**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG THƯƠNG**

**TP.HỒ CHÍ MINH**

**🙡🕮🙣**

A blue and white logo with a book and a cap

Description automatically generated

**BÀI BÁO CÁO**

**Môn:** [**Thực hành hệ thống tìm kiếm, ngăn ngừa và phát hiện xâm nhập**](https://sinhvien.hufi.edu.vn/sinh-vien/page-lhp.html?g=o5euUr8rWns8vCmS_s7AmymDwO452g0GFRZ34DzYADA5SC_4VMyGk-k4uuuDvhuuZ9oZxp4xmwPM-dWz0Grjsp77j5kPzbk_Cr_Kk7-DnbXjpBTqC1IUTFrXc9eVX6md)

**✍Đề tài:**

**LAB 2**

Giảng viên**: Bùi Duy Cương**

**SVTH:**

* Huỳnh Thanh Tâm MSSV: 2033210951

*TP. Hồ Chí Minh, ngày 30 tháng 5 năm 2024*

[Mô hình 3](#_Toc168948842)

[1.1 Thiết bị và phần mềm hỗ trợ 4](#_Toc168948843)

[Cấu hình thiết bị mạng 4](#_Toc168948844)

[1.2 Router 1 4](#_Toc168948845)

[1.3 Router 2 4](#_Toc168948846)

[1.4 Router 3 4](#_Toc168948847)

[1.5 Kali linux 5](#_Toc168948848)

[1.6 Win 7 5](#_Toc168948849)

[1.7 Server 6](#_Toc168948850)

[1.8 Cấu hình định tuyến RIP 7](#_Toc168948851)

[1.9 Kiểm tra kết nối giữa các PC 7](#_Toc168948852)

[Cấu hình Cisco IPS 8](#_Toc168948853)

[Thực hiện tấn công 11](#_Toc168948854)

[1.10 Phát hiện và ngăn chặn tấn công Ping of death từ Kali linux 11](#_Toc168948855)

[1.11 Phát hiện và ngăn chặn tấn công scan port 13](#_Toc168948856)

[1.12 Phát hiện và ngăn chặn tấn công Dos 16](#_Toc168948857)

# Mô hình

A diagram of a server

Description automatically generated

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Thiết bị | Interface | Địa chỉ IPv4 | Subnet mask | Default Gateway |
| SG1  (CISCO IPS) | F0/0 | 192.168.10.1 | 255.255.255.0 | N/A |
| S1/0 | 192.168.15.1 | 255.255.255.0 | N/A |
| F1/0 | 192.168.7.1 | 255.255.255.0 | N/A |
| SG2 | S1/0 | 192.168.15.2 | 255.255.255.0 | N/A |
|  | S1/1 | 192.168.20.1 | 255.255.255.0 | N/A |
| SG3 | S1/0 | 192.168.20.2 | 255.255.255.0 | N/A |
|  | F0/0 | 192.168.14.1 | 255.255.255.0 | N/A |
| Kali linux  (Attacker) | F0/0 | 192.168.14.20 | 255.255.255.0 | 192.168.14.1 |
| Server  (Victim) | F0/0 | 192.168.10.33 | 255.255.255.0 | 192.168.10.1 |
| Admin  (SDM) | F0/0 | 192.168.7.21 | 255.255.255.0 | 192.168.7.1 |

## Thiết bị và phần mềm hỗ trợ

* Phần mềm GNS3
* Phần mềm VMWARE
* 3 router
* PC-1: Server với web server
* PC-2: Window7 với SDM
* PC-3: Kali linux

# Cấu hình thiết bị mạng

## Router 1

|  |
| --- |
| R1# configure terminal  R1(config)# interface f0/0  R1(config-if)# ip address 192.168.10.1 255.255.255.0  R1(config-if)# no shutdown  R1(config-if)# exit  R1(config)# interface f0/1  R1(config-if)# ip address 192.168.7.1 255.255.255.0  R1(config-if)# no shutdown  R1(config-if)# exit  R1(config)# interface s1/0  R1(config-if)# ip address 192.168.15.1 255.255.255.0  R1(config-if)# no shutdown |

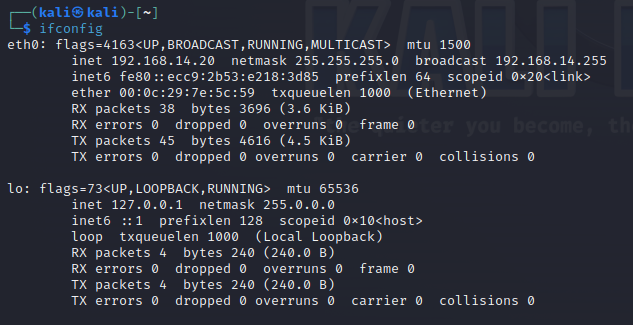
## Router 2

|  |
| --- |
| R2# configure terminal  R2(config)# interface s1/0  R2(config-if)# ip address 192.168.15.2 255.255.255.0  R2(config-if)# no shutdown  R2(config-if)# exit  R2(config)# interface s1/1  R2(config-if)# ip address 192.168.20.1 255.255.255.0  R2(config-if)# no shutdown |

## Router 3

|  |
| --- |
| R3# configure terminal  R3(config)# interface s1/0  R3(config-if)# ip address 192.168.20.2 255.255.255.0  R3(config-if)# no shutdown  R3(config-if)# exit  R3(config)# interface f0/0  R3(config-if)# ip address 192.168.14.1 255.255.255.0  R3(config-if)# no shutdown |

## Kali linux



## Win 7

A screenshot of a computer

Description automatically generated

## Server

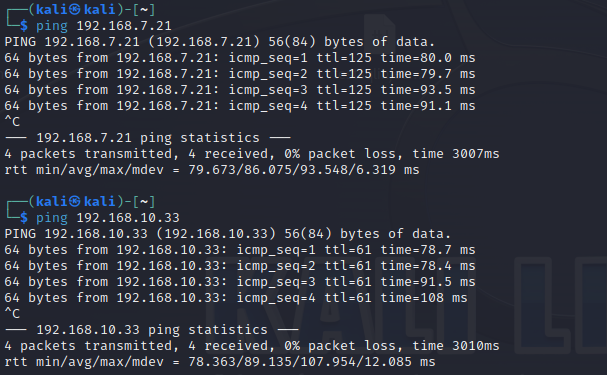
A screen shot of a computer

Description automatically generated

## Cấu hình định tuyến RIP

|  |
| --- |
| Router R1  R1(config)# router rip  R1(config-router)# version 2  R1(config-router)# network 192.168.10.0  R1(config-router)# network 192.168.7.0  R1(config-router)# network 192.168.15.0  Router R2  R2(config)# router rip  R2(config-router)# version 2  R2(config-router)# network 192.168.15.0  R2(config-router)# network 192.168.20.0  Router R3  R3(config)# router rip  R3(config-router)# version 2  R3(config-router)# network 192.168.20.0  R3(config-router)# network 192.168.14.0 |

## Kiểm tra kết nối giữa các PC



# Cấu hình Cisco IPS

A screen shot of a computer

Description automatically generated

Cài đặt SDM trên win7

Tải file SDM giải nén và chạy file SetupA screenshot of a computer

Description automatically generated

* Next

A screenshot of a computer

Description automatically generated

* Next

A screenshot of a software

Description automatically generated

* Tiếp tục đợiA screenshot of a computer security

  Description automatically generatedNhập user password , Đợi tiếp tục và import các signatureA computer screen shot of a computer

  Description automatically generated

# Thực hiện tấn công

## Phát hiện và ngăn chặn tấn công Ping of death từ Kali linux

GỬI GÓI TIN TỚI SERVER VỚI KÍCH THƯỚC LÀ 20000

**Attcker**

A computer screen shot of a program

Description automatically generated

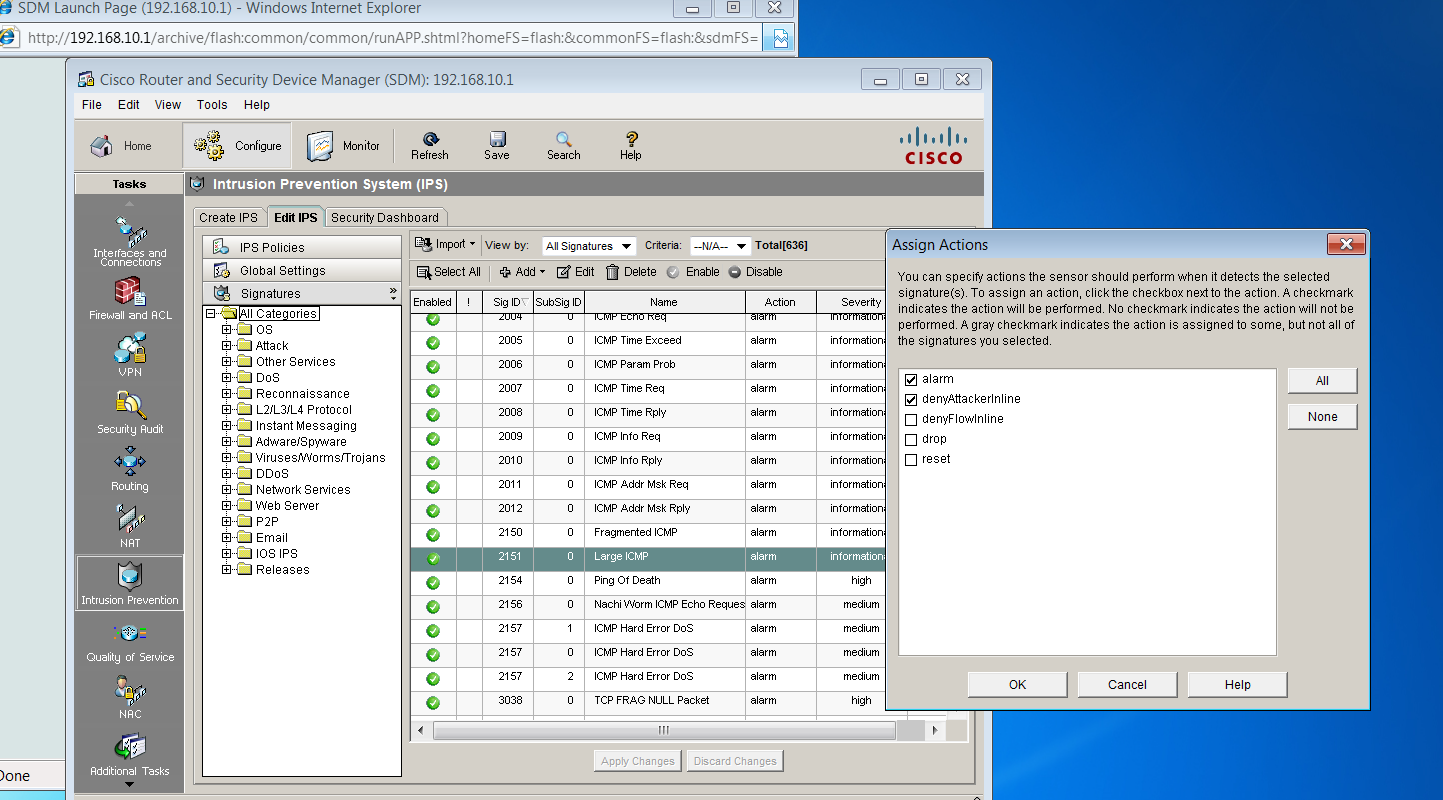
**Router R1**

A screen shot of a computer screen

Description automatically generated

Tiến hành chặn trên ADMIN -SDM

Tại Sig 2151



Click chuột phải chọn actions . Chọn denyAttackerInline và nhấn ok. Apply Changs để áp dụng.

**Kết quả :**

A computer screen with white text

Description automatically generated

**Bị chặn .**

## Phát hiện và ngăn chặn tấn công scan port

**Attcker**

A computer screen shot of a program

Description automatically generated

**Router R1**

A screen shot of a computer screen

Description automatically generated

Tại SIG:3042

A screenshot of a computer

Description automatically generated

Click chuột phải chọn actions . Chọn denyAttackerInline và nhấn ok. Apply Changs để áp dụng.

**Kết quả :**A computer screen shot of a computer program

Description automatically generated

## Phát hiện và ngăn chặn tấn công Dos

**Attacker**

A screen shot of a computer

Description automatically generated

**Router R1**

A black screen with yellow text

Description automatically generated

Chặn trên ADMIN -SDM

SIG ID : 3051

A computer screen shot of a computer

Description automatically generated

**Kết quả:**

A screenshot of a computer

Description automatically generated