Hook netfilter

Tạo ra mã nguồn của một module nhân Linux đơn giản để tạo ra một bộ tường lửa. Mục đích của bộ tường lửa này là chấp nhận các gói tin từ PC của giám đốc và localhost, còn lại sẽ bị chặn.

Các phần quan trọng của mã nguồn:

1. Các tệp tin header được include để sử dụng các hàm và định nghĩa cấu trúc liên quan đến việc xử lý gói tin và tường lửa.

A picture containing text, screenshot, font, design

Description automatically generated

1. Một biến director\_ip (kiểu char\*) được khai báo như một module parameter, cho phép người dùng cung cấp địa chỉ IP của PC giám đốc khi tải module.

A screen shot of a computer

Description automatically generated with low confidence

1. Hàm init\_firewall\_module khởi tạo cấu trúc nf\_hook\_ops nfho và đăng ký hook hook\_func để được gọi khi có gói tin đi qua. Hàm này được gọi khi module được tải vào nhân.

A screen shot of a computer program

Description automatically generated with medium confidence

1. Hàm cleanup\_firewall\_module được gọi khi module được gỡ khỏi nhân, hủy đăng ký hook đã được đăng ký.

A black background with white text

Description automatically generated with low confidence

1. Hàm hook\_func được gọi khi có gói tin đi qua, xử lý chính sách chấp nhận hoặc chặn gói tin dựa trên địa chỉ IP nguồn.

A screen shot of a computer program

Description automatically generated with low confidence

Các bước xử lý chính trong hook\_func:

1. Lấy thông tin header của gói tin IP và TCP.
2. Chuyển đổi địa chỉ IP của PC giám đốc từ chuỗi sang dạng số nguyên.
3. Kiểm tra nếu gói tin đến từ localhost (127.0.0.1) hoặc một địa chỉ IP bất kỳ (0.0.0.0), nếu đúng thì chấp nhận gói tin và in thông báo.
4. Kiểm tra nếu gói tin đến từ PC của giám đốc, nếu đúng thì chấp nhận gói tin và in thông báo.
5. Chặn tất cả các gói tin khác và in thông báo.
6. Cuối cùng, các macro module\_init và module\_exit được sử dụng để chỉ định hàm khởi tạo và dọn dẹp cho module này.