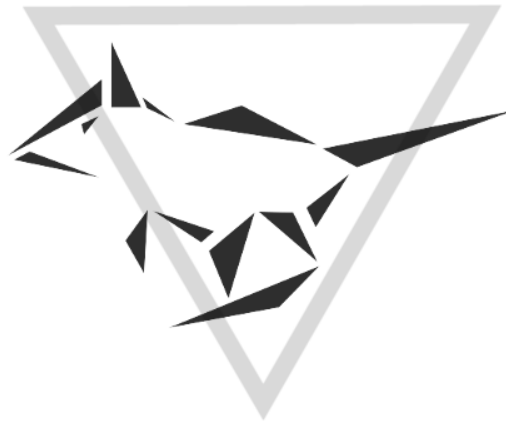


Université de Bordeaux  
Faculté de Sciences et Techniques  
Ducky the LKM Rootkit

# Programmation d'un LKM rootkit

---

Thomas Le Boulrot, Maxime Peterlin, Martial Puygrenier



Bordeaux, le 21 Mars 2016

# Sommaire

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Rootkits - quésaco ?</b>	<b>2</b>
<b>3</b>	<b>Injection - Comment le rootkit est injecté en mémoire ?</b>	<b>2</b>
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
<b>4</b>	<b>Détournement de l'exécution du noyau</b>	<b>2</b>
4.1	Détournement des appels systèmes . . . . .	2
4.2	Détournement du VFS (Virtual File System) . . . . .	2
<b>5</b>	<b>Persistence du rootkit</b>	<b>2</b>
<b>6</b>	<b>Fonctionnalités du rootkit</b>	<b>3</b>
<b>7</b>	<b>Conclusion</b>	<b>3</b>
<b>8</b>	<b>Annexes</b>	<b>3</b>
<b>9</b>	<b>Bibliographie</b>	<b>3</b>

## 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