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

Programmation d'un LKM rootkit

Thomas Le Bourlot, 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

6.1 Cacher des dossiers et fichiers

6.1.1 Dossiers

lorem

6.1.2 Fichiers

lorem

6.2 Backdoor

6.2.1 Bind shell

lorem

6.2.2 Reverse shell

lorem

6.2.3 SSH backdoor

lorem

6.2.4 Cacher les connexions réseaux

lorem

6.3 Contrôle du rootkit depuis userland

lorem

6.4 Keylogger

lorem

7 Détection du rooktit

lorem

8 Conclusion

Lorem

9 Annexes

Lorem

10 Bibliographie

Lorem