HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

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

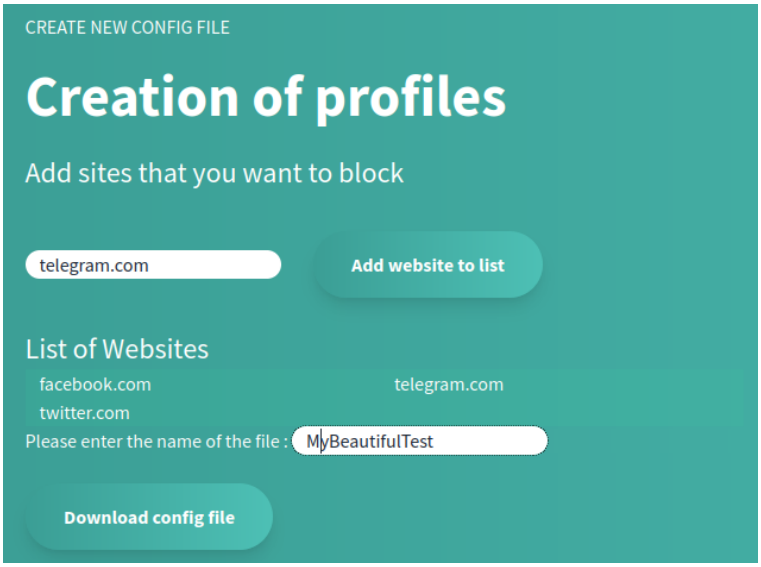
Table des matières

1 Utilisation du script mitmproxy_configfile_start.py

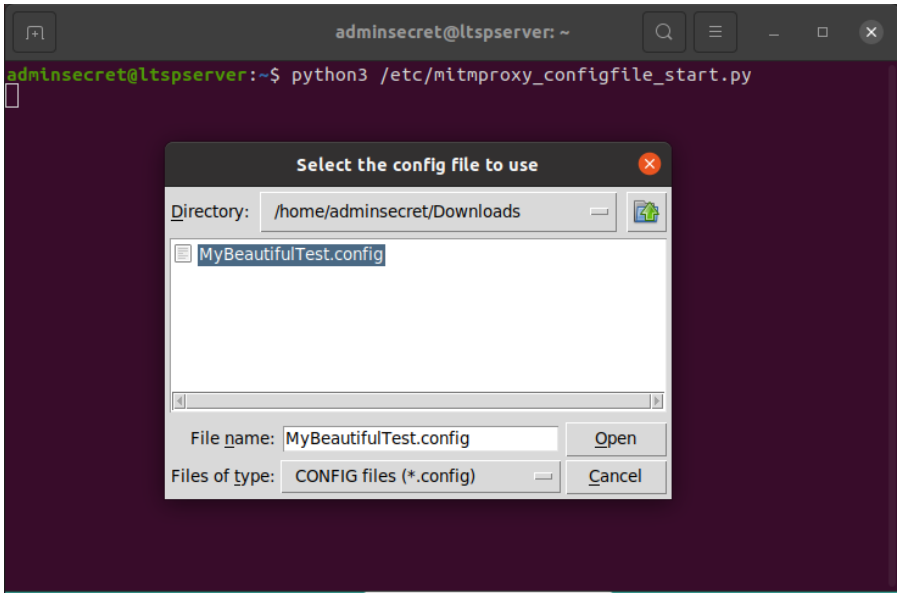
Ce chapitre va expliquer comment utiliser le script mitmproxy_configfile_start.py situé dans le dossier /usr/local/bin/ du serveur. Ce script va permettre de démarrer mitmproxy avec un fichier de configuration contenant les sites à bloquer. Ces fichiers peuvent être générés à l'adresse http://ip-server/block_sites.php. 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



3. Cliquez sur le bouton *Download config file* pour générer le fichier. Celui-ci sera téléchargé dans le dossier Download
4. Lancez le script mitmproxy_configfile_start.py avec la commande python3 /etc/ mitmproxy_configfile_start.py
5. Choisir le fichier généré



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

```
adminsecret@ltspserver:~$ python3 /etc/mitmproxy_configfile_start.py
[sudo] password for adminsecret:
Sites being blocked : ['facebook.com', 'twitter.com', 'telegram.com']
Policy              : black
Loading script redirect_requests.py
Proxy server listening at http://*:8080
```

2 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 :

```
adminsecret@ltspserver:~$ sudo python3 ./veyon_zabbix.py
[sudo] password for adminsecret:
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
Attribute Qt::AA_ShareOpenGLContexts must be set before QCoreApplication is created.
Adding ltsp247 with IP 192.168.67.247
sudo veyon-cli networkobjects add computer ltsp247 192.168.67.247 "" Secret
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
Attribute Qt::AA_ShareOpenGLContexts must be set before QCoreApplication is created.
[OK]
0
Adding Zabbix server with IP 127.0.0.1
Host already handled by veyon not adding it
Adding ltsp206 with IP 192.168.67.206
sudo veyon-cli networkobjects add computer ltsp206 192.168.67.206 "" Secret
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
Attribute Qt::AA_ShareOpenGLContexts must be set before QCoreApplication is created.
[OK]
0
Adding ltsp227 with IP 192.168.67.227
sudo veyon-cli networkobjects add computer ltsp227 192.168.67.227 "" Secret
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
Attribute Qt::AA_ShareOpenGLContexts must be set before QCoreApplication is created.
[OK]
0
Adding ltsp129 with IP 192.168.67.129
sudo veyon-cli networkobjects add computer ltsp129 192.168.67.129 "" Secret
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
Attribute Qt::AA_ShareOpenGLContexts must be set before QCoreApplication is created.
[OK]
0
```

3 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.

```
adminsecret@ltspserver:~$ sudo python3 ./capture_traffic.py
RAM Available in GB 4.65
It will be better for you to choose the second method because the first one uses a lot of RAM and this could
cause your PC to slow-down
==================================
Choose the method you want to use
[1] Live Method consumes a lot of RAM
[2] Capture mode can create a file with 1GB of size be careful with the disk space
Enter our choice :
```

2. Choisir un nom de capture. Attention, étant le nom de l'index sur Elasticsearch, une certaine nomenclature sera à respecter

```
adminsecret@ltspserver:~$ sudo python3 ./capture_traffic.py
RAM Available in GB 4.65
It will be better for you to choose the second method because the first one uses a lot of RAM and this could
cause your PC to slow-down
==================================
Choose the method you want to use
[1] Live Method consumes a lot of RAM
[2] Capture mode can create a file with 1GB of size be careful with the disk space
Enter our choice : 2
Enter the name of the capture : mybeautifultest
```

3. 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.

```
adminsecret@ltspserver:~$ sudo python3 ./capture_traffic.py
RAM Available in GB 4.65
It will be better for you to choose the second method because the first one uses a lot of RAM and this could
cause your PC to slow-down
==================================
Choose the method you want to use
[1] Live Method consumes a lot of RAM
[2] Capture mode can create a file with 1GB of size be careful with the disk space
Enter our choice : 2
Enter the name of the capture : mybeautifultest
ElasticSearch is already running
Starting Logstash...
Logstash started
Capture has started
Press Ctrl-C to stop the captures
Name of the pcap file : /tmp/wireshark_ens345RJO60.pcapng
```

4. Une fois le transfert sur Elasticsearch terminé. Le script arrêtera le logiciel Logsatsh.

```
adminsecret@ltspserver:~$ sudo python3 ./capture_traffic.py
RAM Available in GB 4.64
It will be better for you to choose the second method because the first one uses a lot of RAM and this could
cause your PC to slow-down
==================================
Choose the method you want to use
[1] Live Method consumes a lot of RAM
[2] Capture mode can create a file with 1GB of size be careful with the disk space
Enter our choice : 2
Enter the name of the capture : mybeautifultest
ElasticSearch is already running
Starting Logstash...
Logstash started
Capture has started
Press Ctrl-C to stop the captures
Name of the pcap file : /tmp/wireshark_ens340OA460.pcapng
^C
Running as user "root" and group "root". This could be dangerous.
The capture is now available in elasticsearch with the name mybeautifultest
Stoping Logstash...
Logstash stopped
```

4 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.