**ĐẠI HỌC BÁCH KHOA HÀ NỘI**

**TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**─────── \* ───────**

****

**BÁO CÁO TUẦN 3**

Môn học: Project II (IT - 3931)

Đề tài: Network Security with IDS/IPS: Detection and Prevention of Network Attacks in a Virtualized Environment

|  |  |
| --- | --- |
| **Sinh viên thực hiện:** | **Ngô Trung Hiếu - 20225316**  **Kỹ thuật máy tính 04 – K67** |
| **Giảng viên hướng dẫn:** | **Nguyễn Quốc Khánh** |

**Hà Nội – 2025**

**Mục lục**

**No table of contents entries found.**

Đặt địa chỉ IP tĩnh

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

NAT rule trên pfsense cho phép gói tin ICMP đi từ máy ảo attacker (10.0.2.4) đi đến máy ảo victim (192.168.1.101)

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

Tải snort cho pfsense, ta vào System 🡪 Package Manager 🡪 Available Packages. Sau đó ta tìm kiếm snort package để tải về.

A screenshot of a computer

AI-generated content may be incorrect.

Sau đó ta có thể kiểm tra kết quả download ở Installed Packages

A screenshot of a computer

AI-generated content may be incorrect.

Tạo thêm rule cho phép máy ảo attacker truy cập website dvwa trên máy ảo victim. Ta vào Firewall 🡪 NAT 🡪 Port Forward, vào thêm 2 rule cho phép máy ảo attacker gửi gói tin TCP cổng 80 (http) và 443 (https) truy cập đến DVWA trên máy ảo victim.

A screenshot of a computer

AI-generated content may be incorrect.

Truy cập website DVWA trên máy ảo attacker với url: <http://192.168.1.101/dvwa>, trong đó 192.168.1.101 là địa chỉ IP của máy ảo victim. Tài khoản và mật khẩu truy cập lần lượt là *dvwa* và *password*

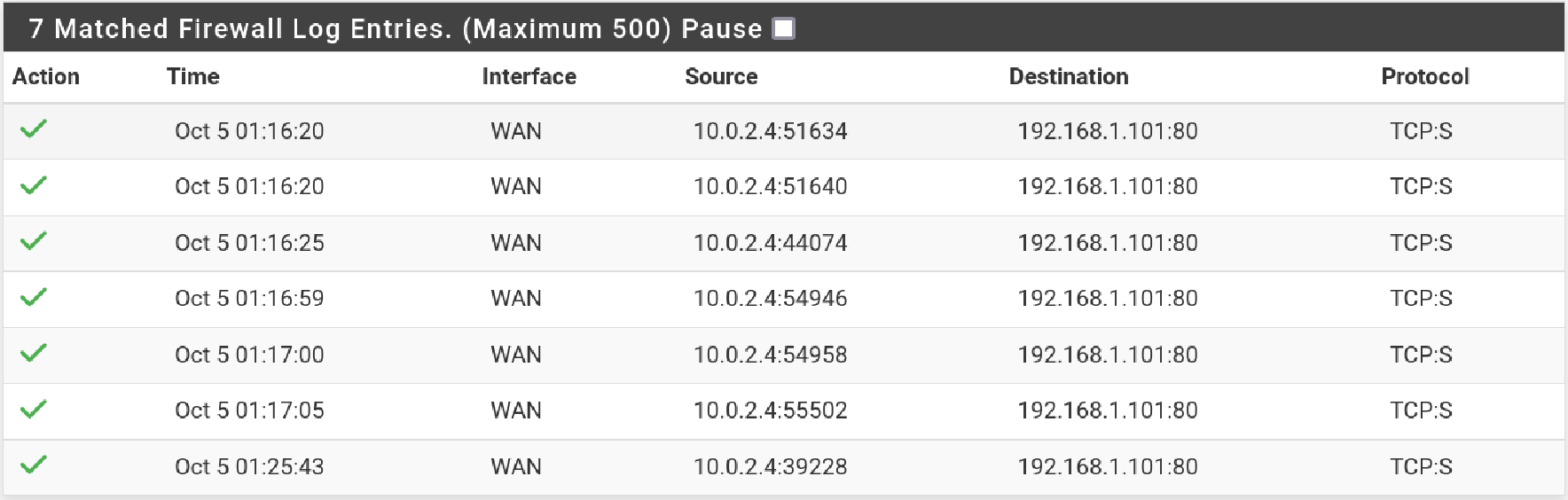
A screenshot of a computer

AI-generated content may be incorrect.

Màn hình chính

A screenshot of a computer

AI-generated content may be incorrect.



Snort package là tập hợp đầy đủ các thành phần giúp phát hiện, cảnh báo và ngăn chặn tấn công mạng. Trong đó:

Snort Engine: lõi xử lý, phân tích gói tin mạng.

Rules: tập luật phát hiện tấn công (community, registered, ET).

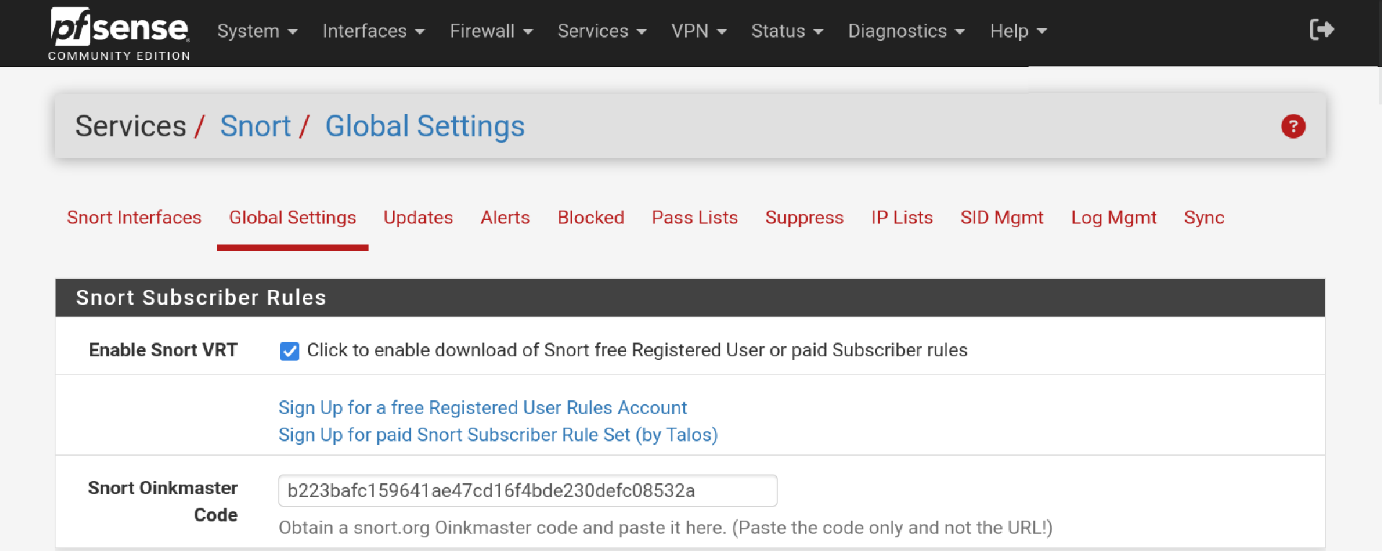
Preprocessors: tiền xử lý gói tin, phát hiện bất thường như port scan, HTTP lỗi.

Detection Engine: so khớp gói tin với rules để phát hiện hoặc chặn tấn công.

Output Plugins: ghi log, cảnh báo hoặc xuất dữ liệu ra giao diện.

Giao diện quản lý (GUI): trên pfSense giúp cấu hình, xem alert và cập nhật rules dễ dàng.

Vì nó bao gồm các tập luật sẽ có ích trong việc thử nghiệm các tấn công mà không phải viết lại tự đầu, nên ta sẽ cài Snort package trên pfSense và cấu hình global. Ta chọn Service 🡪 Snort 🡪 Global Settings. Chọn *Enable Snort VRT* để cho phép tải xuống các tập luật miễn phí, và chọn một số Snort package của community.



A screenshot of a computer

AI-generated content may be incorrect.

Sau khi lựa chọn các package xong ta chọn *Save* để Snort có thể bắt đầu tải về. Ta có thể xem tình trạng tải xuống ở Services 🡪 Snort 🡪 Updates.

A screenshot of a computer

AI-generated content may be incorrect.

Để có thể tạo luật cho chế độ IDS Snort, ta sẽ sang Services 🡪 Snort 🡪 Interfaces.

A screenshot of a computer

AI-generated content may be incorrect.

Em sẽ tạo luật phát hiện gói tin ICMP của máy ảo attacker gửi cho máy ảo victim với thông điệp *“ICMP detected 10.0.2.4”*. Sau đó, để kiểm tra luật có hoạt động thành công không, ta thử ping từ attacker sang victim, rồi qua phần Services 🡪 Snort 🡪 Alerts.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Ta kiểm tra tương tự với gói tin TCP khi đăng nhập trang web dvwa trên máy ảo victim được máy ảo attacker gửi đi.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Ngoài ra, ta có thể xuất file .pcap từ pfsense để có thể lấy gói tin đó cho Wireshark phân tích nội dung. Đầu tiên, ta vào Diagnostics 🡪 Packet Capture và chọn *Start* để pfsense bắt đầu lắng nghe.

A screenshot of a computer

AI-generated content may be incorrect.

Sau đó ta đăng nhập vào dvwa từ máy attacker.

A screenshot of a computer

AI-generated content may be incorrect.

Cuối cùng chọn chọn *Stop* để có thể xuất gói .pcap và mở nó bằng Wireshark.

A screenshot of a computer

AI-generated content may be incorrect.