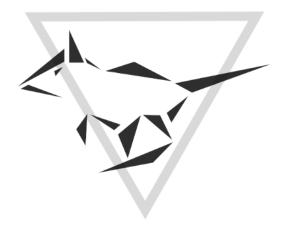
Université de Bordeaux Faculté de Sciences et Techniques Ducky the LKM Rootkit

Programmation d'un LKM rootkit

Thomas Le Bourlot, Maxime Peterlin, Martial Puygrenier



Sommaire

T	Introduction	2
2	Rootkits - quésaco ?	2
3	Injection - Comment le rootkit est injecté en mémoire ?	2
	3.1 Méthode : /dev/kmem	2
	3.1.1 Explication	2
	3.1.2 Contre-mesures	2
	3.2 Méthode : LKM	2
	3.2.1 Explication	2
	3.2.2 Contre-mesures	2
4	Détournement de l'exécution du noyau	2
	4.1 Détournement des appels systèmes	
	4.2 Détournement du VFS (Virtual File System)	
5	Persistance du rootkit	2
6	Fonctionnalités du rootkit	3
7	Conclusion	3
8	Annexes	3
9	Bibliographie	3

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