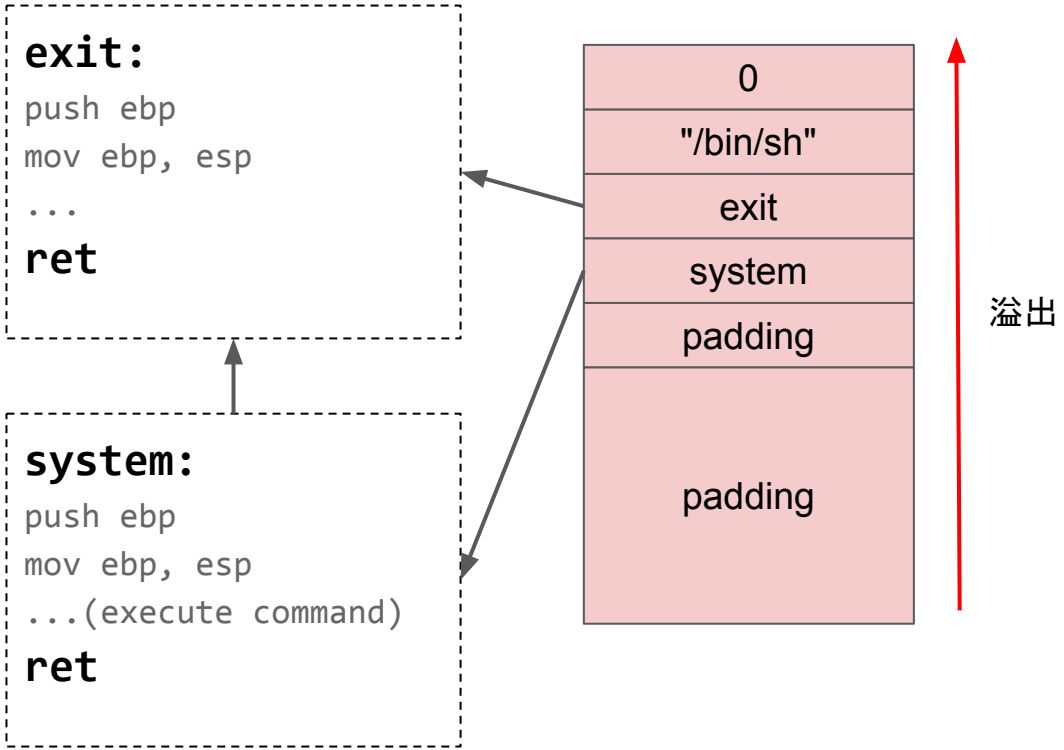
恶意代码分析

第三章：栈溢出、Shellcode与ROP

重新思考 return to libc

- 利用return to libc，我们调用了system("/bin/sh")和exit(0)
- system() 和 exit() 函数本质上都是以 ret 指令结尾的代码片段
- 那如果是其他ret结尾的代码片段呢？例如几条指令组成的小代码片段。同样可行！

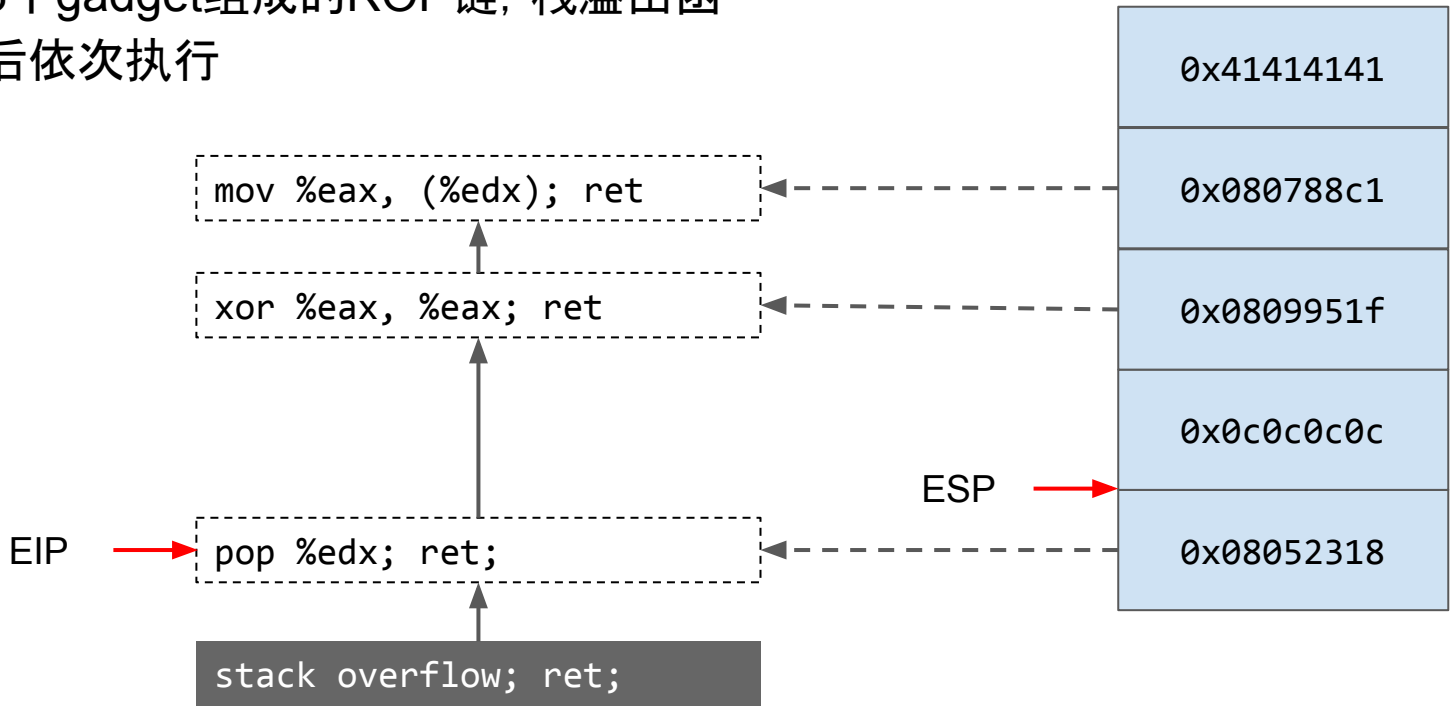


第3节：ROP(Return Oriented Programming)

- 通过拼接以ret指令结尾的代码片段来实现某些功能的技术，称为ROP（Return Oriented Programming）
- 以ret指令结尾的小段代码片段我们称为ROP gadget，例如：pop edx; ret
- 为实现某一功能拼接而成的多个ROP gadget，我们称为ROP链（ROP Chain）
- 在栈上（从返回地址开始）填充的用于执行ROP链的数据，我们称为ROP载荷（ROP Payload）
- ROP技术是Return to libc的扩展，Return to libc是ROP的一种特殊情况，即ROP gadget恰好是libc函数的情形

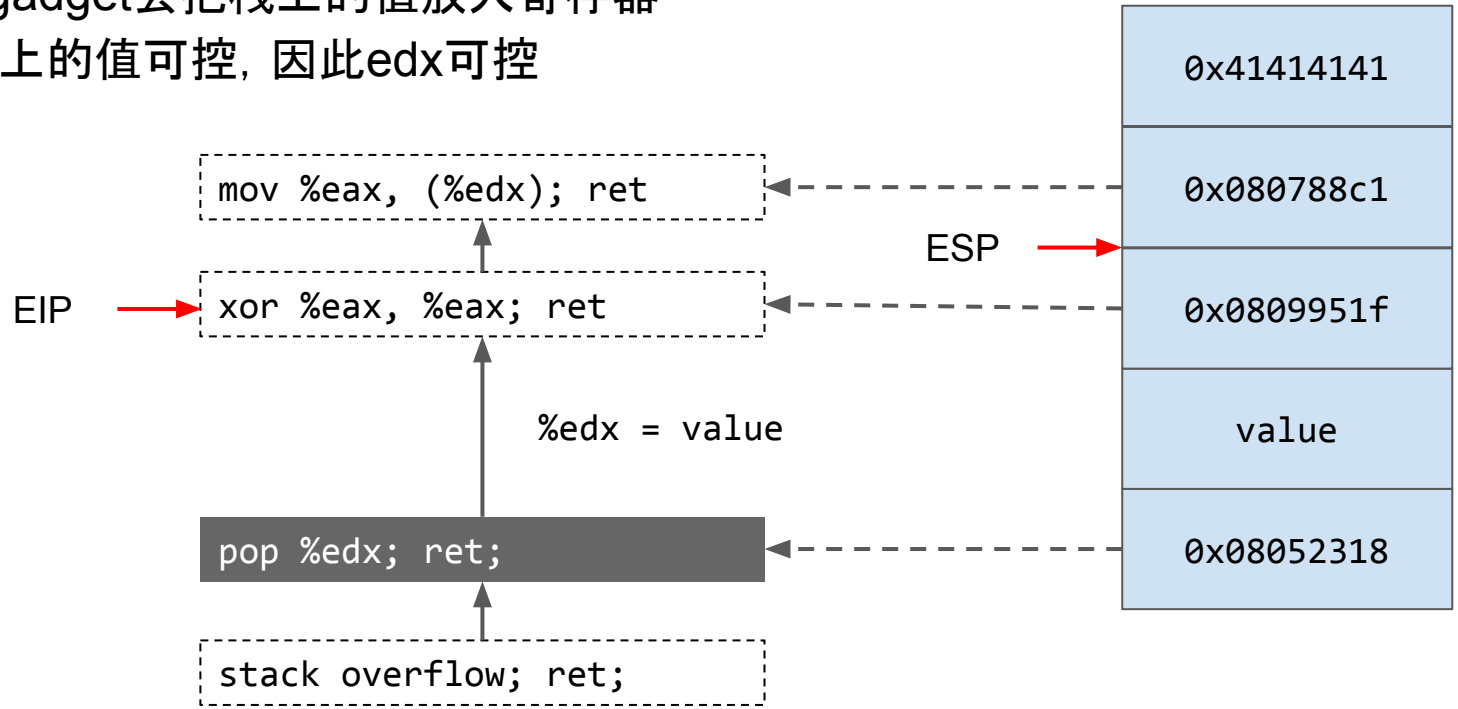
ROP链的执行过程

这是由3个gadget组成的ROP链，栈溢出函数返回后依次执行



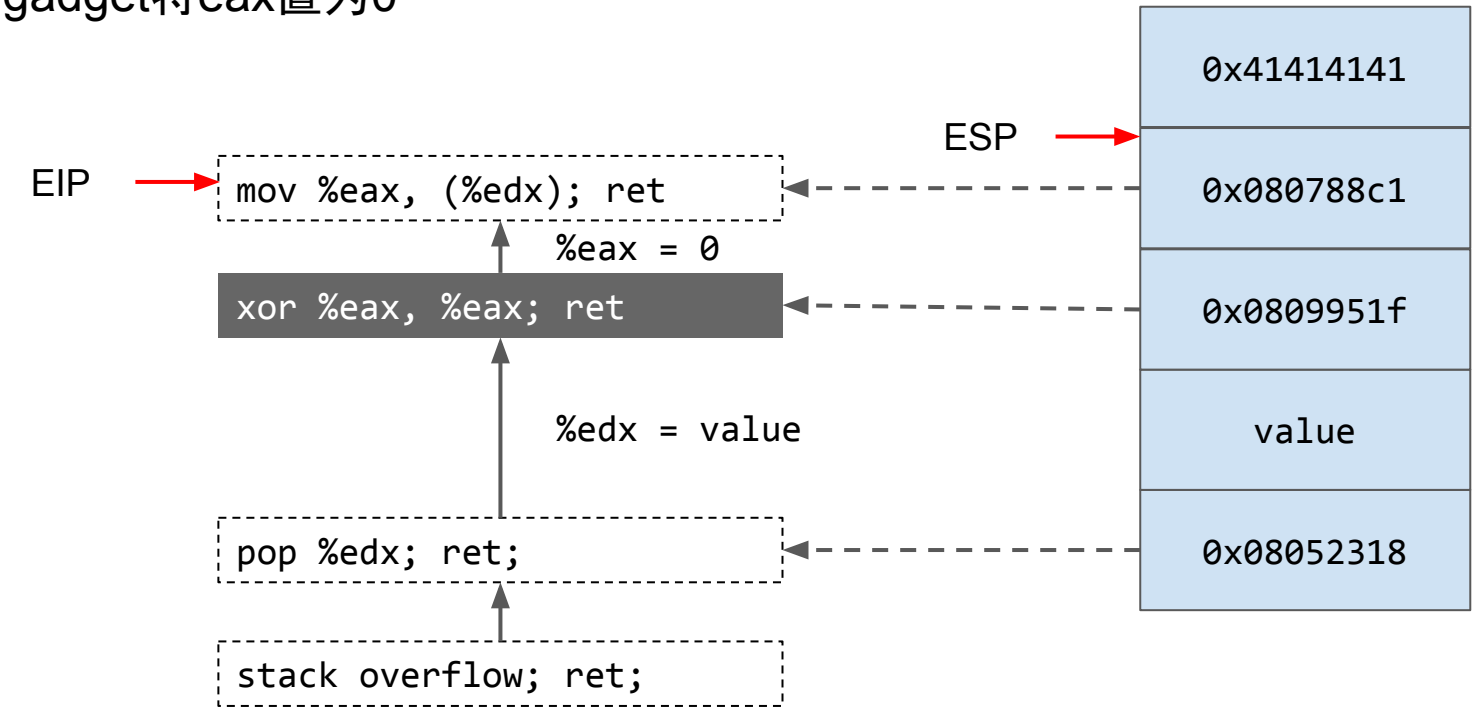
ROP链的执行过程

第一个gadget会把栈上的值放入寄存器edx，栈上的值可控，因此edx可控



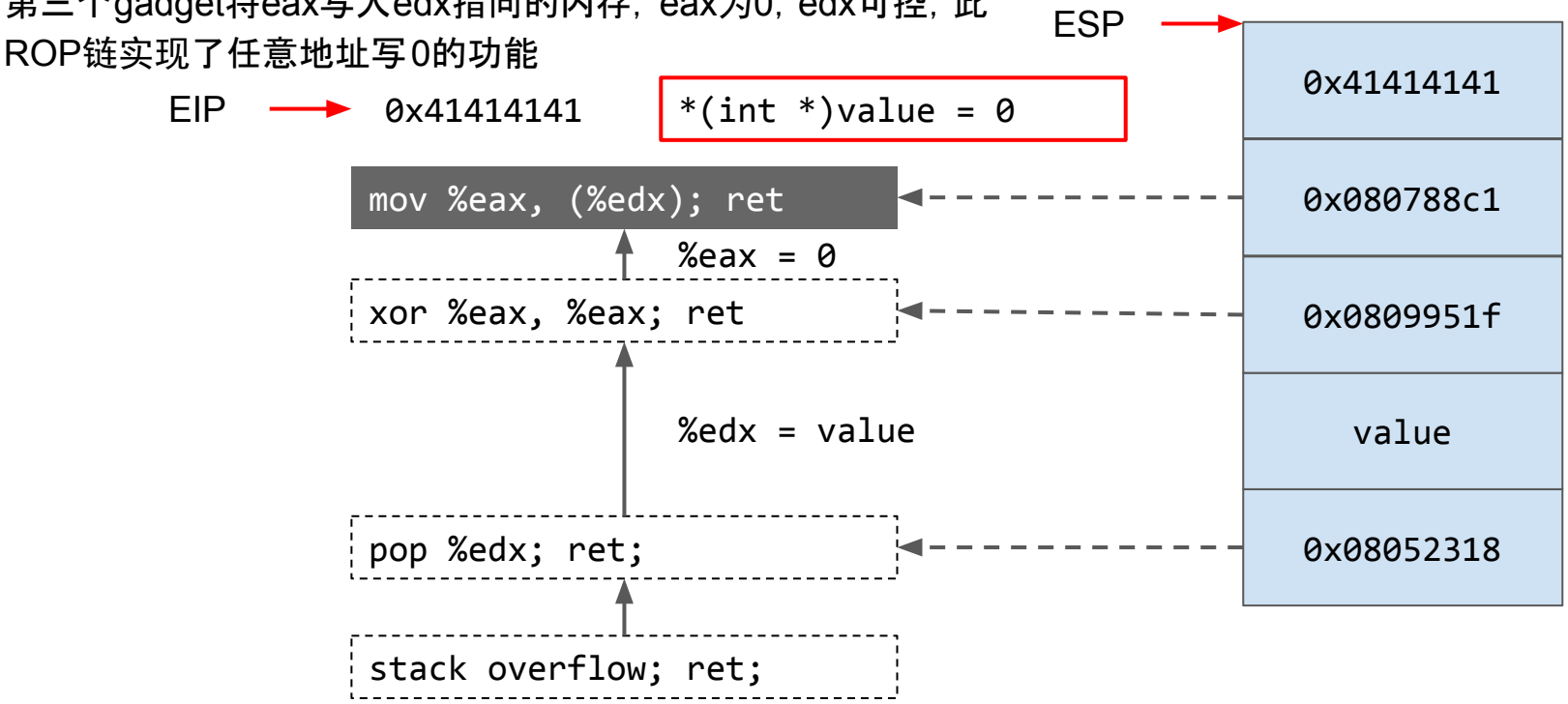
ROP链的执行过程

第二个gadget将eax置为0



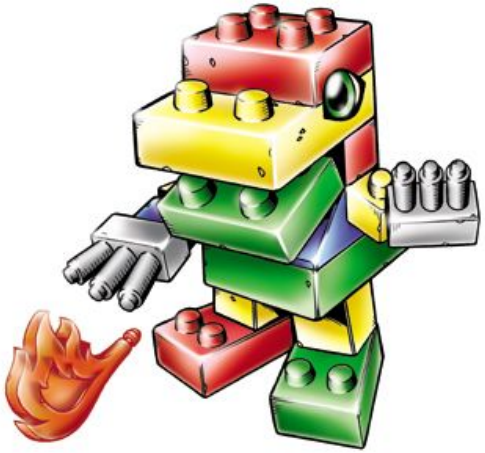
ROP链的执行过程

第三个gadget将eax写入edx指向的内存，eax为0，edx可控，此ROP链实现了任意地址写0的功能



Gadget与ROP Payload的关系

Gadgets



Payload

ROP的扩展——JOP、COP

- 换汤不换药，把使用的代码片段从ret结尾扩展到jmp/call结尾
- JOP（Jump Oriented Programming）
  - pop esi ; jmp dword [esi-0x70]
- COP（Call Oriented Programming）
  - mov eax, dword [esp+0x48] ; call dword [eax+0x10] ;

ROP Gadget 搜索工具

- ROPGadget
  - https://github.com/JonathanSalwan/ROPgadget
- rp
  - https://github.com/0vercl0k/rp
- ropper
  - https://github.com/sashs/Ropper
- xrop
  - https://github.com/acama/xrop

使用工具 rp 寻找 Gadgets

```
$ rp -f ropasaurusrex -r 3
A total of 102 gadgets found.
0x080484d0: adc edi, dword [ebx+0x0804951C] ; nop  ; sub ebx, 0x04 ; call eax ;
0x080483ed: add al, 0x08 ; call eax ;
0x080484d4: add al, 0x08 ; nop  ; sub ebx, 0x04 ; call eax ;
0x080483e9: add al, 0x24 ; sub al, 0x95 ; add al, 0x08 ; call eax ;
0x080483c1: add al, 0x5B ; pop ebp ; ret  ;
0x080482e7: add byte [eax+0x5B], bl ; leave  ; ret  ;
0x080482c5: add byte [eax], al ; add byte [ebx-0x7F], bl ; ret  ;
0x080484f7: add byte [ebx-0x7F], bl ; ret  ;  (1 found)
0x080482e5: add dword [eax], eax ; add byte [eax+0x5B], bl ; leave  ; ret  ;
0x080483be: add dword [ebx+0x5D5B04C4], eax ; ret  ;  (1 found)
0x080483b9: add eax, 0x08049628 ; add dword [ebx+0x5D5B04C4], eax ; ret  ;
0x080483bf: add esp, 0x04 ; pop ebx ; pop ebp ; ret  ;
0x0804841a: dec ecx ; ret  ;
0x08048506: leave  ; ret  ;
...
$ rp -f /lib/i386-linux-gnu/libc.so.6  -r 3
Trying to open '/lib/i386-linux-gnu/libc.so.6'..
A total of 109981 gadgets found.
```

-f 指定搜索gadget的ELF文件

-r 参数指定gadget最小长度