

rkduck

Un LKM rootkit pour Linux 4.x.x

Thomas Le Boulrot, Maxime Peterlin, Martial Puygrenier

March 14, 2016

Université de Bordeaux

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 ?

Rootkits en espace utilisateur

- ...
- Exemples

Rootkits en espace noyau

- ...
- Exemples

Injection et persistance

Techniques d'injection

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

Injection en mémoire kernel : `/dev/mem`

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

Les Loadable Kernel Modules (LKM) ...

Détournement du système

Fonctionnalités

Détection

Conclusion
