

Engenharia Reversa no Linux

Fernando Mercês
fernando@mentebinaria.com.br





O que é Engenharia Reversa?

O que é Engenharia Reversa?

Engenharia Reversa (ER), em inglês Reversing Engineering (RE), é uma técnica, por vezes definida como arte, de se entender como um dispositivo ou software funciona sem possuir seu esquema/código-fonte.

No caso de software, é útil para estudar como os programas executam as rotinas e se comportam no sistema, resolver problemas com softwares mal feitos ou não mais suportados, portar drivers de dispositivos, dentre outros.



Foi (e ainda é) amplamente utilizada para o desenvolvimento de drivers no Linux.

The background features a complex, abstract pattern of glowing lines and a grid. The lines are primarily blue and cyan, radiating from the bottom left towards the top right. Overlaid on these are horizontal bands of a repeating grid pattern in a golden-brown or orange hue. The overall effect is a sense of digital data or a futuristic interface.

E isso é crime?

E isso é crime?

Depende de como utilizada. Obter o código-fonte de softwares proprietários sem autorização é crime. Alterá-los também. Essa técnica é conhecida como cracking e encarada como crime em vários países, inclusive no nosso.



**Por que reverter
no Linux?**

Por que reverter no Linux?

- Aprendizado de como os programas se comportam no sistema.
- Resolução de problemas (troubleshooting).
- Adaptação de drivers de dispositivos.
- Análise de programas desconhecidos.
- Criar outro programa compatível com o formato ou protocolo utilizado pelo que sofrerá a ER

Por que reverter no Linux?

- Adicionar ou remover funções de programas.
- Descobrir funções não documentadas de programas.
- Recriar o código-fonte do programa.
- Documentar o comportamento do programa, para programas sem documentação.

The background is a dark, abstract composition. It features numerous horizontal lines of glowing binary code (0s and 1s) in shades of orange and yellow. These lines are set against a backdrop of vibrant, multi-colored light trails in shades of blue, green, and cyan, which appear to be moving or vibrating. The overall effect is a sense of digital data and motion.

Arquivos binários

Arquivos binários

- Como o próprio nome sugere, um arquivo binário é um conjunto de bits.
- Seu formato deve ser especificado e conhecido pelo sistema operacional.
- Suas instruções ASM e arquitetura devem ser conhecidas pelo microprocessador.
- Editável como qualquer outro arquivo.
- Compactável e criptografável com métodos especiais.

O formato ELF

Este é o formato padrão de arquivos executáveis, bibliotecas e outros arquivos binários nos sistemas GNU/Linux, originário do System V.

ELF é acrônimo de Executable and Linkable Format (Formato *linkável* e executável).



No Windows o formato de arquivos executáveis é o PE (Portable Executable), conhecido também por MZ.

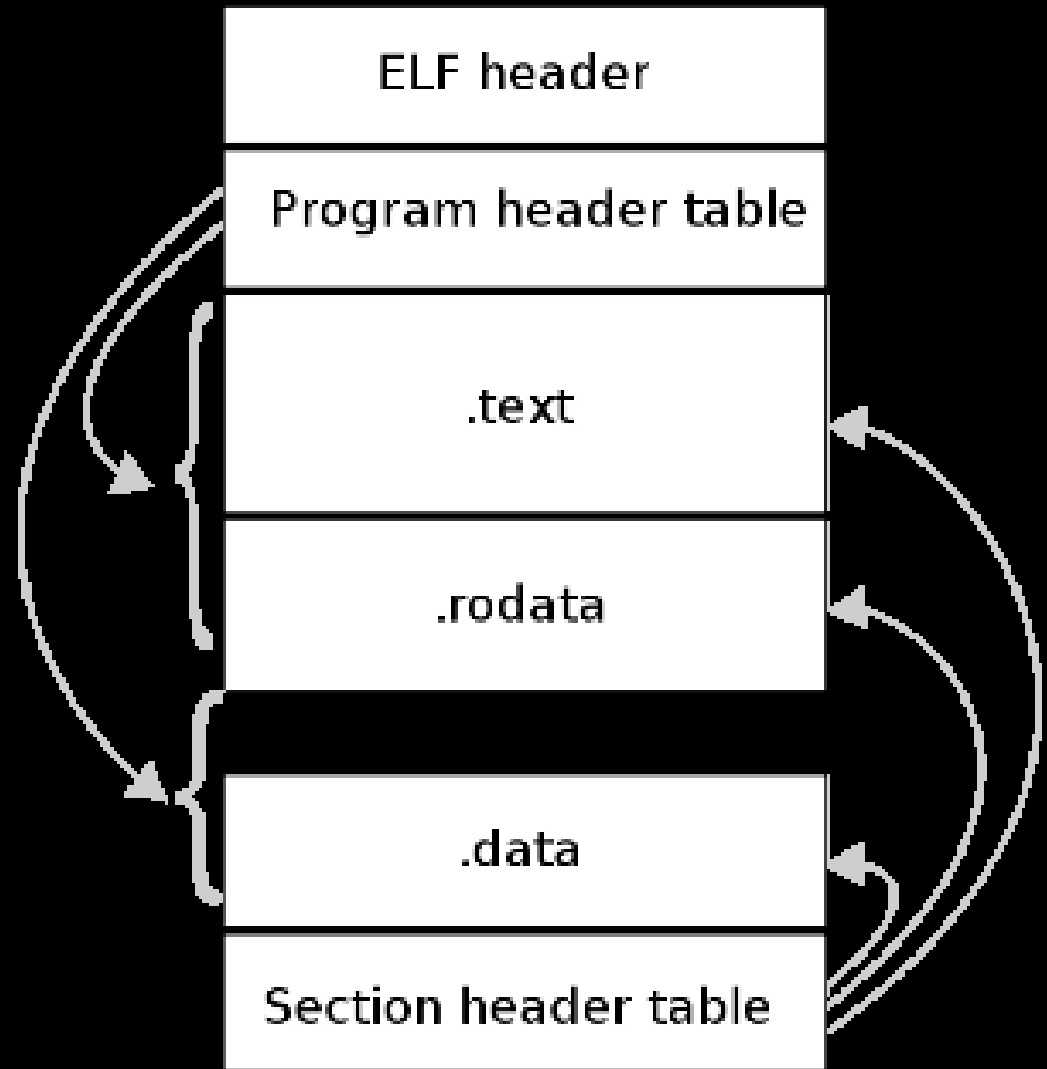
O formato ELF

Program header table especifica os segmentos.

Section header table especifica as seções.

As **seções** pertencem aos segmentos.

Os bytes fora das seções são chamados **bytes órfãos** (orphan bytes).



Formato ELF



Assembly (ASM)

- Linguagem de máquina.
- Os fabricantes de microprocessadores fornecem documentação das instruções ASM aceitas por sua arquitetura.
- Existem duas principais representações da linguagem Assembly, a Intel e a AT&T. O Linux costuma trabalhar com a segunda.
- Toda instrução ASM tem seu equivalente em hexadecimal, que por sua vez, possui seu equivalente em binário mas nem sempre em ASCII.



Ferramentas para ER no Linux

Ferramentas para ER no Linux

Antes de utilizar as ferramentas, vamos compilar um pequeno software no Linux, em C.

```
#include <stdio.h>  
  
int main() {  
    printf("VOL DAY I");  
    return 0;  
}
```

Ferramentas para ER no Linux

- strings » localiza textos imprimíveis em arquivos.
- readelf » exibe informações sobre binários ELF.
- hexdump » exibe a representação em hexadecimal de arquivos.
- objdump » exibe a estrutura de binários ELF.
- strace » exibe as chamadas de sistema que um binário faz e seus retornos.
- hte » editor de arquivos executáveis.

Ferramentas para ER no Linux



Ferramentas para ER no Linux

Para a demonstração do **strace**, vamos escrever um novo programa, que tenta apagar um arquivo.

```
#include <stdio.h>  
  
int main() {  
    remove("/sbin/ifconfig");  
    return 0;  
}
```

strace



Ferramentas para ER no Linux

Para a próxima demonstração, vamos incrementar nosso programa `hello.c` com um condicional.

```
#include <stdio.h>  
  
int main() {  
    int i=1;  
    if (i=1)  
        printf("VOL DAY I");  
    else  
        printf("VOL NIGHT I");  
    return 0;  
}
```

Byte patching com
o hte





Packers

Packers

- Comprime o arquivo binário.
- Injeta código para descompressão em memória.
- Protege o software contra disassemblers.
- São removíveis (unpacking).

UPX



The background features a dark, almost black, space filled with numerous thin, glowing lines in shades of cyan and blue. These lines radiate from the bottom-left corner, creating a sense of depth and movement. Overlaid on this is a grid of small, glowing orange squares, which appear to be arranged in a pattern that recedes into the distance, similar to a perspective view of a grid. The overall effect is a futuristic, digital, or data-oriented aesthetic.

Debugging

O debugger

- Permite executar de um binário passo-a-passo, para analisar seu comportamento.
- Aliado a um disassembler, permite alterações em tempo de execução (*runtime*) no código.
- É possível setar *breakpoints* para a execução parar. Isto facilita a análise, principalmente num arquivo grande.

O gdb (**GNU Debugger**)

- Debugger em modo texto com bons recursos.
- Necessita que o software tenha sido compilado com seus symbols, para um debugging eficiente.
- Possui implementações gráficas (GUI) disponíveis nos repositórios das distros.

Demonstração gdb



Para saber mais...

HoneyNet Project

<http://honeynet.org>

Introduction to Reversing Engineering in Linux

www.acm.uiuc.edu/sigmil/RevEng

Linux Assembly

<http://asm.sourceforge.net>

www.tldp.org/HOWTO/Assembly-HOWTO

Fenris RE package

<http://lcamtuf.coredump.cx/fenris>

Mente Binária

www.mentebinaria.com.br

Perguntas /
Comentários ?

Obrigado!

Fernando Mercês
fernando@mentebinaria.com.br

