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/

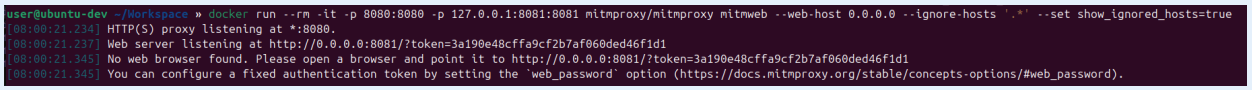
Eseguire il server proxy con TLS inspection disabilitata

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

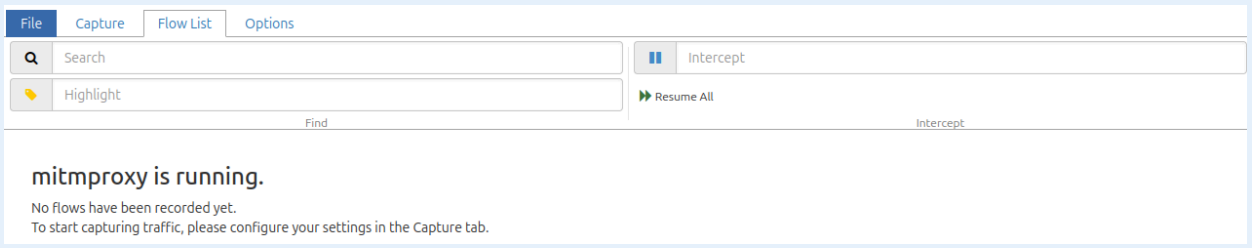


Esempio di output corretto

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

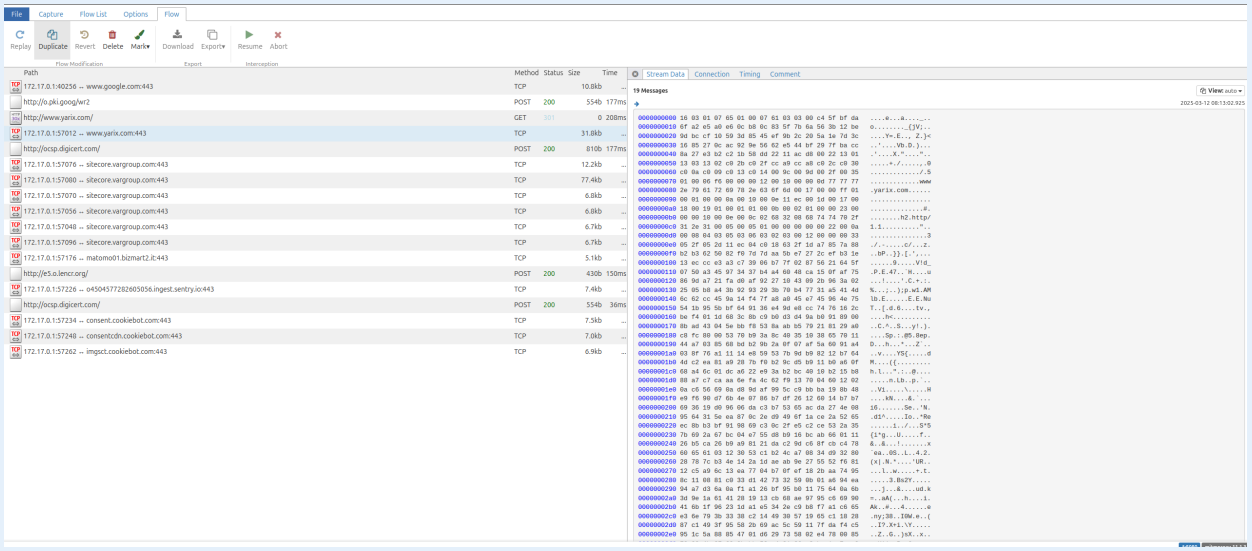
Per generare traffico è necessario configurare il proprio browser all'interno della macchina virtuale, dicendogli di indirizzare tutto il traffico attraverso il nostro server proxy.

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



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.

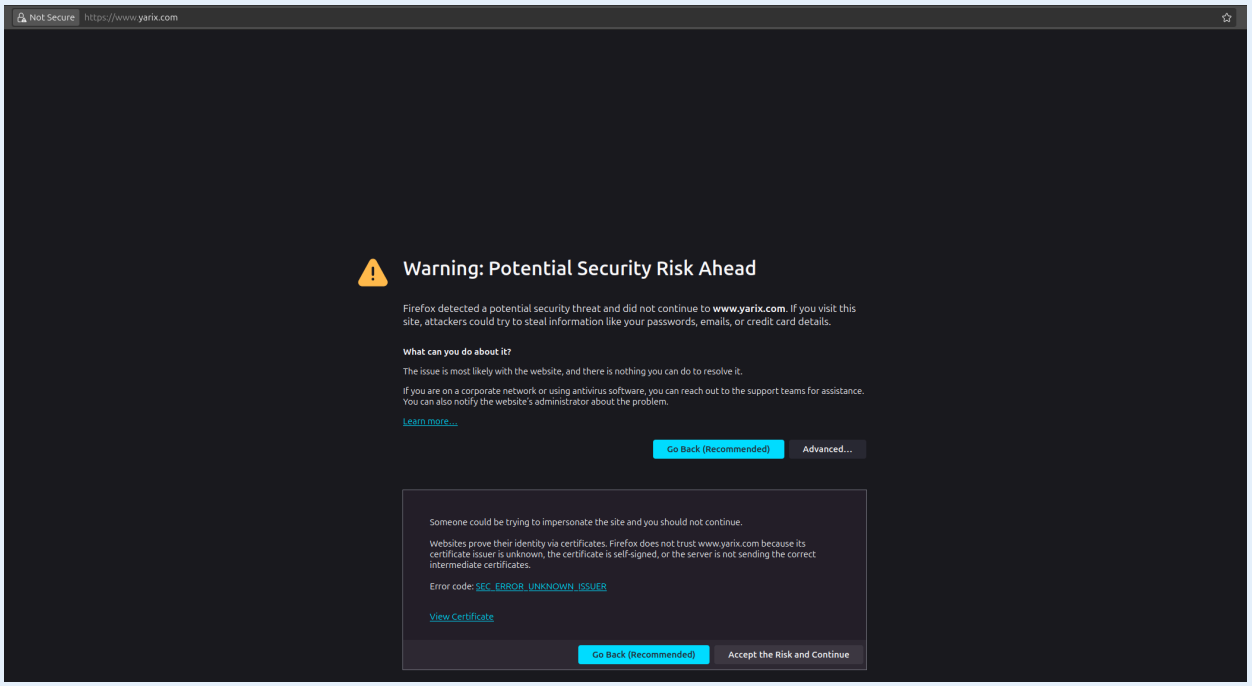
Eseguire il server proxy con TLS inspection abilitata

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
```

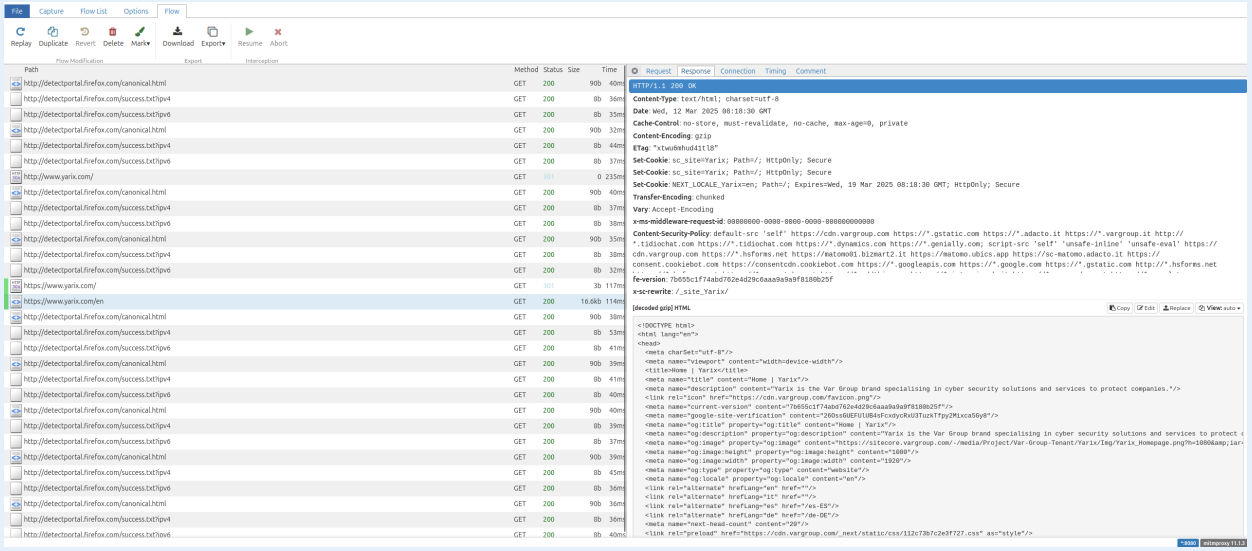
Questo comando abilita la TLS inspection. Gli step di configurazione sono uguali alla sezione precedente.

Info



Collegato al server proxy, l'utente visualizza un avviso di sicurezza quando prova ad accedere a siti web con protocollo https

Info



Abilitando TLS inspection è possibile visualizzare anche il contenuto di trasmissioni https.

Una volta finito il LAB, ricordarsi di disabilitare il proxy dalle impostazioni del browser