```
  | |
  | |
 _| |_
 _|   |_
/  ee\_                |_ _| |_ __| _|_ _| |_| _|  _| _| |_
 .<    __0           | | | | | | -_| _| .'| _| -| .'|
/\ \.-.' \           |_| |_|_|__|_|_| |__|_| |_|_|__|_|
J \.|'.\/ \
| |_.|. | | |   [--]   Backdoor Creator for Remote Acces [--
\_.' .|-' /    [--]   Created by: Edo Maland (Screetsec) [--
 L   /|o'--'\    [--]         Version: 1.9.6            [--
 |  /\/\/\    \   [--]        Codename: Whistle         [--
 J /                                        Screetsec   [--
 J /                                        Linux.org   [--
 |/            /                                        [--
  \      .'.\.                        TO BEGIN:         [--
___)_/\_(___\. [--] ._____[--
(__._./  \_.__)'\_.-----------------------------------------
```

Instalación y configuración de theFatRat y Shellter

SANTIAGO PEÑARANDA MEJIA

```
[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

LO QUE VAMOS HACER EN ESTA ACTIVIDAD ES LA INSTALACIÓN Y CONFIGURACIÓN DE **THEFATRAT** Y **SHELLTER**. A CONTINUACIÓN VAMOS A PROCEDER CON LA INSTALACIÓN DE THEFATRAT.

LO PRIMERO ES BUSCAR EN EL NAVEGADOR EL REPOSITORIO DE GITHUB DE LA HERRAMIENTA, PARA ELLO VAMOS A ESCRIBIR EN NUESTRO NAVEGADOR PREFERIDO LO SIGUIENTE "THEFATRAT GITHUB" Y LE DAMOS A ENTER
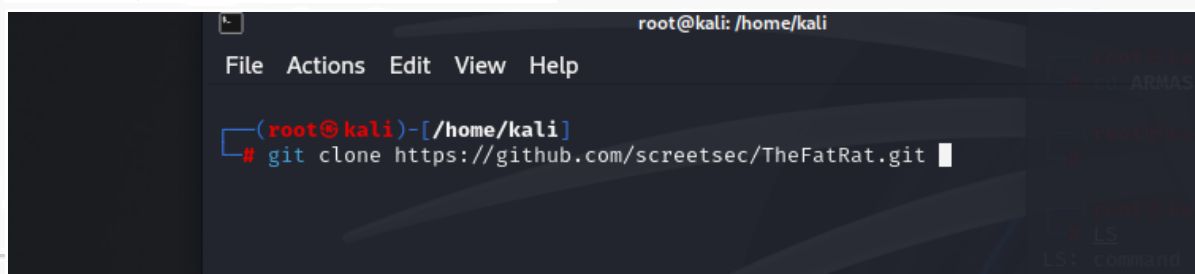
Y NOS DIRIGIMOS A EL PRIMER ENLACE QUE NOS APARECE
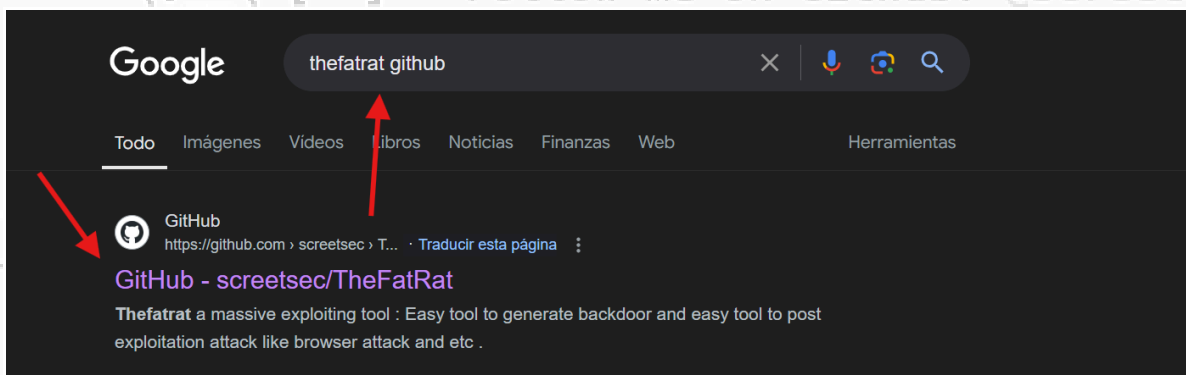

```
[01]    Create Backdoor with msfvenom
[02]    Create Fud 100% Backdoor with Fudwin 1.0
[03]    Create Fud Backdoor with Avoid v1.2
[04]    Create Fud Backdoor with backdoor-factory [embed]
[05]    Backdooring Original apk [Instagram, Line,etc]
[06]    Create Fud Backdoor 1000% with PwnWinds [Excelent]
[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
```
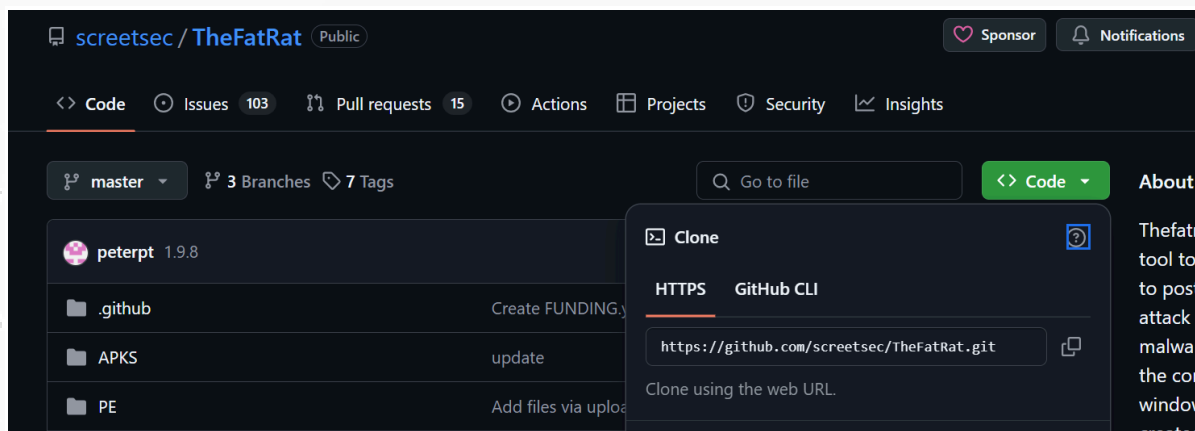
AHORA ENTRAMOS A KALI LINUX Y ESCRIBIMOS EL SIGUIENTE COMANDO QUE VES EN PANTALLA, Y COPIAMOS EL REPOSITORIO


```
[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
```

Una vez ya copiado lo que vamos hacer es entrar a la herramienta con el comando "cd"

Ahora lo que vamos hacer es ejecutar el setup.sh para que se nos descargue completamente la herramienta `BASH SETUP.SH` Una vez ya descargada la herramienta para ejecutarla solo basta con escribir `FATRAT` y de ahí en adelante ir creando el malware.

```
[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
```

```
                                         [--]   Backdoor Creator for Remote Acces [--]
                                         [--]   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]:
```

SHELLTER

```
[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
```

BIEN, AHORA PROSEGUIREMOS CON LA DESCARGA DE SHELLTER, PERO ANTES DE INICIAR LA DESCARGA ME GUSTARÍA EXPLICARTE PRIMERAMENTE QUE TODO ES SHELLTER.

SHELLTER ES UNA HERRAMIENTA QUE SIRVE PARA INYECTAR CÓDIGO EN ARCHIVOS EJECUTABLES, ESTA HERRAMIENTA LA PODEMOS ENCONTRAR EN LOS REPOSITORIOS DE NUESTRO KALI.

Y PARA INSTALARLA SOLO BASTA CON ESCRIBIR

```
root@kali: /home/kali/ARMAS/TheFatRat

File   Actions   Edit   View   Help

┌──(root㉿kali)-[/home/kali/ARMAS/TheFatRat]
└─# apt search shellter
```

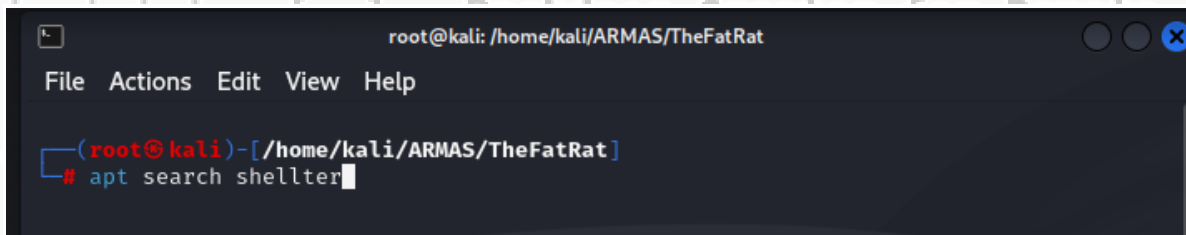UNA VEZ YA DESCARGADA LA EJECUTAMOS CON EL COMANDO **SHELLTER** QUE BÁSICAMENTE ES LLAMARLA

```
[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
```

```
                      ____ _  _ ____ _    _    ___ ____ ____
                      |\   __\|\  \|\  \|\   _ \  _   \    |\   \|\__  __\   _ \|\  _ \ _ \
                       \ \  \_|\ \  \ \\\ \ \  \_/\ \ \ \    \ \  \\|_ \  \_\ \ \\ \ \/|\ \ \
                        \ \___    \ _   \ \  \ \/_\|_\ \ \    \ \ \   \ \ \ \/_\|/ \ \  \ _\
                         \|__|\    \ \\\ \ \__\|_\\\ \__\_\ \ \__\   \ \ \ \_\\\ \__\ \ \
                          __\\ \ \_\ \_\ \_\____\  \____\ \ \_\ \ \_\_\ \_\  \__\_\__ \
                          |\_____\|_|\|_|\|____|\|____|\|____|\|_|  \|____|\|_|\|_| v7.2
                          \|_____|  www.ShellterProject.com


        Index
        =======

        [1]  What is it?
        [2]  How does it work?
        [3]  What does it trace?
        [4]  Why do I need Shellter?
        [5]  What types of applications can I use?
        [6]  Can I use encoded/self-decrypting payloads?
        [7]  Does Shellter provide any type of encoding?
        [8]  What does 'Dynamic Thread Context Keys' aka DTCK mean?
        [9]  Does Shellter provide any ready to use payloads?
        [10] What is the Stealth Mode?
        [11] What is Thread Context Aware polymorphic code?
        [12] What is Reflective DLL loading?
        [13] What about self-modifying code?
        [14] What about relocations?
        [15] What about Multi-Thread Applications?
        [16] What about Anti-Reversing tricks?
        [17] What if the target process dies during tracing?
        [18] What if an internal engine related error occurs?
        [19] How do execution flow filters work?
        [20] How much time does it need for tracing and log filtering?
        [21] What options does Shellter provide?
        [22] What is the purpose of verification stage?
        [23] System Requirements
        [24] What should I do if I want to send feedback?
        [25] What should I do if I want to report a bug?
        [26] What should I do if I don't like it?
```

Y LISTO ESTA SERÍA LA RESPECTIVA INSTALACIÓN DE THEFATRAT Y SHELLTER.

```
[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
```

```
    |       |
    |_____|
   _|_____|_
  /    ee\_                 |_ _| | |_  ___|   _|__| |_|  _  |___|‾| |_
.< ___    _O                | | | | | |  | -_|   _|  .'| _|    -| .'| _|
/\  \.-.' \                 |_| |_|_|___|__|   |___|_| |_|_|_|__|
J  \.|'.\/ \
| |_.|. | | |      [--]    Backdoor Creator for Remote Acces [--
\__.' .|-' /       [--]    Created by: Edo Maland (Screetsec) [--
L    /|o'--'\      [--]           Version: 1.9.6               [--
|   /\/\/\   \     [--]          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
```