**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:**

**LAB3**

Giảng viên**: Bùi Duy Cương**

**SVTH:**

* Huỳnh Thanh Tâm MSSV: 2033210951

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

[Mô hình 4](#_Toc168619783)

[Mục tiêu 4](#_Toc168619784)

[Kịch bản 5](#_Toc168619785)

[Thực hiện 5](#_Toc168619786)

[1.1 Thiết lập các thông số mạng cho các máy 5](#_Toc168619787)

[1.2 Phát cảnh báo và ngăn chặn tấn công Ping of death 8](#_Toc168619788)

[1.3 Phát cảnh báo và ngăn chặn tấn công Scanning Port 10](#_Toc168619789)

[1.4 Phát cảnh báo và ngăn chặn tấn công vào PORT 22 12](#_Toc168619790)

[1.5 Phát hiện và ngăn chặn tấn công UDP testing 13](#_Toc168619791)

[1.6 Cảnh báo và ngăn chặn HTTP test 15](#_Toc168619792)

[1.7 Attacker tấn công đến Victim theo các kịch bản: 17](#_Toc168619793)

[1.7.1 TCP Connect 17](#_Toc168619794)

[1.7.2 TCP SYN 19](#_Toc168619795)

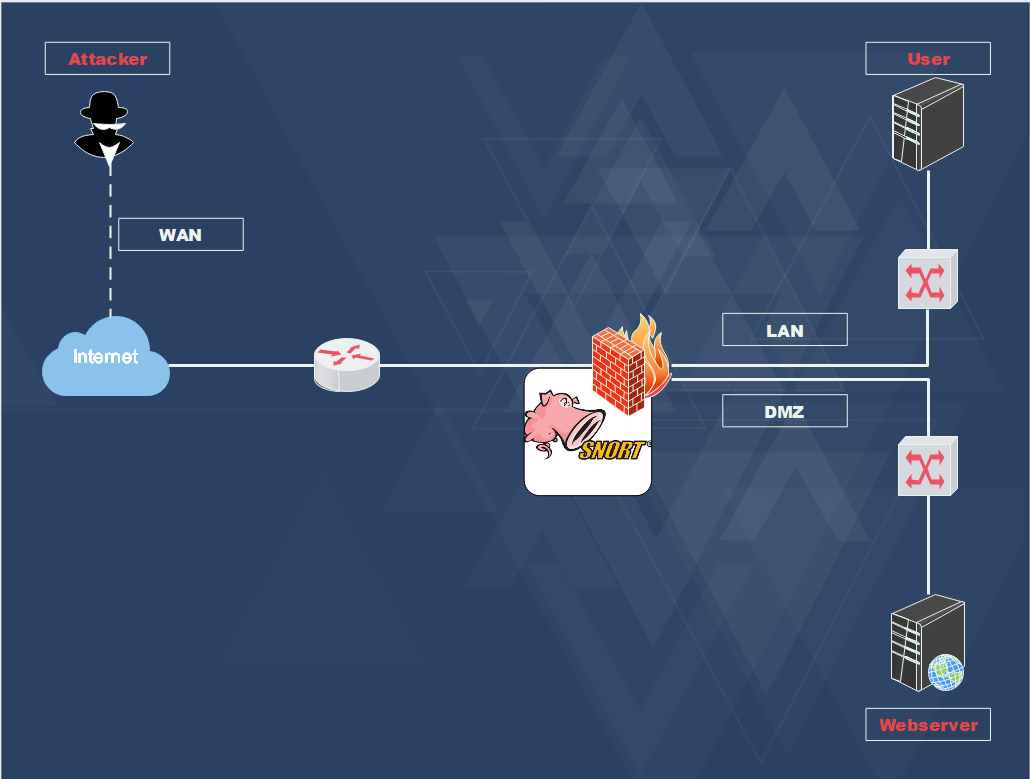
[1.7.3 TCP ACK 20](#_Toc168619796)

[1.7.4 UDP Connect 22](#_Toc168619797)

[1.8 Sử dụng công cụ Metasploit hoặc HPing3 để thực hiện kỹ thuật tấn công Syn flood 23](#_Toc168619798)

[1.9 Biên soạn và thực hiện thêm 1 kịch bản mới (khác biệt so với các câu trên) dựa trên mô hình có sẵn 25](#_Toc168619799)

# Mô hình



|  |  |  |  |
| --- | --- | --- | --- |
| Máy | Hệ điều hành | Địa chỉ IPv4 | Interface |
| Attacker | Kali linux | 192.168.11.129/24 | VMNet 8 |
| IDS/IPS | Pfsense | 192.168.11.139/24  192.168.10.100/24  192.168.20.10/24 | VMNet 8 (WAN)  VMNet 1 (LAN)  VMNet 2 (DMZ) |
| User | Window 10 | 192.168.10.8 | VMMet 1 |
| Victim | Ubuntu 8.04 | 192.168.20.19 | VMMet 2 |

Phần mềm triển khai Vmware Workstation, các hệ điều hành liên quan.

# Mục tiêu

Cài đặt snort trên pfsense

Xây dựng các tình huống/ kịch bản cho việc khảo sát hệ thống Snort IDS/IPS

# Kịch bản

Giả lập hệ thống pfsense Snort IDS/IPS , phát hiện và ngăn chặn các xâm nhập của attacker đến victim trong môi trường mạng. Từ đó, phát triển các kịch bản, tình huống, khác nhau nhằm tìm hiểu, phân tích, khảo sát, thực nghiệm hệ thống Snort IDS/IPS.

# Thực hiện

## Thiết lập các thông số mạng cho các máy

Attacker

* Các thông số mạng

A screenshot of a computer screen

Description automatically generated

* Kiểm tra kết nối máy Victim

A screenshot of a computer program

Description automatically generated

Pfsense

* Các thông số mạng

A black screen with white text

Description automatically generated

* Kiểm tra kết nối

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Victim

* Các thông số mạng

A screenshot of a computer

Description automatically generated

* Kiểm tra kết nối

A screen shot of a computer

Description automatically generated

Cài đặt snort trên pfsense

System-> package manager

A screenshot of a computer

Description automatically generated

* Available Packages

A screenshot of a computer

Description automatically generated

* Tìm kiếm snort -> install

A screenshot of a computer

Description automatically generated

## Phát cảnh báo và ngăn chặn tấn công Ping of death

Attacker tấn công victim

* Attack sử dụng Ping of Death thông qua lệnh :

ping 192.168.20.19 -s 10000

* Lưu lượng ICMP trên Wireshark của máy Victim

A screenshot of a computer

Description automatically generated

Viết rule phát cảnh báo khi gặp tấn công Ping of death

* Truy cập Services -> Snort -> Add interface DMZ -> DMZ rule -> Custom rules

alert icmp any any -> $HOME\_NET any (msg:"--> Ping of death attack!"; dsize:>10000; gid:1000001; sid:1000001;rev:1;)

* Cách cảnh báo được gửi về

A screenshot of a computer

Description automatically generated

* Cập nhật rule ngăn chặn tấn công Ping of Death

drop icmp any any -> $HOME\_NET any (msg:"--> chan Ping of death attack!"; dsize:>10000; gid:1000002; sid:1000002;rev:1;)

* Các log được gửi về

A screenshot of a computer

Description automatically generated

## Phát cảnh báo và ngăn chặn tấn công Scanning Port

alert tcp any any -> 192.168.20.19 81 (msg:"Scanning Port 81"; sid:1000005; rev:1;)

attacker

A computer screen with white text

Description automatically generated

* Hiển thị log cảnh báo

A screenshot of a computer

Description automatically generated

* Cập nhật rule ngăn chặn scanning port

drop tcp any any -> 192.168.20.19 81 (msg:"Scanning Port 81"; sid:1000006; rev:1;)

* Hiển thị log ngăn chặn

A screenshot of a computer

Description automatically generated

## Phát cảnh báo và ngăn chặn tấn công vào PORT 22

alert tcp any any -> any 22 (msg:"ssh connection=>Attempt"; sid:1000004;)

attacker

A screen shot of a computer

Description automatically generated

* Hiển thị log cảnh báo

A screenshot of a computer

Description automatically generated

* Cập nhật rule ngăn chặn connect tới Port 22

drop tcp any any -> any 22 (msg:"chan ssh connection=>Attempt"; sid:1000004;)

* Hiển thị log ngăn chặn

A screenshot of a computer

Description automatically generated

## Phát hiện và ngăn chặn tấn công UDP testing

Attacker

A close up of a computer screen

Description automatically generated

* Hiển thị log cảnh báo

A screenshot of a computer

Description automatically generated

* Cập nhật rule ngăn chặn gửi gói tin UDP

drop udp any any -> any any (msg:"chan UDP Tesing Rule"; sid:1000006;rev:1;)

* Hiển thị log ngăn chặn

A screenshot of a computer

Description automatically generated

## Cảnh báo và ngăn chặn HTTP test

Attacker

A computer screen with numbers and symbols

Description automatically generated

* Hiển thị log cảnh báo

A screenshot of a computer

Description automatically generated

* Cập nhật rule ngăn chặn

drop tcp any any -> $HOME\_NET 80 (msg:"chan HTTP Test!!!"; classtype:not-suspicious; sid:1000005; rev:1;)

* Hiển thị log ngăn chặn

A screenshot of a computer

Description automatically generated

## Attacker tấn công đến Victim theo các kịch bản:

### TCP Connect

Attacker

A screenshot of a computer program

Description automatically generated

* Hiển thị log cảnh báo

A screenshot of a computer

Description automatically generated

* Cập nhật rule ngăn chặn

drop tcp any any -> $HOME\_NET any (msg:"chan TCP Connect Scan Detected"; flags:S; sid:1000001; rev:1;)

* Hiển thị log ngăn chặn

A screenshot of a computer

Description automatically generated

### TCP SYN

alert tcp any any -> $HOME\_NET any (msg:"TCP SYN Scan Detected"; flags:S; sid:1000002; rev:1;)

Attacker

A computer screen shot of a computer

Description automatically generated

* Hiển thị log cảnh báo

A screenshot of a computer

Description automatically generated

* Cập nhật rule ngăn chặn TCP SYN

drop tcp any any -> $HOME\_NET any (msg:"chan TCP SYN Scan Detected"; flags:S; sid:1000002; rev:1;)

* Hiển thị log ngăn chặn

A screenshot of a computer

Description automatically generated

### TCP ACK

alert tcp any any -> $HOME\_NET any (msg:"TCP ACK Scan Detected"; flags:A; sid:1000004; rev:1;)

attacker

A computer screen shot of a computer code

Description automatically generated

* Hiển thị log cảnh báo

A screenshot of a computer

Description automatically generated

* Cập nhật rule ngăn chặn

drop tcp any any -> $HOME\_NET any (msg:"chan TCP ACK Scan Detected"; flags:A; sid:1000009; rev:1;)

* Hiển thị log ngăn chặn

A screenshot of a computer

Description automatically generated

### UDP Connect

alert udp any any -> $HOME\_NET any (msg:"UDP Connect Scan Detected"; sid:1000005; rev:1;)

attacker

A screen shot of a computer

Description automatically generated

* Hiển thị log cảnh báo

A screenshot of a computer

Description automatically generated

* Cập nhật rule ngăn chặn

drop udp any any -> $HOME\_NET any (msg:"chan UDP Connect Scan Detected"; sid:1000008; rev:1;)

* Hiển thị log ngăn chặn

A screenshot of a computer

Description automatically generated

## Sử dụng công cụ Metasploit hoặc HPing3 để thực hiện kỹ thuật tấn công Syn flood

alert tcp any any -> $HOME\_NET any (msg:"Syn Flood Detected"; flags:S; threshold:type threshold, track by\_src, count 100, seconds 10; sid:1000008; rev:1;)

attacker

A screenshot of a computer

Description automatically generated

* hiển thị log cảnh báo

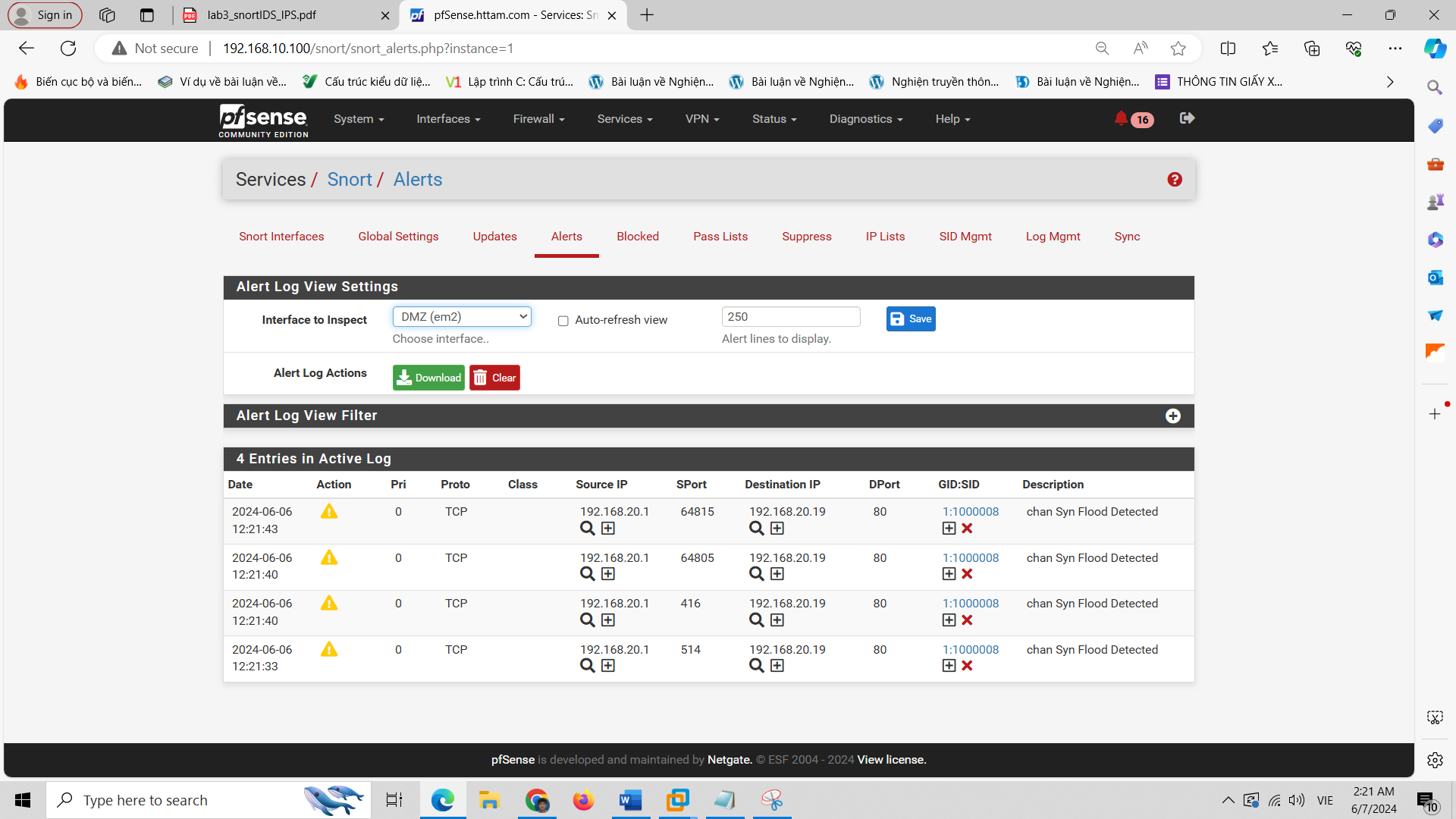
A screenshot of a computer

Description automatically generated

* cập nhật rule ngăn chặn

drop tcp any any -> $HOME\_NET any (msg:"chan Syn Flood Detected"; flags:S; threshold:type threshold, track by\_src, count 100, seconds 10; sid:1000008; rev:1;)

* hiển thị log ngăn chặn



## Biên soạn và thực hiện thêm 1 kịch bản mới (khác biệt so với các câu trên dựa trên mô hình có sẵn

Tấn công sql injection

Rule

alert tcp any any -> any 80 (msg:"SQL Injection Attempt"; flow:to\_server,established; content:"'"; nocase; content:" or "; nocase; pcre:"/(\%27)|(\')|(\-\-)|(\%23)|(#)/i"; classtype:web-application-attack; sid:1000001; rev:1;)

Attacker

1. Tạo payload.txt
2. Tạo testsqlinjection.sh
3. Cấu hình file

#!/bin/bash

# URL của trang web bạn muốn kiểm thử

url="http://192.168.20.19/dvwa/login.php"

# Đọc từng dòng trong tệp payloads.txt và gửi yêu cầu POST

while IFS= read -r payload

do

# Gửi yêu cầu HTTP POST với payload

response=$(curl -s -o /dev/null -w "%{http\_code}" -X POST -d "username=${payload}&password=anypassword" "$url")

# Kiểm tra mã trạng thái HTTP và hiển thị phản hồi

echo "Payload: $payload => HTTP Status: $response"

done < "payloads.txt"

1. Chạy file

A screenshot of a computer screen

Description automatically generated

* Hiển thị log cảnh báo

A screenshot of a computer

Description automatically generated

* Cập nhật rule ngăn chặn tấn công SQL injection

drop tcp any any -> any 80 (msg:"chan SQL Injection Attempt"; flow:to\_server,established; content:"'"; nocase; content:" or "; nocase; pcre:"/(\%27)|(\')|(\-\-)|(\%23)|(#)/i"; classtype:web-application-attack; sid:1000001; rev:1;)

* Hiển thị log ngăn chặn

A screenshot of a computer

Description automatically generated