TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

HƯỚNG DẪN CÀI ĐẶT
Phần mềm thu thập chứng cứ sự cố an toàn thông tin trên máy tính sử dụng hệ điều hành Linux

TRẦN QUANG HUY
huy.tq173180@sis.hust.edu.vn

Ngành Mạng và Truyền thông dữ liệu
Chuyên ngành Kỹ thuật máy tính

Giảng viên hướng dẫn: PGS. TS. Nguyễn Linh Giang
Chữ ký của GVHD

Bộ môn: Truyền thông và Mạng máy tính
Viện: Công nghệ thông tin - Truyền thông

HÀ NỘI, 12/2021

ĐỀ TÀI TỐT NGHIỆP

Phần mềm thu thập chứng cứ sự cố an toàn thông tin trên máy tính sử dụng hệ điều hành Linux.

Giáo viên hướng dẫn
Ký và ghi rõ họ tên

HƯỚNG DẪN TẠO TỆP TIN THỰC THI PHẦN MỀM

Trong bản hướng dẫn này, chúng ta sẽ đi vào quá trình tạo tệp tin thực thi phần mềm dựa trên mã nguồn Python đã xây dựng.

Môi trường cài đặt sử dụng trong bản hướng dẫn là hệ điều hành Ubuntu 20.04 LTS. Phiên bản hệ điều hành này đã được cài đặt sẵn Python 3.8.10. Đây cũng là phiên bản Python được sử dụng để phát triển phần mềm.

Bước 1: Mở cửa sổ dòng lệnh. Cài đặt trình quản lý thư viện PIP của Python bằng các câu lệnh sau:

$ sudo apt update

$ sudo apt install python3-pip

Bước 2: Cài đặt PyInstaller bằng câu lệnh:

$ pip install pyinstaller

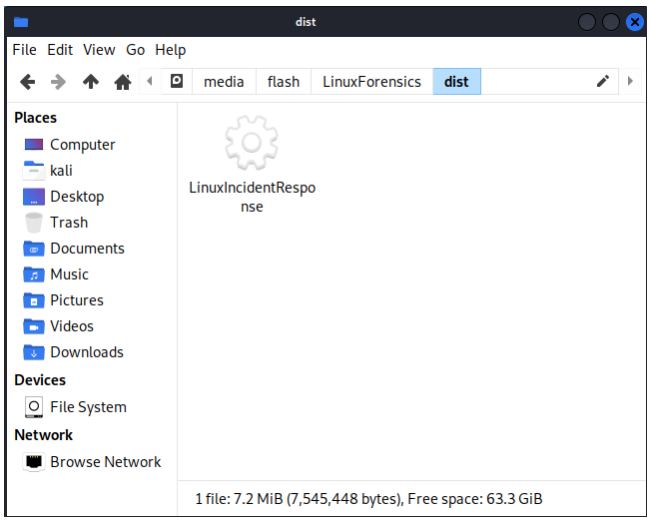
Bước 3: Truy cập thư mục chính của phần mềm, nơi chứa tệp tin execute.py. Mở cửa sổ dòng lệnh tại đây và chạy câu lệnh sau:

$ pyinstaller -D -F -n LinuxIncidentResponse -c "execute.py"

```
kooriboh@WingedKubiboh:~/Documents/LinuxForensics$ pyinstaller -D -F -n LinuxIncidentResponse -c "execute.py"
44 INFO: PyInstaller: 4.8
44 INFO: Python: 3.8.10
55 INFO: Platform: Linux-5.13.0-28-generic-x86_64-with-glibc2.29
55 INFO: wrote /home/kooriboh/Documents/LinuxForensics/LinuxIncidentResponse.spec
57 INFO: UPX is not available.
59 INFO: Extending PYTHONPATH with paths
['/home/kooriboh/Documents/LinuxForensics']
185 INFO: checking Analysis
185 INFO: Building Analysis because Analysis-00.toc is non existent
186 INFO: Initializing module dependency graph...
187 INFO: Caching module graph hooks...
192 INFO: Analyzing base_library.zip ...
```

Hình 0-1 Thực thi câu lệnh pyinstaller

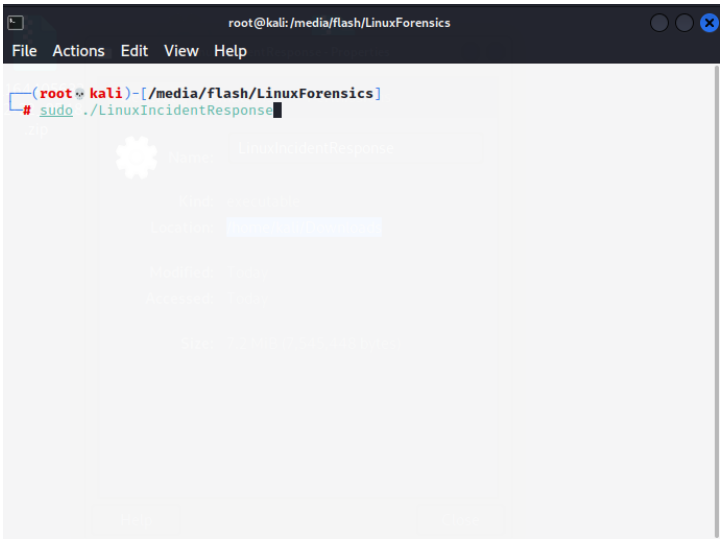
Sau khi câu lệnh được thực thi, một thư mục mới có tên "dist" sẽ xuất hiện tại thư mục chính của phần mềm. Truy cập thư mục này, ta thấy tệp tin LinuxIncidentResponse xuất hiện.



Hình 0-2 Tệp tin thực thi LinuxIncidentResponse

Tệp tin thực thi có thể được chạy trên các máy tính sử dụng hệ điều hành Linux, yêu cầu cần có GLIBC phiên bản từ 2.29 trở lên (do yêu cầu của thư viện từ Python 3.8 và PyInstaller).

Để chạy tệp tin thực thi, người dùng cần mở cửa sổ dòng lệnh tại thư mục chứa tệp tin và sử dụng câu lệnh: *sudo ./LinuxIncidentResponse*.



Hình 0-3 Khởi động phần mềm