ĐẠI HỌC ĐÀ NẴNG

TRƯỜNG ĐẠI HỌC BÁCH KHOA

KHOA CÔNG NGHỆ THÔNG TIN

Tel. (+84.0236) 3736949, Fax. (84-511) 3842771

Website: http://dut.udn.vn/khoacntt, E-mail: cntt@dut.udn.vn

A blue and white logo with black text

Description automatically generated

BÁO CÁO THỰC TẬP TUẦN 2

THỰC TẬP TỐT NGHIỆP

Đề tài:

Gửi gói tin bằng Scapy để kiểm tra tường lửa.

|  |  |  |
| --- | --- | --- |
| Họ và tên | Mã số sinh viên | Lớp học phần |
| Thân Nguyên Minh Quân | 102200148 | 20Nh14 |
| Hoàng Huân | 102200131 | 20Nh14 |
| Huỳnh Nguyễn Tấn Sang | 102200230 | 20Nh14 |

CBHD: TS Nguyễn Thế Xuân Ly

Đà Nẵng, 11/2024

**Mục Lục**

I. NỘI DUNG TUẦN 2 3

II. TRIỂN KHAI CÁC YÊU CẦU 3

**1.** **Cài đặt Scapy và các thư viện cần thiết** 3

**2. Configure IPv6 VlanID** 4

**2.1.** **Thiết lập IPv6 trên Windows** 4

**2.2. Thiết lập VLAN ID trên Windows** 6

**3.** **Viết chương trình gửi và nhận gói tin bằng Scapy** 6

**3.1.** **Gửi gói tin ở máy nguồn** 6

**3.2.** **Nhận gói tin và xử lí payload ở máy đích** 6

**4.** **Demo** 7

**4.1.** **Đổi IP máy nguồn, gửi gói tin bằng Scapy** 7

**4.2**. **Đổi địa chỉ máy đích, không có tường lửa** 7

**4.2.1. IPv6** 7

**4.2.2.** **IPv4** 8

**4.3. Xây dựng tường lửa ngăn chặn** 9

**4.3.1. Rules chặn Ipv4** 9

**4.3.2. Rules chặn Ipv6** 10

**4.3.3. Rules tổng quát** 12

**4.4. Kết quả và nhận xét tổng thể báo cáo tuần 2** 13

# **NỘI DUNG TUẦN 2**

Tập trung vào Scapy với việc gửi gói tin từ Windows đến Raspberry Pi 4 để kiểm tra xem tường lửa có hoạt động tốt hay không. Scapy có thể giúp sửa đổi các gói tin Ethernet với trường này:  
 - Ethernet (địa chỉ MAC nguồn/đích, Ethertype)  
 - ID Vlan  
 - IPv4/IPv6  
 - Giao thức: TCP/UDP/ICMP...

Sau khi thiết lập IPv6 và VLAN trên Windows thì phát triển các chương trình python cho phép thay đổi các trường của gói tin Ethernet.

Giả sử đã thay đổi các tham số trên card mạng và điều chỉnh tương ứng trong mã nguồn. Thì cần triển khai những việc sau để kiểm tra và thay đổi tưởng lửa trên thiết bị đích (Raspberry).

1. Viết chương trình cho phép chạy trên Raspberry để nhận/gửi và thực thi các thay đổi tham số card mạng trên Raspbery từ máy nguồn Windows (đóng vai trò tấn công) //giả sử lúc này tường lửa trên Raspberry đã tắt.

2. Bật lại tường lửa trên Raspberry và kiểm tra lại việc có thực thi được thay đổi tham số card mạng hay không?

# **II. TRIỂN KHAI CÁC YÊU CẦU**

1. **Cài đặt Scapy và các thư viện cần thiết**

* Triển khai scapy trên Windows:

+ Tải về và cài đặt phiên bản mới nhất của pythong: https://www.python.org

+ Cài đặt python-pip:

+ Tải về get-pip.py (https://bootstrap.pypa.io/get-pip.py) và lưu vào cùng thư mục python đã cài

+ Mở cmd trong thư mục python đã cài và gõ lệnh sau để cài đặt python-pip

python get-pip.py



+ Sau khi cài đặt thành công python-pip thì gõ các lệnh sau để cài thêm các gói cần thiết:

*pip install scapy*

*pip install netaddr*

*pip install sqlalchemy*

**2. Configure IPv6 VlanID**

Hướng dẫn thiết lập IPv6 và VLAN ID trên Windows và WebOS trên Raspberry để kiểm tra kết quả thực thi chương trình (có thay đổi thông số IPv6 và VLAN ID) được hay không?)

### **2.1.** **Thiết lập IPv6 trên Windows**

Trên Windows: *Control Panel → Network Connection → Select Ethernet→ Properties → Internet Protocol Version 6 (TCP/IPv6)* và gõ địa chỉ sau (đây chỉ là địa chỉ ví dụ, có thể sử dụng địa chỉ IPv6 khác tuỳ ý)

IPv6 address: fd53:xxxx:xxx:5::13; Subnet prefix length: 64

A screenshot of a computer

Description automatically generated

Vào Settings hoặc dùng lệnh ifconfig để cấu hình IPv6 trên WebOS: IPv6 address: fd53:xxxx:xxx:5::14; Subnet prefix length: 64

Kiểm tra kết nối IPv6 giữa Windows và WebOS

***Windows + R → cmd → ping fd53:xxxx:xxx:5::14 -t***

A screenshot of a computer program

Description automatically generated

### **2.2. Thiết lập VLAN ID trên Windows**

*Control Panel --> Network Connection → Select Ethernet → Properties→ Configure → Advanced --> Set VLAN ID to 5*

1. **Viết chương trình gửi và nhận gói tin bằng Scapy**
   1. **Gửi gói tin ở máy nguồn**

**Import các thư viện cần thiết**   
 *from scapy.all import \**

*from scapy.layers.inet import \**

*from scapy.layers.inet6 import \**

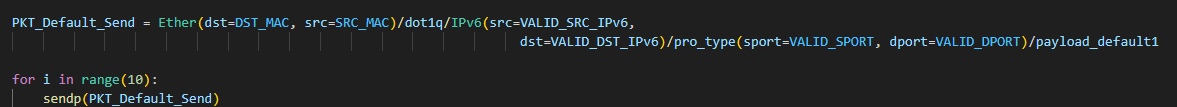
*from netaddr import \**

*from sqlalchemy import false*

**Các thông số cần thiết cho gói tin:**

SRC\_MAC,DST\_MAC,VLAN\_ID,VALID\_SRC\_IPv6,VALID\_DST\_IPv6VALID\_SPORT, VALID\_DPORT,pro\_type = TCP.

**Payload gửi gói tin:**



**Payload đổi Ipv6 của máy đích:**

A computer screen with text and numbers

Description automatically generated

* 1. **Nhận gói tin và xử lí payload ở máy đích**

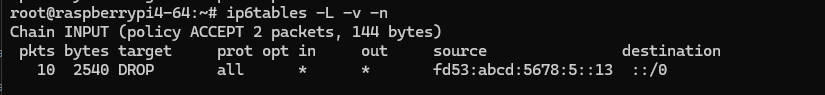
Lắng nghe các gói tin IPv4 và Ipv6 sau đó kiểm tra payload (raw\_payload) trong các gói tin đó. Nếu payload chứa lệnh os.system, nó sẽ thực thi lệnh đó trên hệ thống bằng cách sử dụng exec().

**A screen shot of a computer program

Description automatically generated**

1. **Demo**
   1. **Đổi IP máy nguồn, gửi gói tin bằng Scapy**

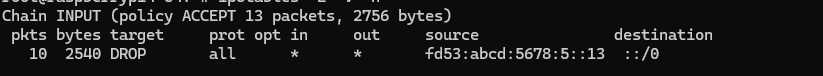
**Rules Iptables chặn Ipv4 10.10.22.115 và Ipv6 fd53:abcd:5678:5::13**



**Đổi IP nguồn thành địa chỉ khác sau đó gửi lại gói tin:**



**Không chặn được**



**Thay đổi địa chỉ MAC**



**Bắt gói tin bằng Wireshark địa chỉ MAC nguồn đã được đổi**

A screenshot of a computer

Description automatically generated

**4.2**. **Đổi địa chỉ máy đích, không có tường lửa**

**4.2.1. IPv6**

**Địa chỉ đích ban đầu**

A computer screen with white text

Description automatically generated

**Bật listen lắng nghe ở máy đích:**

A computer screen with white text

Description automatically generated

**Kết quả:   
A screen shot of a computer

Description automatically generated**

#### **IPv4**

**Payload**

A black screen with white text

Description automatically generated

**Địa chỉ đích ban đầu**

A screenshot of a computer program

Description automatically generated

**Bật listen để lắng nghe ở máy đích:**

A computer screen shot of a black background

Description automatically generated

**Kết quả:**

A screen shot of a computer

Description automatically generated

**4.3. Xây dựng tường lửa ngăn chặn**

**4.3.1. Rules chặn Ipv4**

**Payload tấn công:**

**A screen shot of a computer

Description automatically generated**

**Rules chặn:**

iptables -A INPUT -s 10.10.22.115 -j DROP

A screenshot of a computer program

Description automatically generated

**Kết quả:**

Thông báo chặn 10 gói tin

A screenshot of a computer

Description automatically generated

**Nhưng payload vẫn được thực thi:**

A computer screen with white text

Description automatically generated

**4.3.2. Rules chặn Ipv6**

**Ban đầu:**

**A computer screen with white text

Description automatically generated**

**Payload tấn công:**

A computer screen with white text

Description automatically generated

**Rules chặn:**

*ip6tables -A INPUT -s fd53:abcd:5678:5::13 -j DROP*

A screenshot of a computer program

Description automatically generated

**Kết quả:**

Các gói tin đến từ Ipv6 fd53:abcd:5678:5::13 đã bị chặn thành công bằng Iptables

A screen shot of a computer

Description automatically generated

**Tuy nhiên payload vẫn được thực thi:** IP đã bị đổi

A screen shot of a computer

Description automatically generated

**4.3.3. Rules tổng quát**

Sử dụng WhiteList để cho phép IP nguồn hợp lệ,kết nối TCP, Port 22, còn lại DROP INPUT.

A computer screen shot of white text

Description automatically generated

**Kết quả:** Iptables vẫn hoạt động tốt và chặn các gói tin.

Ipv6 chỉ accept IP hợp lệ còn lại DROP hết

A screenshot of a computer program

Description automatically generated

Ipv4 cũng tương tự

A computer screen with white text

Description automatically generated

**Tuy vậy thì payload vẫn được thực thi, lí do là:** iptables chỉ kiểm tra các thông tin ở **Layer 3 (IP)** và **Layer 4 (TCP)** như **địa chỉ IP** và **cổng**, chứ không phân tích dữ liệu trong **payload** (ví dụ lệnh os.system như trong code của nhóm).

**4.4. Kết quả và nhận xét tổng thể báo cáo tuần 2**

Về Scapy để gửi gói tin thì nhóm đã hoàn thành và cho ra kết quả như mong đợi là gửi gói tin với máy đích cũng như thay đổi IP nguồn để giả mạo tránh rules iptables.

Tường lửa vẫn hoạt động tốt và chặn các gói tin như đúng yêu cầu, tuy nhiên thì các payload trong gói tin vẫn hoạt động và exec thành công.

**Nhận xét**: Scapy là thư viện hỗ trợ gửi gói tin tốt trong Python và Iptables có thể drop các gói tin nhưng không thể chặn các payload trong gói tin thực thi.