BỘ CÔNG THƯƠNG

**TRƯỜNG ĐẠI HỌC CÔNG THƯƠNG TP. HCM**

**KHOA CÔNG NGHỆ THÔNG TIN**

---------------------------



**BÁO CÁO MÔN HỌC**

**THỰC HÀNH HỆ THỐNG TÌM KIẾM, NGĂN NGỪA VÀ PHÁT HIỆN XÂM NHẬP**

**HỌ VÀ TÊN: Võ Văn Vũ Nhân**

**MSSV: 2033210904**

**LỚP: 12DHBM07**

*TP. HỒ CHÍ MINH, tháng 06 năm 2024*

Mục lục

[I. Mô hình: 3](#_Toc169106906)

[II. Tiến hành cài đặt 4](#_Toc169106907)

[1. Cài đặt snort trên pfsense 4](#_Toc169106908)

[2. Thông số mạng của thiết bị, test ping 5](#_Toc169106909)

[3. Ping of death 6](#_Toc169106910)

[4. Tiến hành thực hiện ở một số rule khác: 10](#_Toc169106911)

*[4.1.](#_Toc169106912)**[Scaning port 81:](#_Toc169106912)* [10](#_Toc169106912)

*[4.2.](#_Toc169106913)**[Kiểm tra kết nối ftp:](#_Toc169106913)* [12](#_Toc169106913)

*[4.3.](#_Toc169106914)**[Testing UDP](#_Toc169106914)* [14](#_Toc169106914)

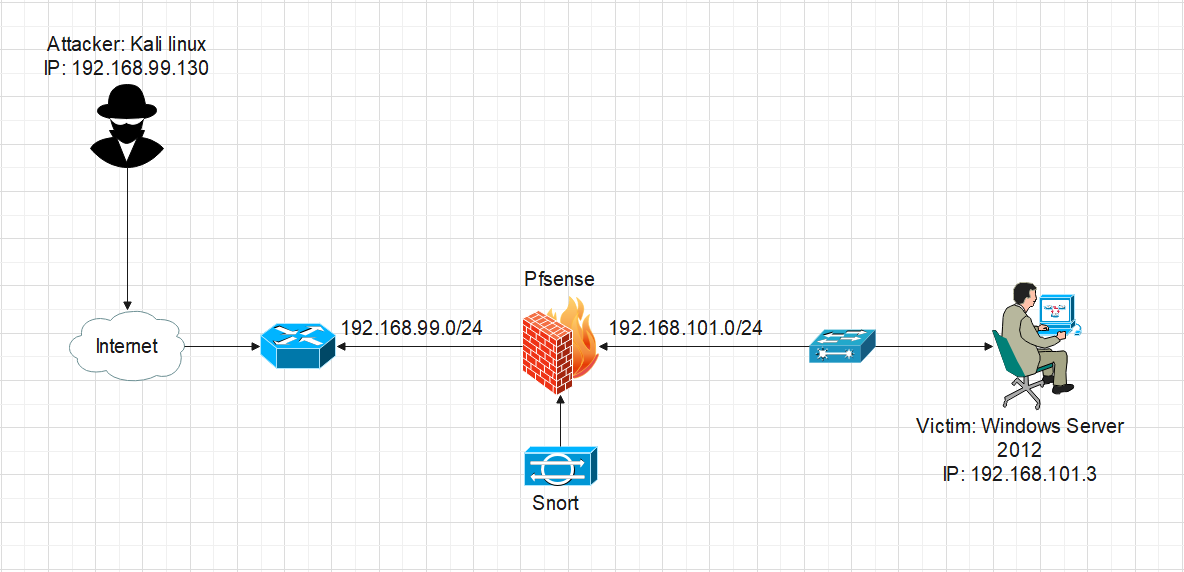
*[4.4.](#_Toc169106915)**[Thông báo truy cập HTTP](#_Toc169106915)* [16](#_Toc169106915)

*[4.5.](#_Toc169106916)**[Nmap thực hiện quét](#_Toc169106916)* [18](#_Toc169106916)

*[4.6.](#_Toc169106917)**[Dùng hping3 để thực hiện synflood:](#_Toc169106917)* [29](#_Toc169106917)

*[4.7.](#_Toc169106918)**[Các kỹ thuật khác](#_Toc169106918)* [33](#_Toc169106918)

# Mô hình:



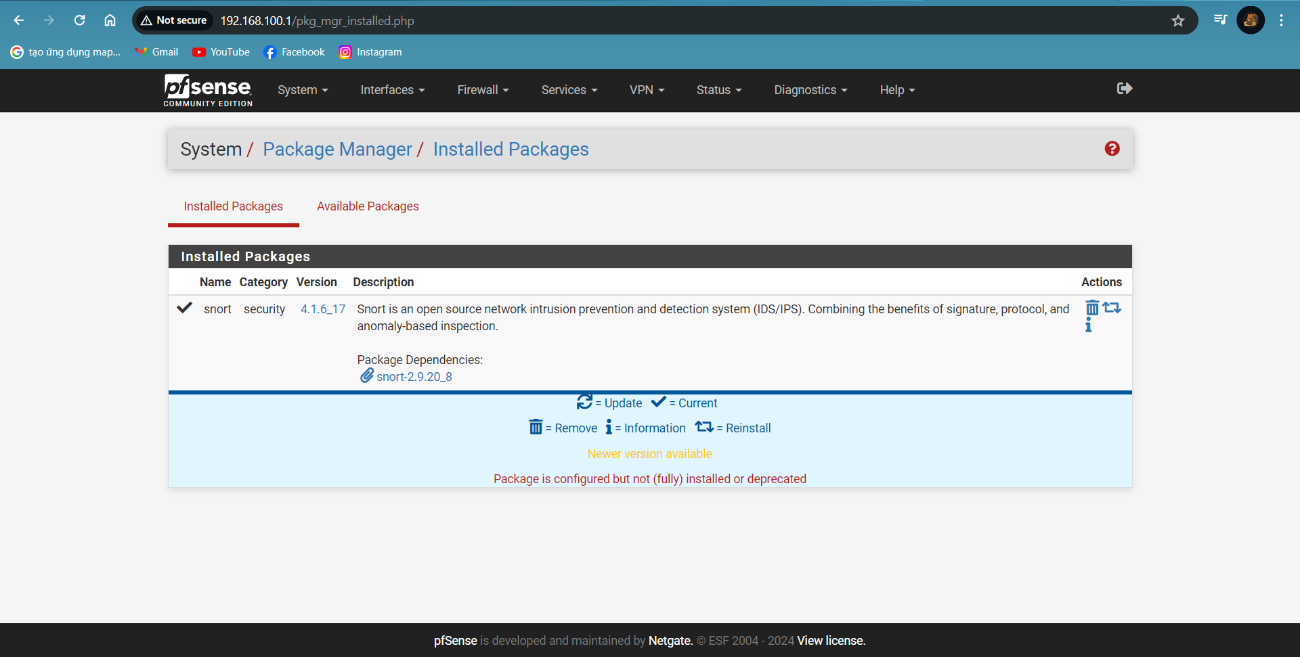
Mô tả mô hình:

|  |  |  |  |
| --- | --- | --- | --- |
| **Máy** | **Hệ điều hành** | **Địa chỉ IP** | **Interface** |
| **Firewall** | Pfsense | 192.168.99.128 | VMNet8 |
| 192.168.101.1 | VMNet2 |
|
| **Attacker** | Kali Linux | 192.168.99.x | VMNet8 |
| **Victim** | Windows Server 2012/ Windows 7 | 192.168.101.x | VMNet2 |

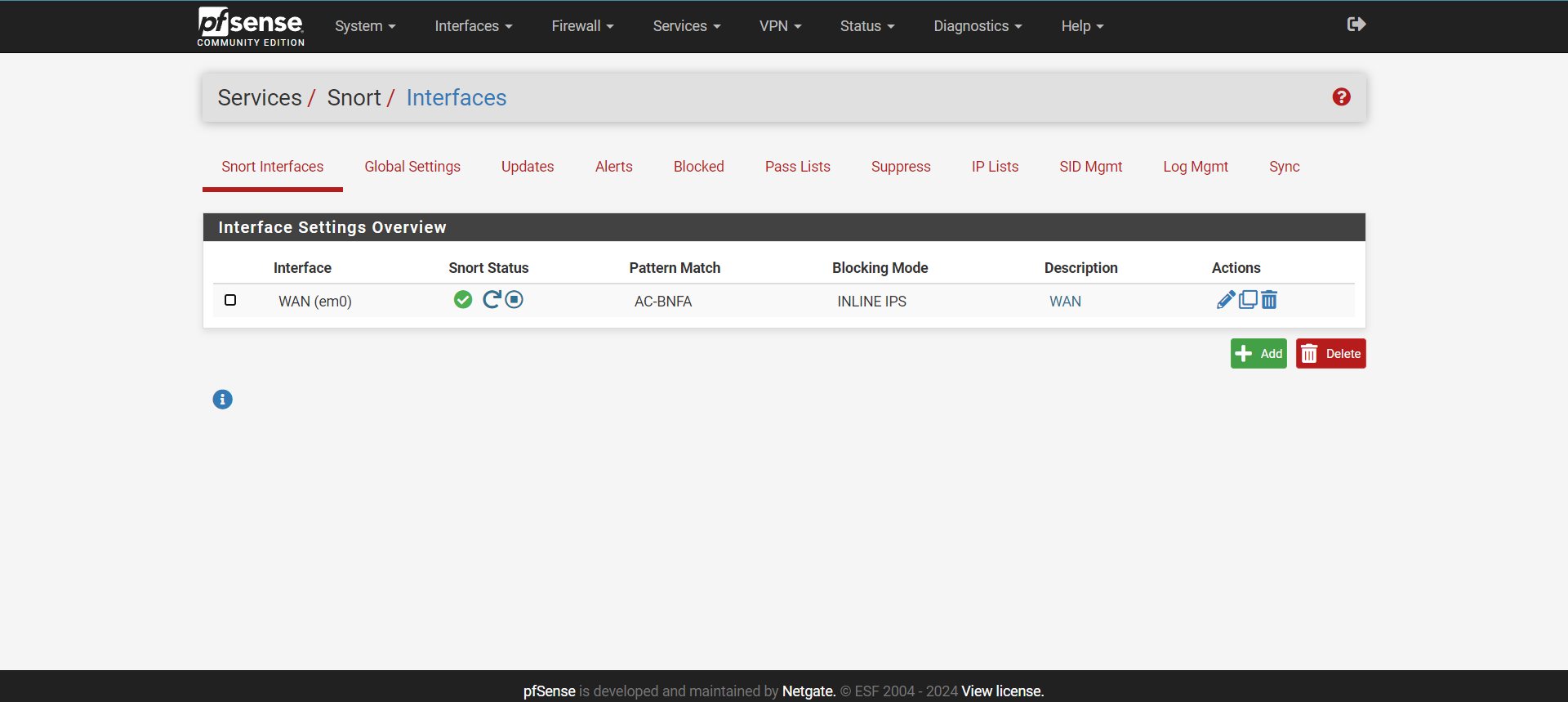
# Tiến hành cài đặt

## Cài đặt snort trên pfsense

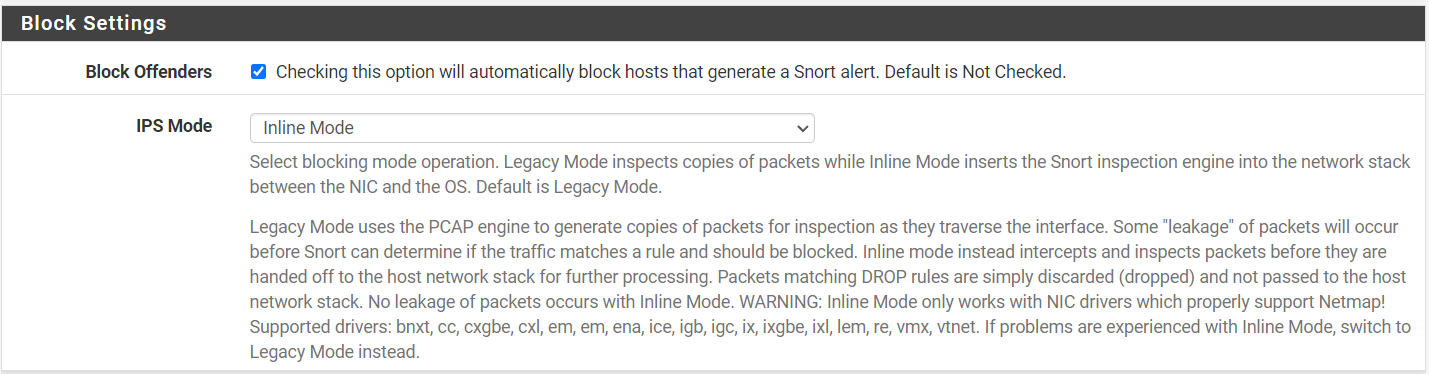
* Vào System -> Package Manager -> Available Packages để tải snort về, sau khi hoàn thành cài đặt, snort sẽ hiển thị ở phần Installed Packages

****

* Vào Services -> Snort -> Add để tạo interface và ta thực hiện chỉnh sửa rule trên interface này

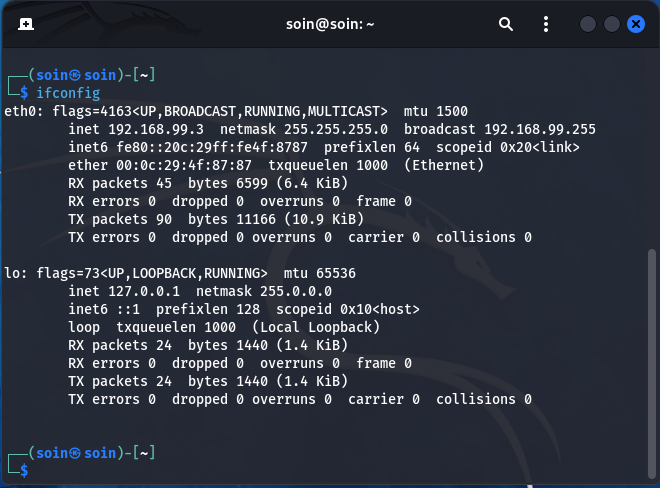


* Phần Blocked chọn Inline Mode cho Snort:

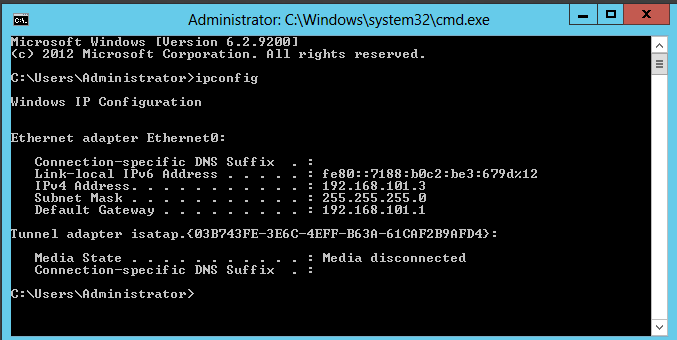


## Thông số mạng của thiết bị, test ping

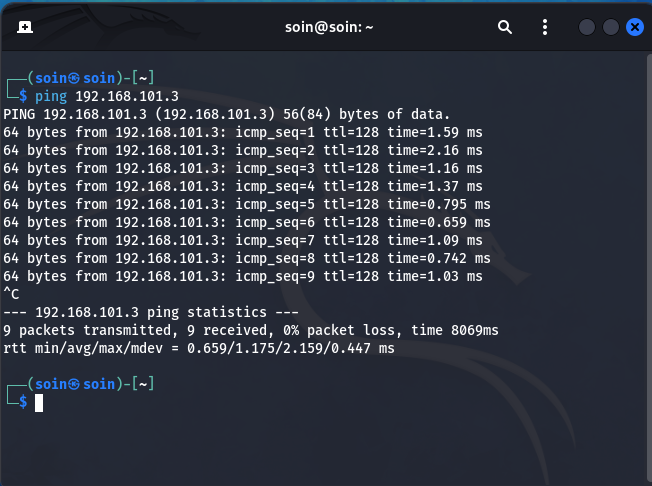
Thông số mạng của máy attacker:



Thông số mạng máy victim:



Kiểm tra ping từ máy attaker đến máy victim:



## Ping of death

* Đầu tiên ta tiến hành kiểm tra ping of death với rule sau:

*alert icmp any any -> $HOME\_NET any (msg:"--> Ping Of Death Attack!"; dsize:>10000; gid:1000001; sid:1000001; rev:1;)*

* Giải thích rule:

*alert:* Biểu thị đây là rule Snort để tạo cảnh báo.

*icmp:* Chỉ ra rằng rule này áp dụng cho lưu lượng ICMP (Internet Control Message Protocol), bao gồm các lệnh ping.

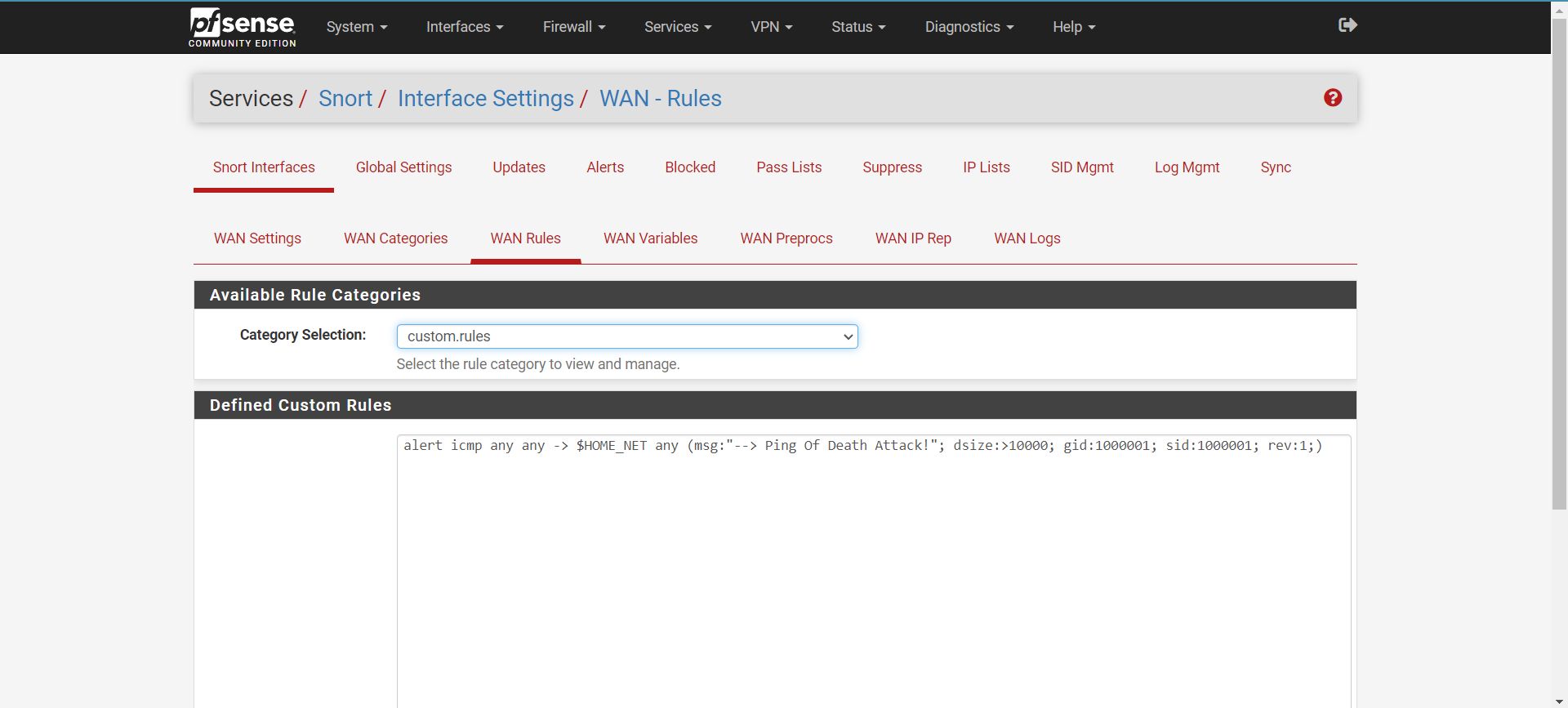
*any any:* Cho biết nguồn (any) có thể đến từ bất kỳ đâu và đích (any) có thể là bất kỳ cổng nào trên thiết bị trong mạng nội bộ của bạn ($HOME\_NET). $HOME\_NET là biến được định nghĩa trước trong Snort, đại diện cho mạng nội bộ đáng tin cậy của bạn.

*dsize:>10000:* Đây là phần quan trọng nhất của rule. Nó kiểm tra kích thước phần dữ liệu (dsize) của gói tin ICMP. Rule sẽ kích hoạt nếu kích thước dữ liệu lớn hơn 10000 byte. Một lệnh ping hợp lệ thường có kích thước payload nhỏ hơn nhiều.

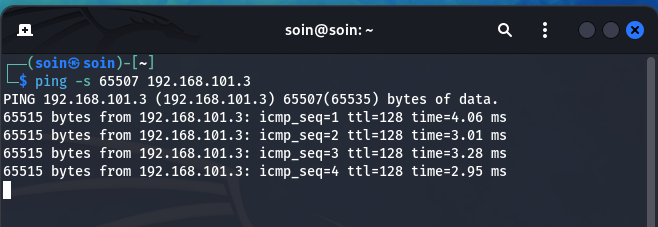
*gid:* Có thể đề cập đến Group ID (gid) được sử dụng để phân loại rule Snort (thường không liên quan đến người dùng).

*sid:* Đây là mã định danh rule duy nhất (Security ID - sid).

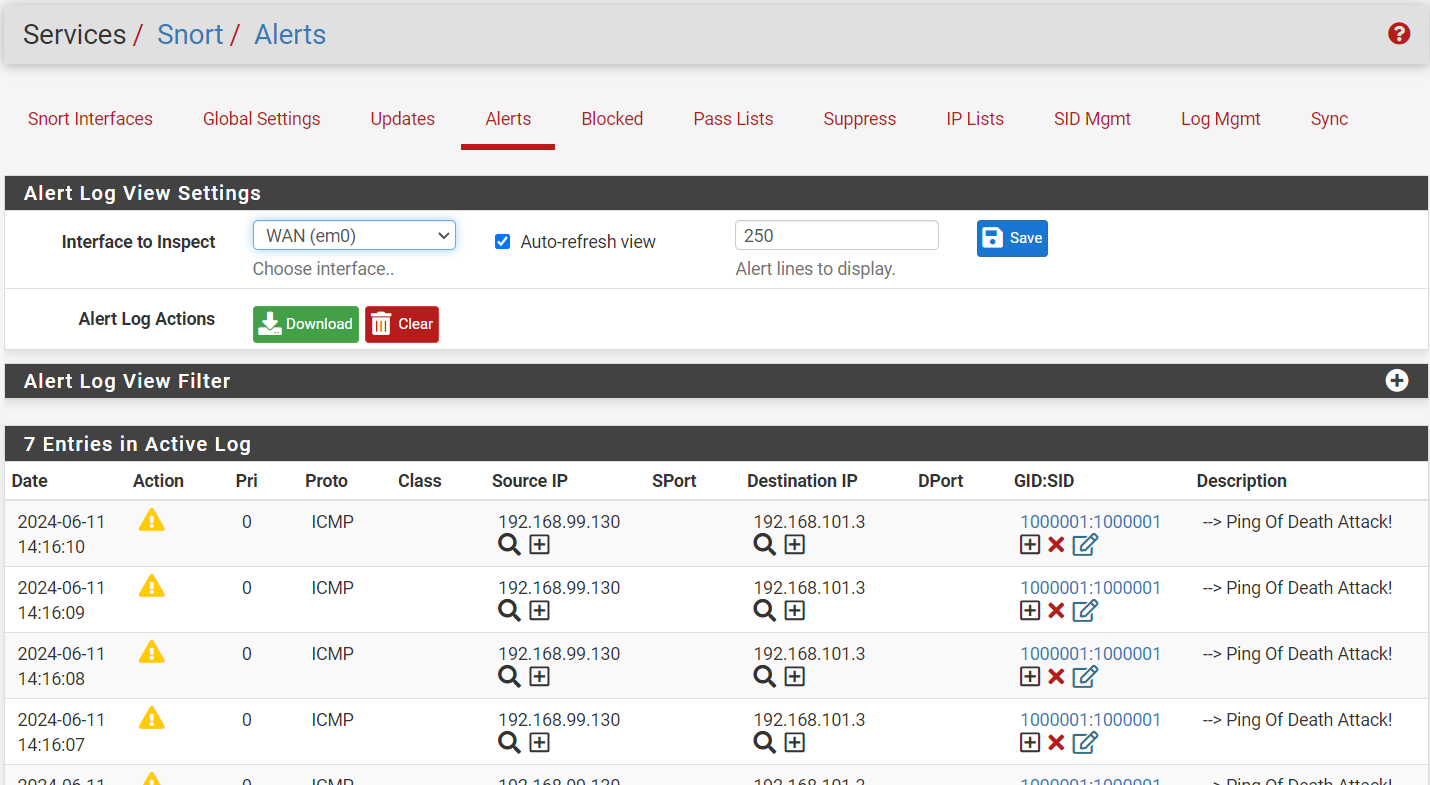
*rev:1:* Biểu thị đây là phiên bản 1 của rule.



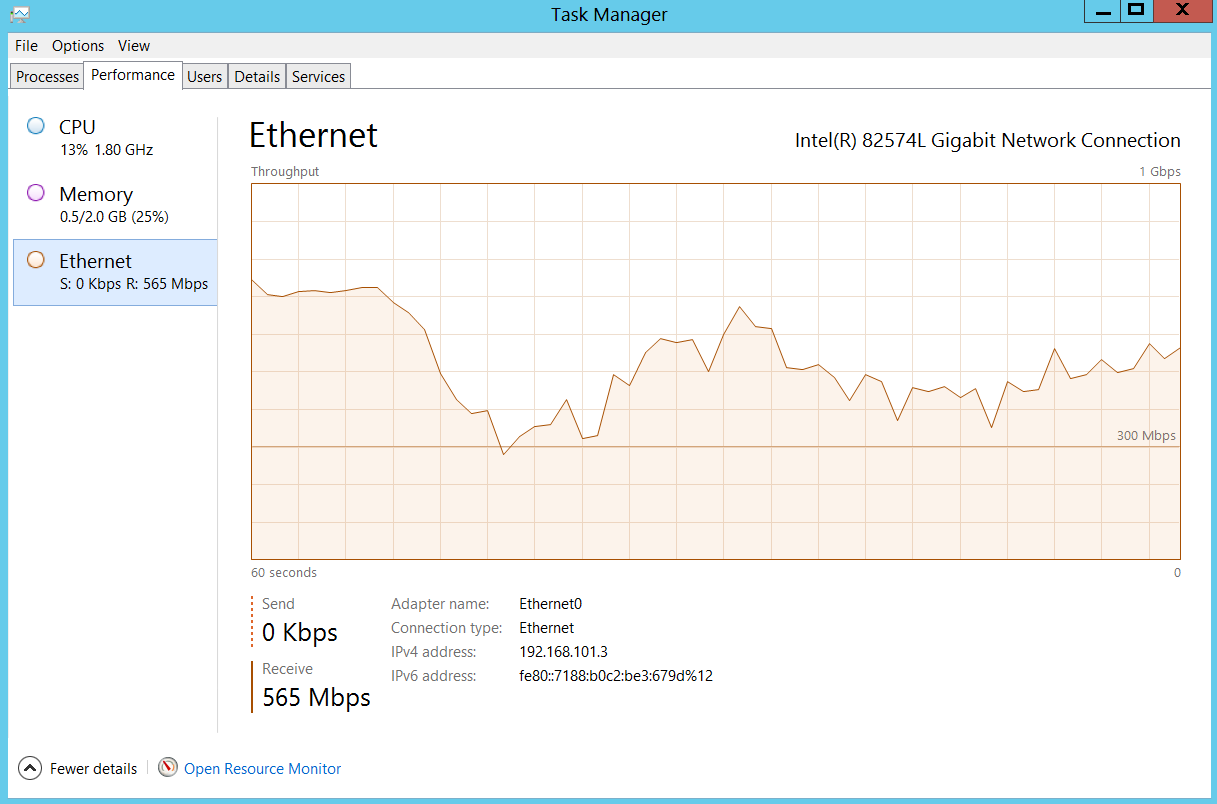
* Lưu lại và qua máy kali để tiến hành kiểm thử:



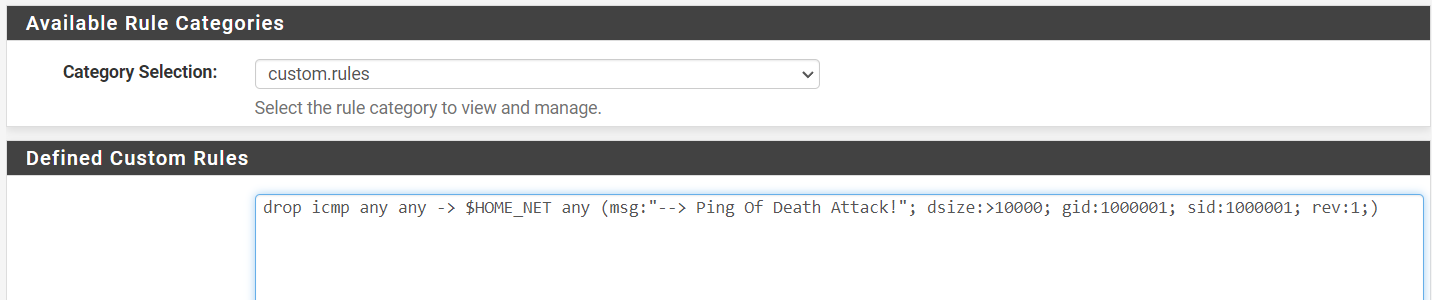
* Snort đã cảnh báo:



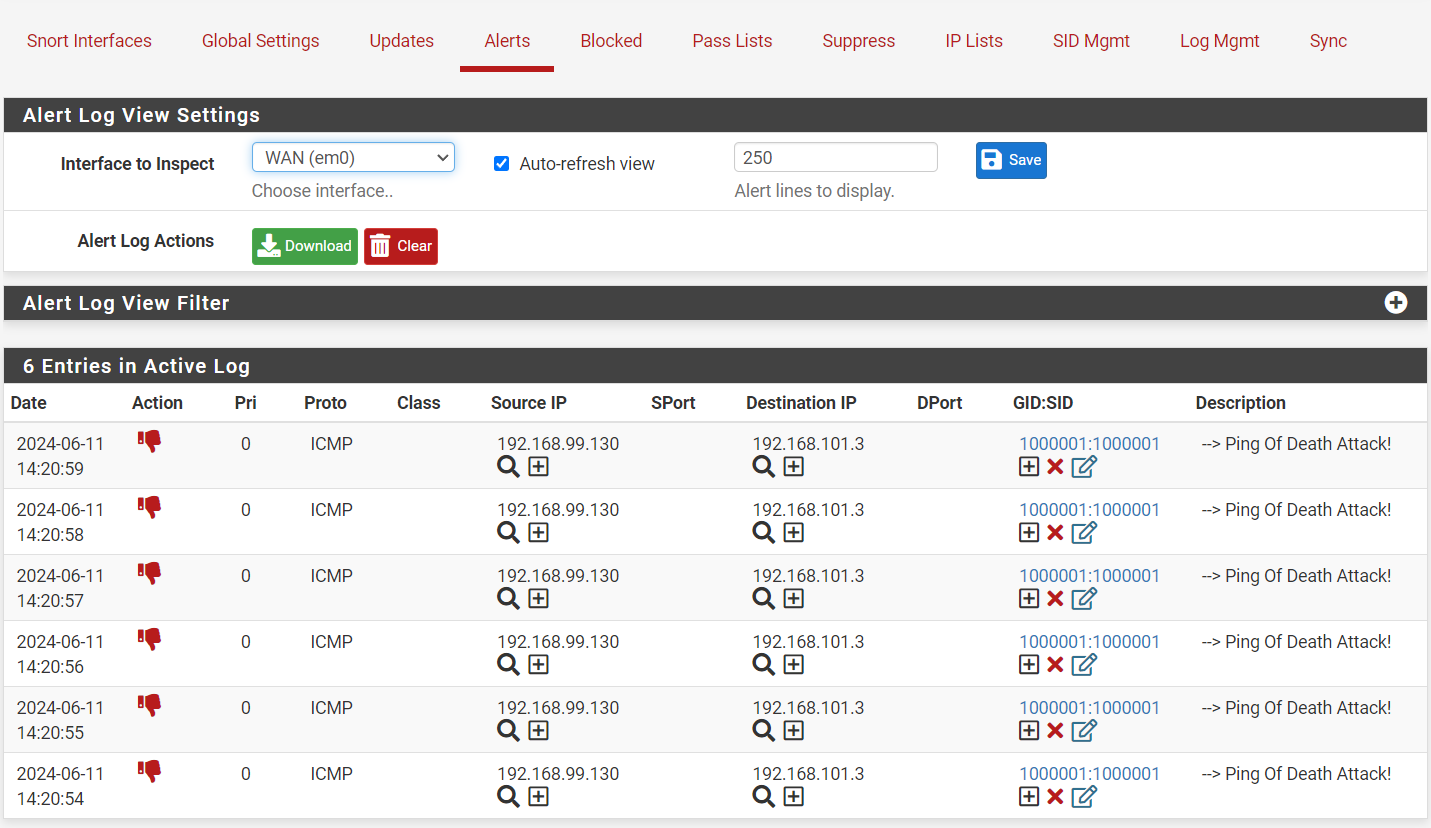
* Ở máy victim mục throughput xuất hiện bất thường:



* Chỉnh sửa lại rule và tiến hành ping of death lại để xem kết quả:



* Sau khi tấn công ta đã thấy cuộc tấn công đã bị chặn:



## Tiến hành thực hiện ở một số rule khác:

### *Scaning port 81:*

* Ta có rule như sau:

*alert icmp any any -> $HOME\_NET 81 (msg:"Scaning Port 81"; sid:1000005; rev:1;)*

* Giải thích rule:

*alert:* Đây là keyword cho biết đây là một rule cảnh báo trong Snort.

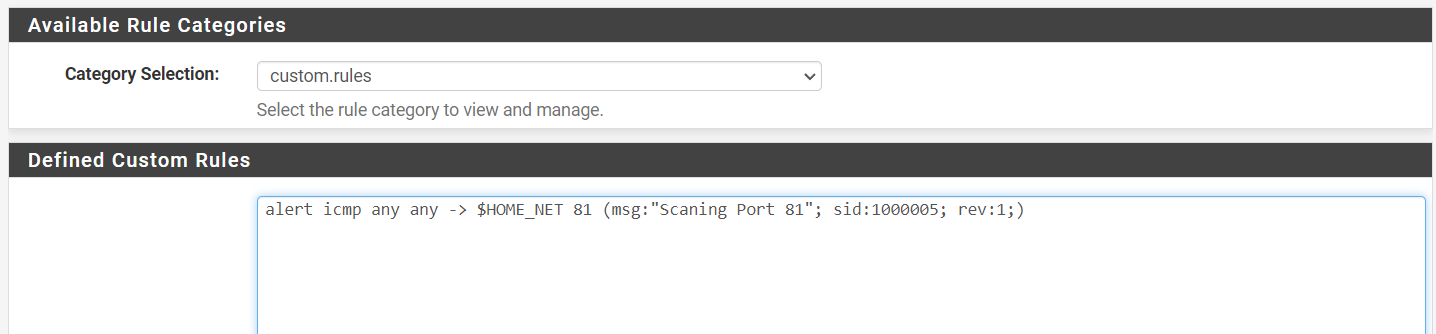
*icmp:* Chỉ định rule này dành cho giao thức ICMP, thường được sử dụng cho các lệnh ping.

*any any:* Nguồn (any) có thể là bất kỳ đâu và đích (any) là cổng 81 trên một thiết bị trong mạng nội bộ của bạn ($HOME\_NET).

*81:* Cổng đích là 81, thường được sử dụng cho giao thức HTTP (web traffic).

*sid:* Đây là mã định danh duy nhất của rule (Security ID - sid).

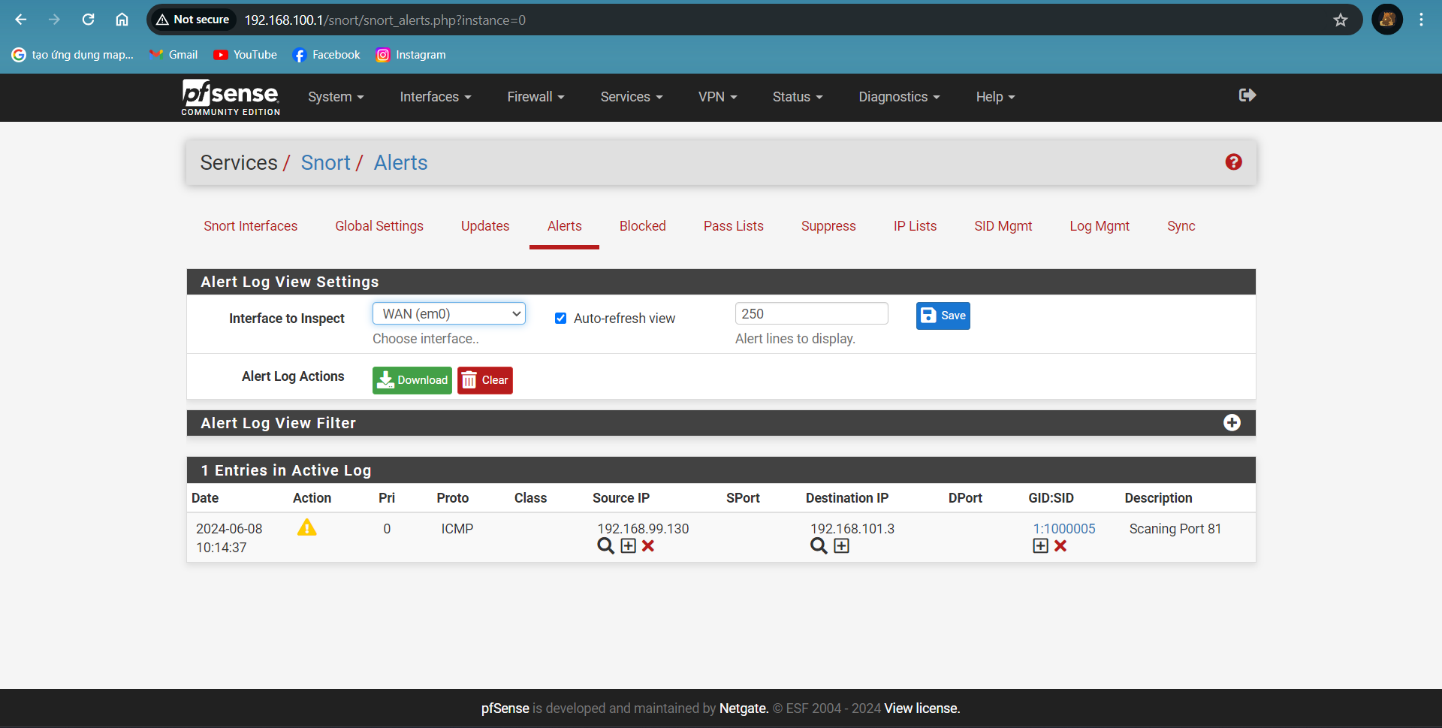
*rev:1:* Biểu thị đây là phiên bản 1 của rule.



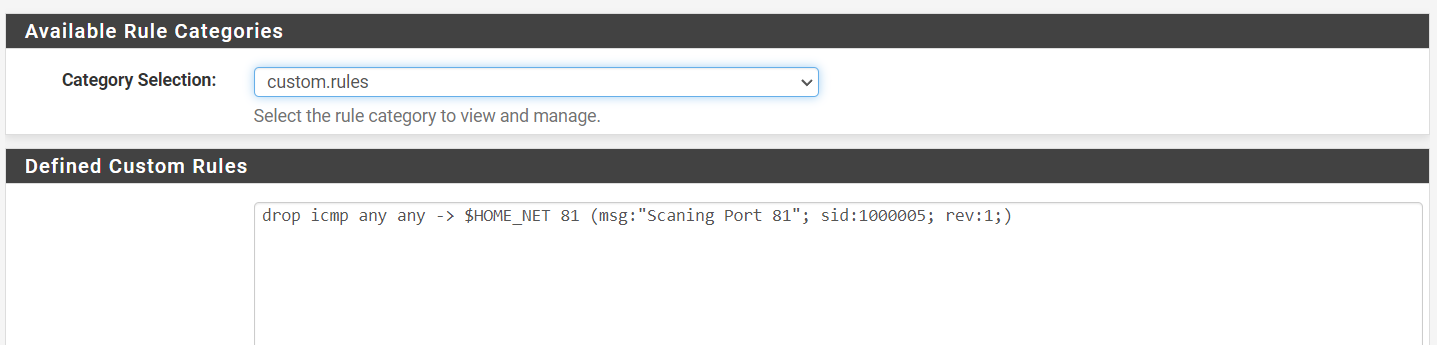
* Sử dụng nmap để thực hiện kiểm thử



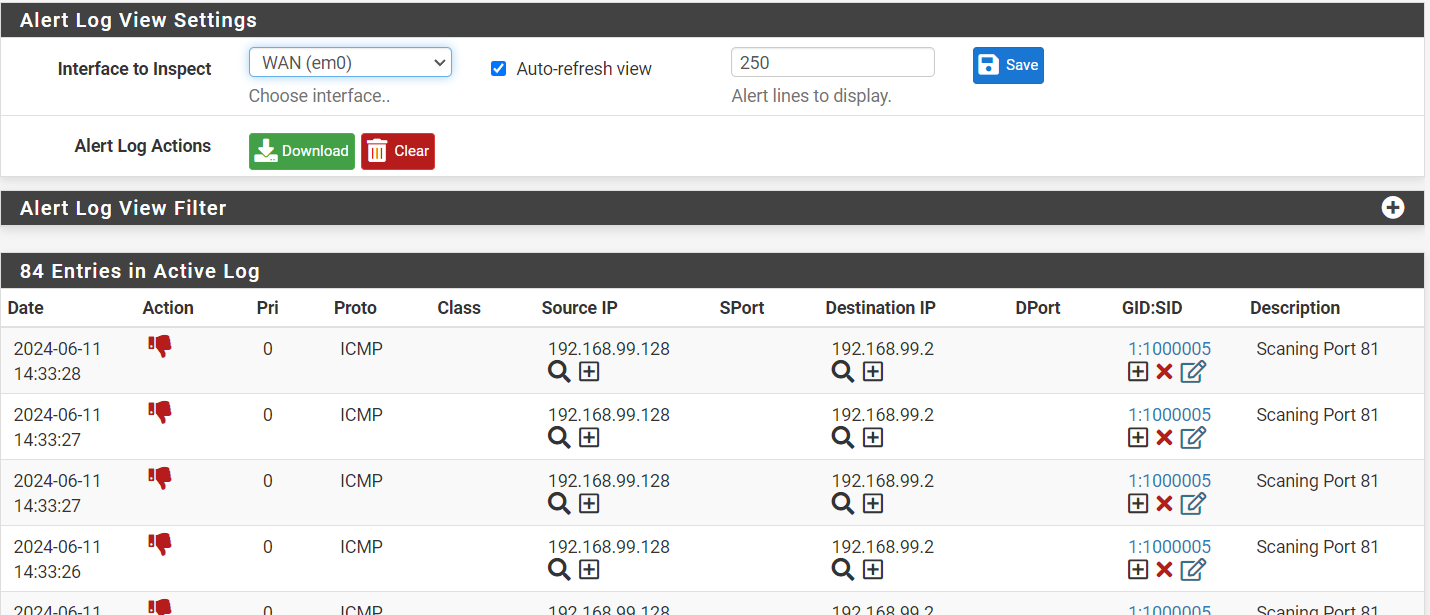
* Snort vẫn phát hiện được:



* Chỉnh sửa lại rule để ngăn chặn cuộc tấn công này:



* Ở mục alert ta thấy cuộc tấn công đã bị chặn:



### *Kiểm tra kết nối ftp:*

(đề ssh, được nộp theo nhóm nên em chỉnh sang ftp):

* Ta có rule sau:

*alert tcp any any -> $HOME\_NET 21 (msg:"FTP connection=>Attempt"; sid:1000004;)*

* Giải thích rule:

*alert:* Đây là một rule Snort để tạo cảnh báo.

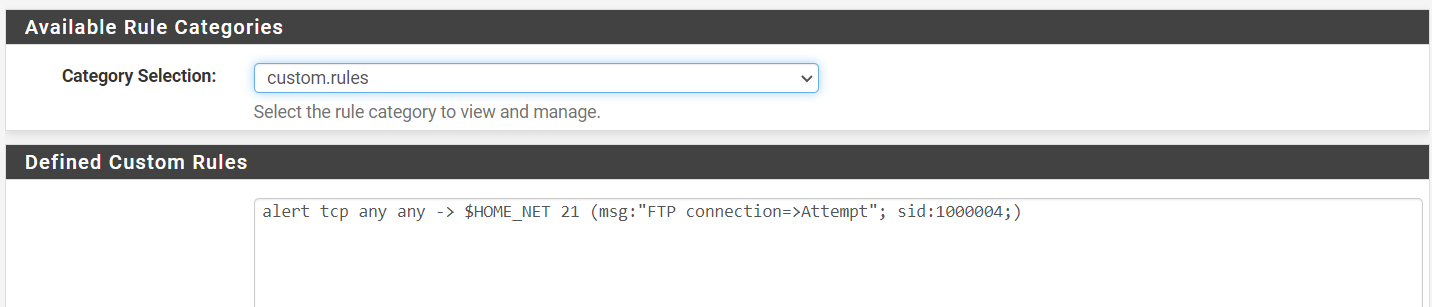
*tcp:* Cho biết rule này dành cho giao thức TCP, thường được sử dụng để thiết lập các kết nối đáng tin cậy.

*any any:* Nguồn (any) có thể là bất kỳ đâu và đích (any) là cổng 21 trên thiết bị thuộc mạng nội bộ của bạn ($HOME\_NET). Cổng 21 là cổng mặc định cho dịch vụ FTP (File Transfer Protocol).

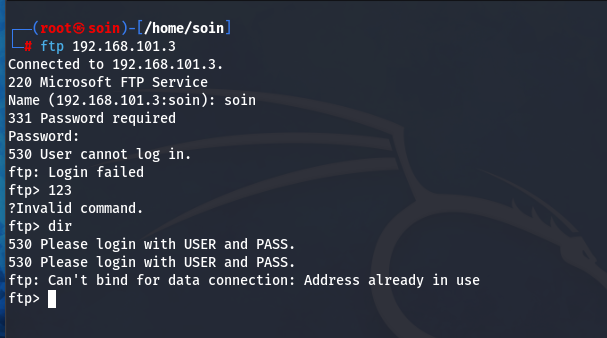
*msg:*"FTP connection=>Attempt";: Đây là thông báo sẽ được ghi lại trong nhật ký bảo mật (security log) nếu rule kích hoạt. Nó cho biết rule phát hiện một nỗ lực kết nối FTP đến mạng nội bộ.

*sid:* Đây là mã định danh duy nhất của rule (Security ID - sid).

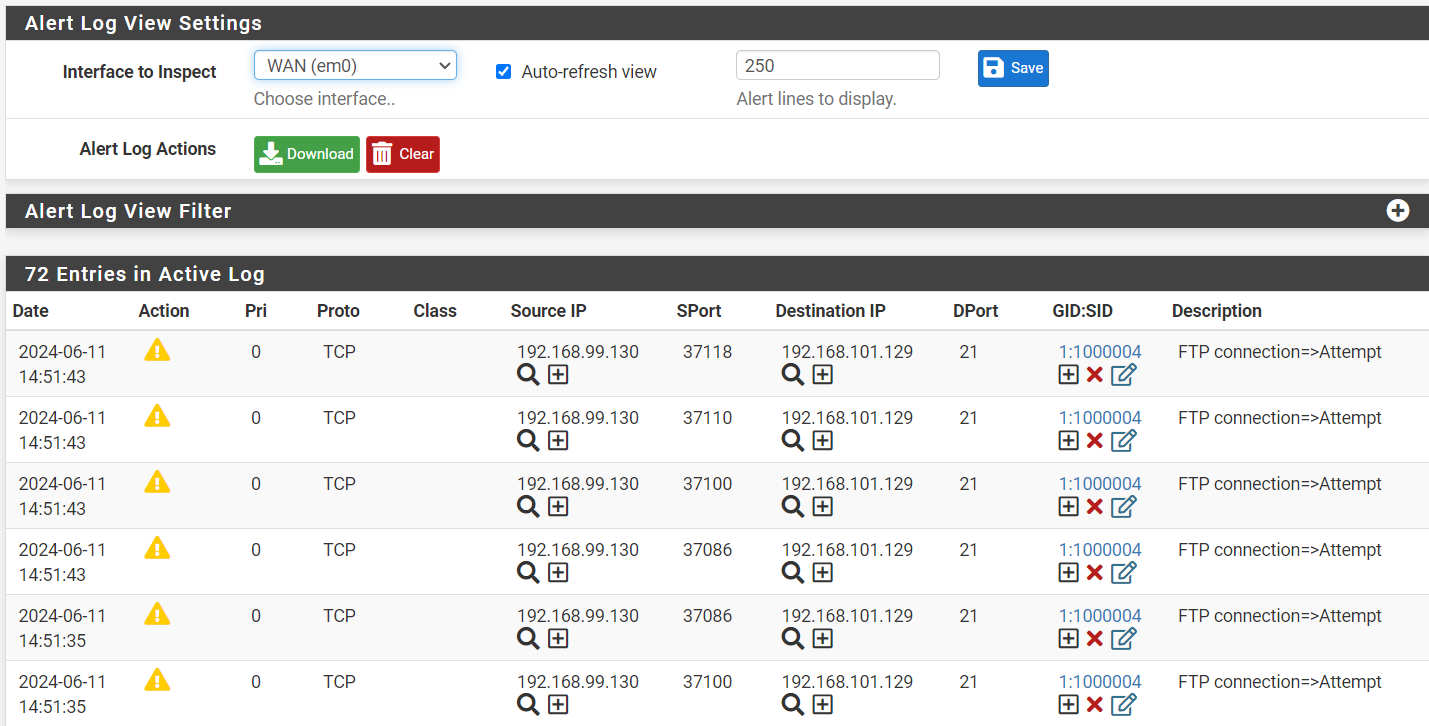
* Cài đặt rule cho snort:



* Từ máy kali tiến hành kết nối qua ftp nạn nhân:



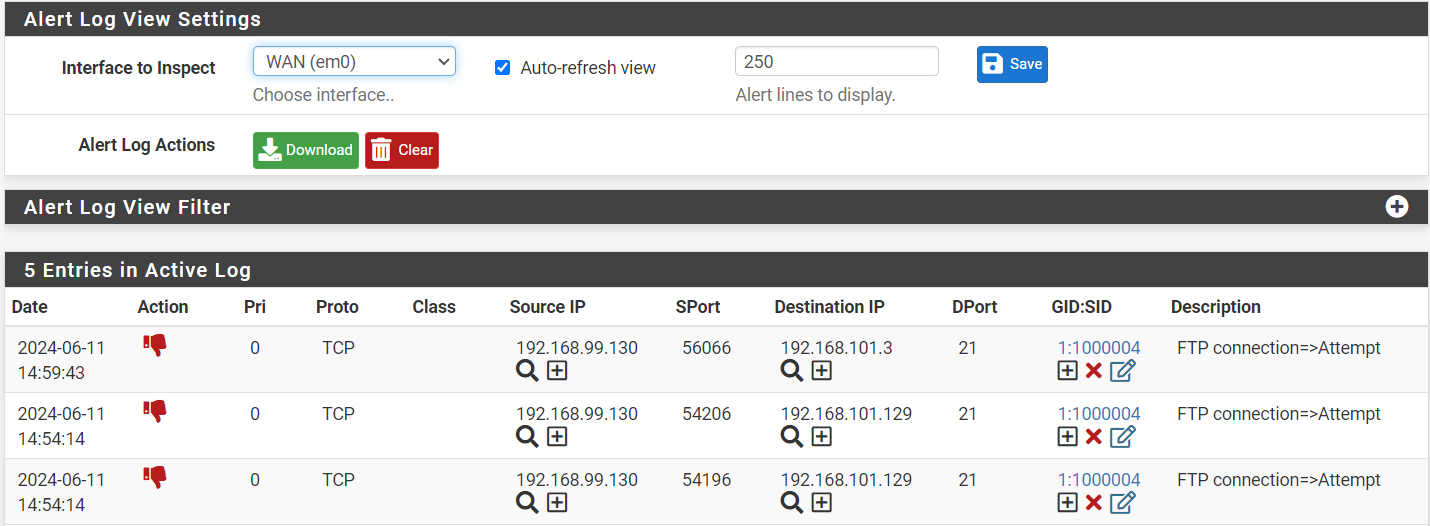
* Snort phát cảnh báo:



* Chỉnh sửa rule để ngăn chặn cuộc tấn công này:



* Snort đã drop được:



### *Testing UDP*

* Ta có rule sau:

*alert icmp any any -> any any (msg:"UDP Tesing Rule"; sid:1000006;rev:1;)*

* Giải thích rule:

*alert:* Mặc dù thường biểu thị rule cảnh báo, trong trường hợp này, nó có thể là cách gọi chung cho một rule trong Snort.

*icmp:* Cho biết rule áp dụng cho lưu lượng ICMP (Internet Control Message Protocol), bao gồm các lệnh ping.

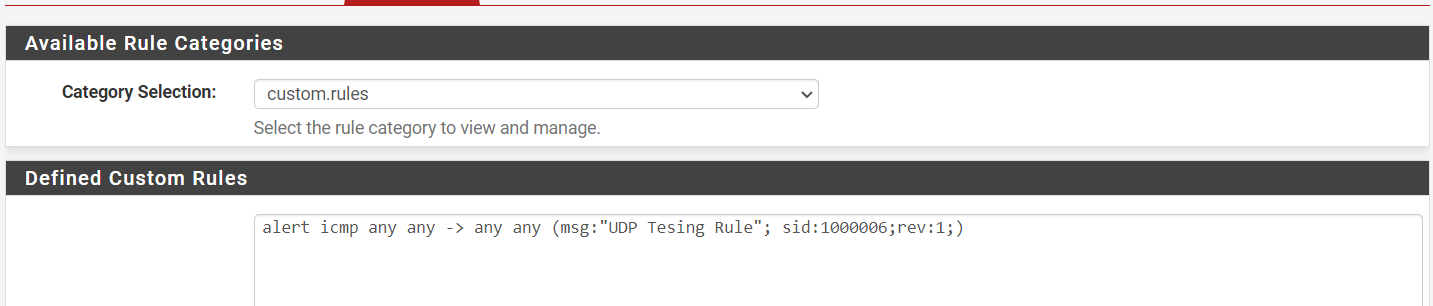
*any any:* Chỉ ra nguồn (any) có thể đến từ bất kỳ đâu và đích (any) có thể là bất kỳ cổng nào trên bất kỳ thiết bị nào.

*msg:"UDP Tesing Rule";:* Thông báo này cho thấy đây là rule thử nghiệm cho giao tiếp UDP (User Datagram Protocol). Nó có thể ghi lại thông tin về bất kỳ lưu lượng ICMP nào cho mục đích giám sát, không nhất thiết để cảnh báo về vấn đề bảo mật.

*sid:* Đây là mã định danh rule duy nhất (Security ID - sid).

*rev:1:* Biểu thị đây là phiên bản 1 của rule.

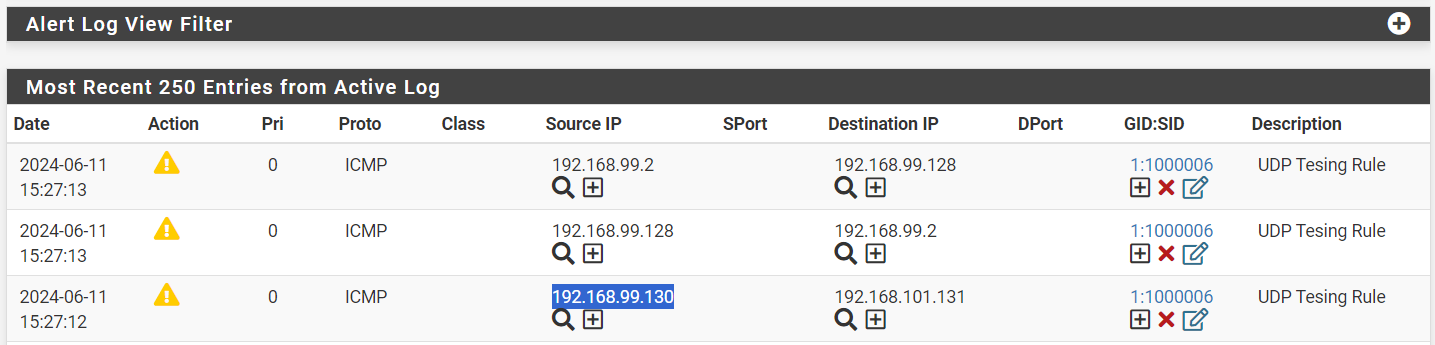
* Chỉnh rule trên snort:



* Sử dụng hping3 để giả mạo icmp thành udp:

*hping3 --udp -S <source\_ip> -p 51820 --dst <target\_ip>*

* Snort vẫn phát hiện được:

**

### *Thông báo truy cập HTTP*

* Ta có rule sau:

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

* Giải thích rule:

*alert tcp:* Quy định rằng luật áp dụng cho lưu lượng truy cập TCP (Transmission Control Protocol).

*any any:* Chỉ ra rằng luật sẽ kích hoạt cho bất kỳ địa chỉ IP nguồn nào và bất kỳ cổng nguồn nào.

*-> $HOME\_NET*: Xác định điểm đến của lưu lượng truy cập là mạng gia đình. $HOME\_NET có khả năng là biến được định nghĩa trước trong hệ thống bảo mật của bạn, đại diện cho mạng nội bộ bạn muốn bảo vệ.

*80:* Chỉ định cổng đích là 80, đây là cổng tiêu chuẩn cho lưu lượng truy cập HTTP.

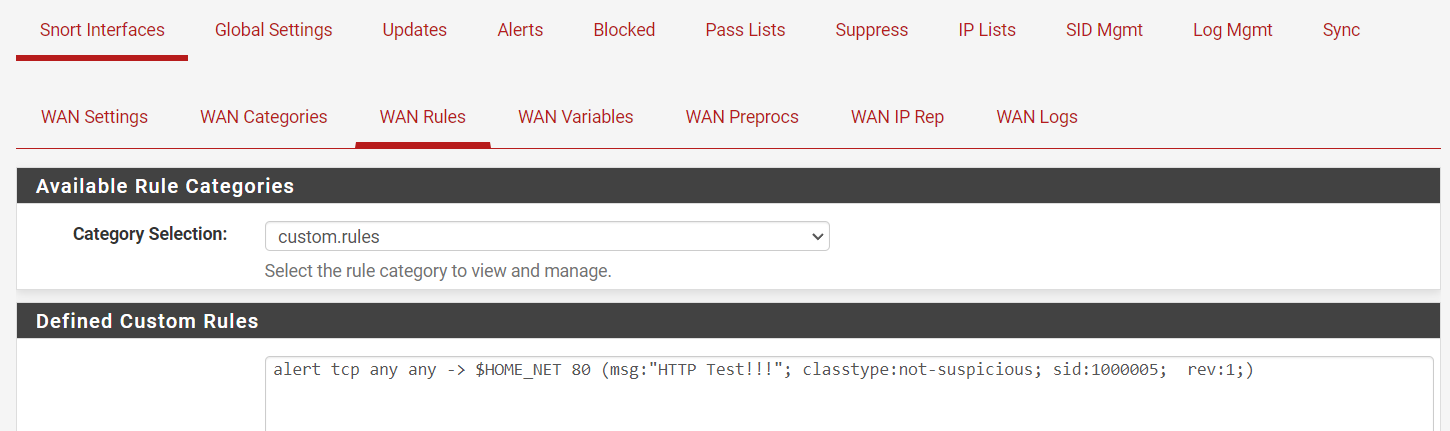
*msg:"HTTP Test!!!"*: Đây là thông báo tùy chỉnh sẽ được ghi lại nếu luật kích hoạt. Nó cho biết đây là quy tắc kiểm tra cho lưu lượng truy cập HTTP.

*classtype:not-suspicious:* Phân loại rõ ràng lưu lượng truy cập là không đáng ngờ. Điều này rất quan trọng vì các hệ thống bảo mật thường có phân loại được định nghĩa trước cho các loại lưu lượng truy cập khác nhau (ví dụ: đáng ngờ, bất thường, v.v.).

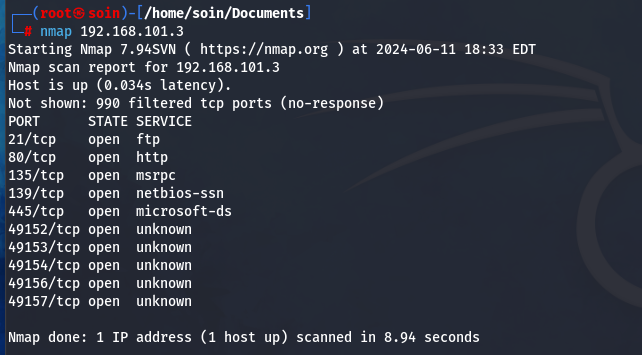
*sid:1000005:* Đây là mã định danh duy nhất (Mã chữ ký) được gán cho quy tắc này.

*rev:1:* Khả năng cao cho biết số phiên bản của quy tắc, bắt đầu từ 1.

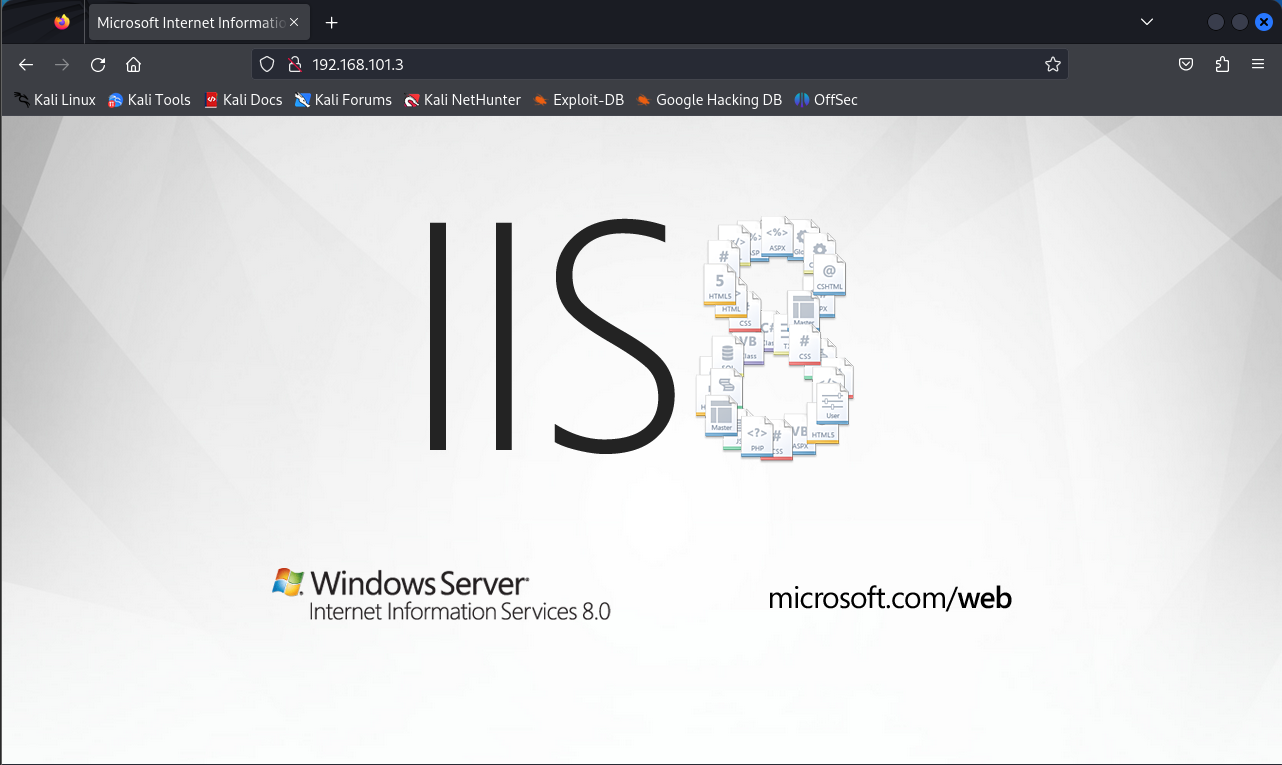
* Chỉnh rule ở snrot:



* Qua nmap ta thấy ở máy victim có dịch vụ http:



* Vào firefox truy cập vào máy nạn nhân:



* Ta thấy snort đã phát ra cảnh báo:



### *Nmap thực hiện quét*

* TCP Connect scan: *nmap -sT <target\_ip\_or\_range>*

Rule: *alert tcp any any -> $HOME\_NET any (msg: "TCP Connect Scan"; flags: S; sid: 1;)*

* Giải thích rule:

*alert tcp:* Loại cảnh báo - Đây là cảnh báo cho lưu lượng truy cập TCP.

*any any:* Nguồn và cổng nguồn - Rule sẽ kích hoạt bất kể địa chỉ IP nguồn, cổng nguồn nào.

*-> $HOME\_NET:* Đích - Mạng nhà của bạn, được biểu thị bằng biến $HOME\_NET.

*any:* Cổng đích - Rule sẽ kích hoạt cho bất kỳ cổng nào trên mạng nội bộ của bạn.

*msg: "TCP Connect Scan";:* Thông báo - Khi rule kích hoạt, nó sẽ ghi lại cảnh báo "TCP Connect Scan" để thông báo cho bạn về khả năng quét.

*flags: S;:* Kiểm tra cờ - Rule chỉ kích hoạt nếu gói tin có cờ SYN được đặt (cho biết nỗ lực khởi tạo kết nối).

*sid: 1;:* Mã SID - Gán mã định danh duy nhất (SID) là "1" cho rule này để dễ dàng tham khảo và quản lý.

* TCP SYN scan: *nmap -sS <target\_ip\_or\_range>*

Rule: *alert tcp any any -> $HOME\_NET any (msg: "TCP SYN Scan"; flags: S; sid: 2;)*

* Giải thích rule:

*alert tcp:* Loại cảnh báo - Đây là cảnh báo cho lưu lượng truy cập TCP.

*any any:* Nguồn và cổng nguồn - Rule sẽ kích hoạt bất kể địa chỉ IP nguồn, cổng nguồn nào.

*-> $HOME\_NET:* Đích - Mạng nhà của bạn, được biểu thị bằng biến $HOME\_NET.

*any:* Cổng đích - Rule sẽ kích hoạt cho bất kỳ cổng nào trên mạng nội bộ của bạn.

*msg: "TCP SYN Scan";:* Thông báo - Khi rule kích hoạt, nó sẽ ghi lại cảnh báo "TCP SYN Scan" để thông báo cho bạn về khả năng quét SYN.

*flags: S;:* Kiểm tra cờ - Rule chỉ kích hoạt nếu gói tin có cờ SYN được đặt (cho biết nỗ lực khởi tạo kết nối TCP).

*sid: 2;:* Mã SID - Gán mã định danh duy nhất (SID) là "2" cho rule này để dễ dàng tham khảo và quản lý.

* Inverse TCP Flag: *nmap -sN <target\_ip\_or\_range>*

Rule: *alert tcp any any -> $HOME\_NET any (msg: "NULL Scan (*Inverse TCP Flag*)"; flags: 0; sid: 3;)*

* Giải thích rule:

*alert tcp:* Loại cảnh báo - Đây là cảnh báo cho lưu lượng truy cập TCP.

*any any:* Nguồn và cổng nguồn - Rule sẽ kích hoạt bất kể địa chỉ IP nguồn, cổng nguồn nào.

*-> $HOME\_NET:* Đích - Mạng nhà của bạn, được biểu thị bằng biến $HOME\_NET.

*any:* Cổng đích - Rule sẽ kích hoạt cho bất kỳ cổng nào trên mạng nội bộ của bạn.

*msg: "NULL Scan (Inverse TCP Flag)";:* Thông báo - Khi rule kích hoạt, nó sẽ ghi lại cảnh báo "NULL Scan (Inverse TCP Flag)" để thông báo cho bạn về khả năng quét NULL.

*flags: 0;:* Kiểm tra cờ - Rule chỉ kích hoạt nếu gói tin không có bất kỳ cờ TCP nào được đặt (cờ bằng 0).

*sid: 3;:* Mã SID - Gán mã định danh duy nhất (SID) là "3" cho rule này để dễ dàng tham khảo và quản lý.

* FIN Scan: *nmap -sF <target\_ip\_or\_range>*

Rule: *alert tcp any any -> $HOME\_NET any (msg: "FIN Scan"; flags: F; sid: 4;)*

* Giải thích rule:

*alert tcp:* Loại cảnh báo - Đây là cảnh báo cho lưu lượng truy cập TCP.

*any any:* Nguồn và cổng nguồn - Rule sẽ kích hoạt bất kể địa chỉ IP nguồn, cổng nguồn nào.

*-> $HOME\_NET:* Đích - Mạng nhà của bạn, được biểu thị bằng biến $HOME\_NET.

*any:* Cổng đích - Rule sẽ kích hoạt cho bất kỳ cổng nào trên mạng nội bộ của bạn.

*msg: "FIN Scan";:* Thông báo - Khi rule kích hoạt, nó sẽ ghi lại cảnh báo "FIN Scan" để thông báo cho bạn về khả năng quét FIN.

*flags: F;:* Kiểm tra cờ - Rule chỉ kích hoạt nếu gói tin có cờ FIN được đặt (cho biết yêu cầu kết thúc kết nối).

*sid: 4;:* Mã SID - Gán mã định danh duy nhất (SID) là "4" cho rule này để dễ dàng tham khảo và quản lý.

* XMAS Scan: *nmap -sX <target\_ip\_or\_range>*

Rule: *alert tcp any any -> $HOME\_NET any (msg: "XMAS Scan"; flags: FPU; sid: 5;)*

* Giải thích rule:

*alert tcp:* Loại cảnh báo - Đây là cảnh báo cho lưu lượng truy cập TCP.

*any any:* Nguồn và cổng nguồn - Rule sẽ kích hoạt bất kể địa chỉ IP nguồn, cổng nguồn nào.

*-> $HOME\_NET:* Đích - Mạng nhà của bạn, được biểu thị bằng biến $HOME\_NET.

*any:* Cổng đích - Rule sẽ kích hoạt cho bất kỳ cổng nào trên mạng nội bộ của bạn.

*msg: "XMAS Scan";:* Thông báo - Khi rule kích hoạt, nó sẽ ghi lại cảnh báo "XMAS Scan" để thông báo cho bạn về khả năng quét XMAS.

*flags: FPU;:* Kiểm tra cờ - Rule chỉ kích hoạt nếu gói tin có các cờ F, P và U được đặt:

*F (FIN):* Yêu cầu kết thúc kết nối.

*P (PUSH):* Yêu cầu dữ liệu được đẩy đến lớp ứng dụng.

*U (URG):* Yêu cầu xử lý khẩn cấp.

*sid: 5;:* Mã SID - Gán mã định danh duy nhất (SID) là "5" cho rule này để dễ dàng tham khảo và quản lý.

* TCP ACK Scan: *nmap -sA <target\_ip\_or\_range>*

Rule: *alert tcp any any -> $HOME\_NET any (msg: "TCP ACK Scan"; flags: A; sid: 6;)*

* Giải thích rule:

*alert tcp:* Loại cảnh báo - Đây là cảnh báo cho lưu lượng truy cập TCP.

*any any:* Nguồn và cổng nguồn - Rule sẽ kích hoạt bất kể địa chỉ IP nguồn, cổng nguồn nào.

*-> $HOME\_NET:* Đích - Mạng nhà của bạn, được biểu thị bằng biến $HOME\_NET.

*any:* Cổng đích - Rule sẽ kích hoạt cho bất kỳ cổng nào trên mạng nội bộ của bạn.

*msg: "TCP ACK Scan";:* Thông báo - Khi rule kích hoạt, nó sẽ ghi lại cảnh báo "TCP ACK Scan" để thông báo cho bạn về khả năng quét TCP ACK.

*flags: A;:* Kiểm tra cờ - Rule chỉ kích hoạt nếu gói tin có cờ A (ACK) được đặt, cho biết sự xác nhận cho một kết nối TCP đã được thiết lập trước đó.

*sid: 6;:* Mã SID - Gán mã định danh duy nhất (SID) là "6" cho rule này để dễ dàng tham khảo và quản lý.

* UDP Connect Scan: *nmap -sU <target\_ip\_or\_range>*

Rule: *alert udp any any -> $HOME\_NET any (msg: "UDP Connect Scan"; sid: 7;)*

* Giải thích rule:

*alert udp:* Loại cảnh báo - Đây là cảnh báo cho lưu lượng truy cập UDP.

*any any:* Nguồn và cổng nguồn - Rule sẽ kích hoạt bất kể địa chỉ IP nguồn, cổng nguồn nào.

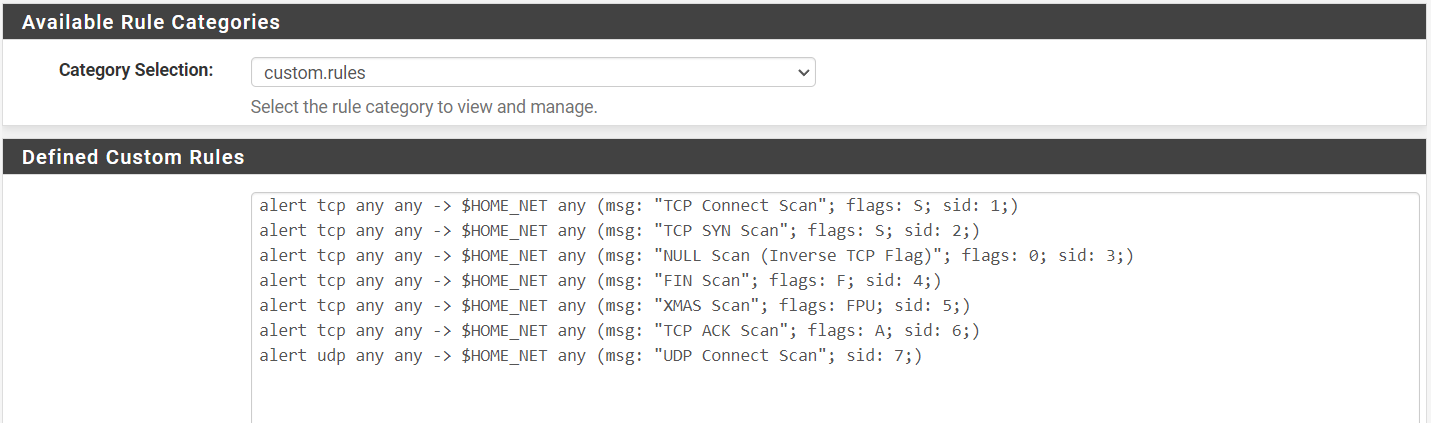
*-> $HOME\_NET:* Đích - Mạng nhà của bạn, được biểu thị bằng biến $HOME\_NET.

*any:* Cổng đích - Rule sẽ kích hoạt cho bất kỳ cổng nào trên mạng nội bộ của bạn.

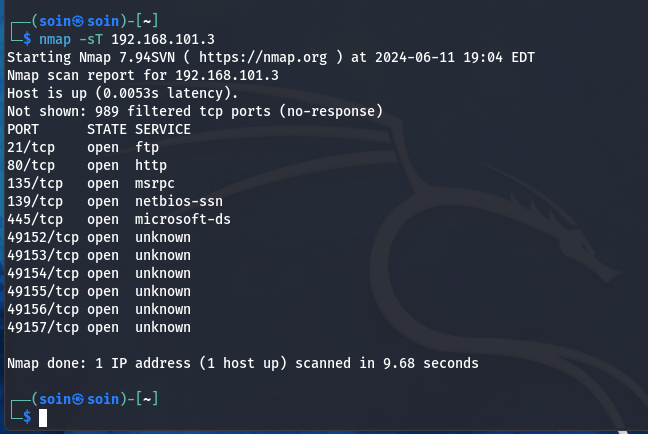
*msg: "UDP Connect Scan";:* Thông báo - Khi rule kích hoạt, nó sẽ ghi lại cảnh báo "UDP Connect Scan" để thông báo cho bạn về khả năng quét kết nối UDP.

*sid: 7;:* Mã SID - Gán mã định danh duy nhất (SID) là "7" cho rule này để dễ dàng tham khảo và quản lý.

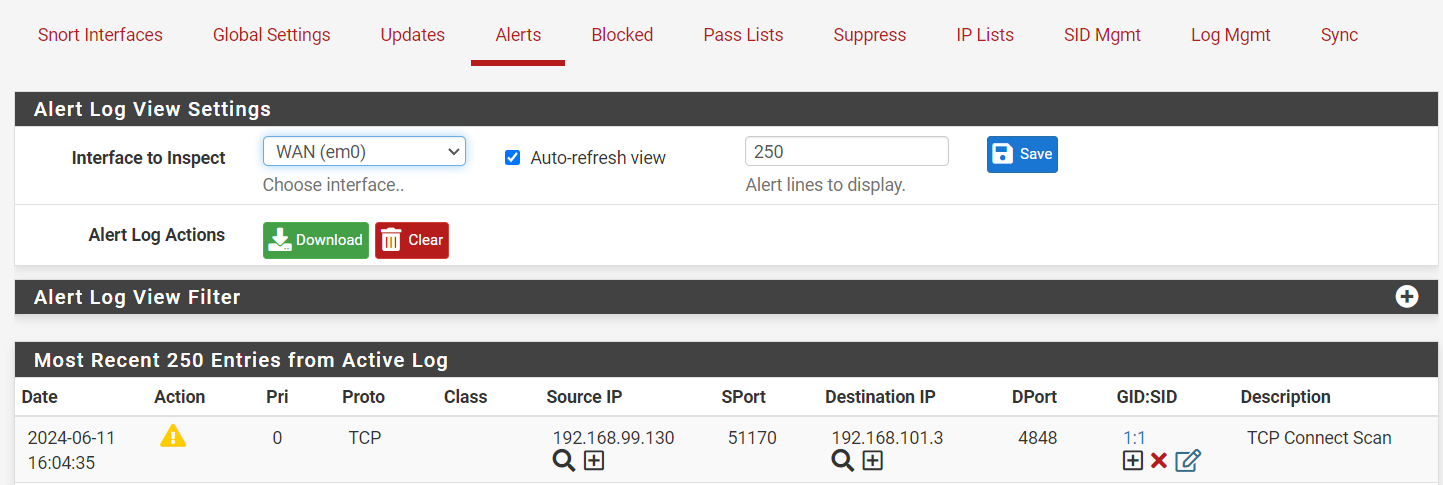
* Thêm rule vào snort và kiểm tra lần lượt:



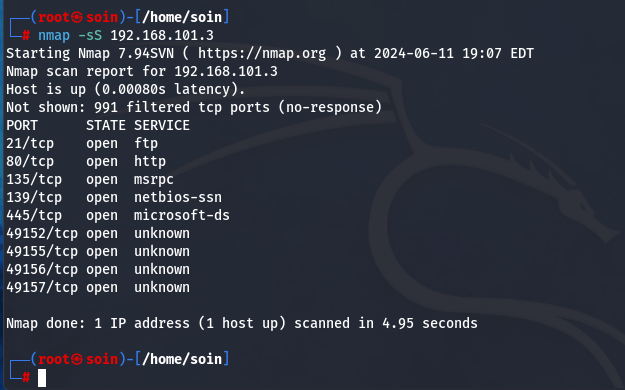
- Đầu tiên kiểm tra TCP Connect:



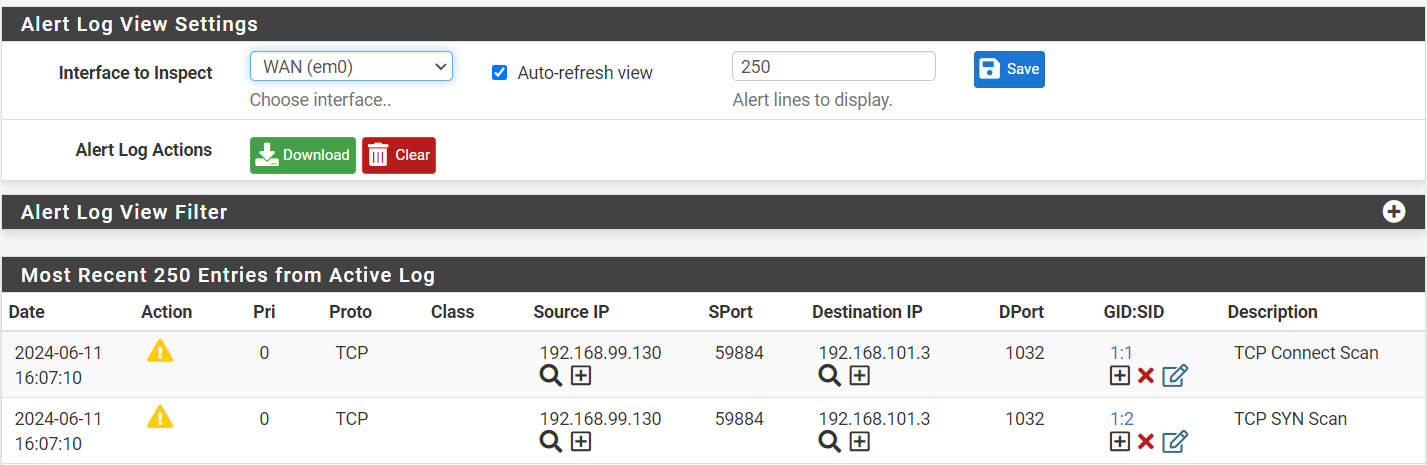
* Snort phát hiện:



* SYN Scan:



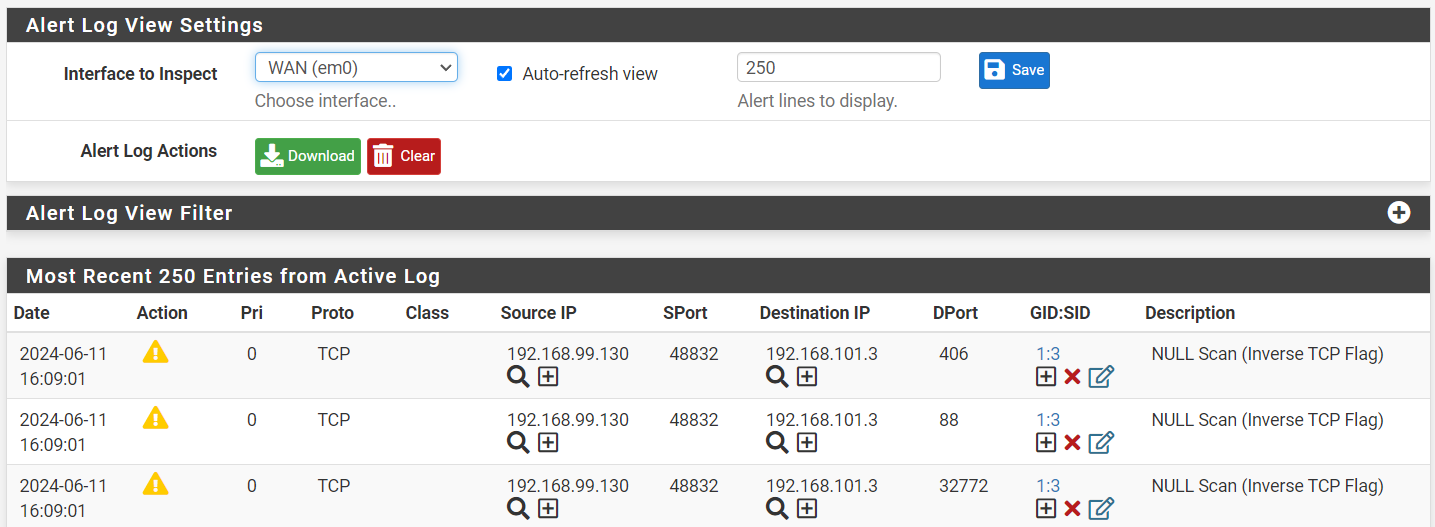
* Snort phát hiện được:



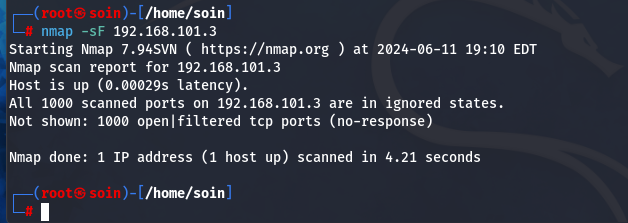
* Inverse TCP Flag (NULL Scan)



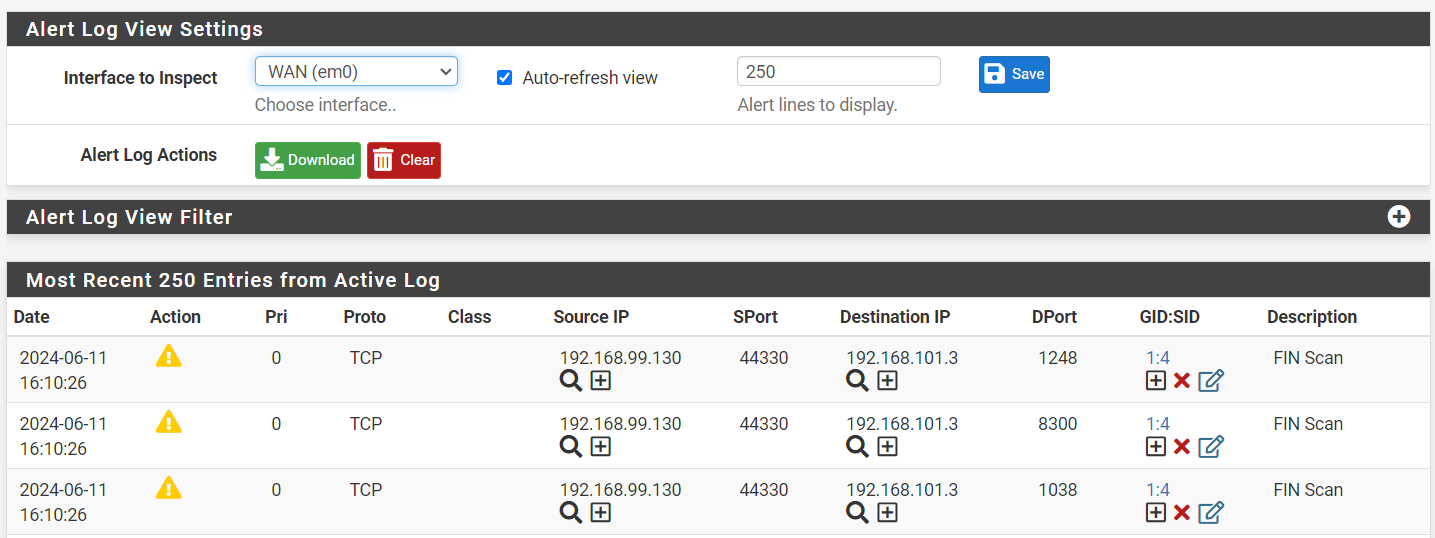
* Snort phát hiện:



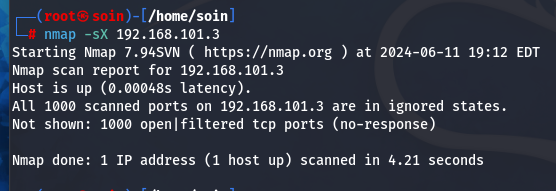
* FIN Scan:



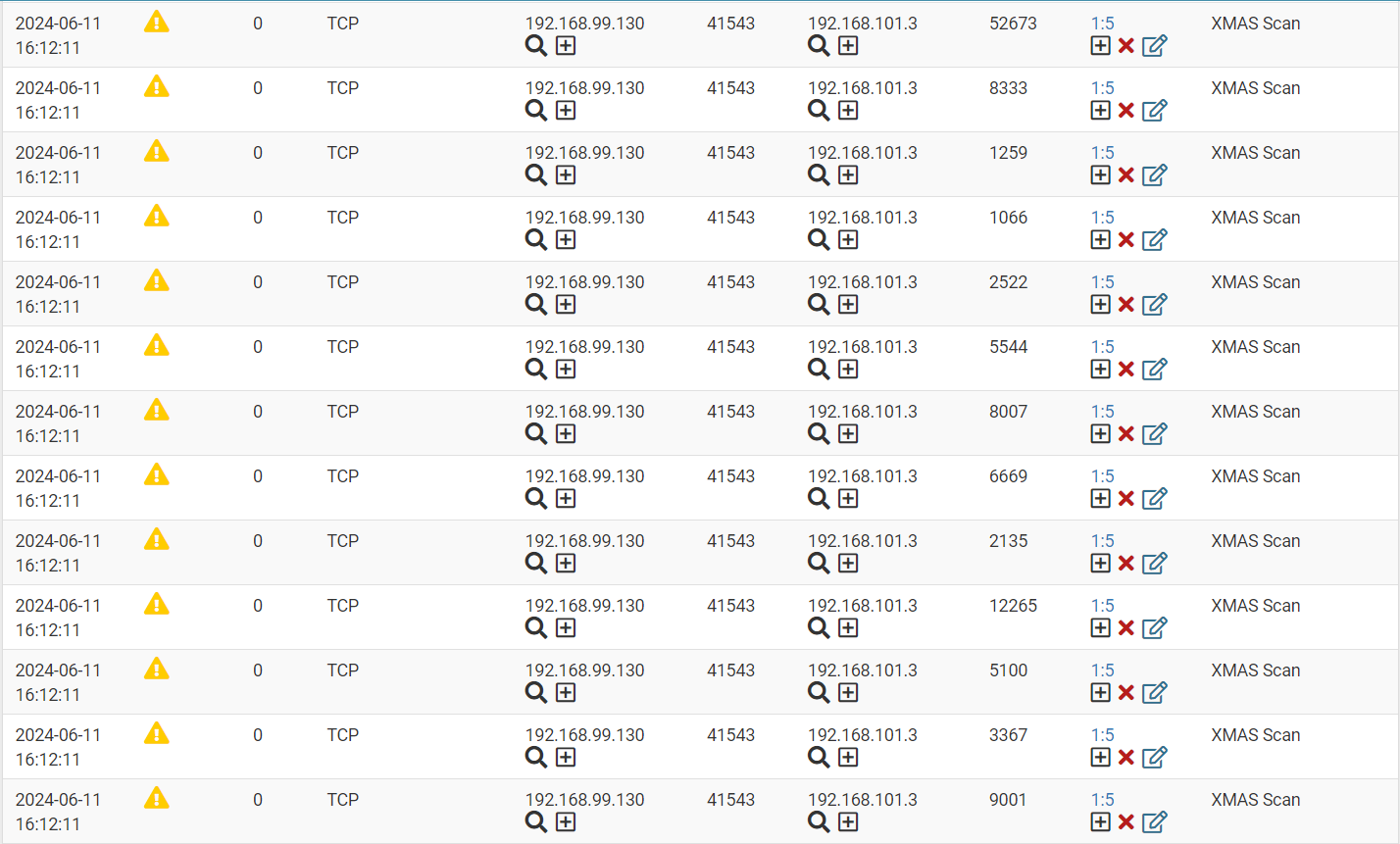
* Snort phát hiện:



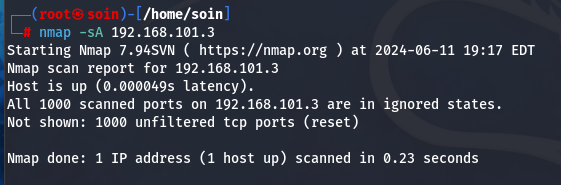
* XMAS Scan:



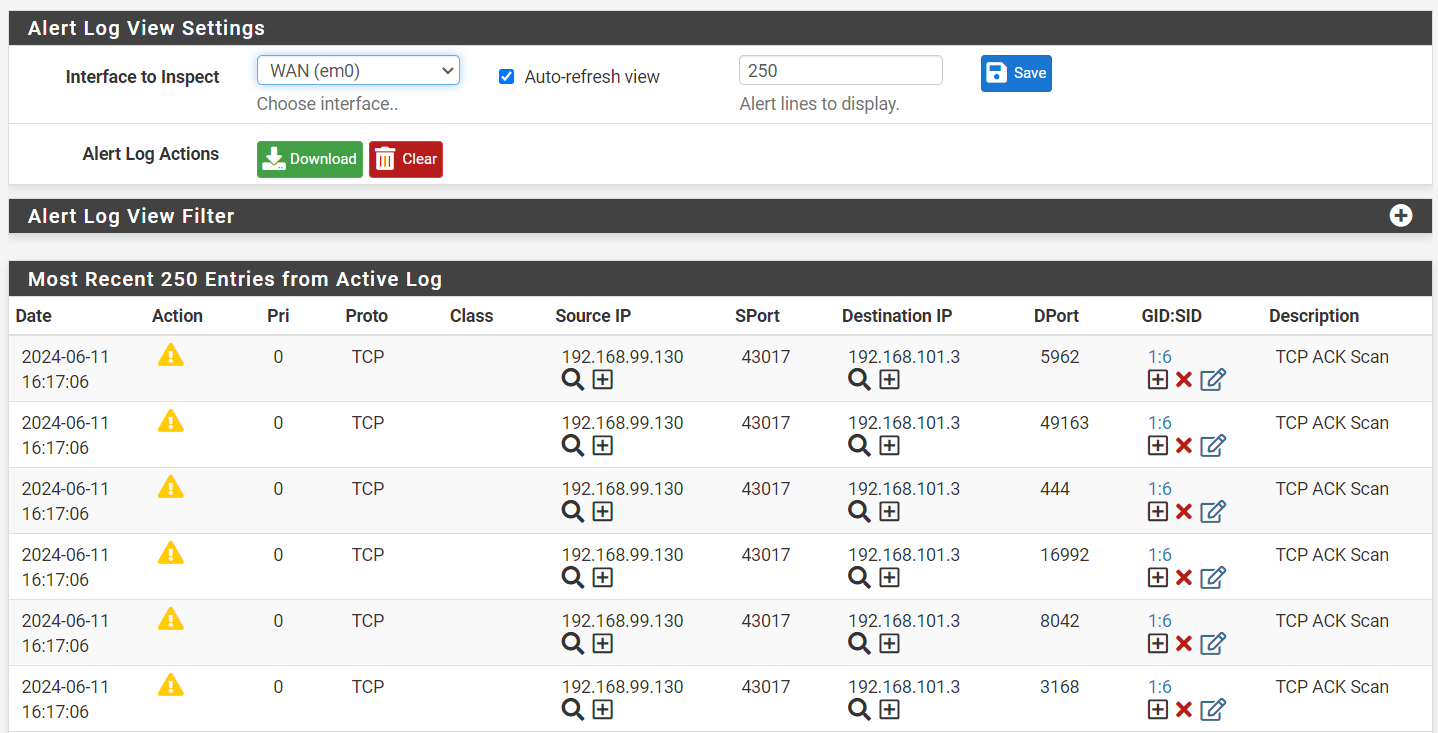
* Snort phát hiện:



* TCP ACK Scan:



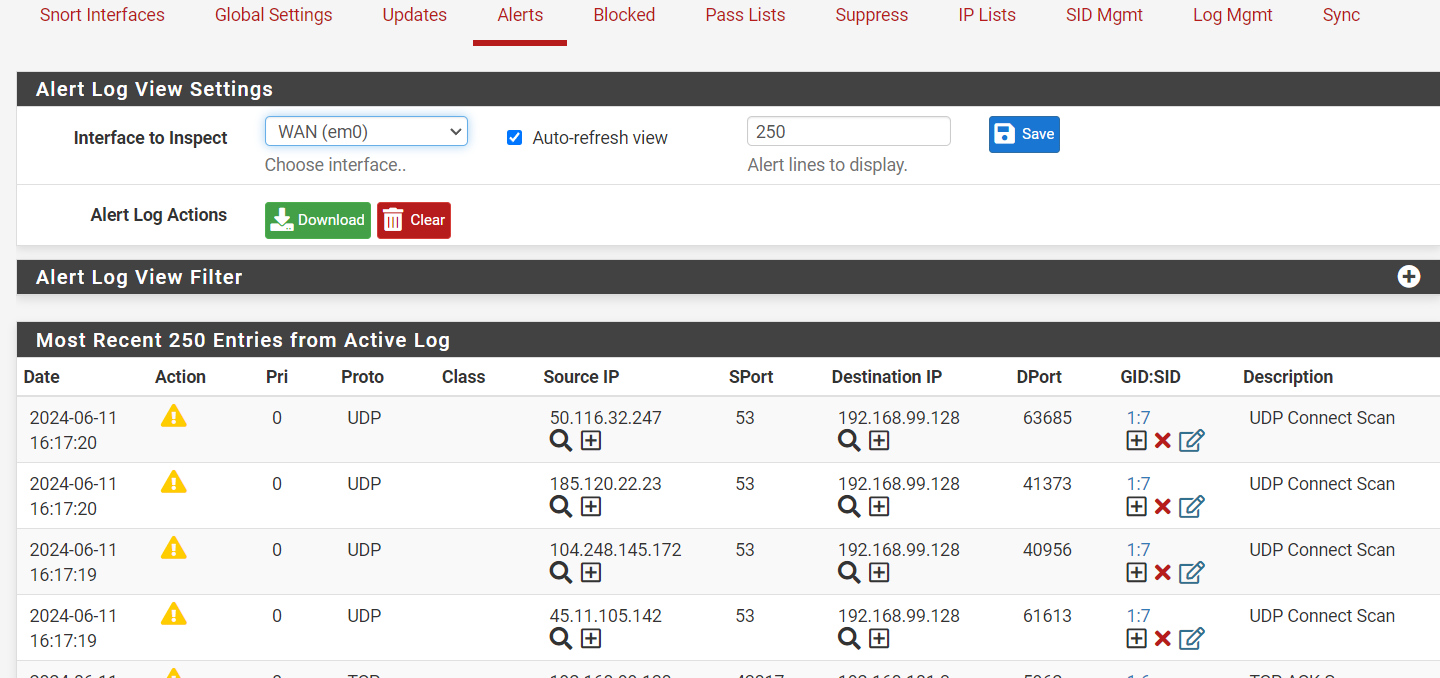
* Snort phát hiện:



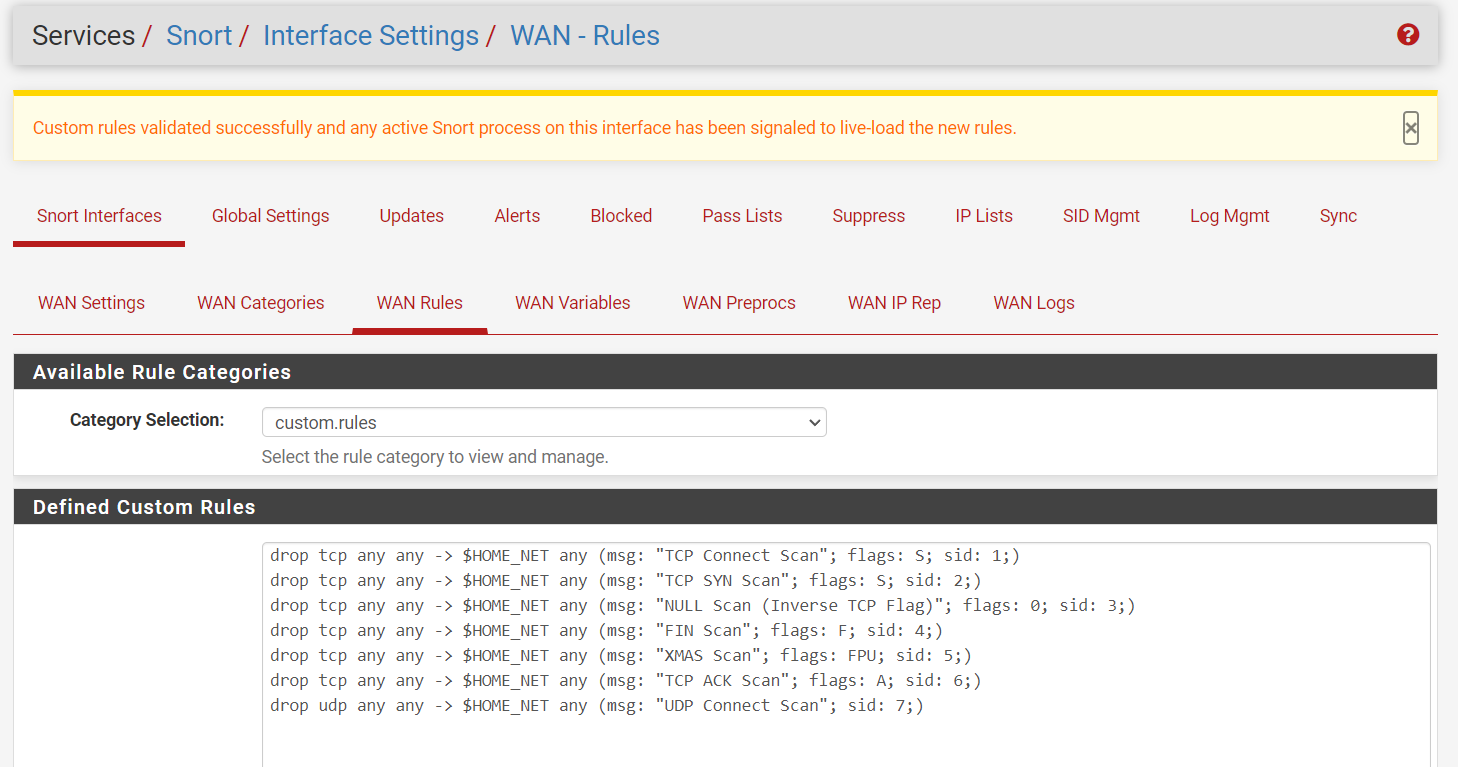
* UDP Connect Scan:



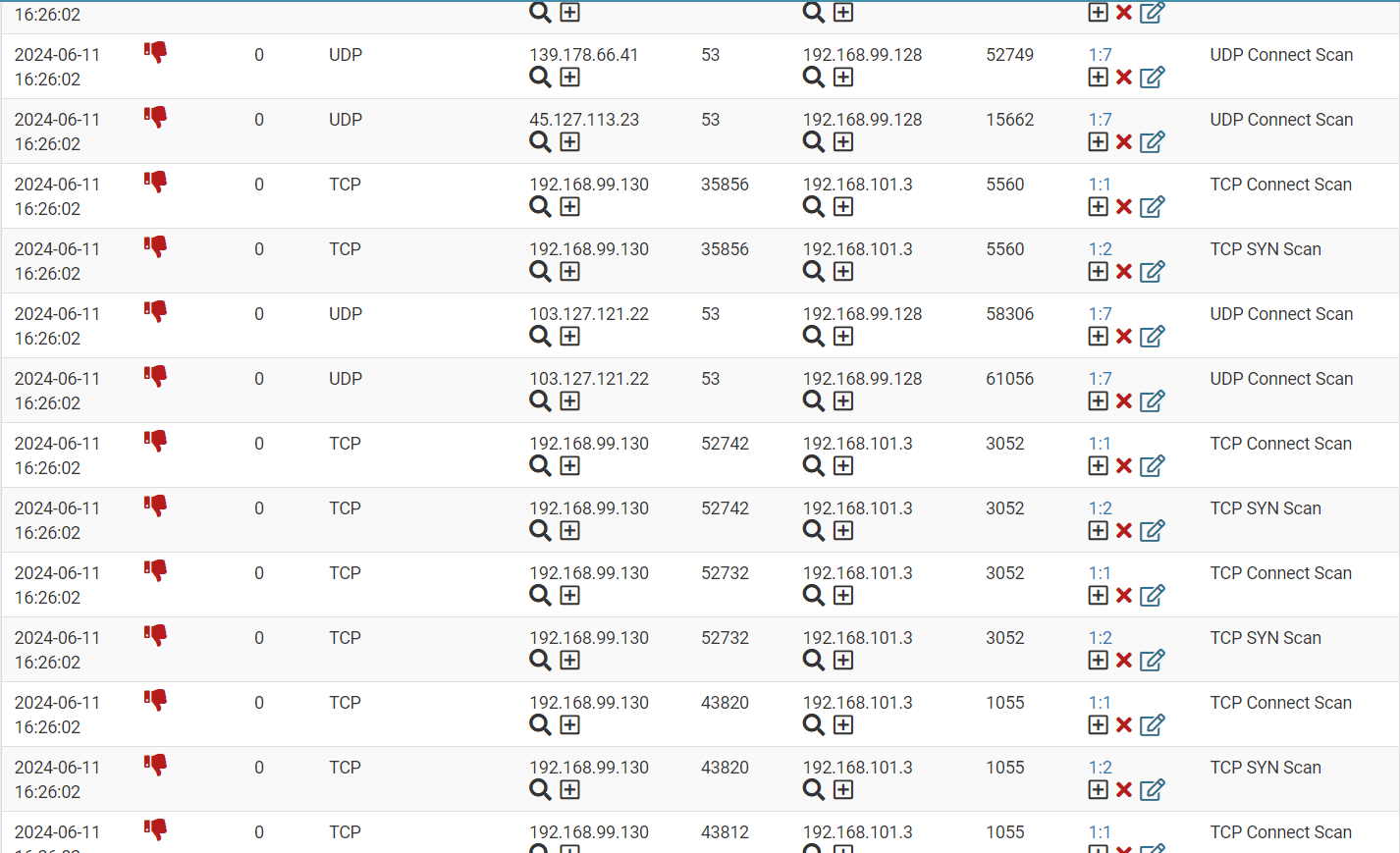
* Snort phát hiện:

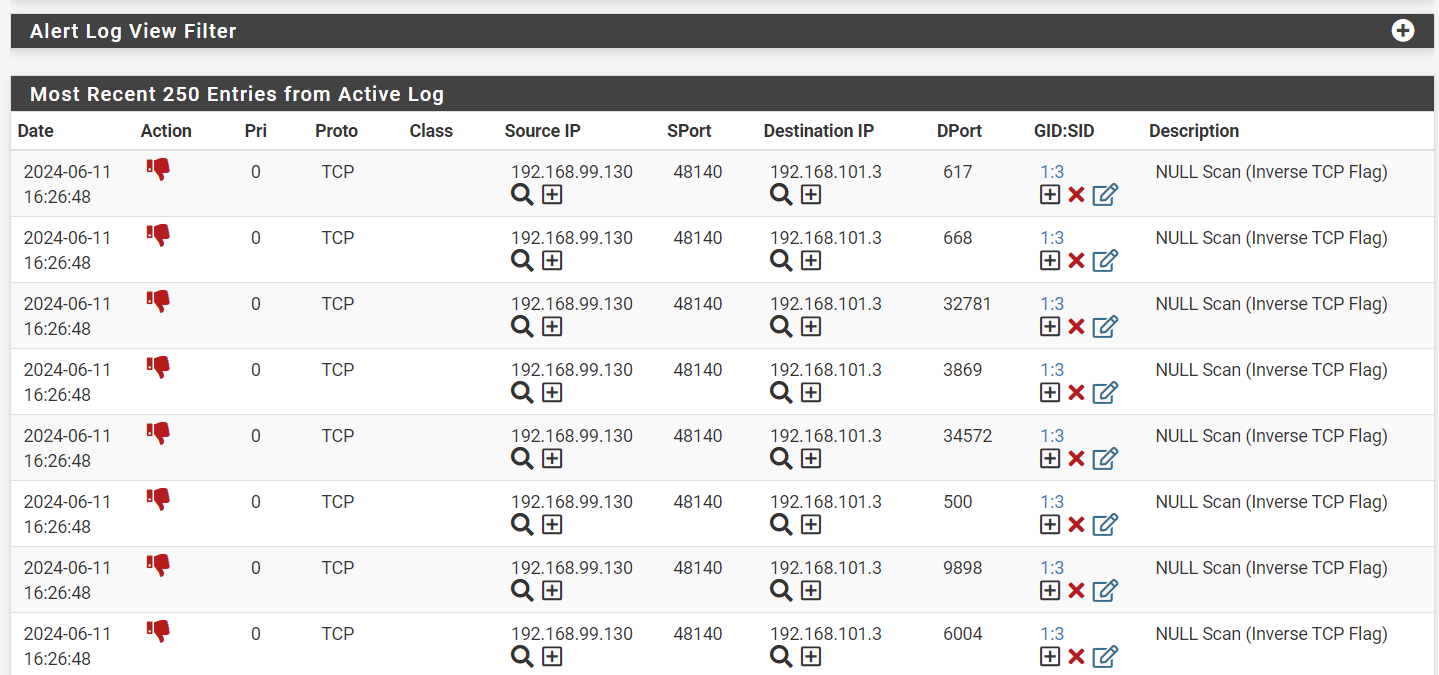


* Tiến hành drop các kỹ thuật quét:



* Snort drop:





### *Dùng hping3 để thực hiện synflood:*

* Ta có rule sau:

*alert tcp any any -> $HOME\_NET any (msg: "SYN Flood Attack"; flags: S; threshold: type threshold, track by\_src, count 20, seconds 3; sid: 1; rev: 1;)*

* Giải thích rule:

*alert tcp:* Loại cảnh báo - Đây là một cảnh báo cho lưu lượng truy cập TCP.

*any any:* Nguồn - Bất kỳ địa chỉ IP nguồn nào và bất kỳ cổng nguồn nào có thể kích hoạt rule này.

*-> $HOME\_NET:* \*\* đích\*\* - Mạng nhà của bạn, được biểu thị bằng $HOME\_NET (có thể là một biến được định nghĩa trước trong hệ thống bảo mật của bạn).

*any:* Cổng đích - Bất kỳ cổng nào trên mạng nhà của bạn.

*msg: "SYN Flood Attack";:* Thông báo - Khi rule kích hoạt, nó sẽ ghi lại cảnh báo với nội dung "SYN Flood Attack" để thông báo cho bạn về khả năng xảy ra tấn công.

*flags: S:* Kiểm tra cờ - Rule chỉ kích hoạt nếu gói tin có cờ SYN được đặt, cho biết đây là gói tin khởi tạo kết nối TCP.

*threshold: type threshold:* Kiểu ngưỡng - Sử dụng ngưỡng dựa trên số lượng.

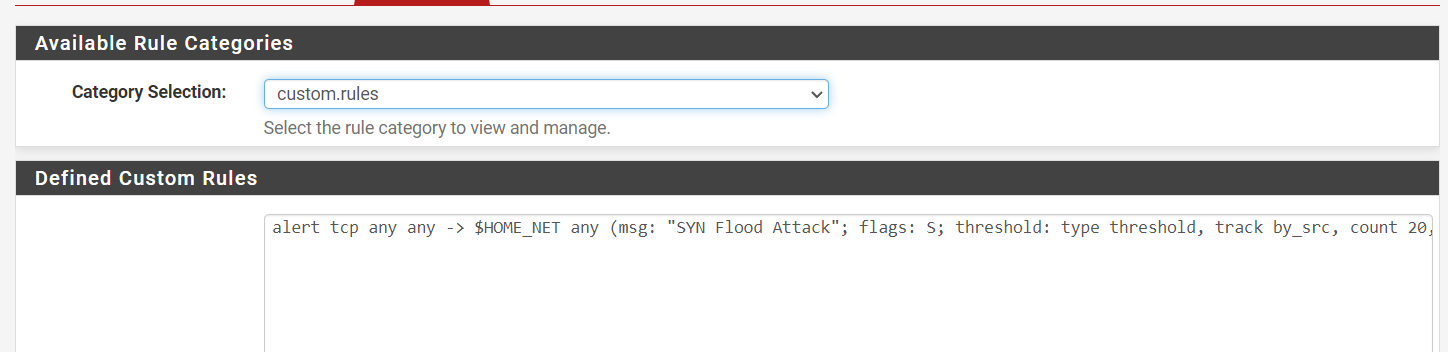
*track by\_src:* Theo dõi theo nguồn - Theo dõi số lần kích hoạt của rule theo từng địa chỉ IP nguồn.

*count 20:* Số lượng kích hoạt - Rule sẽ kích hoạt nếu có 20 hoặc nhiều hơn các gói tin khớp với điều kiện trong vòng 3 giây.

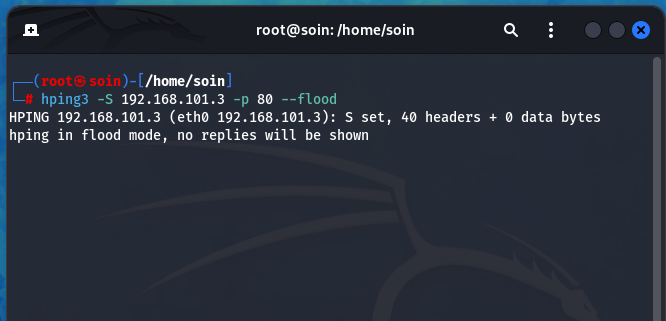
*seconds 3:* Khoảng thời gian - Quy định khoảng thời gian để theo dõi số lượng kích hoạt (3 giây trong trường hợp này).

*sid: 1:* Mã định danh duy nhất (SID) cho rule này.

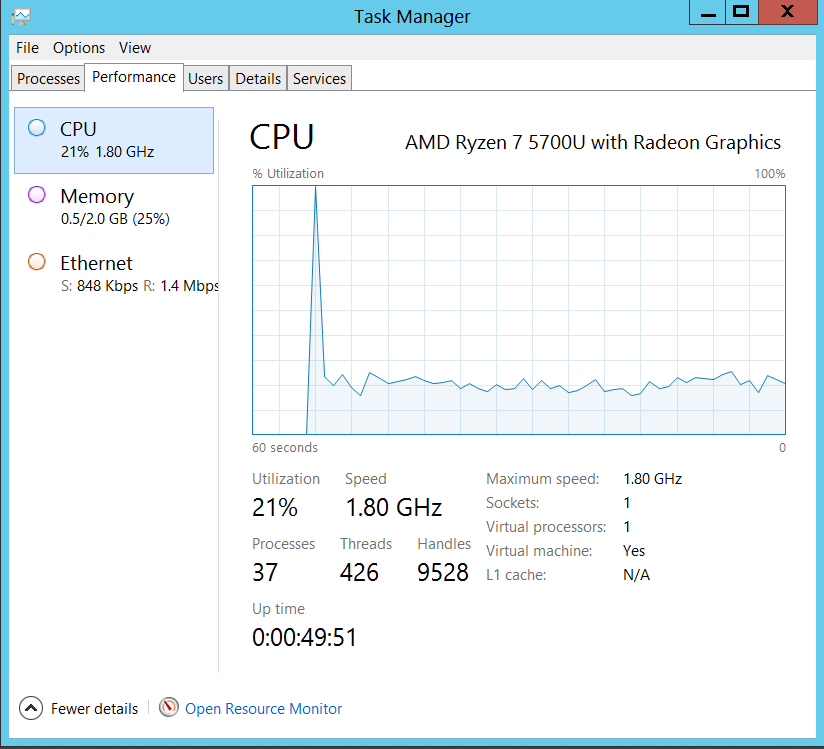
*rev:1:* Số phiên bản của rule.



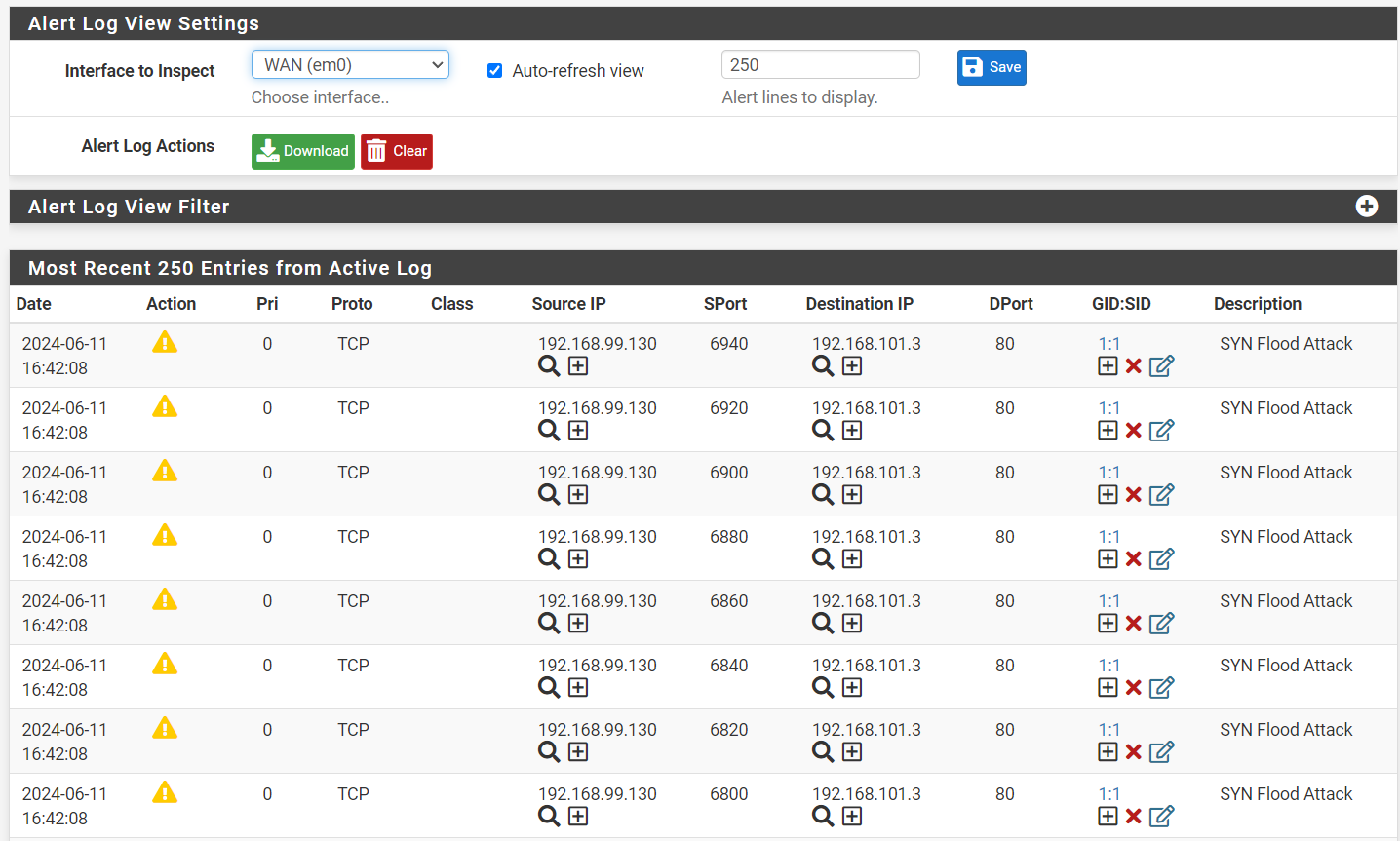
* Sử dụng hping3 để thực hiện synflood:



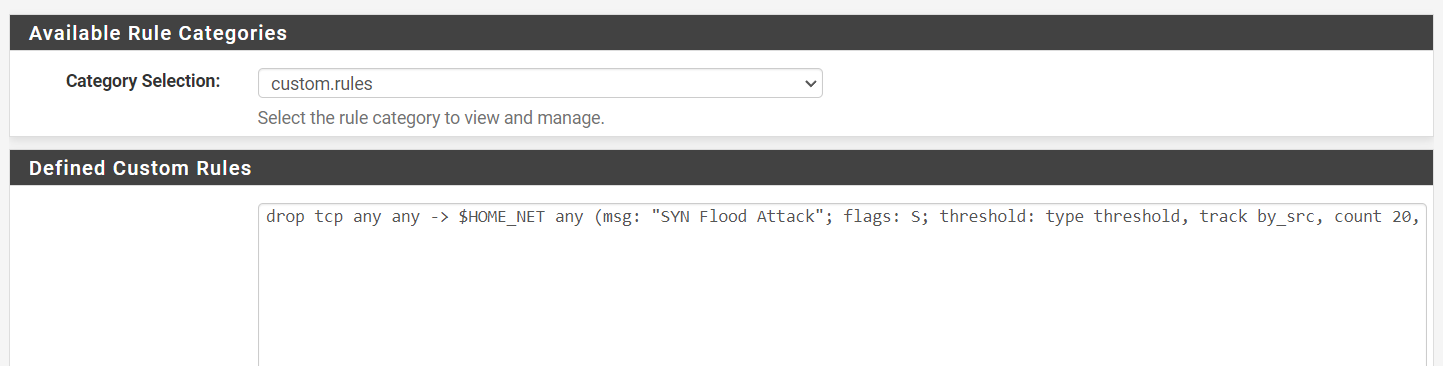
* Ở máy nạn nhân ta thấy CPU tăng bất thường:



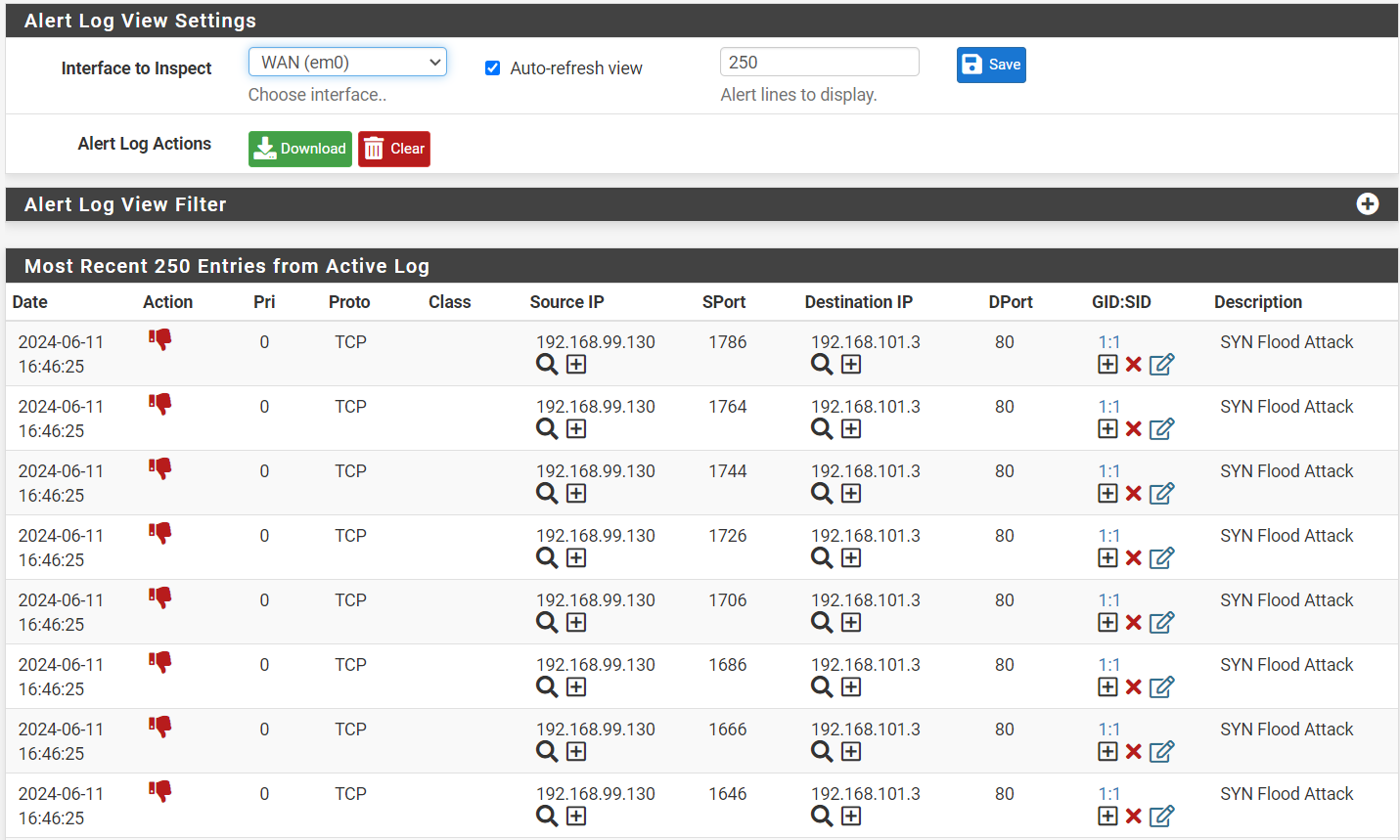
* Snort phát hiện được cuộc tấn công syn flood:



* Ở phần ngăn chặn ta chỉ cần đổi alert thành drop:



* Thực hiện tấn công lại và xem phản ứng của snort:



### *Các kỹ thuật khác*

* Khai thác lổ hổng ms17-010:
* Ta có rule sau:

*alert tcp any any -> any 445 (msg:"ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010"; flow:established,to\_server; content:"|8000a80000000000000000000000000000000000ffff000000000000ffff0000000000000000000000000000000000000000000000f1dfff000000000000000020f0dfff00f1dfffffffffff600004100000000080efdfff|"; reference:cve,CVE-2017-0143; classtype:attempted-admin; sid:1; rev:1; metadata:affected\_product Windows\_XP\_Vista\_7\_8\_10\_Server\_32\_64\_Bit, attack\_target Client\_Endpoint, created\_at 2017\_05\_16, deployment Perimeter, former\_category CURRENT\_EVENTS, performance\_impact Low, signature\_severity Major, updated\_at 2019\_07\_26;)*

* Giải thích rule:

*alert:* Thông báo cảnh báo khi phát hiện hoạt động khớp với quy tắc.

*tcp:* Giao thức mạng được sử dụng (TCP trong trường hợp này).

*any:* Bất kỳ địa chỉ IP nguồn nào*.*

*any:* Bất kỳ địa chỉ IP đích nào.

*->:* Biểu thị lưu lượng truy cập từ nguồn đến đích.

*445:* Cổng đích (445 là cổng mặc định cho SMBv1).

*flow:established,to\_server:* Phần này cho biết rule chỉ kiểm tra các gói tin trong luồng đã thiết lập (established flow) và được gửi đến server (to\_server). Lỗ hổng EternalBlue thường được khai thác trong giai đoạn sau khi kết nối SMB đã được thiết lập.

*content:"|8000a80000000000000000000000000000000000ffff000000000000ffff0000000000000000000000000000000000000000000000f1dfff000000000000000020f0dfff00f1dfffffffffff600004100000000080efdfff|":* Đây là phần quan trọng nhất của rule. Nó định nghĩa mẫu nội dung (payload) cụ thể được sử dụng trong exploit EternalBlue. Chuỗi ký tự dài này là một phần của gói tin được kẻ tấn công gửi đến server SMB bị lỗ hổng. Suricata sẽ so sánh nội dung của gói tin với chuỗi này để phát hiện lỗ hổng.

*reference:cve,CVE-2017-0143:* Chỉ tham chiếu đến lỗ hổng CVE-2017-0143 (EternalBlue).

*classtype:attempted-admin:* Phân loại sự kiện này là một nỗ lực truy cập quản trị (attempted admin).

*sid:2024297; rev:2:* sid (Security Identifier) là một mã định danh duy nhất cho rule này. rev (revision) cho biết đây là phiên bản thứ 2 của rule.

*metadata:* Phần metadata cung cấp thêm thông tin về rule, bao gồm:

*affected\_product:* Các sản phẩm Windows bị ảnh hưởng bởi lỗ hổng.

*attack\_target:* Mục tiêu của tấn công là điểm cuối của client (Client\_Endpoint).

*created\_at:* Ngày rule được tạo (16/05/2017).

*deployment:* Vị trí triển khai rule (khu vực Perimeter).

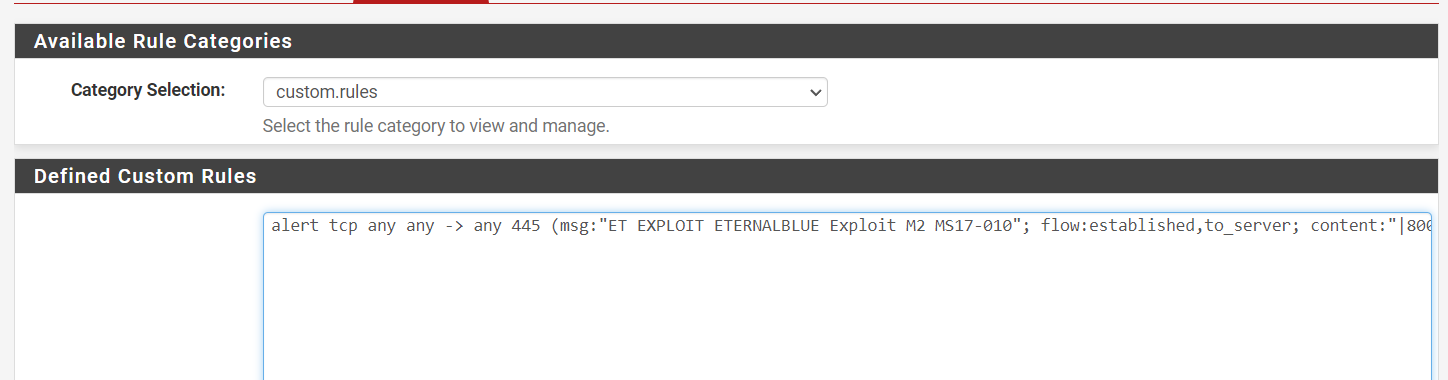
*former\_category:* Thể loại cũ của rule (CURRENT\_EVENTS).

*performance\_impact:* Tác động đến hiệu suất hệ thống (thấp - Low).

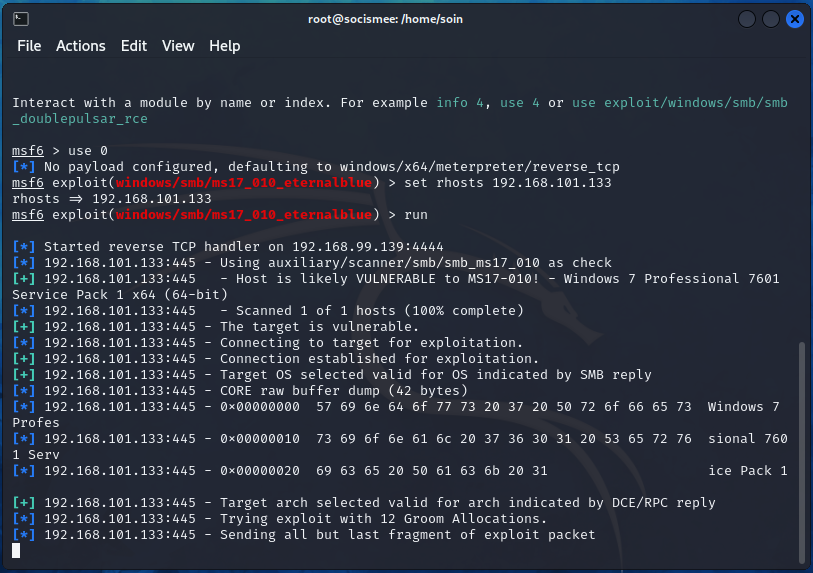
*signature\_severity:* Mức độ nghiêm trọng của lỗ hổng (cao - Major).

*updated\_at:* Ngày rule được cập nhật lần cuối (26/07/2019).

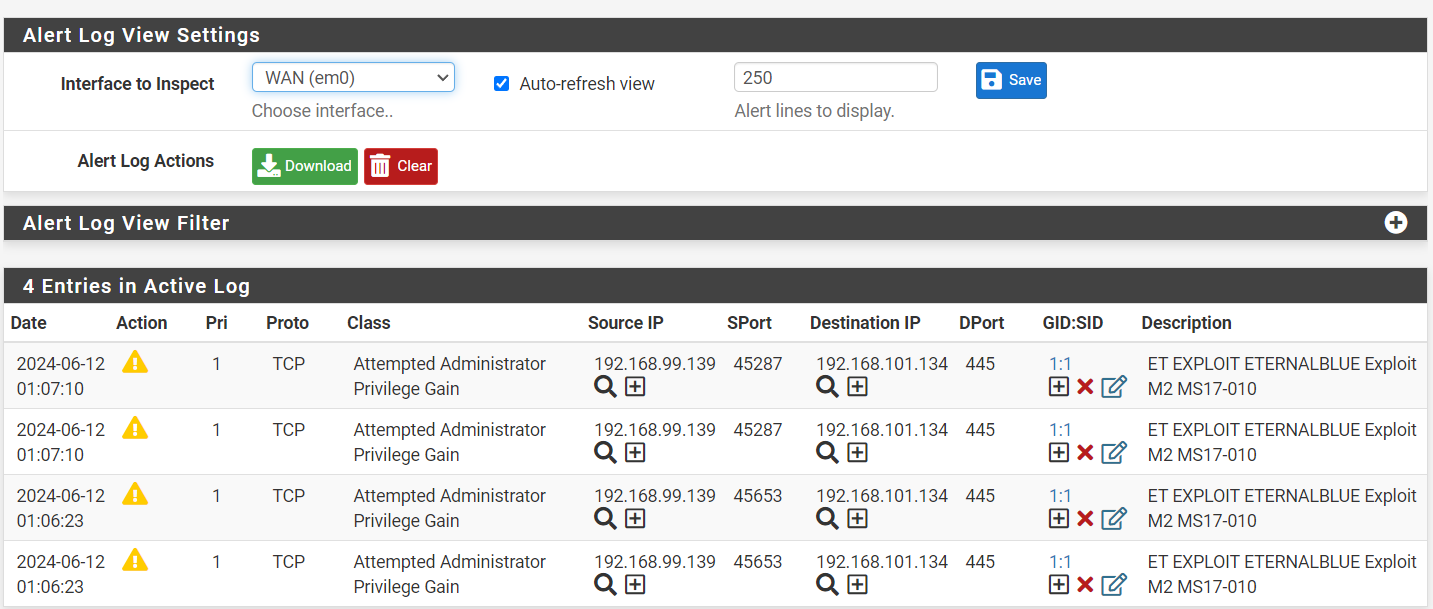
* Ta cài đặt rule trên snort:



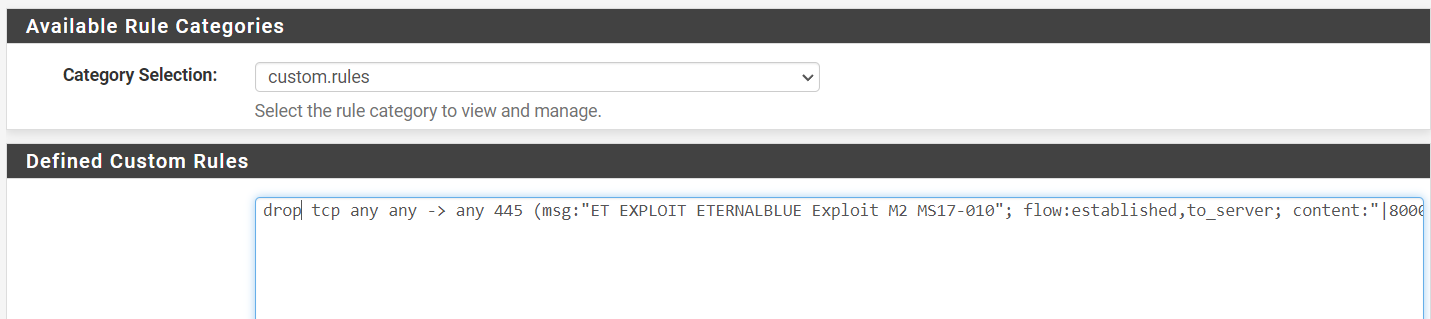
* Thực hiện tấn công từ kali vào máy nạn nhân có chưa lỗ hổng ms17-010:



* Snort phát ra cảnh báo:



* Ta tiến hành ngăn chặn cuộc tấn công này:



* Cuộc tấn công đã bị ngăn chặn:

