
# Aula 03

# Engenharia Reversa e Análise de Malware

Ronaldo Pinheiro de Lima
crimescibernéticos.com@gmail.com

# Aula 03

2.12. Exemplo de código em C e Assembly

2.13. Mais informações: linguagem assembly e arquitetura Intel x86

2.14. **Lab-02-01:**
Entendo na prática o funcionamento da pilha com o OllyDbg

# Exemplo de código em C e Assembly

```
int main(int argc, char* argv)

programateste.exe -r filename.txt
argc = 3
argv[0] = programateste.exe
argv[1] = -r
argv[2] = filename.txt
```

```
int main(int argc, char* argv[]){

        if (argc != 3) { return 0; }

        if (strncmp(argv[1], "-r", 2) == 0)
        {
                DeleteFileA(argv[2]);
        }
        return 0;
}
```

# Exemplo de código em C e Assembly

```
004113CE    cmp     [ebp+argc], 3 ❶
004113D2    jz      short loc_4113D8
004113D4    xor     eax, eax
004113D6    jmp     short loc_411414
004113D8    mov     esi, esp
004113DA    push    2                   ; MaxCount
004113DC    push    offset Str2         ; "-r"
004113E1    mov     eax, [ebp+argv]
004113E4    mov     ecx, [eax+4]
004113E7    push    ecx                 ; Str1
004113E8    call    strncmp ❷
004113F8    test    eax, eax
004113FA    jnz     short loc_411412
004113FC    mov     esi, esp ❸
004113FE    mov     eax, [ebp+argv]
00411401    mov     ecx, [eax+8]
00411404    push    ecx                 ; lpFileName
00411405    call    DeleteFileA
```

# Mais informações: arquitetura x86 e assembly

## *Manuais Intel*

Descrição detalhada das arquitetura, ambiente de programação, registradores, memória, instruções, otimizações de compiladores, etc.

Downloads: http://intel.ly/u7ZHpu e http://intel.ly/x1cLz5.

## *Livro Art Of Assembly*

Conteúdo completo e detalhado sobre a linguagem. Está disponível online para ser baixado gratuitamente.

Download: http://www.artofasm.com/index.html.

# Lab-02-01:

## Prática com OllyDbg, funcionamento da Pilha

***Material necessário:***

- Máquina virtual com Windows XP 32-bit
- OllyDbg
- Arquivo: Lab-02-01.exe

# Obrigado!

A explicação detalhada de todos os tópicos está na apostila.

**Ronaldo Pinheiro de Lima**
crimescibernetico.com@gmail.com
http://www.crimescibernetico.com
@crimescibernet