**Họ và tên: Tăng Dũng Cẩm**

**MSSV: 22520141**

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

Ý nghĩa của danh sách ACL: Cho phép bất kì gói tin SMTP có cổng 25 từ bên ngoài được vào mạng nội bộ, không phân biệt từ nguồn nào và đích.

* Danh sách ACL trên hợp lí đối với mạng cần cung cấp dịch vụ SMTP, khi đó cổng 25 cần được cho phép để hệ thống hoạt động.
* Vì thiếu các điều kiện ràng buộc IP bên ngoài (\* tương ứng với bất kì địa chỉ nào), mọi nguồn bên ngoài đều có thể gữi gói SMTP. Điều đó tạo cơ hội cho các cuộc tấn công spam mail, làm tăng lưu lượng mạng và tốn tài nguyên, các email chứa mã độc gây nguy hiểm cho hệ thống. Vì thế danh sách ACL trên có tính bảo mật kém.

**Bài 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 trực tiếp với bất kỳ host nào trong vùng mạng nội bộ.**

**Cấu hình trên router ngoài mạng nội bộ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **int addr** | **int port** | **ext addr** | **ext port** | **action** | **comments** |
| 192.63.16.4 | 80 | \* | \* | allow | Cho phép HTTP từ ngoại vi vào Webserver |
| 192.63.16.4 | 443 | \* | \* | allow | Cho phép HTTPS từ ngoại vi vào SMTP server |
| 192.63.16.5 | 25 | \* | \* | Allow | Cho phép SMTP từ ngoại vi vào SMTP server |
| 192.63.16.6 | 80 | \* | \* | Allow | Cho phép HTTP từ ngoại vi vào máy chủ Proxy |
| 192.63.16.6 | 443 | \* | \* | Allow | Cho phép HTTPS từ ngoại vi vào máy chủ Proxy |
| 192.63.8.0/24 | \* | \* | \* | Deny | Chặn tất cả truy cập trừ ngoại vi đến mạng nội bộ |
| \* | \* | \* | \* | Allow | Cho phép tất cả các truy cập còn lại vào DMZ |

**Cấu hình trên router trong mạng nội bộ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **int addr** | **int port** | **ext addr** | **ext port** | **action** | **comments** |
| 192.63.8.0/24 | \* | 192.63.16.0/24 | \* | allow | Cho phép mạng nội bộ kết nối với các máy chủ trong DMZ |
| 192.63.16.0/24 | \* | 192.63.8.0/24 | \* | Deny | Chặn DMZ giao tiếp với các thiết bị trong mạng nội bộ |
| 192.63.8.0/24 | \* | \* | \* | deny | Chặn mọi kết nối từ Internet đến mạng nội bộ |
| \* | \* | \* | \* | Allow | Cho phép các trường hợp còn lại |

**Bài 3: Lập bảng so sánh quy mô, đặc điểm, giá cả... các phần mềm tường lửa phổ biến hiện nay.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Phần mềm** | **Quy mô** | **Đặc điểm** | **Hệ điều hành hỗ trợ** | **Giá cả** | **Ưu điểm** | **Nhược điểm** |
| AVS Firewall | Cá nhân | Giao diện đơn giản  Bảo vệ chống quảng cáo và pop-up. Bộ lọc nội dung web cơ bản. | Windows | Miễn phí | Phù hợp với người dùng mới. -Kiểm soát lưu lượng dễ dàng. | Chỉ hỗ trợ Windows. |
| NetDefender | Cá nhân và doanh nghiệp nhỏ | Tường lửa nguồn mở  Giao diện đơn giản. Hỗ trợ theo dõi lưu lượng mạng trực tiếp | Windows | |  | | --- | | Miễn phí |  |  | | --- | |  | | Hoàn toàn miễn phí. Phù hợp với người am hiểu mạng cơ bản. | Giao diện không hiện đại, khó dùng với người mới. |
| Comodo Firewall | Cá nhân và doanh nghiệp nhỏ | Tường lửa hai chiều  Tích hợp bảo mật web (DNS).  Chế độ bảo vệ chống xâm nhập | Windows | Miễn phí; bản cao cấp giá từ 29.99 USD/năm | Bản miễn phí mạnh mẽ. Dễ sử dụng. | Một số tính năng nâng cao yêu cầu trả phí. |
| ZoneAlarm Free Firewall | Cá nhân và doanh nghiệp nhỏ | Bảo vệ chống phần mềm gián điệp (Anti-Spyware). "Stealth Mode" để bảo vệ khỏi hacker. | Windows | Miễn phí; bản cao cấp từ 39.95 USD/năm | Dễ cài đặt và sử dụng.  Bảo mật tốt cho người dùng cá nhân. | Phiên bản miễn phí bị giới hạn tính năng nâng cao. |