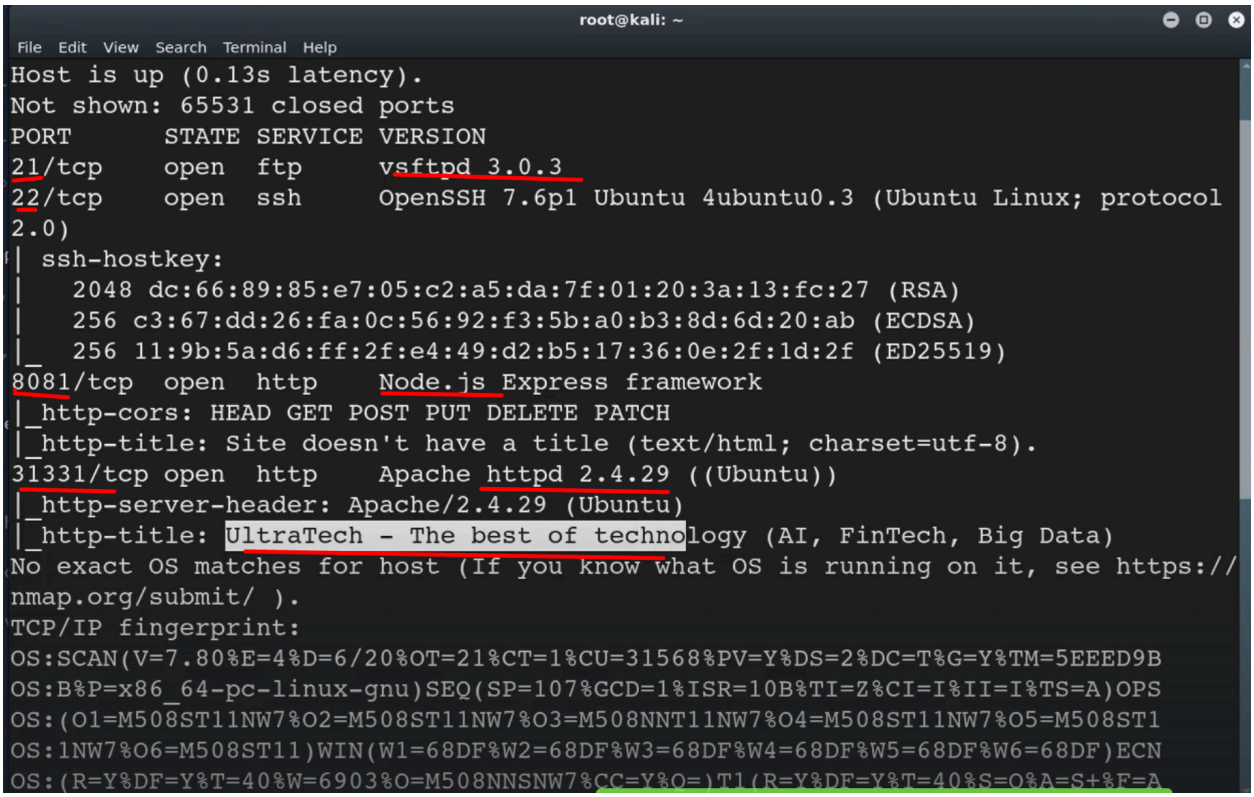
Ultra Tech - THM (Done)

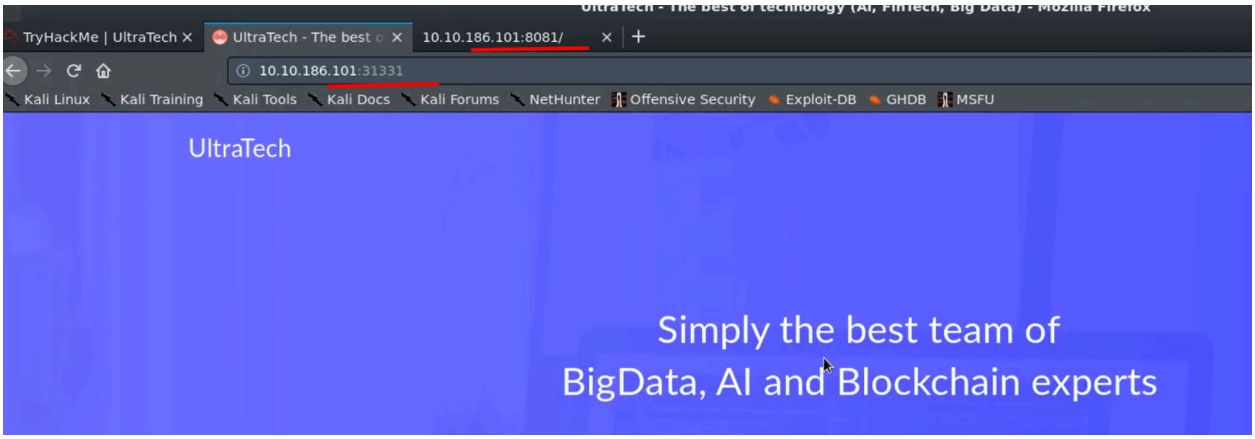
https://tryhackme.com/r/room/ultratech1

Gaining a Foothold

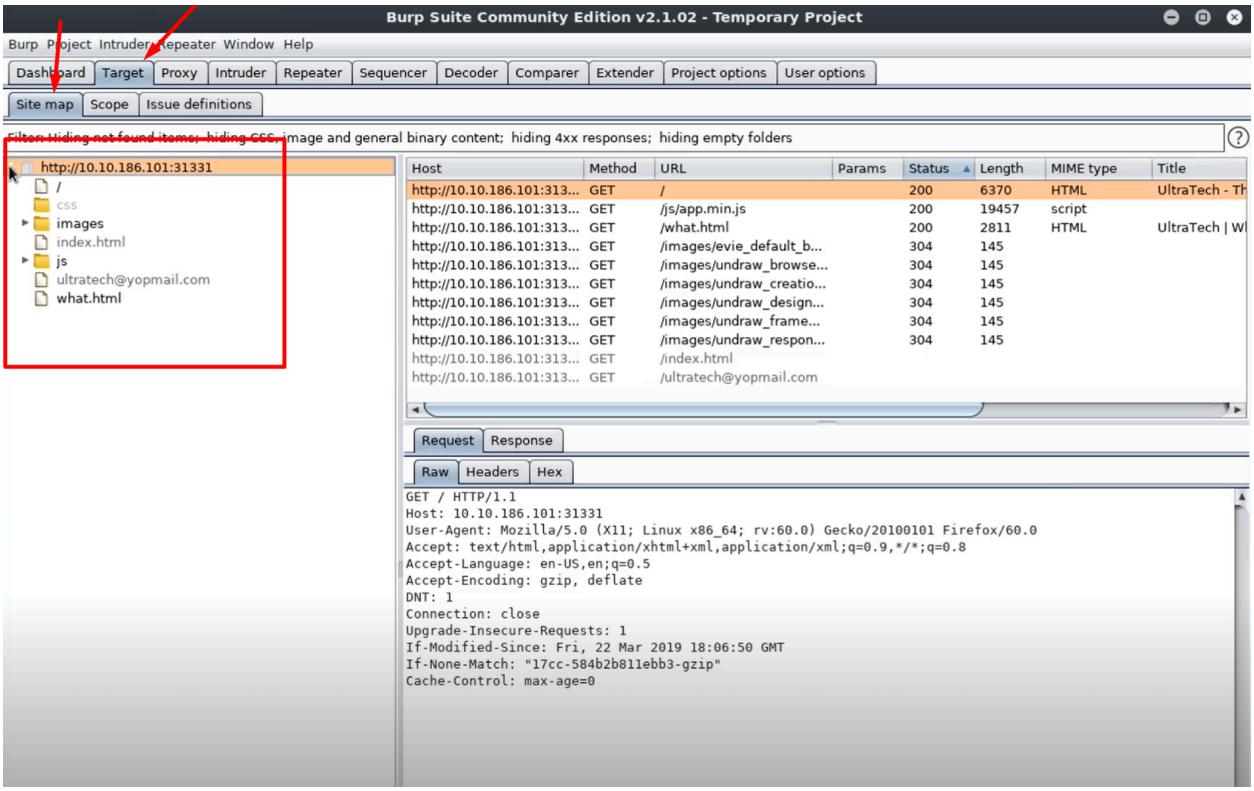
nmap



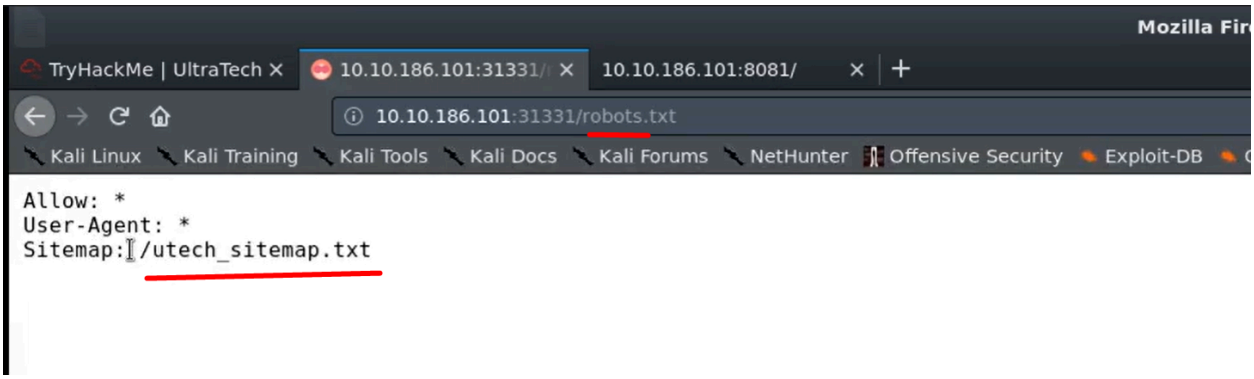
check ports 31331 and 8081

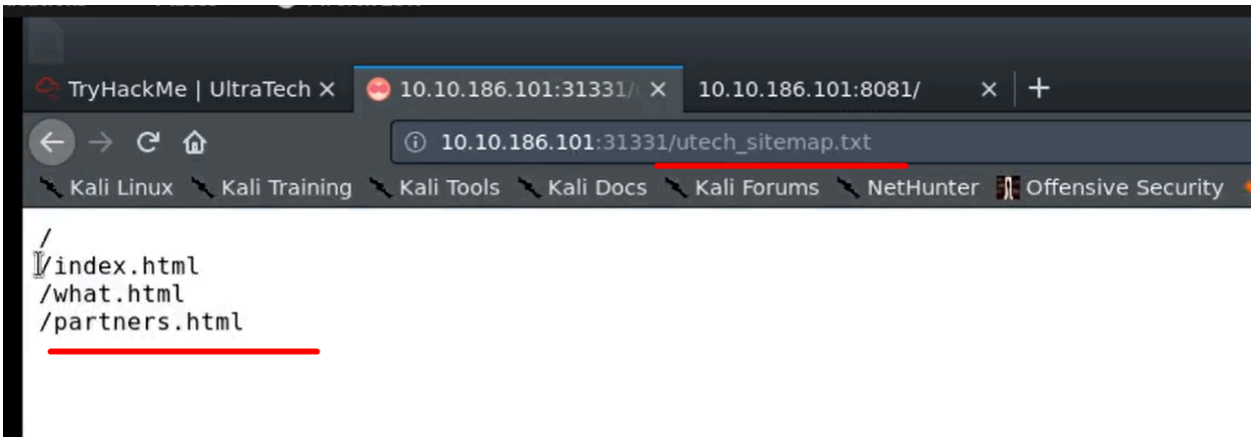


Always turn on intercept on Burp while you testing website. It will crawl the website.

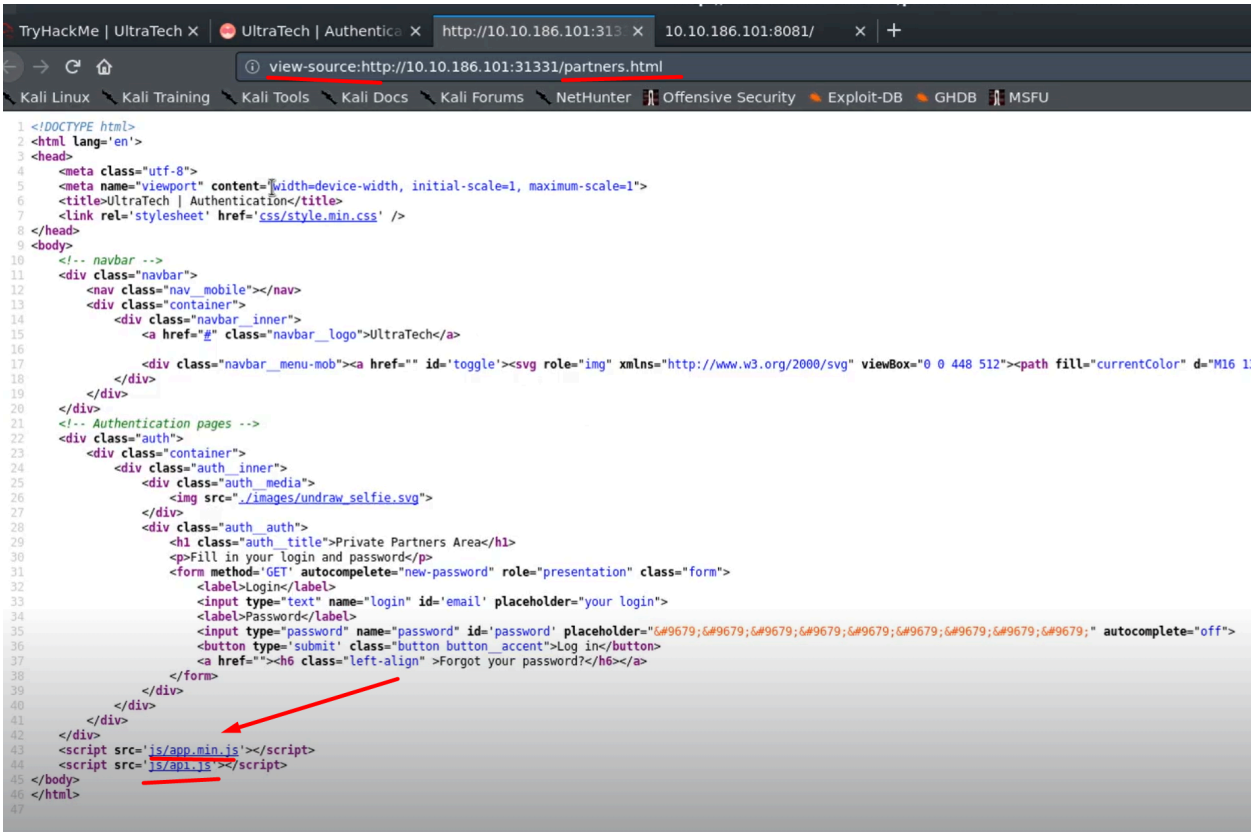


Check robots.txt

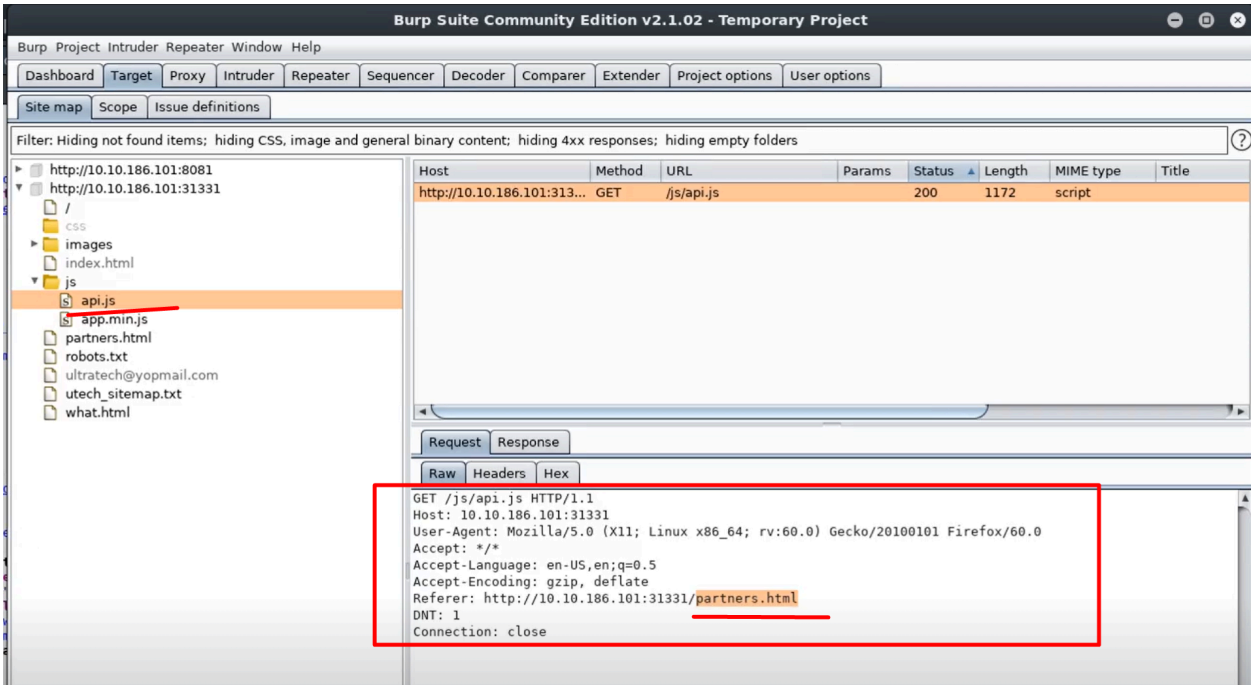




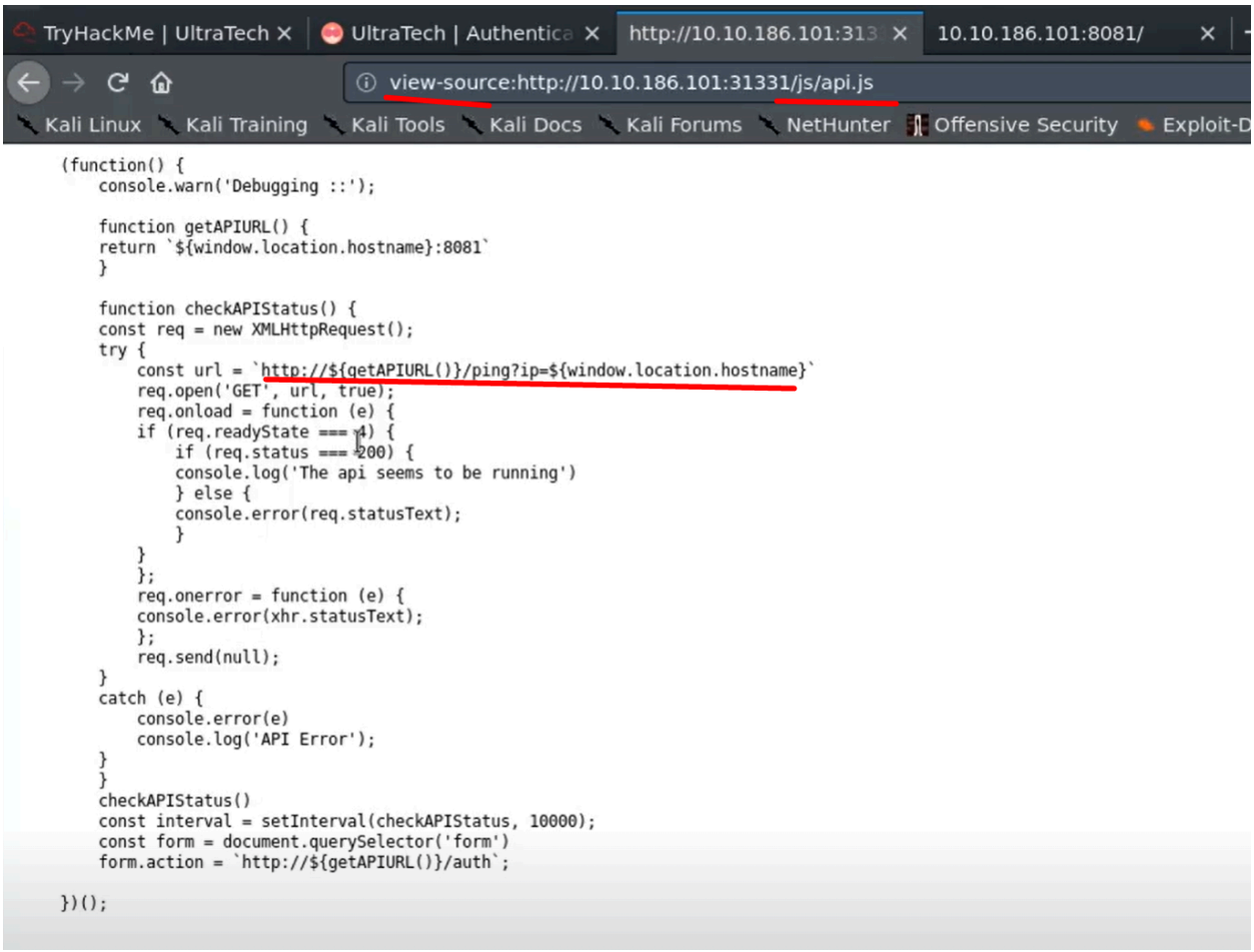
View Page source. It has js api.



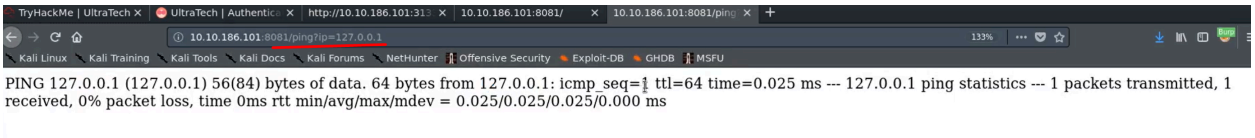
Also can see on Burp



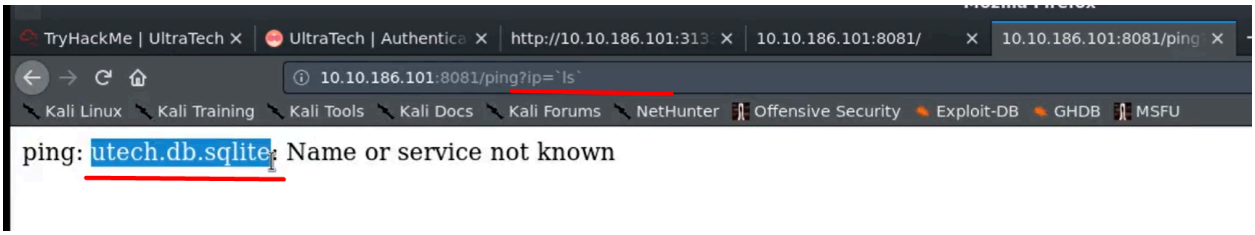
Click on api.js. We saw its running cmd in script.



We can ping. This is cmd execution.



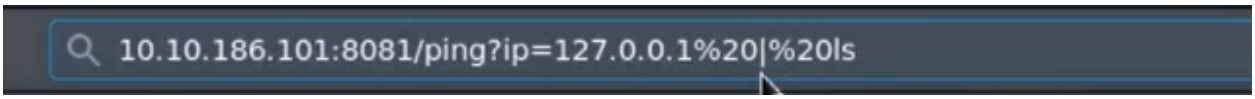
Is. Anything between backticks (`) takes pure precedence (priority) over everything else in the cmd.



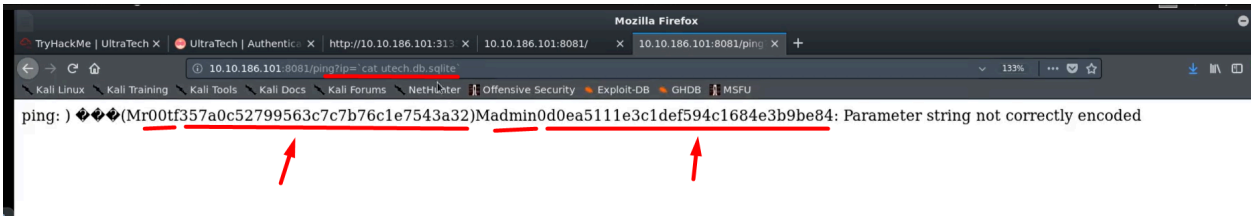
We can also try like this.

%20=space

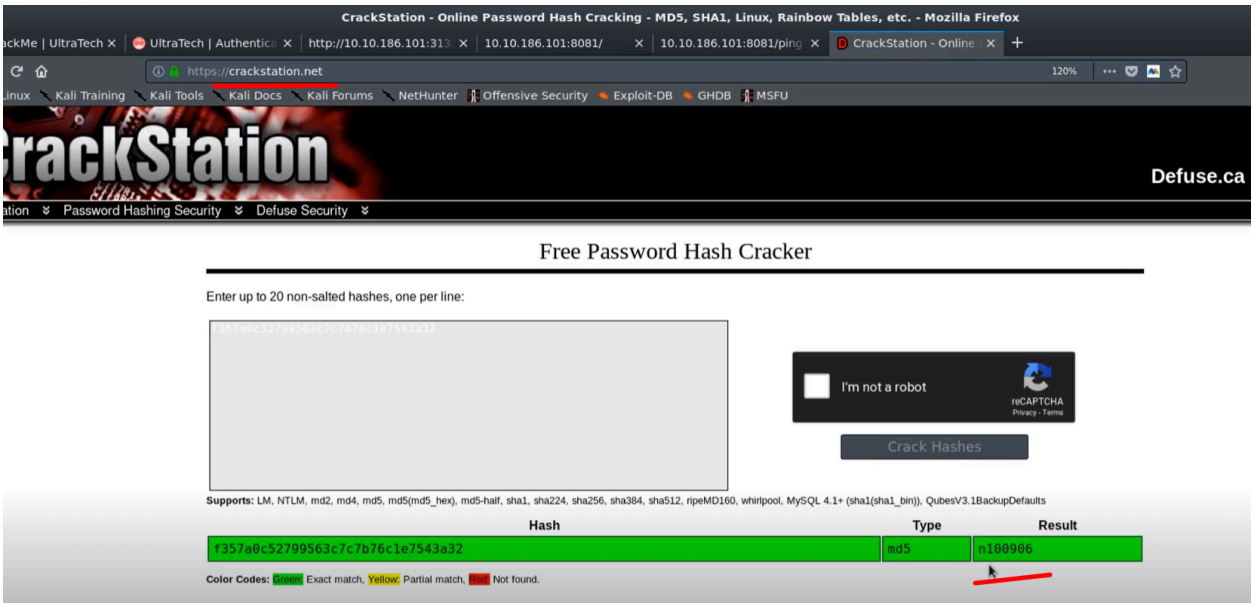
| = pipe



Cat out. These are usernames and their hashes.

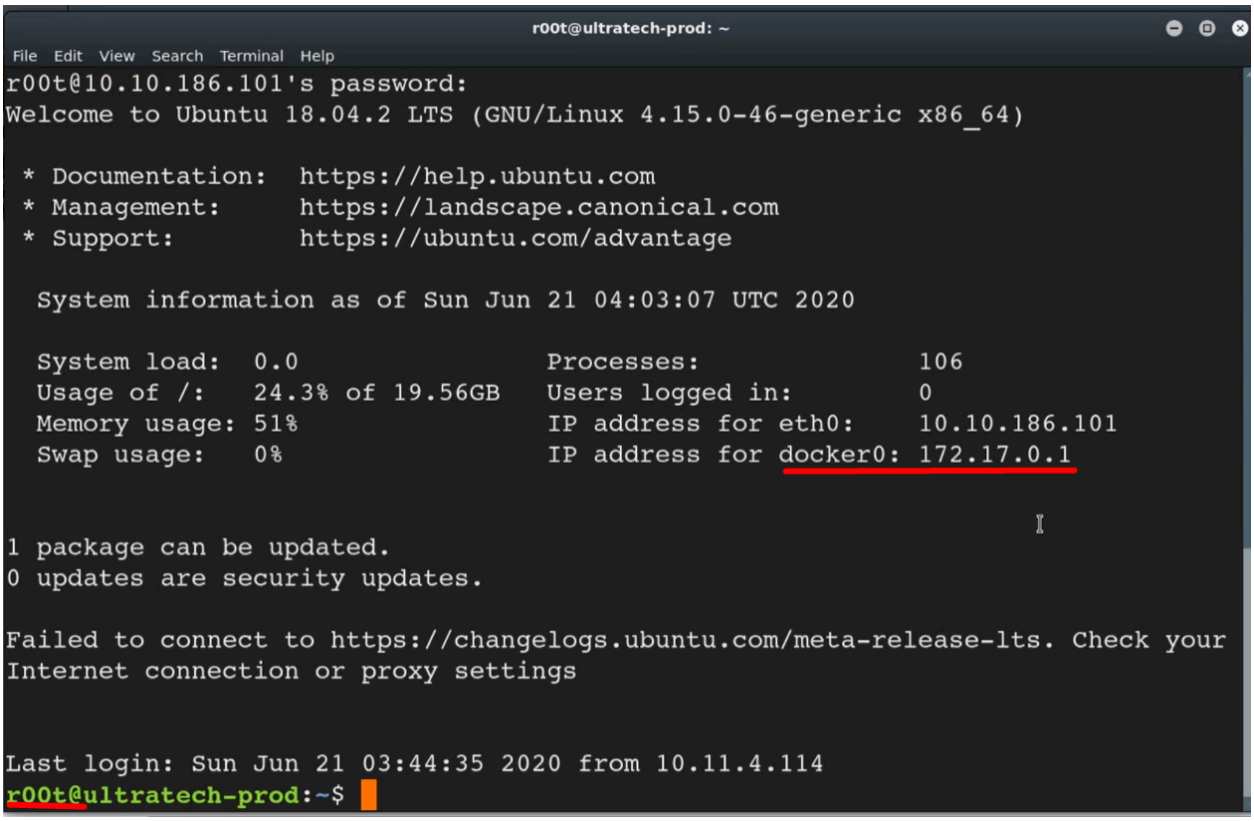


Crack the hash.



Login ssh.

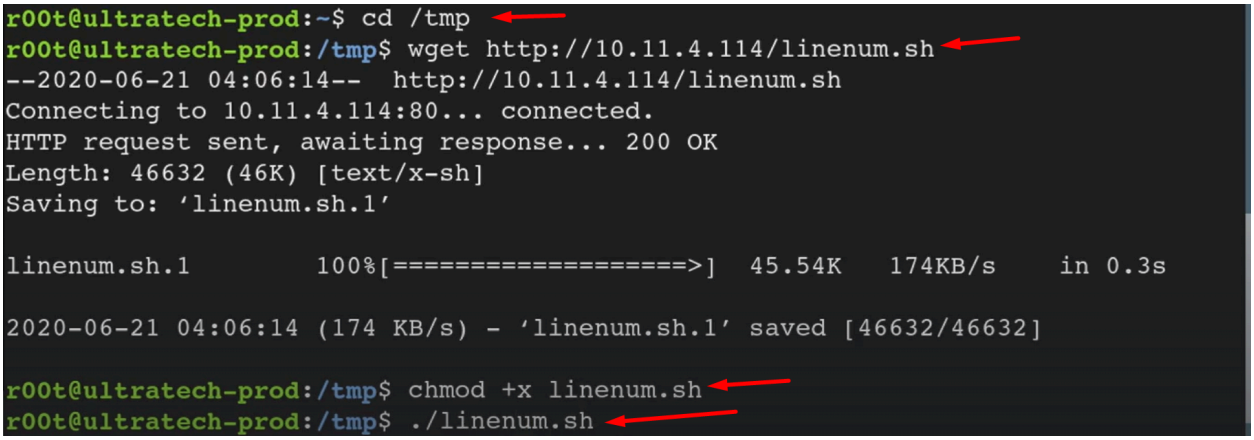
We got user shell. r00t is a user. And the box is running on docker.



Escalation via Docker

Run linenum. Don't forget to host server on kali

```
python -m SimpleHTTPServer 80
wget
```

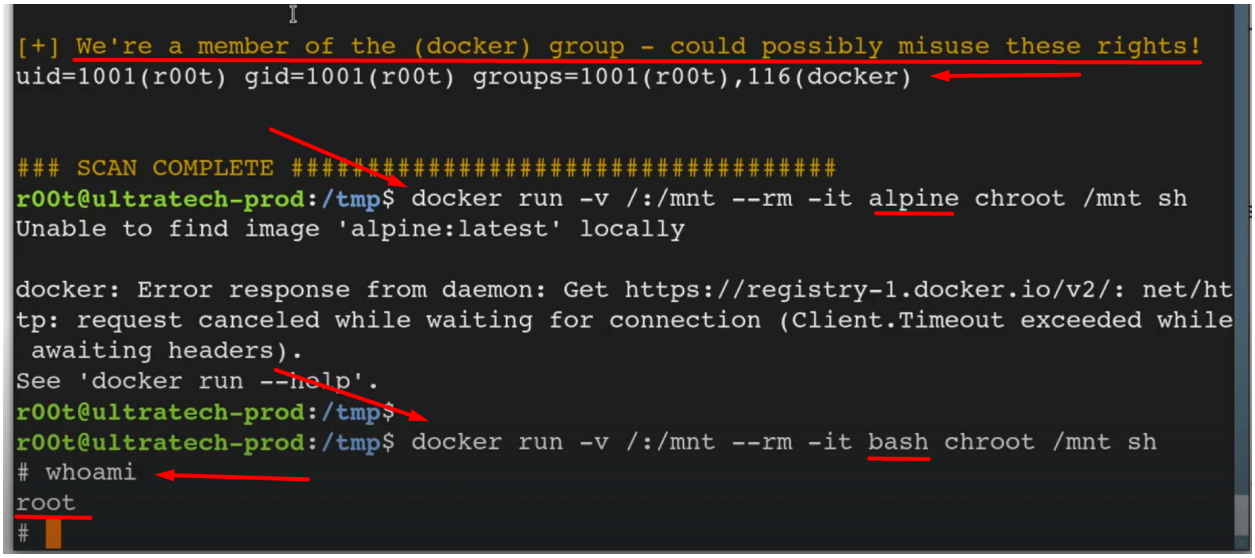


Linenum result

Check docker on gtfobin.

Change alpine to bash. We are not executing alpine. We are executing bash.

```
docker run -v /:/mnt --rm -it bash chroot /mnt sh
```



Now we are root!