**LAB 3: Pfsense tích hợp IDS/IPS**

1. **Mô hình thực hiện**

**A diagram of a computer

Description automatically generated**

**Kịch bản:** : Kẻ tấn công sử dụng Kali Linux để thực hiện tấn công vào server. Kẻ tấn công sử dụng kỹ thuật tấn công DoS gửi lượng lớn các gói tin đến server để tiến hành tấn công nhằm mục đích đánh sập server.

1. **Chuẩn bị mô hình**
2. **Pfsense với 2 card mạng Vmnet 1 và Vmnet 8**

Card mạng Lan 192.168.10.100/24

Card mạng Wan 192.168.89.128/24

A screenshot of a computer

Description automatically generated

1. **Máy window 10 đóng vai trò cấu hình Pfsense (Vmnet1)**

Ip của máy là 192.168.10.101/24

A computer screen shot of a computer screen

Description automatically generated

1. **Máy server đóng vai trò nạn nhân (Vmnet1)**

Ip của máy là 192.168.10.102/24

A computer screen shot of a computer

Description automatically generated

1. **Máy kali đóng vai trò attacker (Vmnet8)**

Ip của máy là 192.168.89.130/24

A computer screen shot of a computer screen

Description automatically generated

1. **Kiểm tra máy kali với card mạng Vmnet8 có thể ping thấy máy server với card mạng Vmnet1 và ngược lại**

A computer screen shot of a computer screen

Description automatically generated

A computer screen shot of a computer screen

Description automatically generated

1. **Cài đặt Snort trên Pfsense**

A screenshot of a computer

Description automatically generated

1. **Viết Rules**
2. **Rules chống ddos**

reject tcp any any -> any any (msg:"phát hiện & ngăn chặn tấn công dos"; sid: 1000005; rev:1; detection\_filter:track by\_dst, count 500, seconds 3;)

reject udp any any -> any any (msg:"phát hiện & ngăn chặn tấn công dos"; sid: 1000006; rev:1; detection\_filter:track by\_dst, count 500, seconds 3;)

1. **Rules chống Nmap scan**

alert tcp any any -> 192.168.10.102 any (msg:"Nmap Scan Detected"; flow:to\_server,established; content:"Nmap"; nocase; detection\_filter:track by\_src, count 10, seconds 60; sid:1000001;)

1. **Thử nghiệm**
2. **Dos attack**

A screenshot of a computer

Description automatically generated

Sử dụng tool PentMenu để Dos máy server

A screenshot of a computer

Description automatically generated

Tiến hành TCP SYN FLOOD

A screenshot of a computer

Description automatically generated

Kết quả hiển thị, Snort phát hiện và ngăn chặn.