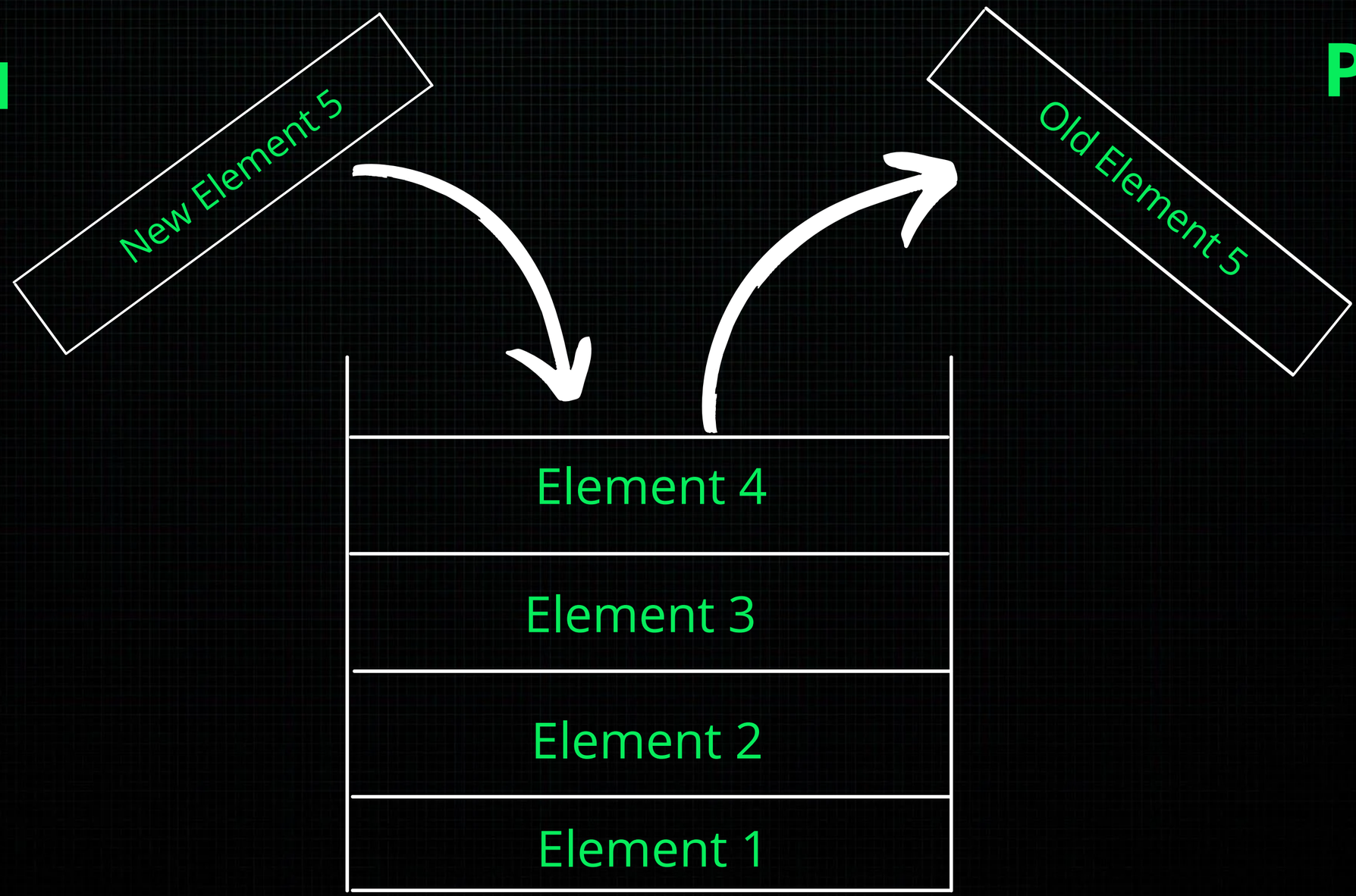

Pwn - Stacks

Stack


PUSH
POP
New Element 5
Old Element 5
Element 4
Element 3
Element 2
Element 1

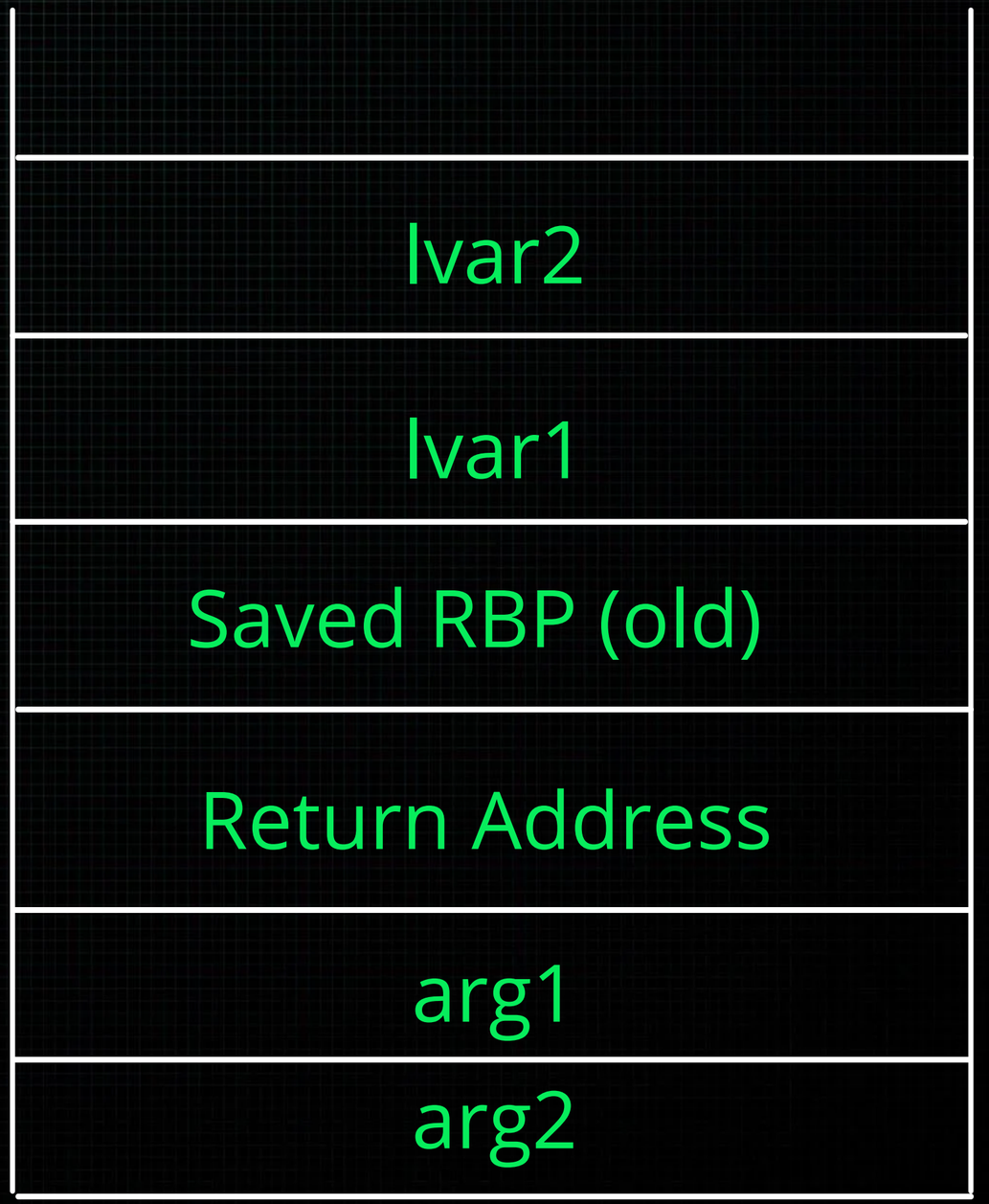
STACK

While going Up the Stack

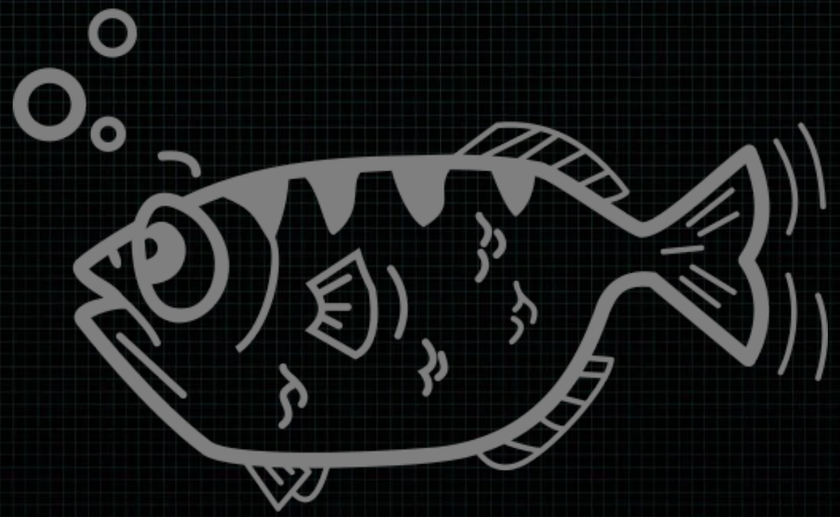
Memory Addresses Value Decreases

Sample Function and Stack

```
int sample(int arg1,float arg2)
{
int lvar1=arg1;
float lvar2=arg2;
return lvar1 + (int) lvar2;
}
```



Debuggers



GNU DeBugger

Take a look at an example !


GDB-EXTENSIONS
gef➤
pwndbg>
gdb-peda$

Decompilers

IDA PRO

*Note: They Make Life Easier !

Buffer Overflow

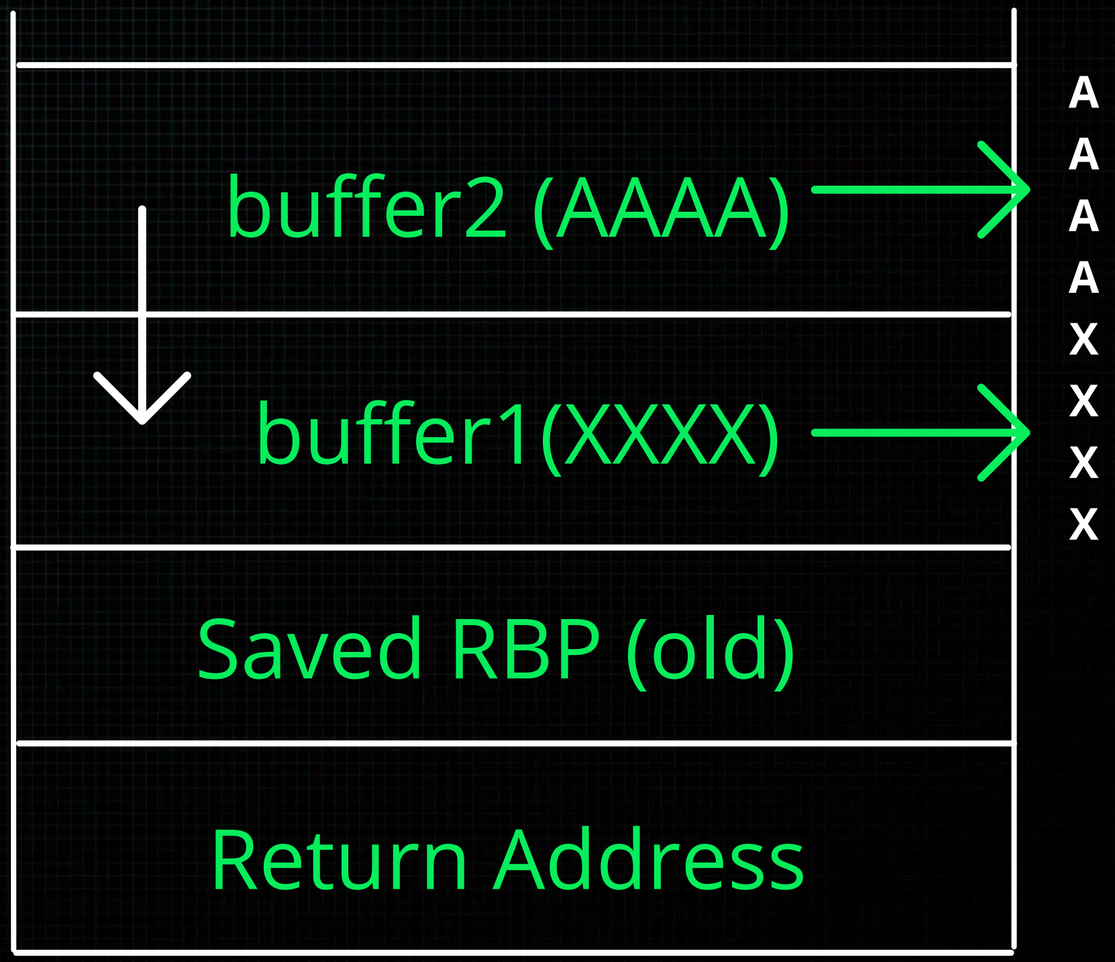
```
int main()
{
char buffer1[6];
char buffer2[4];
gets(buffer2);
puts(buffer1);
}
```

Code

Input : AAAAXXXX

Output: XXXX

IO



Stack

PWNTOOLS

```
$ pip3 install pwntools
```

```
from pwn import *

elf = ELF("./a.out")
p = elf.process()

payload = b'AAAA' + b'SHELL'
p.sendline(payload)
p.interactive()
```

Th@nk$ f0r W47ch1n9 !

Next Video ▶

IP manipulation