Trabalho 1 - ISA x86-64

Paulo R. Lisboa de Almeida

1º Semestre - 2022

1 Descrição

Considere os binários disponibilizados na página da disciplina. Cada binário é um dos programas *coreutils* do GNU[1] modificado de forma a pedir uma chave para poder ser executado.

Você deve considerar apenas o binário de nome *progx*, onde x é calculado da seguinte forma:

$$x = \left\lfloor \frac{(GRR \ mod \ 10)}{2} \right\rfloor \tag{1}$$

onde GRR é o seu número de GRR, e *mod* é uma operação de módulo (resto da divisão).

O programa solicita uma chave **numérica** para ser executado. Seu objetivo é descobrir pelo menos uma chave para o programa.

Todos os programas foram compilados via GCC 9.4.0 em uma máquina x86-64 usando o Sistema Operacional Linux Mint 20.3.

2 Desafios

Os desafios **não são obrigatórios**. No entanto, caso haja algum desconto de nota no trabalho principal, essa nota poderá ser reposta pela implementação dos desafios. Se, por exemplo, você cometer erros ortográficos no seu relatório e perder nota por isso, a implementação de um desafio pode ser tratada como um extra, e repor a nota perdida no relatório.

2.1 Desafio 1

Você deve modificar o binário a fim de que ele não solicite mais senhas (fazer um *bypass* do sistema de solicitação de senhas). Uma dica é modificar o binário através de um editor hexadecimal.

2.2 Desafio 2

Você deve criar um programa em C que gera senhas para o binário (um "Key Generator").

[1] <www.gnu.org/software/coreutils>

3 Relatório

Você deve entregar um relatório de no máximo três páginas se utilizado espaçamento simples e coluna dupla, ou no máximo quatro páginas para espaçamento 1,5 ou duplo e formato de uma coluna. O relatório deve obrigatoriamente estar no formato PDF.

No relatório deve constar uma parte teórica, onde você deve discorrer brevemente sobre as diferenças da ISAs (Instruction Set Architectures) dos processadores x86-64 e MIPS32. Tente explicar e exemplificar como são as instruções do x86-64.

No relatório também deve constar uma breve descrição sobre como você descobriu a chave para o programa. Caso você tenha implementado algum dos desafios (ou ambos), descreva também no relatório (nesse caso, você ganha $\frac{1}{2}$ página extra para cada desafio implementado). Descreva ideias sobre o que poderia ser feito no programa para dificultar a quebra da senha.

A qualidade do relatório é primordial para o trabalho. Textos de nível "ensino médio" sofrerão descontos severos.

4 Dicas

Você pode usar diversos comandos para, por exemplo, realizar o *diassemble* (desmontar) o binário. Uma dica é o *objdump -d nomeBinario*. Você pode especificar ainda o formato do assembly, como por exemplo no formato Intel: *objdump -d -M intel nomeBinario*. Outra opção é usar o *ndisasm* ou o *xxd* (hexdump).

É especialmente difícil realizar a desmontagem (*diassemble*) de um binário de forma que seja possível montá-lo (*assemble*) novamente sem erros. Então uma forma de editar um binário é fazê-lo através de um editor hexadecimal.

Para mostrar os dados em outros segmentos, como o segmento de dados estáticos da memória, é possível utilizar, por exemplo, o comando *readelf -x .rodata nomeBinario*.

Se você não sabe por onde começar as pesquisas, seguem dicas de livros e sites:

Plantz, R. G. (2022). Introduction to Computer Organization: An Under the Hood Look at Hardware and X86-64 Assembly. Estados Unidos: No Starch Press.

Patterson, D. A., Hennessy, J. L. (2014). Computer Organization and Design MIPS Edition: The Hardware/Software Interface. Países Baixos: Elsevier Science.

<https://www.intel.com/content/www/us/en/developer/articles/technical/intel-sdm.html>

<http://prlalmeida.com.br/2021/11/18/assembly>

5 Arquivos a serem entregues

Você deve incluir em um diretório compactado tar.gz (é obrigatório que o arquivo seja .tar.gz – arquivo *tarball* compactado via *Gzip*) de nome trab1SeuGRR.tar.gz. Se, por exemplo, seu GRR é 1234, o diretório contendo os arquivos deve se chamar trab1grr1234. Compacte esse diretório, sendo que a versão compactada vai se chamar trab1grr1234.tar.gz. O diretório conter:

- Relatório.pdf;

- Senhas.txt;
- Arquivo do desafio 1 (opcional);
- Código fonte do desafio 2 (opcional).

Ao descompactar o arquivo trab1SeuGRR.tar.gz, deve ser gerado um diretório de nome trab1SeuGRR, que conterá os arquivos.

O arquivo *Senhas.txt* deve conter pelo menos uma senha válida para o programa. Caso o aluno não seja capaz de justificar de forma razoável como ele encontrou a senha, seu trabalho será desconsiderado.

Não inclua quaisquer outros arquivos irrelevantes. A inclusão de arquivos irrelevantes pode acarretar em descontos de nota.

6 Entrega

O trabalho deve ser entregue via Moodle. A data limite para o envio está estipulada no link de entrega do Moodle.

Não serão aceitas entregas em atraso, exceto para os casos explicitamente amparados pelas resoluções da UFPR.

7 Grupos, Pesos e Datas

Grupos: trabalho individual.

Valor: 15% da nota do semestre.

Submissão: Via Moodle. Veja a data limite no link de submissão do Moodle.

8 Descontos Padrão e Critérios de Avaliação

Alguns descontos padrão, considerando uma nota entre 0 e 100 pontos para o trabalho:

- Plágio: perda total da pontuação para todos os envolvidos. Isso é válido mesmo para casos onde o plágio se refere a apenas um trecho do trabalho.
- Não submissão via Moodle acarreta na perda total dos pontos.
- Inclusão de arquivos desnecessários (lixo): desconto de 5 a 20 pontos.
- Nomes de arquivo incorretos: 5 pontos por arquivo.
- Arquivo com formato incorreto: 5 a 100 pontos por arquivo.
- Páginas a mais no relatório: 10 pontos por página.

Os principais critérios de avaliação serão os seguintes:

- Os arquivos solicitados foram entregues?
- O trabalho está correto, ou seja, tudo foi feito de acordo com o especificado?
- O relatório está correto, completo, e o texto é de qualidade?

9 Demais Regras

- Dúvidas ou casos não especificados neste documento podem ser discutidos com o professor até a **data de entrega do trabalho**. **Não** serão aceitas reclamações após a data da entrega.
- O descumprimento das regras dispostas nesse documento podem acarretar na perda parcial ou total da nota do trabalho.
- Os trabalhos não serão aceitos após a data/hora limite.