**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

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

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



**TÌM HIỂU BÀI THỰC HÀNH**

**PTIT – YARA**

Giảng viên: TS. Đinh Trường Duy

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

## 1.1. Mục đích

* Giúp sinh viên hiểu về khái niệm cách sử dụng công cụ yara để phát hiện mã độc.

## 1.2. Yêu cầu đối với sinh viên

* Có kiến thức cơ bản về hệ điều hành Linux, mã độc, phân tích tĩnh.
* Kiến thức về yara: cấu trúc của file luật yara
* Tiêu đề (Header): Bắt đầu bằng từ khóa "rule" và tên đặt cho luật. Ví dụ: "rule MyRule".
* Metadata: Thông tin bổ sung về luật như tác giả, mô tả, ngày tạo, ...
* Strings: Đây là phần quan trọng nhất của một file luật YARA. Nó chứa các mẫu chuỗi (string patterns) mà YARA sẽ tìm kiếm trong các file hoặc quá trình đích. Mỗi mẫu chuỗi bắt đầu bằng từ khóa "strings" và có thể chứa các biểu thức chính quy (regular expressions).
* Condition: Điều kiện xảy ra khi một mẫu chuỗi được phát hiện. Điều kiện được đặt trong dấu ngoặc nhọn và có thể sử dụng các toán tử logic như AND (&&), OR (||), NOT (!) để kết hợp nhiều mẫu chuỗi.
* Ví dụ về 1 luật của yara:

rule MyRule{

meta:

author = "John Doe"

description = "Detects a specific malware variant"

created\_date = "2022-01-01

strings:

$my\_string = "malware\_sample"

condition:

$my\_string

}

## 1.3. Nội dung thực hành

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

*imodule https://github.com/mei3011/ptit-yara*

Labtainer ptit-yara

(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin 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 **yara**.
* Sinh viên làm các nhiệm vụ dưới đây để hoàn thành bài lab:
* **Nhiệm vụ 1: Đọc file “rule.yar” để xem các luật có sẵn**
* Trên terminal **yara** sử dụng lệnh “nano rule.yar” để xem các luật có sẵn.

nano rule.yar

* Yêu cầu sinh viên đọc hiểu các luật trong file rule.yar
* **Nhiệm vụ 2: Phát hiện IP độc hại trong file “example.txt” với yara**
* Sau khi xem qua các luật, mở file example.txt sẽ thấy có 1 địa chỉ ip, sinh viên cần thêm địa chỉ ip này vào luật trong file rule.yar.
* Dùng yara để phát hiện ip trong file example.txt

yara rule.yar example.txt

* **Nhiệm vụ 3: Phát hiện chuỗi “HelLo wOrld” trong file “example.txt” với yara**
* Mở file rule.yar để viết luật phát hiện chuỗi “HelLo wOrld”

rule Nocase{

strings:

$s = “hello world” nocase

condition:

$s

}

* Lưu file và chạy lại yara với file example.txt
* Câu hỏi: nocase này có tác dụng gì, nếu xóa đi sẽ có ảnh hưởng như thế nào đến luật này?
* **Nhiệm vụ 4: Phát hiện được mẫu mã độc cho trước với yara**
* Sau khi hiểu cách hoạt động của yara, tiến hành thử nghiệm phát hiện trên mẫu mã độc malware.exe
* Tìm kiếm các chuỗi đặc trưng của malware.exe

strings malware.exe

* Sau khi tìm được các chuỗi đặc trưng của mẫu mã độc, viết luật để phát hiện malware.exe là mã độc (viết ít nhất 3 đặc trưng của mã độc)
* Kết thúc bài lab:
* Trên terminal đầu tiên sử dụng câu lênh sau để kết thúc bài lab:

stoplab yara

* 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-yara