

LAB2 Malicious proxy

Installare docker engine su VM linux.

Cliccare sul sistema operativo della VM al seguente link e seguire le istruzioni:

<https://docs.docker.com/engine/install/>

Eseguire il server proxy con TLS inspection disabilitata

Lanciare da terminale il seguente comando docker:

```
docker run \
  --rm -it -p 8080:8080 -p 127.0.0.1:8081:8081 \
  mitmproxy/mitmproxy \
  mitmweb --web-host 0.0.0.0 --ignore-hosts '.*' \
  --set show_ignored_hosts=true
```

Il comando lancia il proxy server 'mitmweb' con le opzioni '--web-host 0.0.0.0 --ignore-hosts '.*' --set show_ignored_hosts=true'.

Info

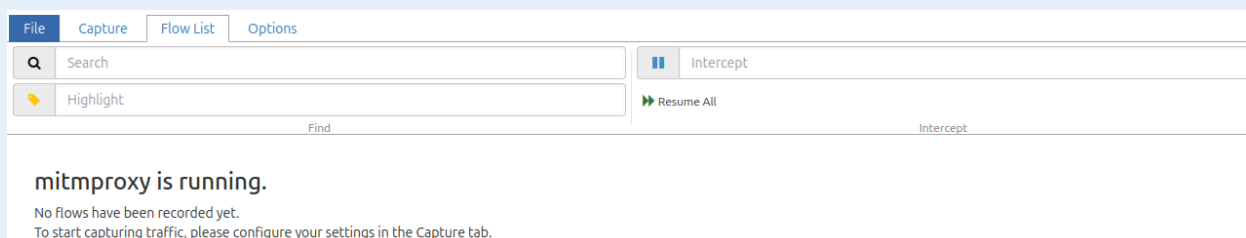
```
user@ubuntu-dev: ~/workspace * docker run --rm -it -p 8080:8080 -p 127.0.0.1:8081:8081 mitmproxy/mitmproxy mitmweb --web-host 0.0.0.0 --ignore-hosts '.*' --set show_ignored_hosts=true
[08:00:21.235] HTTP(S) proxy listening at *:8080.
[08:00:21.237] Web server listening at http://0.0.0.0:8081/?token=3a190e48cffa9cf2b7af060ded46f1d1
[08:00:21.345] No web browser found. Please open a browser and point it to http://0.0.0.0:8081/?token=3a190e48cffa9cf2b7af060ded46f1d1
[08:00:21.345] You can configure a fixed authentication token by setting the 'web_password' option (https://docs.mitmproxy.org/stable/concepts-options/#web_password).
```

Esempio di output corretto

Per sospendere l'esecuzione è sufficiente premere la combinazione di tasti CTRL+C

Una volta che il server proxy è in esecuzione, potete cliccare sul link a terminale (Web server listening at ...) per visualizzare una pagina dove poter monitorare tutte le richieste che passano attraverso il server proxy.

Info



Web UI di mitmproxy

Per generare traffico è necessario configurare il proprio browser all'interno della macchina virtuale, dicendogli di indirizzare tutto il traffico attraverso il nostro server proxy.

L'impostazione cambia a seconda del browser, usa pure google per trovare altre guide a riguardo.

Il server proxy è di tipo HTTP ed esegue localmente all'indirizzo <http://127.0.0.1:8080>

Una volta configurato il proxy, è sufficiente navigare su qualche sito per vedere tutte le informazioni raccolte dal proxy nella webui aperta al punto precedente.

Info

File	Capture	Flow List	Options	Flow	
Replay	Duplicate	Revert	Delete	Mark	Download
Export	Export	Export	Export	Export	Export
Resume	Resume	Resume	Resume	Resume	Resume
Abort	Abort	Abort	Abort	Abort	Abort
Path	Method	Status	Size	Time	Stream Data
127.17.0.1:40256 → www.google.com:443	TCP	10.8kb
http://o.gki.google.it/	POST	200	554b	177ms	...
http://www.yarix.com/	GET	200	0	208ms	...
http://scip.digitel.com/	POST	200	810b	177ms	...
127.17.0.1:157076 → sitecore.vargroup.com:443	TCP	12.2kb
127.17.0.1:157080 → sitecore.vargroup.com:443	TCP	77.4kb
127.17.0.1:157070 → sitecore.vargroup.com:443	TCP	6.8kb
127.17.0.1:157056 → sitecore.vargroup.com:443	TCP	6.8kb
127.17.0.1:157048 → sitecore.vargroup.com:443	TCP	6.7kb
127.17.0.1:157096 → sitecore.vargroup.com:443	TCP	6.7kb
127.17.0.1:157176 → matomoni.bizmat2.it:443	TCP	5.1kb
http://es.silencer.org/	POST	200	430b	150ms	...
127.17.0.1:157226 → o4504377282605056.ingest.sentry.io:443	TCP	7.4kb
http://scip.digitel.com/	POST	200	554b	36ms	...
127.17.0.1:157224 → consent.cookiebot.com:443	TCP	7.3kb
127.17.0.1:157248 → consent.cookiebot.com:443	TCP	7.0kb
127.17.0.1:157262 → imgct.cookiebot.com:443	TCP	6.9kb

Web UI di mitmproxy con alcuni pacchetti catturati e loggati. Da notare come per le connessioni criptate il contenuto del traffico non è leggibile, ma solo il dominio di destinazione.

Eseguire il server proxy con TLS inspection abilitata

Lanciare da terminale il seguente comando docker:

```
docker run \
  --rm -it -p 8080:8080 -p 127.0.0.1:8081:8081 \
  mitmproxy/mitmproxy \
  mitmweb --web-host 0.0.0.0
```

Questo comando abilita la TLS inspection. Gli step di configurazione sono uguali alla sezione precedente.

Info

