

Travail de Bachelor 2020-2021

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

***Annexe B***

Procédure d’utilisation des scripts Python

Date : 29.07.2021

Auteur : Stéphane Teixeira Carvalho

**Table des matières**

[1 Utilisation du script mitmproxy\_configfile\_start.py 3](#_Toc77620182)

[2 Utilisation du script veyon\_zabbix.py 5](#_Toc77620183)

[2.1 Mise en place connexion Zabbix 5](#_Toc77620184)

[2.2 Importation du tableau de bord Zabbix 8](#_Toc77620185)

[3 Configuration de Grafana pour Elasticsearch 10](#_Toc77620186)

[3.1 Mise en place connexion ElasticSearch 10](#_Toc77620187)

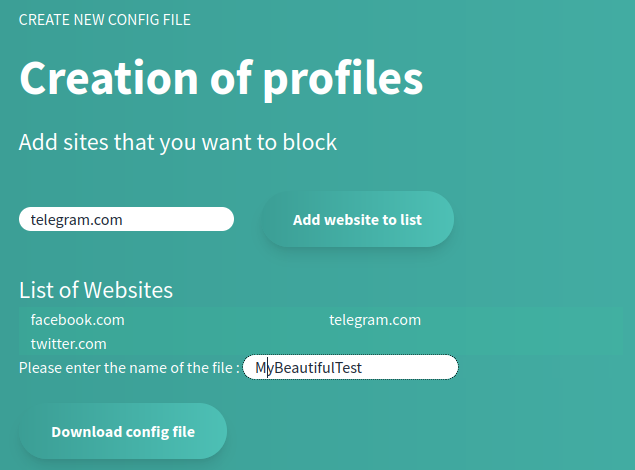
[3.2 Importation du tableau de bord Elasticsearch 11](#_Toc77620188)

# Utilisation du script mitmproxy\_configfile\_start.py

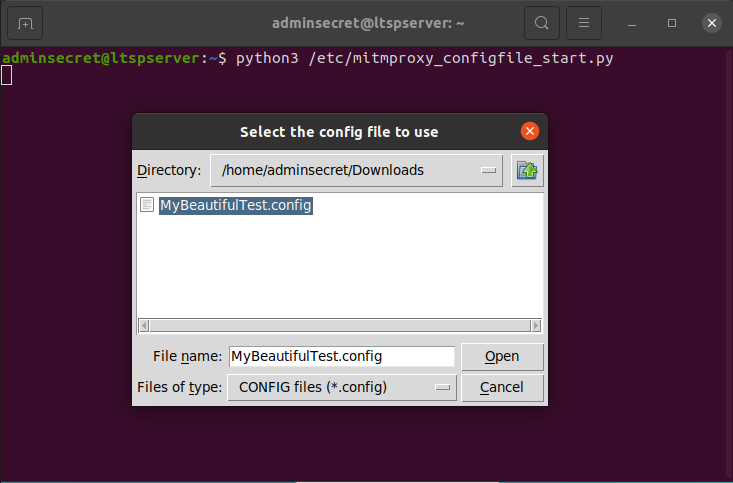
Ce chapitre va expliquer comment utiliser le script mitmproxy\_configfile\_start.py situé dans le dossier /etc du serveur. Ce script va permettre de démarrer mitmproxy avec un fichier de configuration contenant les sites à bloquer. Les fichiers de configurations peuvent être généré à l’adresse <http://ip-server/block_sites.php>. 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 :

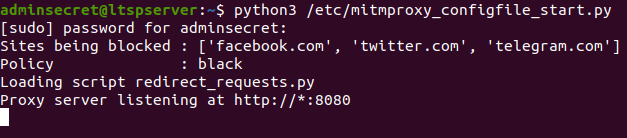
* + 1. Allez sur le site <http://ip-server/block_sites.php> et entrer les 3 adresses dans la liste.
    2. Mettre un nom pour le fichier de configuration



* + 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



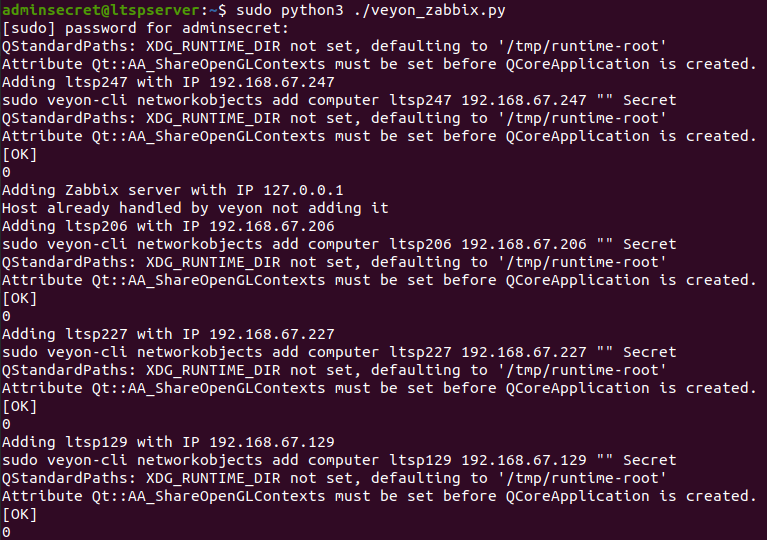
* + 1. Vous pouvez vérifier le bon fonctionnement du fichier en regardant les sites que MitmProxy va bloquer.



# Utilisation du script veyon\_zabbix.py

Ce chapitre va expliquer comment utiliser le script veyon\_zabbix.py situé dans le dossier Python\_Scripts à la racine des annexes. Ce script va permettre de configurer les machines disponibles sur le réseau dans Veyon pour pouvoir surveiller leur écran. Pour pouvoir l’utiliser vous devrez avoir les droits administrateurs sur la machine ainsi qu’un serveur Zabbix fonctionnel et Veyon d’installer.

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

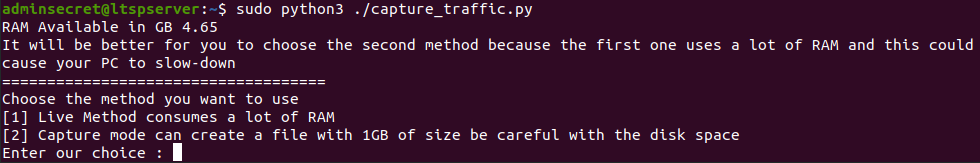


# Utilisation du script capture\_trafic.py

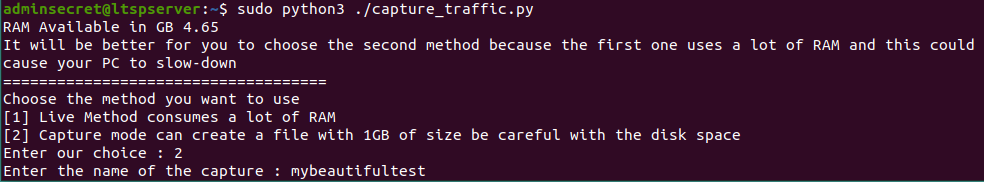
Ce chapitre va expliquer comment utiliser le script capture\_trafic.py situé dans le dossier Python\_Scripts à la racine des annexes. Ce script va permettre de capturer le trafic générer par les clients pour le transmettre à Elasticsearch et pouvoir visualiser la capture sur Grafana.

Voici un exemple d’exécution de script

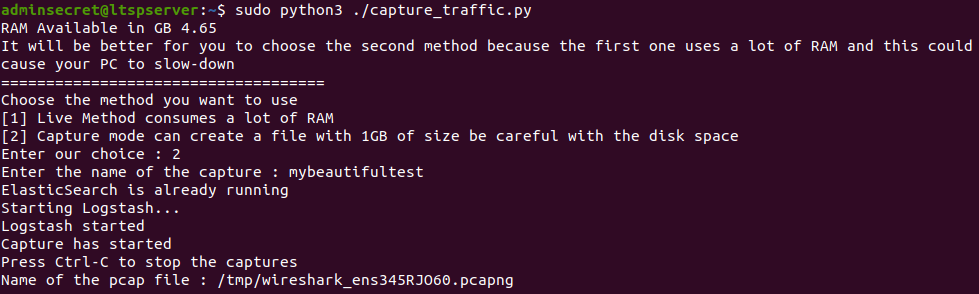
* + 1. Choisir parmi les 2 méthodes mises à disposition. Un conseil vous sera donné sur la méthode à préférer si peu de RAM est disponible sur votre machine.



* + 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 arrêter une capture 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.

