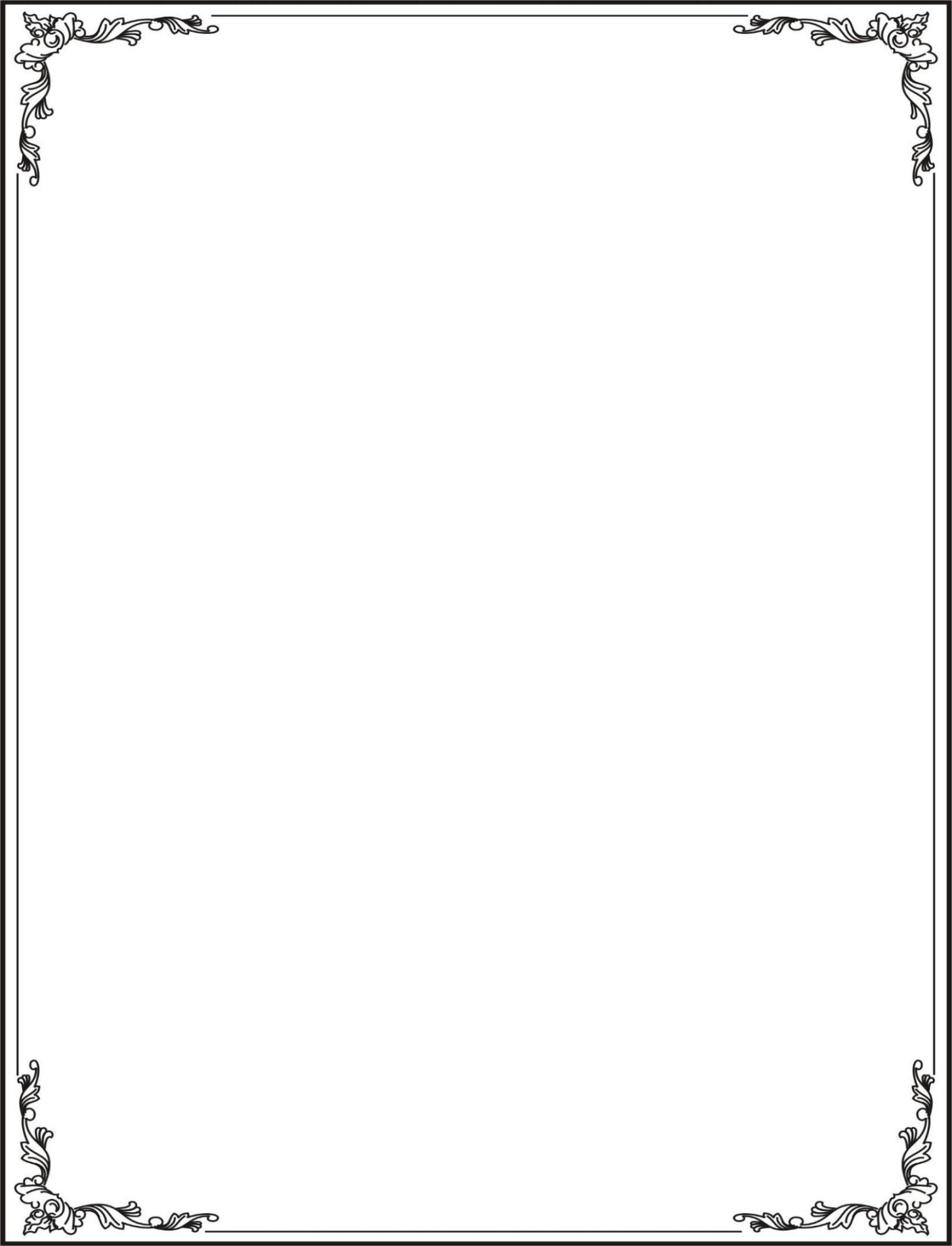
****

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

KHOA CÔNG NGHỆ THÔNG TIN

------------



**Báo cáo nguyên lý hệ điều hành**

**Đề tài: Nghiên cứu tìm hiểu về Hệ thống bảo vệ trong HĐH Linux.**

|  |  |
| --- | --- |
| **GVHD** | **Nguyễn Thanh Hải** |
| **Sinh viên** | Nguyễn Văn Đức  Lê Hồng Hạnh  Đặng Xuân Hoàng  Đỗ Thị Khánh Minh  Lê Quốc Việt |
| **Nhóm** | 12 |
| **Lớp** | 20212IT6025008. **Khóa:** 15 |

**Hà Nội – Năm 2022**

**MỤC LỤC**

[LỜI MỞ ĐẦU 2](#_30j0zll)

[CHƯƠNG 1 : TỔNG QUAN VỀ BẢO VỆ VÀ AN TOÀN HỆ THỐNG 3](#_1fob9te)

[*1.1. Tổng quan về bảo vệ hệ thống* 3](#_3znysh7)

[*1.1.1. Mục tiêu của bảo vệ hệ thống* 3](#_2et92p0)

[*1.1.2. Miền bảo vệ* 4](#_tyjcwt)

[1.1.2.1. Khái niệm miền bảo vệ 4](#_3dy6vkm)

[1.1.2.2. Cấu trúc miền bảo vệ 4](#_1t3h5sf)

[*1.1.3. Ma trận quyền truy cập* 5](#_4d34og8)

[*1.2. An toàn hệ thống* 5](#_2s8eyo1)

[*1.2.1. Các vấn đề về an toàn hệ thống* 6](#_17dp8vu)

[*1.2.2. Các cơ chế an toàn hệ thống* 6](#_3rdcrjn)

[1.2.2.1. Kiểm định danh tính 6](#_26in1rg)

[1.2.2.2. Ngăn chặn nguyên nhân từ phía các chương trình 6](#_lnxbz9)

[1.2.2.3. Ngăn chặn nguyên nhân từ phía hệ thống  7](#_35nkun2)

[1.2.2.4. Giám sát các nguyên nhân  7](#_1ksv4uv)

[*1.3. Lệnh Chmod* 8](#_44sinio)

[CHƯƠNG 2: LINUX FIREWALL 9](#_2jxsxqh)

[*2.1. Dùng công cụ dò tìm để khảo sát hệ thống* 10](#_z337ya)

[*2.2. Phát hiện sự xâm nhập qua mạng* 12](#_1y810tw)

[*2.3. Kiểm tra khả năng bị xâm nhập* 13](#_2xcytpi)

[*2.4. Đối phó khi hệ thống bị tấn công* 13](#_3whwml4)

[CHƯƠNG 3: THIẾT LẬP TƯỜNG LỬA IPTABLES CHO LINUX 15](#_2bn6wsx)

[*3.1. Giới thiệu về Iptables* 15](#_qsh70q)

[*3.2. Lập cấu hình Iptables cho máy chủ phục vụ web* 16](#_3as4poj)

[*3.2.1. Thiết lập các tham số cho nhân* 16](#_1pxezwc)

[*3.2.2. Nạp các Module cần thiết cho iptable.* 17](#_49x2ik5)

[*3.2.3. Nguyên tắc đặt luật là "Drop trước, Accept sau".* 17](#_2p2csry)

[*3.2.4. Lọc ICMP vào và chặn ngập lụt PING.* 17](#_147n2zr)

[*3.2.5. Reject quét cổng TCP và UDP.* 18](#_3o7alnk)

[*3.2.6. Phát hiện quét cổng bằng Nmap.* 19](#_23ckvvd)

[*3.2.7. Chặn ngập lụt SYN.* 20](#_ihv636)

[KẾT LUẬN 21](#_32hioqz)

**LỜI MỞ ĐẦU**

Linux là một phần mềm Hệ điều hành mã nguồn mở đã và đang phát triển rất mạnh mẽ ở trên thế giới. Nó đã tạo nên một sự bùng nổ trong tin học và ngày càng trở thành một trong những hệ điều hành phổ biến nhất hiện nay. Các ưu điểm mà hệ điều hành này mang đến cho người sử dụng là rất to lớn. Tuy nhiên ở Việt Nam, Linux vẫn chưa được nhiều người dùng biết đến, hay sử dụng nó một cách thành thạo bởi vì với người dùng thông thường không có nhu cầu tìm tòi khám phá sẽ sử dụng các hệ điều hành có sẵn thuần tuý như Windows trên hầu hết Laptop và máy tính hiện nay, đồng thời là MacOS trên macbook và imac. Dù vậy, với mã nguồn mở và các chương trình trên Linux chúng ta có thể học hỏi những kiến thức lập trình vốn không thể tìm thấy ở các hệ điều hành kể trên.

Bởi lý do đó, trong đồ án này chúng ta sẽ cùng tìm hiểu một phần rất quan trọng đó là “Hệ thống bảo vệ trong hệ điều hành Linux” bằng việc hiểu rõ các khái niệm liên quan đến bảo vệ và an toàn, từ đó tiến sâu vào cách thức hoạt động của cơ chế bảo vệ để sử dụng chúng một cách hiệu quả.

**CHƯƠNG 1 : TỔNG QUAN VỀ BẢO VỆ VÀ AN TOÀN HỆ THỐNG**

* 1. ***Tổng quan về bảo vệ hệ thống***
     1. *Mục tiêu của bảo vệ hệ thống*

Khi các tiến trình hoạt động song hành trong hệ thống thì một tiến trình gặp lỗi có thể ảnh hưởng đến các tiến trình khác và ảnh hưởng tới toàn bộ hệ thống. Hệ điều hành cần phải phát hiện, ngăn chặn không cho lỗi lan truyền và đặc biệt là phát hiện lỗi tiềm ẩn trong hệ thống để tăng cường độ tin cậy.

Mặt khác mục tiêu của bảo vệ hệ thống còn chống truy nhập bất hợp lệ, bảo đảm cho các tiến trình khi hoạt động trong hệ thống sử dụng tài nguyên phù hợp với quy định của hệ.

Bảo vệ hệ thống cần phải cung cấp một cơ chế và chiến lược để quản trị việc sử dụng tài nguyên, quyết định những đối tượng nào trong hệ thống được bảo vệ và quy định các thao tác thích hợp trên đối tượng này.

* + 1. *Miền bảo vệ*
       1. Khái niệm miền bảo vệ

Một hệ thống máy tính bao gồm tập hợp các chủ thể và tập hợp các khách thể. Chủ thể bao gồm các tiến trình và người sử dụng còn khách thể có thể coi là các tài nguyên của máy tính.

Để có thể kiểm soát được tình trạng sử dụng tài nguyên trong hệ thống, hệ điều hành chỉ cho phép các chủ thể truy nhập tới các khách thể mà nó có quyền sử dụng và vào những thời điểm cần thiết nhằm hạn chế các lỗi xảy ra do tranh chấp tài nguyên.

Mỗi chủ thể trong hệ thống sẽ hoạt động trong một miền bảo vệ nào đó. Một miền bảo vệ sẽ xác định các khách thể mà chủ thể trong miền đó được phép truy nhập và thực hiện các thao tác.

* + - 1. Cấu trúc miền bảo vệ

Các khả năng thao tác mà chủ thể có thể thực hiện trên các thể được gọi là quyền truy nhập (access right). Mỗi quyền truy nhập được định nghĩa bởi một bộ hai thành phần <đối tượng{quyền thao tác}>.Như vậy ta có thể hình dung miền bảo vệ là một tập hợp các quyền truy nhập,xác định các thao tác mà chủ thể có thể thực hiện trên các khách thể . Các miền bảo vệ khác nhau có thể giao nhau một số quyền truy nhập.

Một tiến trình hoạt động và miền bảo vệ có thể tồn tại hai mối liên kết:

*- Liên kết tĩnh:* trong suốt thời gian tồn tại của tiến trình trong hệ thống, tiến trình chỉ hoạt động trong một miền bảo vệ . Trong trường hợp tiến trình trên những tập tài nguyên khác nhau. Như vậy trong liên kết tỉnh , miền bảo vệ phải xã định ngay từ đầu các quyền truy cập cho tiến trình trong tất các giai đoạn xử lý. Điều này khiến cho tiến trình sẽ được dư thừa quyền trong một giai đoạn xử lí nào đó và vi phạm nguyên lí need- to-know. Để đảm bảo được nguyên lí này phải có khả năng cập nhật nội dung miền bảo vệ qua các giai đoạn xử lí khác nhau để đảm bảo các quyền tối thiểu của tiến trình trong miền bảo vệ tại một thời điểm.

*- Liên kết động:* Cơ chế này cho phép tiến trình chuyển đổi từ miền bảo vệ này sang miền bảo vệ khác trong suốt thời gian tồn tại trong hệ thống của nó. Để tuân thủ nguyên lý need-to-know,thay vì sửa đổi nội dung miền bảo vệ, hệ thống có thể tạo ra các miền bảo vệ mới với nội dung thay đổi tùy theo từng giai đoạn xử lí của tiến trình và chuyển tiền trình sang hoạt động tại các miền bảo vệ phù hợp với từng thời điểm.

* + 1. *Ma trận quyền truy cập*

Để biểu diễn miền bảo vệ, các hệ điều hành sẽ cài đặt các ma trận quyền truy nhập trong đó các hàng của ma trận biểu diễn các miền bảo vệ , các cột biểu diễn khách thể. Phần tử (i,j) của ma trận xác định quyền truy nhập của các chủ thể thuộc miền bảo vệ Dĩ có thể thao tác đối với khách thể 0.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Object  Subject | F1 | F2 | F3 | Printer |
| D1 | Đọc/ghi | Xử lý | Đọc/ghi |  |
| D2 |  | Ghi |  | In |
| D3 | Xử lý |  | Đọc | In |

*Bảng 1: Ma trận quyền truy nhập*

Cơ chế bảo vệ được cung cấp khi ma trận quyền truy nhập được cài đặt, khi đó chúng ta có thể áp dụng các chiến lược bảo vệ bằng cách đặc tả nội dung các phần tử tương ứng của ma trận - xác định các quyền truy xuất ứng với từng miền bảo vệ.

Ma trận quyền truy nhập cũng cung cấp một cơ chế thích hợp để định nghĩa và thực hiện một sự kiểm soát nghiêm ngặt mối liên hệ giữa các chủ và khách thể.

* 1. ***An toàn hệ thống***
     1. *Các vấn đề về an toàn hệ thống*

Hệ thống được coi là an toàn nếu các tài nguyên được sử dụng đúng quy định trong mọi hoàn cảnh, điều này khó có thể đạt được trong thực tế. Thông thường, cơ chế an toàn hệ thống bị vi phạm vì các nguyên nhân vô tình hoặc cố ý. Việc ngăn chặn các nguyên nhân cố ý là rất khó khăn và gần như không thể đạt hiệu quả hoàn toàn.

Bảo đảm an toàn hệ thống ở cấp cao như chống lại các nguyên nhân hỏa hoạn, thiên tai, mất điện,… cần được thực hiện ở mức độ vật lý (các trang thiết bị đảm bảo an toàn cho hệ thống) và nhân sự (chọn lựa các nhân viên tin cậy làm việc trong hệ thống). Nếu an toàn môi trường được đảm bảo thì an toàn của hệ thống sẽ được duy trì tốt nhờ các cơ chế của hệ điều hành.

Cần chú ý rằng nếu bảo vệ hệ thống có thể đạt độ tin cậy 100% thì các cơ chế an toàn hệ thống được cung cấp chỉ nhằm ngăn chặn bớt các tình huống bất lợi hơn là đạt đến độ an toàn tuyệt đối

* + 1. *Các cơ chế an toàn hệ thống*
       1. Kiểm định danh tính

Để đảm bảo an toàn, hệ điều hành cần phải giải quyết tốt vấn đề kiểm định danh tính (authentication). Hoạt động của hệ thống bảo vệ phụ thuộc vào khả năng xác định các tiến trình đang xử lý. Khả năng này đến lượt nó lại phụ thuộc vào việc xác định người dung đang sử dụng hệ thống để có thể kiểm tra người dùng này được phép thao tác trên những tài nguyên nào.

Cách tiếp cận phổ biến nhất để giải quyết vấn đề là sử dụng mật khẩu (password) để kiểm định danh tính của người sử dụng. Mỗi khi người dùng muốn sử dụng một tài nguyên, hệ thống sẽ so sánh mật khẩu của họ nhập vào với mật khẩu được lưu trữ, nếu đúng họ mới được phép sử dụng tài nguyên. Mật khẩu có thể được áp dụng để bảo vệ cho từng đối tượng trong hệ thống, thậm chí cùng một đối tượng sẽ có các mật khẩu khác nhau tương ứng với các quyền truy cập khác nhau.

Cơ chế mật khẩu rất đơn giản và dễ sử dụng do đó được các hệ điều hành áp dụng rộng rãi, tuy nhiên điểm yếu nghiêm trọng của nó là khả năng bảo mật mật khẩu rất khó đạt được sự hoàn hảo. Những tác nhân tiêu cực có thể tìm ra mật khẩu của người khác nhờ nhiều cách thức khác nhau.

* + - 1. Ngăn chặn nguyên nhân từ phía các chương trình

Trong môi trường hoạt động mà một chương trình được tạo lập bởi một người lại có thể được người khác sử dụng rất có thể sẽ xảy ra các tình huống sử dụng sai chức năng, từ đó dẫn tới những hậu quả không lường trước. Hai trường hợp điển hình gây mất an toàn hệ thống có  thể đề xuất là:

- Ngựa thành Troy: Khi người sử dụng A kích hoạt một chương trình (do người sử dụng B viết) dưới danh nghĩa của mình (trong miền bảo vệ được gán tương ứng cho người sử dụng A), chương trình này có thể trở thành “chú ngựa thành Troy” vì khi đó các đoạn lệnh trong chương trình có thể thao tác với các tài nguyên mà người sử dụng A có quyền nhưng người sử dụng B lại bị cấm. Những chương trình kiểu này đã lợi dụng hoàn cảnh để gây ra các tác hại đáng tiếc.

- Lỗ hổng bảo mật (Trap-door): Mối đe dọa đặc biệt nguy hiểm và khó chống đỡ do vô tình hoặc cố ý của các lập trình viên khi xây dựng chương trình. Các lập trình viên có thể để lại một “cánh cửa nhỏ” trong phần mềm của họ để thông qua đó can thiệp vào hệ thống. Chính “cách cửa nhỏ này” đã tạo cơ chế cho các hacker xâm nhập và phá hoại hệ thống của người sử dụng. Việc phát hiện các “các cánh cửa nhỏ” để đối phó rất phức tạp vì cần phải tiến hành phân tích chương trình nguồn để tìm ra chỗ sơ hở.

* + - 1. Ngăn chặn nguyên nhân từ phía hệ thống

Hầu hết các tiến trình hoạt động trong hệ thống đều có thể tạo ra các tiến trình con. Trong cơ chế hoạt động này, các tài nguyên hệ thống rất dễ bị sử dụng sai mục đích gây mất an toàn cho hệ thống. Hai mối đe dọa biến theo phương pháp này là:

- Các chương trình sâu (Worm): Một chương trình sâu là chương trình lợi dụng cơ chế phát sinh ra các tiến trình con của hệ thống để đánh bại chính hệ thống .Chương trình sâu có khả năng tự động phát sinh các bản sao trong hệ thống sau đó chiếm dụng tài nguyên, làm ngưng trệ hoạt động của các tiền trình khác và toàn bộ hệ thống.

- Các chương trình virus: Virus là một chương trình phá hoại khá nguy hiểm đối với các hệ thống thông tin. Khác với các chương trình sâu là những chương trình hoàn chỉnh, virus chỉ là các đoạn mã có khả năng lây nhiễm vào các chương trình chính thống và từ đó tàn phá hệ thống.

* + - 1. Giám sát các nguyên nhân

Nhìn chung, việc đảm bảo an toàn hệ thống là rất phức tạp vì nó liên quan tới yếu tố con người. Hệ điều hành chỉ chó thể áp dụng một số biện pháp để giảm bớt thiệt hại như lập lập nhật ký sự kiện để ghi nhận các tình huống xảy ra trong hệ thống. Ví dụ như theo dõi:

- Người sử dụng cố gắng nhập mật khẩu nhiều lần.

- Cá tiến trình với định danh nghi ngờ không được ủy quyền.

- Các tiến trình lạ trong các thư mục hệ thống.

- Các chương trình kéo dài thời gian xử lí một cách đáng ngờ.

- Các tệp tin và thư mục bị khóa không hợp lý.

- Kích thước các chương trình hệ thống bị thay đổi…

Việc kiểm tra thường kỳ và ghi nhận những thông tin này giúp hệ thống phát hiện kịp thời các nguy cơ, cho phép phân tích, dự đoán và tìm phương pháp đối phó.

* 1. ***Lệnh Chmod***

Change Mode – Chmod (chế độ thay đổi) là một lệnh Linux được sử dụng để đặt quyền Đọc, Viết  và Thực thi cho các loại người dùng khác nhau.

Chmod chính là thao tác thay đổi các quyền sau:

- “Read” (Đọc): viết tắt là “r”, và được biểu diễn bằng số 4  
 - “Write” (Ghi / Chỉnh sửa): viết tắt là “w”, và được biểu diễn bằng số 2  
 - “Execute” (Thực thi): viết tắt là “x”, và được biểu diễn bằng số 1

Chmod cùng lúc thay đổi quyền hạn trên các file/thư mục với các đối tượng sau:

-   “Owner” – chủ sở hữu của file/thư mục  
 -   “Group” – Nhóm mà Owner là thành viên  
 -   “Public / Others/ Everybody”: những người còn lại

Chmod 755 có nghĩa như sau :



Chmod = 755 cho các thư mục có nghĩa là:  
 -7 = 4 + 2 + 1 : Người sở hữu thư mục có quyền đọc thư mục (read); chỉnh sửa thư mục (write); liệt kê các thư mục và file bên trong (execute)  
 - 5 = 4 + 0 + 1 : Những người cùng nhóm chỉ có quyền đọc thư mục (read); liệt kê các thư mục và file bên trong (execute)  
 -5 = 4 + 0 + 1 : Những người còn lại chỉ có quyền đọc thư mục (read); liệt kê các thư mục và file bên trong (execute)

**CHƯƠNG 2: LINUX FIREWALL**

An toàn hệ thống luôn luôn là một vấn đề sống còn của mạng máy tính và firewall là một thành phần cốt yếu cho việc đảm bảo an ninh.

Một firewall là một tập hợp các quy tắc, ứng dụng và chính sách đảm bảo cho người dùng truy cập các dịch vụ mạng trong khi mạng bên trong vẫn an toàn đối với các kẻ tấn công từ Internet hay từ các mạng khác. Có hai loại kiến trúc firewall cơ bản là : Proxy/Application firewall và filtering gateway firewall. Hầu hết các hệ thống firewall hiện đại là loại lai (hybrid) của cả hai loại trên.

Nhiều công ty và nhà cung cấp dịch vụ Internet sử dụng máy chủ Linux như một Internet gateway. Những máy chủ này thường phục vụ như máy chủ mail, web, ftp, hay dialup. Hơn nữa, chúng cũng thường hoạt động như các firewall, thi hành các chính sách kiểm soát giữa Internet và mạng của công ty. Khả năng uyển chuyển khiến cho Linux thu hút như là một thay thế cho những hệ điều hành thương mại.

Tính năng firewall chuẩn được cung cấp sẵn trong kernel của Linux được xây dựng từ hai thành phần : ipchains và IP Masquerading.   
  
Linux IP Firewalling Chains là một cơ chế lọc gói tin IP. Những tính năng của IP   
Chains cho phép cấu hình máy chủ Linux như một filtering gateway/firewall dễ dàng. Một thành phần quan trọng khác của nó trong kernel là IP Masquerading, một tính năng chuyển đổi địa chỉ mạng (network address translation- NAT) mà có thể che giấu các địa chỉ IP thực của mạng bên trong. Để sử dụng ipchains, bạn cần thiết lập một tập các luật mà quy định các kết nối được cho phép hay bị cấm.

Các nguyên tắc Ipchains Thực hiện các chức năng sau:

- Accept: The packet is okay; allow it to pass to the appropriate chain   
Cho phép chuyển gói tin qua chain thích hợp

- Deny: The packet is not okay; silently drop it in the bit bucket. Không   
đồng ý , bị rớt.

- Reject: The packet is not okay; but inform the sender of this fact via   
an ICMP packet. Không đồng ý, những sự việc của người gửi qua gói ICMP

- Masq: Used for IP masquerading (network address translation). Sử   
dụng cho IP masquerading ( việc dịch địa chỉ mạng)

- Redirect: Send this packet to someone else for processing. Gửi gói tin   
này đến một người khác để xử lý

- Return: Terminate the rule list. Hoàn thành danh sách các quy tắc

*Chú ý:* Các gói Ipfw(ipfilters/iptable) dưới hệ điều hành BSD cung cấp hoạt động tương tự Ipchains.   
***Ví dụ:***   
# Cho phép các kết nối web tới Web Server của bạn   
/sbin/ipchains -A your\_chains\_rules -s 0.0.0.0/0 www -d 192.16.0.100 1024: -j ACCEPT

# Cho phép các kết nối từ bên trong tới các Web Server bên ngoài   
/sbin/ipchains -A your\_chains\_rules -s 192.168.0.0/24 1024: -d 0.0.0.0/0 www -j   
ACCEPT   
# Từ chối truy cập tất cả các dịch vụ khác   
/sbin/ipchains -P your\_chains\_rules input DENY   
Ngoài ra, bạn có thể dùng các sản phẩm firewall thương mại như Check Point FireWall-1, Phoenix Adaptive Firewall, Gateway Guardian, XSentry Firewall, Raptor, hay rất nhiều các phiên bản miễn phí, mã nguồn mở cho Linux như T.Rex Firewall, Dante, SINUS, TIS Firewall Toolkit, …

***2.1. Dùng công cụ dò tìm để khảo sát hệ thống***

Thâm nhập vào một hệ thống bất kỳ nào cũng cần có sự chuẩn bị. Hacker phải xác định ra máy đích và tìm xem những port nào đang mở trước khi hệ thống có thể bị xâm phạm. Quá trình này thường được thực hiện bởi các công cụ dò tìm (scanning tool), kỹ thuật chính để tìm ra máy đích và các port đang mở trên đó. Dò tìm là bước đầu tiên hacker sẽ sử dụng trước khi thực hiện tấn công. Bằng cách sử dụng các công cụ dò tìm như Nmap, hacker có thể rà khắp các mạng để tìm ra các máy đích có thể bị tấn công. Một khi xác định được các máy này, kẻ xâm nhập có thể dò tìm các port đang lắng nghe. Nmap cũng sử dụng một số kỹ thuật cho phép xác định khá chính xác loại máy đang kiểm tra.

Bằng cách sử dụng những công cụ của chính các hacker thường dùng, người quản trị hệ thống có thể nhìn vào hệ thống của mình từ góc độ của các hacker và giúp tăng cường tính an toàn của hệ thống. Có rất nhiều công cụ dò tìm có thể sử dụng như: Nmap, strobe, sscan, SATAN, …

Nmap Là chữ viết tắt của "Network exploration tool and security scanner" . Đây là chương trình quét hàng đầu với tốc độ cực nhanh và cực mạnh. Nó có thể quét trên mạng diện rộng và đặc biệt tốt đối với mạng đơn lẻ. NMAP giúp bạn xem những dịch vụ nào đang chạy trên server (services/ports:web server,ftp server,pop3, ), server đang dùng hệ điều hành gì, loại tường lửa mà server sử dụng, và rất nhiều tính năng khác. Nói chung NMAP hỗ trợ hầu hết các kỹ thuật quét như : ICMP (ping sweep), IP protocol, Null scan, TCP SYN (half open), NMAP được đánh giá là công cụ hàng đầu của các Hacker cũng như các nhà quản trị mạng trên thế giới.

Quét an toàn Nmap là một trong số công cụ quét an toàn được sử dụng rộng   
rãi nhất sẵn có. Nmap là một cổng quét mà chống lại các nhân tố, các cách khác tàn phá đến mạng của bạn. Nó có thể phát sinh ra nhiều kiểu gói mà thăm dò các ngăn xếp TCP/IP trên những hệ thống của bạn.

Nmap có thể phát sinh ra một danh sách của những cổng mở dịch vụ trên hệ   
thống của bạn, thâm nhập firewalls, và cung cấp những tin quấy rầy, không tin cậy   
đang chạy trên host của bạn. Nmap security có sẵn tại : <http://www.insecure.org>   
Dưới đây là một ví dụ sử dụng Nmap:   
# nmap -sS -O 192.168.1.200   
Starting nmap V. 2.54 by Fyodor (fyodor@dhp.com, [www.insecure.org/nmap](http://www.insecure.org/nmap)/)   
Interesting ports on comet (192.168.1.200):   
Port State Protocol Service   
7 open tcp echo   
19 open tcp chargen   
21 open tcp ftp   
…  
TCP Sequence Prediction: Class=random positive increments   
Difficulty=17818 (Worthy challenge)   
Remote operating system guess: Linux 2.2.13   
Nmap run completed 1 IP address (1 host up) scanned in 5 seconds

Tuy nhiên, sử dụng các công cụ này không thể thay thế cho một người quản trị có kiến thức. Bởi vì việc dò tìm thường dự báo một cuộc tấn công, các site nên ưu tiên cho việc theo dõi chúng. Với các công cụ dò tìm, các nhà quản trị hệ thống mạng có thể phát hiện ra những gì mà các hacker có thể thấy khi dò trên hệ thống của mình.

***2.2. Phát hiện sự xâm nhập qua mạng***

Nếu hệ thống của bạn có kết nối vào internet, bạn có thể trở thành một mục tiêu bị dò tìm các lỗ hổng về bảo mật. Mặc dù hệ thống của bạn có ghi nhận điều này hay không thì vẫn không đủ để xác định và phát hiện việc dò tìm này. Một vấn đề cần quan tâm khác là các cuộc tấn công gây ngừng dịch vụ (Denial of Services - DoS), làm thế nào để ngăn ngừa, phát hiện và đối phó với chúng nếu bạn không muốn hệ thống của bạn ngưng trệ.

Hệ thống phát hiện xâm nhập qua mạng (Network Intrusion Detection System - NIDS) theo dõi các thông tin truyền trên mạng và phát hiện nếu có hacker đang cố xâm nhập vào hệ thống (hoặc gây gây ra một vụ tấn công DoS). Một ví dụ điển hình là hệ thống theo dõi số lượng lớn các yêu cầu kết nối TCP đến nhiều port trên một máy nào đó, do vậy có thể phát hiện ra nếu có ai đó đang thử một tác vụ dò tìm TCP port. Một NIDS có thể chạy trên máy cần theo dõi hoặc trên một máy độc lập theo dõi toàn bộ thông tin trên mạng.

Các công cụ có thể được kết hợp để tạo một hệ thống phát hiện xâm nhập qua mạng. Chẳng hạn dùng tcpwrapper để điều khiển, ghi nhận các dịch vụ đã được đăng ký. Các chương trình phân tích nhật ký hệ thống, như swatch, có thể dùng để xác định các tác vụ dò tìm trên hệ thống. Và điều quan trọng nhất là các công cụ có thể phân tích các thông tin trên mạng để phát hiện các tấn công DoS hoặc đánh cắp thông tin như tcpdump, ethereal, ngrep, NFR (Network Flight Recorder), PortSentry, Sentinel, Snort, Khi hiện thực một hệ thống phát hiện xâm nhập qua mạng bạn cần phải lưu tâm đến hiệu suất của hệ thống cũng như các chính sách đảm bảo sự riêng tư.

***2.3. Kiểm tra khả năng bị xâm nhập***

Kiểm tra khả năng bị xâm nhập liên quan đến việc xác định và sắp xếp các lỗ hổng an ninh trong hệ thống bằng cách dùng một số công cụ kiểm tra. Nhiều công cụ kiểm tra cũng có khả năng khai thác một số lỗ hổng tìm thấy để làm rõ quá trình thâm nhập trái phép sẽ được thực hiện như thế nào. Ví dụ, một lỗi tràn bộ đệm của chương trình phục vụ dịch vụ FTP có thể dẫn đến việc thâm nhập vào hệ thống với quyền „root‟. Nếu người quản trị mạng có kiến thức về kiểm tra khả năng bị xâm nhập trước khi nó xảy ra, họ có thể tiến hành các tác vụ để nâng cao mức độ an ninh của hệ thống mạng.

Có rất nhiều các công cụ mạng mà bạn có thể sử dụng trong việc kiểm tra khả năng bị xâm nhập. Hầu hết các quá trình kiểm tra đều dùng ít nhất một công cụ tự động phân tích các lỗ hổng an ninh. Các công cụ này thăm dò hệ thống để xác định các dịch vụ hiện có. Thông tin lấy từ các dịch vụ này sẽ được so sánh với cơ sở dữ liệu các lỗ hổng an ninh đã được tìm thấy trước đó.

Các công cụ thường được sử dụng để thực hiện các kiểm tra loại này là ISS Scanner, Cybercop, Retina, Nessus, cgiscan, CIS, Kiểm tra khả năng bị xâm nhập cần được thực hiện bởi những người có trách nhiệm một cách cẩn thận. Sự thiếu kiến thức và sử dụng sai cách có thể sẽ dẫn đến hậu quả nghiêm trọng không thể lường trước được.   
***2.4. Đối phó khi hệ thống bị tấn công***

Gần đây, một loạt các vụ tấn công nhắm vào các site của những công ty lớn  
như Facebook!, VNP, EBay, Amazon và CNN Interactive gây ra những thiệt hại vô cùng nghiêm trọng. Những tấn công này là dạng tấn công gây ngừng dịch vụ "Denial-Of-Service" mà được thiết kế để làm ngưng hoạt động của một mạng máy tính hay một website bằng cách gửi liên tục với số lượng lớn các dữ liệu tới mục tiêu tấn công khiến cho hệ thống bị tấn công bị ngừng hoạt động, điều này tương tự như hàng trăm người cùng gọi không ngừng tới 1 số điện thoại khiến nó liên tục bị bận.

Trong khi không thể nào tránh được mọi nguy hiểm từ các cuộc tấn công, chúng tôi khuyên bạn một số bước mà bạn nên theo khi bạn phát hiện ra rằng hệ thống của bạn bị tấn công. Chúng tôi cũng đưa ra một số cách để giúp bạn bảo đảm tính hiệu qủa của hệ thống an ninh và những bước bạn nên làm để giảm rủi ro và có thể đối phó với những cuộc tấn công.   
 Nếu phát hiện ra rằng hệ thống của bạn đang bị tấn công, hãy bình tĩnh. Sau đây là những bước bạn nên làm:

* Tập hợp 1 nhóm để đối phó với sự tấn công:   
  - Nhóm này phải bao gồm những nhân viên kinh nghiệm, những người mà có thể giúp hình thành một kế hoạch hành động đối phó với sự tấn công.
* Dựa theo chính sách và các quy trình thực hiện về an ninh của công ty, sử dụng các bước thích hợp khi thông báo cho mọi người hay tổ chức về cuộc tấn công.
* Tìm sự giúp đỡ từ nhà cung cấp dịch vụ Internet và cơ quan phụ trách về an ninh máy tính:

- Liên hệ nhà cung cấp dịch vụ Internet của bạn để thông báo về cuộc tấn công. Có thể nhà cung cấp dịch vụ Internet của bạn sẽ chặn đứng được cuộc tấn công .

- Liên hệ cơ quan phụ trách về an ninh máy tính để thông báo về cuộc

tấn công

* Tạm thời dùng phương thức truyền thông khác (chẳng hạn như qua điện thoại) khi trao đổi thông tin để đảm bảo rằng kẻ xâm nhập không thể chặn và lấy được thông tin.
* Ghi lại tất cả các hoạt động của bạn (chẳng hạn như gọi điện thoại, thay đổi file, …)
* Theo dõi các hệ thống quan trọng trong quá trình bị tấn công bằng các phần mềm hay dịch vụ phát hiện sự xâm nhập (intrusion detection software/services). Điều này có thể giúp làm giảm nhẹ sự tấn công cũng như phát hiện những dấu hiệu của sự tấn công thực sự hay chỉ là sự quấy rối nhằm đánh lạc hướng sự chú ý của bạn(chẳng hạn một tấn   
  công DoS với dụng ý làm sao lãng sự chú ý của bạn trong khi thực sự đây là một cuộc tấn công nhằm xâm nhập vào hệ thống của bạn). Sao chép lại tất cả các files mà kẻ xâm nhập để lại hay thay đổi (như những đoạn mã chương trình, log file, …)
* Liên hệ nhà chức trách để báo cáo về vụ tấn công.

Những bước bạn nên làm để giảm rủi ro và đối phó với sự tấn công trong tương   
lai :

* Xây dựng và trao quyền cho nhóm đối phó với sự tấn công
* Thi hành kiểm tra an ninh và đánh giá mức độ rủi ro của hệ thống
* Cài đặt các phần mềm an toàn hệ thống phù hợp để giảm bớt rủi ro

- Nâng cao khả năng của mình về an toàn máy tính

Các bước kiểm tra để giúp bạn bảo đảm tính hiệu quả của hệ thống an ninh:

* Kiểm tra hệ thống an ninh mới cài đặt : chắc chắn tính đúng đắn của chính sách an ninh hiện có và cấu hình chuẩn của hệ thống.
* Kiểm tra tự động thường xuyên : để khám phá sự “viếng thăm” của những hacker hay những hành động sai trái của nhân viên trong công ty.
* Kiểm tra ngẫu nhiên: để kiểm tra chính sách an ninh và những tiêu chuẩn, hoặc kiểm tra sự hiện hữu của những lỗ hổng đã được phát hiện (chẳng hạn những lỗi được thông báo từ nhà cung cấp phần mềm)
* Kiểm tra hằng đêm những file quan trọng: để đánh giá sự toàn vẹn của những file và cơ sở dữ liệu quan trọng
* Kiểm tra các tài khoản người dùng: để phát hiện các tài khoản không sử dụng, không tồn tại,
* Kiểm tra định kỳ để xác định trạng thái hiện tại của hệ thống an ninh của bạn

**CHƯƠNG 3: THIẾT LẬP TƯỜNG LỬA IPTABLES CHO LINUX**

***3.1. Giới thiệu về Iptables***

Iptables là một ứng dụng dùng để quản lý filtering gói tin và NAT rules hoạt động trên console của linux rất nhỏ và tiện dụng. Được cung cấp miễn phí nhằm nâng cao tính bảo mật trên hệ thống Linux.

Iptables bao gồm 2 phần là netfilter nằm bên trong nhân Linux và iptables nằm ở vùng ngoài nhân. Iptables chịu trách nhiệm giao tiếp với người dùng và sau đó đẩy rules của người dùng vào cho netfilter xử lý. Netfilter thực hiện công việc lọc các gói tin ở mức IP. Netfilter làm việc trực tiếp ở trong nhân của Linux nhanh và không làm giảm tốc độ của hệ thống.

Diagram

Description automatically generated

Iptables được chia làm 4 bảng (table): bảng filter dùng để lọc gói dữ liệu, bảng nat dùng để thao tác với các gói dữ liệu được NAT nguồn hay NAT đích, bảng mangle dùng để thay đổi các thông số trong gói IP và bảng conntrack dùng để theo dõi các kết nối. Mỗi table gồm nhiều mắt xích (chain). Chain gồm nhiều luật (rule) để thao tác với các gói dữ liệu. Rule có thể là ACCEPT (chấp nhận gói dữ liệu), DROP (thả gói), REJECT (loại bỏ gói) hoặc tham chiếu (reference) đến một chain khác.

***3.2. Lập cấu hình Iptables cho máy chủ phục vụ web***

Giả sử như máy chủ phục vụ Web kết nối mạng trực tiếp vào Internet qua card mạng eth0, địa chỉ IP là 1.2.3.4. Bạn cần lập cấu hình tường lửa cho Iptables đáp ứng các yêu cầu sau:

- Cổng TCP 80 (Web-HTTP) mở cho mọi người truy cập web

- Cổng 21 (FTP) chỉ mở cho webmaster (dùng để upload file lên public\_html)

- Cổng 22 (SSH) chỉ mở cho admin (cung cấp shell `root` cho admin để nâng cấp & patch lỗi cho server khi cần)

- Cổng UDP 53 (DNS) để phục vụ tên miền (đây chỉ là ví dụ)

- Chỉ chấp nhận ICMP PING tới với code=0x08, các loại packet còn lại đều bị từ chối

*3.2.1. Thiết lập các tham số cho nhân*

echo 1 > /proc/sys/net/ipv4/tcp\_syncookies

echo 10 > /proc/sys/net/ipv4/tcp\_fin\_timeout

echo 1800 > /proc/sys/net/ipv4/tcp\_keepalive\_time

echo 0 > /proc/sys/net/ipv4/tcp\_window\_scaling

echo 0 > /proc/sys/net/ipv4/tcp\_sack

echo 1 > /proc/sys/net/ipv4/icmp\_echo\_ignore\_broadcasts

echo 0 > /proc/sys/net/ipv4/conf/eth0/accept\_source\_route

tcp\_syncookies=1 bật chức năng DoS SYN qua syncookie của Linux

tcp\_fin\_timeout=10 đặt thời gian timeout cho quá trình đóng kết nối TCP là 10 giây

tcp\_keepalive\_time=1800 đặt thời gian giữ kết nối TCP là 1800 giây

*3.2.2. Nạp các Module cần thiết cho iptable.*

Để sử dụng Iptables, chúng ta cần phải nạp trước các Module cần thiết.

Ví dụ nếu chúng ta muốn dùng chức năng LOG trong Iptables, chúng ta phải nạp Module ipt\_LOG vào trước bằng lệnh # modprobe ipt\_LOG.

MODULES="ip\_tables iptable\_filter ipt\_LOG ipt\_limit ipt\_REJECT ipt\_state for i in $MODULES; do

/sbin/modprobe $MODULES

done

*3.2.3. Nguyên tắc đặt luật là "Drop trước, Accept sau".*

Đây là nguyên tắc mà bạn nên tuân theo. Đầu tiên hãy đóng hết các cổng, sau đó mở dần cách cổng cần thiết. Cách này tránh cho bạn gặp sai sót trong khi đặt luật cho Iptables.

iptables -P INPUT DROP thả packet trước

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT giữ các kết nối hiện tại và chấp nhận các kết nối có liên quan

iptables -A INPUT -i lo -s 127.0.0.1 -j ACCEPT chấp nhận các gói vào looback từ IP 127.0.0.1

iptables -A INPUT -i lo -s 1.2.3.4 -j ACCEPT và 1.2.3.4

BANNED\_IP="10.0.0.0/8 192.168.0.0/16 172.16.0.0/12 224.0.0.0/4 240.0.0.0/5" for i in $BANNED\_IP; do

iptables -A INPUT -i eth0 -s $i -j DROP thả các gói dữ liệu đến từ các IP nằm trong danh sách cấm BANNER\_IP done

*3.2.4. Lọc ICMP vào và chặn ngập lụt PING.*

LOG của Iptables sẽ được ghi vào file /var/log/firewall.log. Bạn phải sửa lại cấu hình cho SYSLOG như sau:

#vi/etc//etc/syslog.conf/var/log/firewall.log # /etc/rc.d/init.d/syslogd restart

Đối với các gói ICMP đến, chúng ta sẽ đẩy qua chain CHECK\_PINGFLOOD để kiểm tra xem hiện tại đang bị ngập lụt PING hay không, sau đó mới cho phép gói vào. Nếu đang bị ngập lụt PING, môđun LOG sẽ tiến hành ghi nhật kí ở mức giới hạn --limit $LOG\_LIMIT và --limit-burst $LOG\_LIMIT\_BURST, các gói PING ngập lụt sẽ bị thả hết.

LOG\_LEVEL="debug"

LOG\_LIMIT=3/m

LOG\_LIMIT\_BURST=1

PING\_LIMIT=500/s

PING\_LIMIT\_BURST=100

iptables -A CHECK\_PINGFLOOD -m limit --limit $PING\_LIMIT --limit-burst $PING\_LIMIT\_BURST -j RETURN

iptables -A CHECK\_PINGFLOOD -m limit --limit $LOG\_LIMIT --limit-burst $LOG\_LIMIT\_BURST -j LOG --log-level $LOG\_LEVEL --log-prefix

"fp=PINGFLOOD:warning a=DROP " iptables -A CHECK\_PINGFLOOD -j DROP

iptables -A INPUT -i eth0 -p icmp --icmp-type echo-request -j CHECK\_PINGFLOOD

iptables -A INPUT -i eth0 -p icmp --icmp-type echo-request -j ACCEPT

*3.2.5. Reject quét cổng TCP và UDP.*

Ở đây bạn tạo sẵn chain reject quét cổng, chúng ta sẽ đẩy vào chain INPUT sau. Đối với gói TCP, chúng ta reject bằng gói TCP với cờ SYN=1 còn đối với gói UDP, chúng ta sẽ reject bằng gói ICMP `port-unreachable`.

iptables-N REJECT\_PORTSCAN

iptables-A REJECT\_PORTSCAN -p tcp -m limit --limit $LOG\_LIMIT --limit-burst $LOG\_LIMIT\_BURST -j LOG --log-level $LOG\_LEVEL --log-prefix

"fp=PORTSCAN:tcp a=REJECT "

iptables-A REJECT\_PORTSCAN -p udp -m limit --limit $LOG\_LIMIT --limit-burst $LOG\_LIMIT\_BURST -j LOG --log-level $LOG\_LEVEL --log-prefix

"fp=PORTSCAN:udp a=REJECT "

iptables-A REJECT\_PORTSCAN -p tcp -j REJECT --reject-with tcp-reset iptables-A REJECT\_PORTSCAN -p udp -j REJECT --reject-with icmp-port-unreachable

*3.2.6. Phát hiện quét cổng bằng Nmap.*

iptables-N DETECT\_NMAP

iptables-A DETECT\_NMAP -p tcp --tcp-flags ALL FIN,URG,PSH -m limit –limit

$LOG\_LIMIT --limit-burst $LOG\_LIMIT\_BURST -j LOG --log-level $LOG\_LEVEL --log-prefix "fp=NMAP:XMAS a=DROP "

iptables-A DETECT\_NMAP -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -m limit --limit $LOG\_LIMIT --limit-burst $LOG\_LIMIT\_BURST -j LOG --log-level $LOG\_LEVEL --log-prefix "fp=NMAP:XMAS-PSH a=DROP "

iptables-A DETECT\_NMAP -p tcp --tcp-flags ALL ALL -m limit --limit $LOG\_LIMIT --limit-burst $LOG\_LIMIT\_BURST -j LOG --log-level $LOG\_LEVEL --log-prefix "fp=NMAP:XMAS-ALL a=DROP "

iptables-A DETECT\_NMAP -p tcp --tcp-flags ALL FIN -m limit --limit $LOG\_LIMIT --limit-burst $LOG\_LIMIT\_BURST -j LOG --log-level $LOG\_LEVEL --log-prefix "fp=NMAP:FIN a=DROP "

iptables-A DETECT\_NMAP -p tcp --tcp-flags SYN,RST SYN,RST -m limit --limit $LOG\_LIMIT --limit-burst $LOG\_LIMIT\_BURST -j LOG --log-level $LOG\_LEVEL --log-prefix "fp=NMAP:SYN-RST a=DROP "

iptables-A DETECT\_NMAP -p tcp --tcp-flags SYN,FIN SYN,FIN -m limit --limit $LOG\_LIMIT --limit-burst $LOG\_LIMIT\_BURST -j LOG --log-level $LOG\_LEVEL --log-prefix "fp=NMAP:SYN-FIN a=DROP "

iptables-A DETECT\_NMAP -p tcp --tcp-flags ALL NONE -m limit --limit $LOG\_LIMIT --limit-burst $LOG\_LIMIT\_BURST -j LOG --log-level $LOG\_LEVEL --log-prefix "fp=NMAP:NULL a=DROP "

iptables-A DETECT\_NMAP -j DROP iptables-A INPUT -i eth0 -p tcp ! --syn -m state --state NEW -j DETECT\_NMAP

Đối với các gói TCP đến eth0 mở kết nối nhưng không đặt SYN=1 chúng ta sẽ chuyển sang chain DETECT NMAP. Đây là những gói không hợp lệ và hầu như là quét cổng bằng nmap hoặc kênh ngầm. Chain DETECT NMAP sẽ phát hiện ra hầu hết các kiểu quét của Nmap và tiến hành ghi nhật kí ở mức --limit $LOG LIMIT và --limit-burst $LOG LIMIT BURST. Ví dụ để kiểm tra quét XMAS, bạn dùng tùy chọn --tcp-flags ALL FIN,URG,PSH nghĩa là 3 cờ FIN, URG và PSH được bật, các cờ khác đều bị tắt. Các gói quà chain DETECT NMAP sau đó sẽ bị DROP hết.

*3.2.7. Chặn ngập lụt SYN.*

Gói mở TCP với cờ SYN được set 1 là hợp lệ nhưng không ngoại trừ khả năng là các gói SYN dùng để ngập lụt. Vì vậy, ở dây bạn đẩy các gói SYN còn lại qua chain CHECK SYNFLOOD để kiểm tra ngập lụt SYN như sau:

iptables-N CHECK\_SYNFLOOD

iptables-A CHECK\_SYNFLOOD -m limit --limit $SYN\_LIMIT --limit-burst

$SYN\_LIMIT\_BURST -j RETURN

iptables-A CHECK\_SYNFLOOD -m limit --limit $LOG\_LIMIT --limit-burst

$LOG\_LIMIT\_BURST -j LOG --log-level $LOG\_LEVEL --log-prefix

"fp=SYN FLOOD:warning a=DROP "

iptables-A CHECK\_SYNFLOOD -j DROP

iptables-A INPUT -i eth0 -p tcp --syn -j CHECK\_SYNFLOOD

**KẾT LUẬN**

Qua quá trình tìm hiểu và nghiên cứu về hệ thống bảo mật ở trong hệ điều hành linux, Nhóm 12 chúng em đã có thêm được kiến thức và đồng thời hiểu biết thêm nhiều điều về bảo mật nói chung và hệ thống bảo mật ở trong hệ điều hành linux nói riêng. Hiểu được tầm quan trọng của việc bảo mật thông tin, một số kiến thức tổng quan về hệ điều hành linux và đồng thời là cơ chế bảo vệ ở trong hệ điều hành linux. Nhờ đó có những kiến thức cần thiết ở trong ngành học Công Nghệ Thông Tin

Điều quan trọng hơn nữa là qua bài tập lớn này chúng em đã học tập được nhiều kinh nghiệm quý báu để làm việc theo nhóm, đồng thời học hỏi được nhiều phương pháp tìm kiếm, tra cứu thông tin. Chúng em đã tìm kiếm được nhiều thông tin bổ ích không những cho bài tập lớn của mình mà ngoài ra còn nhiều thông tin khác liên quan tới ngành học của mình thông qua các kênh thông tin khác nhau như sách và đặc biệt là mạng internet. Tuy nhiên, trong quá trình làm bài tập lớn, chúng em chưa có nhiều kinh nghiệm nên có thể gặp những sai sót, khiếm khuyết mong thầy giáo và các bạn chỉnh sửa, giúp đỡ.

*Chúng em xin chân thành cảm ơn!*

Nhóm sinh viên thực hiện

Một số nguồn bọn trên internet bọn em có tham khảo :

-  [Https://vilbo.asia](https://vilbo.asia)

-  [Https://tailieuxanh.com](https://tailieuxanh.com)

-  [Https://vi.wikipedia.org](https://vi.wikipedia.org)

-  [Https://quantrimang.com](https://quantrimang.com)

-  Https://securitybox.vn