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 |

* Int address = “none”: Có nghĩa là không có ràng buộc về địa chỉ nguồn nội bộ. Bạn đang cho phép mọi địa chỉ nguồn từ bất kỳ nơi nào.
* Int Port = “25”: Port nguồn được thiết lập là 25. 25 là port mặc định cho giao thức SMTP, vì vậy chỉ có gói tin đi từ port này mới được chấp nhận.
* Ext address = “none”: Tương tự như địa chỉ nguồn, không có ràng buộc về địa chỉ đích. Gói tin có thể đi đến bất kỳ địa chỉ nào.
* Ext port = “None”: Không có ràng buộc về cổng đích. Gói tin có thể đi đến bất kỳ cổng nào.
* Action = “allow”: Hành động được đặt là "allow", cho phép gói tin đi qua nếu nó tuân theo các điều kiện được xác định.
* Comments = “Allow ingress SMTP packets”: Ghi chú này mô tả mục đích của luật: cho phép gói tin SMTP đi vào mạng.
* Luật này không hợp lý và bảo mật vì tất cả mọi máy đều có thể tham gia vào mạng với internal port là 25, thay vì SMTP là một máy cố định.

Câu 2:

* Router and packet filter 1: cấm hết chỉ cho vào vùng dmz

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Int addr | Int port | Ext addr | Ext port | Action | Comment |
| 192.63.16.4 | 80, 443 | \* | \* | Allow | Open internal HTTP/HTTPS port |
| 192.63.16.5 | 25, 587, 465 | \* | \* | Allow | Open internal SMTP, SMTPs port |
| 192.63.16.6 | \* | \* | \* | Allow | Open internal all port |
| \* | \* | \* | \* | Block | Block packets from all port |

* Router and packet filter 2: cấm hết chỉ cho vào vùng dmz

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Int addr | Int port | Ext addr | Ext port | Action | Comment |
| 192.63.16.4 | 80, 443 | \* | \* | Allow | Open internal HTTP/HTTPS port |
| 192.63.16.5 | 25, 587, 465 | \* | \* | Allow | Open internal SMTP, SMTPs port |
| 192.63.16.6 | \* | \* | \* | Allow | Open internal all port |
| \* | \* | \* | \* | Block | Block packets from all port |