misp-guard

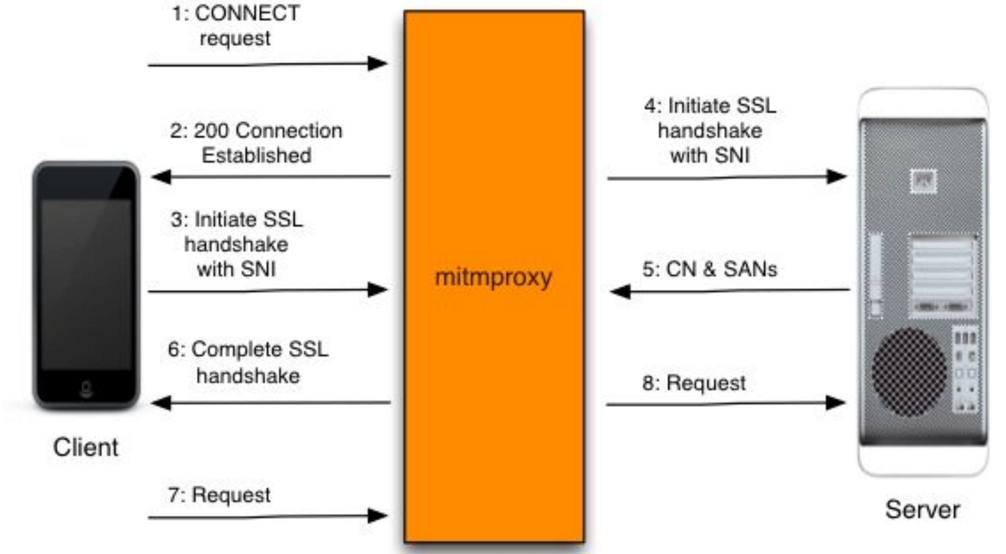
Luciano Righetti

a mitmproxy addon that inspects and blocks outgoing events

https://github.com/MISP/misp-guard

_mitmproxy

"mitmproxy is a free and open source interactive HTTPS proxy."


1: CONNECT request
2: 200 Connection Established
3: Initiate SSL handshake with SNI
4: Initiate SSL handshake with SNI
5: CN & SANs
6: Complete SSL handshake
7: Request
8: Request
mitmproxy
Client
Server

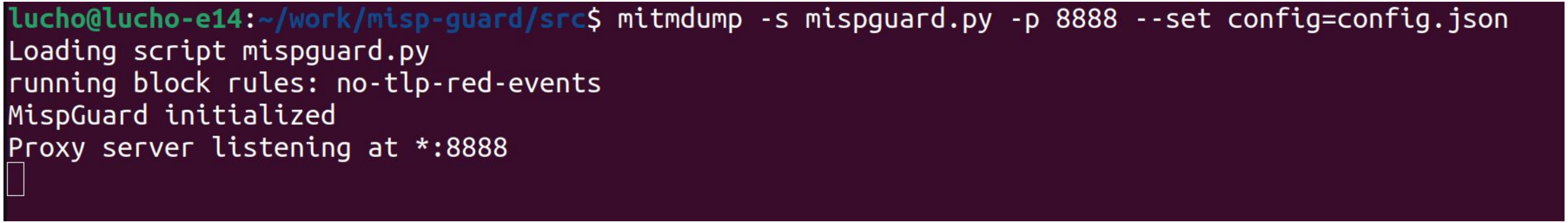
source: *https://mitmproxy.org/*

_setup_1

```
1.   git clone https://github.com/MISP/misp-guard & cd src/

2.   pip install -r requirements.txt

3.   mitmdump -s mispguard.py -p 8888 --set config=config.json
```



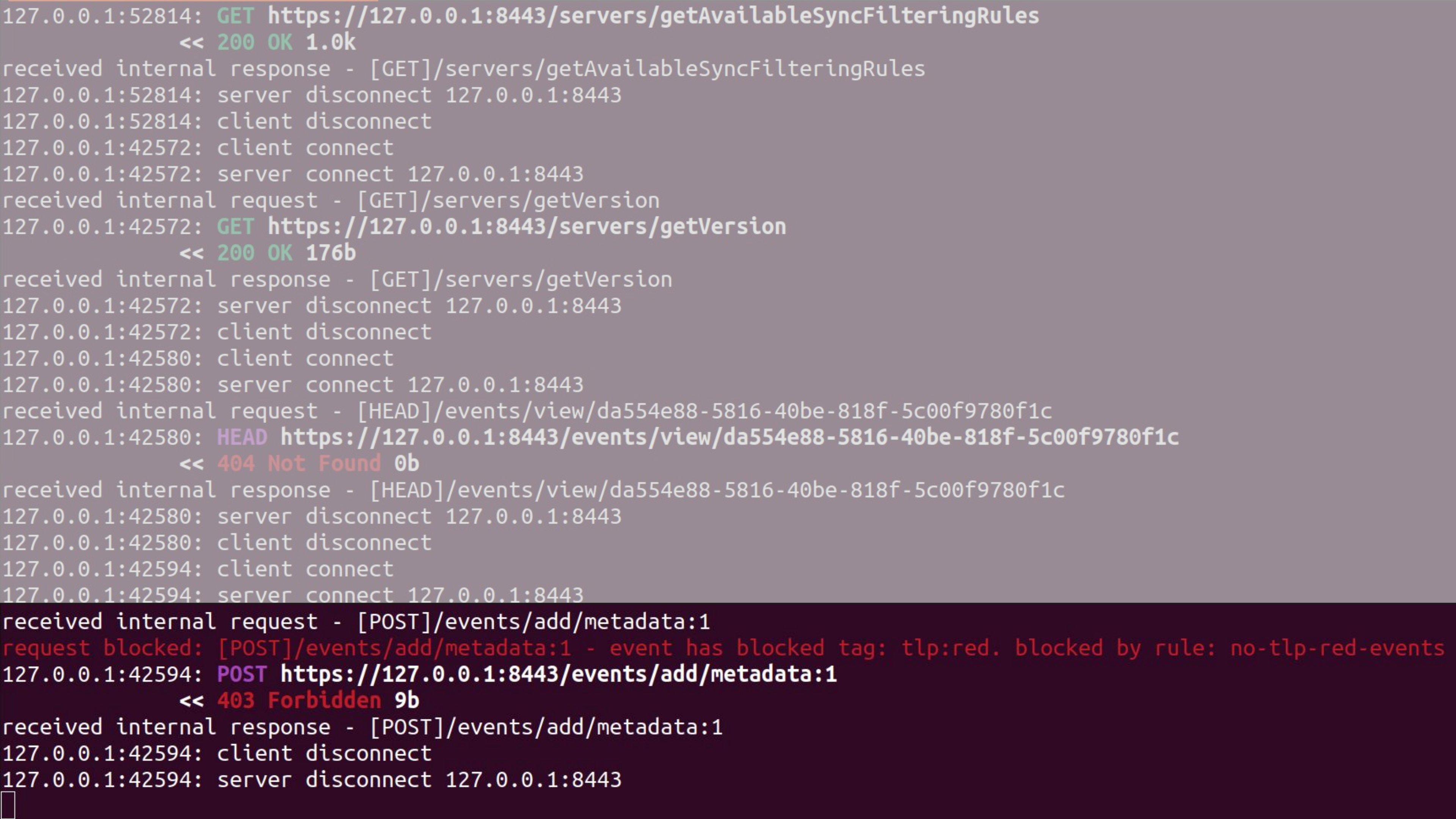
```
lucho@lucho-e14:~/work/misp-guard/src$ mitmdump -s mispguard.py -p 8888 --set config=config.json
Loading script mispguard.py
running block rules: no-tlp-red-events
MispGuard initialized
Proxy server listening at *:8888
```

_setup_2

1. set *Proxy.host* and *Proxy.port* to point to the misp-guard mitmproxy host and port define yo

2. define customs rules in the *config.json* file:
   - *blocked_tags*
   - *blocked_distribution_levels*
   - *blocked_sharing_groups_uuids*
   - *blocked_attribute_types*
   - *blocked_attribute_categories*
   - *blocked_object_types*

3. if external MISP instances are pulling, they should connect to the *misp-guard* instance not to your instance.



```
127.0.0.1:52814: GET https://127.0.0.1:8443/servers/getAvailableSyncFilteringRules
              << 200 OK 1.0k
received internal response - [GET]/servers/getAvailableSyncFilteringRules
127.0.0.1:52814: server disconnect 127.0.0.1:8443
127.0.0.1:52814: client disconnect
127.0.0.1:42572: client connect
127.0.0.1:42572: server connect 127.0.0.1:8443
received internal request - [GET]/servers/getVersion
127.0.0.1:42572: GET https://127.0.0.1:8443/servers/getVersion
              << 200 OK 176b
received internal response - [GET]/servers/getVersion
127.0.0.1:42572: server disconnect 127.0.0.1:8443
127.0.0.1:42572: client disconnect
127.0.0.1:42580: client connect
127.0.0.1:42580: server connect 127.0.0.1:8443
received internal request - [HEAD]/events/view/da554e88-5816-40be-818f-5c00f9780f1c
127.0.0.1:42580: HEAD https://127.0.0.1:8443/events/view/da554e88-5816-40be-818f-5c00f9780f1c
              << 404 Not Found 0b
received internal response - [HEAD]/events/view/da554e88-5816-40be-818f-5c00f9780f1c
127.0.0.1:42580: server disconnect 127.0.0.1:8443
127.0.0.1:42580: client disconnect
127.0.0.1:42594: client connect
127.0.0.1:42594: server connect 127.0.0.1:8443
received internal request - [POST]/events/add/metadata:1
request blocked: [POST]/events/add/metadata:1 - event has blocked tag: tlp:red. blocked by rule: no-tlp-red-events
127.0.0.1:42594: POST https://127.0.0.1:8443/events/add/metadata:1
              << 403 Forbidden 9b
received internal response - [POST]/events/add/metadata:1
127.0.0.1:42594: client disconnect
127.0.0.1:42594: server disconnect 127.0.0.1:8443
```