BÁO CÁO THỰC HÀNH

**Bài thực hành số 03: Introduction Netfilter and Iptables**

**Môn học:** Hệ thống nhúng mạng không dây

**Lớp:** NT131.O12.MMCL.1

**THÀNH VIÊN THỰC HIỆN (Nhóm 11):**

|  |  |  |
| --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** |
| 1 | Lê Hoàng Khánh | 21522205 |
| 2 | Ngô Thế Anh | 21521826 |

|  |
| --- |
| **Điểm tự đánh giá** |
| **10** |

**ĐÁNH GIÁ KHÁC:**

|  |  |
| --- | --- |
| Tổng thời gian thực hiện | 1 tuần. |
| Phân chia công việc | Thế Anh: Iptables.  Hoàng Khánh: Netfilter. |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất, kiến nghị |  |

Phần bên dưới của báo cáo này là báo cáo chi tiết của nhóm thực hiện

MỤC LỤC

[**A.** BÁO CÁO CHI TIẾT 4](#_Toc151517564)

[1. Sửa lại file nkmod.c để hook chỉ DROP các gói tin UDP. 4](#_Toc151517565)

[a. Chỉnh sửa Code. 4](#_Toc151517566)

[b. Thực nghiệm. 4](#_Toc151517567)

[2. DROP các packet có source IP đến từ địa chỉ máy client, chẳng hạn như 192.168.20.22, ACCEPT tất cả các packet còn lại. 6](#_Toc151517568)

[a. Chỉnh sửa Code. 6](#_Toc151517569)

[b. Thực nghiệm. 6](#_Toc151517570)

[3. DROP các gói tin TCP và UDP đi đến với địa chỉ port đích là 80. 7](#_Toc151517571)

[a. Chỉnh sửa Code. 7](#_Toc151517572)

[b. Thực nghiệm. 7](#_Toc151517573)

[4. Tìm cách để in ra địa chỉ nguồn và địa chỉ đích của các gói tin khi thực hiện một tác vụ bất kỳ. 8](#_Toc151517574)

[a. Chỉnh sửa Code. 8](#_Toc151517575)

[b. Thực nghiệm. 8](#_Toc151517576)

[5. Chỉ cho phép các gói tin đi đến uit.edu.vn (biết trước địa chỉ IP) đi ra ngoài, DROP tất cả còn lại. 9](#_Toc151517577)

[a. Chỉnh sửa Code. 9](#_Toc151517578)

[b. Thực nghiệm. 9](#_Toc151517579)

[6. Chặn các gói tin Echo Request đến từ máy client. 10](#_Toc151517580)

[7. Cấm tất cả các gói tin UDP và TCP có port đích là 80 đến từ bất kỳ máy tính nào. 11](#_Toc151517581)

[8. Xoá tất cả rules, thiết đặt chặn các traffic từ máy Ubuntu đến địa chỉ IP máy client và ngược lại, các hoạt động khác bình thường. 12](#_Toc151517582)

[9. Cấm các gói tin đến từ dãy IP chứa máy client, chẳng hạn như 192.168.20.0/24 với IP máy client là 192.168.20.22. Điều gì sẽ xảy ra khi thiết đặt lệnh này? 13](#_Toc151517583)

[10. Để giải quyết điều đặt biệt từ câu số 9, chèn thêm 1 rule để địa chỉ IP Default Gateway có thể giao tiếp bình thường với máy Ubuntu. Kiểm tra lại kết quả thu được 14](#_Toc151517584)

[11. Thiết lập lệnh không cho phép client SSH vào máy Ubuntu. Hãy chứng minh điều đó? 15](#_Toc151517585)

[12. Tìm hiểu và trình bày về cuộc tấn công Deny of Service (DoS), thiết lập rule để phòng chống cuộc tấn công này. 16](#_Toc151517586)

[a. Deny of Service là gì? 16](#_Toc151517587)

[b. Rule phòng chống. 17](#_Toc151517588)

[**B.** TÀI LIỆU THAM KHẢO 18](#_Toc151517589)

# BÁO CÁO CHI TIẾT

## Sửa lại file nkmod.c để hook chỉ DROP các gói tin UDP.

### Chỉnh sửa Code.

Để thực hiện yêu cầu trên ta cần sử lại code như sau.

A screen shot of a computer

Description automatically generated

Khi gói tin đến netfilter sẽ kiểm tra protocol code của gói tin có phải 17 không tức protocol code của UDP nếu đừng thì sẽ log lại vài DROP gói tin này.

### Thực nghiệm.

Sau khi sửa code và complie, load module và thực nghiệm yêu cầu trên.

Thông qua iperf3 ta gửi gói tin UDP từ Client đến máy đã cài netfilter.



Có thể thấy iperf3 chỉ có thể thực hiện quá trình kết nối thông qua giao thức TCP nhưng không thể gửi gói tin UDP đi được.

Ta thử gửi gói tin TCP ở port 80 bằng iperf3.

A screenshot of a computer screen

Description automatically generated

Có thể thấy gói tin đã có thể gửi nhận bình thường thông qua giao thức TCP.

A screen shot of a computer

Description automatically generated

Kiểm tra log ta thấy netfilter đã hoạt động đúng yêu cầu.

## DROP các packet có source IP đến từ địa chỉ máy client, chẳng hạn như 192.168.20.22, ACCEPT tất cả các packet còn lại.

### Chỉnh sửa Code.

Để thực hiện yêu cầu trên ta cần sử lại code như sau.

A computer screen shot of a program

Description automatically generated

Sau khi chỉnh sửa, Netfilter sẽ tiến hành DROP gói tin nếu nó có source ip là 192.168.122.76.

### Thực nghiệm.

A screenshot of a computer screen

Description automatically generated

Có thể thấy gói tin từ Client có IP 192.168.122.76 đã bị DROP kèm theo đó gói tin của Client có ip khác đã được ACCEPT.

## DROP các gói tin TCP và UDP đi đến với địa chỉ port đích là 80.

### Chỉnh sửa Code.

A computer screen shot of a mountain range

Description automatically generated

Sau khi chỉnh sửa, Netfilter sẽ tiến hành kiểm tra cái gói tin có protocol code là 17 và 6 tương ứng với UDP và TCP tiếp sau đó sẽ kiểm tra port đích có phải 80 nếu thoả mãn mọi điều kiện gói tin sẽ bị DROP.

### Thực nghiệm.

Sử dụng iperf3 thực nghiêm yêu cầu trên. Lần lượt sẽ thực nghiệm gửi gói tin qua TCP, UDP ở port 80 và TCP ở port khác với port 80.

A city lights at night

Description automatically generated

Có thể thấy ở lần gửi gói tin qua TCP, UDP ở port 80 iperf3 đã không thể kết nối đến máy chạy Netfilter. Tuy nhiên ở lần gửi qua TCP với port khác 80 thì iperf3 đã hoạt động bình thường chứng tỏ mọi yêu cầu đã được thoả mãn.

## Tìm cách để in ra địa chỉ nguồn và địa chỉ đích của các gói tin khi thực hiện một tác vụ bất kỳ.

### Chỉnh sửa Code.

A screen shot of a computer

Description automatically generated

Sau khi chỉnh sửa, Netfilter sẽ tiến hành log lại địa chỉ nguồn và đích qua Kernel Log.

### Thực nghiệm.

A screenshot of a computer screen

Description automatically generated

Có thể thầy Netfilter đã log lại thông tin địa chỉ nguồn và đích thông qua Kernel Log.

## Chỉ cho phép các gói tin đi đến uit.edu.vn (biết trước địa chỉ IP) đi ra ngoài, DROP tất cả còn lại.

### Chỉnh sửa Code.

Đầu tiên ta sử dụng DNS Lookup để tìm ra địa chỉ IP của uit.edu.vn.

A screenshot of a computer

Description automatically generated

Ta biết được địa chỉ IP của uit.edu.vn sẽ là 118.69.123.140. Sau đó thực hiện chỉnh sửa code.

A screen shot of a computer program

Description automatically generated

Sau khi chỉnh sửa, Netfilter sẽ chỉ ACCEPT các gói tin có tin có địa chỉ nguồn và đích là 118.69.123.140 và DROP tất cả gói tin còn lại.

### Thực nghiệm.

A screenshot of a computer

Description automatically generated

Có thể thấy, có thể thực hiện request đến địa chỉ của uit.edu.vn kèm theo đó các gói tin có địa chỉ nguồn và đích khác với địa chỉ của uit.edu.vn đều bị DROP.

## Chặn các gói tin Echo Request đến từ máy client.

Để chặn gói tin Echo Request thông qua iptables ta sử dụng lệnh sau.

$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j REJECT

Qua lệnh trên iptables sẽ REJECT các gói tin gói tin đến có kiểu icmp là **echo-request.**

A building with many lights

Description automatically generated

Có thể thấy sau khi thực hiện lệnh trên thì đã không thể ping từ máy Client.

## Cấm tất cả các gói tin UDP và TCP có port đích là 80 đến từ bất kỳ máy tính nào.

Để cấm tất cả các gói tin UDP và TCP có port đích là 80 đến từ bất kỳ máy tính nào ta thực hiện lệnh sau.

$ sudo iptables -A INPUT -p tcp --dport 80 -j REJECT

$ sudo iptables -A INPUT -p udp --dport 80 -j REJECT

A screenshot of a computer program

Description automatically generated

Có thể thấy thông iperf3 gói tin đã không thể gửi đi được thông qua giao thức UDP và TCP tại port 80.

## Xoá tất cả rules, thiết đặt chặn các traffic từ máy Ubuntu đến địa chỉ IP máy client và ngược lại, các hoạt động khác bình thường.

Ta có IP của cline là 192.168.122.76. Để thực hiện yêu cầu trên ta thực hiện câu lệnh sau.

$ sudo iptables -A INPUT -s 192.168.122.76 -j REJECT

$ sudo iptables -A OUTPUT -d 192.168.122.76 -j REJECT

Qua câu lệnh trên iptables sẽ REJECT các gói tin đến có địa chỉ nguồn của Client và gói tin đi có địa chỉ địch của Client. Thông qua 2 câu lệnh trên sẽ đảm bằng Client và Server sẽ không thể kết nối được với nhau.

A screenshot of a computer program

Description automatically generated

Có thể thấy Client có địa chỉ 192.168.122.76 không thể kết nối được với Server tuy nhiên Client có địa chỉ khác có thể kết nối được đến Server.

## Cấm các gói tin đến từ dãy IP chứa máy client, chẳng hạn như 192.168.20.0/24 với IP máy client là 192.168.20.22. Điều gì sẽ xảy ra khi thiết đặt lệnh này?

Ta có IP mạng của Client là 192.168.122.0/24.

Để thực hiện yêu cầu trên ta sử dụng câu lệnh sau.

$ sudo iptables -A INPUT -s 192.168.122.0/24 -j REJECT

Thực nghiệm:

A screen shot of a computer

Description automatically generated

Có thể thấy sau khi chặn mọi gói tin đến từ mạng này toàn bộ gói tin từ Client trong mạng đều không thể đến được với Server.

Cùng theo đó Server cũng không thể truy cập được Internet do việc chặn IP mạng cũng chặn luôn gói tin phản hồi từ Default Gateway.

## Để giải quyết điều đặt biệt từ câu số 9, chèn thêm 1 rule để địa chỉ IP Default Gateway có thể giao tiếp bình thường với máy Ubuntu. Kiểm tra lại kết quả thu được

Để thực hiện yêu cầu ta sử dụng câu lệnh sau.

$ sudo iptables -I INPUT 1 -s 192.168.122.1 -j ACCEPT

Ta cần phải thêm rule ACCEPT gói tin từ Default Gateway vào đầu bảng hoặc nằm trên rule từ câu 9, do bảng filter sẽ duyệt từng rule từ trên xuống dưới.

A screenshot of a computer

Description automatically generated

Sau khi thực hiện thêm rule trên Server đã có thể kết nối đến Default Gateway.

## Thiết lập lệnh không cho phép client SSH vào máy Ubuntu. Hãy chứng minh điều đó?

Ta biết được server sử dụng cổng SSH mặc định là 22 và SSH sẽ hoạt động thông qua giao thức TCP.

Ta sẽ thực hiện yêu cầu trên qua câu lệnh sau.

$ sudo iptables -A INPUT -p tcp --dport 22 -j REJECT

Iptables sẽ tiến hành chặn các gói tin đến có giao thức là TCP và port là 22 tức port hoạt động của SSH trên Server.

A computer screen shot of a program

Description automatically generated

Có thể thấy các gói tin có thể gửi bình thường chỉ có SSH là không thể kết nối được.

## Tìm hiểu và trình bày về cuộc tấn công Deny of Service (DoS), thiết lập rule để phòng chống cuộc tấn công này.

### Deny of Service là gì?

Cuộc tấn công Denial of Service (DoS) là một hình thức tấn công mạng mà mục tiêu của nó là làm cho một dịch vụ hoặc hệ thống trở nên không thể sử dụng bởi người dùng hoặc ngăn chặn khả năng truy cập vào tài nguyên trực tuyến. Cuộc tấn công DoS nhằm vào việc làm quá tải hoặc làm cho hệ thống trở nên không thể truy cập bằng cách tạo ra một lượng lớn lưu lượng truy cập hoặc yêu cầu tới một dịch vụ hoặc máy chủ.

Dưới đây là một số đặc điểm chính của cuộc tấn công DoS:

* Quá tải tài nguyên: Cuộc tấn công DoS tạo ra một lượng lớn yêu cầu hoặc kết nối đến một dịch vụ hoặc máy chủ. Điều này có thể gây quá tải tài nguyên của hệ thống, bao gồm băng thông mạng, CPU, bộ nhớ, hoặc các tài nguyên khác.
* Mục tiêu đa dạng: Cuộc tấn công DoS có thể nhắm vào nhiều mục tiêu khác nhau, bao gồm trang web, máy chủ thư điện tử, dịch vụ trực tuyến, hoặc hệ thống mạng.
* Cách thức tấn công: Có nhiều cách thức khác nhau để thực hiện cuộc tấn công DoS. Một số ví dụ bao gồm tạo ra lưu lượng truy cập giả mạo, gửi yêu cầu không hợp lệ hoặc lừa đảo, tấn công phủ định băng thông, và nhiều phương pháp khác.
* Phân tán (DDoS): Đôi khi, tấn công DoS có thể được thực hiện bởi một nhóm máy tính hoặc thiết bị hoạt động đồng thời để tạo ra một cuộc tấn công lớn hơn được gọi là "cuộc tấn công phân tán" (DDoS). Các thiết bị này thường bị kiểm soát bởi kẻ tấn công mà không cần sự thông báo của chủ sở hữu.
* Hậu quả: Cuộc tấn công DoS có thể gây ra sự gián đoạn trong việc truy cập dịch vụ hoặc tài nguyên trực tuyến, dẫn đến mất mát kinh tế, tiêu cực hóa cho danh tiếng, và thậm chí có thể gây hại cho an ninh mạng nếu như cuộc tấn công làm cho hệ thống trở nên dễ bị xâm nhập trong thời gian đó.
* Để bảo vệ khỏi cuộc tấn công DoS, các tổ chức thường triển khai các biện pháp bảo mật mạng, bao gồm việc sử dụng tường lửa, giám sát lưu lượng mạng, giới hạn kết nối đồng thời, và sử dụng dịch vụ bảo vệ chống DDoS.

### Rule phòng chống.

Dưới đấy là một số RULE phòng trống tấn công DoS.

DROP các gói tin không hợp lệ.

$ iptables -t mangle -A PREROUTING -m conntrack --ctstate INVALID -j DROP

DROP các gói tin TCP mời và không được SYN

$ iptables -t mangle -A PREROUTING -p tcp ! --syn -m conntrack --ctstate NEW -j DROP

DROP gói tin SYN với giá trị MSS đáng ngờ

$ iptables -t mangle -A PREROUTING -p tcp -m conntrack --ctstate NEW -m tcpmss ! --mss 536:65535 -j DROP

Giới hạn số kết nối trên một địa chỉ IP nguồn.

$ iptables -A INPUT -p tcp -m connlimit --connlimit-above 111 -j REJECT --reject-with tcp-reset

Chống quét Port

$ iptables -N port-scanning

$ iptables -A port-scanning -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s --limit-burst 2 -j RETURN

$ iptables -A port-scanning -j DROP

# TÀI LIỆU THAM KHẢO