Engenharia Reversa

Abordagem Prática Introdutória em Executáveis

Nathan Guimarães

Departamento de Ciência da Computação - Universidade Tecnologia Federal do Paraná (UTFPR)

Santa Helena – PR - Brazil
nathan.2019@alunos.utfpr.edu.br

Abstract. *This meta article describes the process of reverse engineering an executable using intermodule searching and process overwriting techniques..*

Resumo. *Este artigo descreve o processo de engenharia reversa em um executável utilizando técnicas de buscas por intermodulos e sobrescrita de processos.*

1. Introdução

Supondo que exista um software e que o mesmo necessite de uma manutenção, a única coisa que sabe-se sobre tal programa é que o mesmo foi inscrito há mais de 30 anos e existe uma grande chance dos desenvolvedores desse software já estejam aposentados.

Partindo desse pressuposto e necessário a realização de uma análise, porém tudo que se sabe quando ao software, são informações vagas como a citada anteriormente que de certa forma não acrescentam muito na resolução do problema proposto.

Tendo em mãos apenas o produto final, ou seja, o executável é necessário realizarmos uma análise com esse produto.

É nessa etapa que entra o processo de engenharia reversa, sendo uma atividade que trabalha com um produto existente (um software, uma peça mecânica, uma placa de computador, etc.) tentando entender como este produto funciona, o que ele faz exatamente e como ele se comporta em todas as circunstâncias.

A Engenharia reversa é feita quando desejamos modificar uma peça ou software por outro, ou ate mesmo para entender como tal produto seja ele software ou não, funciona.

Um exemplo a grosso modo utilizando engenharia reversa é um carro, se quissemos saber como um carro funciona porém só temos o carro como produto final, a engenharia reversa seria o processo de desmontar o carro a fim de tentar entender seus componentes e funcionamento dos mesmos.

Tratando de depuradores sabemos que Assembly é a linguagem de máquina se encontra no menor nível de abstração.

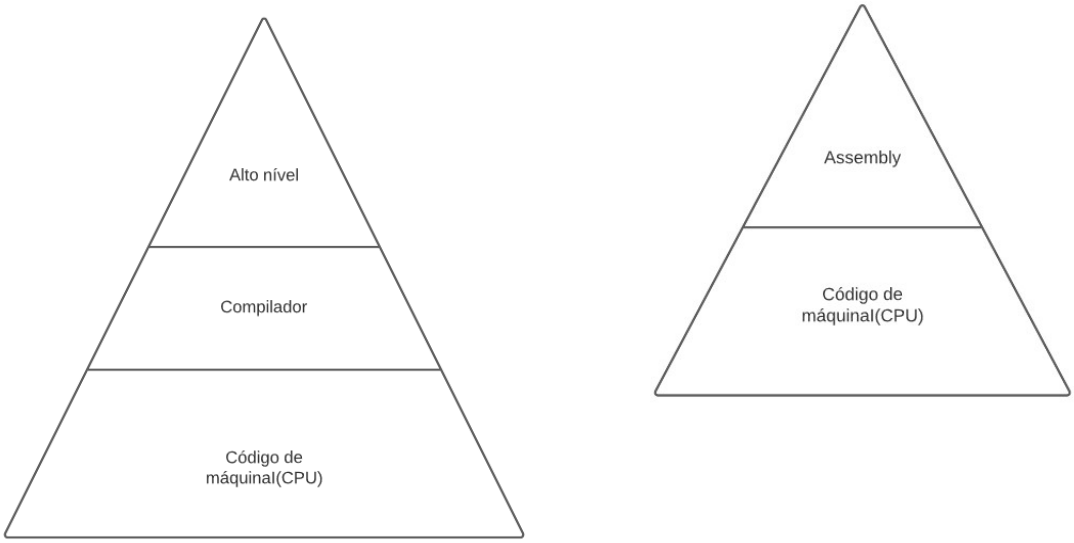
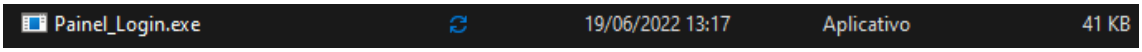


Imagem 1: Comparação de Ambientes

Dessa forma a linguagem Assembly possui mnemônicos que resultam em **1 = 1**, ou seja, semanticamente sua sintaxe equivale ao mesmo código de máquina.

2. Metodologia

O processo de engenharia reversa o qual vamos elaborar como uma abordagem introdutória pressupõe da existência de um executável escrito em linguagem C.



Para estarmos desmontando o executável vamos utilizarmos a ferramenta OnlyDBG disponível em https://www.ollydbg.de/

Uma vez instalada vamos executar a ferramenta com acesso de administrador

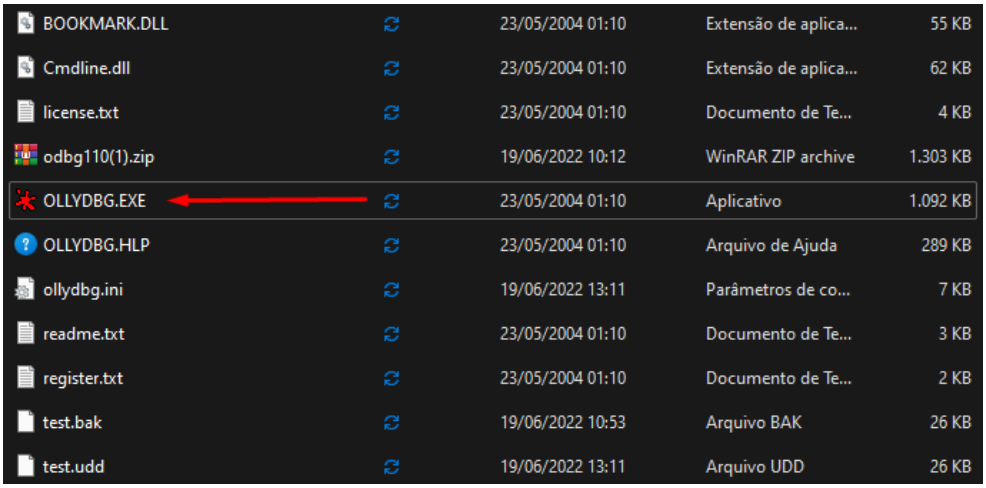


Imagem 2: Pasta Descompactada com Executável

Uma vez aberto, vamos até a aba *File* e abriremos nosso executável o qual desejamos depurar

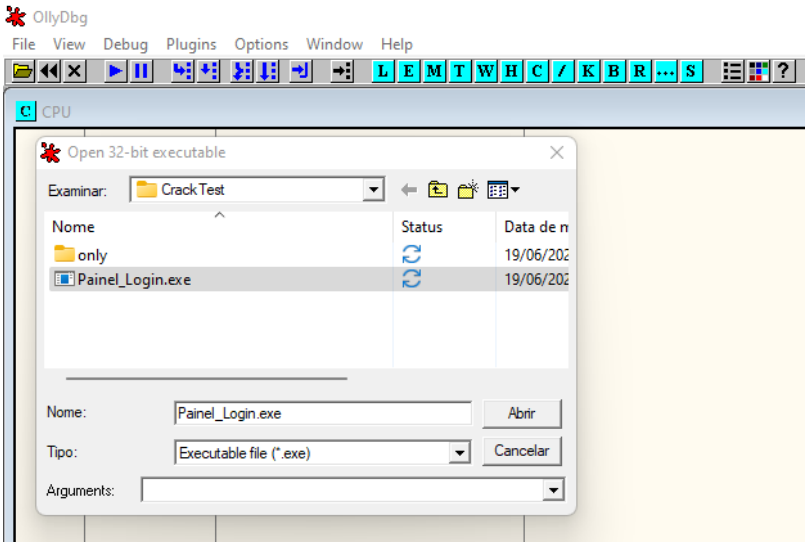


Imagem 3: Abrir Executável a ser Desmontado

Apos aberto o depurador logo exibe nossos códigos de máquina e seus respectivos processos e registradores no baixo nível.

Seguindo os conceitos a respeito da linguagem assembly abordados em sala de aula, é possível realizarmos uma busca pelos intermodulos é possível realizarmos uma busca pela principal *String* e saltarmos o processo responsável pela verificação de validade da senha.

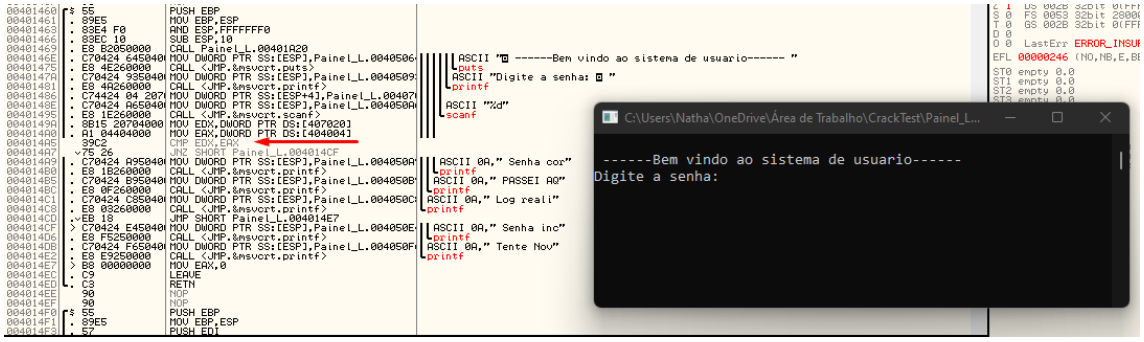


Imagem 4: Localizado Processo

Após localizarmos o processo basta apenas saltarmos e continuar a execução do programa no terminal

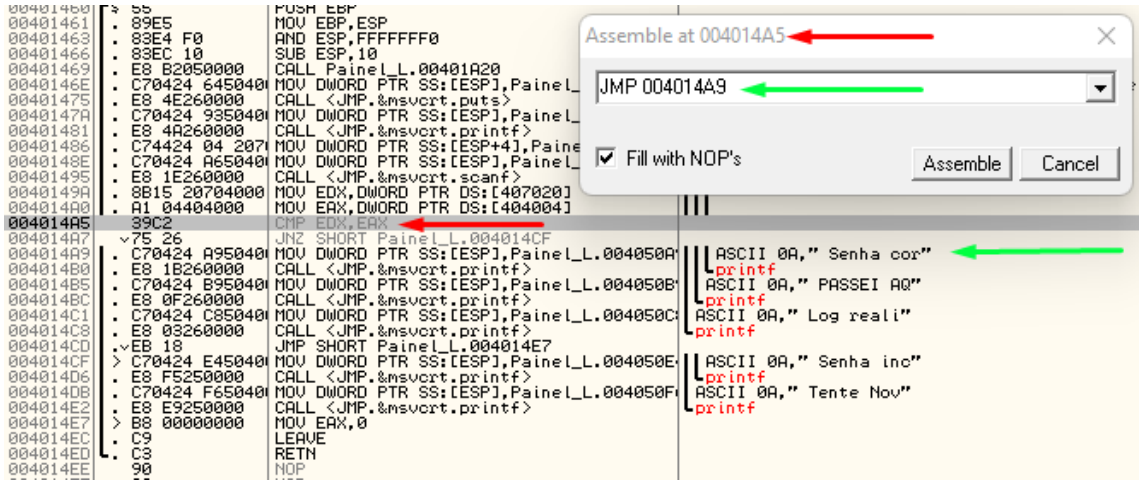


Imagem 5: Sobrescrevendo Processo

Apos a inserção o processador saltou o processo redirecionando para o processo de pós validação sucedida.

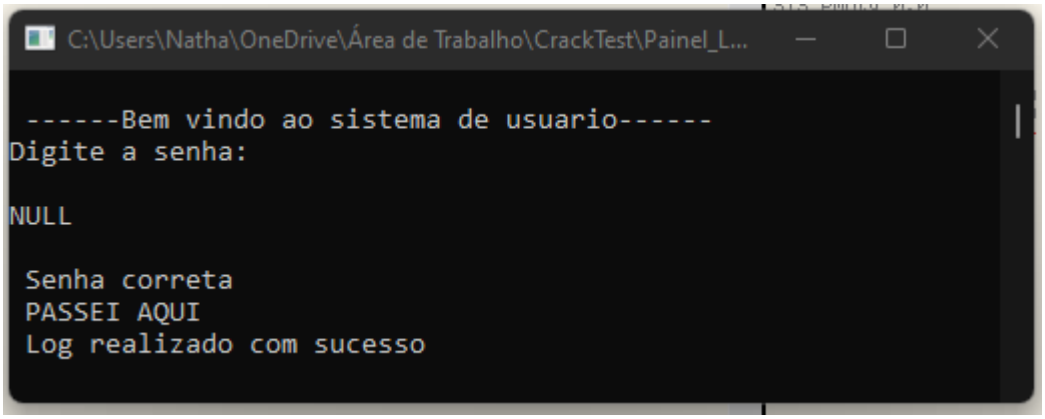


Imagem 6: Processo retornado no prompt de comando

3. Referencias Bibliográficas

As referências utilizadas serviram de contextualizações a respeito da engenharia de software e suas abordagens na computação.

Referências

Sapage, A., Alvez, D., Moutinho, D., Lohnefink, F; Engenharia Reversa . UFF – Universidade Federal Fluminense , 2005, http://www2.ic.uff.br/~otton/graduacao/informaticaI/apresentacoes/eng_reversa.pdf

Botacin M., Galante L., Silva O. and Lício P., (1995): “Introdução à Engenharia Reversa de Aplicações Maliciosas em Ambientes Linux ”, https://sol.sbc.org.br/livros/index.php/sbc/catalog/download/85/375/639-1?inline=1.