A black and white border

Description automatically generated-

# A red circle with a yellow star in the middle Description automatically generatedMỤC LỤC

**TÌM HIỂU BÀI THỰC HÀNH**

***ptit-maldet***

**Giảng viên:** Đỗ Xuân Chợ

**Họ và tên sinh viên:** Nguyễn Quốc Vượng

**Mã sinh viên:** B21DCAT227

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

**KHOA AN TOÀN THÔNG TIN**

[**MỤC LỤC** 1](#_Toc11250)

[**I.** **Lý thuyết** 2](#_Toc11251)

[**1.** **Tính năng chính của Linux Malware Detect** 2](#_Toc11252)

[**2.** **Cách sử dụng Linux Malware Detect** 2](#_Toc11253)

[**3.** **Ưu điểm và Nhược điểm của Linux Malware Detect** 3](#_Toc11254)

[**-** **Ưu điểm:** 3](#_Toc11255)

[**-** **Nhược điểm:** 3](#_Toc11256)

[**II.** **Thực hành** 4](#_Toc11257)

[**1.** **Nhiệm vụ 1:** 4](#_Toc11258)

[**2.** **Nhiệm vụ 2:** 6](#_Toc11259)

[**3.** **Nhiệm vụ 3:** 6](#_Toc11260)

[**4.** **Nhiệm vụ 4:** 7](#_Toc11261)

[**5.** **Checkwork** 8](#_Toc11262)

[**6.** **Liên kết video bài thực hành** 8](#_Toc11263)

[**III.** **Kết luận** 8](#_Toc11264)

# I. Lý thuyết

Linux Malware Detect (LMD) là một công cụ mã nguồn mở được thiết kế để phát hiện và loại bỏ malware trên hệ thống Linux. Nó sử dụng cơ sở dữ liệu chữ ký để so sánh các tập tin trên hệ thống với các mẫu malware đã biết và mẫu nghi ngờ. Công cụ này thường được sử dụng như một phần của chiến lược bảo mật đa lớp, bổ sung cho các giải pháp antivirus khác và các biện pháp bảo mật khác trên hệ thống Linux.

## 1. Tính năng chính của Linux Malware Detect

* **Phát hiện phần mềm độc hại theo phương pháp heuristic**: LMD sử dụng các quy tắc heuristic để phát hiện các dấu hiệu bất thường và mã độc có khả năng gây hại trên hệ thống.
* **Quét và kiểm tra thời gian thực**: Maldet có khả năng giám sát hệ thống theo thời gian thực (real-time monitoring) bằng cách tích hợp với công cụ inotify của Linux.
* **Khả năng tự động cập nhật**: Cơ sở dữ liệu mã độc được cập nhật tự động từ các nguồn như hệ thống malware signatures cộng đồng của mạng LMD.
* **Quản lý và xử lý mã độc**: Có thể tùy chọn tự động xóa, cách ly hoặc cảnh báo khi phát hiện mã độc, giúp quản lý mã độc hiệu quả hơn.

## 2. Cách sử dụng Linux Malware Detect

**- Cấu hình:** LMD có một file cấu hình chính tại để cấu hình các tùy chọn quét, xử lý và báo cáo: */usr/local/maldetect/conf.maldet*

**Một số lệnh trong maldet**

|  |  |
| --- | --- |
| Câu lệnh | Mô tả |
| -a | Để quét tất cả các tập tin trong đường dẫn |
| -b | Để thực hiện các hoạt động ở chế độ nền. |
| -c | Để tải tệp phần mềm độc hại bị nghi ngờ lên rfxn.com để xem xét và băm thành chữ ký |
| -d | Để cập nhật phiên bản đã cài đặt |
| -e | Để xem lần quét gần đây nhất hoặc ID quét cụ thể và báo cáo quét email tới địa chỉ email được cung cấp |
| -h | Để liệt kê tất cả các tùy chọn trợ giúp có sẵn của maldet. |
| -l | Để xem các sự kiện trong tệp nhật ký maldet |
| -n | Để dọn dẹp và khôi phục các lượt truy cập phần mềm độc hại từ báo cáo |
| -p | Để xóa nhật ký, phiên và dữ liệu tạm thời |
| -q | Để cách ly tất cả phần mềm độc hại khỏi báo cáo |
| -r | Để quét tệp được tạo hoặc sửa đổi trong X ngày qua (7 ngày theo mặc định) |
| -s | Để khôi phục tệp đã cách ly từ hàng đợi cách ly về đường dẫn ban đầu hoặc khôi phục tất cả các tệp đã cách ly từ một ID quét cụ thể |
| -u | Để cập nhật chữ ký phát hiện phần mềm độc hại. |

## 3. Ưu điểm và Nhược điểm của Linux Malware Detect

### - Ưu điểm:

* Miễn phí, mã nguồn mở, dễ sử dụng.
* Được tối ưu hóa cho các môi trường lưu trữ web, đặc biệt hữu ích cho các server chạy nhiều website.
* Khả năng cập nhật liên tục từ cộng đồng giúp công cụ luôn được cải tiến.

### - Nhược điểm:

* Chưa mạnh bằng các phần mềm chống mã độc thương mại.
* Khả năng phát hiện có thể thấp đối với các mã độc mới chưa được cập nhật.
* Có thể gây tải nặng cho hệ thống trong các lần quét toàn bộ.

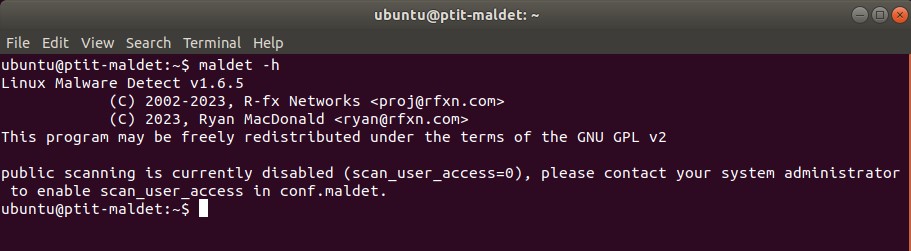
# II. Thực hành

* Khởi động bài lab: *labtianer ptit-maldet*

A screenshot of a computer program

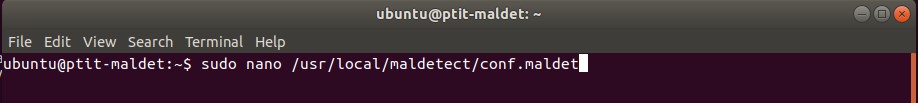
Description automatically generated

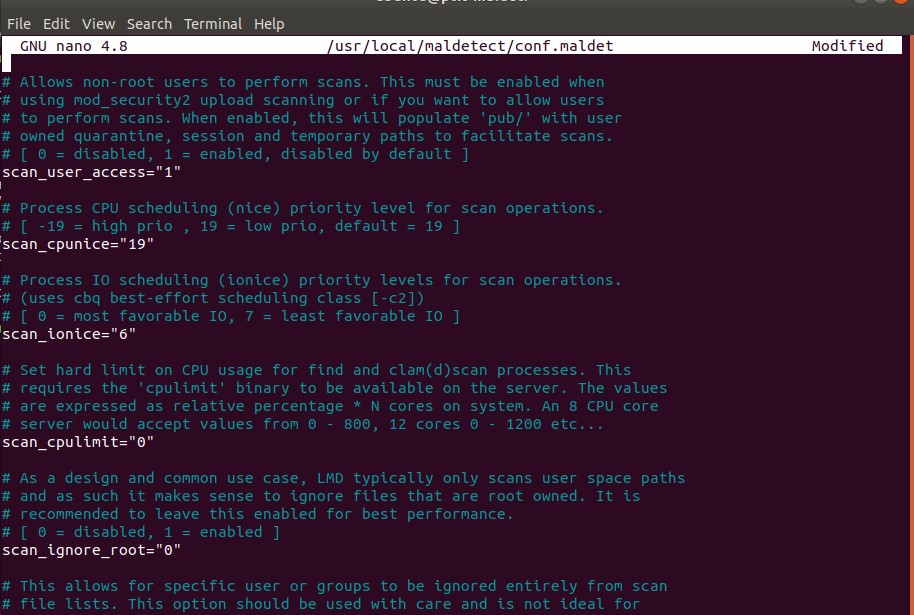
* Xem chức năng của công cụ maldet: *maldet -h*



## 1. Nhiệm vụ 1:

* Thay đổi trường *scan\_user\_access="0"* thành 1 để bật chế độ rà quét công cụ với quyền root, trường *scan\_ignore\_root="1"* thành 0 để cho phép công cụ có quyền rà quét các file do root sở hữu trong file *conf.maldet.*





* Sau khi xác định công cụ hoạt động thành công, thực hiện quét thư mục

*/malware2*: *sudo maldet -a /home/ubuntu/malware2*

A screenshot of a computer

Description automatically generated

## 2. Nhiệm vụ 2:

* Xem báo cáo sau khi thực hiện quét thư mục *malware2* với

*SCAN\_ID=241106-2223.430*

sudo --report 241106-2223.430

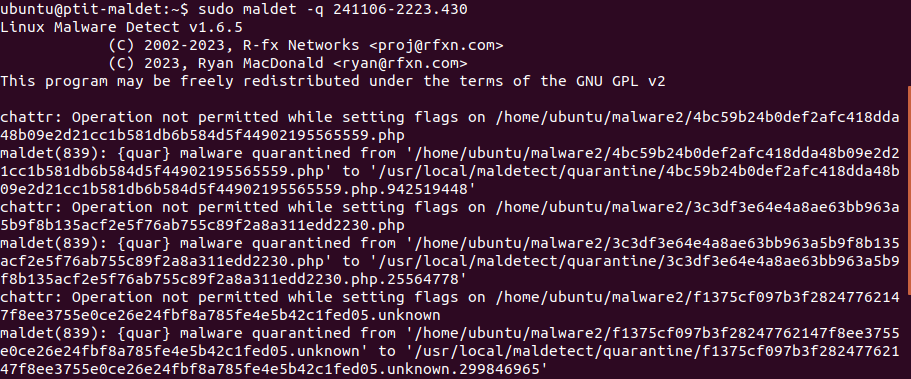
* Sau khi xem báo cáo, quét tổng cộng 8 file trong đó phát hiện 3 file chứa mã độc.

A screenshot of a computer

Description automatically generated

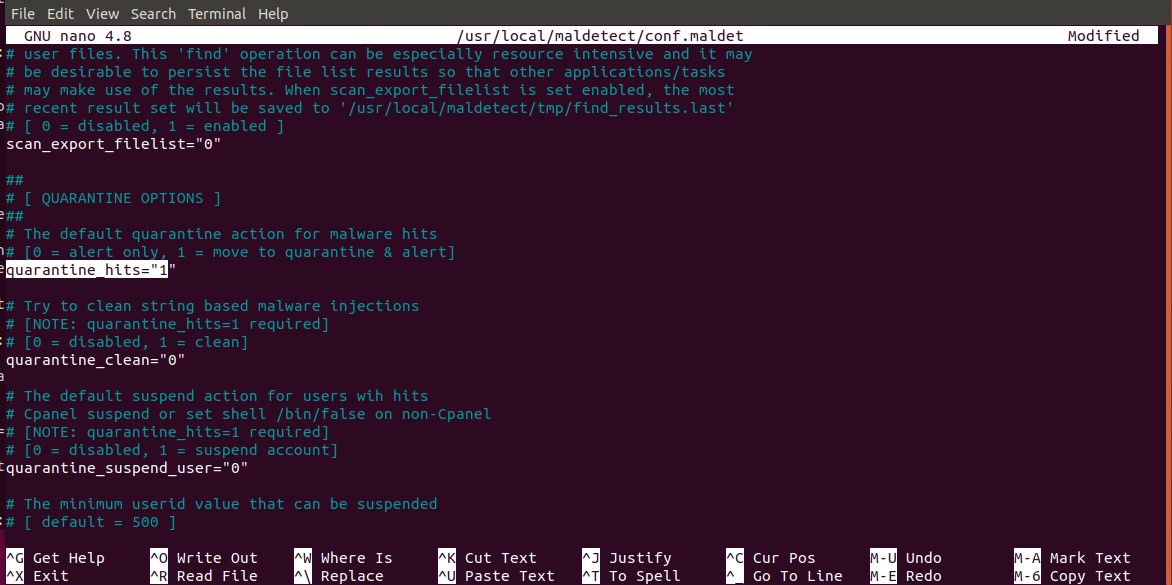
## 3. Nhiệm vụ 3:

- Sử dụng chức năng *quarantine* giúp cách ly và ngăn chặn các tập tin bị nghi ngờ chứa mã độc hại. Chuyển 3 file chứa mã độc trong thư mục */home/ubuntu/malware2* trên sang thư mục có đường dẫn: */usr/local/maldetect/quarantine.*



## 4. Nhiệm vụ 4:

* Thay đổi trường *quarantine\_hits="0"* sẽ được đổi thành 1 trong file *conf.maldet* để sau khi quét thư mục xong các file mã độc tự động chuyển đến thư mục cách ly.



* Thực hiện quét thư mục *malware1.*

A computer screen with white text

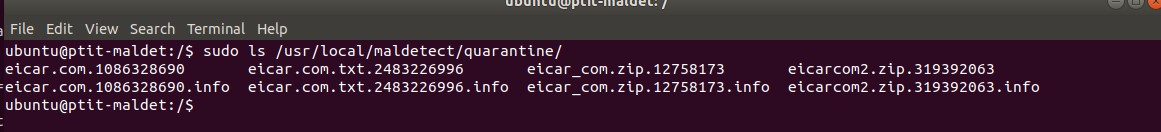
Description automatically generated

* Xem báo cáo sau khi quét xong thư mục *malware1*, ta có thể thấy các file chứa mã độc trong thư mục tự động được chuyển đến thư mục cách ly.

A screenshot of a computer

Description automatically generated

* Kiểm tra thư mục*: ls /usr/local/maldetect/quarantine.*



## 5. Checkwork

A computer screen shot of a code

Description automatically generated

# III. Kết luận

* Tìm hiểu và sử dụng công cụ malware detect trong việc quét các file chứa mã độc.
* Thông qua công cụ maldet, có thể quét, xem báo cáo và chuyển các file chứa mã độc sang một thư mục cách ly một cách tự động hoặc thủ công.