.conf

</command>
<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>
<rules_id>87105</rules_id>
</active-response>

<active-response>
<command>firewall-drop</command>
<location>local</location>
<rules_id>5710,5712,5763</rules_id>
<timeout>600</timeout> <!-- Block trong 10 phút -->
</active-response>
>
```

^D Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^U Paste ^J Justify ^I Go To Line M-E Redo M-A Set Mark M-G Copy

Hình 18. Thiết lập rule chống Brute Force trên Wazuh Manager

- <rules_id>5710,5712,5763</rules_id>: Điều này rất quan trọng. Đây là các ID quy tắc của Wazuh mà khi được kích hoạt, sẽ bắt đầu phản ứng chủ động này.
- Nó sẽ chạy command firewall-drop khi thấy id 5710,5712,5763
- <timeout>600</timeout>: Đặt thời gian hiệu lực của phản ứng chủ động chặn IP trong 600 giây.

```

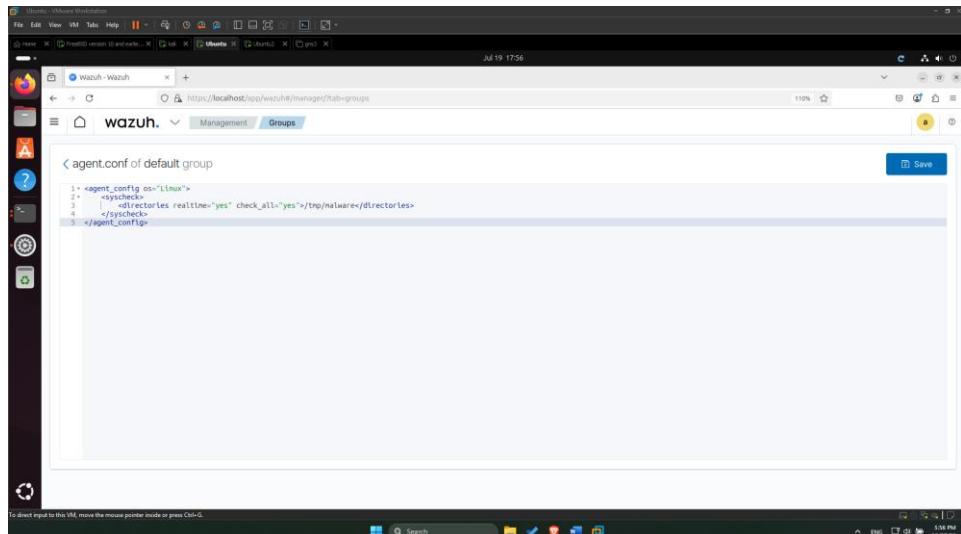
<command>
<name>firewall-drop</name>
<executable>firewall-drop</executable>
<timeout_allowed>yes</timeout_allowed>
</command>
```

Hình 19. Định nghĩa lệnh Firewall-drop chống Brute Force

- <executable>firewall-drop</executable>: Chỉ định tập lệnh hoặc chương trình thực thi mà Wazuh sẽ chạy khi lệnh này được gọi. Nó ngụ ý có một tập lệnh tên firewall-drop trong thư mục phản ứng chủ động.
- Nó sẽ drop ip đó khi thấy id 5710,5712,5763 cảnh báo
- Thị lúc nó ip máy tấn công sẽ bị block

Rule 2 : Cấu hình quét Virus bằng Virus Total

- Quy tắc này tích hợp Wazuh với VirusTotal để phát hiện và xử lý tệp chứa virus/malware. Khi phát hiện, tập lệnh remove-threat.sh sẽ tự động loại bỏ hoặc cách ly mối đe dọa. Đồng thời, syscheck sẽ giám sát thư mục /tmp/malware/directories theo thời gian thực để quét mọi thay đổi hoặc tệp mới.



Hình 20. Cấu hình giám sát thư mục máy Agent trên Wazuh Manager

- <agent_config os="Linux">: Chỉ định rằng cấu hình này áp dụng cho các tác nhân Linux.
- check_all="yes"/tmp/malware/directories</directories>: Cấu hình syscheck để giám sát đường dẫn /tmp/malware/directories trong thời gian thực và thực hiện tất cả các kiểm tra tính toàn vẹn

```
root@khoa-VMware-Virtual-Platform:/var/ossec/ruleset/rules
GNU nano 7.2                               /var/ossec/etc/ossec.conf

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

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/kern.log</location>
</localfile>

<integration>
  <name>virustotal</name>
  <api_key>8d28d96ff6f6b4c95f1618187aad4a5e70f674833fdaca79c4ecb10b7ae6290</api_key>
  <group>syscheck</group>
  <alert_format>json</alert_format>
</integration>

</ossec_config>
```

Hình 21. Tích hợp API của VirusTotal vào Wazuh Manager

- <name>virustotal</name>: Chỉ định tên của tích hợp, đó là VirusTotal.
- <api_key>8d28d96ff6f6b4c95f1618187aad4a5e70f674833fdaca79c4ecb10b7ae6290</api_key>: Đây là khóa API để truy cập dịch vụ VirusTotal.
- <group>syscheck</group>: Liên kết tích hợp này với nhóm syscheck, nghĩa là các cảnh báo của syscheck có thể kích hoạt quét VirusTotal.

```

GNU nano 7.2                               /var/ossec/etc/ossec.conf

<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>
  <rules_id>87105</rules_id>
</active-response>

<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>5710,5712,5763</rules_id>
  <timeout>600</timeout> <!-- Block trong 10 phút -->
</active-response>

<active-response>

```

Hình 22. Định nghĩa ID để báo Log về cho Wazuh Manager

- <disabled>no</disabled>: Đảm bảo phản ứng chủ động này được bật.
- <command>remove-threat</command>: Chỉ định rằng lệnh remove-threat nên được thực thi.
- <location>local</location>: Cho biết thực thi cục bộ.
- <rules_id>87105</rules_id>: Đây là ID quy tắc của Wazuh mà khi được kích hoạt (ví dụ: do phát hiện phần mềm độc hại), sẽ bắt đầu phản ứng chủ động remove-threat.

```

</command>

<command>
  <name>remove-threat</name>
  <executable>remove-threat.sh</executable>
  <timeout_allowed>no</timeout_allowed>
</command>

<active-response>

```

Hình 23. Thiết lập rule xóa file chúa Virus

- <name>remove-threat</name>: Gán tên "remove-threat" cho lệnh này.
- <executable>remove-threat.sh</executable>: Chỉ định rằng tập lệnh remove-threat.sh sẽ được thực thi khi lệnh này được gọi.
- <timeout_allowed>no</timeout_allowed>: Cho biết lệnh này không hỗ trợ tham số timeout.

```

GNU nano 7.2                               remove-threat.sh

#!/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'
fi
read RESPONSE

```

Hình 24. Thực thi cho lệnh remove-threat

- Tự động xử lý thông tin từ Wazuh:** Nó nhận dữ liệu từ Wazuh (dưới dạng JSON), trích xuất các thông tin quan trọng như tên tệp và lệnh.
- Ghi nhật ký hoạt động:** Nó xác định nơi để ghi lại các hoạt động của tập lệnh.
- Thực hiện hành động dựa trên điều kiện:** Nó kiểm tra một điều kiện cụ thể (nếu lệnh là "add") và có thể thực hiện một số hành động, ví dụ như gửi phản hồi trả lại Wazuh.
⇒ Remove-threat.sh khi bị kích hoạt nó sẽ xóa file yêu cầu

Jul 24, 2025 @ 01:15:39.707		007	khoa2-VMware-Virtual-Platform	T1203	Execution	VirusTotal: Alert - /home/khoa2/Downloads/virus.rar - 14 engines detected this file	12	87105
Table	JSON	Rule						
			@timestamp	2025-07-23T18:15:39.707Z				
			_id	e9L0JgBxSqmXILspus				
			agent.id	007				
			agent.ip	192.168.100.3				
			agent.name	khoa2-VMware-Virtual-Platform				
			data.integration	virustotal				
			data.virustotal.found	1				
			data.virustotal.malicious	1				
			data.virustotal.permalink	https://www.virustotal.com/gui/file/9758941534bc3ac4c8633d8e97f193e9ddc21cba755b6863b962c14b74dc3daf/detection/f-9758941534bc3ac4c8633d8e97f193e9ddc21cba755b6863b962c14b74dc3daf-1750928444				
			data.virustotal.positives	14				
			data.virustotal.scan_date	2025-06-26 09:00:44				
			data.virustotal.sha1	c07600267afdd6cf9129d6290b29d61148b1ee61				
			data.virustotal.source.alert_id	1753294537.9251				
			data.virustotal.source.file	/home/khoa2/Downloads/virus.rar				

Hình 25. Kết quả xóa Virus và báo Log lên Dashboard của Wazuh Manager

- Dashboard của wazuh manaer báo Log ID 87105 quét thành công Virus và Virus Total

2.4.2 Demo :

- Chặn brute force : <https://youtu.be/X5Pv6BRk1sE>
- Wazuh virustotal : <https://youtu.be/P0CiYK8LyKE>

2.5. Kịch bản 1 : Tấn Công DDOS

2.5.1 : Kịch bản tấn công Ddos :

1. Chuẩn Bị Môi Trường Ảo Hóa

- Máy chủ Web (Ubuntu Server):** Cài đặt một máy chủ Ubuntu, cấu hình Nginx để chạy một trang web đơn giản. Đây là mục tiêu tấn công của bạn.
- Máy Khách:** Một máy tính bất kỳ để bạn kiểm tra khả năng truy cập vào trang web trước, trong và sau khi tấn công.
- Máy Tấn Công (Kali Linux):** Một máy Kali Linux chứa các công cụ cần thiết để thực hiện các cuộc tấn công DDoS ở nhiều lớp khác nhau.
- Tường Lửa/IDS (pfSense với Suricata):** Một máy pfSense được cài đặt làm tường lửa và hệ thống phát hiện xâm nhập (IDS) Suricata. Mục đích là để giám sát lưu lượng mạng và

ghi lại các cảnh báo khi có tấn công xảy ra.

2. Giai Đoạn 1: Thăm Dò và Kiểm Tra Ban Đầu

- **Thăm dò mục tiêu:** Từ máy Kali, bạn sẽ thực hiện các bước thăm dò cơ bản để xác định các cổng dịch vụ đang mở trên máy chủ Nginx (ví dụ: cổng 80 cho HTTP).
- **Kiểm tra dịch vụ:** Từ máy Khách, bạn sẽ truy cập vào trang web trên máy chủ Nginx để đảm bảo rằng dịch vụ web đang hoạt động bình thường trước khi có bất kỳ cuộc tấn công nào.
- **Kiểm tra giám sát:** Đảm bảo rằng Suricata trên pfSense đang chạy và sẵn sàng ghi lại nhật ký sự kiện.

3. Giai Đoạn 2: Thực Hiện Tấn Công DDoS

Trong giai đoạn này, bạn sẽ sử dụng máy Kali để mô phỏng các kiểu tấn công DDoS khác nhau vào máy chủ Nginx.

- **Tấn công Layer 3/4 (Tầng Mạng/Truyền tải):**
 - Tôi mô phỏng các cuộc tấn công như **SYN Flood** hoặc **UDP Flood**. Các cuộc tấn công này cố gắng làm quá tải tài nguyên mạng hoặc bảng kết nối của máy chủ bằng cách gửi một lượng lớn gói tin không hoàn chỉnh hoặc không mong muốn.
 - **Quan sát:** Máy Khách sẽ không thể truy cập được trang web hoặc truy cập rất chậm. Trên máy chủ Nginx, tài nguyên có thể bị cạn kiệt. Suricata trên pfSense sẽ ghi lại các cảnh báo về các loại tấn công này.
- **Tấn công Layer 7 (Tầng Ứng dụng):**
 - Bạn sẽ mô phỏng các cuộc tấn công như **Slowloris**. Mục tiêu là giữ các kết nối HTTP mở càng lâu càng tốt để tiêu tốn tài nguyên của máy chủ Nginx, ngăn chặn các kết nối hợp lệ khác.
 - **Quan sát:** Trang web sẽ không phản hồi từ máy Khách. Máy chủ Nginx có thể báo cáo các lỗi liên quan đến kết nối hoặc hết thời gian chờ. Suricata có thể ghi lại một số hoạt động bất thường, nhưng các cuộc tấn công Layer 7 đôi khi khó phát hiện hơn bằng IDS đơn thuần.

4. Giai Đoạn 3: Triển Khai Giải Pháp Phòng Chống

Sau khi quan sát tác động của các cuộc tấn công, bạn sẽ triển khai các biện pháp phòng chống:

- **Phòng chống Layer 7 trên Nginx:**
 - Bạn sẽ cấu hình lại **Nginx** để giới hạn số lượng kết nối đồng thời và tốc độ yêu cầu từ một địa chỉ IP. Điều này giúp giảm thiểu tác động của các cuộc tấn công như Slowloris.
 - **Kiểm tra lại:** Sau khi cấu hình, bạn sẽ thử lại tấn công Slowloris từ máy Kali và quan sát xem trang web trên máy Khách có còn truy cập được hoặc ít bị ảnh hưởng

hơn không.

- **Giới hạn gói tin Layer 3/4 với Nftables:**

- Bạn sẽ sử dụng **nftables** trên máy chủ Nginx (hoặc một tường lửa Linux riêng biệt) để tạo ra các quy tắc giới hạn hoặc từ chối các gói tin đáng ngờ đến liên tục. Điều này giúp chống lại SYN Flood và UDP Flood.
- **Kiểm tra lại:** Sau khi cấu hình nftables, bạn sẽ thử lại các cuộc tấn công SYN Flood và UDP Flood từ máy Kali. Quan sát log của nftables để xem các gói tin có bị chặn hay không, và kiểm tra xem trang web trên máy Khách có ổn định hơn không.

2.5.2 : Các bước tấn công :

```
duclong@duclong-virtual-machine:~$ sudo apt install nginx -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nginx is already the newest version (1.18.0-6ubuntu14.6).
0 upgraded, 0 newly installed, 0 to remove and 110 not upgraded.
duclong@duclong-virtual-machine:~$ sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2025-07-08 08:48:31 +07; 1min 7s ago
       Docs: man:nginx(8)
   Process: 1038 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
   Process: 1075 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
 Main PID: 1090 (nginx)
    Tasks: 5 (limit: 4545)
      Memory: 9.0M
        CPU: 151ms
       CGroup: /system.slice/nginx.service
           ├─1090 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
           ├─1091 "nginx: worker process" " "
           ├─1092 "nginx: worker process" " "
           ├─1093 "nginx: worker process" " "
           └─1094 "nginx: worker process" " "

Thg 7 08 08:48:30 duclong-virtual-machine systemd[1]: Starting A high performance web server and a reverse proxy server...
Thg 7 08 08:48:31 duclong-virtual-machine systemd[1]: Started A high performance web server and a reverse proxy server.
```

Hình 26. Cài đặt và xem trạng thái hoạt động của Nginx

- Lệnh sudo apt install nginx -y được thực thi để cài đặt Nginx
- Lệnh sudo systemctl status nginx được sử dụng để xác minh trạng thái hoạt động của Nginx.

```

GNU nano 6.2                                     /etc/nginx/sites-available/my_ddos_website.conf
# Tên miền hoặc địa chỉ IP mà Nginx sẽ phản hồi.
server_name 192.168.100.10; # <--- ĐÃM BẢO ĐỊA CHỈ IP NAY CHÍNH XÁC VỚI MÁY VICTIM CỦA BẠN

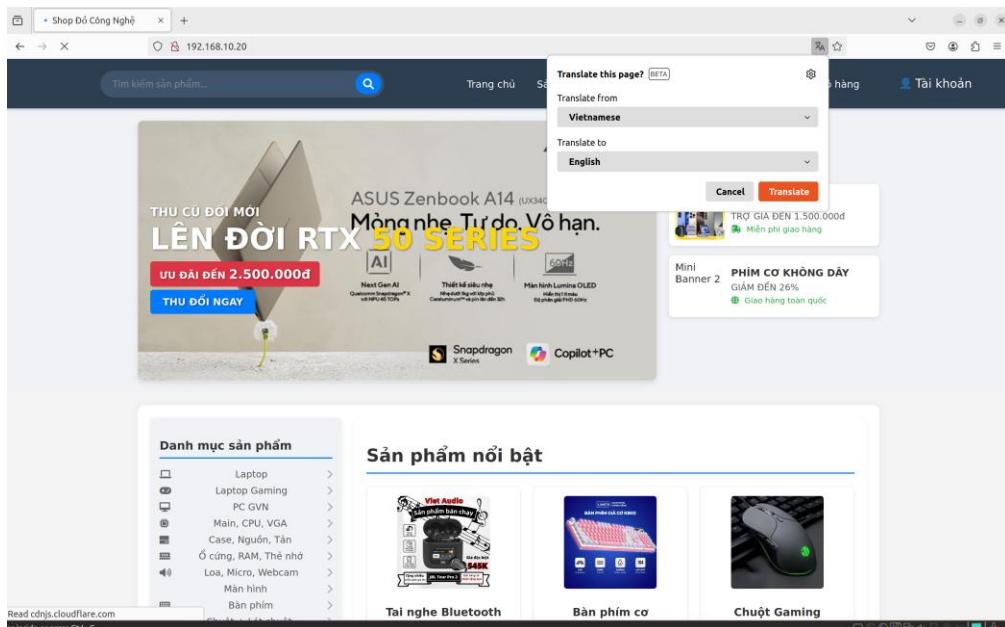
# Khối 'location' chính để xử lý các yêu cầu tới trang web của bạn.
location / {
    # try_files: Nginx sẽ thử tìm kiếm các file theo thứ tự sau:
    # 1. $uri: Trùng khớp chính xác với yêu cầu (ví dụ: http://ip/robots.txt sẽ tìm /public/robots.txt)
    # 2. $uri/: Trùng khớp với thư mục (ví dụ: http://ip/css/ sẽ tìm /public/css/ và sau đó là file index trong đó)
    # 3. /html/$uri: Nếu không tìm thấy ở 1 hoặc 2, thử tìm yêu cầu trong thư mục 'html' con.
    # Ví dụ: Khi truy cập http://ip/login.html, Nginx sẽ tìm /public/login.html (không có).
    # Sau đó nó sẽ tìm /public/html/login.html (có).
    # 4. /html/$uri.html: Nếu yêu cầu không có đuôi .html (ví dụ: http://ip/products),
    # Nginx sẽ thử tìm /public/html/products.html.
    # 5. /html/index.html: Nếu tất cả các cách trên đều không tìm thấy, Nginx sẽ mặc định hiển thị /public/html/index.html (trang chủ).
    # 6. =404: Nếu không tìm thấy bất kỳ file nào sau tất cả các thử nghiệm trên, trả về lỗi 404.
    # --- RULE 5: Áp dụng giới hạn số lượng yêu cầu mỗi giây (Rate Limiting) ---
    # 'burst=10': Cho phép bùng nổ 10 yêu cầu.
    limit_req_status 429;
    try_files $uri $uri.html /html/index.html =404;
}

# Khối 'location' đặc biệt cho yêu cầu tới thư mục gốc '/'
# Điều này đảm bảo khi người dùng chỉ gõ http://192.168.10.20/, nó sẽ hiển thị trang chủ.
location / {
    # Chỉ cần cố gắng tìm file index.html trong thư mục html con.
    try_files /html/index.html =404;
}

```

Hình 27. Cấu hình Nginx và IP máy chủ Nginx được thiết lập để phục vụ trang web.

- Lắng nghe cổng:** Máy chủ lắng nghe trên cổng 80 cho cả IPv4 và IPv6 để xử lý các yêu cầu HTTP.
- Thư mục gốc:** Định nghĩa thư mục gốc (root) của trang web là /var/www/my_ddos_website/public/.
- Xử lý yêu cầu:** Cấu hình location / sử dụng try_files để tìm kiếm các tập tin theo thứ tự nhất định (cart.html, complete.html, dashboard.html, v.v.) và trả về lỗi 404 nếu không tìm thấy.

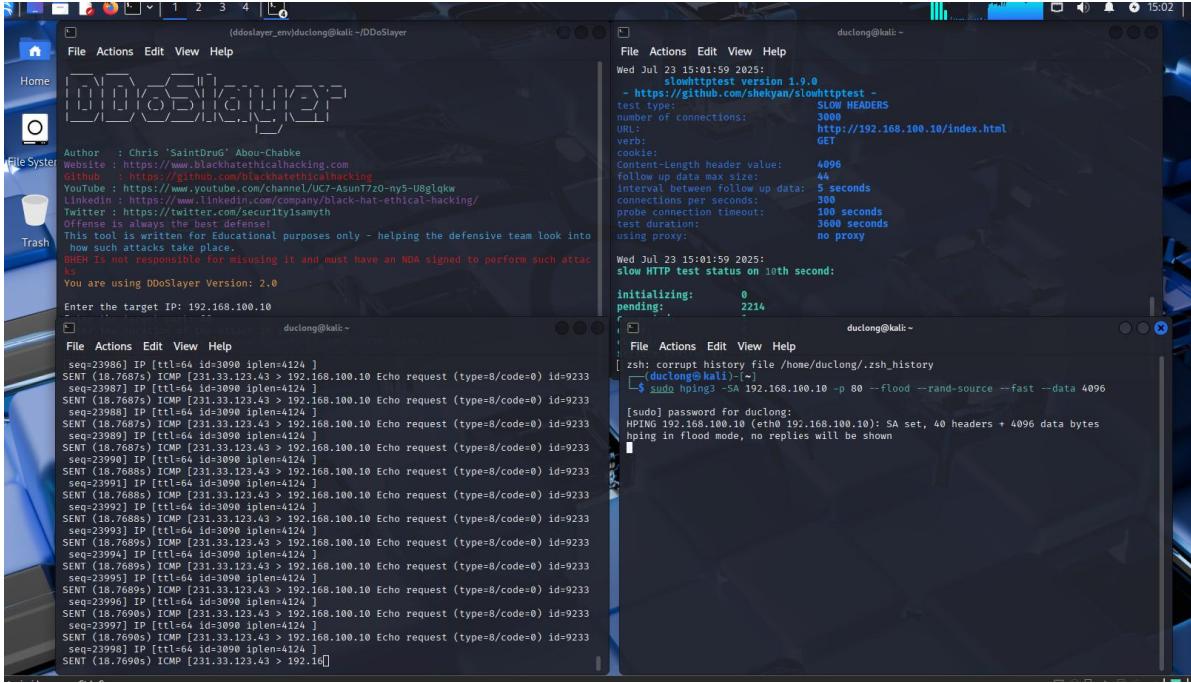


Hình 28. Truy xuất trang web từ máy Client

- Trang web được chạy bằng Nginx
- Truy xuất IP của máy Webserver và đã truy cập vào trang Web thành công

2.5.3 Tấn công khi không phòng chố

Sử dụng 1 máy kali để tấn công Web bằng các lệnh



Hình 29. Các lệnh tấn công Ddos ở Layer 3, 4 & 7 trên Kali

Các lệnh tấn công :

Lệnh : python3 DDoSlayer.py

- Chức năng:** Gửi HTTP GET/POST Flood đến địa chỉ IP 192.168.100.10 qua port 80.
- Phương thức:** Tấn công Layer 7 bằng cách gửi hàng loạt yêu cầu HTTP từ các IP giả mạo để làm quá tải ứng dụng web.
- Mục tiêu:** Làm cho web server Nginx bị nghẽn hoặc từ chối dịch vụ do xử lý số lượng lớn truy vấn HTTP cùng lúc.

Lệnh : sudo nping --icmp --source-ip random --dest-ip 192.168.100.10 --data-length 4096 --rate

http://192.168.100.10/index.html -x 20 -p 100

- Chức năng:** Gửi hàng nghìn kết nối HTTP giữ lâu bằng cách gửi header chậm.
- Phương thức:** Tấn công Layer 7 (HTTP slow headers) – dạng Slowloris.
- Mục tiêu:** Làm web server 192.168.100.10 cạn tài nguyên socket, khiến không phản hồi được người dùng hợp lệ.

Lệnh : sudo nping --icmp --source-ip random --dest-ip 192.168.100.10 --data-length 4096 --rate 100000 --count 0

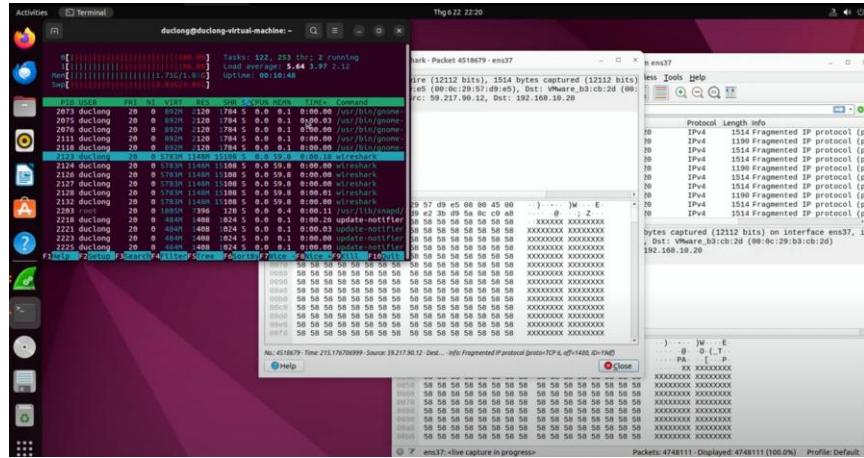
- Chức năng:** Gửi flood ICMP (ping) liên tục với dữ liệu 4096 byte từ IP giả.
- Phương thức:** DDoS Layer 3 – tiêu tốn băng thông và tài nguyên xử lý gói mạng.
- Mục tiêu:** Làm nghẽn web server 192.168.100.10 bằng lượng lớn ICMP.

Lệnh : sudo hping3 -SA 192.168.100.10 -p 80 --flood --rand-source --fast --data 4096

- Chức năng:** Gửi TCP SYN/ACK Flood với dữ liệu lớn và IP giả.
- Phương thức:** DDoS Layer 4 – làm cạn tài nguyên kết nối TCP (socket, queue).

- Mục tiêu:** Gây quá tải cổng 80 của server 192.168.100.10, làm gián đoạn dịch vụ HTTP.

Kết quả tấn công khi không phòng chố :



Hình 30. Giám sát hệ thống khi bị Ddos

Lệnh HTOP

- CPU Usage (100%):** Toàn bộ tài nguyên CPU bị chiếm dụng, đặc biệt là user space (màu xanh) và interrupts (IRQ) tăng (màu đỏ), cho thấy hệ thống đang xử lý quá nhiều yêu cầu/ngắt do tấn công.
- Load Average cao:** Giá trị load average tăng đột biến (vượt quá số core CPU), cho thấy hệ thống đang bị quá tải nghiêm trọng.
- Nhiều tiến trình ksoftirqd, systemd, sshd... chạy liên tục** ⇒ biểu hiện của hệ thống bị ngập lệnh xử lý từ tấn công mạng.

Wireshark:

- Hiển thị nhiều gói IPv4 bị phân mảnh (Fragmented IP).
- Gói dữ liệu chứa byte "58" lặp lại ⇒ dấu hiệu tấn công kiểu flood dữ liệu.
- Gói đến từ địa chỉ giả, đích là 192.168.100.20 ⇒ tấn công Layer 3/4 (ICMP/TCP Flood).

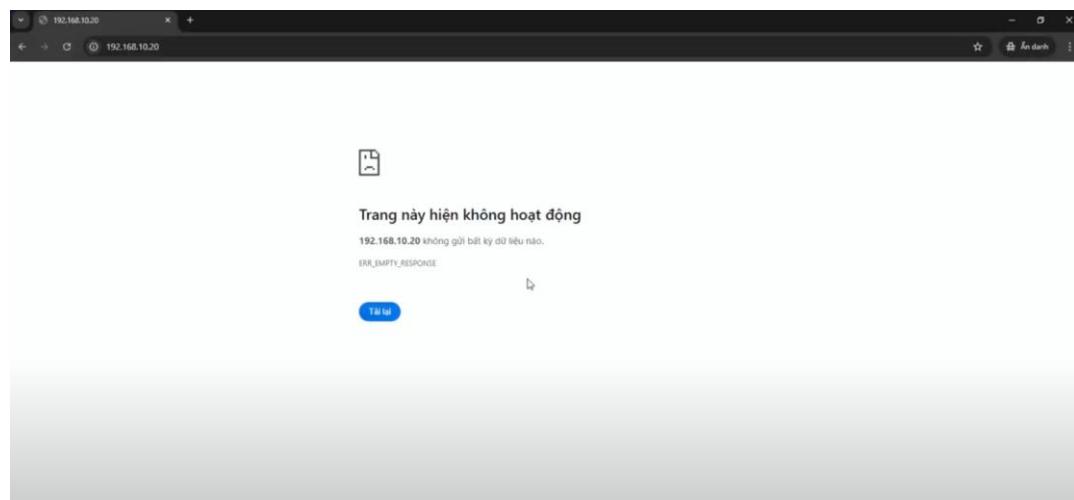
```

duclong@duclong-virtual-machine: ~      duclong@duclong-virtual-machine: ~
duclong@duclong-virtual-machine: ~ $ sudo netstat -an | grep ":80" | grep -c "SYN_RECV"
[sudo] password for duclong:
0
duclong@duclong-virtual-machine: ~ $ sudo netstat -an | grep ":80" | grep -c "SYN_RECV"
512
duclong@duclong-virtual-machine: ~ $ sudo netstat -an | grep ":80" | grep -c "SYN_RECV"
512
duclong@duclong-virtual-machine: ~ $ sudo netstat -an | grep ":80" | grep -c "SYN_RECV"
512
duclong@duclong-virtual-machine: ~ $ sudo netstat -an | grep ":80" | grep -c "SYN_RECV"
512
duclong@duclong-virtual-machine: ~ $ sudo netstat -an | grep ":80" | grep -c "SYN_RECV"
512
duclong@duclong-virtual-machine: ~ $ 

```

Hình 31. Kiểm tra SYN Flood bằng Netstat

- Kết quả: 512 kết nối SYN_RECV liên tục ⇒ dấu hiệu tấn công TCP SYN Flood.
- Cho thấy web server bị ngập kết nối chờ bắt tay TCP, dẫn đến từ chối dịch vụ.



Hình 32. Kết quả tấn công DDoS: Trang web không phản hồi

- Khi dùng 1 máy Client truy xuất web thì "Trang này hiện không hoạt động" kèm theo mã lỗi ERR_EMPTY_RESPONSE.
- Đây là bằng chứng trực quan cho thấy cuộc tấn công DDoS đã thành công, khiến máy chủ web không thể phản hồi các yêu cầu hợp lệ từ người dùng, dẫn đến việc

Xây dựng phòng chống Ddos

Cài đặt Nftables để chống Ddos ở Layer 3 và Layer 4

```
duclong@duclong-virtual-machine:~$ sudo apt update
[sudo] password for duclong:
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 https://packages.wazuh.com/4.x/apt stable InRelease
Hit:5 http://security.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
130 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: https://packages.wazuh.com/4.x/apt/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg)
duclong@duclong-virtual-machine:~$ sudo apt install nftables -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nftables is already the newest version (1.0.2-1ubuntu3).
nftables set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 130 not upgraded.
duclong@duclong-virtual-machine:~$ sudo systemctl enable nftables
Created symlink /etc/systemd/system/sysinit.target.wants/nftables.service → /lib/systemd/system/nftables.service.
duclong@duclong-virtual-machine:~$ sudo systemctl start nftables
duclong@duclong-virtual-machine:~$ sudo nft list ruleset
table inet filter {
```

Hình 33. Cài đặt và khởi động nftables trên Ubuntu

- Cài đặt và kích hoạt nftables – công cụ tường lửa hiện đại thay thế iptables.
- Khởi động dịch vụ để bắt đầu áp dụng các quy tắc lọc gói tin mạng.
- Kiểm tra cấu trúc rule mặc định của hệ thống firewall.
- Là bước chuẩn bị để thiết lập các chính sách bảo vệ hệ thống mạng khỏi các tấn công tầng mạng (Layer 3/4).

```
GNU nano 6.2
/etc/nftables.conf
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
    chain input {
        type filter hook input priority 0;
        policy drop;

        # Cho phép loopback (localhost)
        iif lo accept

        # Cho phép các kết nối đã được thiết lập hoặc liên quan
        ct state established,related accept

        # Cho phép ping
        ip protocol icmp accept

        # Cho phép SSH (giới hạn 3 kết nối mỗi 30s)
        tcp dport 22 ct state new limit rate 3/minute accept

        # Cho phép HTTP & HTTPS (giới hạn tốc độ)
        tcp dport [ 80, 443 ] ct state new limit rate 25/second burst 20 packets accept

        # Giới hạn SYN flood (tấn công TCP handshake)
        tcp flags syn tcp option maxseg size 536 ct state new limit rate 15/second burst 20 packets accept

        # Giới hạn UDP (chống UDP flood)
        udp dport 53 limit rate 5/second accept

        # DROP mặc định cho tất cả còn lại
        drop
    }
}
```

Hình 34. Thiết lập rule cho nftables

- **Danh sách đen (blacklist):** Tự động thêm IP vào nếu có hành vi bất thường như gửi quá nhiều gói SYN/ACK.
- **Giới hạn SYN/ACK:** Nếu vượt quá 10 gói SYN/s hoặc 15 gói ACK/s, IP bị block trong 10 phút.
- **Bảo vệ SSH:** Giới hạn 3 kết nối mới/phút để ngăn brute-force.
- **Bảo vệ Web Server:** HTTP/HTTPS giới hạn ở 15 kết nối mới/s, chặn khi vượt quá.
- **ICMP (Ping):** Cho phép ping nhẹ nhàng nhưng block khi có ICMP flood.
- **Chính sách mặc định:** Drop toàn bộ lưu lượng không được cho phép.

Chống Ddos ở Layer 7 bằng Nginx

Cấu hình Rule trên Nginx

```
include /etc/nginx/conf.d/*.conf;
include /etc/nginx/sites-enabled/*;
limit_conn_zone $binary_remote_addr zone=conn_limit_per_ip:10m;
# Ghi log ở cấp độ 'info' khi kết nối bị giới hạn.
limit_conn_log_level info;
# 'rate=5r/s' : Giới hạn trung bình 5 yêu cầu/giây/IP. Tùy theo ứng dụng, bạn có thể tăng/giảm.
limit_req_zone $binary_remote_addr zone=req_limit_per_ip:10m rate=5r/s;
# Ghi log ở cấp độ 'info' khi yêu cầu bị giới hạn.
limit_req_log_level info;

map $http_user_agent $bad_user_agent {
default 0; # Mặc định là không phải User-Agent xấu
"~*ApacheBench" 1;
"~*curl" 1;
"~*wget" 1;
"~*bot" 1;
"~*nmap" 1;
"~*nikto" 1;
"~*hydra" 1;
"~*^\$*" 1; # Chặn User-Agent hoàn toàn rỗng hoặc chỉ có khoảng trắng
"~*^$" 1; # Chặn User-Agent rỗng (ví dụ: header User-Agent: )
"~*-" 1; # Chặn User-Agent là dấu gạch ngang (ví dụ: header User-Agent: - )
# Thêm các chuỗi User-Agent đáng ngờ khác vào đây nếu bạn phát hiện
# ví dụ: "~*masscan" 1; "~*scanner" 1;
}
```

Hình 35. Cấu hình rule anti Ddos Layer 7 trên Nginx

Lệnh : sudo nano /etc/nginx/nginx.conf để vào Nginx cấu hình Rue

- Giới hạn request và kết nối theo IP để ngăn HTTP Flood (5 request/giây).
- Lọc User-Agent nhằm chặn công cụ tấn công tự động như curl, wget, nmap, nikto, v.v.
- Bảo vệ server khỏi tấn công tầng ứng dụng (Layer 7) như web scanner và bot gửi yêu cầu bất hợp pháp.

```
GNU nano 6.2
server {
    listen 80;           # Nginx sẽ lắng nghe các kết nối HTTP trên cổng 80
    listen [::]:80;      # Hỗ trợ IPv6
    # --- RULE 1: Chặn các User-Agent đáng ngờ ---
    # Đặt lên đầu khối server để chặn yêu cầu sớm nhất có thể.
    if ($http_user_agent ~* "(ApacheBench|curl|wget|bot|nmap|nikto|hydra|^\$User-Agent:)" ) {
        return 403;
    }

    if ($bad_user_agent) {
        return 403; # Trả về lỗi 403 Forbidden
    }
    if ($http_accept = "") { # Nếu header Accept rỗng
        return 403;
    }
    if ($host = "") { # Nếu header Host rỗng
        return 403;
    }
    # 'nodelay': Từ chối ngay lập tức nếu vượt quá burst (không xếp hàng chờ).
    limit_req zone=req_limit_per_ip burst=10 nodelay;
    # --- RULE 2: Giới hạn số lượng kết nối đồng thời (Connection Limiting) --
```

Hình 36. Cấu hình rule lọc các yêu cầu HTTP bất thường

- Cấu hình này giúp Nginx phát hiện và chặn các yêu cầu HTTP bất thường thường dùng trong tấn công Layer 7.
- Nó kiểm tra nếu trường Accept hoặc Host bị đê trống (thường do bot hoặc script gửi request sai chuẩn), thì trả về lỗi 403.
- Ngoài ra, nếu biến \$bad_user_agent có giá trị 1 (được định nghĩa trong nginx.conf bằng lệnh map, chứa các User-Agent nguy hiểm như curl, nmap, hydra, v.v.), thì cũng chặn luôn yêu cầu đó bằng cách trả về 403.
- Cấu hình này được đặt trong file /etc/nginx/sites-enabled/my_ddos_website.conf, nằm trong khối server, và sẽ hoạt động song song với giới hạn tốc độ yêu cầu (limit_req) để

giảm tải và ngăn request bất hợp pháp. Kết quả khi thiết lập phòng chông :

```
Every 1,0s: nft list set lnet filter blacklist
table lnet filter {
    set blacklist {
        type ipv4_addr
        size 65535
        flags dynamic,timeout
        timeout 10m
        elements = { 0.3.186.122 timeout 10m expires 9n39s610ms, 0.9.239.7 timeout 10m expires 9n39s010ms,
        0.10.186.122 timeout 10m expires 9n39s911ms, 0.13.132.19 timeout 10m expires 9n39s899ms,
        0.27.38.151 timeout 10m expires 9n39s610ms, 0.27.115.29 timeout 10m expires 9n39s804ms,
        0.28.208.118 timeout 10m expires 9n39s859ms, 0.43.174.126 timeout 10m expires 9n39s710ms,
        0.49.145.173 timeout 10m expires 9n39s710ms, 0.50.121.181 timeout 10m expires 9n39s918ms,
        0.57.137.201 timeout 10m expires 9n39s610ms, 0.58.121.181 timeout 10m expires 9n39s617ms,
        0.64.247.105 timeout 10m expires 9n39s744ms, 0.87.39.143 timeout 10m expires 9n39s700ms,
        0.96.226.135 timeout 10m expires 9n39s761ms, 0.97.43.103 timeout 10m expires 9n39s919ms,
        0.106.27.254 timeout 10m expires 9n39s817ms, 0.111.228.200 timeout 10m expires 9n39s644ms,
        0.116.124.246 timeout 10m expires 9n39s803ms, 0.137.0.122 timeout 10m expires 9n39s760ms,
        0.145.253.122 timeout 10m expires 9n39s717ms, 0.151.18.106 timeout 10m expires 9n39s756ms,
        0.152.119.115 timeout 10m expires 9n39s610ms, 0.153.119.115 timeout 10m expires 9n39s617ms,
        0.162.48.1 timeout 10m expires 9n39s741ms, 0.176.15.84 timeout 10m expires 9n39s663ms,
        0.178.13.251 timeout 10m expires 9n39s660ms, 0.190.38.165 timeout 10m expires 9n39s594ms,
        0.232.64.208 timeout 10m expires 9n39s922ms, 0.239.222.87 timeout 10m expires 9n39s743ms,
        0.240.179.58 timeout 10m expires 9n39s843ms, 0.242.148.240 timeout 10m expires 9n39s892ms,
        0.244.216.95 timeout 10m expires 9n39s780ms, 0.249.252.116 timeout 10m expires 9n39s700ms,
        0.251.19.101 timeout 10m expires 9n39s720ms, 0.252.19.101 timeout 10m expires 9n39s724ms,
        0.254.64.242 timeout 10m expires 9n39s756ms, 0.261.191.63 timeout 10m expires 9n39s824ms,
        1.9.222.1.1 timeout 10m expires 9n39s612ns, 1.14.226.145 timeout 10m expires 9n39s730ms,
        1.16.52.105 timeout 10m expires 9n39s759ms, 1.27.170.242 timeout 10m expires 9n39s673ms,
        1.27.252.171 timeout 10m expires 9n39s684ms, 1.40.2.122.105 timeout 10m expires 9n39s858ms,
        1.49.19.101 timeout 10m expires 9n39s685ms, 1.51.25.25 timeout 10m expires 9n39s685ms,
        1.55.99.1 timeout 10m expires 9n39s714ms, 1.84.241.0 timeout 10m expires 9n39s869ms,
        1.89.95.3.1 timeout 10m expires 9n39s716ns, 1.90.39.224 timeout 10m expires 9n39s724ns,
        1.106.19.101 timeout 10m expires 9n39s917ms, 1.122.14.97 timeout 10m expires 9n39s724ms,
        1.132.98.229 timeout 10m expires 9n39s708ms, 1.134.120.215 timeout 10m expires 9n39s627ms,
        1.135.119.115 timeout 10m expires 9n39s787ms, 1.139.89.16 timeout 10m expires 9n39s818ms,
        1.151.58.122 timeout 10m expires 9n39s908ms, 1.159.89.16 timeout 10m expires 9n39s819ms,
        1.162.42.122 timeout 10m expires 9n39s797ms, 1.174.140.21 timeout 10m expires 9n39s712ms,
        1.174.162.98 timeout 10m expires 9n39s899ms, 1.175.95.98 timeout 10m expires 9n39s897ms,
        1.188.149.124 timeout 10m expires 9n39s797ms, 1.189.252.194 timeout 10m expires 9n39s720ms,
        1.191.216.174 timeout 10m expires 9n39s738ms, 1.193.83.11 timeout 10m expires 9n39s684ms,
        1.202.19.101 timeout 10m expires 9n39s613ms, 1.203.122.222 timeout 10m expires 9n39s667ms,
        1.216.24.242 timeout 10m expires 9n39s613ms, 1.234.189.188 timeout 10m expires 9n39s667ms,
        1.234.242.14 timeout 10m expires 9n39s660ms, 1.237.9.66 timeout 10m expires 9n39s865ms, }
```

Hình 37. Danh sách IP bị chặn (Blacklist DDoS - nftables)

- Các địa chỉ IP trong danh sách này đã bị hệ thống tự động đưa vào dạng “bị chặn tạm thời” vì có hành vi đáng ngờ — thường là gửi nhiều gói SYN liên tục (tấn công DDoS Layer 3/4).
- Hệ thống sử dụng timeout là 10 phút cho mỗi IP.
Sau thời gian đó, IP sẽ tự động bị gỡ khỏi danh sách nếu không tiếp tục vi phạm.
- Đây là một phần quan trọng trong cơ chế phòng thủ động, giúp giảm tải máy chủ và bảo vệ khỏi các kết nối không hợp lệ hoặc quá tải.

```
duclong@duclong-virtual-machine: ~
Every 1,0s: netstat -n | grep ":80" | grep SYN_RECV | wc -l
53
```

Hình 38. Giám sát kết nối SYN_RECV – Kiểm tra tấn công DDoS TCP SYN

- Lệnh : watch -n 1 'netstat -n | grep ":80" | grep SYN_RECV | wc -l'
- Khi xảy ra cuộc tấn công, giá trị đếm là 53, tức là có 53 kết nối đang chờ hoàn tất bắt tay TCP (3-way handshake).
Trước đó, hệ thống từng ghi nhận liên tục 512 kết nối, cho thấy tấn công đang diễn ra.
- Sau khi triển khai các biện pháp chống DDoS bằng nftables, số lượng kết nối đã giảm

mạnh.

Điều này chứng tỏ firewall đã hoạt động hiệu quả trong việc:

- Phát hiện và chặn IP gửi SYN quá nhiều.
 - Giám sát tài nguyên hệ thống.

Hình 39. Phản hồi Log của Nginx khi bị Ddos ở Layer 7

- **Tệp log đang được theo dõi:**

Hình ảnh hiển thị nội dung tệp /var/log/nginx/access.log được theo dõi thời gian thực bằng lệnh tail -f, nhằm ghi nhận các yêu cầu truy cập web đến máy chủ.

- IP gửi yêu cầu bất thường:

Địa chỉ IP 192.168.10.16 liên tục gửi các yêu cầu HTTP kiểu GET /index.html đến máy chủ.

- Mã phản hồi 403 Forbidden:

Mỗi yêu cầu đều bị Nginx phản hồi với mã trang thái 403, nghĩa là truy cập bị từ chối.

- Nginx là thành phần trực tiếp chẩn truy cập:

Đây không phải do tường lửa hệ thống, mà là do **Nginx đã được cấu hình bảo mật** để chặn HTTP từ IP nghi ngờ (có thể chặn theo IP, User-Agent, tần suất, v.v).

- Minh chứng chống DDoS tầng ứng dụng:

Việc Nginx từ chối liên tục các truy cập bất thường cho thấy **biện pháp phòng thủ DDoS tầng 7** đang hoạt động hiệu quả, giúp ngăn truy cập độc hại vào ứng dụng web.

2.5.4 : Video demo :

Attack DDOS WebSite trên Ubuntu : <https://youtu.be/3Sqopbtvyeo>

Chống DDOS WebSite trên Ubuntu : <https://youtu.be/4xNzOtrYv6w>

2.6 Kịch bản 2 : Tấn công Fishing

2.6.1 Kịch bản mô phỏng Tấn công Phishing và Phòng thủ với Wazuh/ClamAV :

1. Chuẩn Bị Tấn Công:

- **Máy chủ Kẻ Tấn công (Kali Linux):**
 - Sử dụng Gophish để thiết lập chiến dịch lừa đảo.
 - Tạo một email lừa đảo (phishing email) với nội dung hấp dẫn (ví dụ: "Thông báo cập nhật phần mềm khẩn Unikey mới").
 - **Tạo file mã độc:** Chuẩn bị một file nén **Unikey.zip**. Bên trong file .zip này chứa mã độc thực thi.
 - Cấu hình Gophish để khi nạn nhân nhấp vào liên kết trên email, họ sẽ được chuyển hướng đến Trang Đích (Landing Page) giả mạo.
- **Trang Đích (Landing Page):**
 - Thiết kế một trang web giả mạo trông đáng tin cậy (ví dụ: trang đăng nhập dịch vụ phò biển, trang thông báo quan trọng).
 - Tích hợp một nút "Tải xuống" trên trang này. Khi nạn nhân nhấp vào, nút sẽ tự động tải file mã độc **Unikey.zip** từ máy chủ Gophish xuống máy nạn nhân.

2. Thực Hiện Tấn Công:

- **Gửi Email:** Gophish gửi email lừa đảo đã chuẩn bị tới máy nạn nhân (đã cài đặt Wazuh Agent).
- **Nạn nhân Tương tác:**
 - Nạn nhân mở email và nhấp vào liên kết, được chuyển hướng đến Landing Page giả mạo.
 - Trên Landing Page, nạn nhân bị lừa và nhấp vào nút "Tải xuống", khiến file **payload.zip** được tải về máy của họ (thường vào thư mục Downloads).
 - Tiếp đó, nạn nhân giải nén file .zip này và thực thi mã độc bên trong, kích hoạt mã độc.

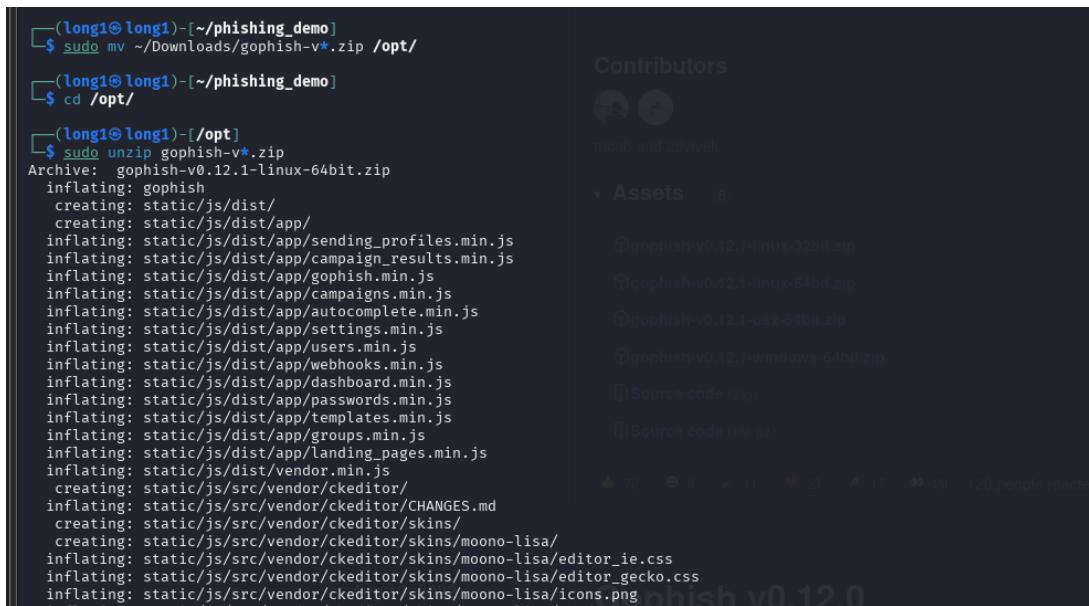
3. Giám Sát và Phát Hiện (Wazuh & ClamAV):

- **Thu thập Dữ liệu (Wazuh Agent):**
 - Wazuh Agent trên máy nạn nhân liên tục giám sát các hoạt động hệ thống (qua cấu hình Auditd và Syscheck).
 - Mọi hành vi đáng ngờ – bao gồm **việc tải xuống file .zip lạ, giải nén file .zip**, thực thi mã độc từ các thư mục tạm thời/thư mục tải xuống, và các hoạt động mạng bất thường của mã độc – đều được ghi lại.
- **Phát hiện Virus (ClamAV tích hợp):**
 - **Ngay khi file payload.zip được tải xuống**, hệ thống đã được cấu hình với

ClamAV sẽ tự động quét các thư mục tải xuống hoặc thư mục đích của file.

- **Wazuh Manager sẽ nhận được cảnh báo từ ClamAV** về việc phát hiện virus/malware trong file payload.zip hoặc file mã độc bên trong nó.
- Wazuh Manager cũng sẽ nhận được các cảnh báo từ Auditd và Syscheck về các hành vi đáng ngờ khác (như giải nén, thực thi).
- **Phản hồi tự động (Xóa/Cách ly):**
 - Dựa trên cấu hình của Wazuh và ClamAV, khi virus/malware được phát hiện, hệ thống sẽ tự động thực hiện hành động đã định (ví dụ: xóa file nhiễm virus khỏi hệ thống hoặc di chuyển vào thư mục cách ly).

2.6.2 Các bước tấn công :



The screenshot shows a GitHub repository page for "Gophish v0.12.1". On the left, there is a terminal window displaying the command-line steps to download and extract the software. On the right, the repository details are shown, including the contributors (mocab and 29vivek) and assets (zip files for various platforms: Linux 32-bit, Linux 64-bit, OS X, Windows, and source code in zip and tar.gz formats). The repository has 120 people reacting.

```
(long1@long1) [~/phishing_demo]
$ sudo mv ~/Downloads/gophish-v*.zip /opt/
(long1@long1) [~/phishing_demo]
$ cd /opt/
(long1@long1) [/opt]
$ sudo unzip gophish-v*.zip
Archive:  gophish-v0.12.1-linux-64bit.zip
  inflating: gophish
  creating: static/js/dist/
  creating: static/js/dist/app/
  inflating: static/js/dist/app/sendings_profiles.min.js
  inflating: static/js/dist/app/campaign_results.min.js
  inflating: static/js/dist/app/gophish.min.js
  inflating: static/js/dist/app/campaigns.min.js
  inflating: static/js/dist/app/autocomplete.min.js
  inflating: static/js/dist/app/settings.min.js
  inflating: static/js/dist/app/users.min.js
  inflating: static/js/dist/app/webhooks.min.js
  inflating: static/js/dist/app/dashboard.min.js
  inflating: static/js/dist/app/passwords.min.js
  inflating: static/js/dist/app/templates.min.js
  inflating: static/js/dist/app/groups.min.js
  inflating: static/js/dist/app/landing_pages.min.js
  inflating: static/js/dist/vendor.min.js
  creating: static/js/src/vendor/ckeditor/
  inflating: static/js/src/vendor/ckeditor/CHANGES.md
  creating: static/js/src/vendor/ckeditor/skins/
  creating: static/js/src/vendor/ckeditor/skins/moono-lisa/
  inflating: static/js/src/vendor/ckeditor/skins/moono-lisa/editor_ie.css
  inflating: static/js/src/vendor/ckeditor/skins/moono-lisa/editor_gecko.css
  inflating: static/js/src/vendor/ckeditor/skins/moono-lisa/icons.png
```

Hình 40. Cài đặt Gophish trên máy Kali

- Cài đặt Gophish từ Github sau đó giải nén ra và chạy

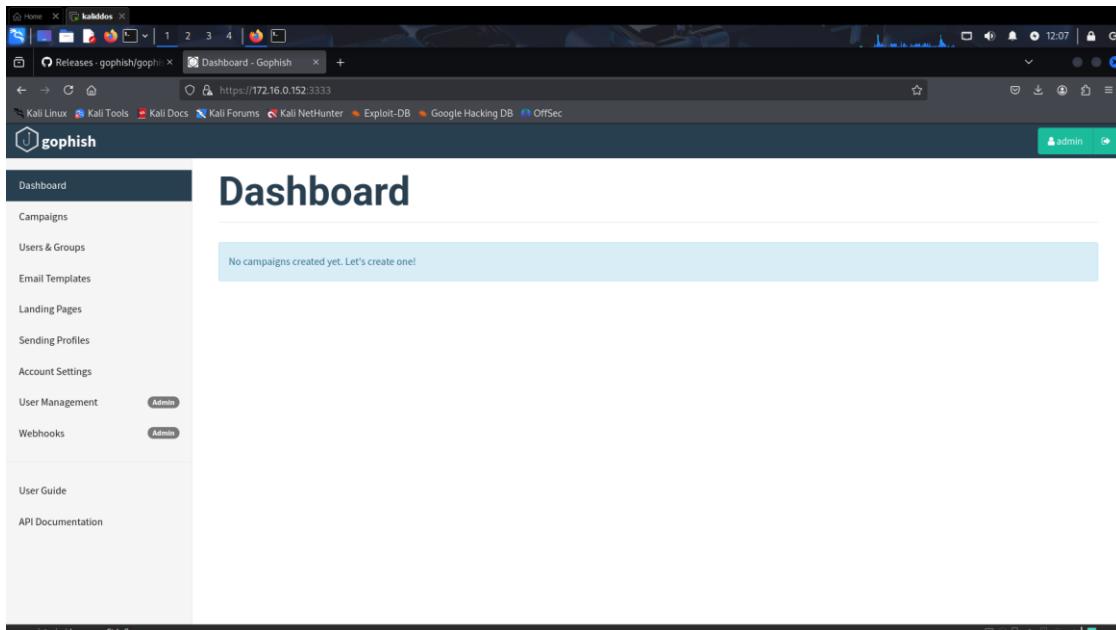
```

└──(root㉿long1)-/opt/gophish
    # sudo ./gophish
    time="2025-07-16T12:04:12-04:00" level=warning msg="No contact address has been configured."
    time="2025-07-16T12:04:12-04:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
    goose: migrating db environment 'production', current version: 0, target: 20220321133237
    OK 20160118194630_init.sql
    OK 20160131153104_0_1.2_add_event_details.sql
    OK 20160211211220_0_1.2_add_ignore_cert_errors.sql
    OK 20160217211342_0_1.2_create_from_col_results.sql
    OK 2016025173824_0_1.2_capture_credentials.sql
    OK 2016027180335_0_1.2_store_smtp_settings.sql
    OK 20160317214457_0_2_redirect_url.sql
    OK 20160605210903_0_2_campaign_scheduling.sql
    OK 20170104220731_0_2_result_statuses.sql
    OK 20170219122503_0_2.1_email_headers.sql
    OK 20170827141312_0_4_utc_dates.sql
    OK 20171027213457_0_4.1_maillogs.sql
    OK 20171208201932_0_4.1_next_send_date.sql
    OK 20180223101813_0_5.1_user_reporting.sql
    OK 20180524203752_0_7.0_result_last_modified.sql
    OK 20180527213648_0_7.0_store_email_request.sql
    OK 20180830215615_0_7.0_send_by_date.sql
    OK 20190105192341_0_8.0_rbac.sql
    OK 20191104103306_0_9.0_create_webhooks.sql
    OK 20200116000000_0_9.0_imap.sql
    OK 20200619000000_0_11.0_password_policy.sql
    OK 20200730000000_0_11.0_imap_ignore_cert_errors.sql
    OK 20200914000000_0_11.0_last_login.sql
    OK 20201201000000_0_11.0_account_locked.sql
    OK 20220321133237_0_4.1_envelope_sender.sql
    time="2025-07-16T12:04:12-04:00" level=info msg="Please login with the username admin and the password a3dcac4f5ec06bf7"
    time="2025-07-16T12:04:12-04:00" level=info msg="Creating new self-signed certificates for administration interface"
    time="2025-07-16T12:04:12-04:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
    time="2025-07-16T12:04:12-04:00" level=info msg="Starting IMAP monitor manager"
    time="2025-07-16T12:04:12-04:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"

```

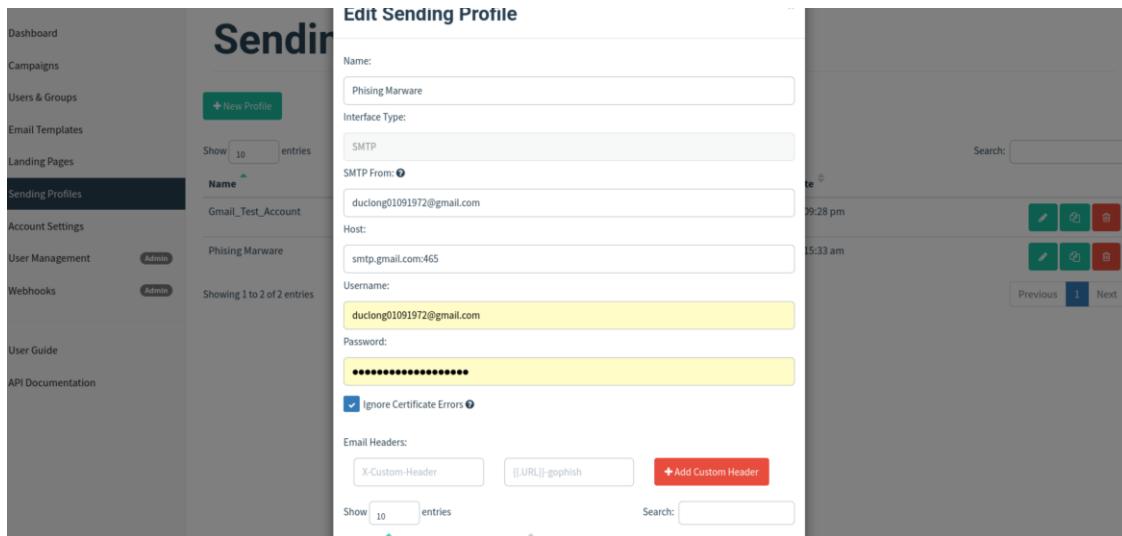
Hình 41. Thực thi gophish để có thẻ truy cập vào giao diện

- Di chuyển vào đường dẫn /opt/gophish sau đó chạy lệnh ./gophish để truy cập giao diện web Gophish



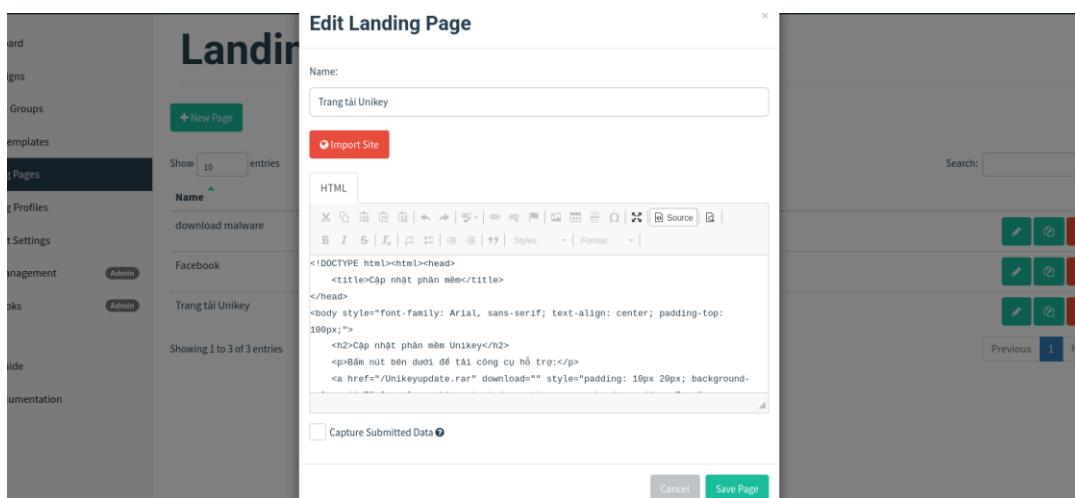
Hình 42. Giao diện chính của Gophish

- Truy cập bằng IP của máy kali và port mà gophish lắng nghe là 3333



Hình 43. Tạo 1 hồ sơ gửi chứa thông tin về máy Chủ SMTP trên Gophish

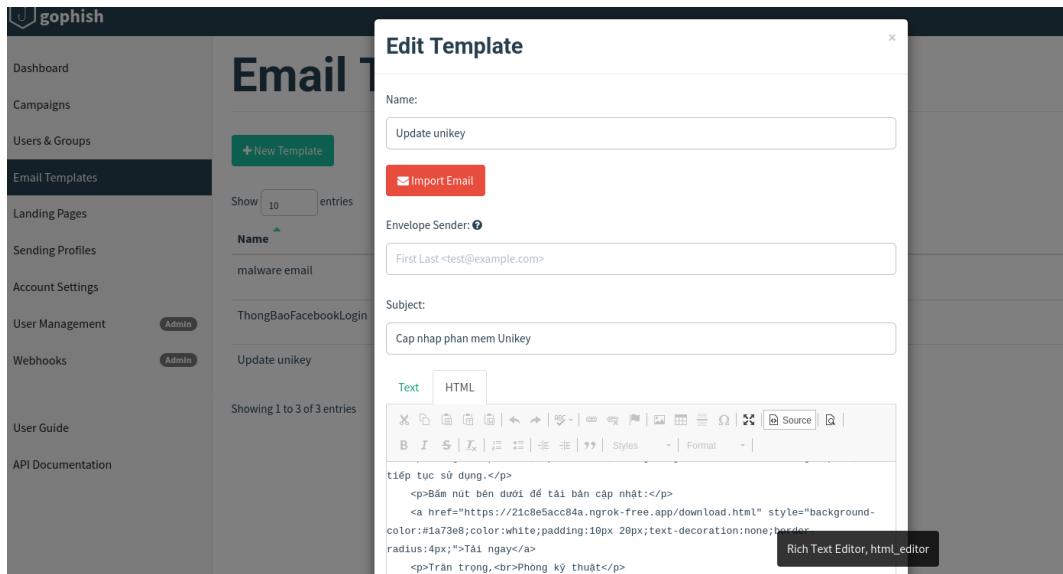
- Tạo 1 trang hồ sơ gửi trên mục Sending Profiles trong Gophish
- **Mục đích:** Cho phép GoPhish gửi email đi. Bạn có thể sử dụng các dịch vụ email hợp pháp (như tài khoản Gmail phụ, Outlook, Zoho Mail...) hoặc một máy chủ SMTP của riêng bạn.



Hình 44. Tạo 1 trang giao diện có nút tải xuống trên Gophish

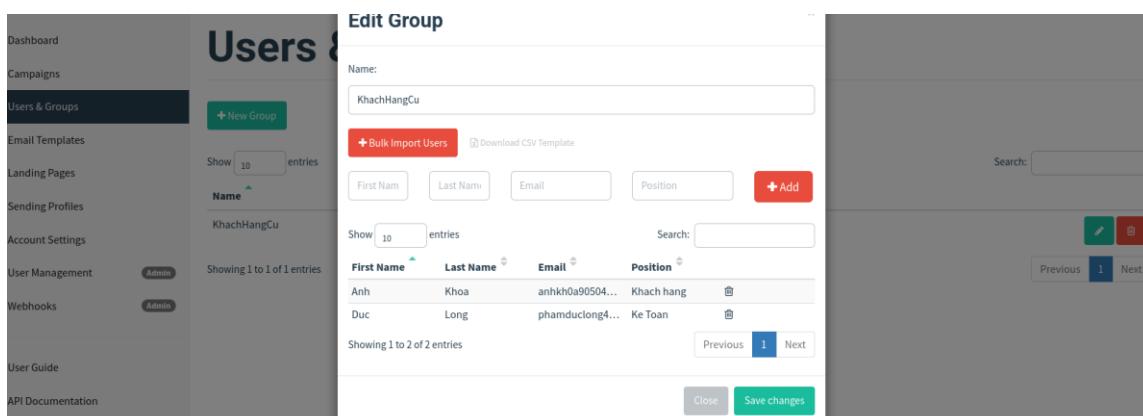
- **Chuyển hướng:** Nạn nhân nhấp vào liên kết trong email lừa đảo và bị chuyển đến trang đích giả mạo.
- **Dụ tải xuống:** Trang này được thiết kế giống thật, có nút "Tải xuống bản cập nhật" để dụ người dùng.

- **Tải mã độc:** Khi nhấn nút, một tệp mã độc (ví dụ: Unikey.zip) được tải về từ máy chủ kẻ tấn công.
- **Thực thi:** Nạn nhân bị lừa chạy tệp vừa tải.
- **Kích hoạt:** Mã độc bắt đầu hoạt động: chiếm quyền, đánh cắp dữ liệu, hoặc cài phần mềm độc hại khác.



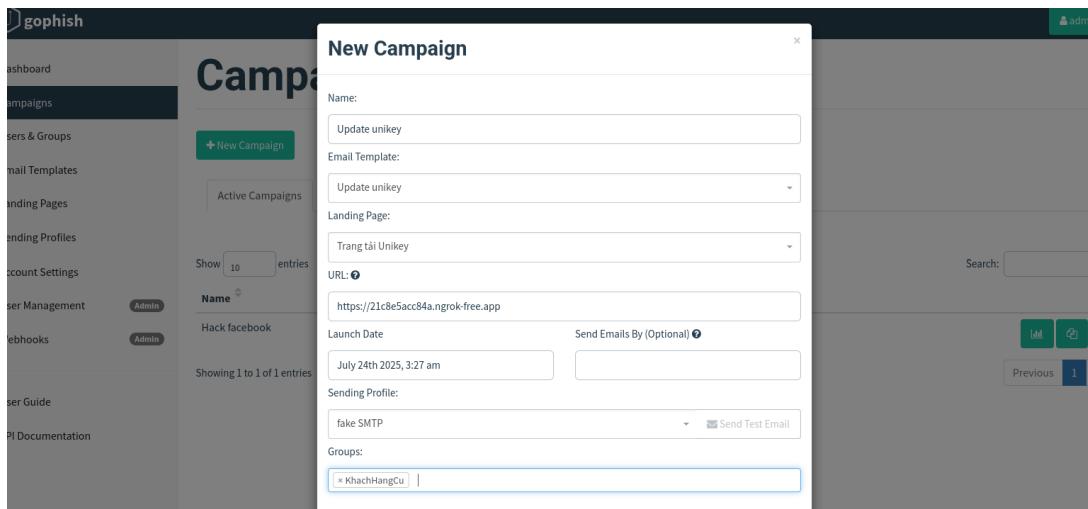
Hình 45. Tạo 1 mẫu Email để gửi đến nạn nhân

- **Mục đích:** Để tạo ra một email trông thuyết phục nhất có thể, khuyến khích nạn nhân thực hiện hành động bạn muốn (ví dụ: nhấp vào liên kết, tải tệp đính kèm).
- **Nội dung:** Thường chứa văn bản, hình ảnh, và một liên kết (URL) dẫn đến **Landing Page** của bạn. GoPhish cho phép bạn sử dụng các biến (ví dụ: {{FirstName}}, {{Email}}, {{URL}}) để cá nhân hóa email cho từng nạn nhân.



Hình 46. Tạo Users & Groups để thực hiện chiến dịch gửi email

- **Cá nhân hóa email:** Sử dụng biến như {{FirstName}}, {{Email}} để tự động chèn thông tin người dùng vào email, giúp email trông thật và thuyết phục hơn.
- **Theo dõi chi tiết:** Ghi nhận hành vi của từng người (mở email, nhấp link, nhập dữ liệu) để đánh giá hiệu quả chiến dịch.



Hình 47. Tạo 1 chiến dịch trên Campaigns

Tạo Campaign trong GoPhish:

Là một mô phỏng tấn công phishing hoàn chỉnh gồm:

- Email:** Nội dung lừa đảo gửi đến nạn nhân.
- Landing Page:** Trang giả mạo hiển thị khi nạn nhân nhấp vào link.
- Users/Groups:** Danh sách người nhận.
- Sending Profile:** Cấu hình gửi email.

Mục đích:

- Giả lập tấn công:** Gửi hàng loạt email phishing đến các mục tiêu.
- Theo dõi hành vi:** Ghi nhận email được mở, nhấp link, gửi dữ liệu, báo cáo email.
- Phân tích kết quả:** Cung cấp báo cáo tỷ lệ nhấp, mở mail, gửi thông tin... để đánh giá mức độ nhận thức và hiệu quả chiến dịch.

Cập nhật phần mềm Unikey

duclong01091972@gmail.com

Xin chào, Chúng tôi phát hiện phần mềm bạn đang dùng đã lỗi thời. Vui lòng cập nhật để tiếp tục sử dụng. Bấm nút bên dưới để tải bản cập nhật: Tài ngay

22:12 Th 4, 23/7

duclong01091972@gmail.com

đến tôi

Xin chào,

Chúng tôi phát hiện phần mềm bạn đang dùng đã lỗi thời. Vui lòng cập nhật để tiếp tục sử dụng.

Bấm nút bên dưới để tải bản cập nhật:

Tải ngay

Tài trọng,
Phóng kỹ thuật

03:32 (1 phút trước)

Hình 48. Email đã được gửi đến nạn nhân

- Khi email đã gửi đến nạn nhân khi nhấn vào sẽ ra 1 đường dẫn đến tải file mã độc



Hình 49. File mã độc đã được tải về máy nạn nhân

Biện pháp phòng chống Fishing

Cấu hình thiết lập rule trên máy Wazuh Agent

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

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

  <scan_on_start>yes</scan_on_start>

  <directories check_all="yes" realtime="yes">/home/khoa2/Downloads</directories>
  <! Directories to check (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>
  <!-- Files/directories to ignore -->
  <ignore>/etc/mtab</ignore>
```

G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
X Exit ^R Read File ^L Replace ^U Paste ^J Justify ^/ Go To Line

Hình 50. Cấu hình giám sát thư mục Downloads trên máy Wazuh Agent

- Dùng lệnh : sudo nano /var/ossec/etc/ossec.conf
- Tùy chọn realtime="yes" cho phép Wazuh phát hiện **ngay lập tức** khi có file mới xuất hiện trong thư mục home/khoa2/download, giúp nhanh chóng phản ứng trước mối nguy hiểm như mã độc hoặc script phishing.

Thiết lập cảnh báo trên máy Wazuh Manager

```

<rule id="100100" level="12">
<if_sid>554</if_sid>
<match>Downloads/.*\.(py|sh|exe|bat)$</match>
<description>● [PHISHING ALERT] Suspicious file extension detected in Downloads folder</description>
<group>phishing,syscheck</group>
</rule>
</group>

```

Hình 51. Rule cảnh báo phishing wazuh manager

- Dùng script/phần mềm có thể gây hại
 - Rule này được thiết kế để **phát hiện các tệp có phần mở rộng nguy hiểm** được tải xuống thư mục /home/khoa2/Downloads trên máy người dùng.
 - Rule sẽ kiểm tra xem **tệp có đuôi .py, .sh, .exe, hoặc .bat** có xuất hiện trong thư mục Downloads hay không.
 - Khi phát hiện, Wazuh sẽ sinh ra một **cảnh báo ở mức độ 12** (cảnh báo mức cao, nguy cơ nghiêm trọng).
 - Rule này được phân vào **nhóm phishing và syscheck**, giúp dễ lọc và quản lý trong giao diện Kibana hoặc Dashboard của Wazuh.
 - Rule sử dụng sự kiện từ rule gốc **sid=554**, đây là **sự kiện phát hiện tệp mới được tạo** trong hệ thống qua cơ chế Syscheck.
- Hỗ trợ phát hiện sớm hành vi tải tệp độc hại hoặc lệnh : sudo nano /var/ossec/etc/rules/local_rules.xml để thiết lập thêm rule
- **Rule ID 100100 (Level 12)**: Cảnh báo nếu file có đuôi .py, .sh, .exe, .bat – thường là script đáng ngờ, thường liên quan đến tấn công phishing, malware, hoặc thực thi mã trái phép.

Thiết lập quét virus khi file phishing có mã độc

```

37 packages can be upgraded. Run 'apt list --upgradable' to see them.
khoa2@khoa2-VMware-Virtual-Platform:~$ sudo apt install clamav clamav-daemon -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  clamav-base clamav-freshclam clamdscan libclamav12
Suggested packages:
  libclamunrar clamav-doc daemon libclamunrar11
The following NEW packages will be installed:
  clamav clamav-base clamav-daemon clamav-freshclam clamdscan libclamav12
0 upgraded, 6 newly installed, 0 to remove and 37 not upgraded.
Need to get 6,886 kB of archives.
After this operation, 32.4 MB of additional disk space will be used.

```

Hình 52. Cài đặt ClamAV và Freshclam

Cài ClamAV & Freshclam và cập nhập database:

- sudo apt install clamav clamav-daemon -y
- sudo systemctl stop clamav-freshclam

```
GNOME nano 7.2                               /usr/local/bin/clamav_realtime.sh
!/bin/bash

-----
# Cấu hình thư mục theo dõi
-----
WATCH_DIRS=
  "/home/khoa2/Downloads"
  "/home/khoa2/Du Lieu Bao Cao"

# Thư mục cách ly nếu file nhiễm virus
QUARANTINE_DIR="/home/khoa2/quarantine"
xattr -p "$QUARANTINE_DIR"

# File log
LOG_FILE="/var/log/clamav_realtime.log"
touch "$LOG_FILE"

# Regex bỏ qua các file tạm
IGNORED_EXTENSIONS=".*\.(part|cdownload|tmp|swp|swx|~)$"

-----
# Hàm xử lý quét file hoặc thư mục
-----
can_target() {
  TARGET="$1"

  # BỎ qua nếu là file tạm
  if [[ "$TARGET" =~ $IGNORED_EXTENSIONS ]]; then
    echo "$(date) BỎ qua file tạm: $TARGET" >> "$LOG_FILE"
    return
  fi

  sleep 3 # ✅ Delay 3 giây để file ổn định
```

Hình 53. Tạo 1 tệp quét Virus ClamAV theo thời gian thực

- Script này dùng để **giám sát thời gian thực** các thư mục chỉ định (như Downloads) và **tự động quét virus** khi có file mới được tạo hoặc di chuyển vào, sử dụng ClamAV (clamdscan).
 - WATCH_DIRS: Chỉ định các thư mục cần theo dõi, ví dụ như thư mục tải về.
 - QUARANTINE_DIR: Tạo thư mục để **cách ly các file nhiễm virus**.
 - IGNORED_EXTENSIONS: Bỏ qua các file tạm (.part, .crdownload, v.v.) để tránh quét nhầm.
 - scan_target(): Hàm thực hiện quét file hoặc thư mục bằng ClamAV, có thêm sleep 3 để file ổn định trước khi quét.
 - inotifywait: Công cụ lắng nghe sự kiện tạo file mới hoặc file được di chuyển vào thư mục.
 - Các log (nhật ký) được ghi lại vào /var/log/clamav_realtime.log để tiện theo dõi lịch sử quét.
 - Script chạy nền và liên tục (wait) để duy trì **bảo vệ thời gian thực**.

```
khoa2@khoa2-VMware-Virtual-Platform:~$ sudo systemctl status clamav-freshclam
● clamav-freshclam.service - ClamAV virus database updater
   Loaded: loaded (/usr/lib/systemd/system/clamav-freshclam.service; disabled)
   Active: active (running) since Tue 2025-07-22 22:08:10 +07; 6s ago
     Docs: man:freshclam(1)
           man:freshclam.conf(5)
           https://docs.clamav.net/
Main PID: 4407 (freshclam)
      Tasks: 1 (limit: 4546)
     Memory: 2.5M (peak: 2.7M)
        CPU: 14ms
      CGroup: /system.slice/clamav-freshclam.service
              └─4407 /usr/bin/freshclam -d --foreground=true

Jul 22 22:08:10 khoa2-VMware-Virtual-Platform systemd[1]: Started clamav-freshclam.
Jul 22 22:08:10 khoa2-VMware-Virtual-Platform freshclam[4407]: ClamAV update pr...
Jul 22 22:08:10 khoa2-VMware-Virtual-Platform freshclam[4407]: Tue Jul 22 22:08:...
Jul 22 22:08:10 khoa2-VMware-Virtual-Platform freshclam[4407]: Tue Jul 22 22:08:...
Jul 22 22:08:10 khoa2-VMware-Virtual-Platform freshclam[4407]: Tue Jul 22 22:08:...
Lines 1-18 (END) .. skipping..
● clamav-freshclam.service - ClamAV virus database updater
   Loaded: loaded (/usr/lib/systemd/system/clamav-freshclam.service; disabled; preset: enabled)
   Active: active (running) since Tue 2025-07-22 22:08:10 +07; 6s ago
     Docs: man:freshclam(1)
           man:freshclam.conf(5)
           https://docs.clamav.net/
Main PID: 4407 (freshclam)
      Tasks: 1 (limit: 4546)
     Memory: 2.5M (peak: 2.7M)
        CPU: 14ms
```

Hình 54. Kiểm tra hoạt động của ClamAV

- **Trạng thái:** Dịch vụ đang ở trạng thái active (running) → Freshclam đang hoạt động và cập nhật virus database.

- **Tuy nhiên:** Dịch vụ vẫn đang ở chế độ disabled (không khởi động cùng hệ thống).
- **Thời gian khởi động gần nhất:** Tue Jul 22 22:08:10 (hiện tại đang chạy được vài giây).
- **Tác vụ của dịch vụ:** Đảm bảo cơ sở dữ liệu virus (clamav) được cập nhật định kỳ qua Internet từ các mirror như database.clamav.net.

```
GNU nano 7.2                                         /etc/systemd/system/clamav-realtime.service
[Unit]
Description=ClamAV Realtime Scan Script
After=network.target

[Service]
ExecStart=/usr/local/bin/clamav_realtime.sh
Restart=always
User=root

[Install]
WantedBy=multi-user.target
```

Hình 55. File cấu hình dịch vụ clamav-realtime.service dùng cho systemd.

Dịch vụ clamav-realtime.service là **lớp vỏ quản lý tự động** cho script clamav_realtime.sh, giúp:

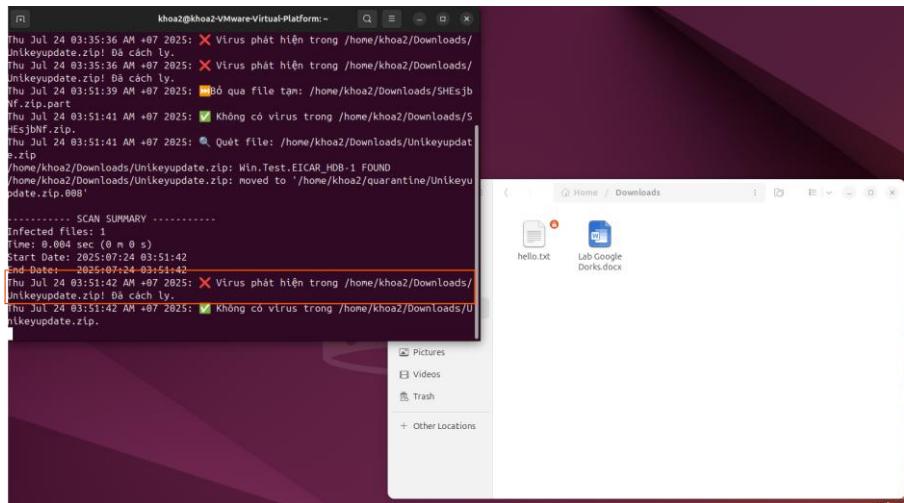
- Tự động chạy script khi khởi động máy.
- Dễ dàng quản lý (bằng systemctl start/stop/status).
- Đảm bảo script luôn hoạt động, kể cả khi bị lỗi giữa chừng.

2.6.3 Kết quả :

Jul 24, 2025 @ 03:35:33.093		● [PHISHING ALERT] Suspicious file extension detected in Downloads folder	12	100100
Table	JSON	Rule		
@timestamp	2025-07-23T20:35:33.093Z			
_id	rtn_OJgBxSqmXlSrJus			
agent.id	007			
agent.ip	192.168.100.3			
agent.name	khoa2-VMware-Virtual-Platform			
decoder.name	syscheck_deleted			
full_log	File '/home/khoa2/Downloads/Unikeyupdate.zip' added Mode: realtime			
id	1753302933.55916			
input.type	log			
location	syscheck			
manager.name	khoa-VMware-Virtual-Platform			
rule.description	● [PHISHING ALERT] Suspicious file extension detected in Downloads folder			
rule.freetimes	1			
rule.groups	local, syslog, sshd, syscheck, rootcheck, malware, phishing_detection, phishing, syscheck			

Hình 56. Wazuh manager báo log level 12 khi Agent tải file phishing

- Cảnh báo:**
[PHISHING ALERT] Suspicious file extension detected in Downloads folder
Phát hiện **file có định dạng đáng ngờ (đáng nghi ngờ chứa mã độc)** trong thư mục **Downloads**.
- File bị phát hiện:**
/home/khoa2/Downloads/Unikeyupdate.zip
- Thời gian ghi nhận:**
2025-07-23T20:35:33.093Z (tức 03:35 sáng ngày 24/07/2025 theo giờ VN)
- Chế độ giám sát:**
Mode: realtime → Hệ thống đang theo dõi **thời gian thực**.
- Nguồn ghi log:**
Agent ID: 007
IP: 192.168.100.3
Tên máy: khoa2-VMware-Virtual-Platform



Hình 57. Kết quả quét virus khi nẠn nhѧn tăi v  và ClamAV x a

- ClamAV d a ph t hi n t p m  d c Unikeyupdate.zip đ c t i v  th  m c Downloads v  d a t y d ng c ch ly.
- Sau khi c ch ly, qu t l i x c nh n kh ng c n d u hi u c u m  d c trong th  m c. Loại m  d c nh n di n l  Win.Test.EICAR_HDB-1.

2.6.4 : Video Demo :

Qu t virus th  m c v  t n c ng phishing : <https://youtu.be/yCHXAqrkuok>

2.7 K ch b n 3 : T n Brute Force

2.7.1 K ch b n m  ph ng t n c ng Brute Force :

M c ti u: Ch ng minh kh  n ng c u Wazuh trong vi c t y d ng ph t hi n v  ch n c c cu c t n c ng v t c n (Brute Force) v o d ch v  SSH.

C c th nh ph n:

- **H t th ng gi m s t Wazuh:** Bao g m Wazuh Manager v  m t Wazuh Agent tr n m y m c ti u.
- **M y ch u m c ti u:** M y t nh c u d ch v  SSH đ ng ho t d ng.
- **M y t n c ng:** M y t nh đ c s u d ng d  th c hi n cu c t n c ng Brute Force.

K ch b n:

1. Chu n B i H t Th ng:

- **T n Wazuh Manager:** D m b o Wazuh d a đ c c u h nh d  nh n di n c c cu c t n c ng Brute Force SSH v  k ch ho t t nh n ng "Active Response". T nh n ng n y s  t y d ng ch n d i a ch  IP c u k  t n c ng tr n m t kho ng th i gian nh t đ nh khi ph t hi n

hành vi đáng ngờ.

- **Trên máy chủ mục tiêu:** Dịch vụ SSH đã được cài đặt và chạy. Wazuh Agent trên máy này đã kết nối và gửi nhật ký về Wazuh Manager.

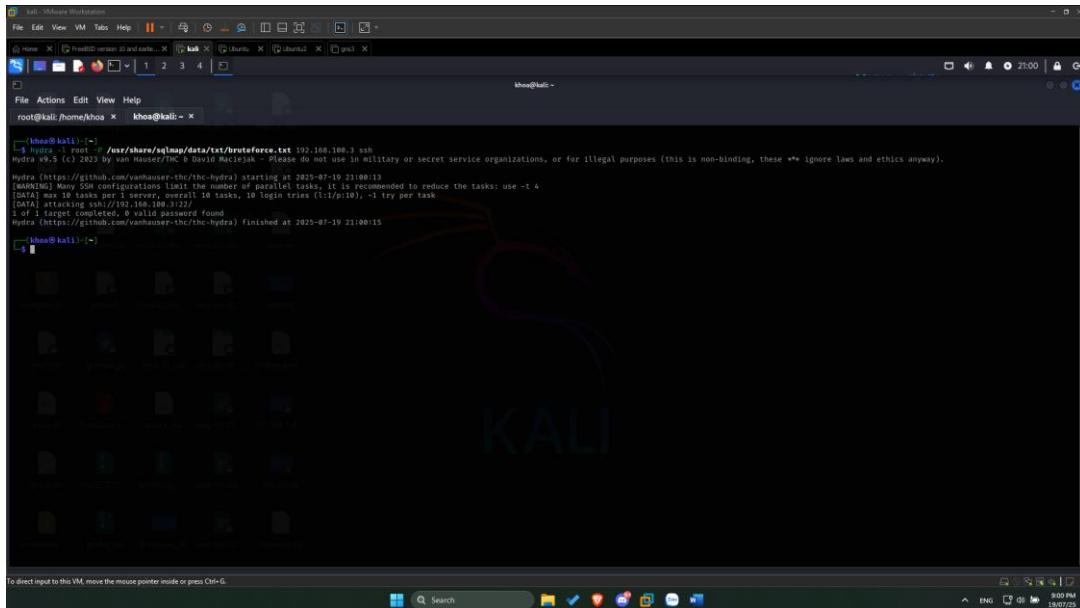
2. Thực Hiện Tấn Công Brute Force:

- **Từ máy tấn công:** Kẻ tấn công sử dụng một công cụ chuyên dụng để liên tục thử các tên người dùng và mật khẩu khác nhau nhằm đăng nhập vào máy chủ mục tiêu qua SSH. Các nỗ lực này sẽ tạo ra hàng loạt bản ghi lỗi đăng nhập trên máy chủ mục tiêu.

3. Giám Sát và Phản ứng của Wazuh:

- **Trên máy chủ mục tiêu (qua Wazuh Agent):** Wazuh Agent liên tục thu thập các nhật ký đăng nhập SSH. Khi phát hiện một số lượng lớn các lần đăng nhập thất bại liên tiếp từ cùng một nguồn, Agent sẽ ngay lập tức gửi các thông tin này về Wazuh Manager.
- **Trên Wazuh Manager:**
 - Wazuh Manager nhận các thông tin cảnh báo từ Agent.
 - Dựa trên các quy tắc đã được thiết lập, Wazuh Manager sẽ xác định đây là một cuộc tấn công Brute Force.
 - Ngay lập tức, Wazuh Manager sẽ kích hoạt "Active Response". Hệ thống sẽ ra lệnh cho máy chủ mục tiêu **thêm một quy tắc vào tường lửa để chặn tất cả các kết nối từ địa chỉ IP của máy tấn công** trong một khoảng thời gian được xác định (ví dụ: 10 phút).
- **Kiểm tra kết quả:**
 - Nếu kẻ tấn công cố gắng kết nối SSH lại từ máy tấn công, họ sẽ không thể truy cập được máy chủ mục tiêu.
 - Các nhật ký của Wazuh sẽ ghi lại chi tiết về việc phát hiện tấn công và hành động chặn IP đã được thực hiện.

2.7.2 Các bước tấn công :



Hình 58. Tấn công brute-force trên máy kali

- Lệnh :hydra -L /usr/share/kalug/data.txt -P /usr/share/kalug/data.txt 192.168.100.3 ssh
- Hydra sử dụng danh sách username và password từ file data.txt để brute-force SSH vào IP **192.168.100.3**.
- [22][ssh] host: 192.168.100.3 login: test password: 123

2.7.3 Kết quả :

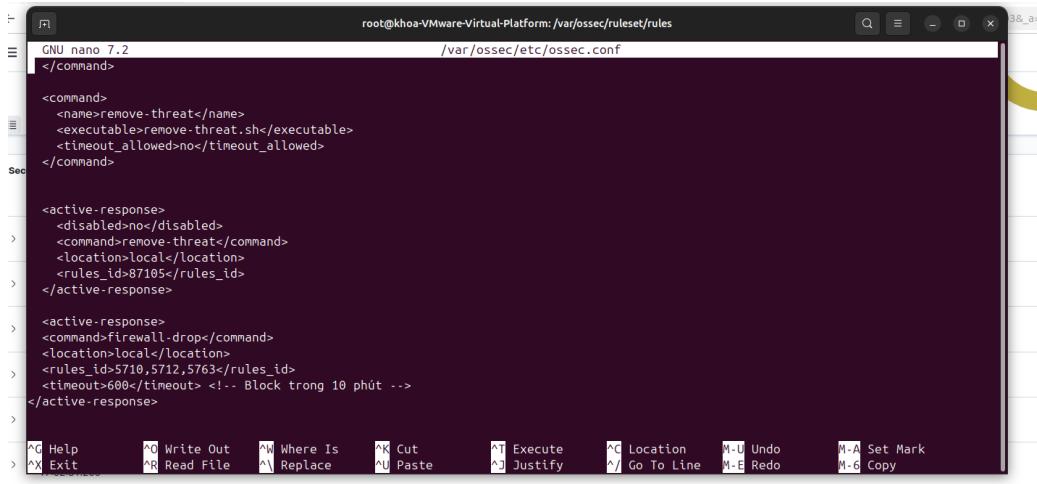
Khi không có System Endpoint

A screenshot of a terminal window showing the Hydra tool attacking an FTP service. The output shows the attack starting at 2023-05-25 11:49:44, with 16 tasks per server and 156 login tries. It successfully finds the credentials 'msfadmin:msfadmin' for host 192.168.99.7.

Hình 59. Khi chưa triển khai bảo mật chống Brute Force

- Hydra – công cụ mạnh mẽ chuyên dùng để thực hiện tấn công brute-force vào các giao thức xác thực như FTP, SSH, HTTP, v.v.
- Hydra đã dò thành công thông tin đăng nhập:
 - **Username:** msfadmin
 - **Password:** msfadmin

Giải pháp phòng tránh Brute Force



```
root@khoa-VMware-Virtual-Platform:/var/ossec/ruleset/rules
GNU nano 7.2
/var/ossec/etc/ossec.conf

</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>
<rules_id>87105</rules_id>
</active-response>

<active-response>
<command>firewall-drop</command>
<location>local</location>
<rules_id>5710,5712,5763</rules_id>
<timeout>600</timeout> <!-- Block trong 10 phút -->
</active-response>
>
```

Hình 60. Thiết lập rule chống Brute Force

Tự động chặn tấn công Brute Force:

- Wazuh định nghĩa một lệnh firewalldrop để chặn lưu lượng mạng.
- Khi có các hành vi tấn công vét cạn (brute force) được phát hiện (liên quan đến các rules_id 5716, 5712, 5763, thường là các lỗi đăng nhập liên tục), phản ứng chủ động này sẽ được kích hoạt.
- Wazuh sẽ tự động thêm một quy tắc vào tường lửa cục bộ của máy bị tấn công để chặn địa chỉ IP của kẻ tấn công trong 600 giây (10 phút), ngăn chặn các nỗ lực tấn công tiếp theo

2.7.4 Video Demo

Tấn Công Brute Force : <https://youtu.be/H2cIWNbxjiY>

Chương III : Kết luận

3.1 : Các phương án bảo mật

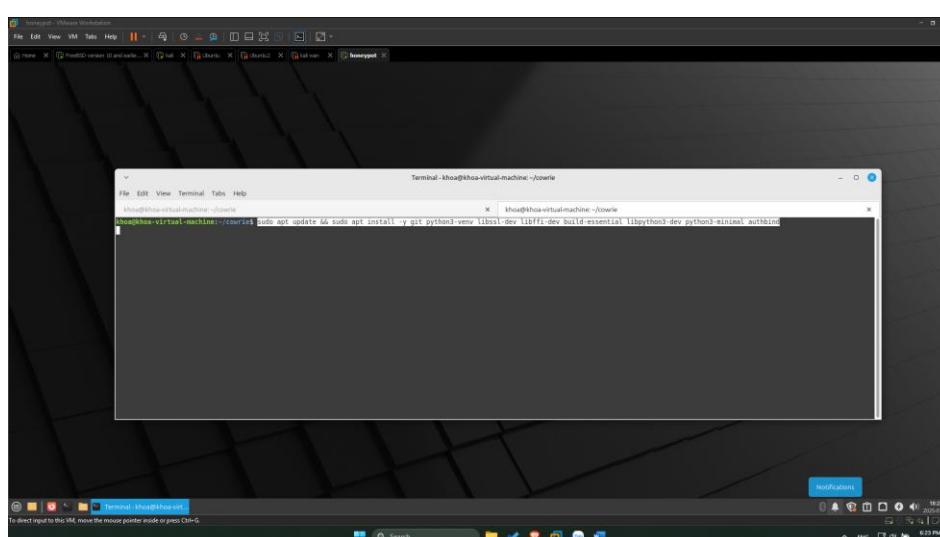
3.1.1 : Khái niệm về Honeypot

- Các đặc điểm và mục đích chính của honeypot:

- **Thu hút kẻ tấn công (Lure attackers):** Honeypot được tạo ra để trông giống như một hệ thống thật, có thể là một máy chủ web, cơ sở dữ liệu, hoặc một phần của mạng nội bộ, với các lỗ hổng bảo mật hoặc dữ liệu giả mạo trông có vẻ giá trị. Điều này kích thích sự tò mò và tham vọng của tin tặc, khiến chúng tương tác với honeypot thay vì các hệ thống thật.
 - **Phát hiện và cảnh báo (Detect and alert):** Khi tin tặc tương tác với honeypot, tất cả các hoạt động của chúng (như quét cổng, cố gắng đăng nhập, thực thi lệnh, tải lên mã độc) đều được ghi lại. Điều này giúp các chuyên gia an ninh mạng phát hiện sớm các cuộc tấn công và nhận diện các mối đe dọa mới.
 - **Thu thập thông tin tình báo (Gather intelligence):** Đây là một trong những mục đích quan trọng nhất của honeypot. Bằng cách quan sát hành vi của tin tặc trong môi trường kiểm soát này, các tổ chức có thể thu thập thông tin quý giá về:
- **Kỹ thuật, chiến thuật và quy trình (TTPs)** mà tin tặc sử dụng.
 - Các loại **mã độc** và công cụ chúng triển khai.
 - Các **lỗ hổng zero-day** (lỗ hổng chưa được biết đến hoặc chưa có bản vá).
 - **Nguồn gốc** của các cuộc tấn công (địa chỉ IP, quốc gia).
 - **Động cơ** của kẻ tấn công.

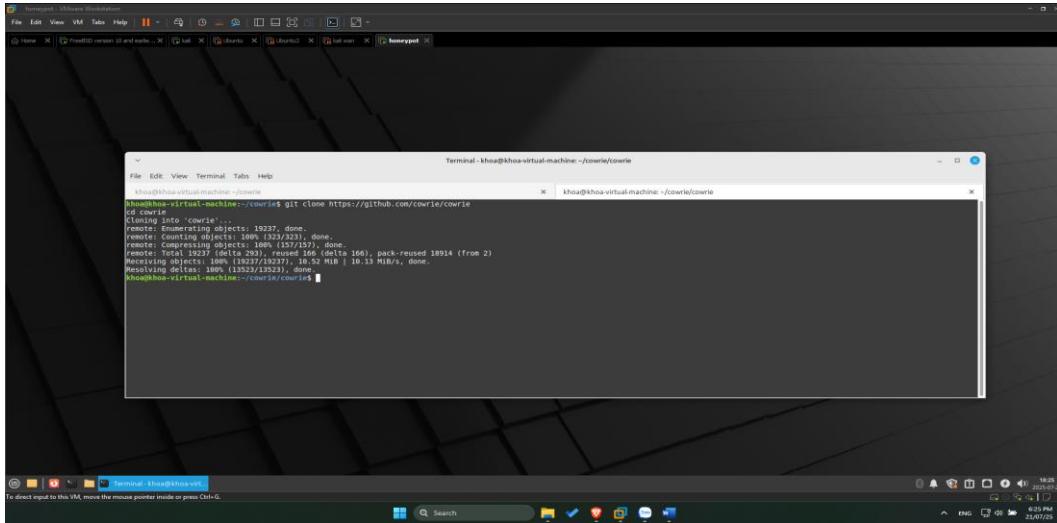
3.1.2 : Cài và cấu hình Honeypot

Bước 1 : Cài các gói cần thiết để chạy Cowrie (Python, thư viện C, v.v.)



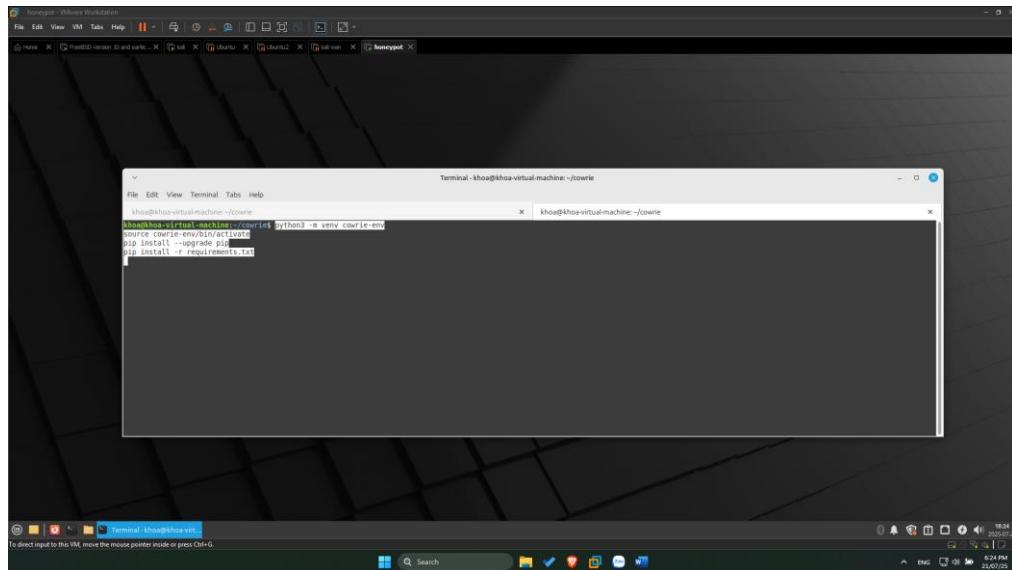
Hình 61. Cài đặt thư viện Python cần thiết

Bước 2 : clone Cowrie



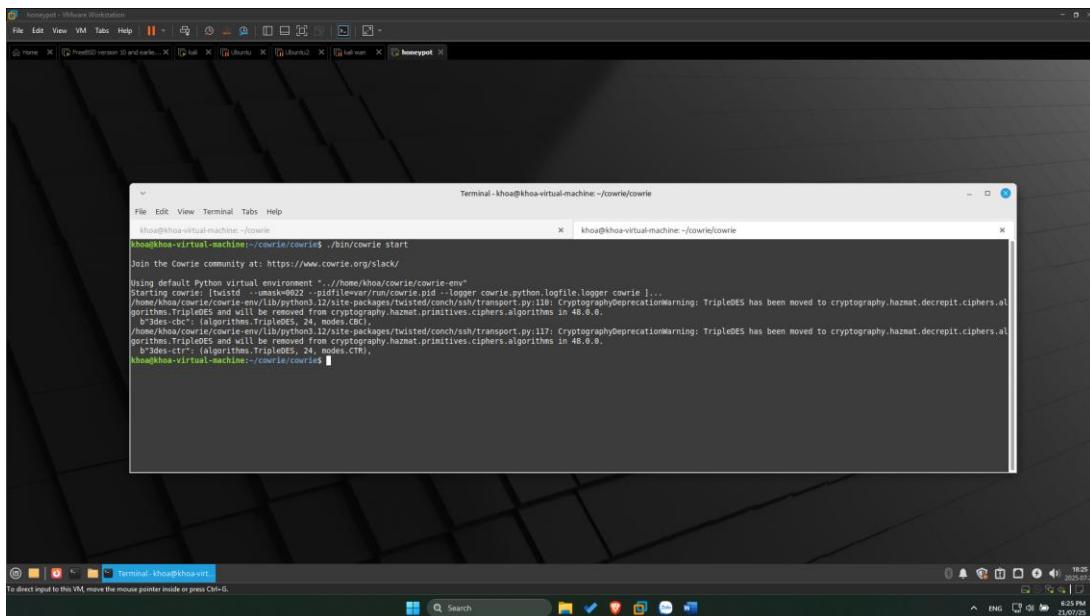
Hình 62. Clown Crowrie

Bước 3 : Tạo môi trường ảo Python và cài dependencies



Hình 63. Cài đặt môi trường cần thiết cho HoneyPot

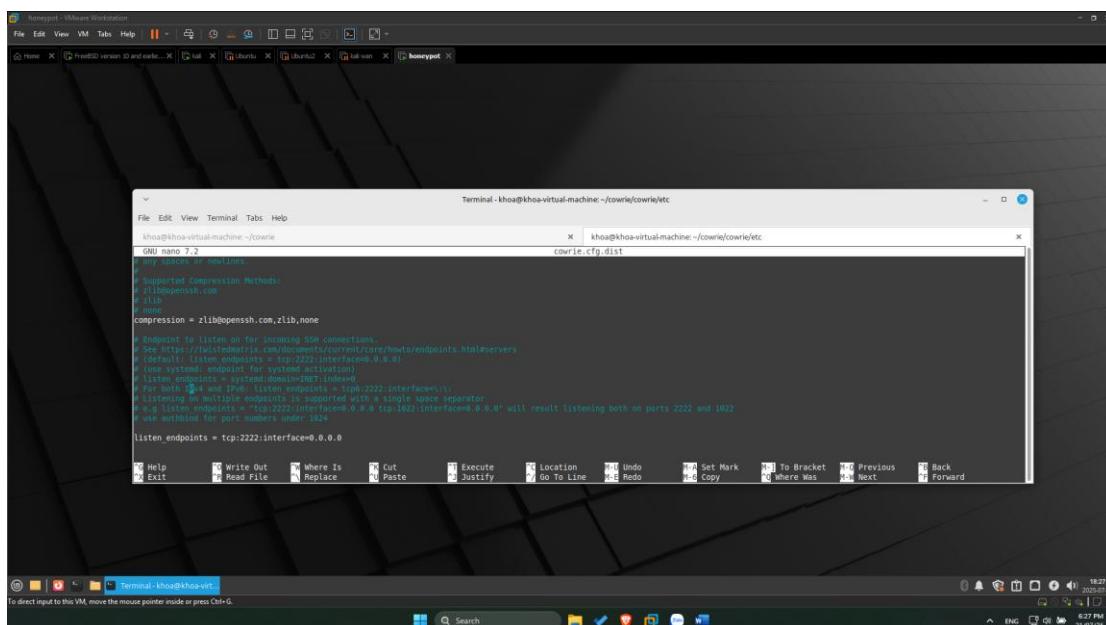
Bước 4 : Chạy Cowrie



Hình 64. Thực thi Crowrie

listen_endpoints = tcp:2222:interface=0.0.0.0

Coi config ở đây nó nói Cowrie sẽ chạy SSH honeypot trên port 2222, chấp nhận kết nối từ bất kỳ địa chỉ IP nào truy cập vào máy.



Hình 65. Cấu hình cowrie

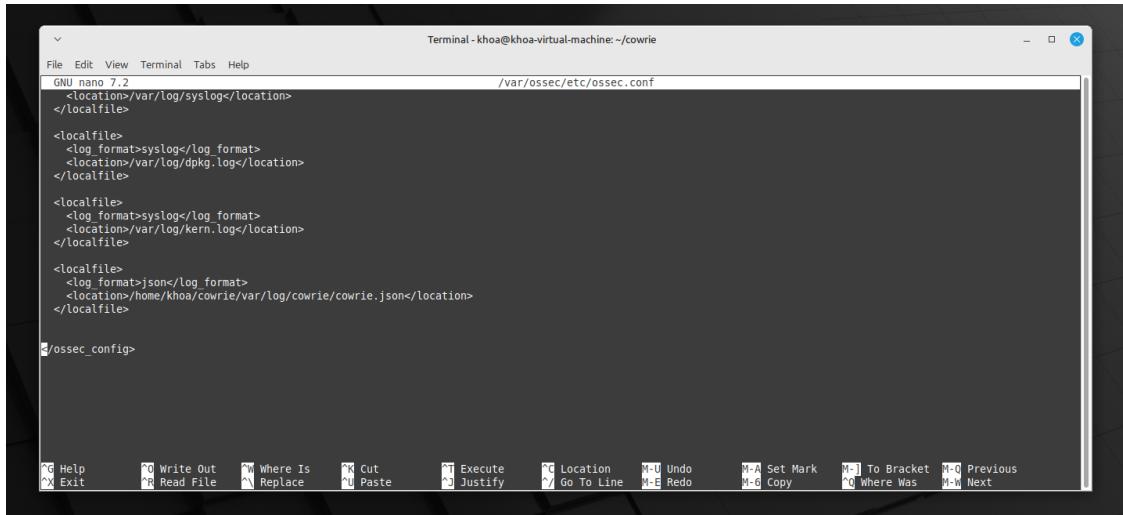
Bước 5 : Kết hợp honeypot với wazuh

```

<localfile>
  <log_format>json</log_format>
  <location>/home/khoa/cowrie/var/log/cowrie/cowrie.json</location>
</localfile>

```

Bỏ đường dẫn log của honeypot cowrie để wazuh agent gửi qua cho wazuh manager



```

<localfile>
  <log_format>json</log_format>
  <location>/home/khoa/cowrie/var/log/cowrie/cowrie.json</location>
</localfile>

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

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/kern.log</location>
</localfile>

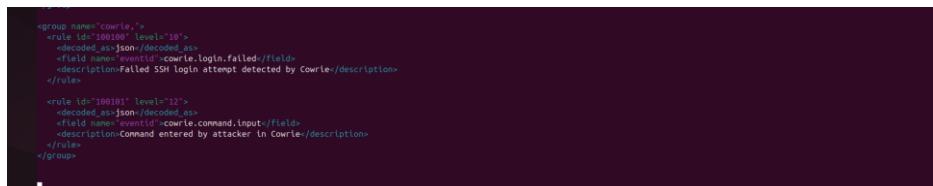
<localfile>
  <log_format>json</log_format>
  <location>/home/khoa/cowrie/var/log/cowrie/cowrie.json</location>
</localfile>

</ossec_config>

```

Hình 66.Thiết lập rules agent báo log

Bên wazuh thêm lệnh báo khi thấy log của honeypot cowrie của agent



```

<group name="cowrie">
  <rule id="100010" level="10">
    <decoded_as>json</decoded_as>
    <field name="eventid">cowrie.login.failed</field>
    <description>Failed SSH login attempt detected by Cowrie</description>
  </rule>

  <rule id="1000101" level="12">
    <decoded_as>json</decoded_as>
    <field name="eventid">cowrie.command.input</field>
    <description>Command entered by attacker in Cowrie</description>
  </rule>
</group>

```

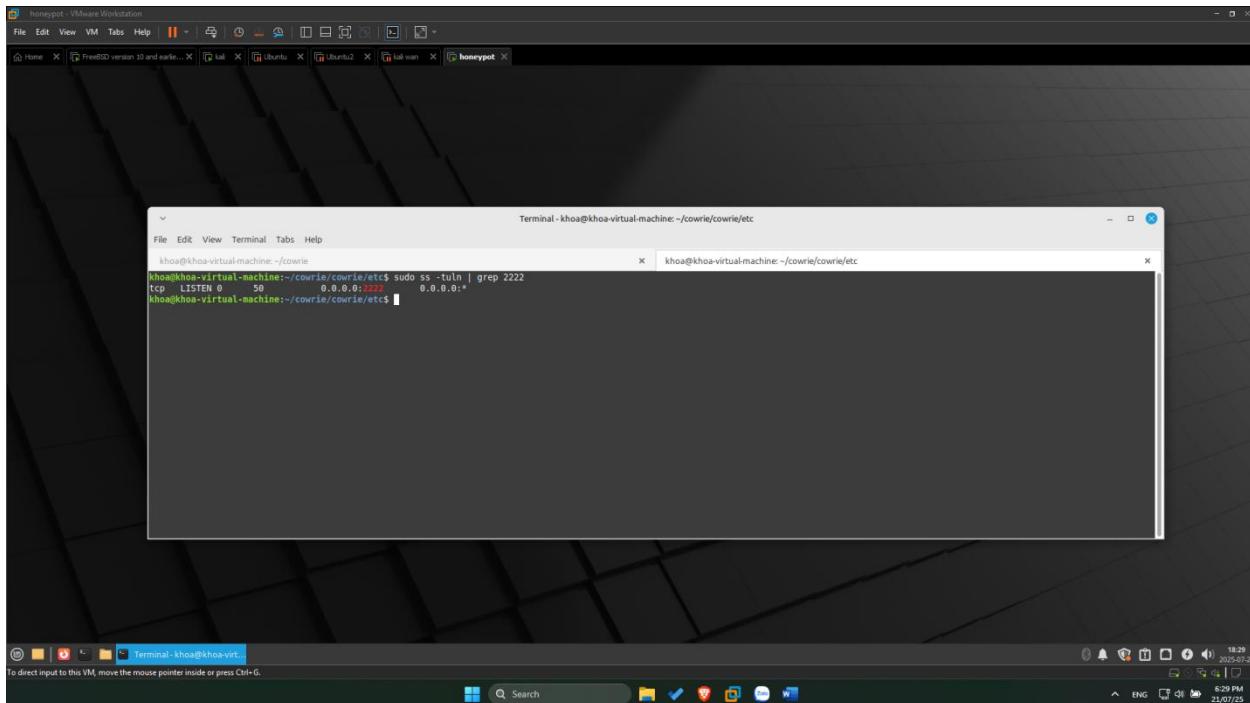
Hình 67. Thiết lập rules báo log HoneyPot trên Wazuh-manager

3.1.3 : Kết quả

Công mở

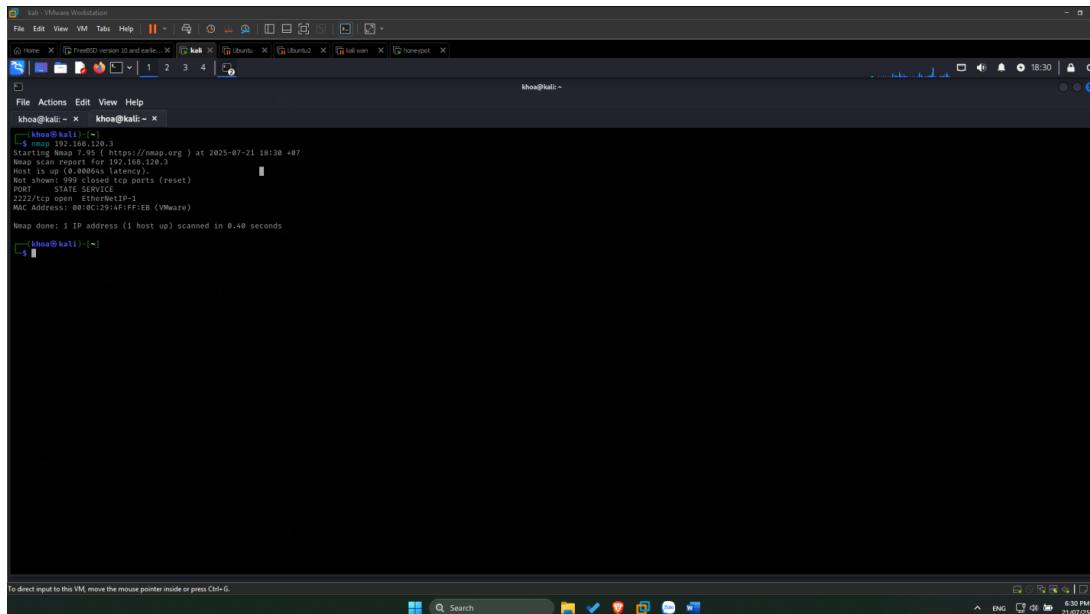
Trường hợp:

Sau nhiều lần thử mật khẩu (brute-force), attacker kết nối thành công vào Cowrie Honeypot bằng user root trên cổng SSH giả lập 2222



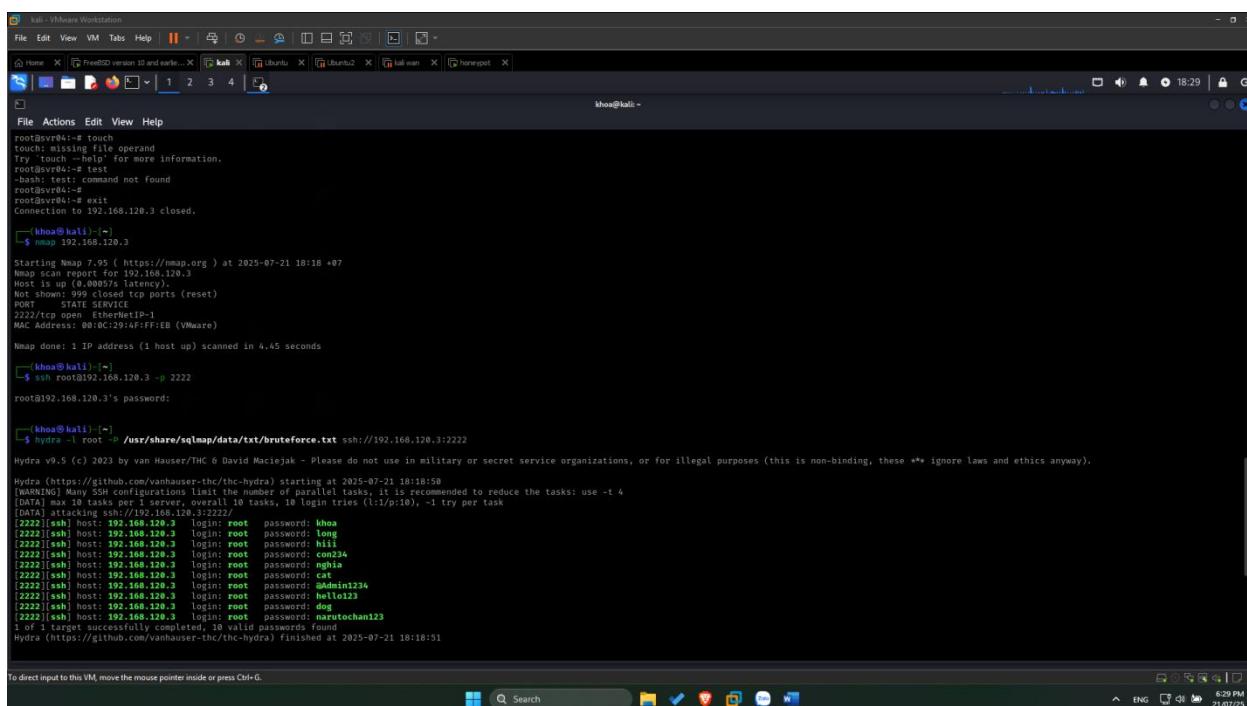
Hình 68.Cổng lắng nghe trên HoneyPot

Nó quét thì thấy mỗi cổng 2222 mở



Hình 69.Tấn công nmap trên kali đến HoneyPot

Máy tấn công kali brute force công 2222 thì mk nào cũng đúng



Hình 70. Kết quả tấn công Brute Force

Và khi ssh qua nó giới hạn nhiều lệnh dù là root vì attacker **SSH vào Cowrie Honeypot**, thì **không kết nối vào hệ thống thật**, mà kết nối vào một **hệ thống giả lập**

```
kali@kali:~$ ssh root@169.254.129.3 -p 2222
root@169.254.129.3's password:
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
copyright files in /usr/share/doc/*/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

root@kali:~# test: command not found
root@kali:~# touch hello.txt
root@kali:~# rm hello.txt
root@kali:~# hello.txt
root@kali:~# rm hello.txt
root@kali:~# ls
root@kali:~# cat hello.txt
TERMINFO: entry not found in terminfo
root@kali:~#
```

Hình 71. Lệnh tấn công SSH trên Kali

Bên honeypot thấy máy attacker làm gì dùng lệnh gì

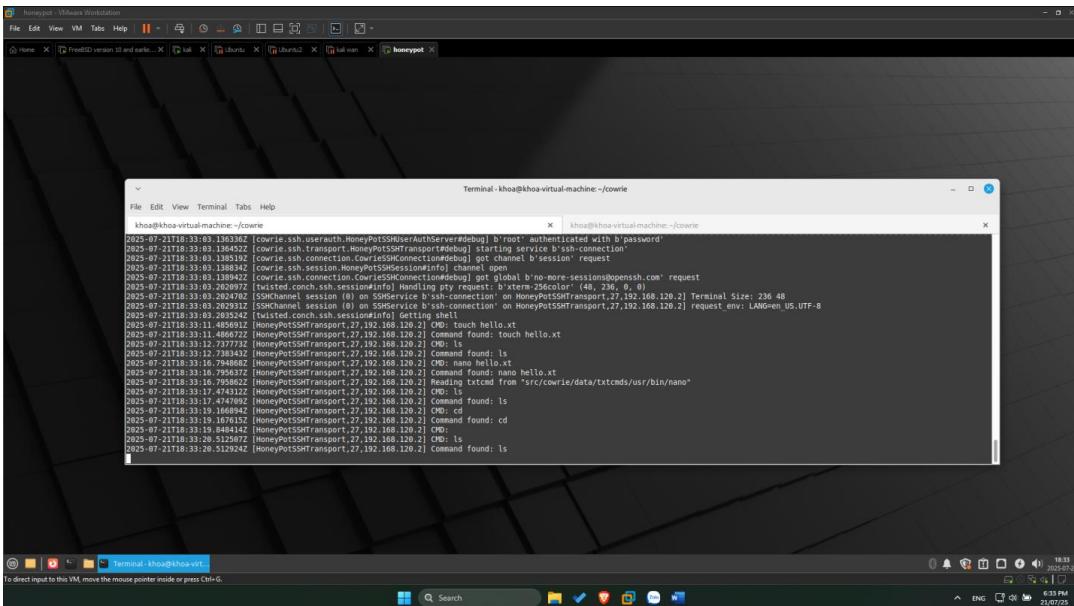
Ghi lại **toàn bộ hoạt động** của attacker:

- IP, thời gian đăng nhập
- Tên user và mật khẩu dùng để login
- Các câu lệnh gõ ra
- File mà attacker có tải về (Cowrie lưu lại bản sao file)

Không thực sự thực thi bất kỳ lệnh nào (chỉ giả lập hoàn toàn môi trường shell)

Các dữ liệu này được lưu lại để:

- Phân tích kỹ thuật
- Báo cáo lên hệ thống SIEM như Wazuh/ELK
- Phát hiện các chiến thuật và công cụ của attacker



Hình 72. Ghi lại log bên máy Honeypot

Máy Wazuh manager sẽ báo log khi bên tấn công ssh vô công của honeypot

Hình 73. Wazuh manager báo log

3.1.4 Video Demo :

Cài và cấu hình Honeypot : <https://youtu.be/JsbvvhstwP8>

Wazuh + Honeypot : <https://www.youtube.com/watch?v=nbwhPs7J5Lw>

TÀI LIỆU THAM KHẢO

STT	Tên	Link truy cập	Ngày truy cập
1	Wazuh	https://documentation.wazuh.com/current/user-manual/capabilities/malware-detection/virus-total-integration.html	16/7/2025
2	Virus Total	https://www.virustotal.com/gui/home/upload	17/7/2025

