Módulo IV: Ingeniería Inversa & Exploiting

Universidad Rey Juan Carlos

Introducción a PWN

Universidad
Rey Juan Carlos

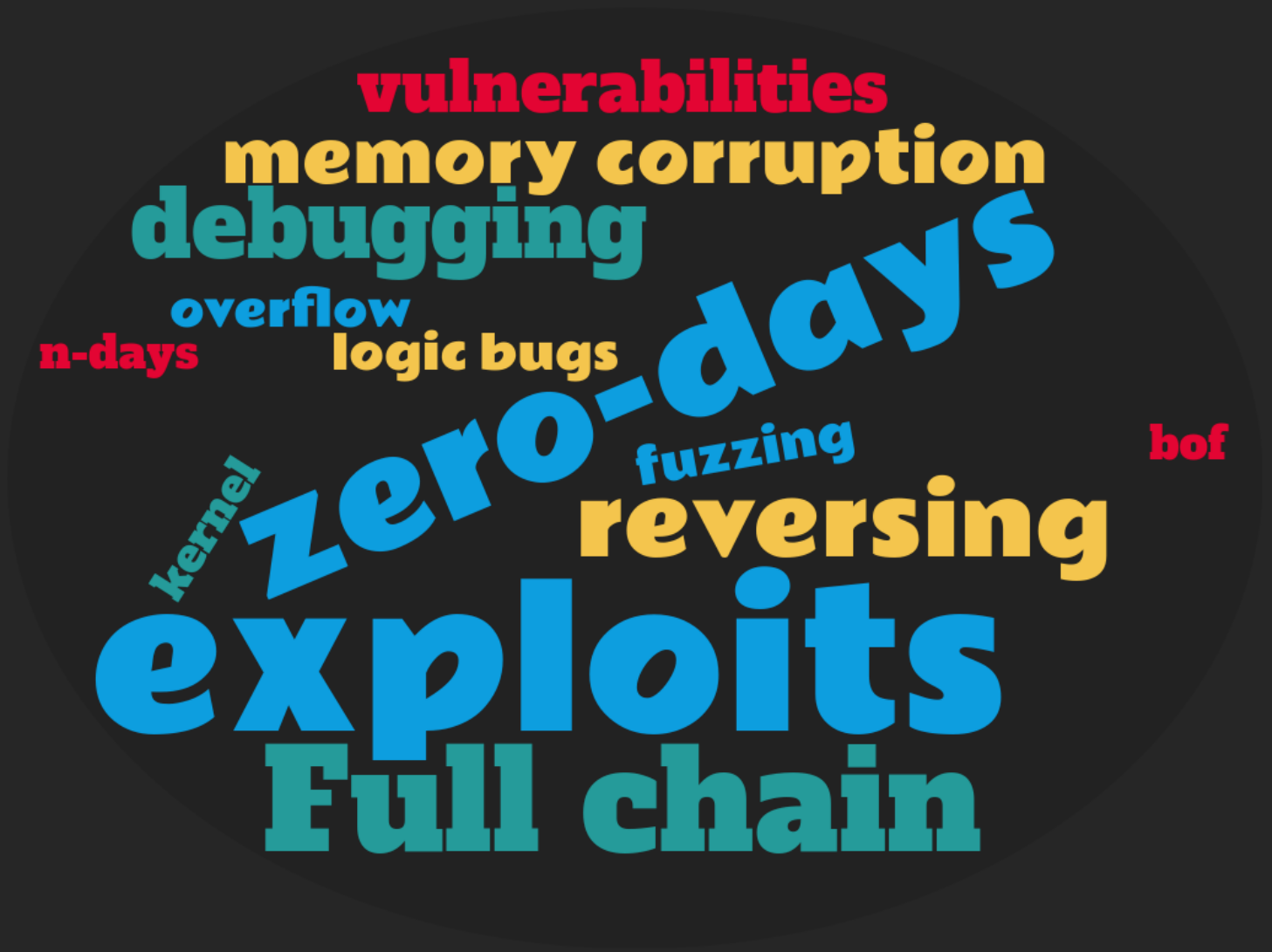
¿Qué es PWN?

- Encontrar vulnerabilidades en programas

- Explotarlas (aprovecharte de ellas)

- Manipular el programa a tu voluntad (tomar el control)

- Conseguir lo que buscas (¡¡LA FLAG!!)



¿Qué es PWN?

SECRET CLUB

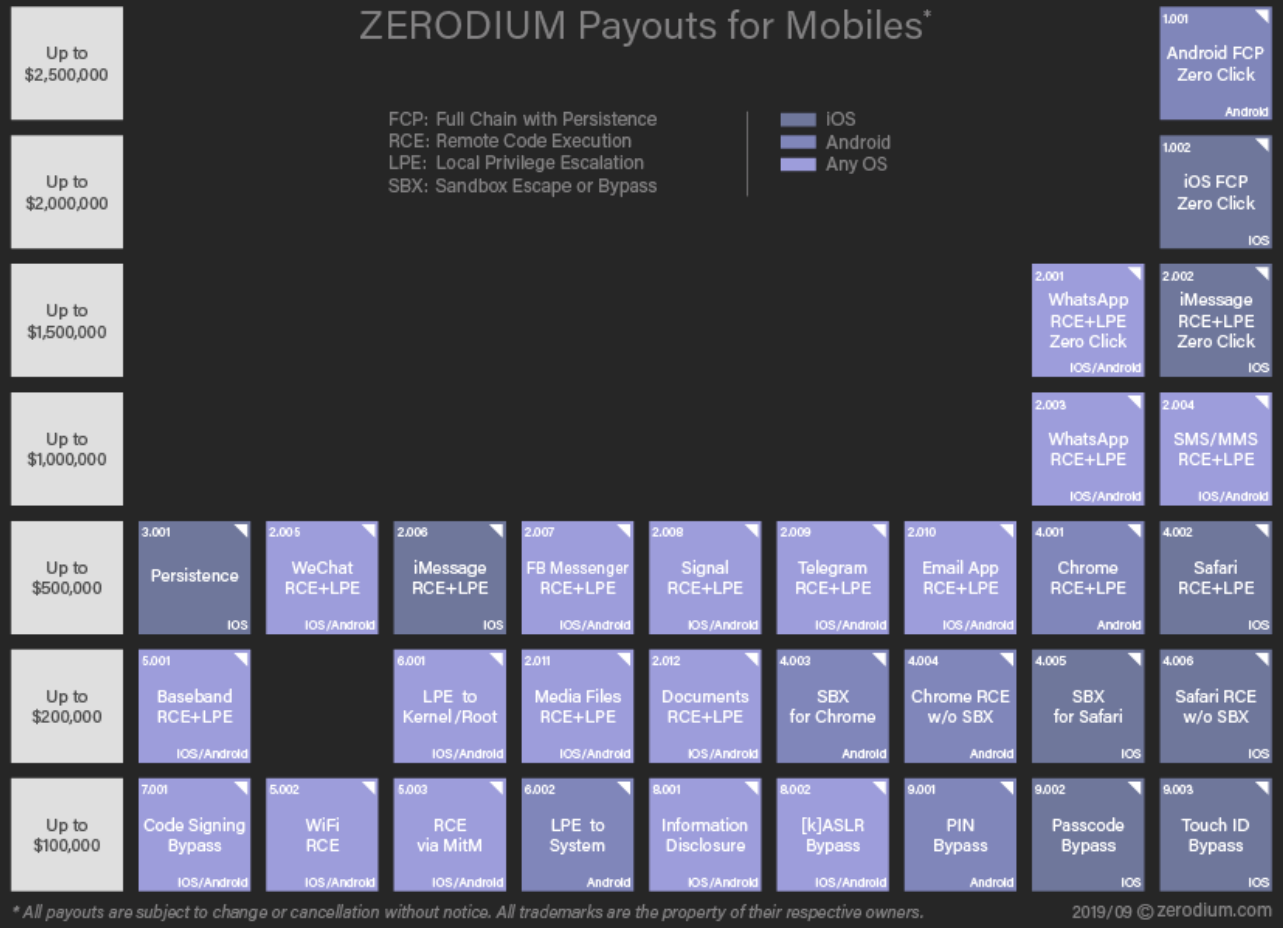
Earn $200K by fuzzing for a weekend: Part 1

addison
May 11, 2022

ESCÁNDALO POLÍTICO

Pegasus: el programa que espía a políticos y gobiernos

- Una investigación periodística revela que varios miembros de los gobiernos catalán y español han sido espiados con este 'spyware'
- Los 'pegasus' contra el terrorismo



Platzi

Certifica a

MARCELO VÁZQUEZ

Por participar y aprobar el

CURSO DE

CÓMO LAVARSE CORRECTAMENTE LAS MANOS

Christian Van Der Henst S
COO DE PLATZI

John Freddy Vega
CEO DE PLATZI

Certificación de aprobación online:

Aprobado el 27 de ABRIL de 2023

3 horas de teoría y práctica

https://platzi.com/@s4vitar/

Código: f830fad2-7a38-4451-b235-c15c0d6586b7

¿Qué es PWN?

¿Qué es PWN?

Introducción a pwntools

Creación de objetos de tipo proceso:

- io = process('./nombreBinario')
- io = remote('IP', PUERTO)

Enviar datos:

- io.sendline(b'AAAA')
- io.sendlineafter(b'entrada:' ,b'AAAA')

Recibir datos:

- datos = io.recvuntil(b'resultado de ')
- datos = io.recvline()
- datos = io.recv(6)

Interactuar:

- io.interactive()

Repo oficial:

https://github.com/Gallopsled/pwntools

Cheatsheet:

https://github.com/Gallopsled/pwntools

Introducción a pwntools

Introducción a GDB (pwndbg)

Comenzar el proceso de depuración:

- gdb ./nombreBinario

Listar todas las funciones:

- info functions

Obtener desensamblado de la función:

- disassemble funcion

Comenzar la ejecución:

- run (r)

Continuar la ejecución:

- continue (c)

Poner breakpoint en main + 468:

- b *main+468

Examinar memoria:

- x/10gx $rsp
- --> mostrar 10 unidades de 8 bytes desde la dirección contenida en RSP

Repo oficial:

https://github.com/pwndbg/pwndbg

Cheatsheet:

https://users.ece.utexas.edu/~adnan/gdb-refcard.pdf

Introducción a GDB (pwndbg)

Resolución de retos de PWN

Listado de retos:

- Kebab amigo
- Pwn is the best category
- Llados pwner
- Kebab amigo II

Kebab amigo (int overflow)

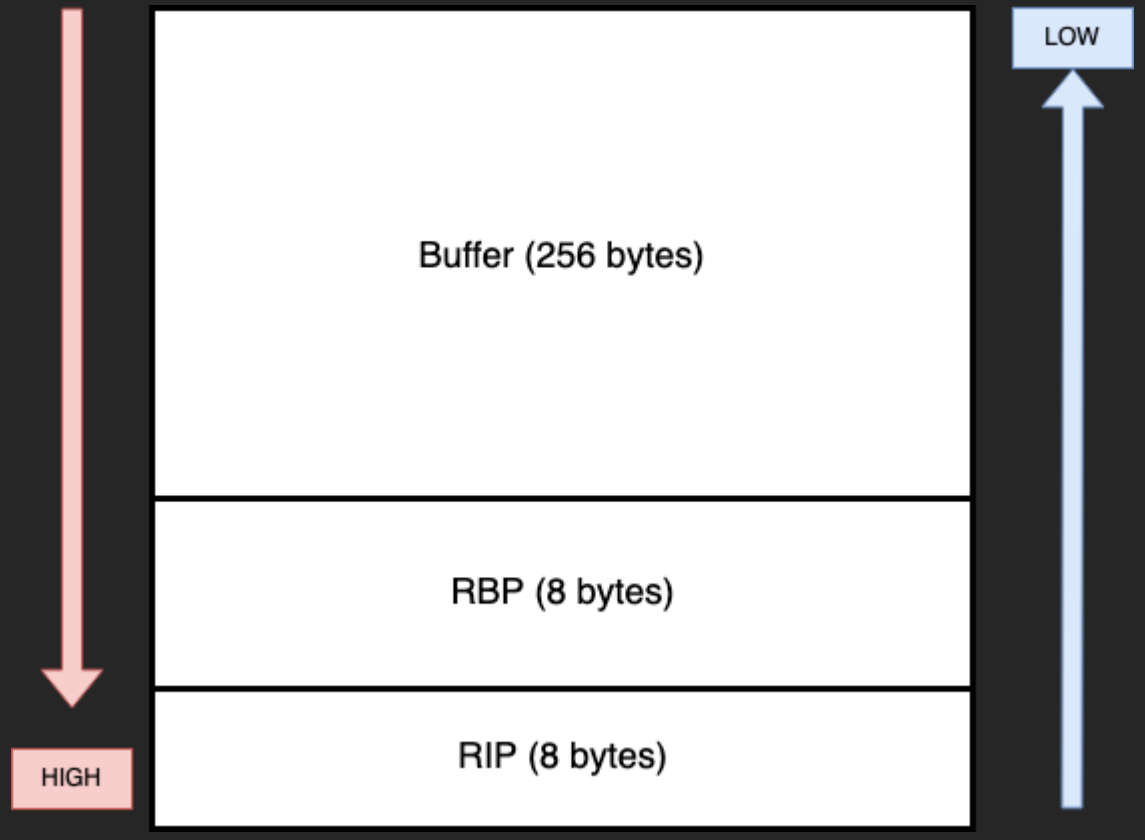
```
(unsigned int)kebab_amigo.rating > MAX_INT
```

=

```
kebab_amigo.rating < 0
```

Pwn is the best category (ret2win)

Se escribe en la pila hacia direcciones de memoria crecientes



La pila crece hacia direcciones de memoria decrecientes

Pwn is the best category

```
GETS(3)                                  Linux Programmer's Manual                                  GETS(3)

NAME
       gets - get a string from standard input (DEPRECATED)

SYNOPSIS
       #include <stdio.h>

       char *gets(char *s);

DESCRIPTION
       Never use this function.

       gets()  reads  a  line from stdin into the buffer pointed to by s until either a terminating newline or EOF, which it replaces with a null byte ('\0').  No check
       for buffer overrun is performed (see BUGS below).
```

Llados pwner (mini ROP)

```
0x0000000000400ae3:
0x0000000000400ae1:
```

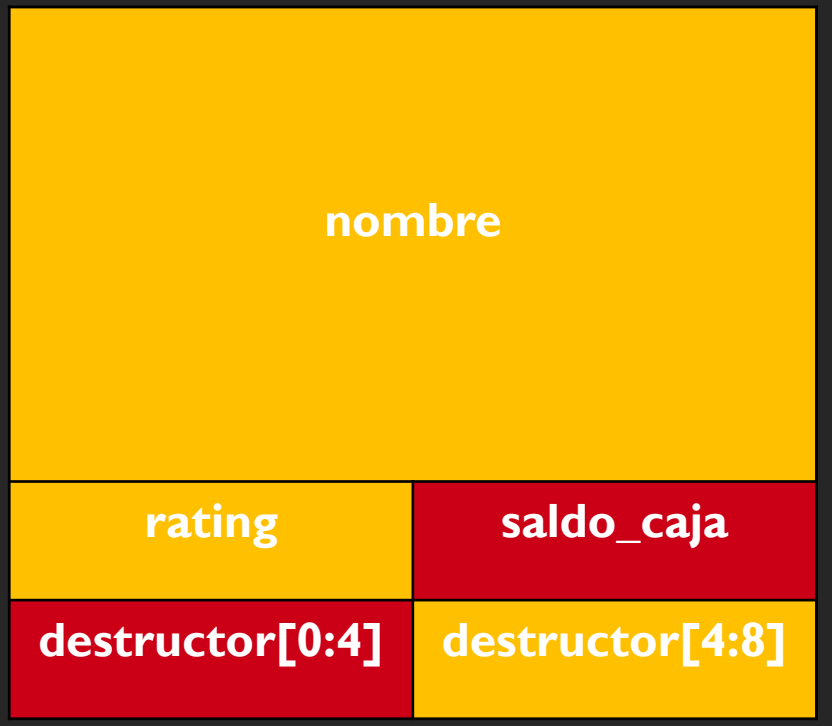
return --> p

ret
eebdaed
15; ret
ffffffff

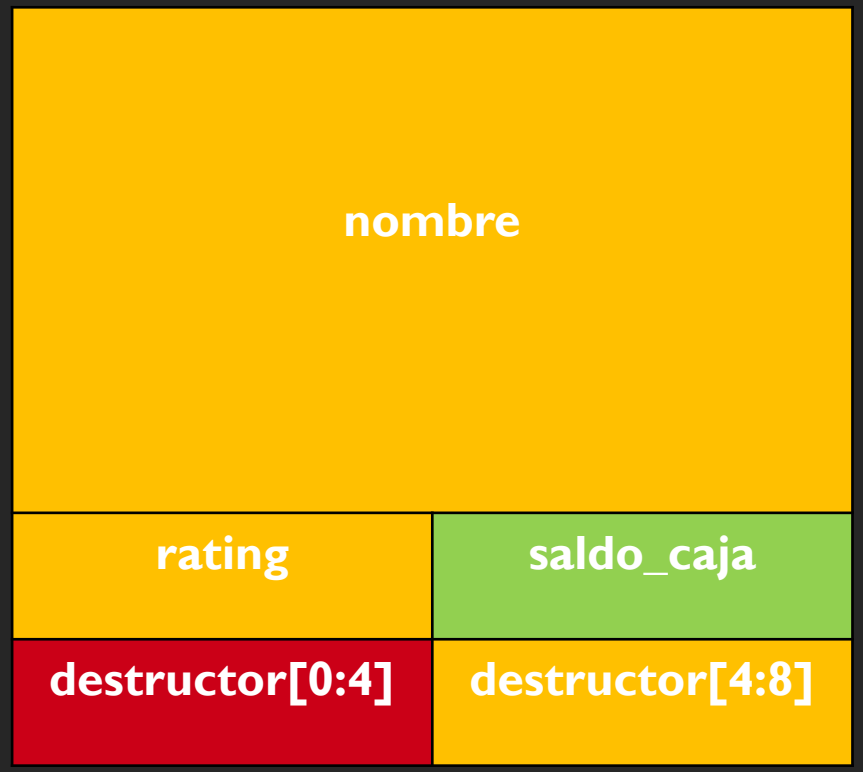
Kebab amigo II (type confusing + ret2libc)

```
struct kebab_amigo_t{
    char nombre[0x20];
    int rating;
    int saldo_caja;
    void (*destructor)();
} kebab_amigo;
```

```
void baklava()
{
    puts("Toma un baklava gratis, encima gratis!");
    puts("Por si quieres dejar propina amigo: ");

    scanf("%ld", &kebab_amigo.saldo_caja);
}
```



Kebab amigo II




```
void banhos_turcos(){
    char respuesta[100];
    puts("Que haces aqui amigo? Esto es solo para empleados!!");
    read(0, respuesta, 0x100);
}
```

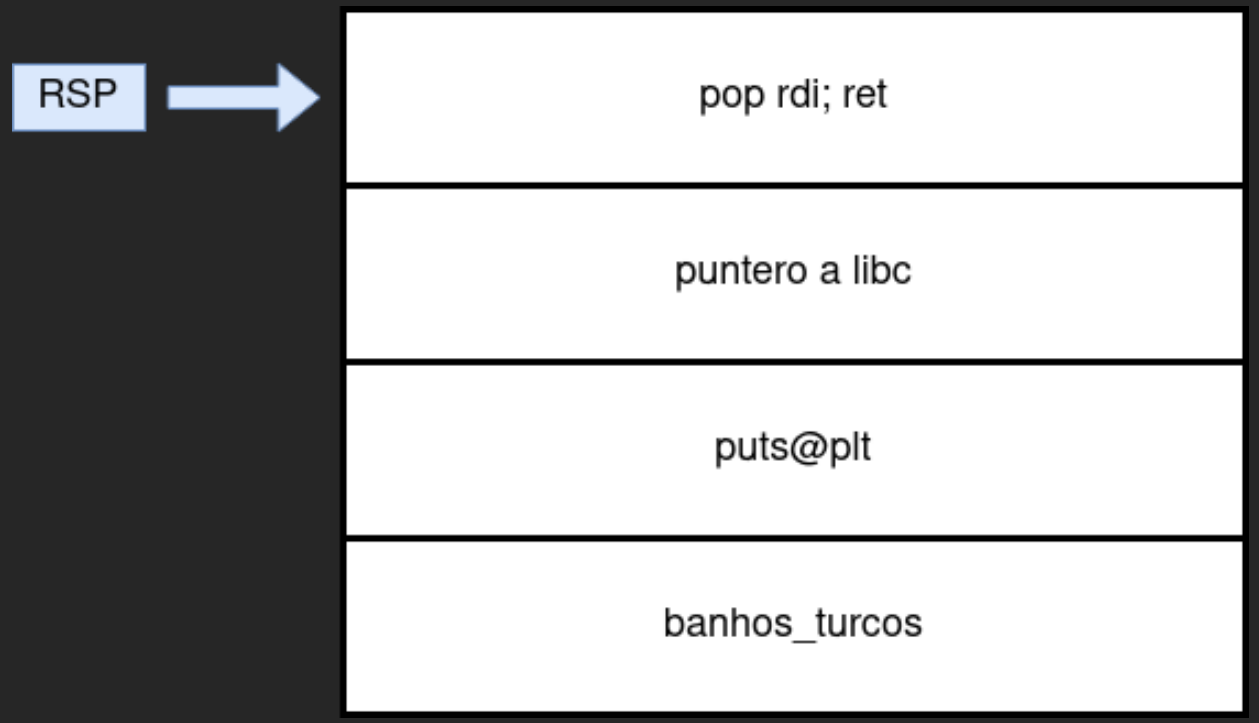
```
pwndbg> i functions banhos_turcos
All functions matching regular expression "banhos_turcos":

Non-debugging symbols:
0x0000000000400b37  banhos_turcos
```

Kebab amigo II

```
void banhos_turcos(){
    char respuesta[100];
    puts("Que haces aqui [illegible] solo para empleados!!");
    read(0, respuesta, 0x100);
}
```

BOF!!

~~Win~~ → Saltamos a LIBC!!



Kebab amigo II

LEAK

```
root@vmi1122080:~/CursoCTF/Retos1/kebab0# python3 xpl.py
[*] '/lib/x86_64-linux-gnu/libc.so.6'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      PIE enabled
[+] Starting local process './chall': pid 69759
puts       @ 0x7f5f1b970e50
libc base  @ 0x7f5f1b8f0000
[*] Switching to interactive mode

$ echo "PWNED!"
PWNED!
```

Módulo IV: Reversing & Exploiting

Tus papis

Universidad
Rey Juan Carlos