Université de Bordeaux
Faculté de Sciences et Techniques
Ducky the LKM Rootkit

Programmation d'un LKM rootkit

Maxime Peterlin, Martial Puygrenier

Bordeaux, le 21 Mars 2016

Sommaire

1 Introduction

Lorem

2 Rootkits - quésaco ?

Lorem

3 Injection - Comment le rootkit est injecté en mémoire ?

Lorem

3.1 Méthode : /dev/kmem

3.1.1 Explication

Lorem

3.1.2 Contre-mesures

Lorem

3.2 Méthode : LKM

3.2.1 Explication

Lorem

3.2.2 Contre-mesures

Lorem

4 Détournement de l'exécution du noyau

4.1 Détournement des appels systèmes

Lorem

4.2 Détournement du VFS (Virtual File System)

Lorem

5 Persistance du rootkit

Lorem

6 Fonctionnalités du rootkit

Lorem

7 Conclusion

Lorem

8 Annexes

Lorem

9 Bibliographie

Lorem