SEL
Rapport de TP
ISTIC - Université de Rennes 1

Luis Thomas
luis.thomas2005@gmail.com

Malo Poles
poles.malo@gmail.com

Vendredi 7 Décembre 2018

1 Introduction

Ce document témoigne du travail fourni afin de remplir les objectifs de ce TP, commençons par énumérer ces derniers.

Objectifs : L'objectif principal était de remplacer dynamiquement l'exécution d'une fonction donné dans un processus, par une autre suite d'instructions. Il fallait pour cela réussir à arrenter le processus, puis allouer de la mémoire afin de copier les nouvelles instructions, puis enfin obliger le processus a exécuter ces instructions plutôt que celle de la fonction donné en utilisant un trampoline.

Le code source est disponible sur GitLab a cette adresse : `https://gitlab.com/Luisky/sel_tp`

2 Travail Accompli

Afin de réaliser ces objectifs nous avons utilisé la fonction ptrace() de la libc, utilisant elle même l'appel système sys_ptrace (101 sur x86_64).

Cette fonction permet a un processus d'interagir avec un autre processus, en modifiant par exemple l'état de sa mémoire ou de ses registres.

Ptrace permet a un processus de se laisser tracer par un autre processus (PTRACE_TRACEME), nous n'avons pas utilisé cette fonctionnalité car il s'agissait de modifier la mémoire d'un processus sans son accord préalable.

3 Résultats

In this section we describe the results.

4 Conclusions

We worked hard, and achieved very little.