

Travail de Bachelor 2020-2021

**SECRET II : SECuRE environment for automatic Test grading, part 2**

***Annexe B***

Procédure d’utilisation des scripts Python

Date : 30.07.2021

Auteur : Stéphane Teixeira Carvalho

**Table des matières**

[1 Utilisation du script mitmproxy\_configfile\_start.py 3](#_Toc78208685)

[2 Utilisation du script discover\_clients\_veyon.py 5](#_Toc78208686)

[3 Utilisation du script capture\_trafic.py 6](#_Toc78208687)

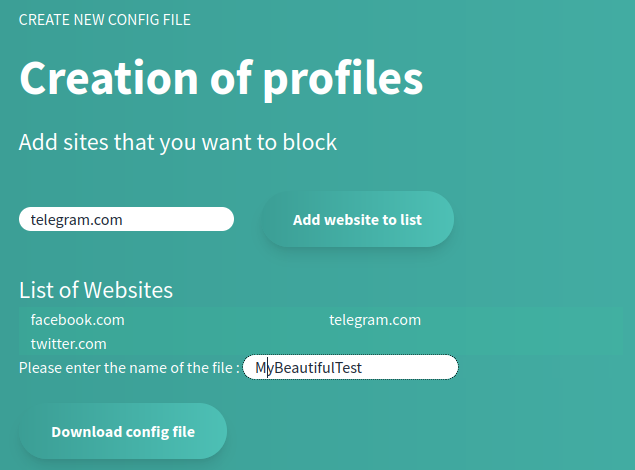
[4 Location des scripts 7](#_Toc78208688)

# Utilisation du script mitmproxy\_configfile\_start.py

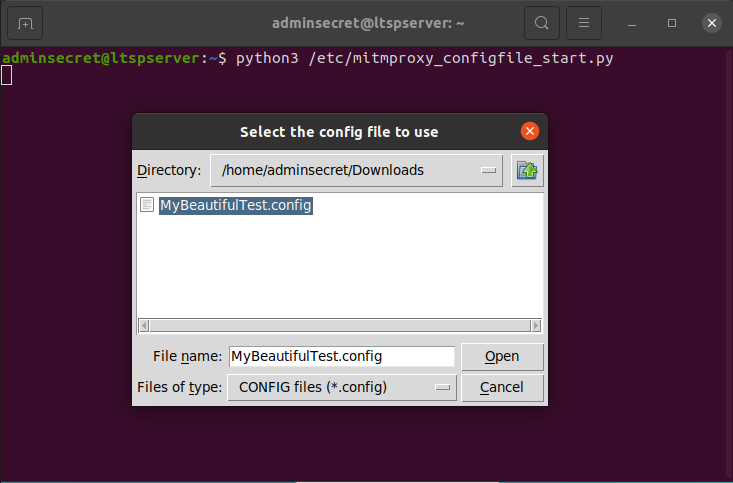
Ce chapitre va expliquer comment utiliser le script mitmproxy\_configfile\_start.py situé dans le dossier /usr/local/bin/ du serveur. Ce script va permettre de démarrer mitmproxy avec un fichier de configuration contenant les sites à bloquer. Ces fichiers peuvent être générés à l’adresse <http://ip-server/block_sites.php>. Pour lancer le script correctement l’utilisateur devra être administrateur de la machine.

Voici un tutoriel mettant en place le blocage des sites facebook.com, twitter.com et telegram.com :

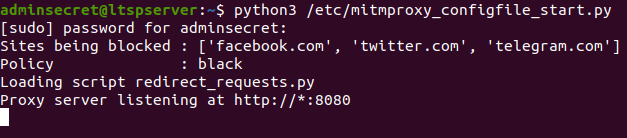
* + 1. Allez sur le site <http://ip-server/block_sites.php> et entrez les 3 adresses dans la liste.
    2. Mettre un nom pour le fichier de configuration



* + 1. Cliquez sur le bouton *Download config file* pour générer le fichier. Celui-ci sera téléchargé dans le dossier Download
    2. Lancez le script mitmproxy\_configfile\_start.py avec la commande python3 /etc/ mitmproxy\_configfile\_start.py
    3. Choisir le fichier généré



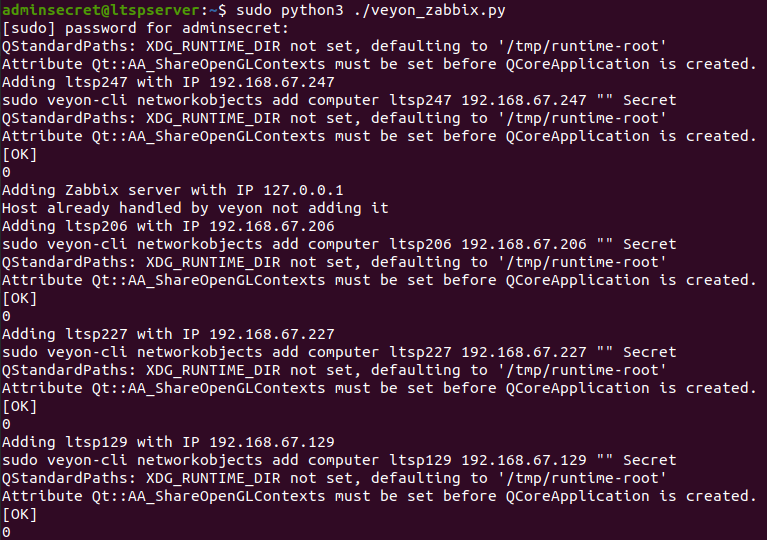
* + 1. Vous pouvez vérifier le bon fonctionnement du fichier en regardant les sites que MitmProxy va bloquer.



# Utilisation du script discover\_clients\_veyon.py

Ce chapitre va expliquer comment utiliser le script discover\_clients\_veyon.py situé dans le dossier /usr/local/bin sur le serveur. Il va permettre de configurer les machines disponibles sur le réseau dans Veyon pour pouvoir surveiller leur écran. Pour pouvoir le lancer vous devrez avoir les droits administrateur sur la machine ainsi qu’un serveur Zabbix fonctionnel et Veyon d’installés.

Aucune entrée utilisateur ne sera demandée pour son exécution. Voici un exemple d’exécution du script :

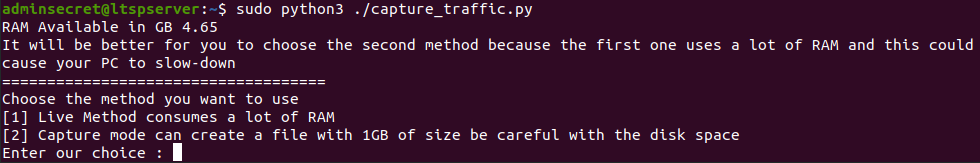


# Utilisation du script capture\_trafic.py

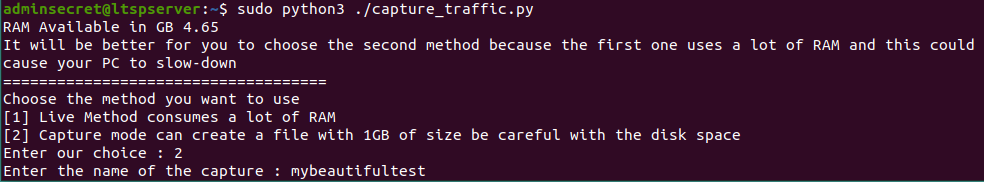
Ce chapitre va expliquer comment utiliser le script capture\_trafic.py situé dans le dossier /usr/local/bin sur le serveur. Ce script va permettre de capturer le trafic généré par les clients pour le transmettre à Elasticsearch et pouvoir visualiser la capture sur Grafana.

Voici un exemple d’exécution de script

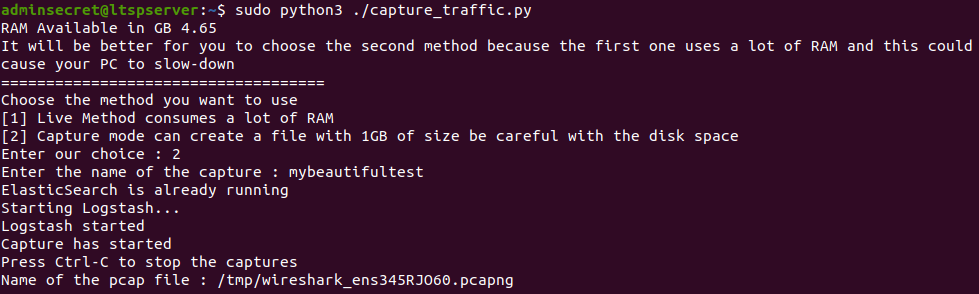
* + 1. Choisir parmi les 2 méthodes mises à disposition. Un conseil vous sera donné sur la méthode à préférer si peu de RAM est disponible sur votre machine.



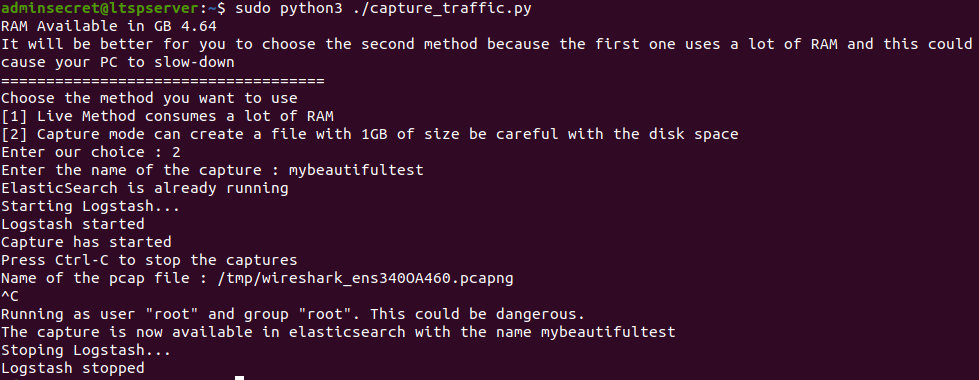
* + 1. Choisir un nom de capture. Attention, étant le nom de l’index sur Elasticsearch, une certaine nomenclature sera à respecter



* + 1. Les services seront démarrés et la capture commencera. Pour l'arrête, il faudra effectuer la suite de touche Ctrl+C. Si Elasticsearch est déjà actif, il ne sera pas démarré.



* + 1. Une fois le transfert sur Elasticsearch terminé. Le script arrêtera le logiciel Logsatsh.



# Location des scripts

Tous les scripts présentés dans ce document sont disponibles dans le dossier /usr/local/bin. Cependant, ils doivent tous être lancés avec des droits administrateur et donc avec le mot clé *sudo* devant python3.

Les scripts sont également disponibles dans le dossier Python\_Script contenu dans le dossier des Annexes. Ainsi, vous pouvez voir le code sans forcément posséder un système SECRET.