**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

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

------o0o------



**TÌM HIỂU BÀI THỰC HÀNH**

**PTIT - MALDET**

Giảng viên: Đinh Trường Duy

# 1. Nội dung và hướng dẫn thực hiện bài thực hành

## *1.1. Mục đích*

Bài thực hành này giới thiệu công cụ Linux Malware Detect. Bài thực hành giúp sinh viên hiểu về khái niệm và biết cách sử dụng công cụ rà quét mã độc Linux Malware Detect.

## *1.2. Yêu cầu đối với sinh viên*

Có kiến thức cơ bản về hệ điều hành Linux, khả năng phát hiện và phân tích mã độc.

## *1.3. Nội dung thực hành*

* Khởi động bài lab:
* Vào terminal, gõ:

*labtainer ptit-maldet*

(*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*)

Sau khi khởi động xong một terminal ảo sẽ xuất hiện, đại diện cho máy ***ptit-maldet***

* Trên terminal ***ptit-maldet*** sử dụng lệnh *"maldet -h"* xem các chức năng được cung cấp bởi công cụ và nhận được thông báo công cụ cần được cấu hình để có thể hoạt động.
* Sinh viên làm các nhiệm vụ dưới đây để hoàn thành bài lab:
* ***Nhiệm vụ 1: Cấu hình và rà quét mã độc với maldet***
* 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.

Bảng 1.1: 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. |

* Đầu tiên sử dụng lệnh *"* *sudo nano /usr/local/maldetect/conf.maldet"* để truy cập và chỉnh sửa file cấu hình
* Thay đổi trường *scan\_user\_access="0"* thành 1 để bật chế độ rà quét công cụ với quyền root. Thay đổi trường *scan\_ignore\_root="1"* thành 0 để cho phép công cụ có quyền rà quét các file do root sở hữu.
* Chạy lệnh *cat /usr/local/maldetect/conf.maldet*, maldet sẽ hiển thị một loạt cấu hình cho công cụ và lệnh *maldet -h* để xem các chức năng giúp công cụ hoạt động.
* Sau khi xác định được công cụ hoạt động thành công. Sử dụng lệnh *sudo maldet -a /home/ubuntu/malware2* để rà quét thư mục */malware2* được cài sẵn trên máy ảo.
* ***Nhiệm vụ 2: Xem chi tiết báo cáo rà quét của công cụ***
* Lệnh *--report* của công cụ maldet được sử dụng để tạo báo cáo về kết quả quét của chương trình. Khi chạy maldet với tùy chọn *--report*, nó sẽ tạo ra một báo cáo chi tiết về các tập tin mà chương trình đã phát hiện là có khả năng chứa mã độc hại. Báo cáo này thường chứa thông tin về các tập tin, loại malware, đường dẫn, và các hành động khuyến nghị.
* Sau khi chạy lệnh *sudo --report [SCAN\_ID]*, maldet sẽ tạo ra một báo cáo về kết quả của quét và hiển thị thông tin tương ứng trên màn hình. Trong đó, *SCAN\_ID* là một định danh duy nhất được tạo ra mỗi khi sinh viên chạy rà quét. *SCAN\_ID* giúp xác định phiên quét cụ thể và cho phép sinh viên theo dõi kết quả của quét đó. Sinh viên có thể kiểm tra báo cáo này để xem thông tin chi tiết về các tập tin bị nghi ngờ và các hành động khuyến nghị để xử lý chúng.
* ***Nhiệm vụ 3: Trả lời câu hỏi và thực hiện yêu cầu đưa ra***
* Chức năng *"quarantine"* của công cụ maldet là một tính năng quan trọng giúp cách ly và ngăn chặn các tập tin bị nghi ngờ chứa mã độc hại. Khi maldet phát hiện một tập tin có khả năng là malware trong quá trình quét, sinh viên có thể chọn để đưa tập tin đó vào chế độ *quarantine.*
* Khi tập tin được đưa vào quarantine, nó sẽ được di chuyển đến một vị trí được chỉ định trước đó, thường là một thư mục riêng biệt trên hệ thống. Điều này giúp ngăn chặn các tập tin bị nghi ngờ gây ra hậu quả tiêu cực cho hệ thống bằng cách ngăn chặn truy cập và thực thi từ các tập tin đó.
* Sinh viên cần sử dụng lệnh *maldet -h* để đọc các chức năng của công cụ và tìm hiểu về cách sử dụng chức năng *quarantine* để đưa các file mã độc vừa quét được vào thư mục *quarantine* của công cụ.
* ***Nhiệm vụ 4: Tự động hóa việc xử lý mã độc cho công cụ***
* Sinh viên cần tiếp tục cấu hình file *conf.maldet* để sau khi công cụ rà quét xong, các file mã độc sẽ được tự động chuyển đến thư mục cách ly của công cụ. Mặc định trường *quarantine\_hits="0"* sẽ được đổi thành 1 để bật chức năng này.
* Sử dụng công cụ quét lại file */malware1*. Sau khi quét xong, mở file report sẽ thấy thông báo các file mã độc ban đầu đã được tự động chuyển sang thư mục */usr/local/maldetect/quarantine.*
* Sử dụng lệnh để kiểm tra thư mục*: ls /usr/local/maldetect/quarantine.*
* Kết thúc bài lab:
* Trên ***terminal*** đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

*stoplab ptit-maldet*

* 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-maldet*