Ho Chi Minh City University of Technology - VNU-HCM
Faculty of Computer Science and Engineering

- - - - - - - - - - - -

MẬT MÃ & AN NINH MẠNG

BÁO CÁO BÀI TẬP LỚN

Đề bài số 04

GVHD: Nguyễn Cao Đạt

Sinh viên: Hoàng Nguyễn Minh Đức 1610755
Trần Thanh Sang 1612939
Thái Thị Thanh Linh 1611830

TP. Hồ Chí Minh, tháng 11 năm 2019

Mục lục

1 Giới thiệu

1.1 Đặt vấn đề

Trong thời gian gần đây, các cuộc tấn công mạng, gián điệp, tội phạm mạng không ngừng gia tăng nhằm đánh cắp dữ liệu, thông tin bí mật nhà nước, phá hoại hệ thống thông tin. Hoạt động tội phạm mạng ngày càng tinh vi, gây ra nhiều hậu quả nghiệm trọng, đe dọa đến trật tự an toàn xã hội, sự ổn định chính trị, an ninh của hầu hết các quốc gia, các vùng lãnh thổ và các tập đoàn lớn.

Vì vậy, một vấn đề cấp bách được đặt ra là phải đảm bảo tính ổn định, sự an toàn của các hệ thống đóng vai trò quan trọng và có ảnh hưởng lớn đến số lượng lớn các người dùng, doanh nghiệp và nhà nước.

Trong bài tập lớn này, nhóm sẽ hiện thực một hệ thống tường lửa với một số chức năng đơn giản để quản lý, theo dõi và bảo vệ hệ thống mạng cục bộ. Các yêu cầu của đề bài sẽ được nhắc đến ở phần sau.

1.2 Nhắc lại đề bài

Trong bài tập lớn này, ta phải triển khai một hệ thống bức tường lửa với nhiều chức năng bổ sung. Bạn có thể dùng các mã nguồn mở có trên web như Shorewall, Squid, SquidGuard, DansGuardian, ClamAV hay Webmin.

Hệ thống phải có những chức năng sau:

- **Firewall**: bộ lọc gói có trạng thái, không giới hạn số lượng giao tiếp mạng, nhiều giao tiếp mạng trên một zone và nhiều zone trên một giao tiếp, quản lý địa chỉ linh động (NAT, PAT).
- **Lọc web**: chặn dựa trên URL, Keyword, Phase, chặn Java Applet, Cookies, Active X.
- **Anti-virus**: Hỗ trợ lọc trên các giao thức HTTP/SMTP/POP3/IMAP/FTP/IM và cơ sở dữ liệu về virus được cập nhật tự động.
- **AntiSpam**: Hỗ trợ lọc dựa trên Real-time Blacklist, Open Relay Database Server. keyword/phase, IP addresses Blacklist và cơ sở dữ liệu về các loại này được cập nhật tự động.
- **Quản trị**: Thông qua web.

1.3 Bố cục của báo cáo

Báo cáo này sẽ được chia thành 4 chương chính, trong đó nội dung của các chương sẽ lần lượt là:

- **Chương 1 - Giới thiệu:** Đặt vấn đề để cho thấy ý nghĩa của đề tài, nhắc lại yêu cầu của đề bài và tóm tắt nội dung báo cáo.
- **Chương 2 - Phân tích và thiết kế hệ thống:**
- **Chương 3 - Hiện thực và đánh giá hệ thống:**
- **Chương 4 - Kết luận:**

Ở cuối báo cáo sẽ là **Tài liệu tham khảo** và **Phụ lục** để tiện theo dõi.

2 Phân tích và thiết kế hệ thống

2.1 Thiết kế hệ thống mạng

2.2 Sơ đồ

Để xây dựng hệ thống tường lửa bảo vệ cho một số thành phần trong mạng, ta cần xây dựng một hệ thống mạng tương ứng, đáp ứng đủ cả về outbound lẫn inbound network tương ứng với hệ thống tường lửa.

Sơ đồ sau đây minh hoạ kiến trúc hệ thống tổng quan mà nhóm đề xuất cho việc hiện thực cũng như xây dựng các kịch bản kiểm thử:

2.3 Mạng con và chia dải địa chỉ

Hệ thống mạng mà nhóm xây dựng bao gồm các thành phần mạng con:

1. Tường lửa: Đây là thành phần chính của bài tập lớn này, bao gồm các chức năng thiết lập, quản lý và theo dõi hệ thống, các chức năng của thành phần này sẽ được giải thích chi tiết sau đó.

2. Mạng LAN: Mạng LAN là một subnet được đặt phía sau bức tương lửa, được bảo vệ bởi các dịch vụ của tường lửa.

3. Mạng DMZ: Mạng DMZ đại diện như một phần của hệ thống mạng với các thiết bị bên trong là các server cung cấp dịch vụ có thể được truy cập từ "Internet". Cần lưu ý rằng giới hạn "Internet" mà nhóm đặt ra trong thiết kế hệ thống mạng chỉ đơn giản là một subnet khác của hệ thống mạng (được gọi là WAN kể từ đây).

4. Mạng WAN: Là một subnet với các client trong đó bao gồm bức tường lửa cần xây dựng. Các kết nối từ mạng WAN này đến các thiết bị trong LAN hay DMZ được xem như là kết nối từ "Internet" trong phạm vi của bài tập lớn này.

5. Internet: Cho phép các truy cập đến những dịch vụ đang được mạng Internet "thật" cung cấp.

Các thành phần này có các (dải) địa chỉ IP sau đây trong kiến trúc hệ thống như hình trên:

1. Hệ thống các mạng con:

Tên	Network ID	Subnet mask	Gateway
WAN	10.0.2.0	255.255.255.0	10.0.2.1
LAN	192.168.0.0	255.255.255.0	192.168.0.1
DMZ	192.168.1.0	255.255.255.0	192.168.1.1
Internet			

2. Các thiết bị trong mạng con:

Tên thiết bị	Địa chỉ IP	Thuộc mạng	Ghi chú
WAN computer	if0: 10.0.2.4/24	WAN	DHCP
LAN computer	if0: 192.168.0.3/24	LAN	DHCP
DMZ server	if0: 192.168.1.3/24	DMZ	Static
pfSense UTM	if0: 10.0.2.15/24 if1: 192.168.0.1/24 if2: 192.168.1.1/24		if0: DHCP if1: Static if2: Static

2.4 Lựa chọn công cụ

Nhóm đã hiện thực thiết kế hệ thống trên nền tảng ảo hoá Oracle VM VirtualBox với cách kết nối các thiết bị như sau:

Tên mạng	Loại	Các interface kết nối
Mạng WAN	NAT Network	WAN computer: if0 pfSense UTM: if0
Mạng LAN	Internal Network	pfSense UTM: if1 LAN computer: if0
Mạng DMZ	Internal Network	DMZ server: if0 pfSense UTM: if2

2.5 Chi tiết thiết kế

Chi tiết thiết kế của hệ thống sẽ được trình bày theo từng thiết bị có trong hệ thống mạng đề xuất:

2.5.1 pfSense UTM

2.5.1.a Tổng quan

pfSense là phần mềm định tuyến/tường lửa mã nguồn mở miễn phí dành cho máy tính dựa trên hệ điều hành FreeBSD được phát triển bởi Netgate. pfSense có thể được cài đặt trên máy tính vật lý hoặc máy ảo để xây dựng hệ thống định tuyến/tường lửa cho mạng.

Trong bài tập lớn này, nhóm sử dụng pfSense phiên bản 2.4.4-p, được cài đặt trên máy ảo có cấu hình: Vi xử lý Intel Core i7 8750H x 3 CPUs và 4GB RAM. Để bổ sung và hoàn thiện pfSense thành 1 UTM đa chức năng, nhóm đã thiết lập và cài đặt thêm các dịch vụ sau đây:

2.5.1.b Firewall rules

a

3 Hiện thực và đánh giá hệ thống

3.1 Hiên thực hệ thống trên môi trường ảo hoá

3.2 Hiện thực chức năng và kiểm thử

4 Kết luận

4.1 Tài nguyên sử dụng

4.2 Kết luận