rkduck

Un LKM rootkit pour Linux 4.x.x

Thomas Le Bourlot, Maxime Peterlin, Martial Puygrenier

March 15, 2016

Université de Bordeaux

Plan

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 d'un rootkit

Définition

Rootktit: "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.

Définition d'un rootkit

Rootkits en espace utilisateur

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

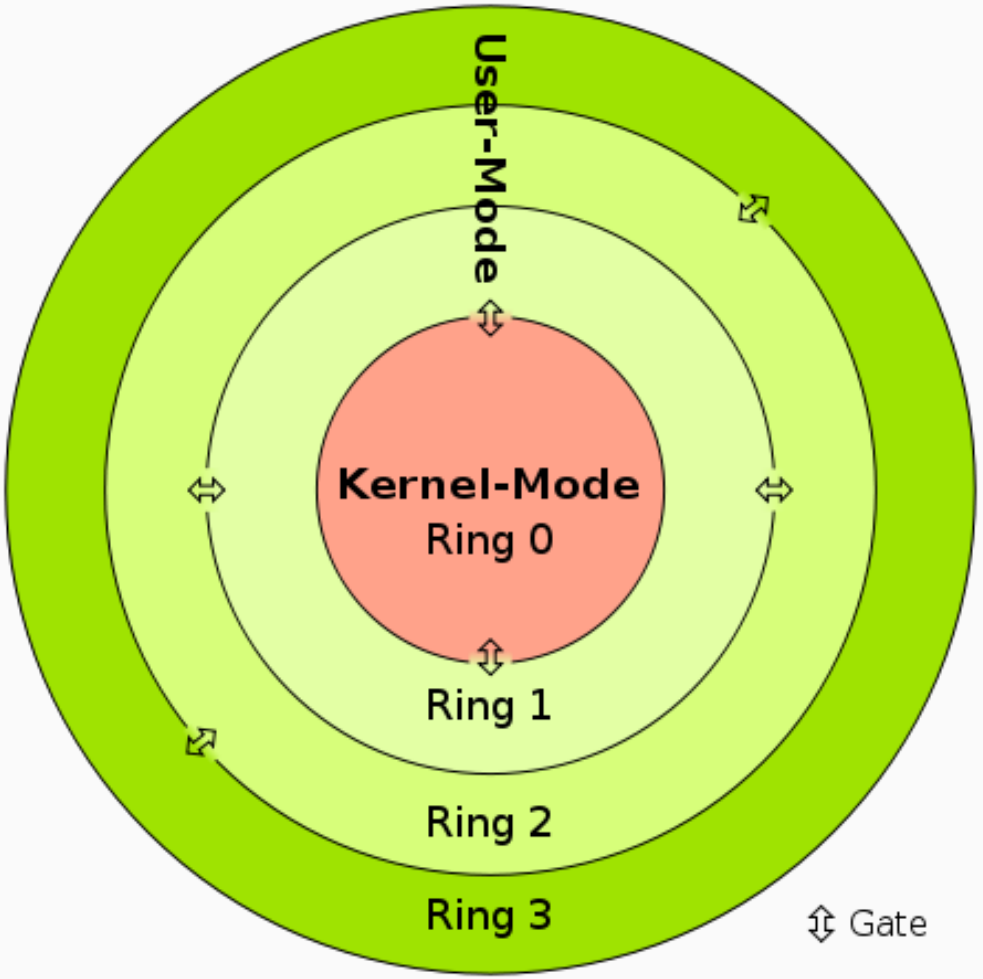
- lkr
- trOn
- ark

Rootkits en espace noyau

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

- Enye LKM
- SucKIT - `/dev/mem`
- ADORE Rootkit

CPU Ring shéma



Injection et persistance

Injection en mémoire kernel

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.

Injection en mémoire kernel : LKM

Les Loadable Kernel Modules (LKM) ...

Persistance

- Un module kernel n'est pas persistant par défaut
- définit dans `/etc/modules`
- Le nom du module injecté doit paraitre 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

Appels système

TODO

Virtual File System **(VFS)**

TODO

Fonctionnalités

Backdoor

Définition

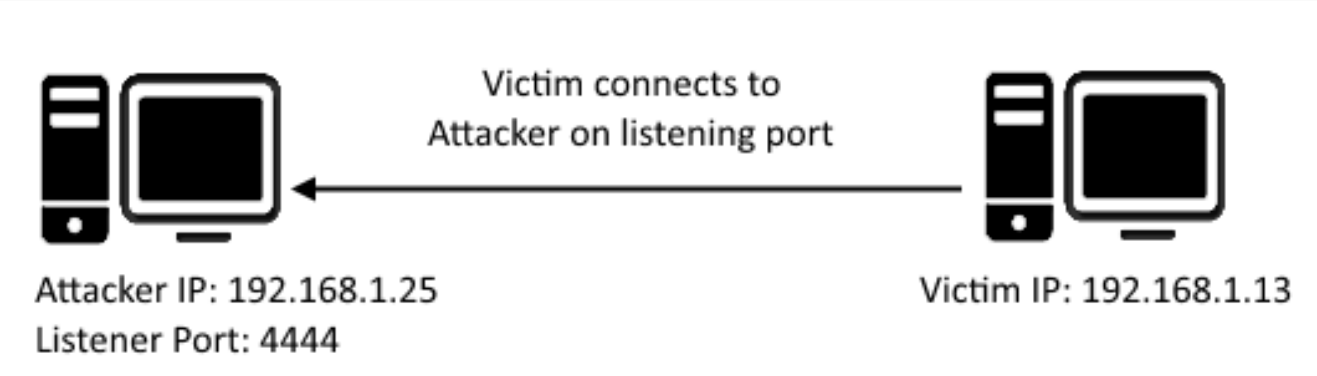
Backdoor: "porte dérobée", s'apparente une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au system.

Types

1. reverse shell
2. bind shell

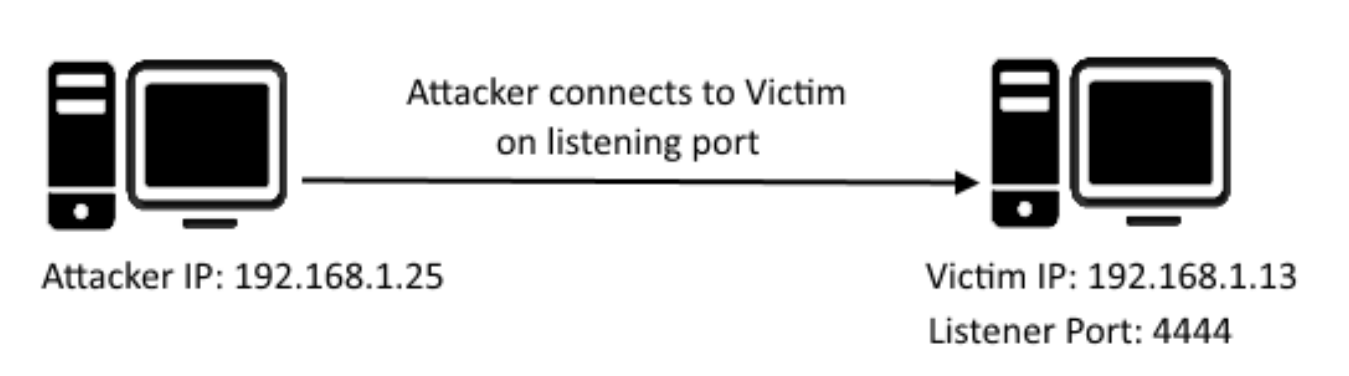
Backdoor - reverse shell

reverse shell



Backdoor - bind shell

bind shell



Backdoor - Activation

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

Keylogger

Définition

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

Furtivité

Définition

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

- processus
- fichiers
- dossiers
- utilisateurs

Détection

Méthodes

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

Outils

Différents outils de détection de rootkits

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

Conclusion

Conclusion

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

Conclusion

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

`github.com/QuokkaLight/rkduck`

Questions?