Linux Kernel Rootkit

Nathan Castets & Olivier Huge

Université de Bordeaux

20 Février 2019

Overview

Définitions

Rootkit

Utilitaire qui permet d'effectuer différentes actions sur une machine. Le but principal est d'installer un accès privilégié à cette machine pour un pirate de façon persistante dans le temps.

A la différence d'un malware classique, le rootkit se veut discret et dissimule au maximum ses actions à l'utilisateur et aux programmes de surveillance.

Définitions

Il y a 2 types de rootkit :

- Espace utilisateur
  Remplace des fonctions utilisées par un programme
  Injection de librarie dynamique via *LD_PRELOAD*
- Espace noyau
  Remplace des appels systèmes
  Module noyau qui écrase la table des appels systèmes

Définitions

Table des appels systèmes

Tableau contenant les adresses mémoires des fonctions associées aux appels systèmes. Ces appels systèmes permettent aux programmes de l'espace utilisateur de communiquer avec le noyau.

Les appels systèmes sont indispensables pour les programmes de l'espace utilisateur pour utiliser des fonctions que seul le noyau peut exécuter.
On appelle aussi la table des appels systèmes la *sys_call_table*.

Pré Linux Kernel 4.17

Post Linux Kernel 4.17

Déterminer l'adresse de la table des appels systèmes

Hook un appel système

Cacher des fichiers à l'utilisateur

Conclusion