**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

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

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



**TÌM HIỂU BÀI THỰC HÀNH**

**PTIT - RADARE2**

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 Radare2. Sinh viên sẽ sử dụng Radare2 để phân tích một tập tin thực thi nhằm xác định một số thuộc tính cơ bản.

## 1.2. Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, mã độc…

## 1.3. Nội dung thực hành

* Khởi động bài lab:

Vào terminal, gõ: *labtainer ptit-radare2*

(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 radare2

* Trong bài lab này sẽ có sẵn file mã độc *sample.c,* được sử dụng để lây nhiễm mã độc vào một số các file khác có đuôi file là *“.c, .cpp, .txt”*.
* File mã độc này bắt đầu được thực thi bằng một payload đơn giản, đầu tiên nó sẽ in ra "YOU HAVE BEEN INFECTED …!!!".
* Sinh viên bắt đầu làm bài thực hành bằng cách chạy lệnh *“./run.sh”* để biên dịch và thực thi đoạn code mã độc trên.
* Sau khi biên dịch xong thì sẽ có file sample sinh ra.
* Chức năng chính của virus là chịu trách nhiệm thực thi payload và tự sao chép. Nó bắt đầu bằng cách gọi hàm mã độc và khởi tạo một số biến. Nó mở tệp hiện tại, chính là chương trình vi-rút, bằng cách sử dụng chức năng fopen.
* Sau đó, nó đọc từng dòng tệp hiện tại, tìm kiếm một chuỗi cụ thể "// VIRUS SAYS HI!" đánh dấu sự bắt đầu của mã virus và "// VIRUS SAYS BYE!" đánh dấu sự kết thúc của mã virus. Nó sao chép mã virus vào một mảng, vì vậy nó có thể được sử dụng để lây nhiễm các tệp khác.
* Sinh viên làm các nhiệm vụ dưới đây để hoàn thành bài lab:
* Nhiệm vụ 1: Xem tổng quan chương trình với radare2
* Radare2 là một công cụ phân tích mã nguồn mở và phục hồi hệ thống mạnh mẽ. Nó có thể được sử dụng để phân tích mã nguồn của nhiều loại tệp khác nhau, bao gồm cả mã độc. Radare2 cung cấp các chức năng để xem mã hợp ngữ, tìm kiếm chuỗi hoặc giá trị nhất định, đặt điểm dừng, và nhiều hơn nữa.
* Đầu tiên sinh viên sử dụng câu lệnh “*r2 ./sample*” để khởi chạy chương trình, radare2 sẽ mở tệp “sample” và chờ nhập các lệnh khác để phân tích.
* Sau khi khởi chạy chương trình thì sử dụng “*aaa*” để xem mô-đun và các hàm.
* Chạy lệnh “*afl*”, radare2 sẽ hiển thị một danh sách các hàm, cùng với một số thông tin về mỗi hàm.
* Nhiệm vụ 2: Xem các hàm code trong chương trình
* “s (địa chỉ hàm) hoặc s (tên hàm)” được sử dụng để di chuyển con trỏ đến hàm trong chương trình.

Ví dụ, s main: di chuyển con trỏ đến hàm main cho phép phân tích và kiểm tra cấu trúc của hàm main.

* Lệnh “*pdf*” trong Radare2 được sử dụng để phân tích cú pháp một hàm. Khi gọi lệnh pdf mà không có tham số, nó sẽ phân tích cú pháp hàm hiện tại (nơi con trỏ đang trỏ đến). Nếu muốn phân tích cú pháp một hàm cụ thể, có thể chỉ định nó như một tham số, ví dụ: pdf @ main để phân tích cú pháp hàm main.
* Ở đây sinh viên sẽ cần phải xem thông tin của 2 hàm “*private\_Function*” mô tả chức năng chính của virus lây nhiễm trong chương trình và hàm “*gene*” được sử dụng để sinh các chữ số và kí tự ngẫu nhiên.
* Nhiệm vụ 3: Khởi chạy debug
* Trong Radare2, *“db, dc”* là các lệnh liên quan đến việc gỡ lỗi:
* *db*: Lệnh này được sử dụng để thiết lập các điểm dừng (breakpoints). Có thể sử dụng db kèm theo điểm vào của chương trình để bắt đầu trình gỡ lỗi và tạm dừng thực thi tại hàm đó. Ví dụ, db main sẽ bắt đầu trình gỡ lỗi và tạm dừng thực thi tại hàm main.
* *dc*: Lệnh này được sử dụng để tiếp tục thực thi chương trình sau khi đã tạm dừng tại một điểm dừng. Nó cho phép kiểm soát quá trình thực thi của chương trình và dừng lại tại các điểm quan trọng để kiểm tra trạng thái của chương trình.
* Sau quá trình nhập các lệnh *db, dc* một vài lần thì chương trình sẽ yêu cầu sinh viên phải nhập thông tin, ở đây sinh viên sẽ nhập input là mã sinh viên của mình và tiếp tục sử dụng lệnh *dc* để thực thi chương trình đến khi xuất hiện dòng chữ “YOU HAVE BEEN INFECTED …” 🡪 hoàn thành nhiệm vụ.
* Nhiệm vụ 4: Tìm kiếm các chuỗi
* Lệnh *“iz”* trong Radare2 được sử dụng để liệt kê tất cả các chuỗi trong chương trình.
* Sau khi chạy xong mã độc, sinh viên có thể thực hiện đọc các file trong hệ thống để xem được hành động lây nhiễm của virus vào các file.
* Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab: *stoplab radare2*

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 radare2*