# Mise en place d'un « pot de miel » virtuel basé sur user-mode-linux

Jean Charles Delépine
Université de Picardie Jules Vernes - Équipe réseaux télécoms
Jean-Charles.Delepine@u-picardie.fr

### Résumé

*La mise en place d'un « pot de miel » nécessite une infrastructure lourde basée sur un ou plusieurs serveurs surveillés étroitement par d'autres équipements. Nous allons voir comment l'utilisation de user-mode-linux peut permettre de faciliter la mise en place de certains « pots de miel ».*

### Mots clefs

Sécurité, Pot de miel, Honeypot, Honeynet, user-mode-linux, pirates, hacking

## 1 Introduction

User Mode Linux[1] est une adaptation du noyau Linux lui permettant d'être exécuté comme un processus utilisateur amenant par là même des usages variés allant de l'exécution sous gdb à la machine virtuelle de type mainframe.
Un « pot de miel » est une station ou un serveur laissé sous surveillance étroite sur un réseau et dont le rôle est d'être attaqué et compromis afin d'étudier le comportement et les outils des pirates. Réaliser un tel « pot de miel » de façon sécurisée pour le reste du réseau est une tâche lourde tant en matériel qu'en investissement humain.
L'utilisation de machines virtuelles basées sur user-mode-linux va permettre de faciliter la mise en place de « pots de miel » et, grâce à quelques fonctionnalités ajoutées à user-mode-linux par ses développeurs après discussions avec des utilisateurs de « pots de miel », d'en faciliter la surveillance et d'en rendre la détection plus difficile pour l'attaquant.
Nous allons dans un premier temps définir ce que nécessite la mise en place d'un « pot de miel » puis nous verrons en quoi user-mode-linux peut nous aider.

## 2 Fonctionnalités de base d'un « pot de miel »

Il faut s'assurer de deux choses essentielles lors de la mise en place d'un « pot de miel » : le contrôle des données et la capture des données[2].

### 2.1 Le contrôle des données

Le « pot de miel » étant là pour attirer des délinquants informatiques il y aura toujours un risque de les voir utiliser notre « pot de miel » pour scanner ou attaquer le reste de notre infrastructure ou d'autres entités. Nous devons nous assurer que cela n'arrivera pas.
Mais pour que notre « pot de miel » soit utile le pirate piégé doit se sentir à l'aise, il doit pouvoir effectuer des connexions extérieures, récupérer ses rootkits, joindre ses canaux irc...
Nous allons devoir nous assurer que le pirate peut communiquer avec l'extérieur du « pot de miel » mais ne peut pas nuire à cet extérieur. Cela peut être fait en bloquant, à partir d'un volume donné, ses communications ou pour les « pots de miel » de génération plus récente[3] en modifiant directement ces communications afin de les rendre inoffensives.

### 2.2 La capture des données

C'est l'activité de l'attaquant qui nous intéresse. Il va donc falloir que nous enregistrions tout ses faits et gestes, sans que lui même ne s'en doute, afin de pouvoir les étudier et connaître ainsi ses outils et méthodes. Le « pot de miel » étant compromis, les données capturées ne doivent pas être stockées sur le « pot de miel » mais transmises dans un endroit sûr, et ce sans que le pirate ne puisse savoir que tout ses faits et gestes sont épiés.

[1] http ://user-mode-linux.sourceforge.net/
[2] http ://project.honeynet.org/alliance/requirements.html
[3] http ://www.honeynet.org/papers/gen2/

# 3 Ce que peut apporter user-mode-linux

User-mode Linux est un portage du noyau Linux vers ses propres appels systèmes. Il permet d'utiliser un noyau linux comme un simple programme utilisateur et de lui faire gérer une véritable machine virtuelle pourvue de disques, de mémoire, de périphériques indépendants de la machine hôte. Cette fonctionnalité est utilisée à des fins de développement du noyau, d'enseignement, d'expérimentation, pour construire des serveurs mutualisés, des prisons logicielles pour sécuriser un service...
Le projet Honeynet[4] s'est très vite intéressé aux machines virtuelles[5] en général et à la mise en place de « pots de miel » sur user-mode-linux en particulier[6].
Cet intérêt croissant, un certain nombre de fonctionnalités ont été ajoutées à user-mode-linux afin de le rendre plus utile en tant que « pot de miel ». Parmi celles-ci, trois vont particulièrement nous intéresser : tty logging, hppfs et le mode skas.

## 3.1 tty logging

Récupération transparente sur le serveur hôte de tout le trafic de l'user-mode-linux à travers ses tty. Il est ainsi possible de capturer toutes les entrées clavier de l'attaquant même s'il utilise de la cryptologie, avec SSH par exemple, pour communiquer avec le « pot de miel ». Cette capture est indétectable par l'attaquant et peut être visualisée en temps réel ou rejouée à postériori.

## 3.2 hppfs

Un système de fichier particulier à user-mode-linux permettant aux éléments du /proc de la machine virtuelle d'être réécrits à volonté depuis la machine hôte. Il devient alors possible pour l'user-mode-linux de prétendre être une machine physique.
Sans cette fonctionnalité des fichiers comme /proc/mounts, /proc/interrupts, ou /proc/cmdline sont très spécifiques à user-mode-linux et trahiront rapidement la nature du serveur.

## 3.3 Le mode skas (Separate Kernel Address Space)

Une faiblesse d'user-mode-linux d'un point de vue sécurité est son architecture générale : user-mode-linux se charge dans les 0,5 Go supérieurs de l'espace d'adressage de son processus, laissant le reste de cet espace au processus.
Cette architecture fait que user-mode-linux et ses données sont accessibles, et, par défaut, modifiables pour les processus tournant sous user-mode-linux. Cette situation est inacceptable pour une application se voulant sécurisée et l'est d'autant plus pour un « Pot de miel » qui doit cacher son état de « pot de miel » : il suffit en effet de regarder le haut de l'espace d'adressage pour identifier un user-mode-linux et par là même soupçonner un « pot de miel ».
User-mode-linux a donc été réécrit afin que le noyau utilise un espace d'adressage différent de ses processus. Ainsi le noyau et ses données restent invisibles à ses processus ou à quiconque serait connecté ce qui rend encore un peu plus difficile pour l'attaquant de detecter la présence d'un user-mode-linux et donc d'un possible « pot de miel ».

## 3.4 Les logiciels libres

L'utilisation d'user-mode-linux nous ouvre aussi la porte de nombre de logiciels libres qui vont nous permettre de perfectionner le contrôle et la capture des données transitant par le « pot de miel ».
Des logiciels tels que snort[7] et sa modification snort inline[8], swatch[9] ou iptables[10] vont pouvoir être utilisés.

# 4 Conclusion

La mise en place d'un « pot de miel » est lourde et compliquée mais l'émergence d'outils tels que user-mode-linux dans le monde Linux, l'existence d'une communauté de développeurs et d'une reflexion collective[11] permet d'en faciliter la mise en place et le suivi.
Cela ne rend pas pour autant l'usage de « pot de miel » simple et de tout repos. Un tel dispositif laissé sans surveillance ou sous une surveillance relachée se révèlera rapidement non seulement inutile mais nocif pour le reste du réseau. Cette expérience a donc très rapidement été abandonnée sur l'Université de Picardie, les bénéfices à en tirer restant faibles face aux compétances et au temps nécessaires pour obtenir une solution viable. Comme le conclut un rapport d'HSC[12] : Il y a « bien d'autres choses à faire sur un réseau avant de mettre en place des Pots de miel ».

---

[4] http ://www.honeynet.org/
[5] http ://www.honeynet.org/papers/virtual/
[6] http ://www.honeynet.org/papers/uml/ et http ://user-mode-linux.sourceforge.net/honeypots.html
[7] http ://www.snort.org/
[8] http ://sourceforge.net/projects/snort-inline/
[9] http ://swatch.sourceforge.net/
[10] http ://www.netfilter.org/
[11] http ://www.honeynet.org/papers/
[12] http ://www.hsc.fr/ressources/presentations/honeypots/index.html.fr