Nhóm 7 (vắng Huỳnh Ngọc Bảo Châu 21520643)

Câu 1. Giả sử một ACL chứa những luật sau để xử lý các gói tin đi vào mạng. Luật này có hợp lý và bảo mật?

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Int addr | Int port | Ext addr | Ext port | Action | Comments |
| \* | 25 | \* | \* | allow | Allow ingress SMTP packets |

Luật này cho phép tất cả gói tin SMTP trên port 25 được truy cập vào mạng nội bộ từ bất kỳ địa chỉ IP nào bên ngoài mạng.

Luậ này không hợp lý và không có bảo mật vì port 25 dễ gặp phải các vấn đề như port 25 thường được sử dụng để gửi email spam. Kẻ tấn công có teh63 sử dụng botnet để gửi hàng loạt các email spam qua port này. Hơn thế nữa port này còn dễ bị tấn công DDoS bằng cách gửi lưu lượng truy cập đến port 25 trên máy chủ email, làm cho máy chủ không thể xử lý được các yêu cầu đến và từ đó làm gián đoạn dịch vụ.

Câu 2. Vùng DMZ chứa 3 server. Địa chỉ IP của router ngoài, router trong và các server như trong hình. Xây dựng các luật ACL sao cho các host ngoại vi có thể trực tiếp truyền thông với các server trong vùng DMZ, nhưng không thể thực hiện truyền thông với bất các host trong vùng mạng nội bộ.

Ảnh có chứa văn bản, biểu đồ, Phông chữ, ảnh chụp màn hình

Mô tả được tạo tự động

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Int addr | Int port | Ext addr | Ext port | Action | Comments |
| 192.63.16.4 | \* | \* | \* | allow | Cho phép truy cập tới web server |
| 192.63.16.5 | \* | \* | \* | allow | Cho phép truy cập tới SMTP server |
| 192.63.16.6 | \* | \* | \* | allow | Cho phép truy cập proxy server |
| 192.63.8.2 | \* | 192.63.8.1 | \* | block | Không cho phép truy cập tới vùng mạng LAN |
| 192.63.8.3 | \* | 192.63.8.1 | \* | block | Không cho phép truy cập tới vùng mạng LAN  interval |