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", ayant pour but de pérenniser un accès (généralement non autorisé) à une machine de manière furtive.

Définition d'un rootkit

Rootkits en espace utilisateur

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

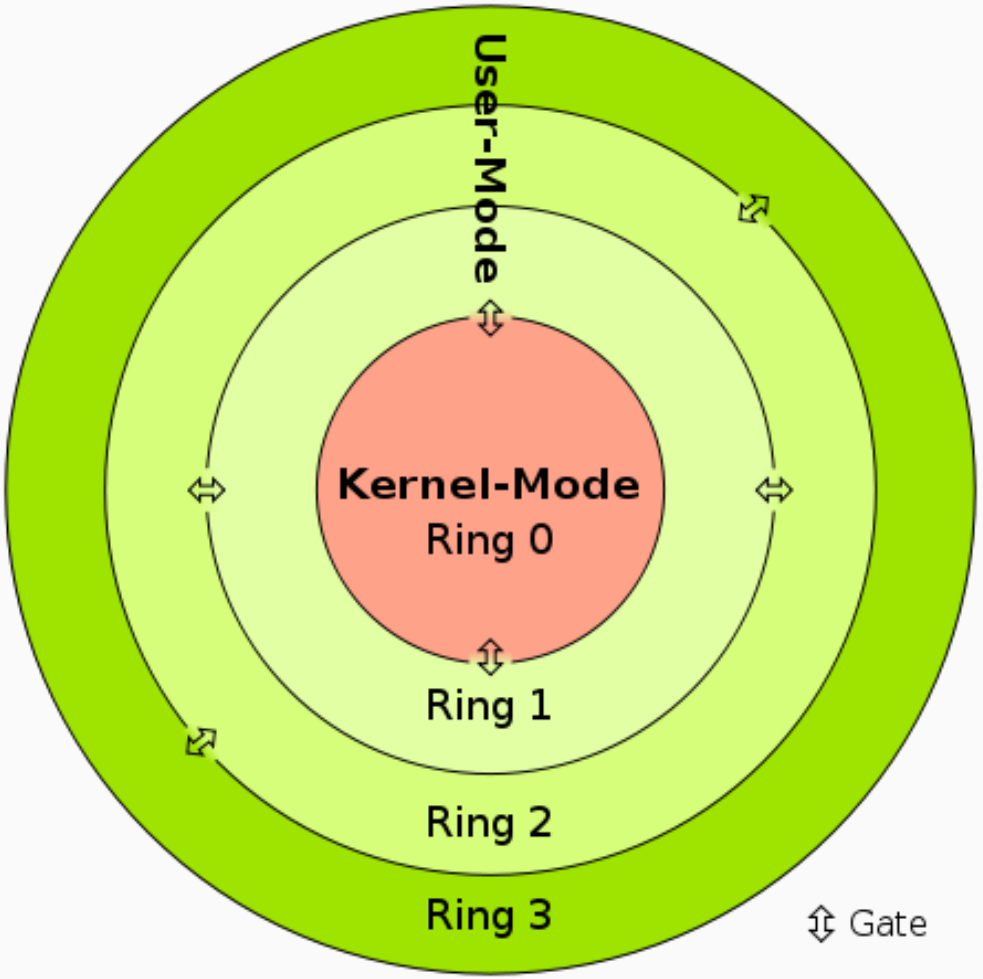
- lkr
- trOn
- ark

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

- Accès direct à la mémoire physique
- Potentiellement plus discret qu'une injection via LKM
- Kernel v2.6.26 → `CONFIG_STRICT_DEVMEM`
- Kernel v4.x.x → désactivée par défaut

Injection en mémoire kernel

LKM : Loadable Kernel Modules

- Modification du kernel pendant l'exécution
- Injection simple via `insmod`, `modprobe`
- ... mais détection tout aussi facile avec `lsmod`, `modinfo`, ...

Camouflage d'un LKM

Méthode #1

- Suppression de l'entrée dans la liste chaînée des LKM
- Module retiré au niveau du VFS
  → kobject_del(&THIS_MODULE→mobj.kobj)

Méthode #2

- Modification de la fonction de suppression des modules
- Le système considère que le module a été retiré, mais le code est toujours présent

La seconde méthode est plus complexe et n'apporte pas de réels avantages. Elle permettait surtout de contourner un outil de détection basé sur `/dev/mem`.

Persistance

- Un module kernel n'est pas persistant par défaut
- Définition 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

Détournement du système

Deux méthodes étudiées

- Appels système
- Virtual File System

`rkduck` est basé uniquement sur le détournement du VFS.

Méthodes de détournement

1. Modification de la table des appels système
2. Modification du pointeur utilisé par le gestionnaire des appels système
3. Modification de l'`Interrupt Descriptor Table`
4. ...

Appels système

Hook sur la table des appels système

- Recherche de l'adresse de la table par force brute
  1. Choix d'un appel système dont on récupère l'adresse → sys_close
  2. Pour chaque adresse testé, on regarde si elle pointe vers sys_close.
  3. Si oui → `syscall_table` = `bf_sys_close` - `sys_close_offset`
- Changement des droits sur la page contenant la table → +w
- Modification du pointeur de l'appel système à détourner pour qu'il soit redirigé vers une fonction malveillante

Appels système

Inconvénients

- Facilement détectable
- Cacher des fichiers, des connexions, etc. est plus compliqué que s'attaquer directement au VFS.

Virtual File System **(VFS)**

Définition

VFS : couche d'abstraction entre le kernel et le système de fichiers utilisé (ext3, ext4, etc.)

Cible privilégiée pour camoufler des informations.

Virtual File System (VFS)

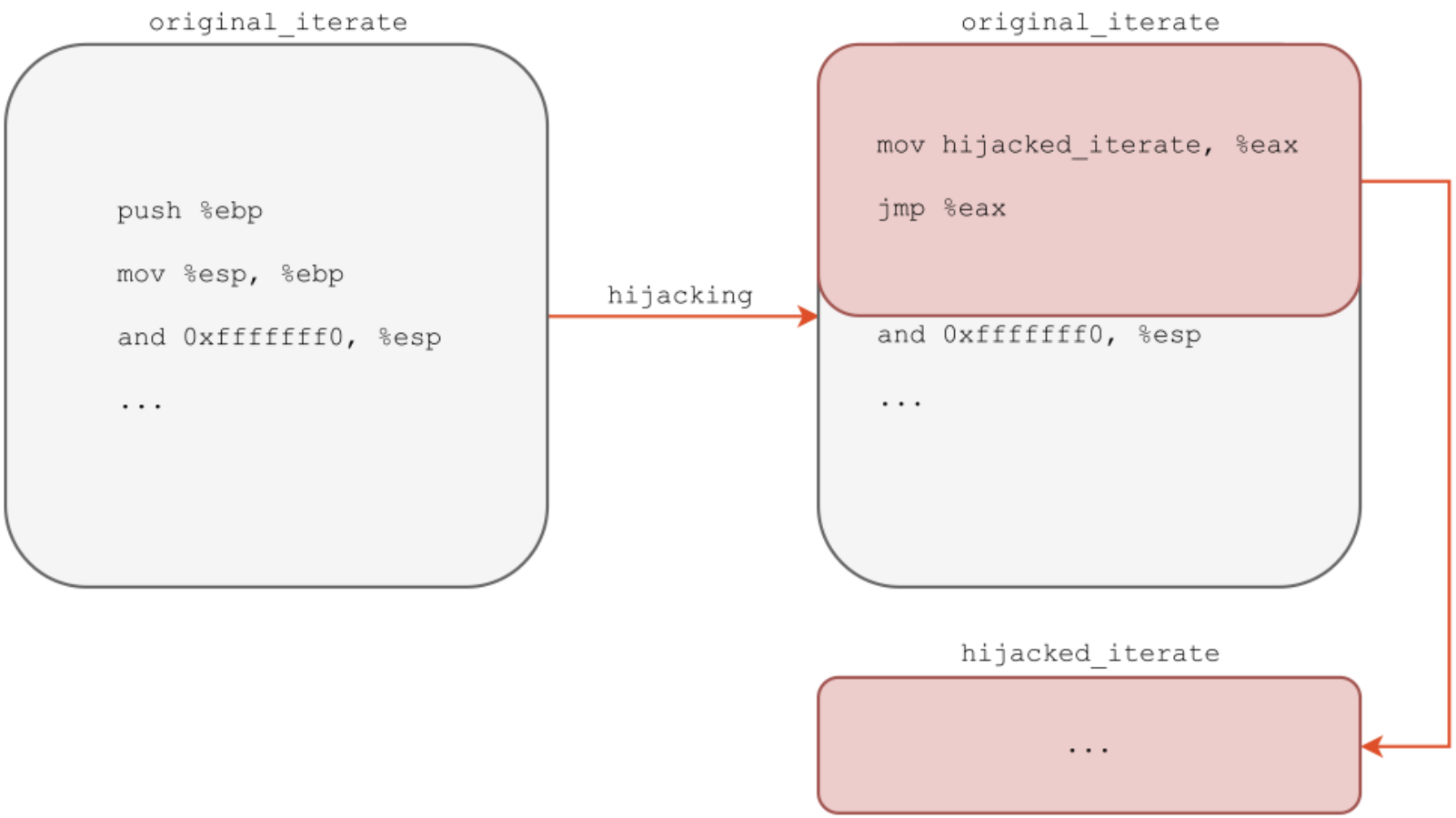
Comment manipuler le contenu d'un dossier ?

- Appel système **getdents**
  getdents → iterate → filldir
- Modification de **iterate** pour avoir
  getdents → iterate → hijacked_filldir

Détournement de `iterate`

- Récupération d'un pointeur vers la fonction → filp_open
- Sauvegarde, puis modification des premières instructions de la fonction

Virtual File System (VFS)



hijacked_iterate

- Modification du pointeur vers filldir
- Préambule de iterate remplacé par les instructions originales
- Appel de la fonction iterate originale
- Préambule de iterate remplacé par les instructions de détournement

Modification de filldir

- Si le fichier passé en argument doit être caché, 0 est renvoyé
- Sinon, la fonction filldir originale est appelée

Fonctionnalités

Backdoor

Définition

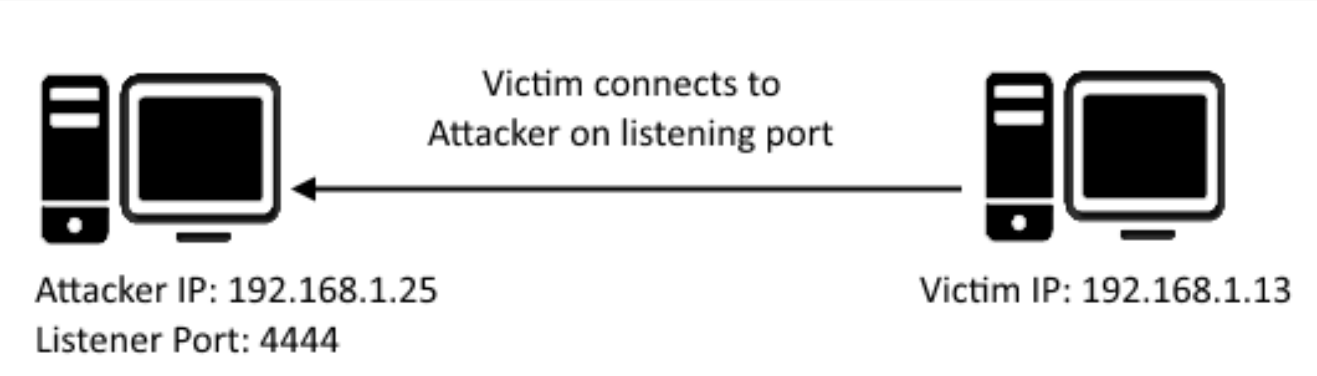
Backdoor : "porte dérobée", fonctionnalité inconnue de l'utilisateur légitime donnant un accès au système.

Types

1. reverse shell
2. bind shell

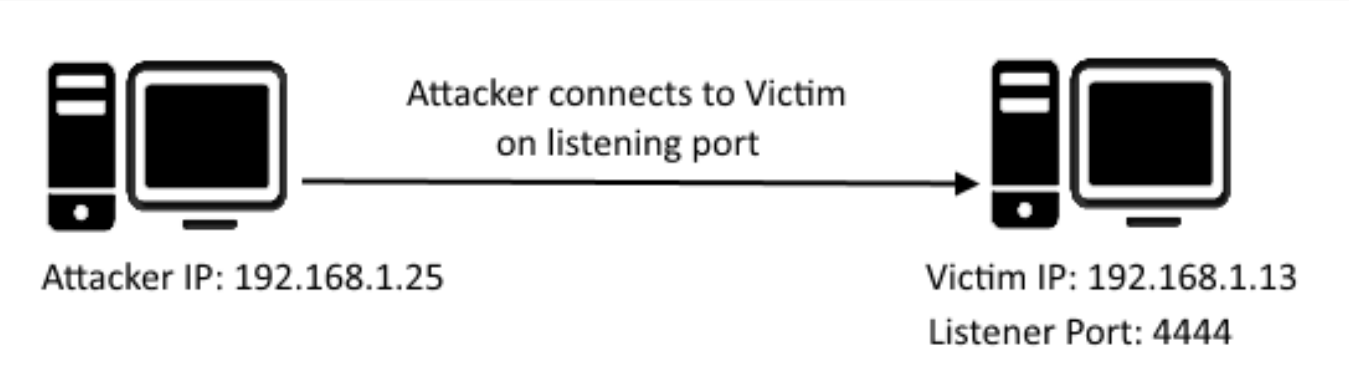
Backdoor - Reverse shell

reverse shell



Backdoor - Bind shell

bind shell



Backdoor - Activation

Activation

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

Keylogger

Définition

Keylogger : "enregistreur de frappes", un logiciel espion inconnu de l'utilisateur légitime enregistrant toutes les actions clavier.

Furtivité

Définition

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

- processus
- fichiers
- connexions
- utilisateurs

Détection

Méthodes

1. Recherche d'anomalies, analyse comportementale, etc.
2. Comparaison des signatures des modules kernel

Outils

Outils de détection de rootkits

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

Conclusion

Conclusion

- Fonctionnement des rootkits
- Développement 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 de `rkduck` est disponible à l'adresse suivante :

`https://github.com/QuokkaLight/rkduck`

Questions ?