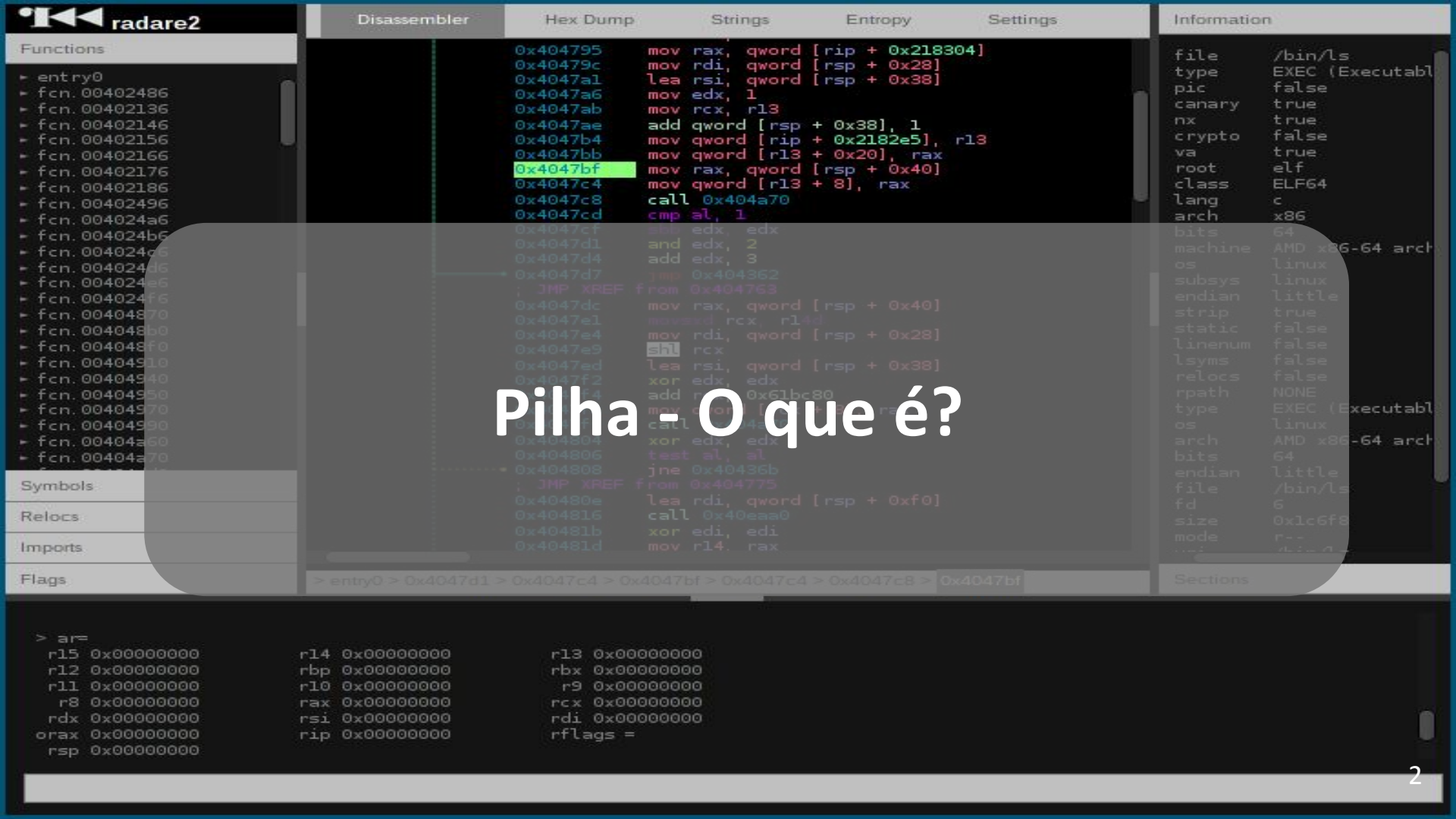
ICMC USP SÃO CARLOS

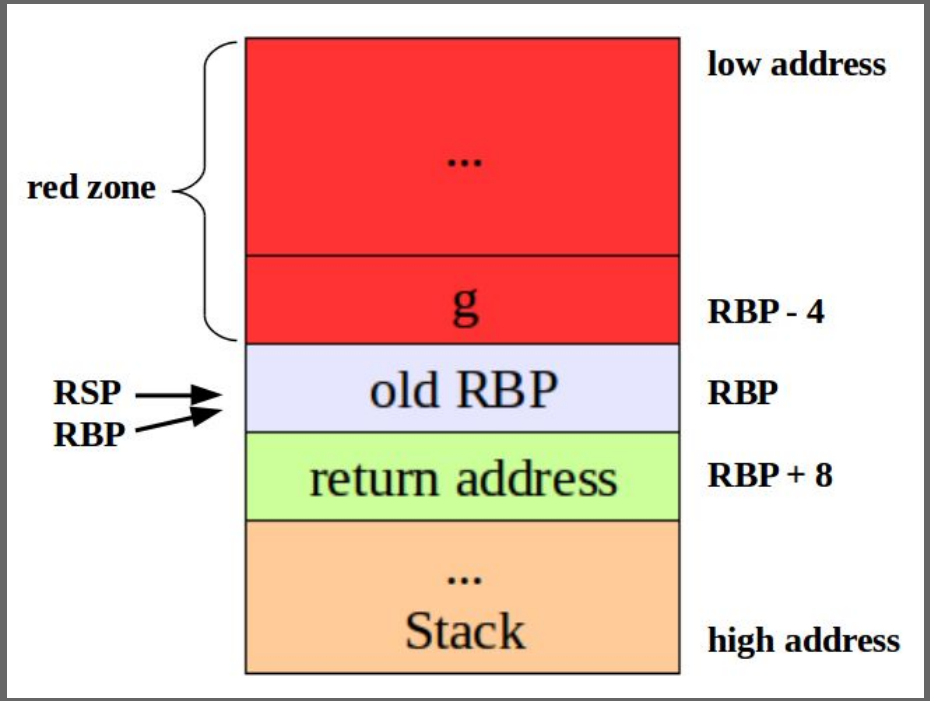
GANESH

Engenharia Reversa

asrever ed etnerf


radare2
Disassembler
Hex Dump
Strings
Entropy
Settings
Information
Functions
Symbols
Relocs
Imports
Flags
Sections
Pilha - O que é?

Funcionamento da pilha



- Pilha
  - rsp: stack pointer (topo)
  - rbp: base pointer (base)

Como manipular?

- Push / Pop
- add / sub
- lea

```
push rbp

pop rbp


sub rsp, 0x10

add rsp, 0x10


lea eax, DWORD PTR[rbp - 0xa]
```

Por que é importante

- Declaração de variáveis

- Chamada de funções
  - retorno
  - rbp

Exemplo

```c
#include <stdio.h>

int main(){
     printf("Hello, world!\n");
     return 0;
}
```

```
0000000000001139 <main>:
    1139: 55                        push   rbp
    113a: 48 89 e5                  mov    rbp,rsp
    113d: 48 8d 3d c0 0e 00 00      lea    rdi,[rip+0xec0]        # 2004 <_IO_stdin_used+0x4>
    1144: e8 e7 fe ff ff            call   1030 <puts@plt>
    1149: b8 00 00 00 00            mov    eax,0x0
    114e: 5d                        pop    rbp
    114f: c3                        ret
```

Ferramentas úteis

- objdump
- Hexdump (xxd)
- gdb [+ peda]
- nasm

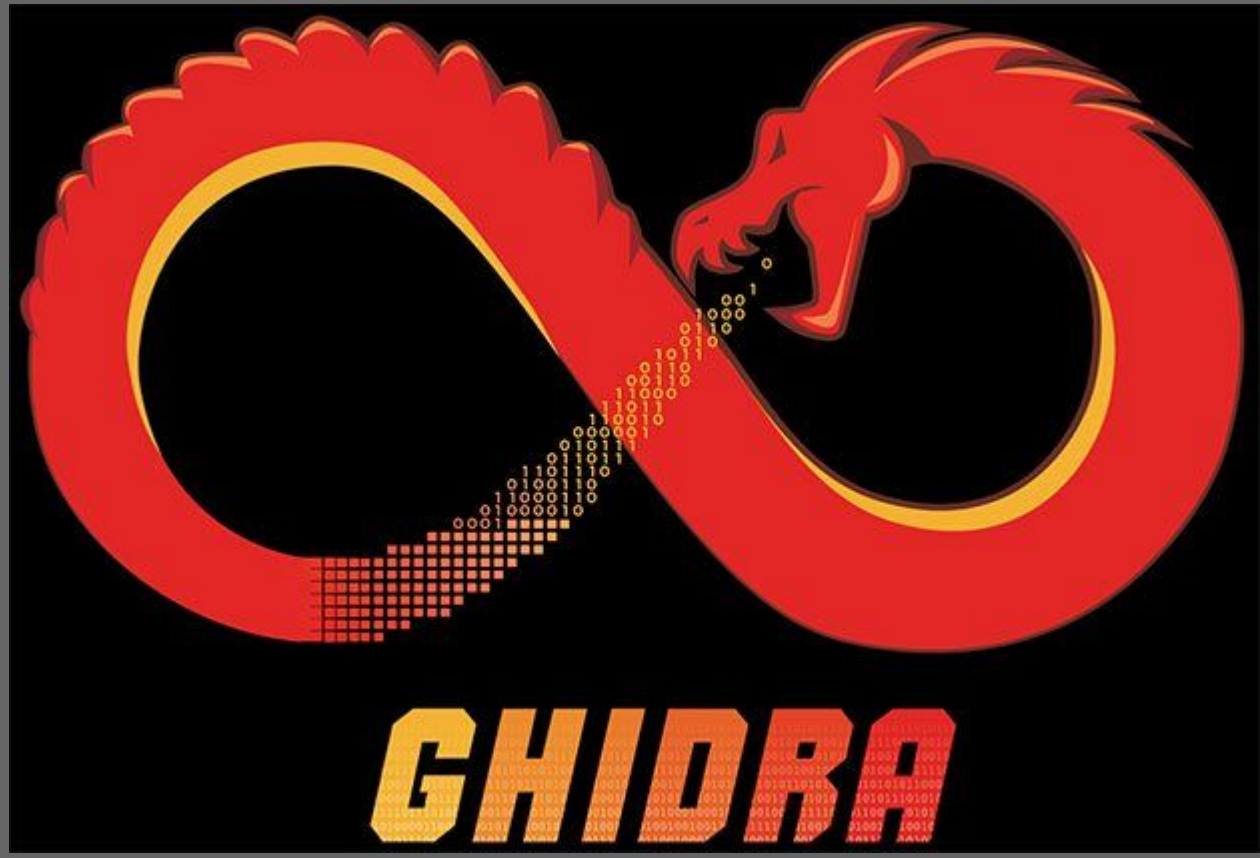
```
$ objdump -Mintel -d prog

$ hexdump prog

$ nasm -f elf64 prog.asm
$ ld -s -o prog prog.o -m elf_x86_64
$ ./prog ; echo $?
```

Ferramentas

- GDB

Ferramenta OP

- Ghidra



GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br