



Curso de Hacking ético Master. D

Ejercicio 10
Evasión de Detección con
TheFatRat y Shellter

Alumno: Julián Gordon

Índice

Introducción	3
Instalación de TheFatRat	4
Ejecución de TheFatRat	8
Instalación de Shellter	11
Ejecución de Shellter	13
Conclusiones	14

Introducción

En este ejercicio, mostraremos la instalación de dos herramientas muy importantes que son TheFatRat y Shellter. El nombre **“TheFatRat”** proviene del término "RAT" que significa "Remote Administration Tool" (Herramienta de Administración Remota). Es un conjunto de herramientas que se utiliza para generar backdoors en sistemas informáticos. con el objetivo de probar la seguridad y la resistencia de las redes. Ofrece una variedad de payloads para diferentes sistemas operativos, incluyendo Windows, Linux y Android. Incluye características diseñadas para evadir la detección de antivirus y otras medidas de seguridad, como la capacidad de cifrar payloads y utilizar técnicas de ofuscación.

Shellter, a su vez, es una herramienta de pentesting diseñada para la inyección de shellcode en ejecutables existentes, específicamente en archivos binarios de formato Portable Executable (PE). Su objetivo principal es proporcionar una forma de ofuscar y ocultar payloads maliciosos en ejecutables legítimos, lo que nos puede ser muy útil en nuestras pruebas de pentesting y en el desarrollo de exploits.

Instalación de TheFatRat

Para instalar TheFatRat, primero debemos clonar el repositorio de github:

<https://github.com/screetsec/TheFatRat>

Luego debemos darle permisos de ejecución al archivo setup.sh y ejecutarlo. En las siguientes imágenes podemos observar este proceso.

```
(root@kali)-[/home/kali]
# cd /opt/

(root@kali)-[/opt]
# git clone https://github.com/screetsec/TheFatRat
```

```
root@kali: /opt/TheFatRat

File Actions Edit View Help

(root@kali)-[/home/kali]
# cd /opt/

(root@kali)-[/opt]
# ls
microsoft nessus TheFatRat

(root@kali)-[/opt]
# cd TheFatRat

(root@kali)-[/opt/TheFatRat]
# ls
APKS      backdoor_apk  chk_tools  fatrat  icons  java  lists  PE  powerfull.sh  README.md  setup.sh  tools  update
autorun   CHANGELOG.md  config     grab.sh  ISSUES.md  LICENSE  logs  postexploit  prog.c.backup  release  temp  troubleshoot.md

(root@kali)-[/opt/TheFatRat]
# chmod +x setup.sh

(root@kali)-[/opt/TheFatRat]
# ./setup.sh
```

File Actions Edit View Help

root@kali: /opt/TheFatRat

Setup Script for FATRAT 1.9.7

64Bit OS detected

Checking type of shell

[local]

[*] Checking for internet connection

[✓] ::[Internet Connection]: CONNECTED!

[✓] Xterm.....[found]

[?] Checking Mingw Version.....Error

TheFatRat detected an incorrent version of mingw installed

Do you wish to remove it and install the appropriate one ?

Choose (yes/no) : yes

Removing mingw as requested... Error

Setup was unable to remove mingw Installation

[✓] Dns-Utills[found]

[✓] Mono-Denvelop Utills[found]

[✓] Gcc compiler.....[found]

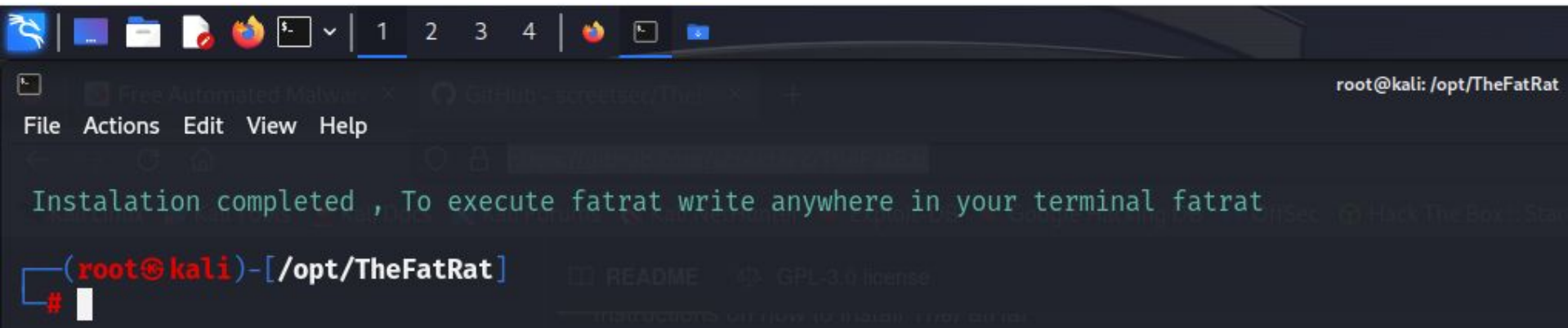
[✓] Apache2[found]

[✓] Gnome Terminal.....[found]

[✓] UPX Compressor.....[found]

[✓] Ruby.....[found]

[✓] Python2.....[found]



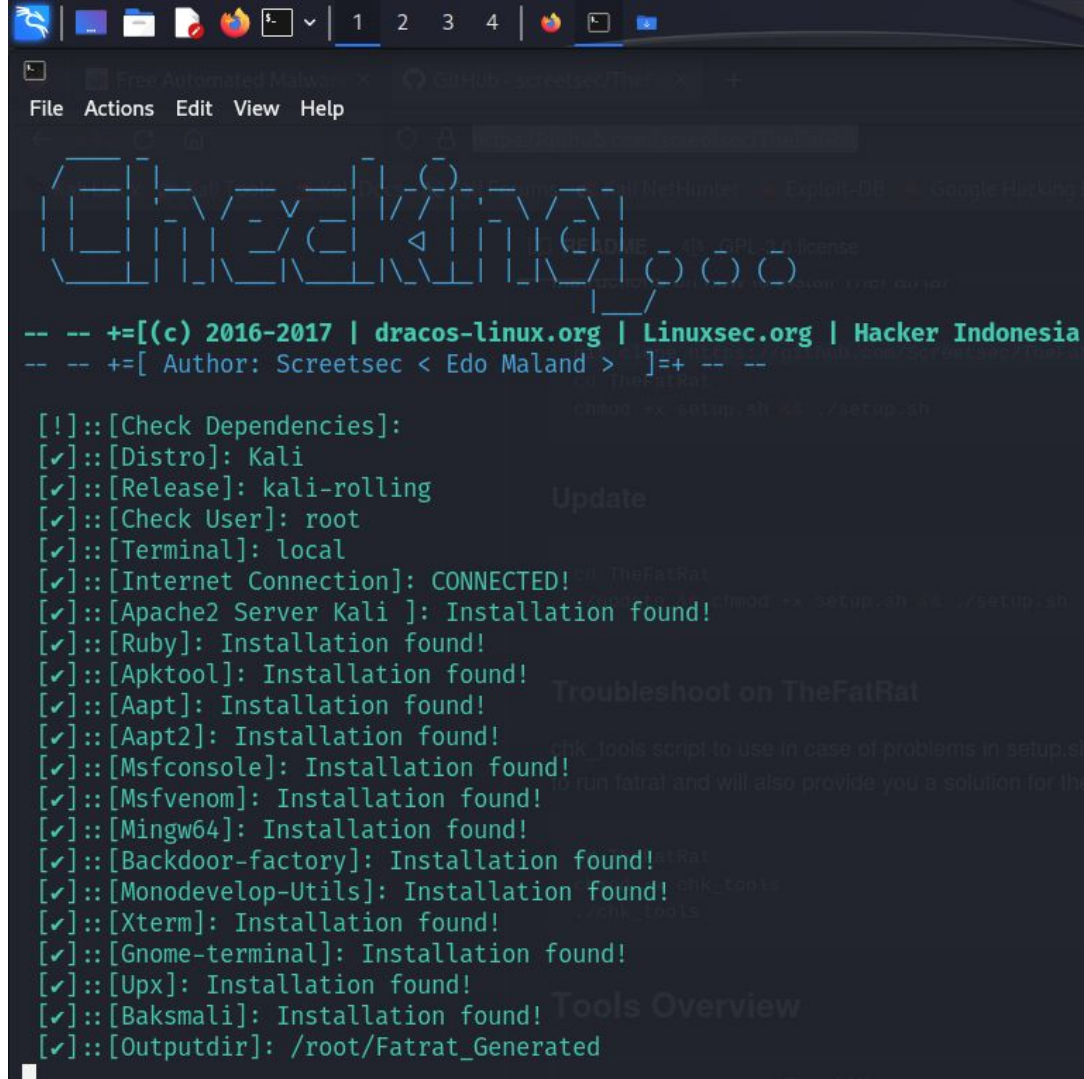
```
root@kali: /opt/TheFatRat

File Actions Edit View Help

Instalation completed , To execute fatrat write anywhere in your terminal fatrat

(root@kali)-[/opt/TheFatRat]
#
```

En la imagen anterior, podemos observar que la instalación se realizó exitosamente.

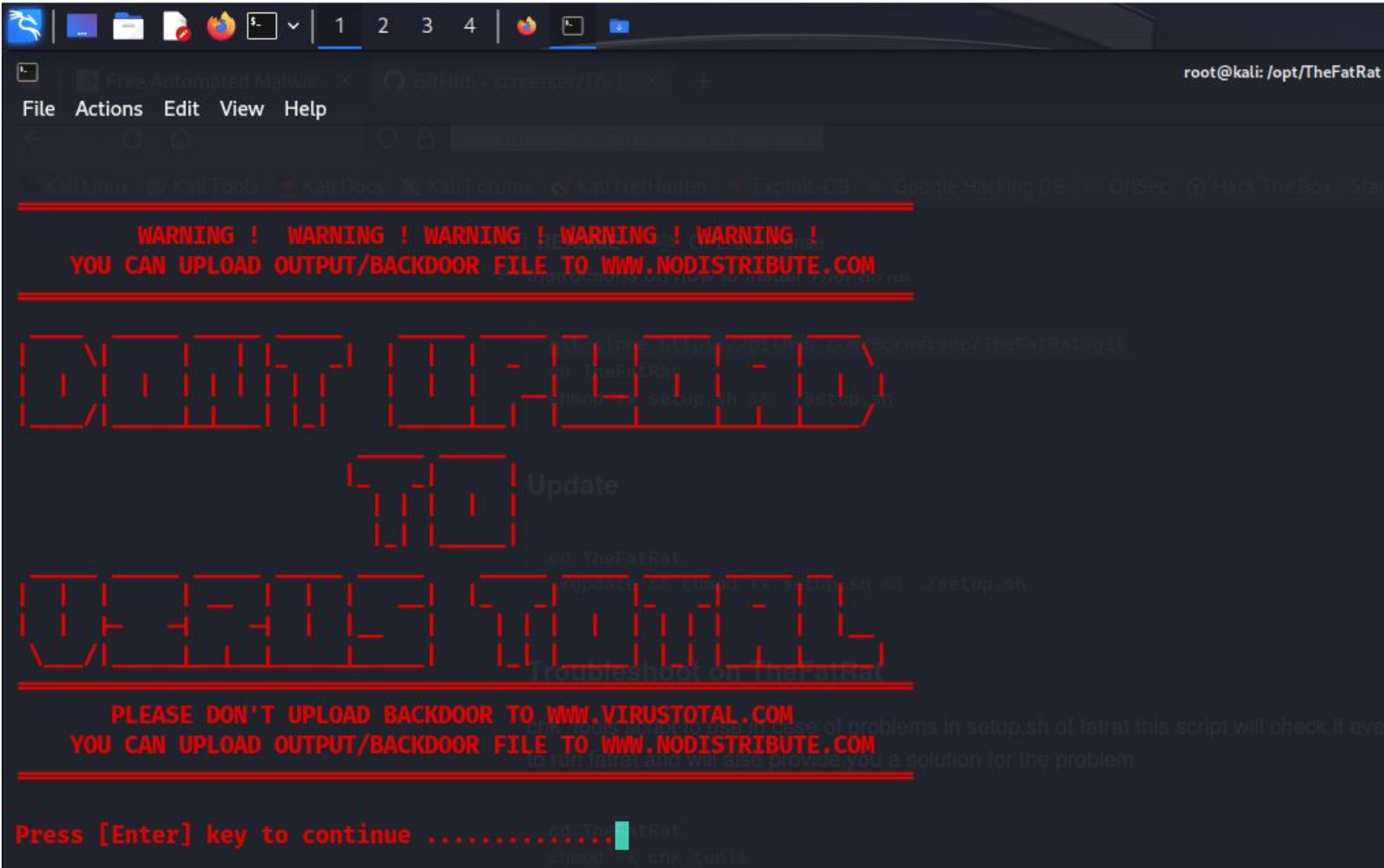


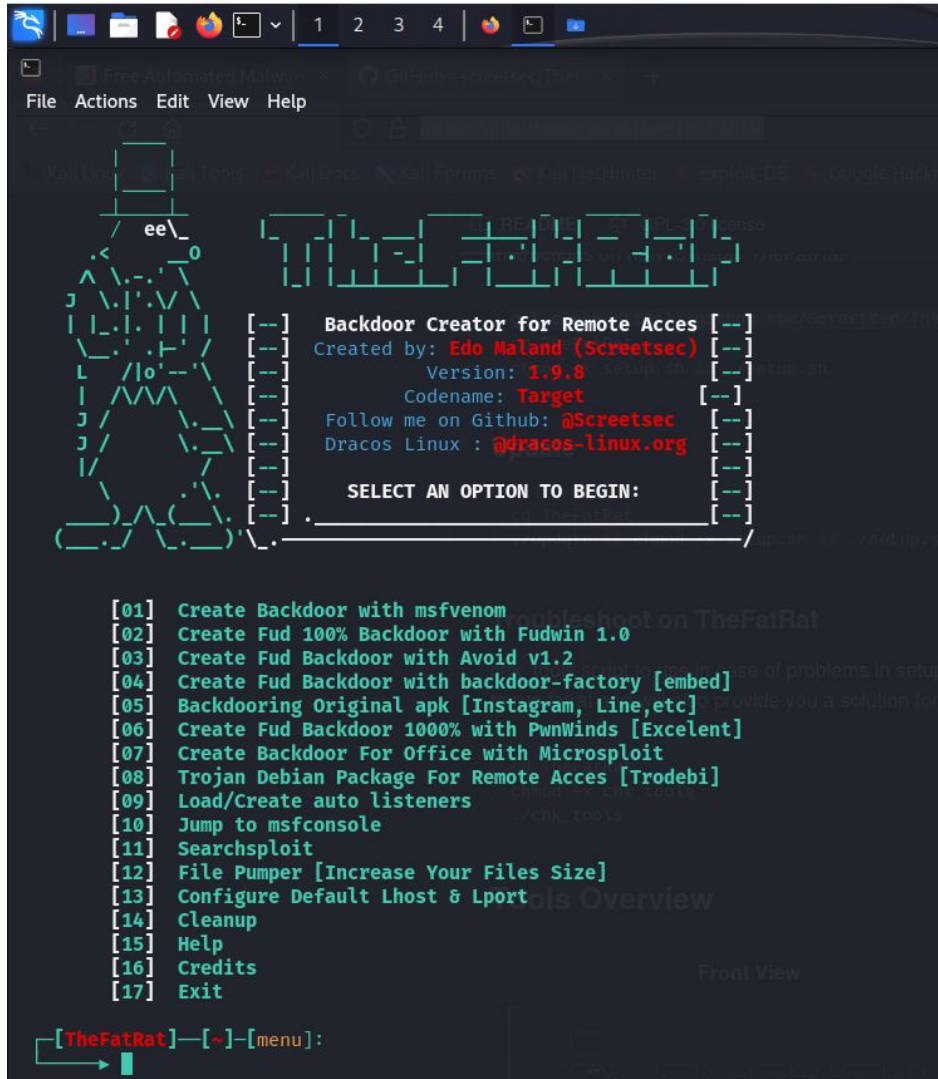
```
-- -- +=[(c) 2016-2017 | dracos-linux.org | Linuxsec.org | Hacker Indonesia
-- -- +=[ Author: Sreetsec < Edo Maland > ]+= -- --

[!]:[Check Dependencies]:
[✓]:[Distro]: Kali
[✓]:[Release]: kali-rolling
[✓]:[Check User]: root
[✓]:[Terminal]: local
[✓]:[Internet Connection]: CONNECTED!
[✓]:[Apache2 Server Kali ]: Installation found!
[✓]:[Ruby]: Installation found!
[✓]:[Apktool]: Installation found!
[✓]:[Aapt]: Installation found!
[✓]:[Aapt2]: Installation found!
[✓]:[Msfconsole]: Installation found!
[✓]:[Msfvenom]: Installation found!
[✓]:[Mingw64]: Installation found!
[✓]:[Backdoor-factory]: Installation found!
[✓]:[Monodevelop-Utils]: Installation found!
[✓]:[Xterm]: Installation found!
[✓]:[Gnome-terminal]: Installation found!
[✓]:[Upx]: Installation found!
[✓]:[Baksmali]: Installation found!
[✓]:[Outputdir]: /root/Fatrat_Generated
```

Ahora ejecutamos la herramienta con el comando :

“fatrat”



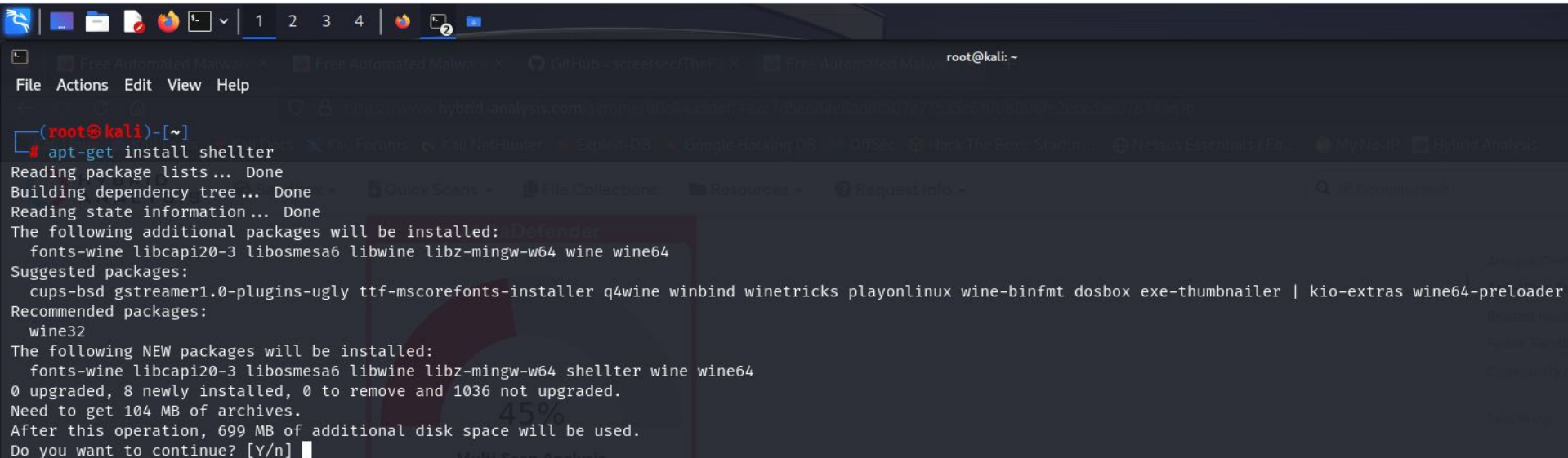


```
File Actions Edit View Help
Backdoor Creator for Remote Acces
Created by: Edo Maland (Screeetsec)
Version: 1.9.8
Codename: Target
Follow me on Github: @Screeetsec
Dracos Linux : @dracos-linux.org
SELECT AN OPTION TO BEGIN:
[01] Create Backdoor with msfvenom
[02] Create Fud 100% Backdoor with Fudwin 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]:
```

Ahora en esta imagen, podemos observar, con la herramienta ejecutándose, cómo es su interfaz.

Instalación de Shellter

Para instalar Shellter, lo haremos con la herramienta apt-get install. Podemos observar este proceso en la siguiente imagen.



```
(root@kali)-[~]
# apt-get install shellter
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed: Defender
 fonts-wine libcap120-3 libosmesa6 libwine libz-mingw-w64 wine wine64
Suggested packages:
 cups-bsd gstreamer1.0-plugins-ugly ttf-mscorefonts-installer q4wine winbind winetricks playonlinux wine-binfmt dosbox exe-thumbnailer | kio-extras wine64-preloader
Recommended packages:
 wine32
The following NEW packages will be installed:
 fonts-wine libcap120-3 libosmesa6 libwine libz-mingw-w64 shellter wine wine64
0 upgraded, 8 newly installed, 0 to remove and 1036 not upgraded.
Need to get 104 MB of archives.
After this operation, 699 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

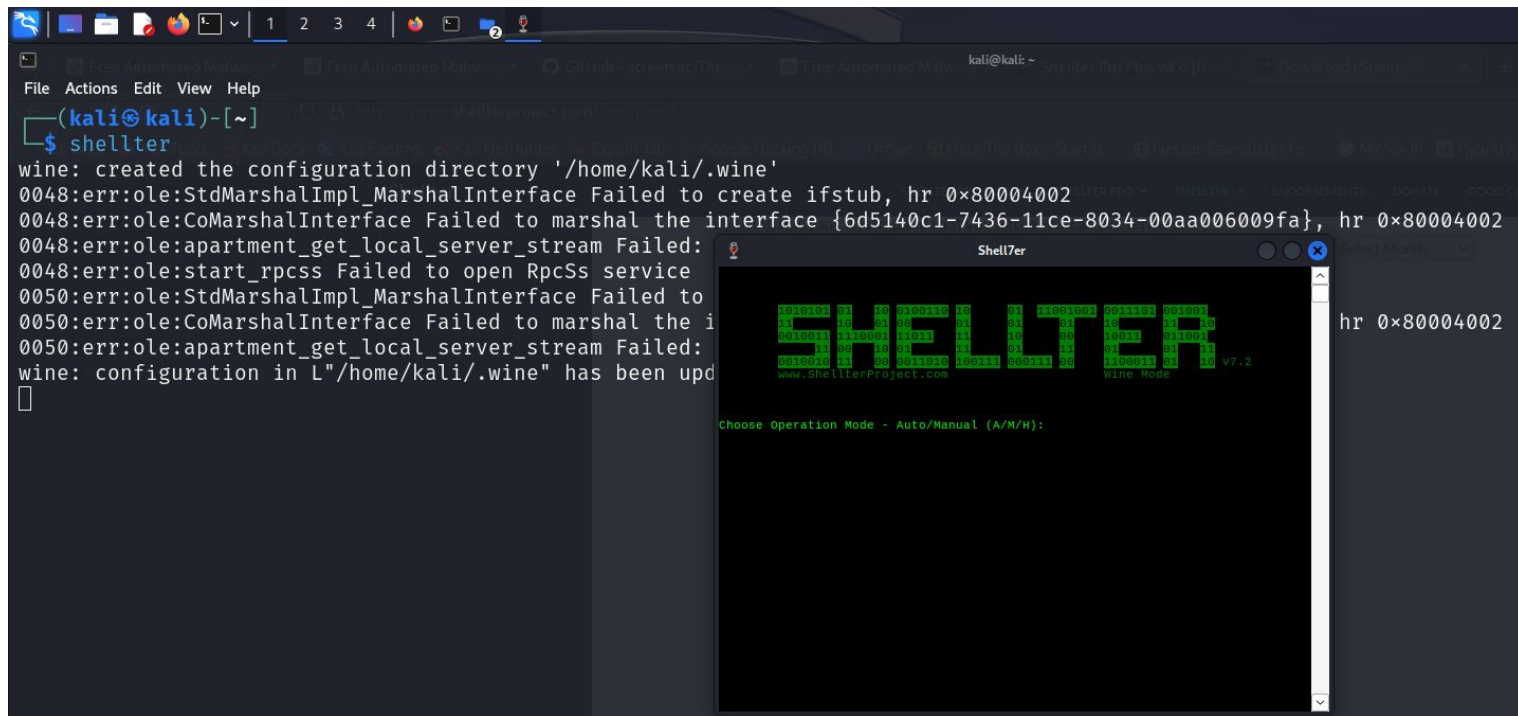
Al intentar ejecutar 'shellter' , nos aparece el siguiente error, por lo que debemos instalar algunos componentes para que funcione correctamente. Usamos el comando: 'dpkg --add-architecture i386 && apt-get update && apt-get install wine32:i386'

```
(root@kali)-[~]
# shellter
(Message from Kali developers)

You may need to install the wine32 package first:
# dpkg --add-architecture i386 && apt update && apt -y install wine32

it looks like wine32 is missing, you should install it.
multiarch needs to be enabled first. as root, please
execute "dpkg --add-architecture i386 && apt-get update &&
apt-get install wine32:i386"
wine: created the configuration directory '/root/.wine'
0048:err:ole:StdMarshalImpl_MarshalInterface Failed to create ifstub, hr 0x80004002
0048:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, hr 0x80004002
0048:err:ole:apartment_get_local_server_stream Failed: 0x80004002
0048:err:ole:start_rpcss Failed to open RpcSs service
0050:err:ole:StdMarshalImpl_MarshalInterface Failed to create ifstub, hr 0x80004002
0050:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, hr 0x80004002
0050:err:ole:apartment_get_local_server_stream Failed: 0x80004002
wine: failed to open L"C:\\windows\\syswow64\\rundll32.exe": c0000135
wine: configuration in L"/root/.wine" has been updated.
013c:err:environ:init_peb starting L"Z:\\usr\\share\\windows-resources\\shellter\\shellter.exe" in experimental wow64 mode
013c:err:module:load_wow64_ntdll failed to load L"\\??\\C:\\windows\\syswow64\\ntdll.dll" error c0000135
013c:err:virtual:virtual_setup_exception stack overflow 1456 bytes addr 0x170057031 stack 0x4b0a50 (0x4b0000-0x4b1000-0x5afd20)
```

Luego de instalar los componentes que nos faltaban, ejecutamos shellter desde la terminal y nos abrirá una nueva ventana con el programa funcionando. Podemos ver este paso en la siguiente imagen.



```
(kali@kali)-[~]  
$ shellter  
wine: created the configuration directory '/home/kali/.wine'  
0048:err:ole:StdMarshalImpl_MarshalInterface Failed to create ifstub, hr 0x80004002  
0048:err:ole:CoMarshalInterface Failed to marshal the interface {6d5140c1-7436-11ce-8034-00aa006009fa}, hr 0x80004002  
0048:err:ole:apartment_get_local_server_stream Failed:  
0048:err:ole:start_rpcss Failed to open RpcSs service  
0050:err:ole:StdMarshalImpl_MarshalInterface Failed to  
0050:err:ole:CoMarshalInterface Failed to marshal the i  
0050:err:ole:apartment_get_local_server_stream Failed:  
wine: configuration in L"/home/kali/.wine" has been upda  
[  
  
Shell7er  
1616163 31 10 0100110 11 31 11081001 001101 001001  
11 10 01 00 01 01 11 10 00 1001 011001  
0010011 0110001 11011 11 10 00 1001 011001  
11 10 01 10 01 11 01 11 01 01 11  
0010010 01 00 0011010 10011 000111 00 110011 01 10  
www.ShellterProject.com Wine Mode v7.2  
  
Choose Operation Mode - Auto/Manual {A/M/H):
```

Conclusiones

Con la realización de este ejercicio, aprendimos a instalar y ejecutar 2 herramientas que son muy útiles para la evasión de detección en una auditoría, TheFatRat y Shellter.

Una vez que creamos nuestro malware con TheFatRat, podemos verificar si los motores de Antivirus lo pueden detectar, o no, subiendo el fichero creado al sitio web de Hybrid Analysis (<https://www.hybrid-analysis.com/>), y luego ir modificando nuestro fichero, para que sea indetectable ante la mayoría de antivirus. Este sitio web nos da información muy importante y detallada de lo que hace este ejecutable.

Comprendemos que Shellter, es una herramienta que nos puede servir para introducir un troyano en un archivo ejecutable existente, y cuenta con potentes medidas para evadir la detección de antivirus. Resulta ser una herramienta muy útil para infectar archivos que ya están en uso.