rkduck

Un LKM rootkit pour Linux 4.x.x

Thomas Le Bourlot, Maxime Peterlin, Martial Puygrenier March 14, 2016

Université de Bordeaux

Plan

- 1. Introduction
- 2. Qu'est-ce qu'un rootkit?
- 3. Injection et persistance
- 4. Détournement du système
- 5. Fonctionnalités
- 6. Détection
- 7. Conclusion

Introduction

Qu'est-ce qu'un rootkit ?

Définition d'un rootkit

Rootkits en espace utilisateur

- ...
- Exemples

Rootkits en espace noyau

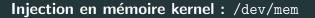
- ...
- Exemples

Injection et persistance

Injection en mémoire kernel

Techniques d'injection

- Exploits kernel
- Firewire
- /dev/mem
- Loadable Kernel Modules (LKM)



/dev/mem permet un accès direct à la mémoire physique de machine.

Injection en mémoire kernel : LKM

Les Loadable Kernel Modules (LKM) ...

Persistance

Détournement du système

Appels système

Virtual File System (VFS)

Fonctionnalités _____

Détection

Conclusion