ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

Đề tài: Research and deploy NG-Antivirus solution

GVHD: ThS. Nguyễn Duy

Nhóm:

Nguyễn Đại Nghĩa	**21521182**
Hoàng Gia Bảo	**21521848**

GIỚI THIỆU (INTRODUCTION)

1. Bối cảnh:

Trong thời đại công nghệ số ngày càng phát triển, các mối đe dọa an ninh mạng đang trở nên phức tạp và nguy hiểm hơn bao giờ hết. Các kỹ thuật tấn công hiện đại như tấn công không dùng tệp (fileless attacks), mã độc nhúng trong bộ nhớ, và scripting độc hại thông qua PowerShell đang khiến các phần mềm antivirus (AV) truyền thống dần mất hiệu quả. Những giải pháp truyền thống này chỉ tập trung vào việc phát hiện mã độc dựa trên chữ ký (signature-based detection) hoặc heuristic, và không đủ khả năng chống lại các cuộc tấn công phức tạp, đa giai đoạn.

Trong bối cảnh này, Next-Generation Antivirus (NGAV) ra đời như một bước tiến quan trọng trong lĩnh vực bảo mật điểm cuối (endpoint security). NGAV sử dụng công nghệ trí tuệ nhân tạo (AI), học máy (machine learning), và phân tích hành vi để phát hiện và ngăn chặn các cuộc tấn công tinh vi. Không chỉ dừng lại ở việc phát hiện mã độc, NGAV còn tập trung vào việc giám sát và phân tích các sự kiện liên quan đến tệp, quy trình, ứng dụng và kết nối mạng, từ đó xây dựng một lớp bảo vệ toàn diện và chủ động.

Một xu hướng nổi bật trong lĩnh vực này là sự tích hợp giữa NGAV với các giải pháp Endpoint Detection and Response (EDR), chẳng hạn như Wazuh, nhằm nâng cao khả năng phát hiện và phản ứng với các mối đe dọa trong thời gian thực. Khi kết hợp với các công cụ như ClamAV, một công cụ quét mã độc mã nguồn mở, các tổ chức có thể tận dụng sức mạnh của cả hai hệ thống để xây dựng một giải pháp bảo mật điểm cuối hiệu quả, toàn diện và tiết kiệm chi phí.

Trong đề tài này, chúng tôi tập trung nghiên cứu và triển khai NGAV như một giải pháp bảo mật tiên tiến, kết hợp với các công cụ mã nguồn mở để tối ưu hóa hiệu quả bảo vệ. Đề tài không chỉ cung cấp cái nhìn tổng quan về NGAV mà còn thử nghiệm khả năng tích hợp giữa NGAV, ClamAV, và Wazuh, nhằm đánh giá tính hiệu quả của giải pháp trong môi trường thực tế.

2. Sơ lược :

Next-Generation Antivirus (NGAV) là một giải pháp bảo mật hiện đại dành cho bảo vệ điểm cuối (endpoint security), nâng cấp đáng kể từ các phần mềm antivirus truyền thống. NGAV sử dụng cách tiếp cận dựa trên hệ thống (system-centric) và đám mây, vượt xa các phương pháp dựa trên chữ ký (signature-based) hoặc heuristic. Công nghệ này kết hợp phân tích dự đoán dựa trên trí tuệ nhân tạo (AI), học máy (machine learning), và thông tin tình báo về mối đe dọa (threat intelligence) để:

- Phát hiện và ngăn chặn các cuộc tấn công có hoặc không sử dụng mã độc (fileless attacks).
- Xác định các hành vi và chiến thuật nguy hiểm (Tactics, Techniques, and Procedures - TTPs) từ các nguồn chưa biết.
- Thu thập và phân tích dữ liệu toàn diện từ điểm cuối để tìm ra nguyên nhân gốc rễ.

- Phản ứng với các mối đe dọa mới và phức tạp mà phần mềm antivirus truyền thống không thể phát hiện.

Wazuh là một nền tảng bảo mật mã nguồn mở mạnh mẽ, được thiết kế để cung cấp các khả năng EDR, bao gồm:

- **Giám sát điểm cuối thời gian thực:**
  - Theo dõi thay đổi tệp (file integrity monitoring - FIM).
  - Phát hiện hành vi bất thường như truy cập trái phép, thay đổi cấu hình, hoặc thực thi script độc hại.
- **Phân tích nhật ký (log analysis):**
  Tích hợp với các nguồn dữ liệu bảo mật (như firewall, IDS/IPS, hoặc chính ClamAV) để phân tích các sự kiện và đưa ra cảnh báo.
- **Phát hiện và phản ứng:**
  - Phân tích hành vi dựa trên quy tắc để phát hiện tấn công.
  - Kích hoạt các hành động phản ứng tự động (ví dụ: cô lập endpoint, chặn IP).
- **Khả năng mở rộng và tích hợp:**
  Wazuh dễ dàng tích hợp với các công cụ bảo mật khác (như ClamAV) và các giải pháp SIEM để tăng khả năng phát hiện và phản ứng.

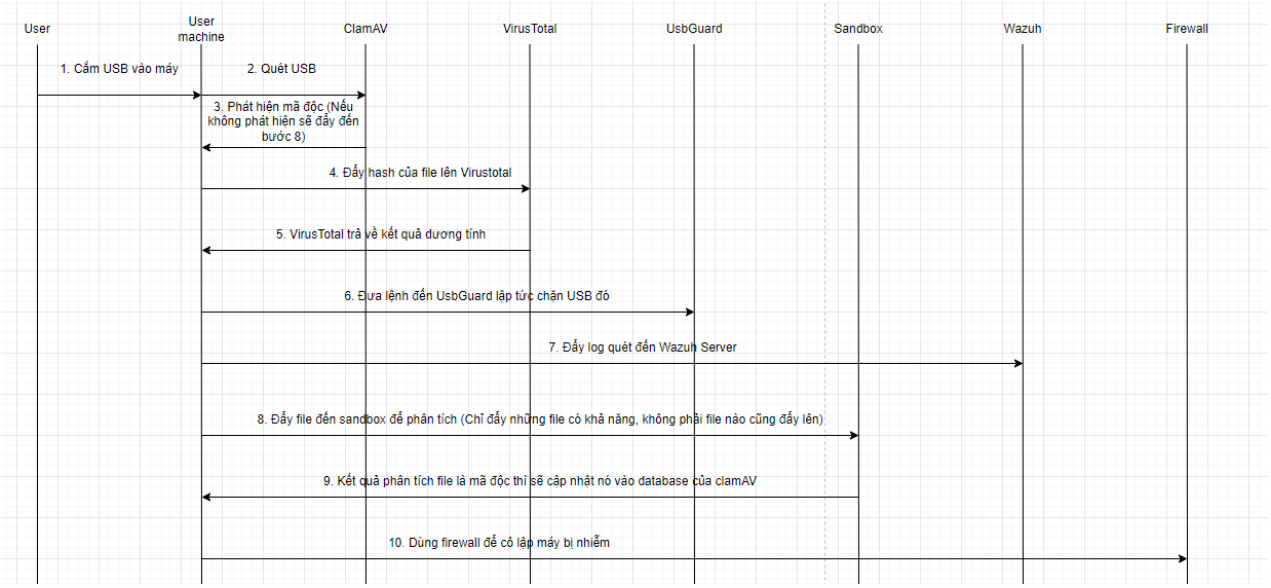
3. **Mục tiêu và phạm vi làm của nhóm:**
   Mục tiêu khi kết hợp EDR của Wazuh ,ClamAV, Sandbox,USBguard

- **Phát hiện mối đe dọa chính xác hơn**
  - **Giám sát toàn diện và thời gian thực**: Tích hợp Wazuh để giám sát và theo dõi các hoạt động trên các điểm cuối trong thời gian thực, giúp phát hiện nhanh chóng mọi hành vi bất thường hoặc có nguy cơ gây hại đối với hệ thống.
  - **Phát hiện mã độc đã biết và chưa biết**: Sử dụng ClamAV để xác minh các tệp nghi ngờ, nhận diện và phát hiện các mã độc đã được xác định trong cơ sở dữ liệu cũng như mã độc chưa biết thông qua phương pháp phân tích heuristic và cập nhật cơ sở dữ liệu thường xuyên.
  - **Phát hiện tấn công không dùng tệp (fileless attacks)**: sử dụng các phương pháp phân tích hành vi từ Wazuh để phát hiện các quy trình hoặc hành vi bất thường không liên quan đến các tệp cụ thể. Điều này giúp phát hiện và ngăn chặn các cuộc tấn công tiềm ẩn ngay cả khi không có tệp độc hại trực tiếp.
- **Quản lý bảo mật thiết bị ngoại vi hiệu quả**
  - **Kiểm soát truy cập USB với USBGuard**: Triển khai USBGuard để kiểm soát kết nối USB, bảo vệ hệ thống khỏi việc mã độc lây lan thông qua các thiết bị USB không xác định. USBGuard giúp ngừng kết nối thiết bị không rõ nguồn gốc và chỉ cho phép các thiết bị USB được xác thực trước đó. Điều này giúp giảm thiểu nguy cơ lây lan mã độc qua thiết bị ngoại vi.
  - **Cách ly và hạn chế rủi ro từ USB**: Cấu hình hệ thống để tự động quét các thiết bị USB khi cắm vào và cô lập các thiết bị USB có dấu hiệu nguy hiểm ngay lập tức, ngăn chặn sự lây lan mã độc ngay từ bước kết nối.
- **Cải thiện quản lý sự kiện bảo mật**

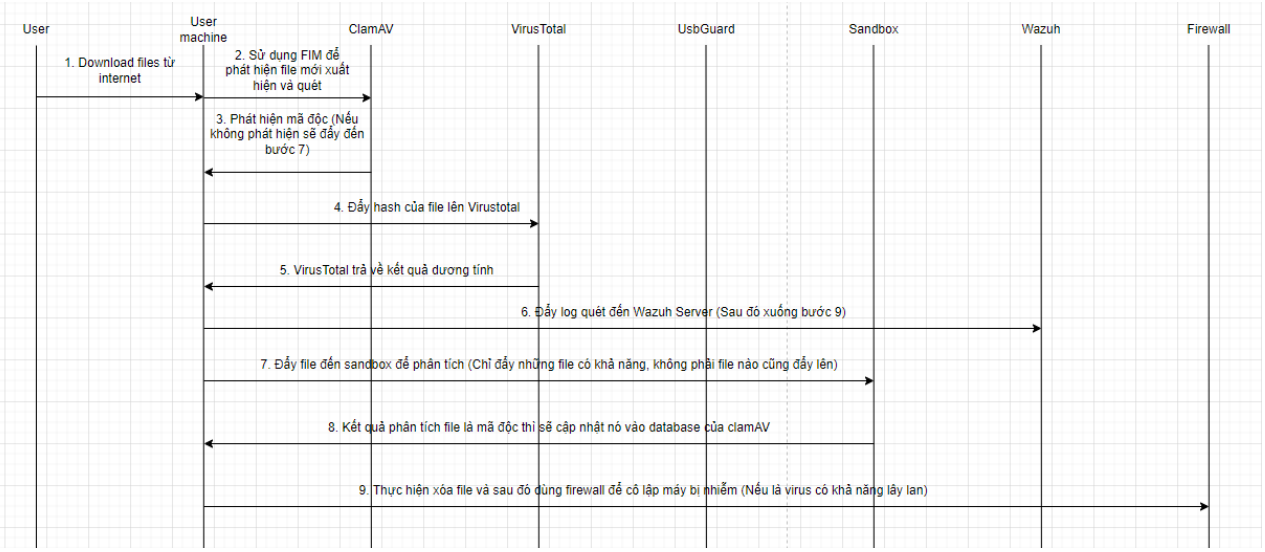
    - **Hệ thống tổng hợp dữ liệu bảo mật**: Tích hợp dữ liệu từ Wazuh và ClamAV, tạo ra một bảng điều khiển tập trung để giám sát và quản lý các sự kiện bảo mật. Điều này sẽ giúp đội ngũ bảo mật dễ dàng theo dõi các mối đe dọa, phân tích và phản ứng kịp thời.
    - **Phân tích nguyên nhân gốc rễ (Root Cause Analysis)**: Phát triển quy trình phân tích nguyên nhân gốc rễ để xác định nguyên nhân sâu xa của các sự cố bảo mật và nhanh chóng giải quyết các vấn đề. Điều này giúp ngăn chặn các sự cố tái diễn và đảm bảo tính ổn định của hệ thống.
- **Triển khai giải pháp bảo mật hiệu quả và tiết kiệm**
    - **Giải pháp bảo mật nguồn mở**: Sử dụng các giải pháp bảo mật nguồn mở như Wazuh và ClamAV để giảm chi phí bản quyền mà không làm giảm chất lượng bảo vệ. Điều này giúp doanh nghiệp giảm thiểu chi phí mà vẫn duy trì hiệu quả bảo mật cao.
    - **Khả năng tùy chỉnh giải pháp**: Xây dựng một giải pháp có khả năng tùy chỉnh cao, phù hợp với nhu cầu cụ thể của các doanh nghiệp vừa và nhỏ hoặc môi trường hoạt động đặc thù. Điều này giúp mở rộng và tối ưu hóa hệ thống bảo mật theo yêu cầu của từng tổ chức.
- **Đánh giá và cải tiến qua môi trường thực tế**
    - **Thử nghiệm và tối ưu hóa**: Triển khai hệ thống trên các hệ thống máy chủ và máy trạm thực tế để kiểm tra hiệu quả phối hợp giữa Wazuh và ClamAV trong điều kiện môi trường hoạt động thực tế. Ghi nhận các kết quả về tốc độ phát hiện, số lượng mối đe dọa được xử lý, và thời gian phản ứng để tối ưu hóa hệ thống và cải thiện hiệu quả bảo mật.
    - **Phân tích kết quả thử nghiệm**: Dựa trên các thử nghiệm thực tế, xác định các yếu tố cần cải tiến và tối ưu hóa giải pháp bảo mật, bao gồm việc điều chỉnh các thuật toán phân tích, nâng cấp cơ sở dữ liệu và cấu hình hệ thống cho phù hợp với các yêu cầu bảo mật mới.
- **Nâng cao khả năng ngăn chặn mối đe dọa mới nổi**
    - **Dự đoán và ngăn chặn các mối đe dọa mới**: Tích hợp dữ liệu từ Wazuh và ClamAV để nhận diện các mẫu hành vi mới, giúp hệ thống có khả năng dự đoán và ngăn chặn các tấn công chưa từng được ghi nhận. Điều này giúp hệ thống luôn sẵn sàng ứng phó với các mối đe dọa mới mà chưa có dấu hiệu rõ ràng trong cơ sở dữ liệu.
    - **Chiến lược bảo mật chủ động**: Phát triển chiến lược bảo mật chủ động bằng cách sử dụng phân tích dự đoán (predictive analytics) và thông tin tình báo mối đe dọa (threat intelligence). Phân tích này sẽ giúp phát hiện và ngăn chặn các mối đe dọa tiềm ẩn trước khi chúng có thể gây hại.
- **Tăng cường khả năng phân tích và cô lập mã độc qua Sandbox (CapeV2)**
    - **Phân tích hành vi mã độc với Sandbox**: Triển khai CapeV2 sandbox để phân tích hành vi mã độc trong môi trường an toàn, nhằm phát hiện các mẫu tấn công tinh vi. Các tệp nghi ngờ sẽ được đẩy vào sandbox để kiểm tra chi tiết, phát hiện và phân tích các hoạt động độc hại trước khi chúng có thể gây ra thiệt hại cho hệ thống.
    - **Xây dựng cơ sở dữ liệu mẫu mã độc**: Các mã độc được phát hiện và phân tích trong sandbox sẽ được sử dụng để làm giàu cơ sở dữ liệu ClamAV, giúp hệ thống ngày càng mạnh mẽ hơn trong việc nhận diện các mối đe dọa mới và chưa được biết đến.

II. KIẾN TRÚC HỆ THỐNG ĐỀ XUẤT

Dưới đây là sequence flow trong trường hợp user cắm USB vào máy:



Dưới đây là sequence flow trong trường hợp user download files từ internet về:



III. PHƯƠNG PHÁP TRIỂN KHAI

1. Mô Tả Tổng Quan Hệ Thống

Hệ thống bảo mật được triển khai nhằm phát hiện và ngăn chặn mã độc từ các nguồn như USB và tải file từ internet. Hệ thống bao gồm các thành phần chính sau:

- **ClamAV**: Phần mềm quét virus mã nguồn mở.
- **USBGuard**: Công cụ quản lý và bảo vệ các thiết bị USB.
- **VirusTotal**: Dịch vụ kiểm tra mã độc từ nhiều công cụ antivirus khác nhau.
- **Capev2**: Sandbox để phân tích và phát hiện mã độc.
- **Wazuh**: Hệ thống giám sát và ghi log.
- **Firewall**: Công cụ ngăn chặn và cô lập các máy nhiễm virus trong mạng (Firewall là bước cuối cùng mà nhóm sẽ làm, nên là thời điểm hiện tại nhóm chưa xác định được sẽ dùng iptables hay pfsense).

Hệ thống thực hiện quét tự động các file khi USB được cắm vào hoặc khi người dùng tải file từ internet về máy, từ đó phát hiện mã độc và đưa ra các biện pháp bảo vệ.

2. Chuẩn Bị Môi Trường Triển Khai

Trước khi triển khai hệ thống, các yêu cầu về phần cứng và phần mềm đã được nhóm chuẩn bị đầy đủ:

- **Phần cứng**:
  - Máy host chạy ubuntu server có khả năng chạy các phần mềm quét virus và bảo mật.
  - Máy ảo chạy Wazuh Server và Capev2.

- **Phần mềm**:
  - **ClamAV**: Cài đặt trên máy host để quét các file và USB.
  - **USBGuard**: Cài đặt trên máy host để quản lý các thiết bị USB và thực hiện việc chặn USB khi phát hiện mã độc.
  - **VirusTotal**: Cấu hình API để có thể gửi file lên dịch vụ này và nhận kết quả kiểm tra mã độc.
  - **Capev2**: Cài đặt và cấu hình sandbox để phân tích các file nghi ngờ.
  - **Wazuh**: Cài đặt agent trên máy host, server trên máy ảo khác, để gửi log về server, ghi lại các sự kiện bảo mật.
  - **Firewall**: Cấu hình tường lửa để cô lập máy bị nhiễm trong trường hợp phát hiện mã độc.

IV. TIẾN ĐỘ ĐẾN THỜI ĐIỂM HIỆN TẠI

Hiện tại nhóm đã deploy thành công được ClamAV, UsbGuard, Wazuh agent, server.

Còn với sandbox, FIM, firewall thì vẫn chưa hoàn thành. Trong đó thì công việc chính hiện tại của nhóm là đang cố gắng deploy thành công sandbox.

Em đã dựng thành công máy ảo sandbox cài Capev2 rồi, và bây giờ thì đang cài đặt và kết nối máy ảo phân tích virus lồng vào máy ảo sandbox trên.

V. TÀI LIỆU THAM KHẢO

Một số trang report về virus : https://tria.ge/ , https://bazaar.abuse.ch/, https://www.virustotal.com/,

ClamAV : https://docs.clamav.net

Wazuh: https://documentation.wazuh.com/current/index.html

UsbGuard: https://usbguard.github.io/documentation/compilation.html

Capev2: https://capev2.readthedocs.io/en/latest/installation/index.html