CÁTEDRA DE CIBERSEGURIDAD CIBERUGR, INCIBE-UGR

Nombre	Enigmatic Vault
Categoría	Crypto
Dificultad	Fácil
Puntos	200

DESCRIPCIÓN DEL RETO

Esta bóveda de Keepass contiene secretos enigmáticos… aunque su clave maestra no lo es tanto. Averigua como acceder a la bóveda para resolver la enigmática flag.

Formato de la flag: todo en mayúscula y con guiones bajos. UGR_ETSIIT_CTF25{ESTO_ES_UN_EJEMPLO}

WRITEUP

1. El reto empieza con una bóveda de Keepass *challenge.kdb*. Podemos saber la versión de la bóveda del Keepass con el siguiente comando.

```
file challenge.kdb
```

```
┌──(kali㉿kali)-[/tmp/challenge]
└─$ ls
challenge.kdb

┌──(kali㉿kali)-[/tmp/challenge]
└─$ file challenge.kdb
challenge.kdb: Keepass password database 1.x KDB, 8 groups, 6 entries, 600000 key transformation rounds
```

2. Vemos que es una bóveda de Keepass v1.x, esta versión es soportada por la herramienta John The Ripper para crackear contraseñas. Utilizamos la herramienta *keepass2john* para extraer y formatear el hash de la clave maestra de la bóveda al formato del cracker de contraseñas John The Ripper.

```
keepass2john challenge.kdb | tee hash.john
```

```
└─$ keepass2john challenge.kdb | tee hash.john
Inlining challenge.kdb
challenge.kdb:$keepass$*1*600000*0*24d4d8bd95babdabf43db867d87d25b2*3c91d8c8cf8712171e498d3c7beba89c2b8a142fd1bd3fee9c9fb4f1ee9aee86*d52da46ffbb7b06ac3a2369112*a2b8eadeffb2615d03197a09fcac078fd3b92e9f23cc894f574d4c07b577d6373279950a3cda3fffe4ceeacaaab6b4673de4384c610b5e2623ce56271a365a47d4c3d414547a3745918daa8da77d163c611296a37796e3fcb21cc7f741d6515a24ccc88d95bf7895682fbcc7b3076a737c9cdf7cf76d841477ea747ab6e4f4bb5237441dc2023267ca791eb52fe9791552426761e6a77eb061ef70ded4d354ab275a594cf883ea94e598496f1d5d63bf9d04bf53ed3aac820b5913d1de476cc63e577a86eb1861a33dd2ccee6102b8ad3edee4e0c7e5eb544b541ba55d5c7008dbcaf6cefd80488e1d9cf250f6f3e91b9807d3c5b8e9fa8d9b056d3abf24912c6c7f7dd841bfedcc86bec0958dd99a143fc6ede571cdaa6c18d5fa5c353b75726c28ec1be5f53a5466da17252a3ee682bb4c4466f30cd9f1c0b32ea0d233650ceddea6e442597b60fe9891d402e462ff58eb9c2ac6367924e3e4390eadf2fc1d4859aa20655e08ae8abb9a0aa1f8af44e76e520d50f5f6c7097a4dab0b6c0cc333d802c9c2f51bee6e3ac062113e4368871cc9a9ac805357d5d6a1254f354ebcfb00482d85d07300a3b30b62029fa82ee096086b8cef85da3ae750a1ab02d89594c820d0385a3d711d2dfe1dfde833864fa6cecbb552627da11834988598c9d772d6191368f2adf18fee1ec317bc2282404146aa12b72a3238db60ee1cf8b1ae5f81180439f6c032dbc5230f89ed1a7ca15470f77b74dcb0b4bceaa8d08f1117bc1795fe30baccad8bce43e1e9f62c8507a1f9501267d33e75d1c2868d43034462f75ba21c3f5d9d2553faf54141fab15ec031186a5f047f17cfeca4692681073705 4c2ebc354f856c32043e99b81ef29a99e8747193b119286984aa21a383b741afef06d8f8c949c3a22eee09ac4a99c32fa7032a95efc64feb4aef1144f1b12a07dec73cf2c7f7c884a6a771e8ab488cabca5ae951cbbd071fc2206beb9c5bc157a8971e1ec00249babbc08f778ca73817108cfb624a74c6e45156cf4e8b305ad5a9c3dc42b102c2ab5bc7920051aabef8d8946b7272d0f95c1bbbe9c4ad4d495ba7cc7aa676b7d641ef5dd9e4ef23715f4b105553e639b2a1c64dcf5b31470c18da6776ae99ac517ea261a179acd130c8885f7d1c78d2521dc8037a45e365269d8164341d87aaa8f587254267546a5cf7fab6ea9a1b9676950360780f2151abc5876695797f8532129ff755e3ebe451c02637fedbd096ece720d3e790b9f0d1ae9f001b2e5bed3c768396526db6eabd85adc5102d956bd9ea03bfe8f66d5c776abf2b01e582449c0a412d5c28af73bbd1de828b726d5917add49bd4d97d8b6b8eeec26e263b3d4b260401230fc0c0b3d155467628b7c87076e588d162edad8b8656814a03185b75d54e0281204b78659ed265f0127210d4e067622d4d0365e77e5e84942686c3bbce76d90897c68eb6ccd9c388767dfe3c0894ffdb990d4949e66372d37d42feebefd9c58decce3a79033522180baa18ccdd621a98de0f54f0610f1b0c524346df533a6a9c786d20f7321a309a8b0cef270b23215e9070081ac424a5b40b99140fe748c79b76d9d8614859ac0983e6543a2b2cab6d34bbe658516dd0e5998bc2db24ccc5235bd3f9cdb8cc7ceaca9b8302742f603ff1badfd9bfb6237b2360bb9f6e8712709e0d11031dfa122cf2e13ae1693c84cd978ee1115740dc677208e6a5049f2c2406f93ac46c1975ef23710070c92ee4fd92ff7e419263474886 9e43791fa3fe035e9185c49d381a4e1f9cce091c66c04ed0514743b3384426da101f732103548c063397c83f8ed18f64b38178ce09be041ccb50621d3673b4b112219113f422a07af419cf649a71388a189dfdd9c40a603d6b1e93bdf6b6cc23f306423c16d47921d4efd922fe4eb687156b4a032df9f737af24f370b8416ff80f27a19ff36da2c4886bafd007a7d820e6ef646c1339f88ac47940512a
```

3. Crackeamos el hash con ataque por diccionario usando John The Ripper y el diccionario RockYou.

```
john –wordlist=/path/to/rockyou hash.john
```

```
┌──(kali㉿kali)-[/tmp/challenge]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.john
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 600000 for all loaded hashes
Cost 2 (version) is 1 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
iloveyou         (challenge.kdb)
1g 0:00:00:01 DONE (2025-02-25 05:59) 0.7042g/s 11.26p/s 11.26c/s 11.26C/s 123456..jessica
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

4. Para interactuar con la bóveda de Keepass podemos utilizar un cliente gráfico (GUI) o una interfaz por la línea de comandos. Utilizaremos esta última para nuestro caso con la herramienta *kpcli* (kpcli - A command line interface for KeePass).
5. Abrimos la bóveda utilizando la contraseña que hemos crackeado.

```
kpcli –kdb=challenge.kdb
```

```
┌──(kali㉿kali)-[/tmp/challenge]
└─$ kpcli --kdb=challenge.kdb
Provide the master password: **************************

KeePass CLI (kpcli) v3.8.1 is ready for operation.
Type 'help' for a description of available commands.
Type 'help <command>' for details on individual commands.

kpcli:/>
```

6. Navegamos por la bóveda hasta encontrar un subgrupo *Top Secret*.

```
kpcli:/> ls
=== Groups ===
General/
Backup/
kpcli:/> ls General
=== Groups ===
eMail/
Homebanking/
Internet/
Network/
Top Secret/
Windows/
kpcli:/> ls General/Top\ Secret/
=== Entries ===
0. Config
1. Secret
kpcli:/>
```

7. Si echamos un vistazo a la entrada *Secret*, vemos que aparece una nota con un secreto cifrado.

```
kpcli> get 1 Notes
```

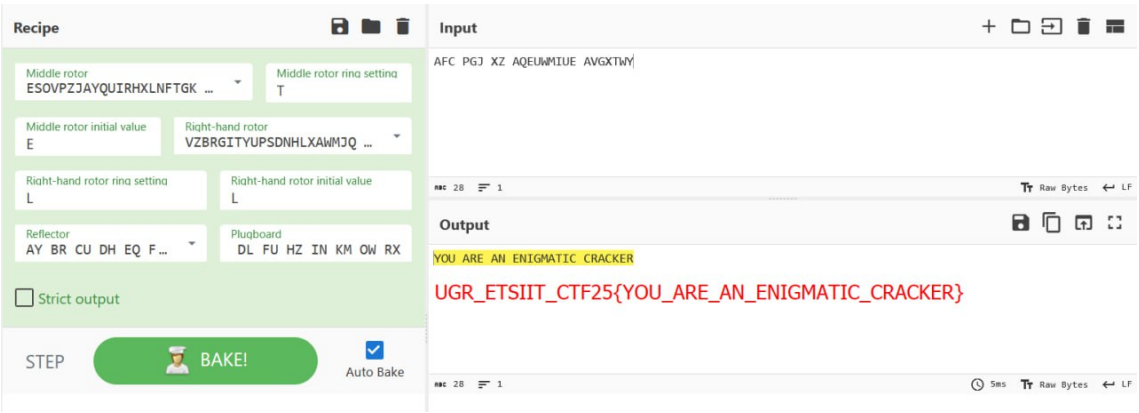
```
kpcli:/General/Top Secret> ls
=== Entries ===
0. Config
1. Secret
kpcli:/General/Top Secret> get 1 Notes
Esta es la respuesta al enigma: AFC_PGJ_XZ_AQEUWMIUE_AVGXTWY
kpcli:/General/Top Secret>
```

8. La misma nota da una pista de que puede estar cifrado con la famosa Máquina Enigma. Para descifrarla tenemos que configurar la máquina, para ello recuperamos la configuración en la otra entrada del grupo llamada *Config* en la parte de *Notes*.

```
kpcli> get 0 Notes
```

```
kpcli:/General/Top Secret> ls
=== Entries ===
0. Config
1. Secret
kpcli:/General/Top Secret> get 0 Notes
Rotors: II IV V
Reflector: B
Ring Settings: 1 20 12
Plugboard: AV BS CG DL FU HZ IN KM OW RX
Start Position: HEL
```

9. Utilizamos esta configuración para descifrar el mensaje con una máquina Enigma. Usamos la herramienta de CyberChef (CyberChef) para ello.



10. Tendremos finalmente la flag en el format UGR_ETSIIT_CTF25{YOU_ARE_AN_ENIGMATIC_CRACKER}.