Họ tên: Trần Trí Dũng

MSSV: HE190680

Lớp: IA1901

8.1 – Creating a shared group directory

cat mimi\_file.txt

* Kết quả: Lệnh này thất bại với thông báo lỗi "Permission denied"
* Lý do: Tệp mimi\_file.txt được Mimi tạo với quyền 600 (chỉ chủ sở hữu có quyền đọc/ghi) và ACL chỉ cho phép mrgray đọc tệp. Mommy không phải là chủ sở hữu và không được cấp quyền trong ACL nên không thể đọc tệp này.

cat mr\_gray\_file.txt

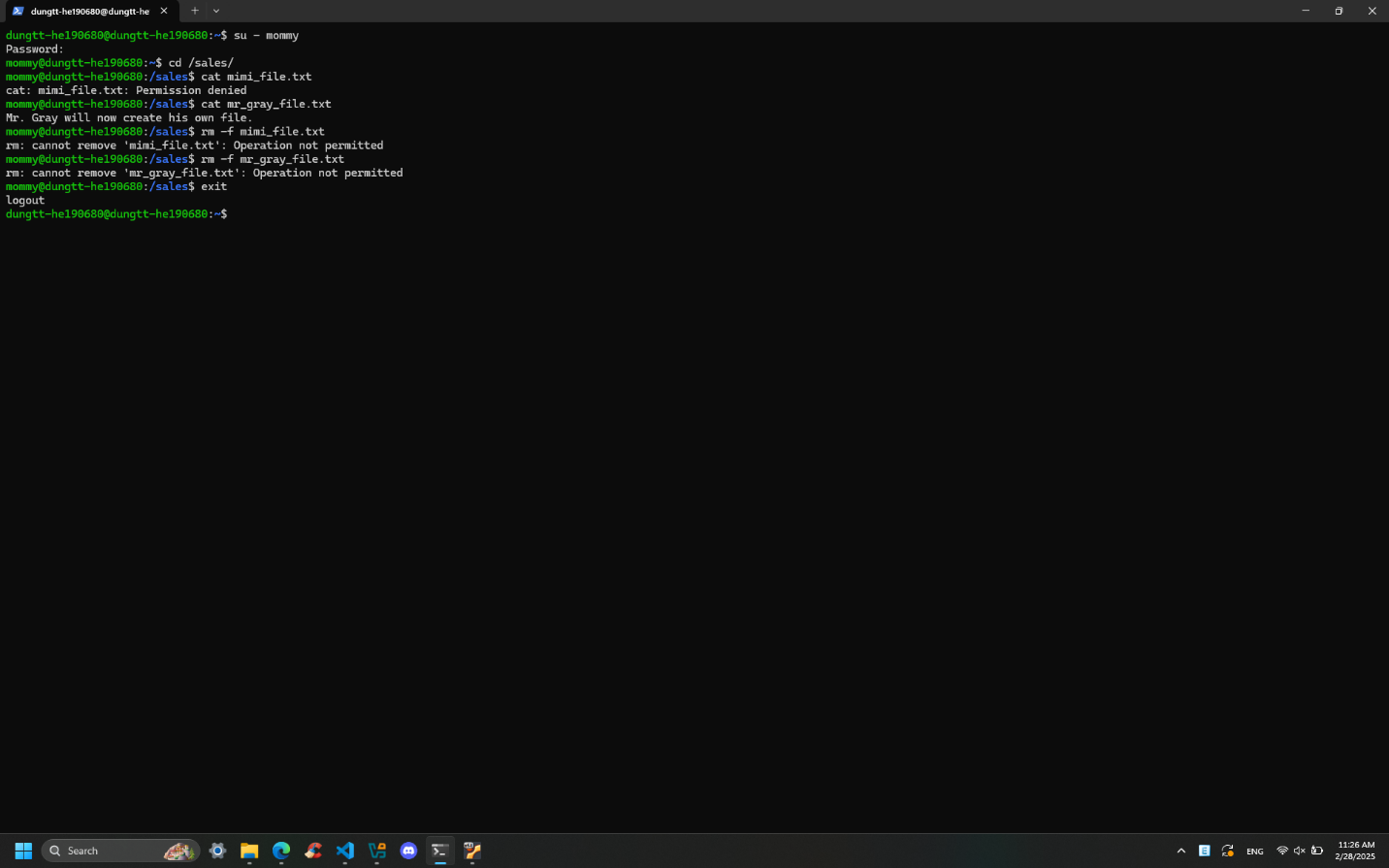
* Kết quả: Hiển thị nội dung "Mr. Gray will now create his own file."
* Lý do: Khi mr\_gray tạo tệp trong thư mục /sales, tệp sẽ được tạo với quyền mặc định. Vì thư mục /sales có SGID bit (2), các tệp mới được tạo sẽ kế thừa nhóm sales. Người dùng mommy thuộc nhóm sales nên có thể đọc tệp nếu quyền nhóm cho phép đọc.

rm -f mimi\_file.txt

* Kết quả: Lệnh này thất bại với thông báo "Operation not permitted"
* Lý do: Thư mục /sales được thiết lập với sticky bit (1), điều này có nghĩa là chỉ chủ sở hữu của tệp, chủ sở hữu của thư mục, hoặc root mới có thể xóa tệp. Mommy không phải là chủ sở hữu của tệp mimi\_file.txt nên không thể xóa nó.

rm -f mr\_gray\_file.txt

* Kết quả: Lệnh này cũng thất bại với thông báo "Operation not permitted"
* Lý do: Tương tự như trên, do sticky bit trên thư mục /sales, mommy không thể xóa tệp của mr\_gray dù có thể đọc nó.



8.2 – SELinux type enforcement

tmp\_t là loại SELinux mới được gán cho tệp, thay thế cho loại ban đầu là httpd\_sys\_content\_t (loại mặc định cho nội dung web của Apache).

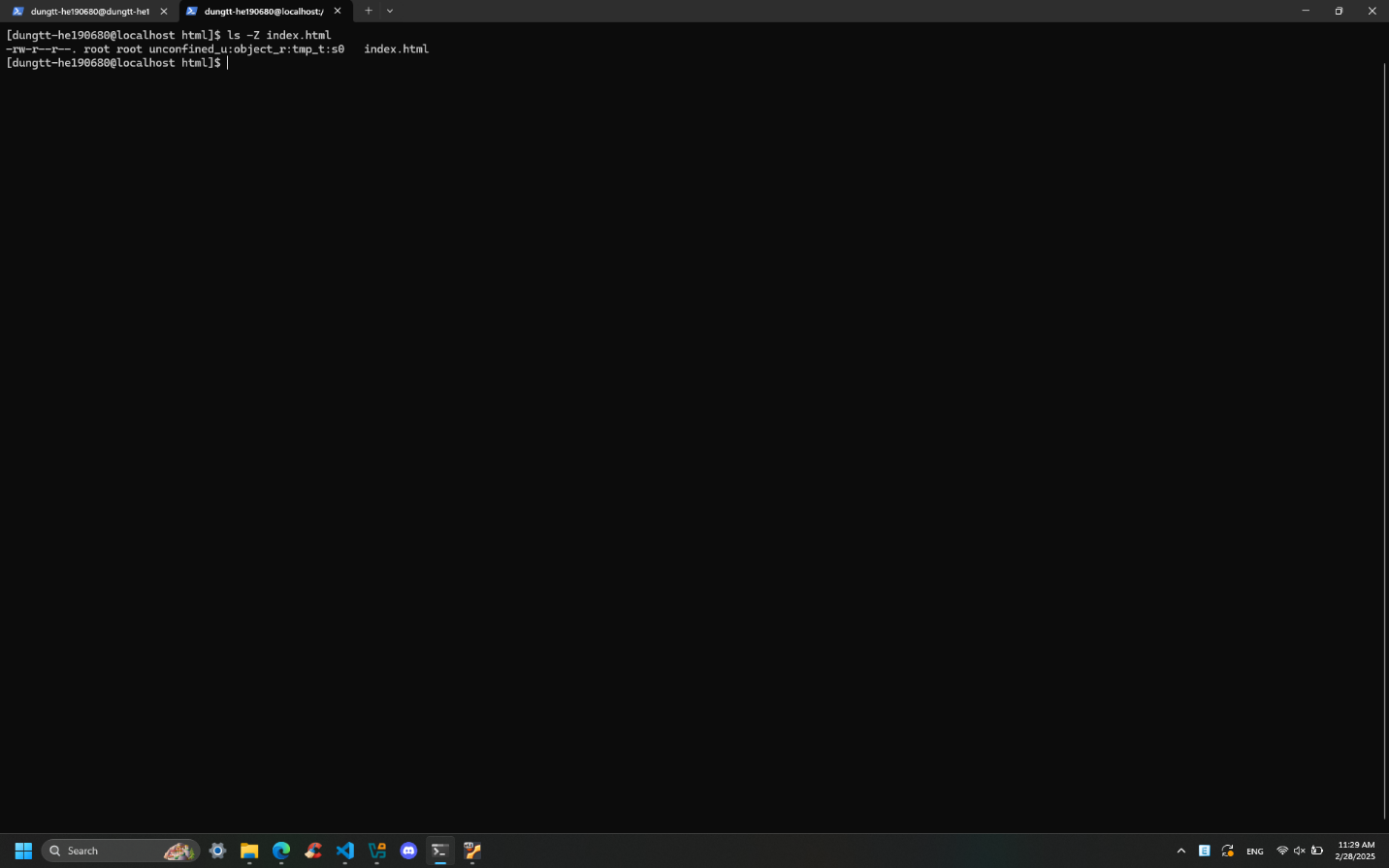
httpd\_sys\_content\_t là loại SELinux được thiết kế đặc biệt cho các tệp nội dung web mà Apache được phép đọc và phục vụ.

tmp\_t là loại SELinux dành cho các tệp tạm thời, thường được sử dụng trong thư mục /tmp và các vùng tạm thời khác.

Khi tệp index.html có loại tmp\_t, Apache sẽ không còn có quyền đọc tệp này theo chính sách SELinux.

Điều này sẽ dẫn đến việc trang web không thể truy cập được nữa, mặc dù các quyền tệp thông thường (DAC - Discretionary Access Control) vẫn cho phép Apache đọc tệp.

Nếu thử truy cập trang web sau thay đổi này thì sẽ nhận được lỗi 403 Forbidden hoặc tương tự.



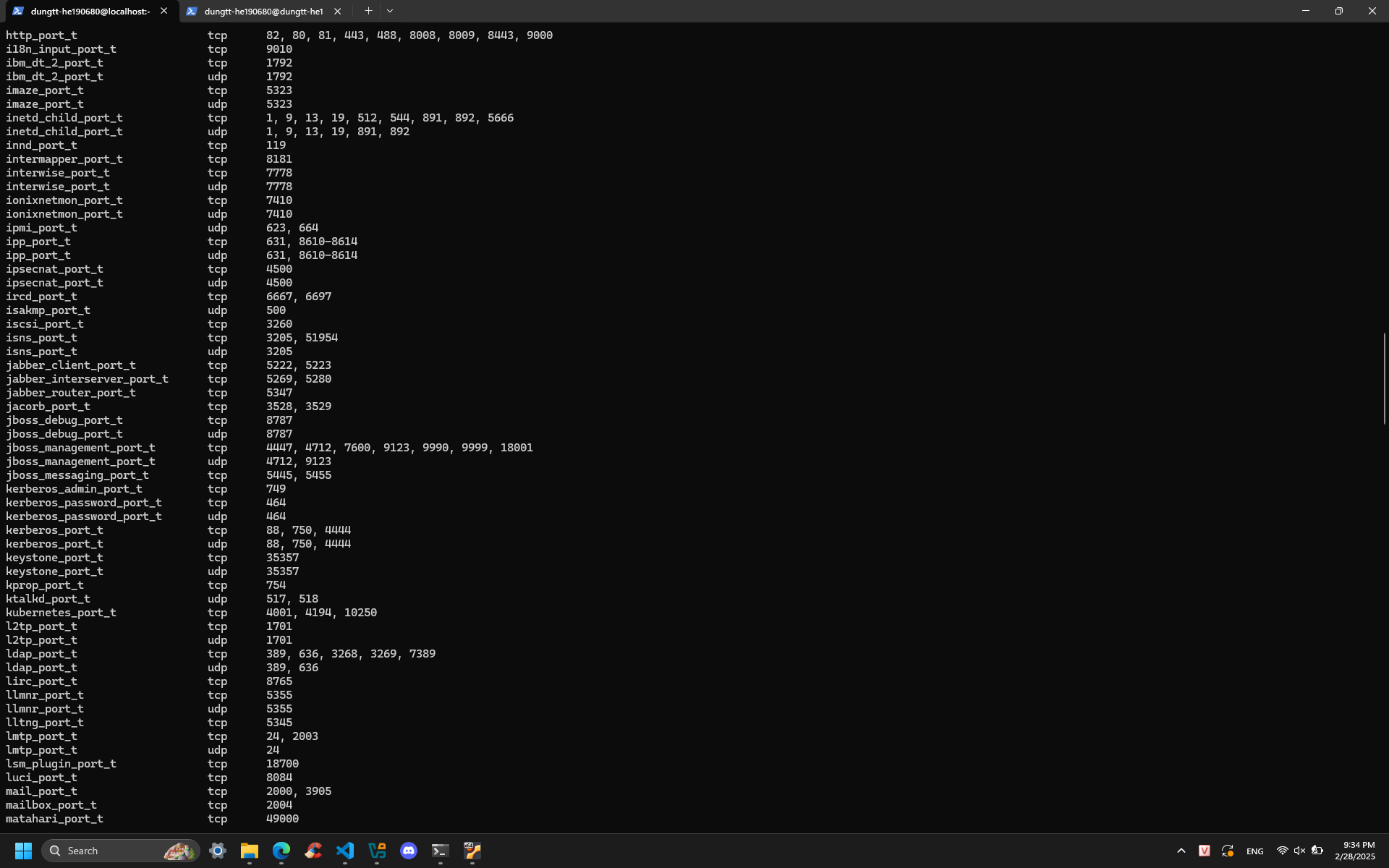
9.1 – SELinux Booleans and ports

Cổng 82 đã được thêm vào danh sách các cổng được gán loại http\_port\_t. Điều này có nghĩa là Apache (và các dịch vụ web khác) giờ đây được phép lắng nghe trên cổng 82 theo chính sách SELinux.

http\_port\_tlà loại SELinux được sử dụng để xác định các cổng mà các dịch vụ web như Apache được phép sử dụng. Các cổng tiêu chuẩn như 80 (HTTP) và 443 (HTTPS) mặc định đã được gán loại này.

Ngoài cổng 82 mới thêm vào, có các cổng khác đã được cấu hình sẵn cho http\_port\_t như 80, 81, 443, 488, 8008, 8009, 8443, 9000, v.v.

Trước khi thêm cổng 82, Apache không thể lắng nghe trên cổng này vì SELinux ngăn chặn điều đó, ngay cả khi cấu hình Apache đã được thay đổi. Sau khi thêm cổng 82 vào danh sách được phép, Apache có thể khởi động thành công và lắng nghe trên cổng này.



9.2 – Troubleshooting an AppArmor profile

Lệnh apparmor\_status | grep smbd hiển thị các tiến trình liên quan đến Samba (smbd) đang được giám sát và quản lý bởi AppArmor.

Có ba tiến trình /usr/sbin/smbd với các PID khác nhau (848, 877, 878) đang hoạt động. Đây là bình thường vì Samba thường tạo nhiều tiến trình để xử lý các kết nối khác nhau.

Ngoài ra còn có tiến trình /usr/lib/x86\_64-linux-gnu/samba/samba-bgqd (PID 881) cũng đang chạy dưới sự kiểm soát của AppArmor. Đây là một thành phần của Samba chịu trách nhiệm cho các tác vụ nền.

