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: INT1484-02
TÊN BÀI: ACL – DANH SÁCH ĐIỀU KHIỂN TRUY NHẬP TRÊN LINUX

Sinh viên thực hiện:

B22DCAT063 Lê Tiến Dương

Giảng viên: PGS.TS. Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC BẢNG BIỂU

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 kiểm soát truy cập
DoS	Denial of Service	Tấn công từ chối dịch vụ

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

Danh sách kiểm soát truy cập (Access Control List - ACL) là một công cụ bảo mật mạng quan trọng, được sử dụng để kiểm soát lưu lượng truy cập mạng. Dưới đây là một số lý thuyết cơ bản về ACL:

1.2.1 Định nghĩa và vai trò

- Định nghĩa: ACL là một tập hợp các quy tắc được sử dụng để lọc lưu lượng mạng. Các quy tắc này xác định xem lưu lượng truy cập nào được phép hoặc bị từ chối dựa trên các tiêu chí cụ thể.

- Vai trò:
  - Kiểm soát truy cập: ACL cho phép quản trị viên mạng xác định rõ ràng ai được phép truy cập vào các tài nguyên mạng và những hành động nào họ có thể thực hiện.
  - Bảo mật: ACL giúp bảo vệ mạng khỏi các mối đe dọa bên ngoài và bên trong bằng cách ngăn chặn lưu lượng truy cập trái phép.
  - Quản lý lưu lượng: ACL có thể được sử dụng để ưu tiên hoặc hạn chế lưu lượng truy cập mạng dựa trên các tiêu chí cụ thể.
  - Giám sát: ACL có thể được sử dụng để ghi lại các hoạt động truy cập mạng, giúp quản trị viên theo dõi và phân tích lưu lượng truy cập.

1.2.2 Các loại acl

- ACL tiêu chuẩn (Standard ACLs):
  - Lọc lưu lượng dựa trên địa chỉ IP nguồn.
  - Đơn giản và dễ cấu hình.
  - Thường được đặt gần đích của lưu lượng.
- ACL mở rộng (Extended ACLs):
  - Lọc lưu lượng dựa trên địa chỉ IP nguồn và đích, cổng, giao thức, v.v.
  - Linh hoạt và mạnh mẽ hơn ACL tiêu chuẩn.
  - Thường được đặt gần nguồn của lưu lượng.

1.2.3 Cách thức hoạt động của acl

- ACL hoạt động bằng cách kiểm tra các gói dữ liệu mạng và so sánh chúng với các quy tắc được xác định trong danh sách.
- Nếu một gói dữ liệu phù hợp với một quy tắc, hành động tương ứng (cho phép hoặc từ chối) sẽ được thực hiện.

- ACL xử lý các quy tắc theo thứ tự từ trên xuống dưới. Khi một gói dữ liệu khớp với một quy tắc, quá trình xử lý sẽ dừng lại.

1.2.4 Các thành phần của acl

- Số ACL: Xác định danh sách ACL.
- Điều kiện (Condition): Xác định tiêu chí lọc lưu lượng.
- Hành động (Action): Xác định hành động được thực hiện khi một gói dữ liệu khớp với một điều kiện (cho phép hoặc từ chối).
- Wildcard mask: Được sử dụng để xác định các bit nào trong địa chỉ IP cần được so sánh.

1.2.5 Ứng dụng của acl

- Kiểm soát truy cập vào các tài nguyên mạng như máy chủ, cơ sở dữ liệu, v.v.
- Ngăn chặn các cuộc tấn công mạng như tấn công từ chối dịch vụ (DoS).
- Ưu tiên lưu lượng mạng cho các ứng dụng quan trọng.
- Giám sát và ghi lại các hoạt động truy cập mạng.

1.2.6 Một số điểm cần lưu ý

- Chỉ có thể thiết lập 1 ACL trên giao thức cho mỗi hướng trên mỗi interface.
- Một interface có thể có nhiều ACL.
- Router không thể lọc traffic mà bắt đầu từ chính nó.
- Câu lệnh nào đặt trước thì xử lý trước.
- Khi 1 câu lệnh mới thêm vào danh sách, nó sẽ đặt cuối danh sách.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

- Phần mềm ảo hóa: VMWare Workstation.
- Máy trạm chạy hệ điều hành Linux cài đặt Labtainer.

2.2 Các bước thực hiện

2.2.1 Khởi động bài lab

labtainer acl

```
student@ubuntu:~/labtainer/labtainer-student$ labtainer -r acl

Please enter your e-mail address:  [B22DCAT063]
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
```

Hình 1 – Khởi động bài lab

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

User	Password
bob	password4bob
alice	password4alice
harry	password4harry

Bảng 1. Danh sách tài khoản và mật khẩu

```
acl login: bob
Password:
[bob@acl ~]$
```

Hình 2 – Đăng nhập người dùng bob

```
acl login: alice
Password:
[alice@acl ~]$
```

Hình 3 – Đăng nhập người dùng alice

```
acl login: harry
Password:
[harry@acl ~]$
```

Hình 4 – Đăng nhập người dùng harry

Trong bài thực hành này, sinh viên sẽ sử dụng các lện 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.

2.2.2 Các nhiệm vụ

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

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

cd/shared_data

ls -l

```
[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]$
```

Hình 5 – Liệt kê các quyền trên file, thư mục

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.

```
[alice@acl shared_data]$ cat accounting.txt
some numbers
[alice@acl shared_data]$
```

Hình 6 – Alice có thể xem nội dung file accounting.txt

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

```
[alice@acl shared_data]$ getfacl accounting.txt
# file: accounting.txt
# owner: root
# group: root
user::rw-
user:alice:r--
user:harry:rw-
group::r--
mask::rw-
other::---
```

Hình 7 – Xem acl của file

Người dùng Harry có quyền sửa đổi với file accounting.txt, chuyển đến terminal của Harry thực hiện lệnh:

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

```
[harry@acl ~]$ echo "more stuff" >> /shared_data/accounting.txt
[harry@acl ~]$
```

Hình 8 – Harry sửa đổi file 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.

```
[alice@acl shared_data]$ echo "more stuff" >> /shared_data/accounting.txt
-bash: /shared_data/accounting.txt: Permission denied
[alice@acl shared_data]$
```

Hình 9 – Alice không có quyền sửa đổi file

2.2.2.2 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.

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

Hình 10 – Cho phép alice đọc file

Sau đó, với tư cách là người dùng Alice, hãy xác nhận khả năng đọc tệp này.

```
[alice@acl shared_data]$ cat /shared_data/bob/bobstuff.txt
bob's stuff
[alice@acl shared_data]$
```

Hình 11 – Xác nhận khả năng đọc tệp của alice

Đồng thời, với tư cách là người dùng Harry, hãy xác nhận rằng anh ta thiếu quyền đọc file này.

```
[harry@acl ~]$ cat /shared_data/bob/bobstuff.txt
cat: /shared_data/bob/bobstuff.txt: Permission denied
[harry@acl ~]$
```

Hình 12 – Xác nhận harry thiếu quyền đọc tệp

2.2.2.3 Nhiệm vụ 3: Cài đặt ACL 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 thưc 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.

```
[alice@acl alice]$ echo "Linux" > temp.txt
[alice@acl alice]$
```

Hình 13 – Tạo file

```
[alice@acl alice]$ getfacl temp.txt
# file: temp.txt
# owner: alice
# group: alice
user::rw-
group::rw-
other::---
```

Hình 14 – Kiểm tra quyền

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

```
[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 15 – Cho phép bob đọc các file mới 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?

```
[alice@acl alice]$ echo "abc" > temp2.txt
[alice@acl alice]$
```

Hình 16 – Tạo file mới

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

```
[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::---
```

Hình 17 – Sửa lại acl mặc định trên thư mục alice

Đăng nhập vào Bob và thực hiện kiểm tra lại.

```
[bob@acl ~]$ cat /shared_data/alice/temp2.txt
abc
[bob@acl ~]$
```

Hình 18 – Đăng nhập bob và đọc file

Harry sẽ không đọc được file temp2.txt.

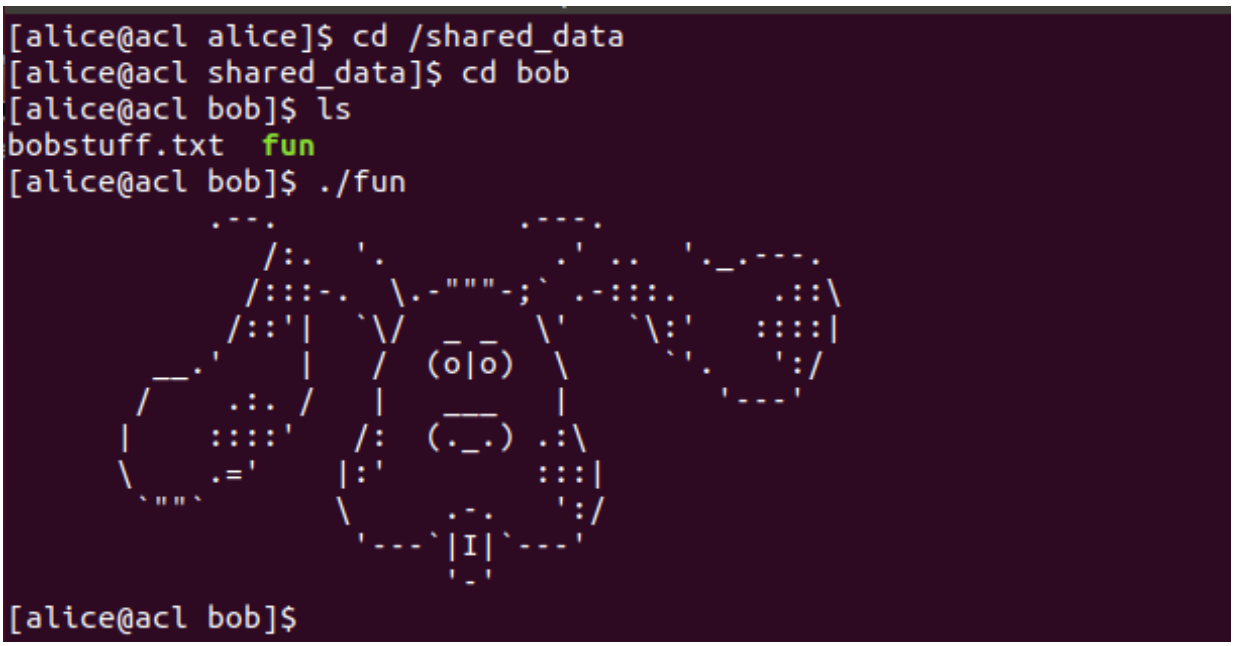
```
[harry@acl ~]$ cat /shared_data/alice/temp2.txt
cat: /shared_data/alice/temp2.txt: Permission denied
[harry@acl ~]$
```

Hình 19 – Harry không đọc được file

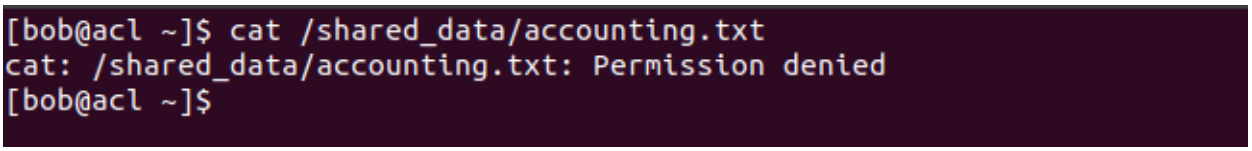
2.2.2.4 Nhiệm vụ 4: Trojan Horses

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.

Lúc đầu khi alice chạy script này, chưa có tệp bản sao được tạo ra, bob vẫn chưa có quyền truy cập vào thông tin.



Hình 20 – Chạy script



Hình 21 – Bob chưa có quyền đọc file

Sửa file fun như sau:

vim fun

Hình 22 – Sửa lại file fun

Cấp quyền cho Alice được tạo file.

```
[bob@acl bob]$ setfacl -m o::rwx /shared_data/bob/
[bob@acl bob]$ getfacl .
# file: .
# owner: bob
# group: bob
user::rwx
group::r-x
other::rwx

[bob@acl bob]$
```

Hình 23 – Cấp quyền tạo file cho alice

Chạy lại script bằng người dùng Alice, thấy một tệp bản sao đã được tạo ra có tên trojan.txt, Bob sẽ có quyền truy cập thông tin của file này.

```
[alice@acl bob]$ ./fun
           .---.             .----.
              /:.  '.         .' ..  '._.---.
             /:::-.  \.-"""-;` .-:::.     .::\
            /::'|  `\/   _ _   \'   `\:'   ::::|
         __.'    |   /  (o|o)  \      `'.    ':/
       /    .:. /   |    ___    |         '---'
      |    ::::'    /:  (._.) .:\
      \    .='     |:'         :::|
       `"""`       \      .-.    ':/
                    '---`|I|`---'
                         '-'
[alice@acl bob]$ ls
bobstuff.txt  fun  trojan.txt
[alice@acl bob]$
```

Hình 24 – Chạy lại script

```
[bob@acl bob]$ cat trojan.txt
some numbers
more stuff
[bob@acl bob]$ rm trojan.txt
[bob@acl bob]$ cat trojan.txt
some numbers
more stuff
[bob@acl bob]$
```

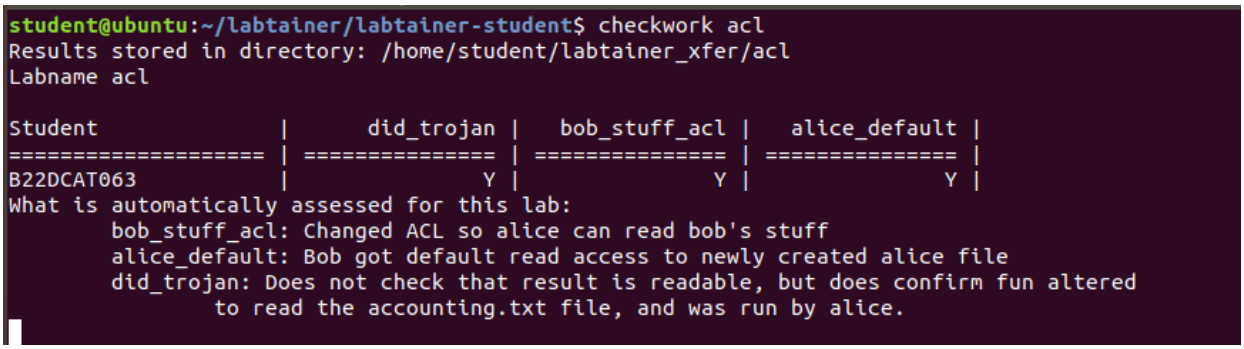
Hình 25 – Bob có quyền truy cập file trojan.txt

2.2.3 Kết thúc lab

stoplab acl

CHƯƠNG 3. KẾT QUẢ THỰC HÀNH

Màn hình checkwork bài thực hành:



Hình 26 – Kết quả checkwork

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] Wikipedia:https://vi.wikipedia.org/wiki/Danh_s%C3%A1ch_%C4%91i%E1%BB%81u_khi%E1%BB%83n_truy_c%E1%BA%ADp