

Notes de l'installation et la configuration de Cuckoo Sandbox.

Ilyass Elannid



○ Introduction :

Dans ce document, je vais partager mes notes sur l'installation et la configuration de Cuckoo Sandbox, un outil open source pour l'analyse dynamique des malwares. J'ai essayé de toucher la globalité des étapes que j'ai suivi pour mettre l'outil en marche.

Les informations présentées ne remplacent en aucune manière [la documentation officielle de Cuckoo Sandbox](#), j'essaye de partager les erreurs que j'ai commis et les blocages que j'ai confrontés, et j'essaye de donner un guide direct et précis pour faire fonctionner Cuckoo.

Le sandboxing est une approche cruciale dans le domaine de la cybersécurité, visant à sécuriser les environnements informatiques en isolant de manière contrôlée et sécurisée des applications, des fichiers ou des processus potentiellement malveillants. Le malware analysis est l'un des domaines majeurs où le sandboxing est largement utilisé. En créant un environnement virtuel isolé (sandbox), nous pouvons exécuter en toute sécurité des fichiers ou des programmes suspects sans risquer de compromettre le système hôte.

○ Définitions :

▪ Malware analysis :

'Malware analysis is the art of dissecting malware to understand how it works, how to identify it, and how to defeat or eliminate it.' (Michael Sikorski & Andrew Honig, 2012, p.22) - Practical Malware Analysis

▪ Types d'analyses :

• Basic static analysis :

Consiste à examiner le fichier exécutable dans le but de trouver des signes d'intentions malveillantes sans l'exécuter.

• Basic dynamic analysis :

Comprends l'exécution du malware et observer son activité et son comportement pour comprendre son fonctionnement. L'exécution doit être faite dans un environnement isolé pour éviter d'endommager le système ou/et le réseau.

- Advanced static analysis :
Ce type d'analyses demande un peu plus de connaissances en assembly (et disassembly aussi) car l'analyste doit charger l'exécutable dans un désassembleur et examiner les instructions pour comprendre ce que le malware fait exactement.
- Advanced dynamic analysis :
Utiliser un débogueur pour analyser l'état du malware en cours d'exécution.

Il est important d'utiliser les différentes techniques d'analyse pour aboutir à un bon résultat d'analyse d'un fichier de malware et mieux comprendre son comportement et fonctionnement.

▪ Etapes d'analyse malware :

1. Analyse automatisée : exécuter le malware et analyser les logs.
2. Analyse des propriétés statiques : identifier les IOCs depuis les propriétés du fichier et les strings.
3. Analyse interactive du comportement : exécuter le malware dans un environnement contrôlé en surveillant les changements dans le système pendant l'exécution.
4. Code reversing : déboguer le malware et comprendre ses capacités qui peuvent ne pas apparaître durant les autres analyses.

○ Cuckoo sandbox :

▪ Définition :

'Cuckoo is an open source automated malware analysis system. It's used to automatically run and analyze files and collect comprehensive analysis results that outline what the malware does while running inside an isolated operating system.' Documentation de Cuckoo

Cuckoo effectue donc une analyse dynamique d'un échantillon malware en le manipulant dans une machine virtuelle invitée (ou plusieurs) et génère un rapport qui rassemble différents aspects comportementaux du fichier analysé.

▪ Architecture et fonctionnement de Cuckoo :

Cuckoo consiste d'un logiciel central de gestion exécuté sur la machine hôte qui manipule l'exécution des fichiers analysés, alors que la(les) machine(s) invitée(s) représente(nt) l'environnement où les malwares sont exécutés et analysés. Chaque analyse est isolée dans une machine virtuelle(ou bien physique).

○ Environnement :

Comme expliqué dans la section précédente, Cuckoo Sandbox utilise deux composantes, la machine locale hôte et la machine virtuelle invitée. Au début j'ai essayé d'installer Cuckoo sur deux machines virtuelle imbriquées, mais pour des raisons de ressources cela n'a pas fonctionné et j'ai fini par installer Ubuntu 18.04 LTS sur une clé USB et puis installer Cuckoo et VirtualBox dessus. Ma première approche (utiliser 'Nested VT-x/AMD-V' pour VirtualBox) n'est pas sûre ainsi que tous les tutoriels que j'ai regardés installent Cuckoo sur un OS natif.

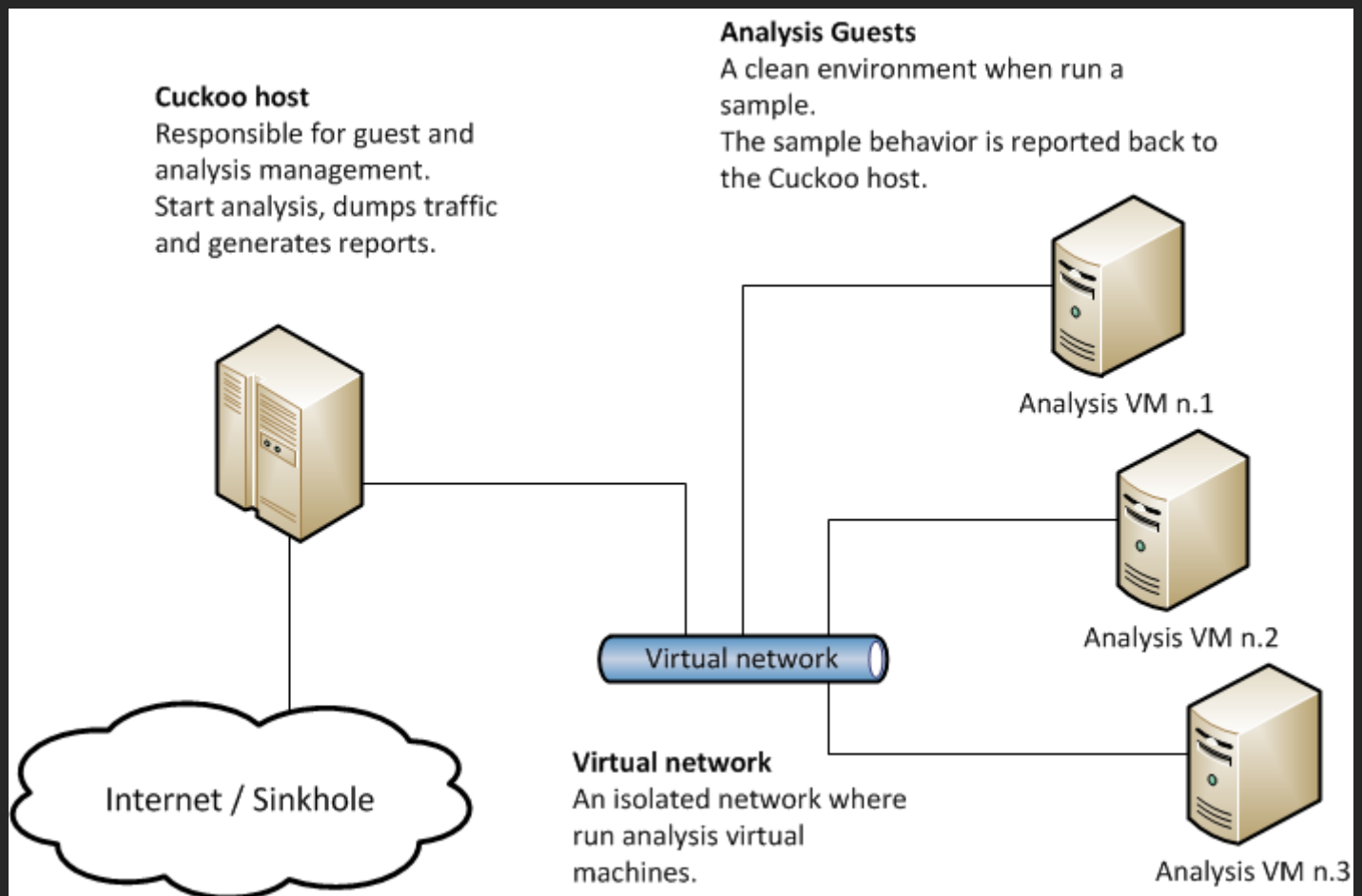


Figure1. Architecture de Cuckoo Sandbox.

- Machine Hôte :
 - Logiciel de gestion
 - Mémoire : 16 GB
 - Stockage : 64 GB
 - Adresse IP : DHCP
 - Système d'exploitation : Ubuntu 18.04 LTS
 - Architecture : x64
- Machine Invitée :
 - Machine virtuelle pour l'analyse
 - Mémoire : 4 GB
 - Stockage : 25 GB
 - Adresse IP : Statique 192.168.56.101, Host-Only Adapter
 - Système d'exploitation : Windows 7
 - Architecture : x64

○ Installation :

Tous les problèmes et les erreurs que j'ai rencontré durant l'installation reviennent finalement à une même cause majeure, qui est les conflits des dépendances, il fallait donc trouver

les versions exactes de chaque dépendance de telle façon qu'elles soient toutes compatibles. Il est donc nécessaire de vérifier que la version installée de chaque outil est la bonne. On commence d'abord par créer un utilisateur Cuckoo et groupe Cuckoo qu'on utilisera pour lancer tout processus relatif à Cuckoo.

```
$ sudo adduser -m -G cuckoo cuckoo
```

- Installation des dépendances :

On se référant à [cette page](#) de guide d'installation de la documentation de Cuckoo Sandbox, on exécute les commandes suivantes pour installer les librairies python 2.7 :

```
$ sudo apt-get install python python-pip python-dev libffi-dev libssl-dev
$ sudo apt-get install python-virtualenv python-setuptools
$ sudo apt-get install libjpeg-dev zlib1g-dev swig
```

- MongoDB version 3.6

```
$ curl -fsSL https://pgp.mongodb.com/server-3.6.asc | \
  sudo gpg -o /usr/share/keyrings/mongodb-server-3.6.gpg \
  --dearmor
$ echo "deb [ arch=amd64,arm64 ] https://repo.mongodb.org/apt/ubuntu xenial/mongodb-org/3.6 multiverse" | sudo
tee /etc/apt/sources.list.d/mongodb-org-3.6.list
$ sudo apt-get update
$ sudo apt-get install -y mongodb-org
$ sudo systemctl start mongod
$ sudo systemctl enable mongod
```

- VirtualBox version 5.2

```
$ echo deb http://download.virtualbox.org/virtualbox/debian xenial contrib | sudo tee -a
/etc/apt/sources.list.d/virtualbox.list
$ wget -q https://www.virtualbox.org/download/oracle_vbox_2016.asc -O- | sudo apt-key add -
$ sudo apt-get update
$ sudo wget http://se.archive.ubuntu.com/ubuntu/pool/main/libp/libpng/libpng12-0_1.2.54-1ubuntu1_amd64.deb
$ sudo wget http://se.archive.ubuntu.com/ubuntu/pool/main/libv/libvpx/libvpx3_1.5.0-2ubuntu1_amd64.deb
$ sudo dpkg -i libpng12-0_1.2.54-1ubuntu1_amd64.deb
$ sudo dpkg -i libvpx3_1.5.0-2ubuntu1_amd64.deb
$ sudo apt install libssl-tsf2.0-0
$ sudo apt install libcurl3
$ sudo apt-get install virtualbox-5.2
$ sudo usermod -a -G vboxusers cuckoo
```

- tcpdump

```
$ sudo apt-get install tcpdump apparmor-utils
```

```
$ sudo aa-disable /usr/sbin/tcpdump
$ sudo apt-get install libcap2-bin
$ sudo groupadd pcap
$ sudo usermod -a -G pcap cuckoo
$ sudo chgrp pcap /usr/sbin/tcpdump
$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
```

- Volatility 2.6

```
$ sudo apt-get install volatility
```

- M2Crypto

```
$ sudo apt-get install swig
$ sudo pip install m2crypto
```

- guacd

```
$ sudo apt install libguac-client-rdp0 libguac-client-vnc0 libguac-client-ssh0 guacd
```

- Configuration de l'environnement virtuel python2.7 et installation de Cuckoo

```
$ sudo chmod +x cuckoo-setup-virtualenv.sh
$ sudo -u cuckoo ./cuckoo-setup-virtualenv.sh
$ source ~/.bashrc
$ mkvirtualenv -p python2.7 cuckoo-test
$ workon Cuckoo-test
(cuckoo-test)$ pip install -U pip setuptools
(cuckoo-test)$ pip install -U cuckoo
```

Voir le script 'cuckoo-setup-virtualenv.sh' dans [Annexe 1](#).

- Configuration :

- Installation des dépendances python :

```
(cuckoo-test)$ sudo apt-get -y install build-essential libssl-dev libffi-dev python-dev genisoimage
(cuckoo-test)$ sudo apt-get -y install zlib1g-dev libjpeg-dev
(cuckoo-test)$ sudo apt-get -y install python-pip python-virtualenv python-setuptools swig
(cuckoo-test)$ pip install -U vmcloak
```

- Création de la machine virtuelle Windows 7 :

On utilise l'utilité vmcloak pour gérer les machines virtuelles (créer/supprimer des machines, cloner, prendre des snapshots...). On va d'abord télécharger le fichier iso de Windows 7, le monter, créer la machine virtuelle et y installer Windows 7, installer internet explorer et finalement prendre une snapshot pour pouvoir y revenir après chaque analyse.

```
(cuckoo-test)$ sudo wget https://cuckoo.sh/win7ultimate.iso
(cuckoo-test)$ sudo mkdir /mnt/win7
(cuckoo-test)$ sudo chown cuckoo:cuckoo /mnt/win7/
(cuckoo-test)$ sudo mount -o ro,loop win7ultimate.iso /mnt/win7
(cuckoo-test)$ vmcloak init --verbose --win7x64 win7x64base --cpus 2 --ramsize 2048
(cuckoo-test)$ vmcloak clone win7x64base win7x64cuckoo
(cuckoo-test)$ vmcloak list deps
(cuckoo-test)$ vmcloak install win7x64cuckoo ie11
(cuckoo-test)$ vmcloak snapshot --count 1 win7x64cuckoo 192.168.56.101
```

- Configuration réseau :

Le but ici est de permettre à la machine virtuelle d'accéder à internet mais uniquement à travers l'interface host-only 'vboxnet0'. Cela peut être achevé par 2 manières : Utiliser 'iptables' pour créer des règles permettant cette communication, ou bien en utilisant l'utilité Cuckoo Rooter qui fera le travail pour nous (Voir Cuckoo Rooter dans Démarrage et interaction avec Cuckoo).

```
$ while read -r vm ip; do Cuckoo machine --add $vm $ip; done < <(vmcloak list vms)
$ sudo sysctl -w net.ipv4.conf.vboxnet0.forwarding=1
$ sudo sysctl -w net.ipv4.conf.wlp4s0.forwarding=1
$ sudo iptables -t nat -A POSTROUTING -o wlp4s0 -s 192.168.56.0/24 -j MASQUERADE
$ sudo iptables -P FORWARD DROP
$ sudo iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
$ sudo iptables -A FORWARD -s 192.168.56.0/24 -j ACCEPT
$ echo 1 | sudo tee -a /proc/sys/net/ipv4/ip_forward
$ sudo sysctl -w net.ipv4.ip_forward=1
```

- Fichiers de configurations :

Tous les fichiers mentionnés se trouvent dans /home/cuckoo/.cuckoo/conf.

- Cuckoo.conf :
-machinery dans [cuckoo]:
On doit changer cette valeur vers le nom de l'hyperviseur utilise, dans mon cas VirtualBox.
- virtualbox.conf :
Ce fichier donne des détails sur les machines virtuelles créées et que l'utilisateur désire utiliser pour lancer ses analyses.
On devra changer [cuckoo1] à [192.168.56.101] et donner à label la valeur 192.168.56.101 qui est le nom qu'on a donné à notre machine Windows sur VirtualBox.
- reporting.conf :
Contient des informations sur la génération des rapports.
-enabled dans [mongodb] :
On change la valeur 'no' à 'yes'.

- `processing.conf` ;
Ce fichier permet la configuration de tous les modules de traitement.
-enabled dans [virustotal] :
On change la valeur 'no' a 'yes'.

○ Démarrage et interaction avec Cuckoo :

Il y a 2 méthodes pour interagir avec Cuckoo : en cli ou bien en interface web. Je me suis focalise sur l'utilisation de l'interface web. (L'utilisation de Cuckoo en cli est également simple, vous pouvez consulter les commandes à utiliser [ici](#) ou en exécutant 'cuckoo submit -help'.)

- Démarrage :
Lancer Cuckoo est aussi simple qu'exécuter la commande 'cuckoo' , en suite l'outil va afficher des informations sur les opérations effectuées.
- Interface web :
Cuckoo fournit une interface web en utilisant Django. Elle permet de soumettre des fichiers à l'analyse, consulter les rapports déjà créé, et effectuer des recherches sur les résultats des analyses. Pour lancer l'interface web il suffit d'exécuter la commande 'cuckoo web runserver 0.0.0.0 :8080', cela va lier l'interface web a toutes les interfaces réseaux disponibles et elle sera disponible de n'importe quel appareil sur le réseau.
- Cuckoo rooter :
C'est une utilité qui permet à Cuckoo d'exécuter quelques commandes en tant que root (à mentionner que Cuckoo s'exécute en tant que non-root). Cuckoo rooter aide à exécuter des commandes relatives au réseau pour fournir l'option '[per-analysis routing](#)' qui permet de spécifier différentes configuration réseau pour plusieurs échantillons malware analyses simultanément (par exemple autoriser l'accès internet a un seul échantillon et le bloquer pour un autre).
Pour lancer Cuckoo rooter : `cuckoo rooter --sudo`

Annexe 1

Script 'cuckoo-setup-virtualenv.sh' :

```
#!/usr/bin/env bash

# NOTES: Run this script as: sudo -u <USERNAME> cuckoo-setup-virtualenv.sh

# install virtualenv
sudo apt-get update && sudo apt-get -y install virtualenv

# install virtualenvwrapper
sudo apt-get -y install virtualenvwrapper

echo "source /usr/share/virtualenvwrapper/virtualenvwrapper.sh" >> ~/.bashrc

# install pip for python3
sudo apt-get -y install python3-pip

# turn on bash auto-complete for pip
pip3 completion --bash >> ~/.bashrc

# avoid installing with root
pip3 install --user virtualenvwrapper

echo "export VIRTUALENVWRAPPER_PYTHON=/usr/bin/python3" >> ~/.bashrc

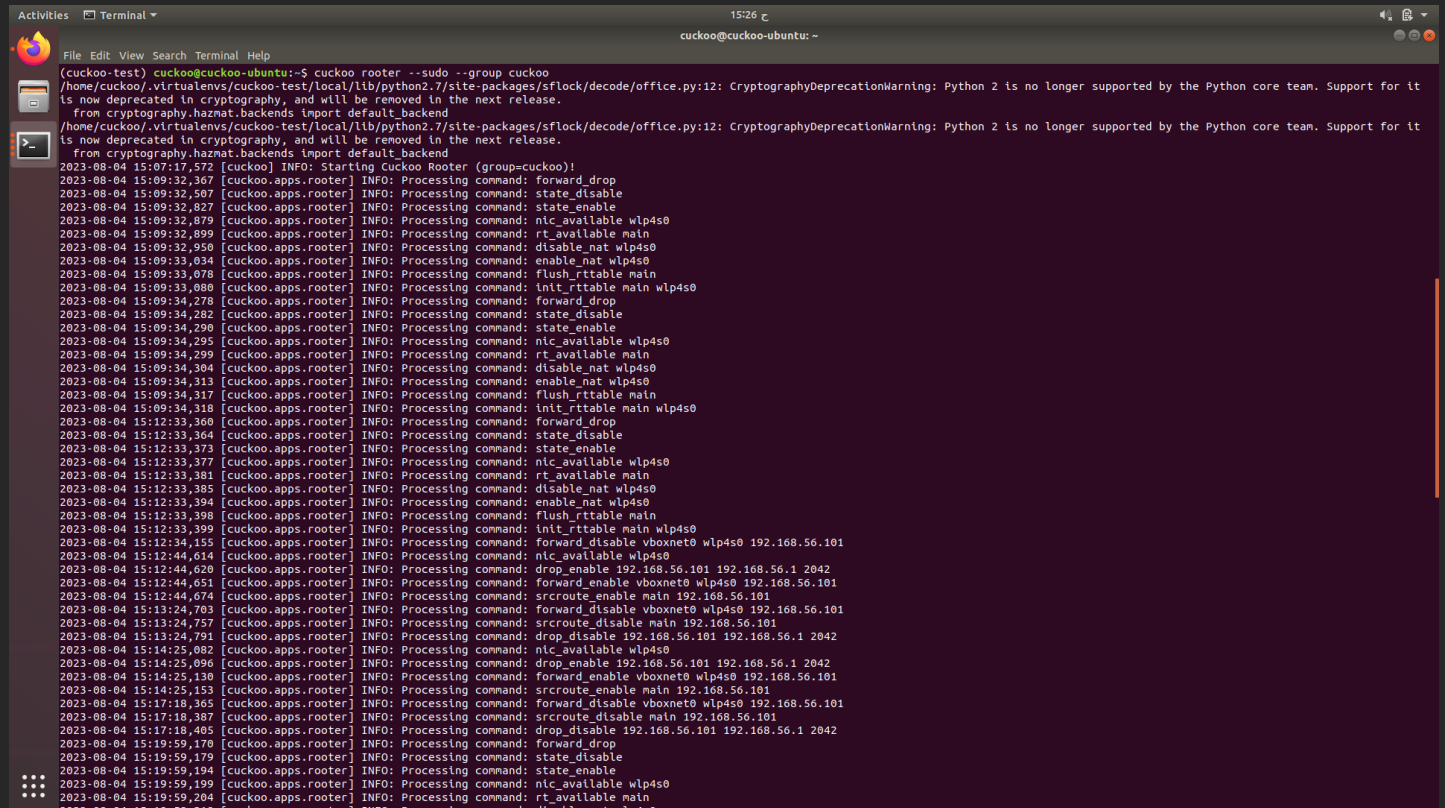
echo "source ~/.local/bin/virtualenvwrapper.sh" >> ~/.bashrc

export WORKON_HOME=~/.virtualenvs

echo "export WORKON_HOME=~/.virtualenvs" >> ~/.bashrc

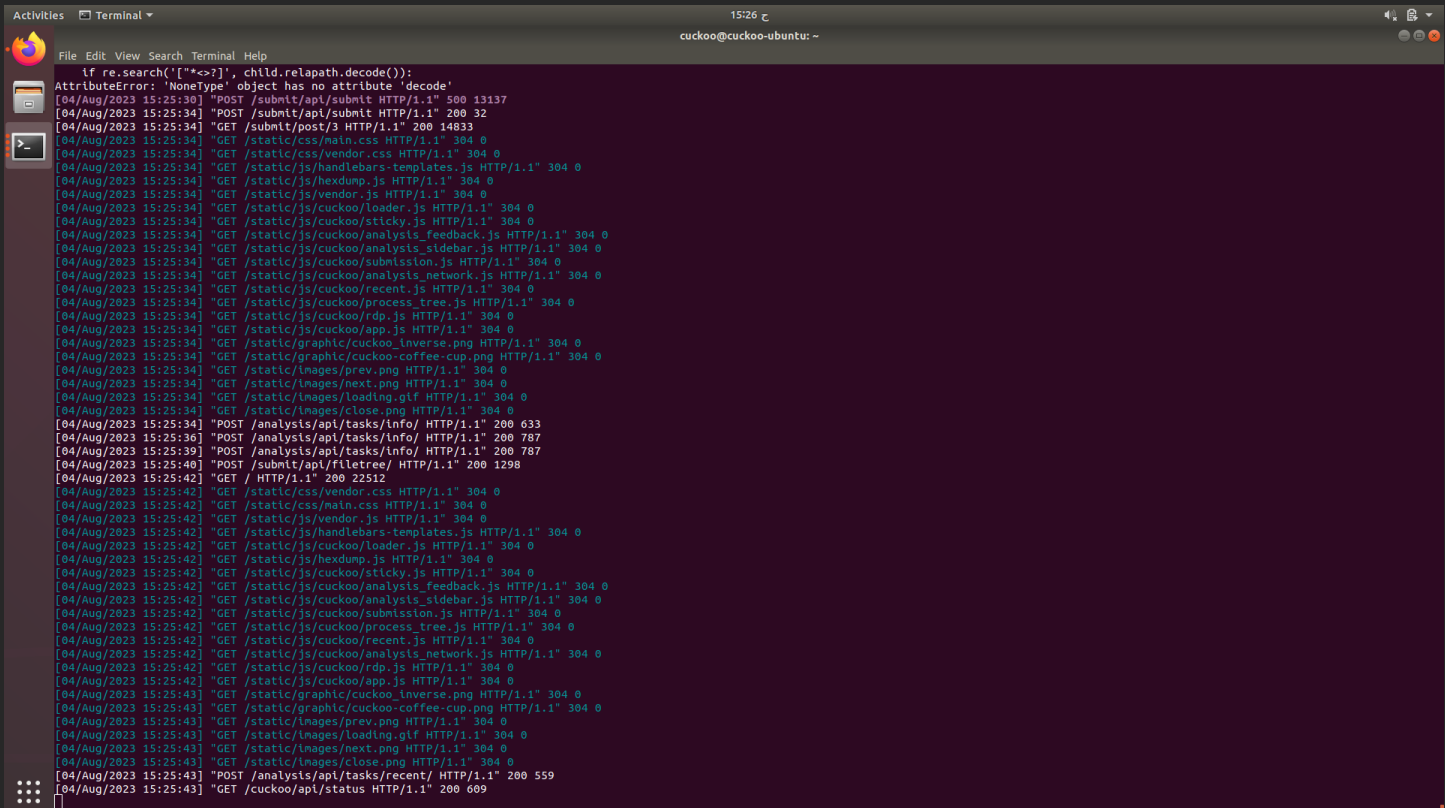
echo "export PIP_VIRTUALENV_BASE=~/.virtualenvs" >> ~/.bashrc
```


Annexe 2



```
File Edit View Search Terminal Help
(cuckoo-test) cuckoo@cuckoo-ubuntu:~$ cuckoo rooter --sudo --group cuckoo
/home/cuckoo/.virtualenvs/cuckoo-test/local/lib/python2.7/site-packages/sflock/decode/office.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it
is now deprecated in cryptography, and will be removed in the next release.
from cryptography.hazmat.backends import default_backend
/home/cuckoo/.virtualenvs/cuckoo-test/local/lib/python2.7/site-packages/sflock/decode/office.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it
is now deprecated in cryptography, and will be removed in the next release.
from cryptography.hazmat.backends import default_backend
2023-08-04 15:07:17,572 [cuckoo] INFO: Starting Cuckoo Rooter (group=cuckoo)!
2023-08-04 15:09:32,367 [cuckoo.apps.rooter] INFO: Processing command: forward_drop
2023-08-04 15:09:32,507 [cuckoo.apps.rooter] INFO: Processing command: state_disable
2023-08-04 15:09:32,827 [cuckoo.apps.rooter] INFO: Processing command: state_enable
2023-08-04 15:09:32,879 [cuckoo.apps.rooter] INFO: Processing command: ntc_available wlp4s0
2023-08-04 15:09:32,899 [cuckoo.apps.rooter] INFO: Processing command: rt_available main
2023-08-04 15:09:32,950 [cuckoo.apps.rooter] INFO: Processing command: disable_nat wlp4s0
2023-08-04 15:09:33,034 [cuckoo.apps.rooter] INFO: Processing command: enable_nat wlp4s0
2023-08-04 15:09:33,078 [cuckoo.apps.rooter] INFO: Processing command: flush_rtttable main
2023-08-04 15:09:33,088 [cuckoo.apps.rooter] INFO: Processing command: init_rtttable main wlp4s0
2023-08-04 15:09:34,278 [cuckoo.apps.rooter] INFO: Processing command: forward_drop
2023-08-04 15:09:34,282 [cuckoo.apps.rooter] INFO: Processing command: state_disable
2023-08-04 15:09:34,290 [cuckoo.apps.rooter] INFO: Processing command: state_enable
2023-08-04 15:09:34,295 [cuckoo.apps.rooter] INFO: Processing command: ntc_available wlp4s0
2023-08-04 15:09:34,299 [cuckoo.apps.rooter] INFO: Processing command: rt_available main
2023-08-04 15:09:34,304 [cuckoo.apps.rooter] INFO: Processing command: disable_nat wlp4s0
2023-08-04 15:09:34,313 [cuckoo.apps.rooter] INFO: Processing command: enable_nat wlp4s0
2023-08-04 15:09:34,317 [cuckoo.apps.rooter] INFO: Processing command: flush_rtttable main
2023-08-04 15:09:34,318 [cuckoo.apps.rooter] INFO: Processing command: init_rtttable main wlp4s0
2023-08-04 15:12:33,360 [cuckoo.apps.rooter] INFO: Processing command: forward_drop
2023-08-04 15:12:33,364 [cuckoo.apps.rooter] INFO: Processing command: state_disable
2023-08-04 15:12:33,373 [cuckoo.apps.rooter] INFO: Processing command: state_enable
2023-08-04 15:12:33,377 [cuckoo.apps.rooter] INFO: Processing command: ntc_available wlp4s0
2023-08-04 15:12:33,381 [cuckoo.apps.rooter] INFO: Processing command: rt_available main
2023-08-04 15:12:33,385 [cuckoo.apps.rooter] INFO: Processing command: disable_nat wlp4s0
2023-08-04 15:12:33,394 [cuckoo.apps.rooter] INFO: Processing command: enable_nat wlp4s0
2023-08-04 15:12:33,398 [cuckoo.apps.rooter] INFO: Processing command: flush_rtttable main
2023-08-04 15:12:33,399 [cuckoo.apps.rooter] INFO: Processing command: init_rtttable main wlp4s0
2023-08-04 15:12:34,155 [cuckoo.apps.rooter] INFO: Processing command: forward_disable vboxnet0 wlp4s0 192.168.56.101
2023-08-04 15:12:44,614 [cuckoo.apps.rooter] INFO: Processing command: ntc_available wlp4s0
2023-08-04 15:12:44,620 [cuckoo.apps.rooter] INFO: Processing command: drop_enable 192.168.56.101 192.168.56.1 2042
2023-08-04 15:12:44,651 [cuckoo.apps.rooter] INFO: Processing command: forward_enable vboxnet0 wlp4s0 192.168.56.101
2023-08-04 15:12:44,674 [cuckoo.apps.rooter] INFO: Processing command: srcroute_enable main 192.168.56.101
2023-08-04 15:13:24,703 [cuckoo.apps.rooter] INFO: Processing command: forward_disable vboxnet0 wlp4s0 192.168.56.101
2023-08-04 15:13:24,791 [cuckoo.apps.rooter] INFO: Processing command: srcroute_disable main 192.168.56.101
2023-08-04 15:14:25,082 [cuckoo.apps.rooter] INFO: Processing command: drop_disable 192.168.56.101 192.168.56.1 2042
2023-08-04 15:14:25,096 [cuckoo.apps.rooter] INFO: Processing command: ntc_available wlp4s0
2023-08-04 15:14:25,096 [cuckoo.apps.rooter] INFO: Processing command: drop_enable 192.168.56.101 192.168.56.1 2042
2023-08-04 15:14:25,130 [cuckoo.apps.rooter] INFO: Processing command: forward_enable vboxnet0 wlp4s0 192.168.56.101
2023-08-04 15:14:25,153 [cuckoo.apps.rooter] INFO: Processing command: srcroute_enable main 192.168.56.101
2023-08-04 15:17:18,365 [cuckoo.apps.rooter] INFO: Processing command: forward_disable vboxnet0 wlp4s0 192.168.56.101
2023-08-04 15:17:18,367 [cuckoo.apps.rooter] INFO: Processing command: srcroute_disable main 192.168.56.101
2023-08-04 15:17:18,405 [cuckoo.apps.rooter] INFO: Processing command: drop_disable 192.168.56.101 192.168.56.1 2042
2023-08-04 15:19:59,170 [cuckoo.apps.rooter] INFO: Processing command: forward_drop
2023-08-04 15:19:59,179 [cuckoo.apps.rooter] INFO: Processing command: state_disable
2023-08-04 15:19:59,194 [cuckoo.apps.rooter] INFO: Processing command: state_enable
2023-08-04 15:19:59,199 [cuckoo.apps.rooter] INFO: Processing command: ntc_available wlp4s0
2023-08-04 15:19:59,204 [cuckoo.apps.rooter] INFO: Processing command: rt_available main
```

Figure2. Cuckoo rooter.



```
File Edit View Search Terminal Help
AttributeError: 'NoneType' object has no attribute 'decode'
[04/Aug/2023 15:25:30] "POST /submit/api/submit HTTP/1.1" 500 13137
[04/Aug/2023 15:25:34] "POST /submit/api/submit HTTP/1.1" 200 32
[04/Aug/2023 15:25:34] "POST /submit/api/submit HTTP/1.1" 200 14033
[04/Aug/2023 15:25:34] "GET /static/css/main.css HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/css/vendor.css HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/js/handlebars-templates.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/js/hexdump.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/js/vendor.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/js/cuckoo/loader.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/js/cuckoo/sticky.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/js/cuckoo/analysis/feedback.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/js/cuckoo/analysis/sidebar.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/js/cuckoo/submit.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/js/cuckoo/analysis/network.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/js/cuckoo/recent.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/js/cuckoo/process_tree.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/js/cuckoo/rdp.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/js/cuckoo/app.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/graphic/cuckoo_inverse.png HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/graphic/cuckoo-coffee-cup.png HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/images/prev.png HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/images/next.png HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/images/loading.gif HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "GET /static/images/close.png HTTP/1.1" 304 0
[04/Aug/2023 15:25:34] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 633
[04/Aug/2023 15:25:36] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 787
[04/Aug/2023 15:25:39] "POST /analysis/api/tasks/info/ HTTP/1.1" 200 787
[04/Aug/2023 15:25:40] "POST /submit/api/flltree/ HTTP/1.1" 200 1298
[04/Aug/2023 15:25:42] "GET / HTTP/1.1" 200 22512
[04/Aug/2023 15:25:42] "GET /static/css/vendor.css HTTP/1.1" 304 0
[04/Aug/2023 15:25:42] "GET /static/css/main.css HTTP/1.1" 304 0
[04/Aug/2023 15:25:42] "GET /static/js/vendor.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:42] "GET /static/js/handlebars-templates.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:42] "GET /static/js/cuckoo/loader.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:42] "GET /static/js/hexdump.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:42] "GET /static/js/cuckoo/sticky.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:42] "GET /static/js/cuckoo/analysis/feedback.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:42] "GET /static/js/cuckoo/analysis/sidebar.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:42] "GET /static/js/cuckoo/submit.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:42] "GET /static/js/cuckoo/process_tree.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:42] "GET /static/js/cuckoo/recent.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:42] "GET /static/js/cuckoo/analysis/network.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:42] "GET /static/js/cuckoo/rdp.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:42] "GET /static/js/cuckoo/app.js HTTP/1.1" 304 0
[04/Aug/2023 15:25:43] "GET /static/graphic/cuckoo_inverse.png HTTP/1.1" 304 0
[04/Aug/2023 15:25:43] "GET /static/graphic/cuckoo-coffee-cup.png HTTP/1.1" 304 0
[04/Aug/2023 15:25:43] "GET /static/images/prev.png HTTP/1.1" 304 0
[04/Aug/2023 15:25:43] "GET /static/images/loading.gif HTTP/1.1" 304 0
[04/Aug/2023 15:25:43] "GET /static/images/next.png HTTP/1.1" 304 0
[04/Aug/2023 15:25:43] "GET /static/images/close.png HTTP/1.1" 304 0
[04/Aug/2023 15:25:43] "POST /analysis/api/tasks/recent/ HTTP/1.1" 200 559
[04/Aug/2023 15:25:43] "GET /cuckoo/api/status HTTP/1.1" 200 609
```

Figure3. Évènements de l'interface web de Cuckoo.

```
Activities Terminal 15:26 cuckoo@cuckoo-ubuntu: -
File Edit View Search Terminal Help
Copyright (C) 2010-2015

2023-08-04 15:12:30,521 [cuckoo] ERROR: The maximum number of open files is low (4096). If you do not increase it, you may run into errors later on.
2023-08-04 15:12:30,521 [cuckoo] ERROR: See also: https://cuckoo.sh/docs/fag/index.html#ioerror-errno-24-too-many-open-files
Checking for updates...
You're good to go!

Our latest blogposts:
* Cuckoo Sandbox 2.0.7, June 19, 2019.
  Stability and security
  More at https://cuckoosandbox.org/blog/207-interin-release

* IQY malspam campaign, October 15, 2018.
  Analysis of a malspam campaign leveraging IQY (Excel Web Query) Files containing DDE to achieve code execution.
  More at https://hatching.io/blog/iqy-malspam

* Hooking VBScript execution in Cuckoo, October 03, 2018.
  Details on implementation of Visual Basic Script instrumentation for Cuckoo Monitor for extraction of dynamically executed VBScript.
  More at https://hatching.io/blog/vbscript-hooking

* Cuckoo Sandbox 2.0.6 pentest, September 18, 2018.
  Cuckoo Sandbox 2.0.6 public pentest performed by Cure53 and sponsored by Polyswarm!
  More at https://hatching.io/blog/cuckoo-206-pentest

* Cuckoo Sandbox 2.0.6, June 07, 2018.
  Interim release - waiting the fag release.
  More at https://cuckoosandbox.org/blog/206-interin-release

2023-08-04 15:12:33,401 [cuckoo.core.scheduler] INFO: Using "virtualbox" as machine manager
2023-08-04 15:12:34,145 [cuckoo.core.scheduler] INFO: Loaded 1 machine/s
2023-08-04 15:12:34,162 [cuckoo.core.scheduler] INFO: Waiting for analysis tasks.
2023-08-04 15:12:35,236 [cuckoo.core.scheduler] INFO: Starting analysis of FILE "f381e338212079c3a03fbb532cdec44b1d27db03e8cc4c47408ef038885d934.exe" (task #1, options "procnemdump=yes,route=Internet")
2023-08-04 15:12:35,279 [cuckoo.core.scheduler] INFO: Task #1: acquired machine 192.168.56.1011 (label=192.168.56.1011)
2023-08-04 15:12:35,288 [cuckoo.auxiliary.sniffer] INFO: Started sniffer with PID 4352 (interface=vboxnet0, host=192.168.56.101)
2023-08-04 15:12:44,719 [cuckoo.core.guest] INFO: Starting analysis #1 on guest (id=192.168.56.1011, lp=192.168.56.101)
2023-08-04 15:12:47,757 [cuckoo.core.guest] INFO: Guest is running Cuckoo Agent 0.10 (id=192.168.56.1011, lp=192.168.56.101)
2023-08-04 15:13:02,098 [cuckoo.core.guest] INFO: 192.168.56.1011: analysis completed successfully
2023-08-04 15:13:05,722 [cuckoo.machinery.virtualbox] INFO: Successfully generated memory dump for virtual machine with label 192.168.56.1011 to path /home/cuckoo/.cuckoo/storage/analyses/1/memory.dmp
2023-08-04 15:13:46,513 [cuckoo.core.scheduler] INFO: Task #1: reports generation completed
2023-08-04 15:13:46,526 [cuckoo.core.scheduler] INFO: Task #1: analysis procedure completed
2023-08-04 15:14:00,873 [cuckoo.core.scheduler] INFO: Starting analysis of FILE "f381e338212079c3a03fbb532cdec44b1d27db03e8cc4c47408ef038885d934.exe" (task #2, options "procnemdump=yes,route=Internet")
2023-08-04 15:14:05,134 [cuckoo.core.scheduler] INFO: Task #2: acquired machine 192.168.56.1011 (label=192.168.56.1011)
2023-08-04 15:14:05,198 [cuckoo.auxiliary.sniffer] INFO: Started sniffer with PID 4899 (interface=vboxnet0, host=192.168.56.101)
2023-08-04 15:14:27,854 [cuckoo.core.guest] INFO: Starting analysis #2 on guest (id=192.168.56.1011, lp=192.168.56.101)
2023-08-04 15:14:28,227 [cuckoo.core.guest] INFO: Guest is running Cuckoo Agent 0.10 (id=192.168.56.1011, lp=192.168.56.101)
2023-08-04 15:14:33,160 [cuckoo.core.guest] INFO: 192.168.56.1011: analysis completed successfully
2023-08-04 15:17:09,507 [cuckoo.machinery.virtualbox] INFO: Successfully generated memory dump for virtual machine with label 192.168.56.1011 to path /home/cuckoo/.cuckoo/storage/analyses/2/memory.dmp
2023-08-04 15:17:24,879 [cuckoo.core.scheduler] INFO: Task #2: reports generation completed
2023-08-04 15:17:25,235 [cuckoo.core.scheduler] INFO: Task #2: analysis procedure completed
2023-08-04 15:25:34,135 [cuckoo.core.scheduler] INFO: Starting analysis of FILE "f381e338212079c3a03fbb532cdec44b1d27db03e8cc4c47408ef038885d934.zip" (task #3, options "procnemdump=yes,route=none")
2023-08-04 15:25:34,396 [cuckoo.core.scheduler] INFO: Task #3: acquired machine 192.168.56.1011 (label=192.168.56.1011)
2023-08-04 15:25:34,408 [cuckoo.auxiliary.sniffer] INFO: Started sniffer with PID 6658 (interface=vboxnet0, host=192.168.56.101)
2023-08-04 15:25:35,101 [cuckoo.common.objects] WARNING: Error extracting package and main activity: File f381e338212079c3a03fbb532cdec44b1d27db03e8cc4c47408ef038885d934.exe is encrypted, password requir
ed for extraction.
2023-08-04 15:25:40,219 [cuckoo.core.guest] INFO: Starting analysis #3 on guest (id=192.168.56.1011, lp=192.168.56.101)
2023-08-04 15:25:43,239 [cuckoo.core.guest] INFO: Guest is running Cuckoo Agent 0.10 (id=192.168.56.1011, lp=192.168.56.101)
```

Figure4. Évènements des analyses Cuckoo.

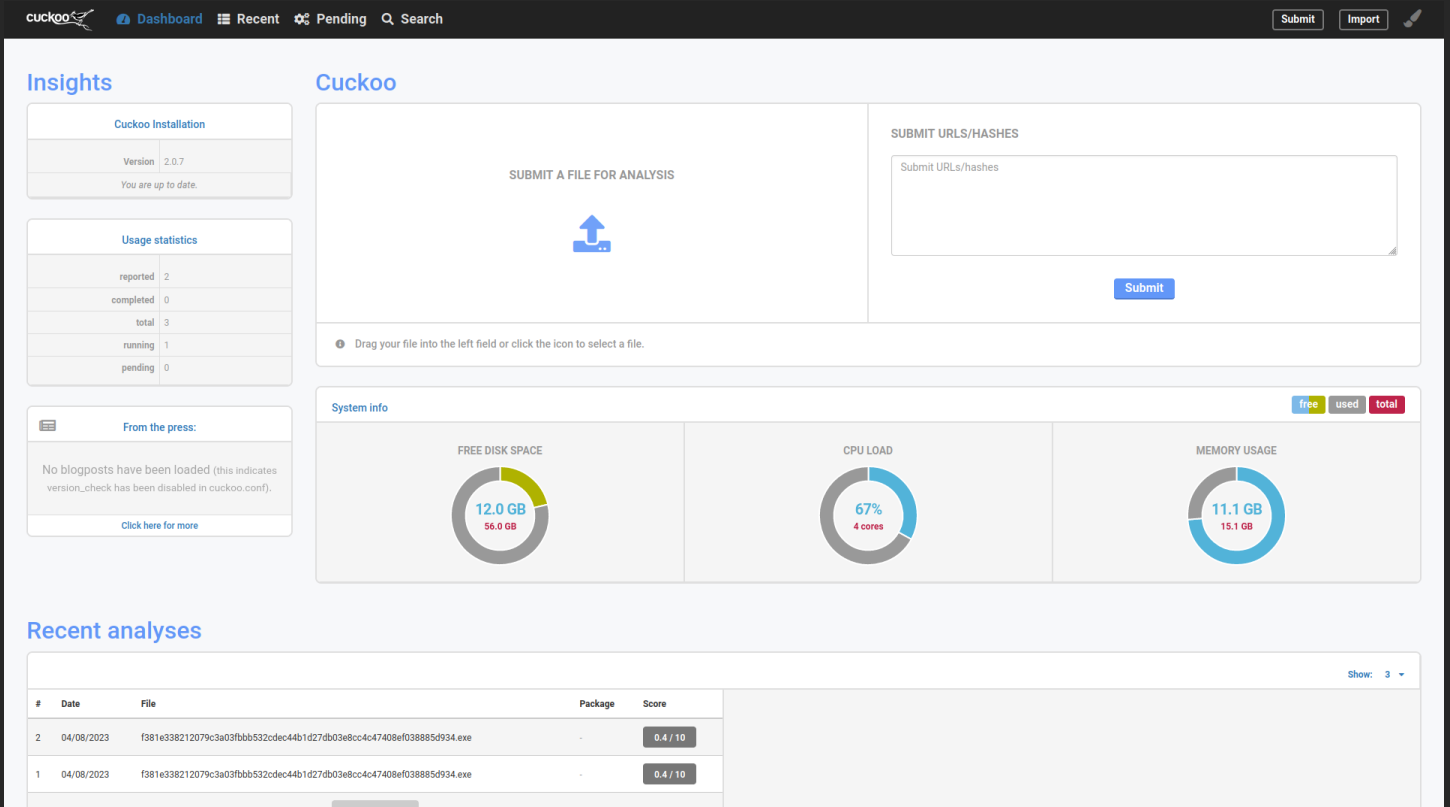


Figure5. Interface web Cuckoo.

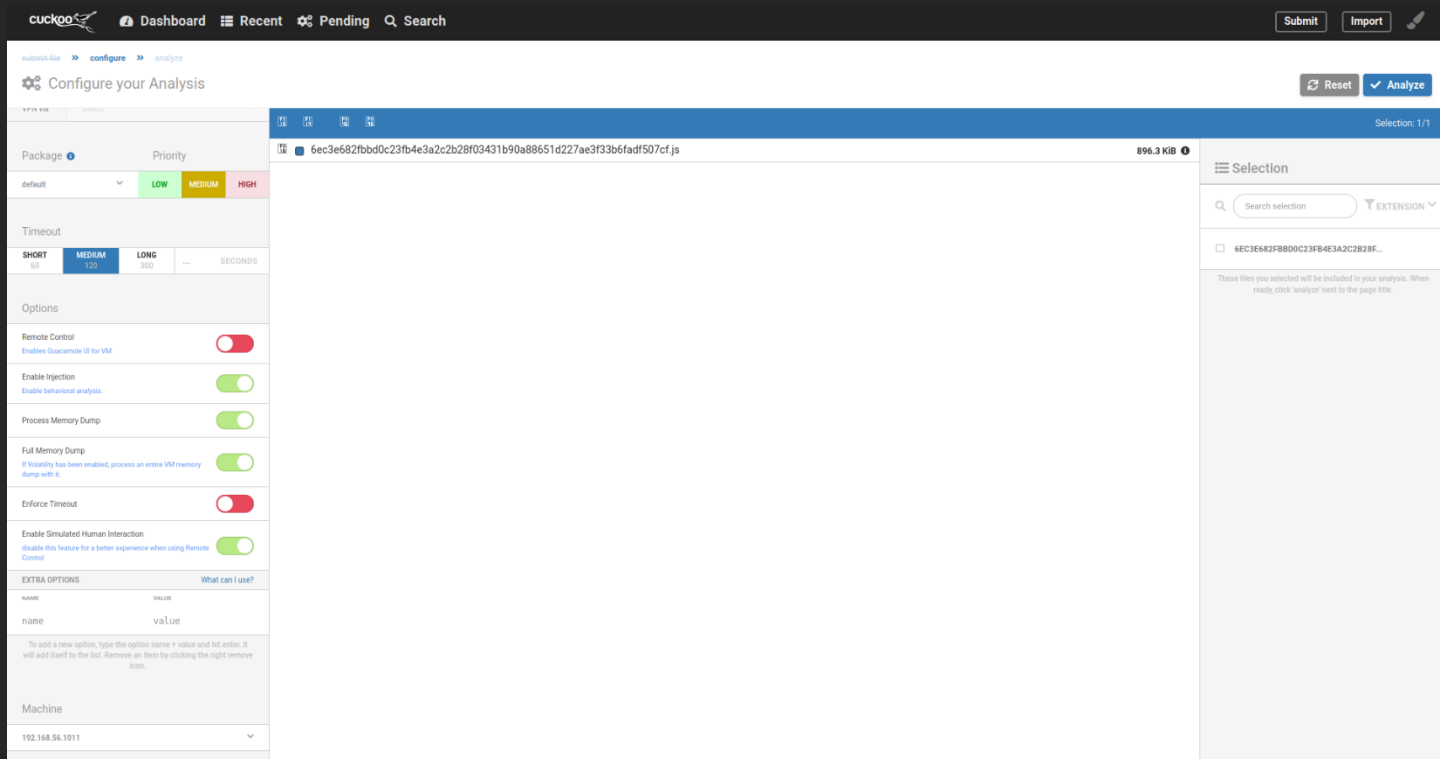


Figure6. La page ‘Configure your Analysis’ de l’interface web Cuckoo.

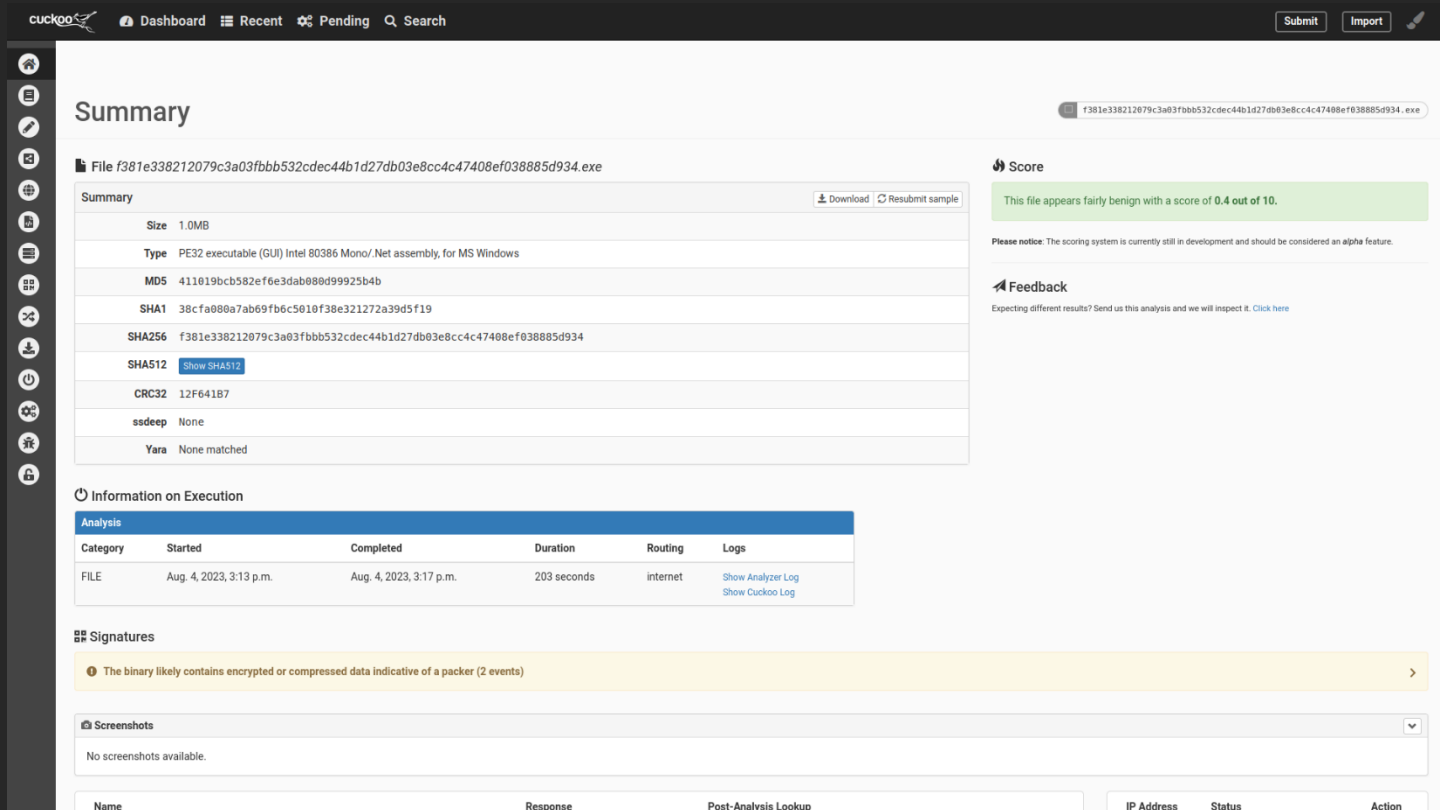


Figure6. Exemple d’un rapport généré par Cuckoo.