1. Mục đích.

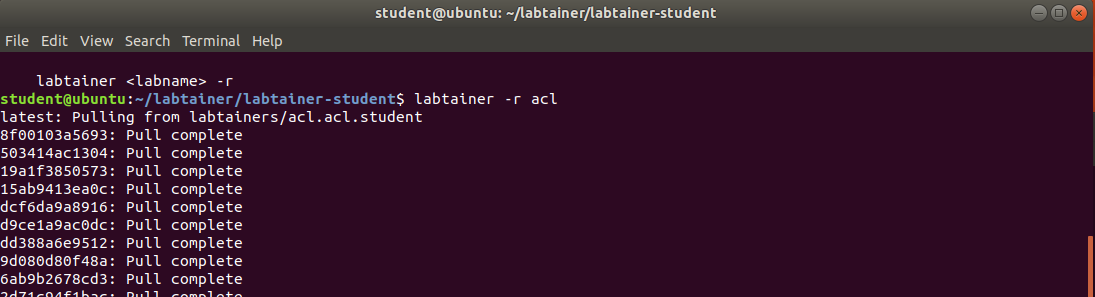
Rèn luyện kỹ năng cấu hình cấp quyền cho người dùng hoặc nhóm người dùng truy cập các tập tin trên hệ thống bằng việc sử dụng danh sách điều khiển truy cập ACL.

2. Yêu cầu đối với sinh viên.

Nắm được kiến thức về điều khiển truy cập trên Linux.

3. Nội dung thực hành.

Khởi động lab: labtainer -r acl



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

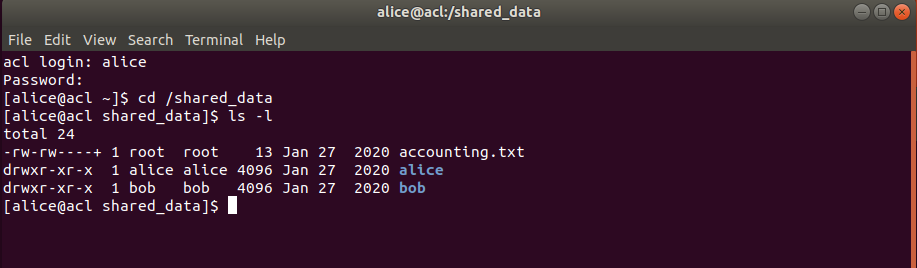
|  |  |
| --- | --- |
| User | Password |
| bob | password4bob |
| alice | password4alice |
| harry | password4harry |

**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:

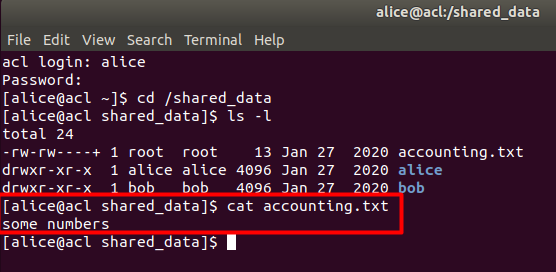
cd /shared\_data

ls -l

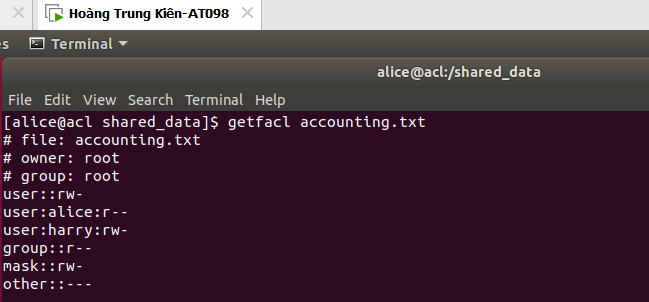


Chúng ta sẽ thấy các quyền trên file accounting.txt và 2 thư mục. Kiểm tra xem“Alice” có thể xem nội dung file accounting.txt hay không? Sử dụng lệnh cat để đọc file

Nhìn lại vào danh sách quyền truy cập các file, thư mục. Lưu ý với file accounting.txt có cài đặt quyền là: -rw-rw----+



Biểu tượng + ở cuối cho biết tệp này có thêm quản lý bằng ACL ngoài các quyền UNIX tiêu chuẩn "rw" cho người dùng và nhóm người dùng. Ta kiểm tra quyền ACL của file này sử dụng lệnh: *getfacl accounting.txt*



**user::rw-**: Mục này áp dụng cho **chủ sở hữu tập tin**. Dấu hai chấm kép (::) biểu thị chủ sở hữu mà không cần chỉ định tên người dùng. Nó cấp quyền **đọc** (r) và **ghi** (w) cho chủ sở hữu

**user:alice:r--**: Mục này áp dụng cho một người dùng cụ thể tên **Alice**. Nó chỉ cấp quyền **đọc** (r) cho Alice, nhưng không có quyền ghi hoặc thực thi.

**user:harry:rw-**: Mục này áp dụng cho một người dùng cụ thể tên **Harry**. Nó cấp quyền **đọc** (r) và **ghi** (w) cho Harry.

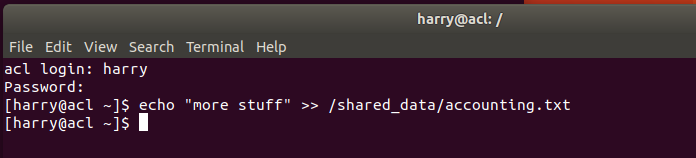
**group::r--**: Mục này áp dụng cho **nhóm tập tin**. Nó chỉ cấp quyền **đọc** (r) cho nhóm, nhưng không có quyền ghi hoặc thực thi.

**mask::rw-**: Mục này định nghĩa **quyền tối đa** có thể được cấp cho người dùng và nhóm (ngoại trừ chủ sở hữu) thông qua các mục ACL riêng lẻ. Ngay cả khi một mục riêng lẻ cho phép quyền ghi, mark có thể giới hạn nó ở chế độ chỉ đọc.

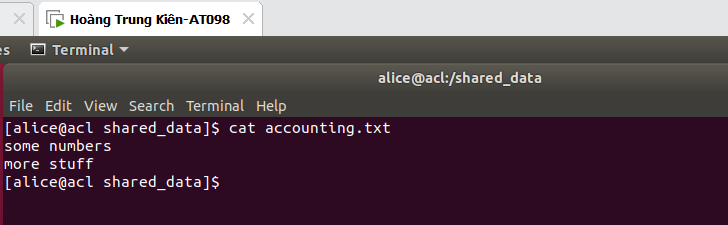
**other::---**: Mục này áp dụng cho **tất cả người dùng khác** không được đề cập rõ ràng trong danh sách. Nó không cấp **quyền nào** (---) cho họ, nghĩa là họ không thể đọc, ghi hoặc thực thi tập tin.

=> Như trên ta thấy hary có quyền w file, 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.

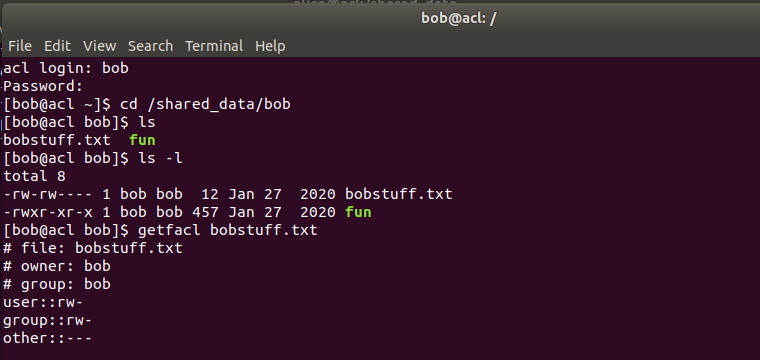


**Nhiệm vụ 2: Cài đặt ACL trên một file**

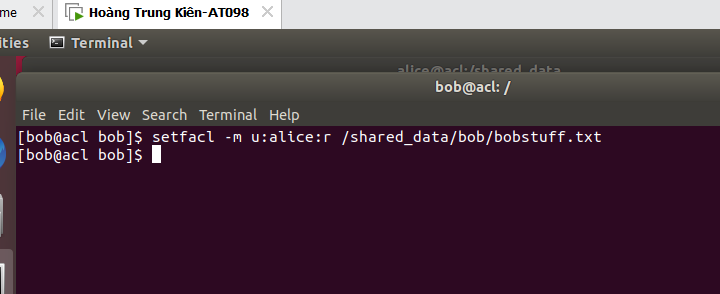
Với tư cách là người dùng Bob, hãy sử dụng lệnh setfacl để cho phép Alice đọc file /shared\_data/bob/bobstuff.txt. Sau đó, với tư cách là người dùng Alice, hãy xác nhận khả năng đọc tệp này. Đồng thời, với tư cách là người dùng Harry, hãy xác nhận rằng anh ta không có quyền đọc file này.

*Setfacl –m “u:alice:r” /shared\_data/bob/bobstuff.txt*

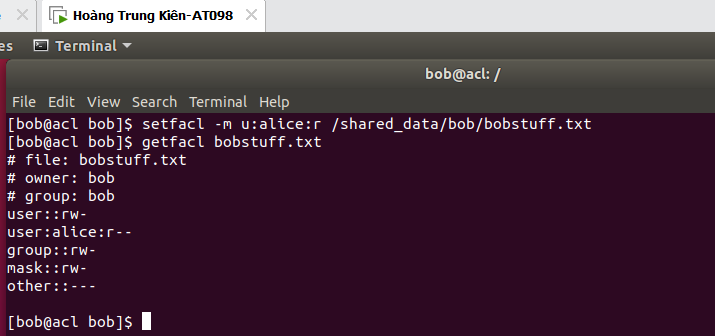
Kiểm tra quyền ACL của file bobstuff.txt

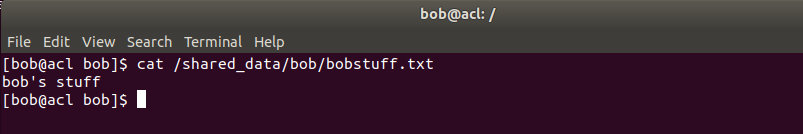


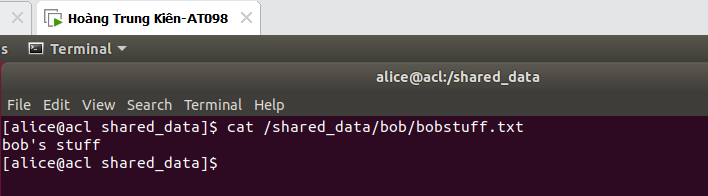
Cấp quyền đọc cho alice



Kiểm tra lại quyền ACL với file bobstuff.txt thì thấy alice đã được cấp quyền đọc file



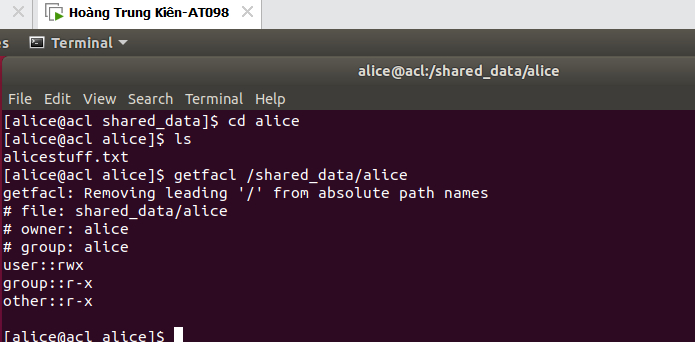
Ta kiểm tra xem alice đã đọc được file bobstuff.txt chưa



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

Với tư cách là người dùng Alice, 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 Alice và Bob thôi.

Kiểm tra quyền acl của thư mục alice

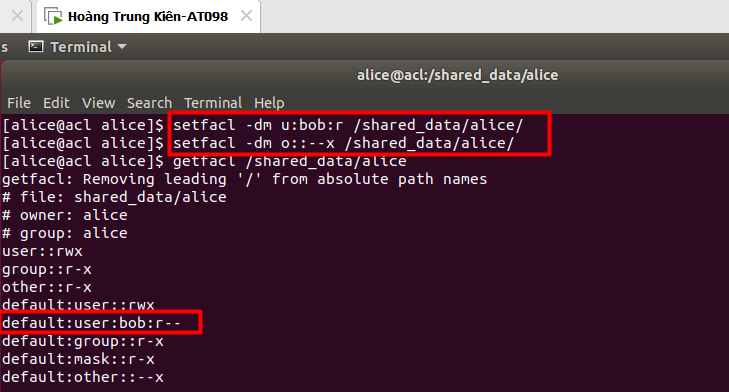


=> Nhận thấy bob không có quyền đọc, ta sẽ thêm quyền đọc cho bob

Đặt ACL mặc định trên thư mục alice để cho phép ngoài Alice chỉ Bob đọc các file mới được tạo:

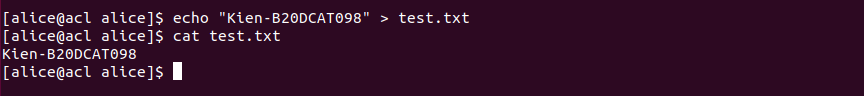
setfacl –dm “u:bob:r” /shared\_data/alice/

setfacl –dm “o::--x” /shared\_data/alice/

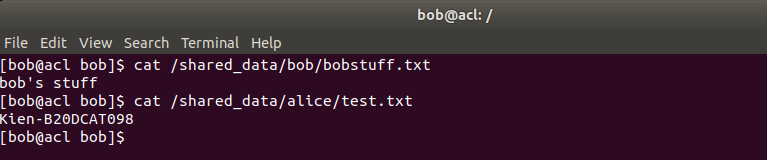


⇒ bob đã có quyền r

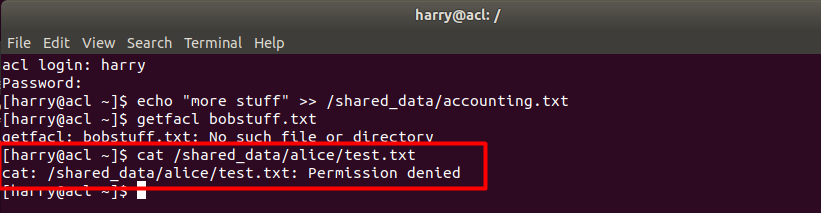
Tạo một file mới khác trong /shared\_data/alice và kiểm tra quyền của nó: Tạo file test.txt trong thư mục alice



Kiểm tra xem bob có quyền đọc file test này không



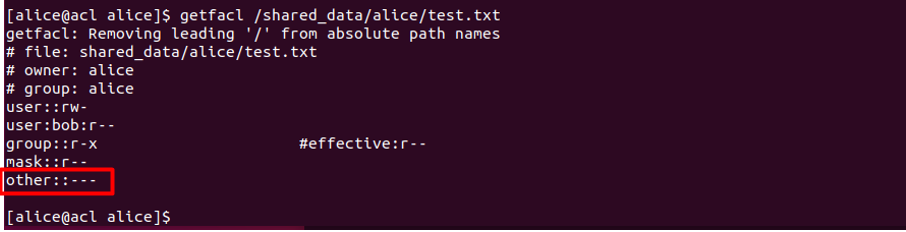
Kiểm tra xem harry có quyền đọc file này không



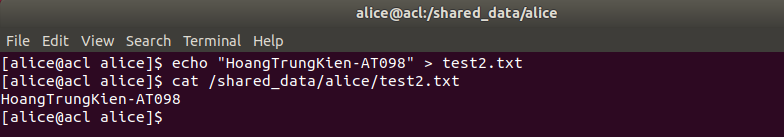
Không có vì ta đã xóa quyền đọc của harry ở trên bằng câu lệnh:

setfacl –dm “o::--x” /shared\_data/alice/

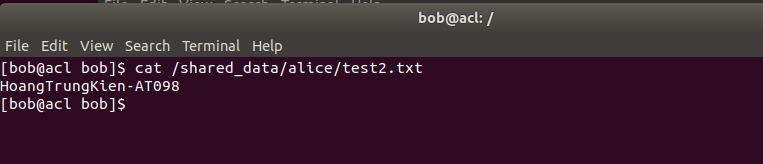
Kiểm tra lại quyền acl với thư mục alice



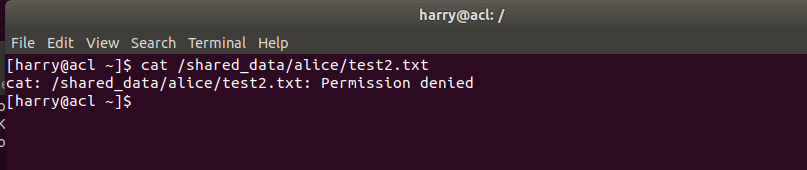
tạo 1 file test2.txt khác



Kiểm tra xem Bob có đọc được không



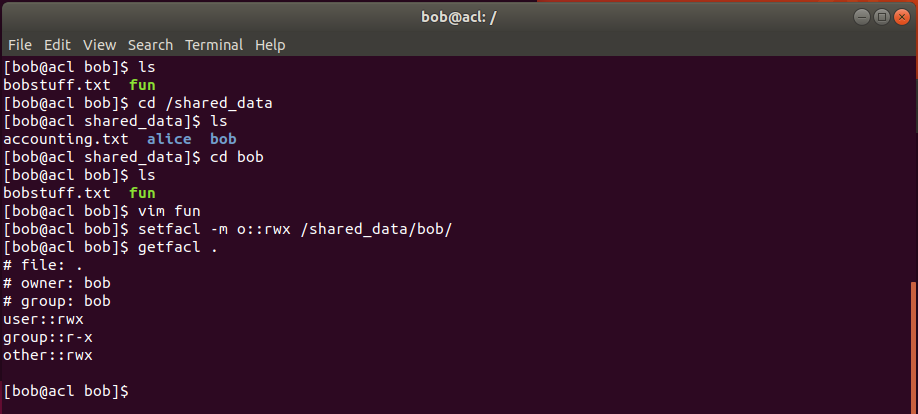
Kiểm tra xem harry có đọc được không



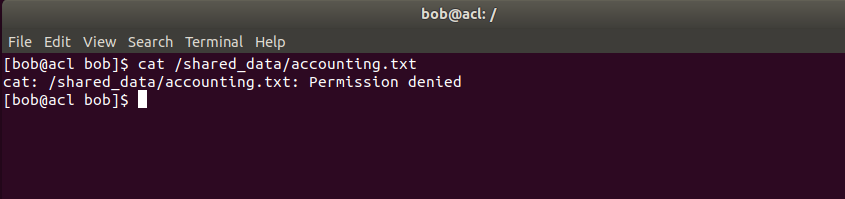
=> Harry không có quyền đọc

Nhiệm vụ 4: Trojan Horses

Kiểm tra lại phân quyền cho file /shared\_data/accounting.txt. Bob không thể đọc file này nhưng anh ý rất muốn biết nội dung của nó. Bob biết Alice kém về nghệ thuật ASCII nên anh ý đã tạo ra một script /shared\_data/bob/fun. Bob sửa script đó sao cho nếu Alice (hay Harry) chạy script này nó sẽ tạo ra một bản sao của file accounting.txt theo một cách nào đó cho phép Bob nhìn thấy nội dung. Cần chắc chắn rằng khi Bob chạy script này, nó không cung cấp cho Bob khả năng truy cập vào dữ liệu. Nhưng khi nó được chạy bởi Alice thì Bob có thể tiếp cận được thông tin. Chúc ý sự khác nhau giữa việc Bob có thể truy cập được file và việc Bob có khả năng tiếp cận được thông tin trong file.



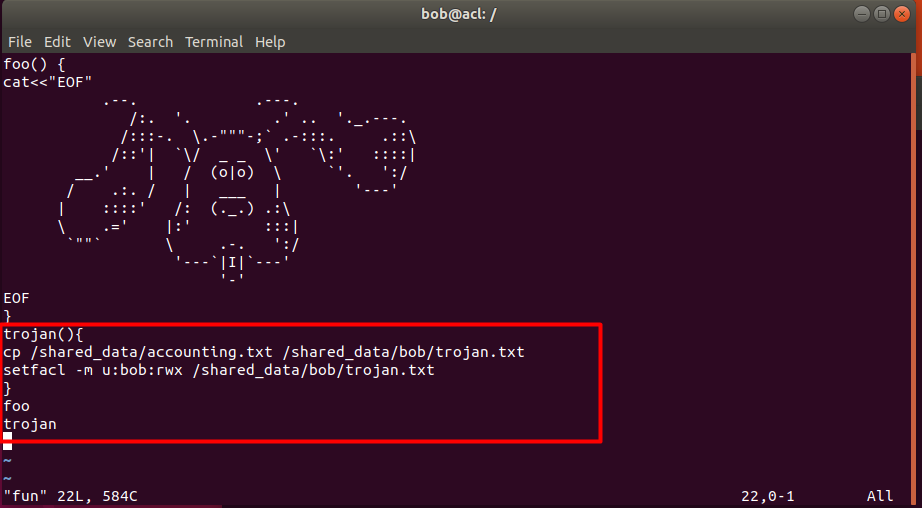
bob không có quyền đọc file accounting.txt



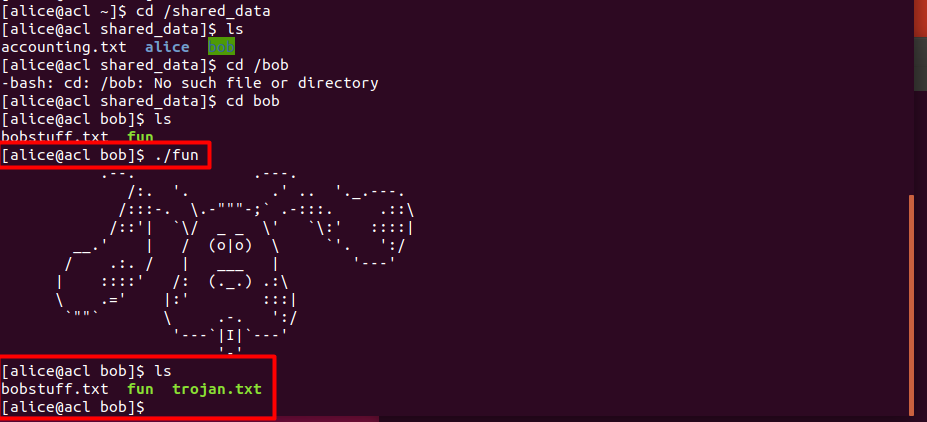
bob tạo trojan để có thể đọc file accounting.txt bằng cách sửa file fun

Gõ vim fun

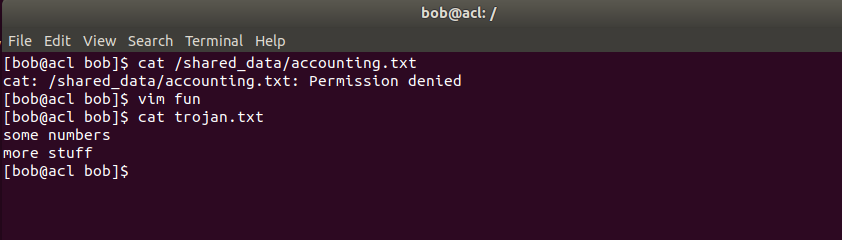
Sửa lại nội dung file như sau:



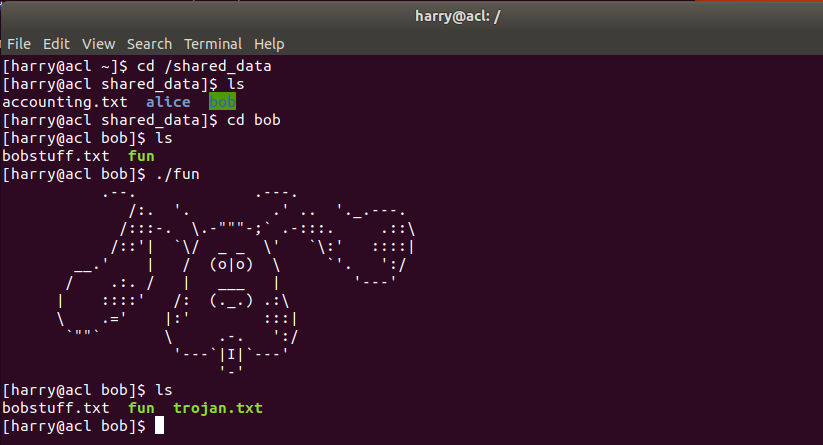
Thực thi file fun bởi alice

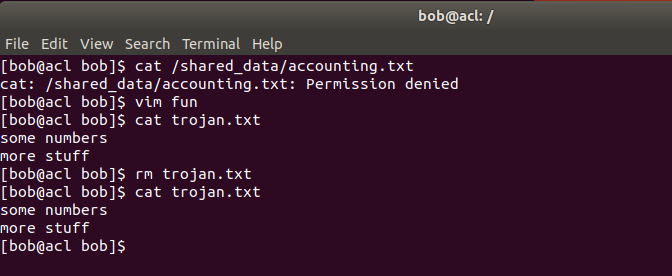


=> nội dung file accounting.txt đã được copy vào file trojan.txt bob có thể đọc được:



Tương tự ta tấn công với người dùng harry vì người dùng harry có quyền đọc file accounting.txt





Checkwork

