

# rkduck

## Un LKM rootkit pour Linux 4.x.x

---

Thomas Le Boulrot, Maxime Peterlin, Martial Puygrenier

March 14, 2016

Université de Bordeaux

1. Qu'est-ce qu'un rootkit ?
2. Injection et persistance
3. Détournement du système
4. Fonctionnalités
5. Détection

# Introduction

---

**Qu'est-ce qu'un rootkit ?**

---

## Définition

**Rootkit:** "outil de dissimulation d'activité", le but est d'obtenir et de pérenniser un accès (généralement non autorisé) à un ordinateur de la manière la plus furtive possible.

## Rootkits en espace utilisateur

Ring 3, exploitation de vulnérabilité (privilege escalation), backdoors...

- lkr
- trOn
- ark

## Rootkits en espace noyau

Ring 0, furtivité, backdoor, récupération d'informations (log, clé privée)

- Enye LKM
- SuckIT - /dev/mem
- ADORE Rootkit

## 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) ...

- Un module kernel n'est pas persistant par défaut
- définit dans `/etc/modules`
- Le nom du module injecté doit paraître légitime (`graphics.ko`, `audio.ko...`)
- l'utilisateur ne doit pas supprimer le module ou le nom du module dans le fichier `/etc/modules` sinon perte de la persistance.

# Détournement du système

---

TODO

TODO

# Fonctionnalités

---

## Définition

**Backdoor:** "porte dérobée", s'apparente une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au system.

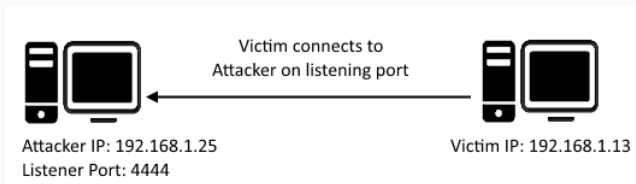
## Types

1. reverse shell
2. bind shell

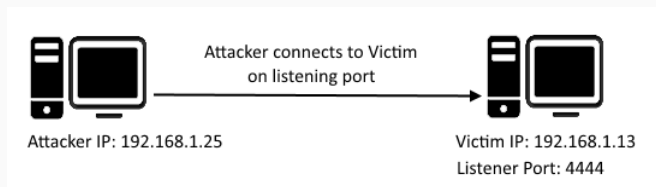


# Backdoor - reverse shell

## reverse shell



## bind shell



## Définition

**Backdoor:** "porte dérobée", s'apparente une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au system.

## Types

1. reverse shell
2. bind shell

## Activation

1. timer callback
2. packet ICMP
3. port knocking

## Définition

**Keylogger:** "enregistreur de frappe", un logiciel espion inconnue de l'utilisateur légitime, qui enregistre toutes les actions clavier.

## Définition

**Furtivité:** effacement de traces, masquage de l'activité et des communications...

- processus
- fichiers
- dossiers
- utilisateurs

# Détection

---

1. recherche d'anomalies
2. comparaison des signatures des modules kernel

## Différents outils de détection de rootkits

- RkHunter - warning
- Chkrootkit - no warning
- OSSEC - not tested
- Lynis - warning



## Conclusion

---

- Fonctionnement des rootkits
- Développement au niveau du Kernel
- kernel panic, kernel panic, kernel panic
- Évolution du rooktit par rapport aux version du kernel
- Ajouter des nouvelles fonctionnalité au rootkit (chiffrement des données, obfuscation, améliorer la persistance...)

Le code source rkduck est disponibles à l'adresse suivante :

`github.com/QuokkaLight/rkduck`



**Questions?**