

Bài thực hành: Tìm hiểu về công cụ ClamAV

**TÌM HIỂU BÀI THỰC HÀNH**

**PTIT - ClamAV**

**Giảng viên:** Đinh Trường Duy

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

* + 1. Nội dung và hướng dẫn bài thực hành
  1. Mục đích

Bài lab này nhằm giúp sinh viên hiểu về cách sử dụng ClamAV để phát hiện mã độc trên hệ thống máy tính. ClamAV là một công cụ mã nguồn mở dành cho Linux và Unix, được sử dụng phổ biến để quét và phát hiện các mối đe dọa từ mã độc, virus, và phần mềm độc hại khác. Trong khi YARA là một công cụ mã hóa mở và một ngôn ngữ phân tích malware, được sử dụng để tạo các quy tắc để phát hiện các mẫu mã độc hại dựa trên các đặc điểm cụ thể của chúng.

YARA có thể tích hợp với ClamAV thông qua việc sử dụng các plugin hoặc scripts phù hợp. Bằng cách này, ClamAV có thể sử dụng quy tắc YARA để tăng cường khả năng phát hiện malware của nó. Khi ClamAV quét các tệp tin hoặc thư mục, nó có thể sử dụng quy tắc YARA để kiểm tra xem các tệp tin này có khớp với các điều kiện được xác định trong quy tắc hay không. Nếu có sự khớp, ClamAV có thể cảnh báo về sự hiện diện của mẫu độc hại mà quy tắc YARA đã xác định. Điều này giúp cải thiện khả năng phát hiện và ngăn chặn các mối đe dọa từ phần mềm độc hại trên hệ thống sử dụng ClamAV.

Để hiểu hơn cách viết luật YARA, sinh viên có thể tham khảo link sau:

[*https://yara.readthedocs.io/en/stable/writingrules.html*](https://yara.readthedocs.io/en/stable/writingrules.html)

* 1. Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, công cụ ClamAV và VirusTotal.

* 1. Nội dung thực hành

ClamAV là một công cụ miễn phí dùng để phát hiện và loại bỏ virus và phần mềm độc hại trên hệ thống máy tính. Nó cung cấp khả năng quét tệp tin, email và các tài nguyên web để bảo vệ khỏi các mối đe dọa tiềm ẩn. ClamAV thường được sử dụng trên các máy chủ và hệ thống Linux để bảo vệ dữ liệu và cung cấp một lớp bảo vệ bổ sung cho người dùng

**Khởi động bài lab:**

- Vào terminal, gõ:

*labtainer ptit-clamav*

*(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)*

**Các nhiệm vụ:**

- Task 1: Chạy và cập nhật cơ sở dữ liệu ClamAV.

+ Sau khi khởi động xong 1 terminal ảo sẽ xuất hiện. Trên terminal **ảo**thực hiện kiểm tra trạng thái ứng dụng ClamAV:

*sudo systemctl status clamav-freshclam.service*

+ Nếu ứng dụng ClamAV đang hoạt động, hãy dừng lại để cập nhật cơ sở dữ liệu bằng câu lệnh sau:

*sudo systemctl stop clamav-freshclam.service*

Lệnh **freshclam** là một công cụ trong ClamAV được sử dụng để cập nhật cơ sở dữ liệu virus definitions một cách định kỳ. Khi được chạy, freshclam kết nối đến các máy chủ ClamAV để tải về các cập nhật mới nhất về các mẫu virus và phần mềm độc hại. Việc cập nhật định kỳ giúp đảm bảo rằng ClamAV luôn có thông tin mới nhất về các mối đe dọa, tăng khả năng phát hiện và ngăn chặn các vấn đề bảo mật trên hệ thống máy tính.

+ Trên terminal sử dụng lệnh **freshclam**:

*sudo apt update*

*sudo freshclam*

Câu lệnh trên sẽ cập nhập lại các tệp trong **/var/lib/clamav.** Sinh viên có thể mở các file database ở đây để xem thêm về các luật có sẵn.

- Task 2: Quét 1 file độc hại.

+ Lệnh **clamscan** trong ClamAV được sử dụng để quét các tệp tin hoặc thư mục để phát hiện và loại bỏ virus và phần mềm độc hại. Sinh viên hãy quét thử file **testfile.exe** với cú pháp cơ bản của lệnh clamscan như sau:

*sudo clamscan <filename>*

- Task 3: Quét thư mục độc hại.

+ Trong thư mục **malware** có 1 file chứa mã độc. Bây giờ hãy quét cả thư mục file bằng ClamAV:

*sudo clamscan <foldername>*

* ClamAV có thông báo phát hiện được mã độc không? Tại sao?

+ Bây giờ nhiệm vụ của sinh viên là vào thư mục malware và tạo mã hash MD5 của các file trong thư mục malware bằng lệnh:

*md5sum <filename>*

+ Sau đó, sinh viên sử dụng công cụ trực tuyến Virustotal để quét thử các file trong thư mục malware.

* Các file nào trong thư mục malware là file độc?

+ Tìm kiếm thành công file mã độc, sinh viên thực hiện tạo file chứa chữ ký mã độc:

*sigtool --md5 <filename> > md5.hdb*

+ Tiếp theo, sinh viên di chuyển file chữ ký vào trong **/var/lib/clamav** và thực hiện cập nhật lại cơ sở dữ liệu của clamAV.

+ Cuối cùng, sinh viên thực hiện quét lại thư mục chứa mã độc.

- Task 4: Viết rule Yara.

+ Trong thư mục gốc của lab có 1 malware là **backdoor.py**, sinh viên thực hiện sử dụng công cụ trực tuyến VirusTotal và ClamAV để quét thử.

* Kết quả sau khi quét như thế nào?

+ Bây giờ, hãy mở tệp malware và kiểm tra xem có gì đáng ngờ. Sau đó, mở file detect.yara và viết theo định dạng có sẵn.

+ Sinh viên thử quét lại thư mục malware để phát hiện ra file mã độc:

*sudo clamscan -d detect.yara backdoor.py*

**Kết thúc bài lab:**

- Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

*stoplab ptit-clamAV*

- Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

**Khởi động lại bài lab:**

- Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

*labtainer -r ptit-clamav*