

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

**GVHD:** Bùi Duy Cường

**HỌ VÀ TÊN:** Nguyễn Ngọc Lan Anh

**MSSV:** 2033210445

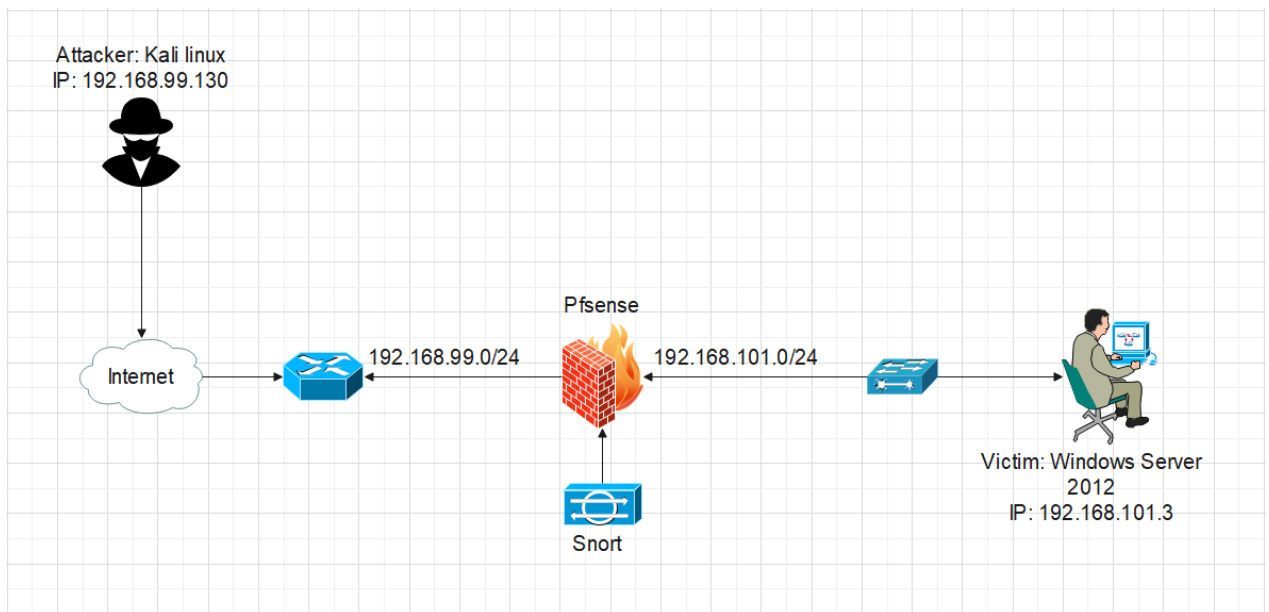
**LỚP:** 12DHBM05

*TP. HỒ CHÍ MINH, tháng 06 năm 2024*

## Mục lục

|      |   |    |
|------|---|----|
| I.   | Mô hình:.....                                   | 3  |
| II.  | Tiến hành cài đặt.....                          | 4  |
| 1.   | Cài đặt snort trên pfsense .....                | 4  |
| 2.   | Thông số mạng của thiết bị, test ping .....     | 5  |
| 3.   | Ping of death .....                             | 6  |
| 4.   | Tiến hành thực hiện ở một số rule khác:.....    | 10 |
| 4.1. | <i>Scaning port 81:</i> .....                   | 10 |
| 4.2. | <i>Kiểm tra kết nối ftp:</i> .....              | 12 |
| 4.3. | <i>Testing UDP</i> .....                        | 14 |
| 4.4. | <i>Thông báo truy cập HTTP</i> .....            | 16 |
| 4.5. | <i>Nmap thực hiện quét</i> .....                | 18 |
| 4.6. | <i>Dùng hping3 để thực hiện synflood:</i> ..... | 29 |
| 4.7. | <i>Các kỹ thuật khác</i> .....                  | 33 |

## I. Mô hình:



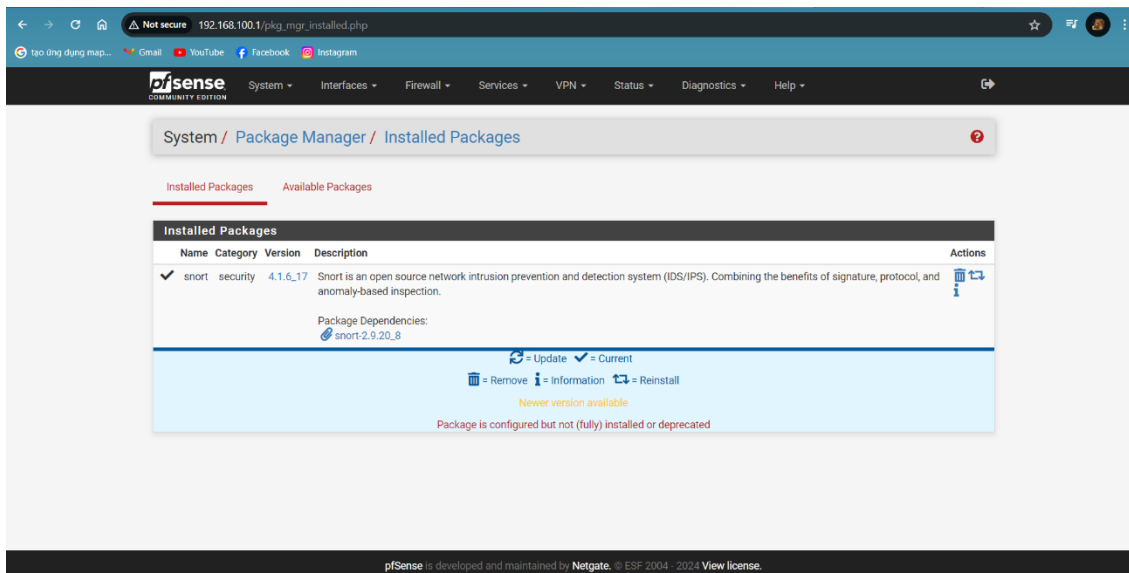
Mô tả mô hình:

| 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/<br>Windows 7 | 192.168.101.x  | VMNet2    |

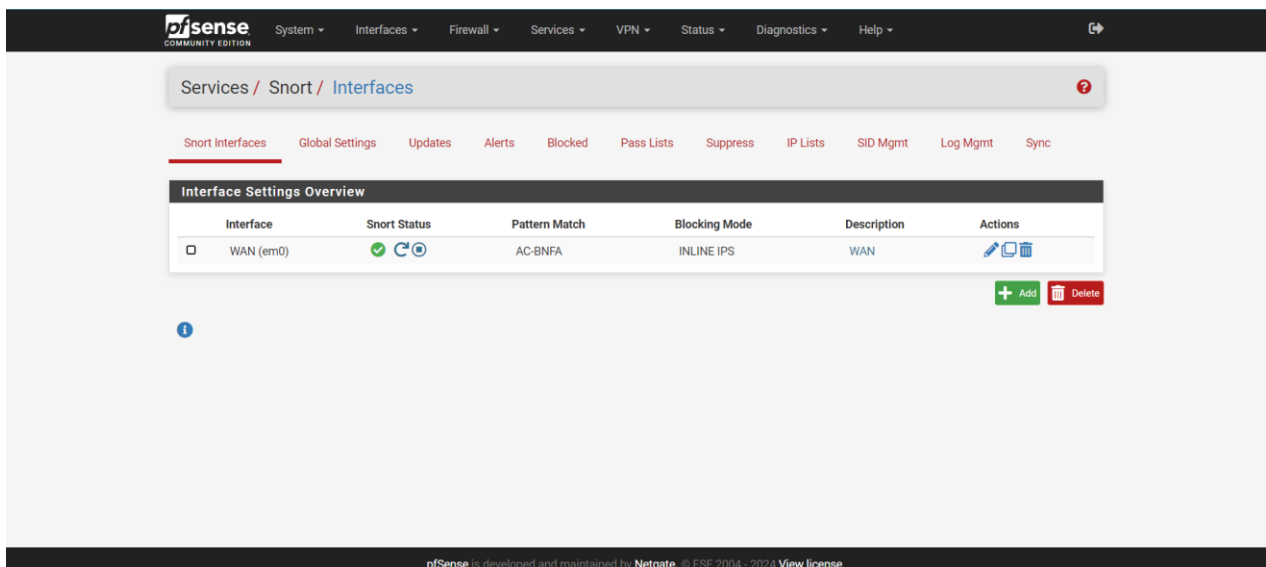
## II. Tiến hành cài đặt

### 1. 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:

Block Settings

Block Offenders

☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode

Inline Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

## 2. Thông số mạng của thiết bị, test ping

Thông số mạng của máy attacker:

```

soin@soin: ~
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.99.3 netmask 255.255.255.0 broadcast 192.168.99.255
    inet6 fe80::20c:29ff:fe4f:8787 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:4f:87:87 txqueuelen 1000 (Ethernet)
    RX packets 45 bytes 6599 (6.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 90 bytes 11166 (10.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 24 bytes 1440 (1.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1440 (1.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

soin@soin: ~
$

```

Thông số mạng máy victim:

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::7188:b0c2:be3:679d%12
    IPv4 Address. . . . . : 192.168.101.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.101.1

Tunnel adapter isatap.{03B743FE-3E6C-4EFF-B63A-61CAF2B9AFD4}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Administrator>
```

Kiểm tra ping từ máy attacker đến máy victim:

```
soin@soin: ~
(soin@soin)-[~]
$ ping 192.168.101.3
PING 192.168.101.3 (192.168.101.3) 56(84) bytes of data.
64 bytes from 192.168.101.3: icmp_seq=1 ttl=128 time=1.59 ms
64 bytes from 192.168.101.3: icmp_seq=2 ttl=128 time=2.16 ms
64 bytes from 192.168.101.3: icmp_seq=3 ttl=128 time=1.16 ms
64 bytes from 192.168.101.3: icmp_seq=4 ttl=128 time=1.37 ms
64 bytes from 192.168.101.3: icmp_seq=5 ttl=128 time=0.795 ms
64 bytes from 192.168.101.3: icmp_seq=6 ttl=128 time=0.659 ms
64 bytes from 192.168.101.3: icmp_seq=7 ttl=128 time=1.09 ms
64 bytes from 192.168.101.3: icmp_seq=8 ttl=128 time=0.742 ms
64 bytes from 192.168.101.3: icmp_seq=9 ttl=128 time=1.03 ms
^C
--- 192.168.101.3 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8069ms
rtt min/avg/max/mdev = 0.659/1.175/2.159/0.447 ms

(soin@soin)-[~]
$
```

### 3. 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.

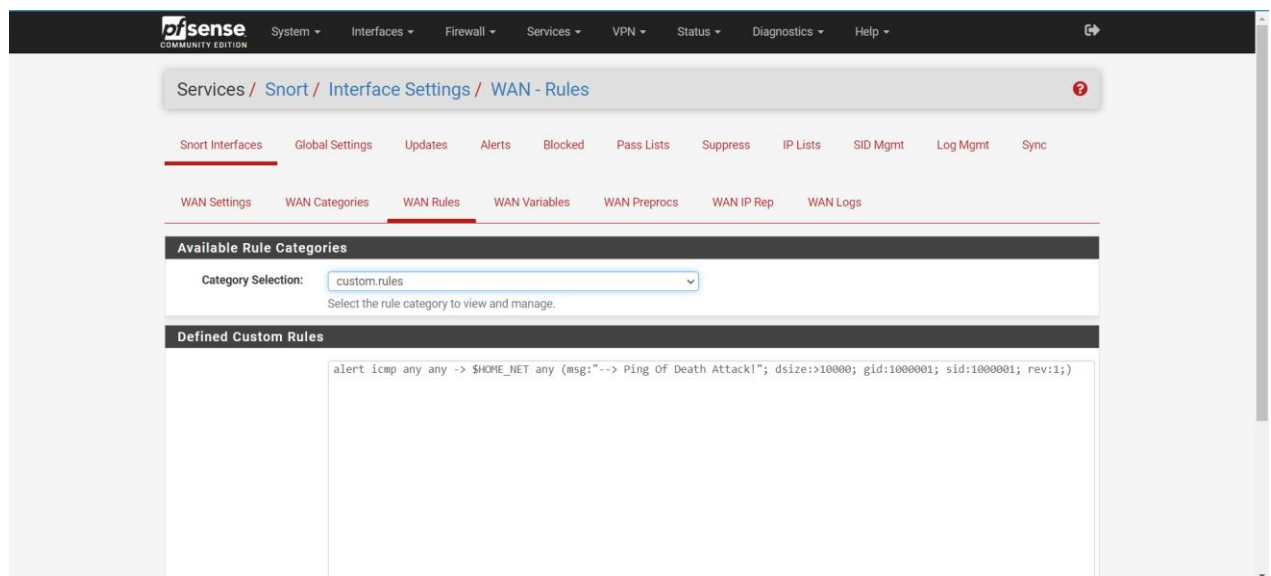
*any any*: Cho biết nguồn (any) có thể đến từ bất kỳ đâu và đích (any) có thể là bất kỳ cổng nào trên thiết bị trong mạng nội bộ của bạn (\$HOME\_NET). \$HOME\_NET là biến được định nghĩa trước trong Snort, đại diện cho mạng nội bộ đáng tin cậy của bạn.

*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:

```
soin@soin: ~  
$ ping -s 65507 192.168.101.3  
PING 192.168.101.3 (192.168.101.3) 65507(65535) bytes of data.  
65515 bytes from 192.168.101.3: icmp_seq=1 ttl=128 time=4.06 ms  
65515 bytes from 192.168.101.3: icmp_seq=2 ttl=128 time=3.01 ms  
65515 bytes from 192.168.101.3: icmp_seq=3 ttl=128 time=3.28 ms  
65515 bytes from 192.168.101.3: icmp_seq=4 ttl=128 time=2.95 ms
```

- Snort đã cảnh báo:

Services / [Snort](#) / Alerts

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

**Alert Log View Settings**

Interface to Inspect: WAN (em0) ☐ Auto-refresh view 250   
Choose interface.. Alert lines to display.

**Alert Log Actions**

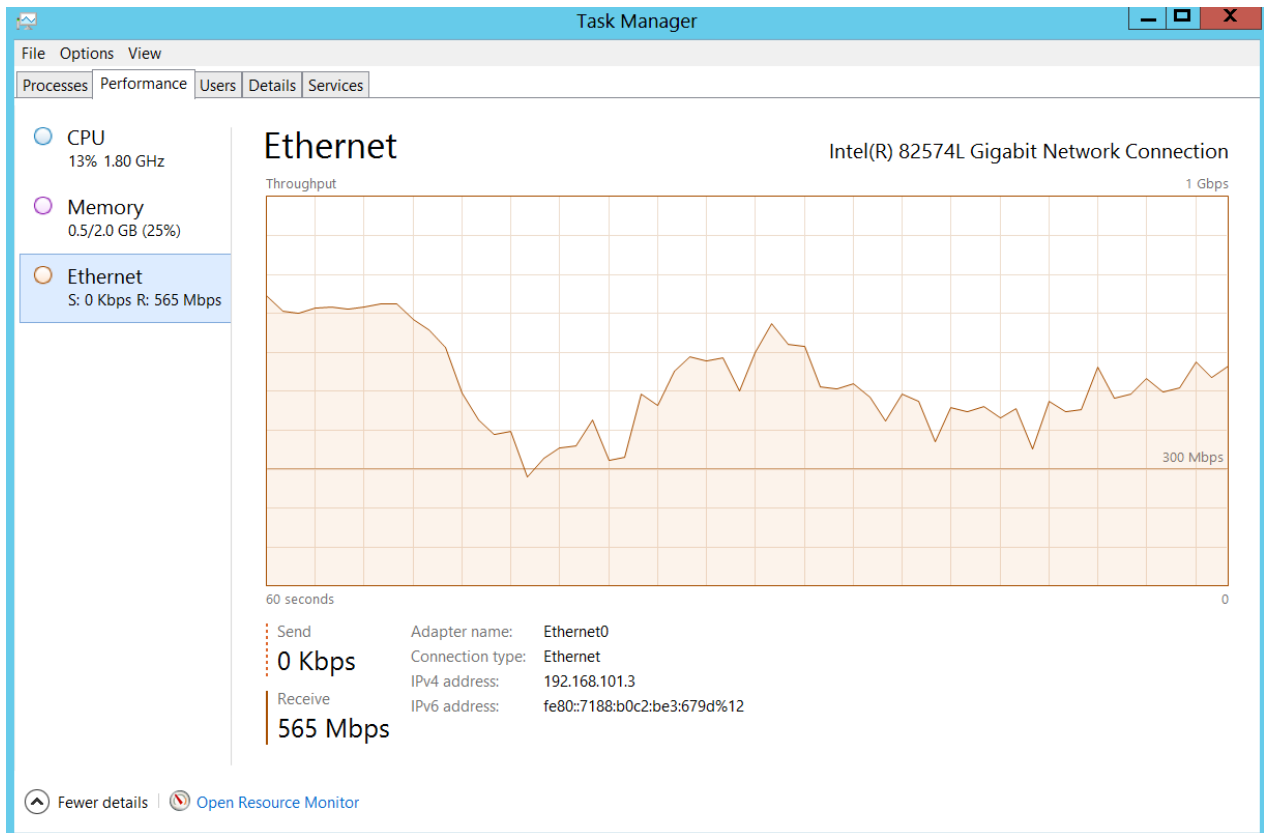
**Alert Log View Filter**

**7 Entries in Active Log**

| Date                | Action | Pri | Proto | Class | Source IP      | SPort | Destination IP | DPort | GID:SID         | Description               |
|---------------------|--------|-----|-------|-------|----------------|-------|----------------|-------|-----------------|---------------------------|
| 2024-06-11 14:16:10 | ⚠      | 0   | ICMP  |       | 192.168.99.130 |       | 192.168.101.3  |       | 1000001:1000001 | --> Ping Of Death Attack! |
| 2024-06-11 14:16:09 | ⚠      | 0   | ICMP  |       | 192.168.99.130 |       | 192.168.101.3  |       | 1000001:1000001 | --> Ping Of Death Attack! |
| 2024-06-11 14:16:08 | ⚠      | 0   | ICMP  |       | 192.168.99.130 |       | 192.168.101.3  |       | 1000001:1000001 | --> Ping Of Death Attack! |
| 2024-06-11 14:16:07 | ⚠      | 0   | ICMP  |       | 192.168.99.130 |       | 192.168.101.3  |       | 1000001:1000001 | --> Ping Of Death Attack! |
| 2024-06-11 14:16:06 | ⚠      | 0   | ICMP  |       | 192.168.99.130 |       | 192.168.101.3  |       | 1000001:1000001 | --> Ping Of Death Attack! |

- 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:

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☒ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

6 Entries in Active Log

| Date                | Action | Pri | Proto | Class | Source IP      | SPort | Destination IP | DPort | GID:SID         | Description               |
|---------------------|--------|-----|-------|-------|----------------|-------|----------------|-------|-----------------|---------------------------|
| 2024-06-11 14:20:59 |        | 0   | ICMP  |       | 192.168.99.130 |       | 192.168.101.3  |       | 1000001:1000001 | --> Ping Of Death Attack! |
| 2024-06-11 14:20:58 |        | 0   | ICMP  |       | 192.168.99.130 |       | 192.168.101.3  |       | 1000001:1000001 | --> Ping Of Death Attack! |
| 2024-06-11 14:20:57 |        | 0   | ICMP  |       | 192.168.99.130 |       | 192.168.101.3  |       | 1000001:1000001 | --> Ping Of Death Attack! |
| 2024-06-11 14:20:56 |        | 0   | ICMP  |       | 192.168.99.130 |       | 192.168.101.3  |       | 1000001:1000001 | --> Ping Of Death Attack! |
| 2024-06-11 14:20:55 |        | 0   | ICMP  |       | 192.168.99.130 |       | 192.168.101.3  |       | 1000001:1000001 | --> Ping Of Death Attack! |
| 2024-06-11 14:20:54 |        | 0   | ICMP  |       | 192.168.99.130 |       | 192.168.101.3  |       | 1000001:1000001 | --> Ping Of Death Attack! |

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

### 4.1. Scanning port 81:

- Ta có rule như sau:

`alert icmp any any -> $HOME_NET 81 (msg:"Scanning 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.

10

Available Rule Categories

Category Selection:

custom.rules

Select the rule category to view and manage.

Defined Custom Rules

```

alert icmp any any -> $HOME_NET 81 (msg:"Scanning Port 81"; sid:1000005; rev:1;)

```

- Sử dụng nmap để thực hiện kiểm thử

soin@soin: ~

(soin@soin)-[~]

\$

nmap -p 81 192.168.101.3

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 17:29 EDT

Nmap scan report for 192.168.101.3

Host is up (0.0035s latency).

PORT STATE SERVICE

81/tcp filtered hosts2-ns

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

(soin@soin)-[~]

\$

- Snort vẫn phát hiện được:

←

→

↺

↻

🏠

⚠ Not secure

192.168.100.1/snort\_alerts.php?instance=0

☆

👤

⋮

🔍 Tạo ứng dụng map...

📧 Gmail

📺 YouTube

📘 Facebook

📷 Instagram

pfSense

COMMUNITY EDITION

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

🔗

Services / Snort / Alerts

?

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

+

1 Entries in Active Log

| Date                | Action | Pri | Proto | Class | Source IP      | SPort | Destination IP | DPort | GID:SID   | Description      |
|---------------------|--------|-----|-------|-------|----------------|-------|----------------|-------|-----------|------------------|
| 2024-06-08 10:14:37 | ⚠      | 0   | ICMP  |       | 192.168.99.130 |       | 192.168.101.3  |       | 1:1000005 | Scanning Port 81 |

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

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

11

Available Rule Categories

Category Selection:

custom.rules

Select the rule category to view and manage.

Defined Custom Rules

```
drop icmp any any -> $HOME_NET 81 (msg:"Scanning Port 81"; sid:1000005; rev:1;)
```

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

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☒ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

84 Entries in Active Log

| Date                | Action | Pri | Proto | Class | Source IP      | SPort | Destination IP | DPort | GID:SID   | Description      |
|---------------------|--------|-----|-------|-------|----------------|-------|----------------|-------|-----------|------------------|
| 2024-06-11 14:33:28 |        | 0   | ICMP  |       | 192.168.99.128 |       | 192.168.99.2   |       | 1:1000005 | Scanning Port 81 |
| 2024-06-11 14:33:27 |        | 0   | ICMP  |       | 192.168.99.128 |       | 192.168.99.2   |       | 1:1000005 | Scanning Port 81 |
| 2024-06-11 14:33:27 |        | 0   | ICMP  |       | 192.168.99.128 |       | 192.168.99.2   |       | 1:1000005 | Scanning Port 81 |
| 2024-06-11 14:33:26 |        | 0   | ICMP  |       | 192.168.99.128 |       | 192.168.99.2   |       | 1:1000005 | Scanning Port 81 |
| 2024-06-11 14:33:26 |        | 0   | ICMP  |       | 192.168.99.128 |       | 192.168.99.2   |       | 1:1000005 | Scanning Port 81 |

## 4.2. Kiểm tra kết nối ftp:

(để 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.

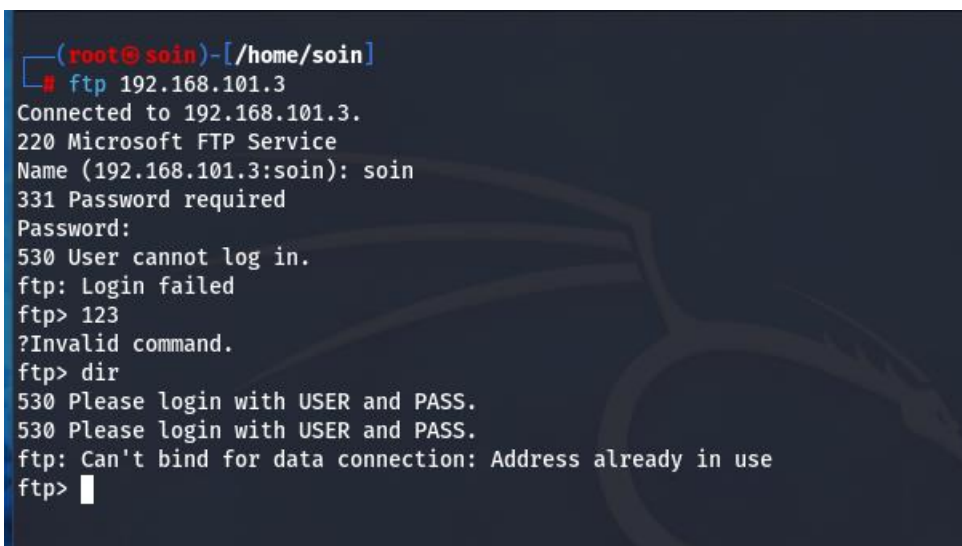
*sid*: Đây là mã định danh duy nhất của rule (Security ID - sid).

- Cài đặt rule cho snort:



The screenshot shows the 'Available Rule Categories' section with a dropdown menu set to 'custom.rules'. Below it, the 'Defined Custom Rules' section contains a single rule: `alert tcp any any -> $HOME_NET 21 (msg:"FTP connection=>Attempt"; sid:1000004;)`.

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



```
(root@soin)-[/home/soin]
ftp 192.168.101.3
Connected to 192.168.101.3.
220 Microsoft FTP Service
Name (192.168.101.3:soin): soin
331 Password required
Password:
530 User cannot log in.
ftp: Login failed
ftp> 123
?Invalid command.
ftp> dir
530 Please login with USER and PASS.
530 Please login with USER and PASS.
ftp: Can't bind for data connection: Address already in use
ftp>
```

- Snort phát cảnh báo:

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☒ Auto-refresh view
 

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

72 Entries in Active Log

| Date                | Action | Pri | Proto | Class | Source IP      | SPort | Destination IP  | DPort | GID:SID   | Description             |
|---------------------|--------|-----|-------|-------|----------------|-------|-----------------|-------|-----------|-------------------------|
| 2024-06-11 14:51:43 |        | 0   | TCP   |       | 192.168.99.130 | 37118 | 192.168.101.129 | 21    | 1:1000004 | FTP connection=>Attempt |
| 2024-06-11 14:51:43 |        | 0   | TCP   |       | 192.168.99.130 | 37110 | 192.168.101.129 | 21    | 1:1000004 | FTP connection=>Attempt |
| 2024-06-11 14:51:43 |        | 0   | TCP   |       | 192.168.99.130 | 37100 | 192.168.101.129 | 21    | 1:1000004 | FTP connection=>Attempt |
| 2024-06-11 14:51:43 |        | 0   | TCP   |       | 192.168.99.130 | 37086 | 192.168.101.129 | 21    | 1:1000004 | FTP connection=>Attempt |
| 2024-06-11 14:51:35 |        | 0   | TCP   |       | 192.168.99.130 | 37086 | 192.168.101.129 | 21    | 1:1000004 | FTP connection=>Attempt |
| 2024-06-11 14:51:35 |        | 0   | TCP   |       | 192.168.99.130 | 37100 | 192.168.101.129 | 21    | 1:1000004 | FTP connection=>Attempt |

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

Available Rule Categories

Category Selection:

custom.rules

Select the rule category to view and manage.

Defined Custom Rules

```
drop tcp any any -> $HOME_NET 21 (msg:"FTP connection=>Attempt"; sid:1000004;)
```

- Snort đã drop được:

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☒ Auto-refresh view
 

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

5 Entries in Active Log

| Date                | Action | Pri | Proto | Class | Source IP      | SPort | Destination IP  | DPort | GID:SID   | Description             |
|---------------------|--------|-----|-------|-------|----------------|-------|-----------------|-------|-----------|-------------------------|
| 2024-06-11 14:59:43 |        | 0   | TCP   |       | 192.168.99.130 | 56066 | 192.168.101.3   | 21    | 1:1000004 | FTP connection=>Attempt |
| 2024-06-11 14:54:14 |        | 0   | TCP   |       | 192.168.99.130 | 54206 | 192.168.101.129 | 21    | 1:1000004 | FTP connection=>Attempt |
| 2024-06-11 14:54:14 |        | 0   | TCP   |       | 192.168.99.130 | 54196 | 192.168.101.129 | 21    | 1:1000004 | FTP connection=>Attempt |

### 4.3. 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:

| Alert Log View Filter                   |        |     |       |       |                |       |                 |       |           |                 |
|---|--------|-----|-------|-------|----------------|-------|-----------------|-------|-----------|-----------------|
| Most Recent 250 Entries from Active Log |        |     |       |       |                |       |                 |       |           |                 |
| Date                                    | Action | Pri | Proto | Class | Source IP      | SPort | Destination IP  | DPort | GID:SID   | Description     |
| 2024-06-11 15:27:13                     |        | 0   | ICMP  |       | 192.168.99.2   |       | 192.168.99.128  |       | 1:1000006 | UDP Tesing Rule |
| 2024-06-11 15:27:13                     |        | 0   | ICMP  |       | 192.168.99.128 |       | 192.168.99.2    |       | 1:1000006 | UDP Tesing Rule |
| 2024-06-11 15:27:12                     |        | 0   | ICMP  |       | 192.168.99.130 |       | 192.168.101.131 |       | 1:1000006 | UDP Tesing Rule |

#### 4.4. 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.

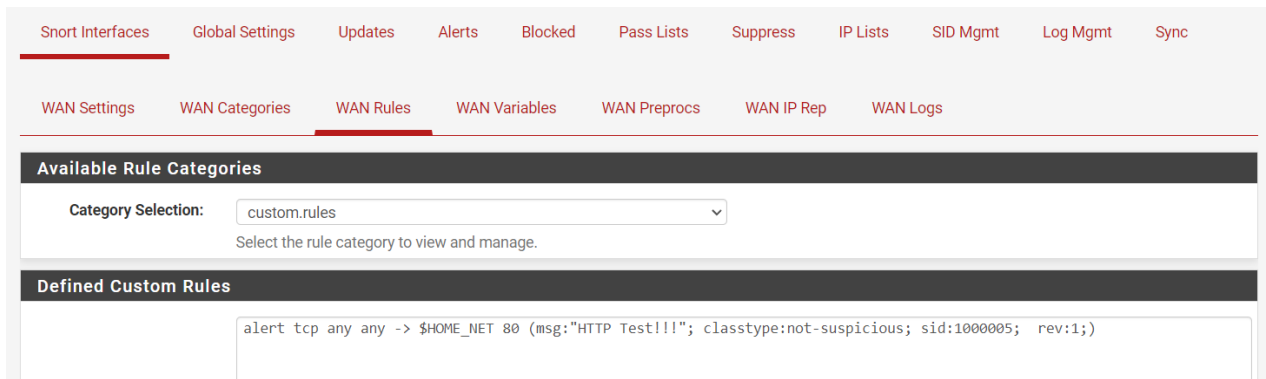
*classtype:not-suspicious*: Phân loại rõ ràng lưu lượng truy cập là không đáng ngờ. Điều này rất quan trọng vì các hệ thống bảo mật thường có phân loại được định nghĩa trước cho các loại lưu lượng truy cập khác nhau (ví dụ: đáng ngờ, bất thường, v.v.).

*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:



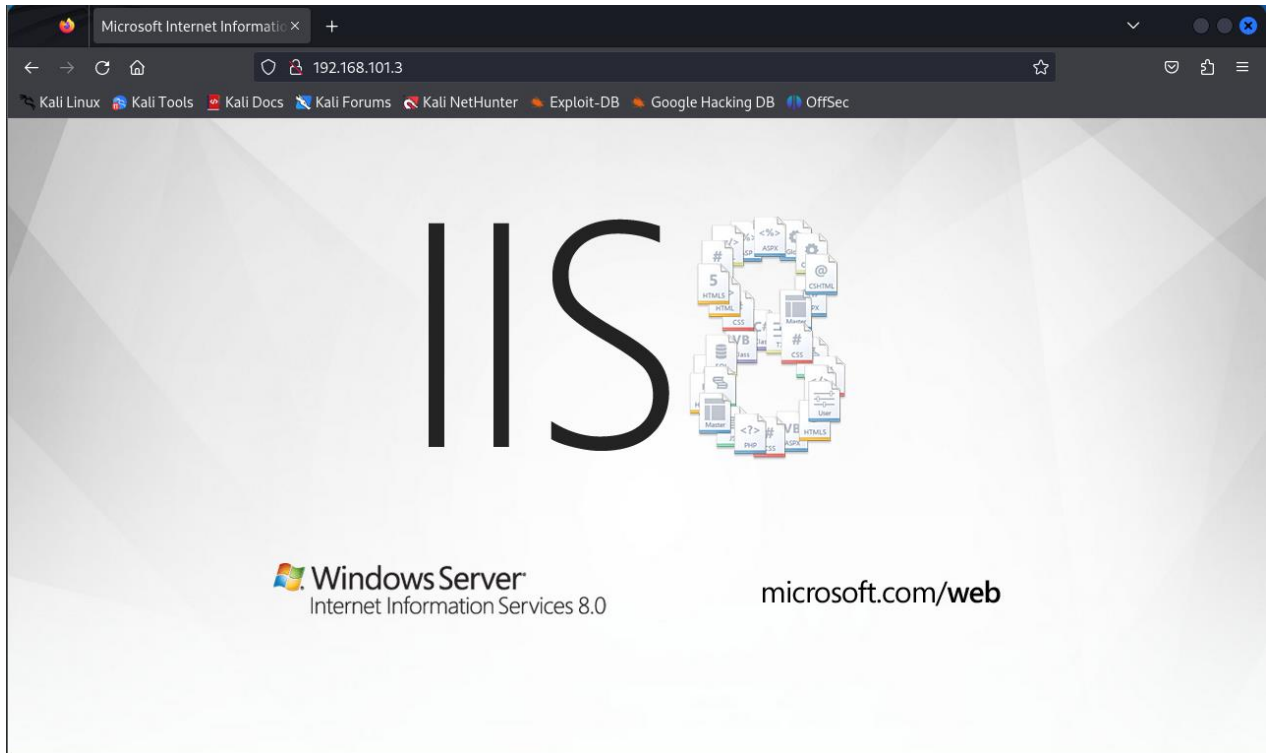


- Qua nmap ta thấy ở máy victim có dịch vụ http:

```
(root@soin)-[/home/soin/Documents]
# nmap 192.168.101.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 18:33 EDT
Nmap scan report for 192.168.101.3
Host is up (0.034s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 8.94 seconds
```

- Vào firefox truy cập vào máy nạn nhân:



- Ta thấy snort đã phát ra cảnh báo:

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☒ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

+

49 Entries in Active Log

| Date                | Action | Pri | Proto | Class                  | Source IP             | SPort | Destination IP       | DPort | GID:SID            | Description  |
|---------------------|--------|-----|-------|------------------------|-----------------------|-------|----------------------|-------|--------------------|--------------|
| 2024-06-11 15:35:38 | ⚠      | 3   | TCP   | Not Suspicious Traffic | 192.168.99.130<br>🔍 + | 52312 | 192.168.101.3<br>🔍 + | 80    | 1:1000005<br>+ ✖ 📝 | HTTP Test!!! |
| 2024-06-11 15:35:38 | ⚠      | 3   | TCP   | Not Suspicious Traffic | 192.168.99.130<br>🔍 + | 52290 | 192.168.101.3<br>🔍 + | 80    | 1:1000005<br>+ ✖ 📝 | HTTP Test!!! |
| 2024-06-11 15:35:38 | ⚠      | 3   | TCP   | Not Suspicious Traffic | 192.168.99.130<br>🔍 + | 52302 | 192.168.101.3<br>🔍 + | 80    | 1:1000005<br>+ ✖ 📝 | HTTP Test!!! |
| 2024-06-11 15:35:28 | ⚠      | 3   | TCP   | Not Suspicious Traffic | 192.168.99.130<br>🔍 + | 52312 | 192.168.101.3<br>🔍 + | 80    | 1:1000005<br>+ ✖ 📝 | HTTP Test!!! |
| 2024-06-11 15:35:28 | ⚠      | 3   | TCP   | Not Suspicious Traffic | 192.168.99.130<br>🔍 + | 52302 | 192.168.101.3<br>🔍 + | 80    | 1:1000005<br>+ ✖ 📝 | HTTP Test!!! |
| 2024-06-11 15:35:28 | ⚠      | 3   | TCP   | Not Suspicious Traffic | 192.168.99.130<br>🔍 + | 52290 | 192.168.101.3<br>🔍 + | 80    | 1:1000005<br>+ ✖ 📝 | HTTP Test!!! |

#### 4.5. 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:

**Available Rule Categories**

Category Selection:  

Select the rule category to view and manage.

**Defined Custom Rules**

```
alert tcp any any -> $HOME_NET any (msg: "TCP Connect Scan"; flags: S; sid: 1;)
alert tcp any any -> $HOME_NET any (msg: "TCP SYN Scan"; flags: S; sid: 2;)
alert tcp any any -> $HOME_NET any (msg: "NULL Scan (Inverse TCP Flag)"; flags: 0; sid: 3;)
alert tcp any any -> $HOME_NET any (msg: "FIN Scan"; flags: F; sid: 4;)
alert tcp any any -> $HOME_NET any (msg: "XMAS Scan"; flags: FPU; sid: 5;)
alert tcp any any -> $HOME_NET any (msg: "TCP ACK Scan"; flags: A; sid: 6;)
alert udp any any -> $HOME_NET any (msg: "UDP Connect Scan"; sid: 7;)
```

- Đầu tiên kiểm tra TCP Connect:

```
(soin@soin)-[~]
$ nmap -sT 192.168.101.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 19:04 EDT
Nmap scan report for 192.168.101.3
Host is up (0.0053s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 9.68 seconds

(soin@soin)-[~]
$
```

- Snort phát hiện:

[Snort Interfaces](#) [Global Settings](#) [Updates](#) [Alerts](#) [Blocked](#) [Pass Lists](#) [Suppress](#) [IP Lists](#) [SID Mgmt](#) [Log Mgmt](#) [Sync](#)

**Alert Log View Settings**  

Interface to Inspect: WAN (em0) ☐ Auto-refresh view 250 Save  
Choose interface.. Alert lines to display.

Alert Log Actions: Download Clear

**Alert Log View Filter** +

**Most Recent 250 Entries from Active Log**

| Date                | Action | Pri | Proto | Class | Source IP      | SPort | Destination IP | DPort | GID:SID | Description      |
|---------------------|--------|-----|-------|-------|----------------|-------|----------------|-------|---------|------------------|
| 2024-06-11 16:04:35 |        | 0   | TCP   |       | 192.168.99.130 | 51170 | 192.168.101.3  | 4848  | 1:1     | TCP Connect Scan |

- SYN Scan:

```
(root@soin)-[/home/soin]
# nmap -sS 192.168.101.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 19:07 EDT
Nmap scan report for 192.168.101.3
Host is up (0.00080s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.95 seconds

(root@soin)-[/home/soin]
#
```

- Snort phát hiện được:

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☒ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

Most Recent 250 Entries from Active Log

| Date                | Action      | Pri | Proto | Class | Source IP                              | SPort | Destination IP                        | DPort | GID:SID                                 | Description      |
|---------------------|-------------|-----|-------|-------|--|-------|---------------------------------------|-------|---|------------------|
| 2024-06-11 16:07:10 | <div></div> | 0   | TCP   |       | 192.168.99.130 <div></div> <div></div> | 59884 | 192.168.101.3 <div></div> <div></div> | 1032  | 1:1 <div></div> <div></div> <div></div> | TCP Connect Scan |
| 2024-06-11 16:07:10 | <div></div> | 0   | TCP   |       | 192.168.99.130 <div></div> <div></div> | 59884 | 192.168.101.3 <div></div> <div></div> | 1032  | 1:2 <div></div> <div></div> <div></div> | TCP SYN Scan     |

- Inverse TCP Flag (NULL Scan)

```
(root@soin)-[/home/soin]
# nmap -sN 192.168.101.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 19:08 EDT
Nmap scan report for 192.168.101.3
Host is up (0.00031s latency).
All 1000 scanned ports on 192.168.101.3 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.21 seconds
```

- Snort phát hiện:



Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

Auto-refresh view

250

Save

Alert lines to display.

Alert Log Actions

Download

Clear

Alert Log View Filter

Most Recent 250 Entries from Active Log

| Date                | Action | Pri | Proto | Class | Source IP      | SPort | Destination IP | DPort | GID:SID | Description                  |
|---------------------|--------|-----|-------|-------|----------------|-------|----------------|-------|---------|------------------------------|
| 2024-06-11 16:09:01 |        | 0   | TCP   |       | 192.168.99.130 | 48832 | 192.168.101.3  | 406   | 1:3     | NULL Scan (Inverse TCP Flag) |
| 2024-06-11 16:09:01 |        | 0   | TCP   |       | 192.168.99.130 | 48832 | 192.168.101.3  | 88    | 1:3     | NULL Scan (Inverse TCP Flag) |
| 2024-06-11 16:09:01 |        | 0   | TCP   |       | 192.168.99.130 | 48832 | 192.168.101.3  | 32772 | 1:3     | NULL Scan (Inverse TCP Flag) |

- FIN Scan:

```
(root@soin)-[/home/soin]
# nmap -sF 192.168.101.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 19:10 EDT
Nmap scan report for 192.168.101.3
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.101.3 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.21 seconds

(root@soin)-[/home/soin]
#
```

- Snort phát hiện:

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

Auto-refresh view

250

Save

Alert lines to display.

Alert Log Actions

Download

Clear

Alert Log View Filter

Most Recent 250 Entries from Active Log













































































| Date                | Action | Pri | Proto | Class | Source IP      | SPort | Destination IP | DPort | GID:SID | Description |
|---------------------|--------|-----|-------|-------|----------------|-------|----------------|-------|---------|-------------|
| 2024-06-11 16:10:26 |        | 0   | TCP   |       | 192.168.99.130 | 44330 | 192.168.101.3  | 1248  | 1:4     | FIN Scan    |
| 2024-06-11 16:10:26 |        | 0   | TCP   |       | 192.168.99.130 | 44330 | 192.168.101.3  | 8300  | 1:4     | FIN Scan    |
| 2024-06-11 16:10:26 |        | 0   | TCP   |       | 192.168.99.130 | 44330 | 192.168.101.3  | 1038  | 1:4     | FIN Scan    |

- XMAS Scan:

```
(root@soin)-[/home/soin]
# nmap -sX 192.168.101.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 19:12 EDT
Nmap scan report for 192.168.101.3
Host is up (0.00048s latency).
All 1000 scanned ports on 192.168.101.3 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.21 seconds
```

- Snort phát hiện:

|                     |   |   |     |   |       |   |       |  |           |
|---------------------|---|---|-----|---|-------|---|-------|--|-----------|
| 2024-06-11 16:12:11 |    | 0 | TCP | 192.168.99.130<br>   | 41543 | 192.168.101.3<br>   | 52673 | 1:5<br>         | XMAS Scan |
| 2024-06-11 16:12:11 |    | 0 | TCP | 192.168.99.130<br>   | 41543 | 192.168.101.3<br>   | 8333  | 1:5<br>         | XMAS Scan |
| 2024-06-11 16:12:11 |    | 0 | TCP | 192.168.99.130<br>   | 41543 | 192.168.101.3<br>   | 1259  | 1:5<br>         | XMAS Scan |
| 2024-06-11 16:12:11 |    | 0 | TCP | 192.168.99.130<br>   | 41543 | 192.168.101.3<br>   | 1066  | 1:5<br>         | XMAS Scan |
| 2024-06-11 16:12:11 |    | 0 | TCP | 192.168.99.130<br>   | 41543 | 192.168.101.3<br>   | 2522  | 1:5<br>         | XMAS Scan |
| 2024-06-11 16:12:11 |    | 0 | TCP | 192.168.99.130<br>   | 41543 | 192.168.101.3<br>   | 5544  | 1:5<br>         | XMAS Scan |
| 2024-06-11 16:12:11 |    | 0 | TCP | 192.168.99.130<br>   | 41543 | 192.168.101.3<br>   | 8007  | 1:5<br>         | XMAS Scan |
| 2024-06-11 16:12:11 |    | 0 | TCP | 192.168.99.130<br>   | 41543 | 192.168.101.3<br>   | 6669  | 1:5<br>         | XMAS Scan |
| 2024-06-11 16:12:11 |  | 0 | TCP | 192.168.99.130<br> | 41543 | 192.168.101.3<br> | 2135  | 1:5<br>   | XMAS Scan |
| 2024-06-11 16:12:11 |  | 0 | TCP | 192.168.99.130<br> | 41543 | 192.168.101.3<br> | 12265 | 1:5<br>   | XMAS Scan |
| 2024-06-11 16:12:11 |  | 0 | TCP | 192.168.99.130<br> | 41543 | 192.168.101.3<br> | 5100  | 1:5<br>   | XMAS Scan |
| 2024-06-11 16:12:11 |  | 0 | TCP | 192.168.99.130<br> | 41543 | 192.168.101.3<br> | 3367  | 1:5<br>   | XMAS Scan |
| 2024-06-11 16:12:11 |  | 0 | TCP | 192.168.99.130<br> | 41543 | 192.168.101.3<br> | 9001  | 1:5<br>   | XMAS Scan |

- TCP ACK Scan:

```
(root@soin)-[/home/soin]
# nmap -sA 192.168.101.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 19:17 EDT
Nmap scan report for 192.168.101.3
Host is up (0.000049s latency).
All 1000 scanned ports on 192.168.101.3 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

- Snort phát hiện:

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☒ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

Most Recent 250 Entries from Active Log

| Date                | Action | Pri | Proto | Class | Source IP      | SPort | Destination IP | DPort | GID:SID | Description  |
|---------------------|--------|-----|-------|-------|----------------|-------|----------------|-------|---------|--------------|
| 2024-06-11 16:17:06 |        | 0   | TCP   |       | 192.168.99.130 | 43017 | 192.168.101.3  | 5962  | 1:6     | TCP ACK Scan |
| 2024-06-11 16:17:06 |        | 0   | TCP   |       | 192.168.99.130 | 43017 | 192.168.101.3  | 49163 | 1:6     | TCP ACK Scan |
| 2024-06-11 16:17:06 |        | 0   | TCP   |       | 192.168.99.130 | 43017 | 192.168.101.3  | 444   | 1:6     | TCP ACK Scan |
| 2024-06-11 16:17:06 |        | 0   | TCP   |       | 192.168.99.130 | 43017 | 192.168.101.3  | 16992 | 1:6     | TCP ACK Scan |
| 2024-06-11 16:17:06 |        | 0   | TCP   |       | 192.168.99.130 | 43017 | 192.168.101.3  | 8042  | 1:6     | TCP ACK Scan |
| 2024-06-11 16:17:06 |        | 0   | TCP   |       | 192.168.99.130 | 43017 | 192.168.101.3  | 3168  | 1:6     | TCP ACK Scan |

- UDP Connect Scan:

```
(root@soin)-[/home/soin]
# nmap -sU 192.168.101.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 19:18 EDT
```

- Snort phát hiện:

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☒ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

Most Recent 250 Entries from Active Log

| Date                | Action | Pri | Proto | Class | Source IP       | SPort | Destination IP | DPort | GID:SID | Description      |
|---------------------|--------|-----|-------|-------|-----------------|-------|----------------|-------|---------|------------------|
| 2024-06-11 16:17:20 |        | 0   | UDP   |       | 50.116.32.247   | 53    | 192.168.99.128 | 63685 | 1:7     | UDP Connect Scan |
| 2024-06-11 16:17:20 |        | 0   | UDP   |       | 185.120.22.23   | 53    | 192.168.99.128 | 41373 | 1:7     | UDP Connect Scan |
| 2024-06-11 16:17:19 |        | 0   | UDP   |       | 104.248.145.172 | 53    | 192.168.99.128 | 40956 | 1:7     | UDP Connect Scan |
| 2024-06-11 16:17:19 |        | 0   | UDP   |       | 45.11.105.142   | 53    | 192.168.99.128 | 61613 | 1:7     | UDP Connect Scan |

- Tiến hành drop các kỹ thuật quét:

Custom rules validated successfully and any active Snort process on this interface has been signaled to live-load the new rules.


[Snort Interfaces](#)
[Global Settings](#)
[Updates](#)
[Alerts](#)
[Blocked](#)
[Pass Lists](#)
[Suppress](#)
[IP Lists](#)
[SID Mgmt](#)
[Log Mgmt](#)
[Sync](#)
[WAN Settings](#)
[WAN Categories](#)
[WAN Rules](#)
[WAN Variables](#)
[WAN Preprocs](#)
[WAN IP Rep](#)
[WAN Logs](#)

## Available Rule Categories

Category Selection:

custom.rules

Select the rule category to view and manage.

## Defined Custom Rules

```
drop tcp any any -> $HOME_NET any (msg: "TCP Connect Scan"; flags: S; sid: 1;)
drop tcp any any -> $HOME_NET any (msg: "TCP SYN Scan"; flags: S; sid: 2;)
drop tcp any any -> $HOME_NET any (msg: "NULL Scan (Inverse TCP Flag)"; flags: 0; sid: 3;)
drop tcp any any -> $HOME_NET any (msg: "FIN Scan"; flags: F; sid: 4;)
drop tcp any any -> $HOME_NET any (msg: "XMAS Scan"; flags: FPU; sid: 5;)
drop tcp any any -> $HOME_NET any (msg: "TCP ACK Scan"; flags: A; sid: 6;)
drop udp any any -> $HOME_NET any (msg: "UDP Connect Scan"; sid: 7;)
```

- Snort drop:

|                     |  |   |     |                |       |                |       |     |                  |
|---------------------|--|---|-----|----------------|-------|----------------|-------|-----|------------------|
| 16:26:02            |  |   |     | Q +            |       | Q +            |       | + X |                  |
| 2024-06-11 16:26:02 |  | 0 | UDP | 139.178.66.41  | 53    | 192.168.99.128 | 52749 | 1:7 | UDP Connect Scan |
| 2024-06-11 16:26:02 |  | 0 | UDP | 45.127.113.23  | 53    | 192.168.99.128 | 15662 | 1:7 | UDP Connect Scan |
| 2024-06-11 16:26:02 |  | 0 | TCP | 192.168.99.130 | 35856 | 192.168.101.3  | 5560  | 1:1 | TCP Connect Scan |
| 2024-06-11 16:26:02 |  | 0 | TCP | 192.168.99.130 | 35856 | 192.168.101.3  | 5560  | 1:2 | TCP SYN Scan     |
| 2024-06-11 16:26:02 |  | 0 | UDP | 103.127.121.22 | 53    | 192.168.99.128 | 58306 | 1:7 | UDP Connect Scan |
| 2024-06-11 16:26:02 |  | 0 | UDP | 103.127.121.22 | 53    | 192.168.99.128 | 61056 | 1:7 | UDP Connect Scan |
| 2024-06-11 16:26:02 |  | 0 | TCP | 192.168.99.130 | 52742 | 192.168.101.3  | 3052  | 1:1 | TCP Connect Scan |
| 2024-06-11 16:26:02 |  | 0 | TCP | 192.168.99.130 | 52742 | 192.168.101.3  | 3052  | 1:2 | TCP SYN Scan     |
| 2024-06-11 16:26:02 |  | 0 | TCP | 192.168.99.130 | 52732 | 192.168.101.3  | 3052  | 1:1 | TCP Connect Scan |
| 2024-06-11 16:26:02 |  | 0 | TCP | 192.168.99.130 | 52732 | 192.168.101.3  | 3052  | 1:2 | TCP SYN Scan     |
| 2024-06-11 16:26:02 |  | 0 | TCP | 192.168.99.130 | 43820 | 192.168.101.3  | 1055  | 1:1 | TCP Connect Scan |
| 2024-06-11 16:26:02 |  | 0 | TCP | 192.168.99.130 | 43820 | 192.168.101.3  | 1055  | 1:2 | TCP SYN Scan     |
| 2024-06-11 16:26:02 |  | 0 | TCP | 192.168.99.130 | 43812 | 192.168.101.3  | 1055  | 1:1 | TCP Connect Scan |

| Alert Log View Filter <span>+</span>    |        |     |       |       |                    |       |                   |       |         |                              |
|---|--------|-----|-------|-------|--------------------|-------|-------------------|-------|---------|------------------------------|
| Most Recent 250 Entries from Active Log |        |     |       |       |                    |       |                   |       |         |                              |
| Date                                    | Action | Pri | Proto | Class | Source IP          | SPort | Destination IP    | DPort | GID:SID | Description                  |
| 2024-06-11 16:26:48                     |        | 0   | TCP   |       | 192.168.99.130<br> | 48140 | 192.168.101.3<br> | 617   | 1:3<br> | NULL Scan (Inverse TCP Flag) |
| 2024-06-11 16:26:48                     |        | 0   | TCP   |       | 192.168.99.130<br> | 48140 | 192.168.101.3<br> | 668   | 1:3<br> | NULL Scan (Inverse TCP Flag) |
| 2024-06-11 16:26:48                     |        | 0   | TCP   |       | 192.168.99.130<br> | 48140 | 192.168.101.3<br> | 32781 | 1:3<br> | NULL Scan (Inverse TCP Flag) |
| 2024-06-11 16:26:48                     |        | 0   | TCP   |       | 192.168.99.130<br> | 48140 | 192.168.101.3<br> | 3869  | 1:3<br> | NULL Scan (Inverse TCP Flag) |
| 2024-06-11 16:26:48                     |        | 0   | TCP   |       | 192.168.99.130<br> | 48140 | 192.168.101.3<br> | 34572 | 1:3<br> | NULL Scan (Inverse TCP Flag) |
| 2024-06-11 16:26:48                     |        | 0   | TCP   |       | 192.168.99.130<br> | 48140 | 192.168.101.3<br> | 500   | 1:3<br> | NULL Scan (Inverse TCP Flag) |
| 2024-06-11 16:26:48                     |        | 0   | TCP   |       | 192.168.99.130<br> | 48140 | 192.168.101.3<br> | 9898  | 1:3<br> | NULL Scan (Inverse TCP Flag) |
| 2024-06-11 16:26:48                     |        | 0   | TCP   |       | 192.168.99.130<br> | 48140 | 192.168.101.3<br> | 6004  | 1:3<br> | NULL Scan (Inverse TCP Flag) |

#### 4.6. *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.

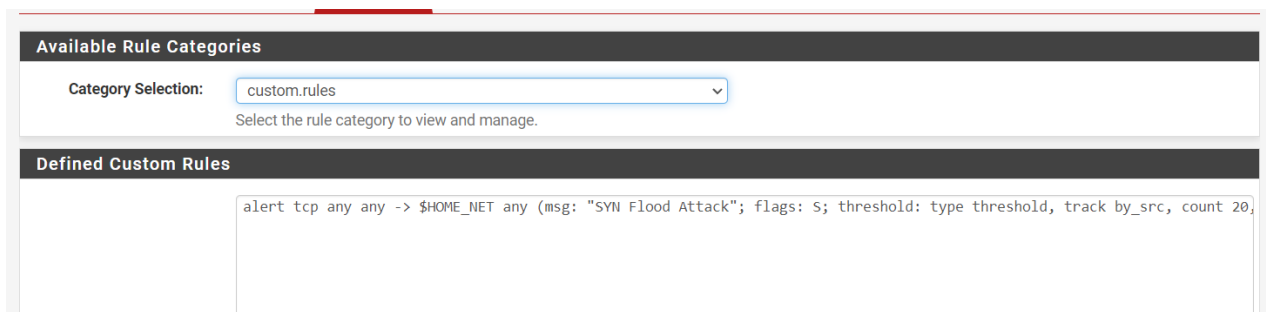
*track by\_src*: Theo dõi theo nguồn - Theo dõi số lần kích hoạt của rule theo từng địa chỉ IP nguồn.

*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.

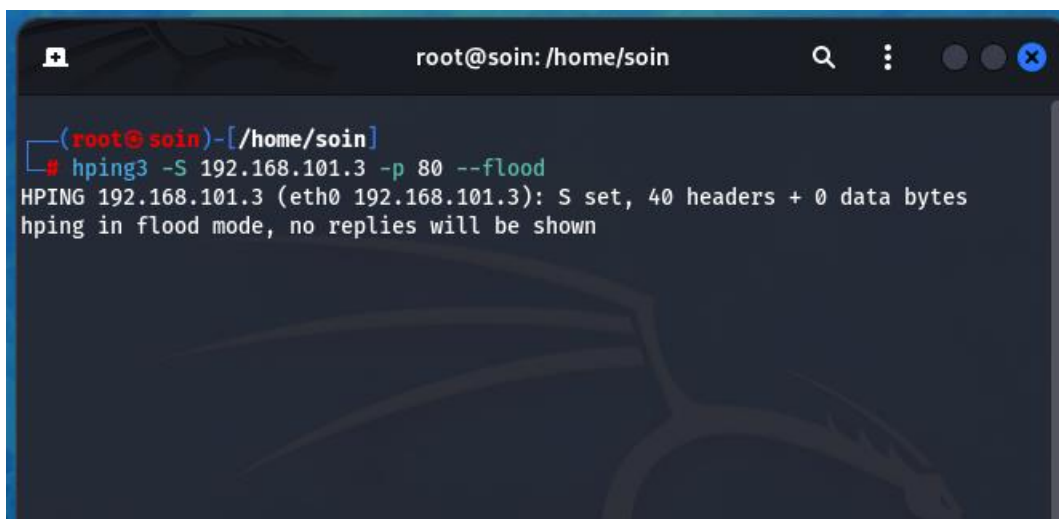
*seconds 3*: Khoảng thời gian - Quy định khoảng thời gian để theo dõi số lượng kích hoạt (3 giây trong trường hợp này).

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

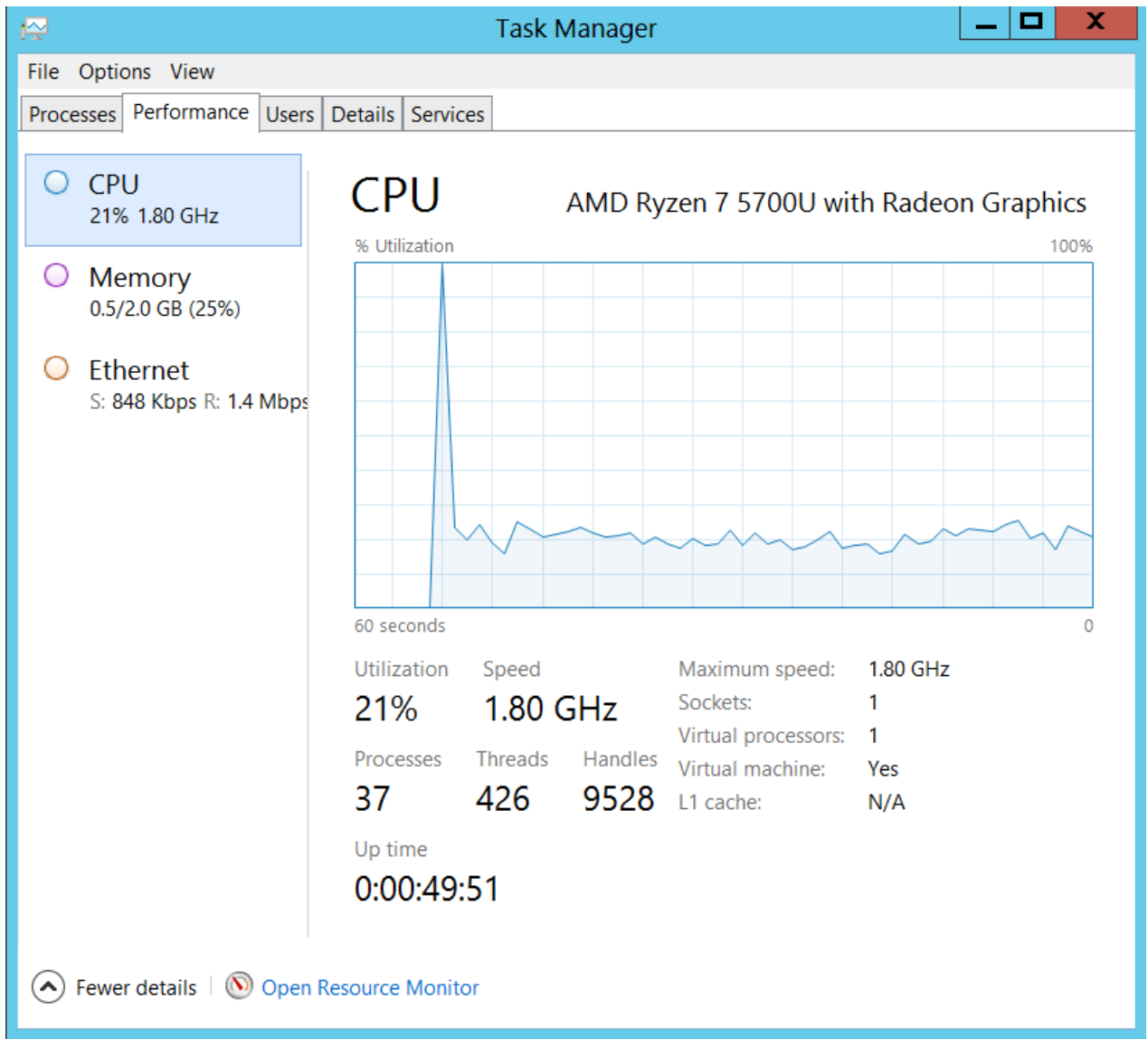
*rev:1*: Số phiên bản của rule.



- 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:

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☒ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

Most Recent 250 Entries from Active Log

| Date                | Action | Pri | Proto | Class | Source IP          | SPort | Destination IP    | DPort | GID:SID | Description      |
|---------------------|--------|-----|-------|-------|--------------------|-------|-------------------|-------|---------|------------------|
| 2024-06-11 16:42:08 |        | 0   | TCP   |       | 192.168.99.130<br> | 6940  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |
| 2024-06-11 16:42:08 |        | 0   | TCP   |       | 192.168.99.130<br> | 6920  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |
| 2024-06-11 16:42:08 |        | 0   | TCP   |       | 192.168.99.130<br> | 6900  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |
| 2024-06-11 16:42:08 |        | 0   | TCP   |       | 192.168.99.130<br> | 6880  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |
| 2024-06-11 16:42:08 |        | 0   | TCP   |       | 192.168.99.130<br> | 6860  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |
| 2024-06-11 16:42:08 |        | 0   | TCP   |       | 192.168.99.130<br> | 6840  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |
| 2024-06-11 16:42:08 |        | 0   | TCP   |       | 192.168.99.130<br> | 6820  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |
| 2024-06-11 16:42:08 |        | 0   | TCP   |       | 192.168.99.130<br> | 6800  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |

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

Available Rule Categories

Category Selection:

custom.rules

Select the rule category to view and manage.

Defined Custom Rules

drop tcp any any -> \$HOME\_NET any (msg: "SYN Flood Attack"; flags: S; threshold: type threshold, track by\_src, count 20,

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



Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☒ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

+

Most Recent 250 Entries from Active Log

| Date                | Action | Pri | Proto | Class | Source IP          | SPort | Destination IP    | DPort | GID:SID | Description      |
|---------------------|--------|-----|-------|-------|--------------------|-------|-------------------|-------|---------|------------------|
| 2024-06-11 16:46:25 |        | 0   | TCP   |       | 192.168.99.130<br> | 1786  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |
| 2024-06-11 16:46:25 |        | 0   | TCP   |       | 192.168.99.130<br> | 1764  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |
| 2024-06-11 16:46:25 |        | 0   | TCP   |       | 192.168.99.130<br> | 1744  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |
| 2024-06-11 16:46:25 |        | 0   | TCP   |       | 192.168.99.130<br> | 1726  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |
| 2024-06-11 16:46:25 |        | 0   | TCP   |       | 192.168.99.130<br> | 1706  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |
| 2024-06-11 16:46:25 |        | 0   | TCP   |       | 192.168.99.130<br> | 1686  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |
| 2024-06-11 16:46:25 |        | 0   | TCP   |       | 192.168.99.130<br> | 1666  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |
| 2024-06-11 16:46:25 |        | 0   | TCP   |       | 192.168.99.130<br> | 1646  | 192.168.101.3<br> | 80    | 1:1<br> | SYN Flood Attack |

#### 4.7. Các kỹ thuật khác

- Khai thác lỗ hồng 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:"/8000a80000000000000000000000000000000000000000000000000ffff000000000000ffff00000
0000000000000000000000000000000000000000000000000000000f1dfff00000000000000000020f0dfff00
f1dfffffffffff6000041000000000080efdfff");
                                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:"/8000a800000000000000000000000000000000ffff000000000000ffff00000000  
00000000000000000000000000000000000000f1dfff000000000000000020f0dfff00f1dffffff  
ffff600004100000000080efdfff"/*: 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 lỗi hỏng.

*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).

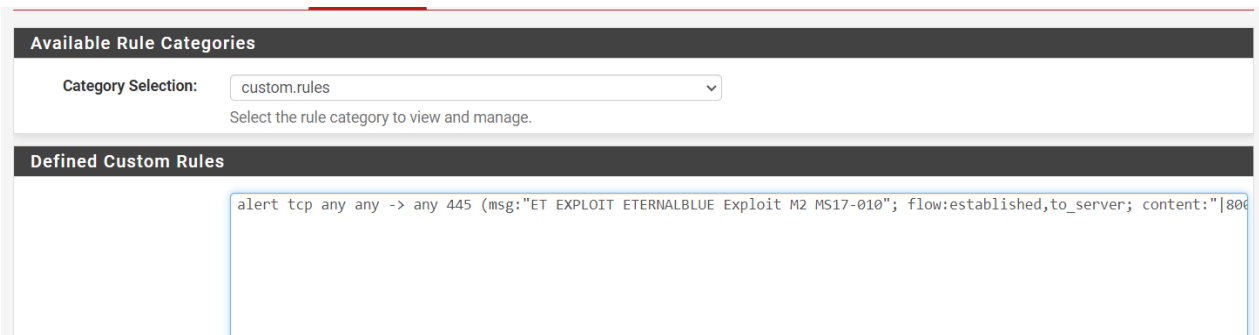
*former\_category*: Thê loại cũ của rule (CURRENT\_EVENTS).

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

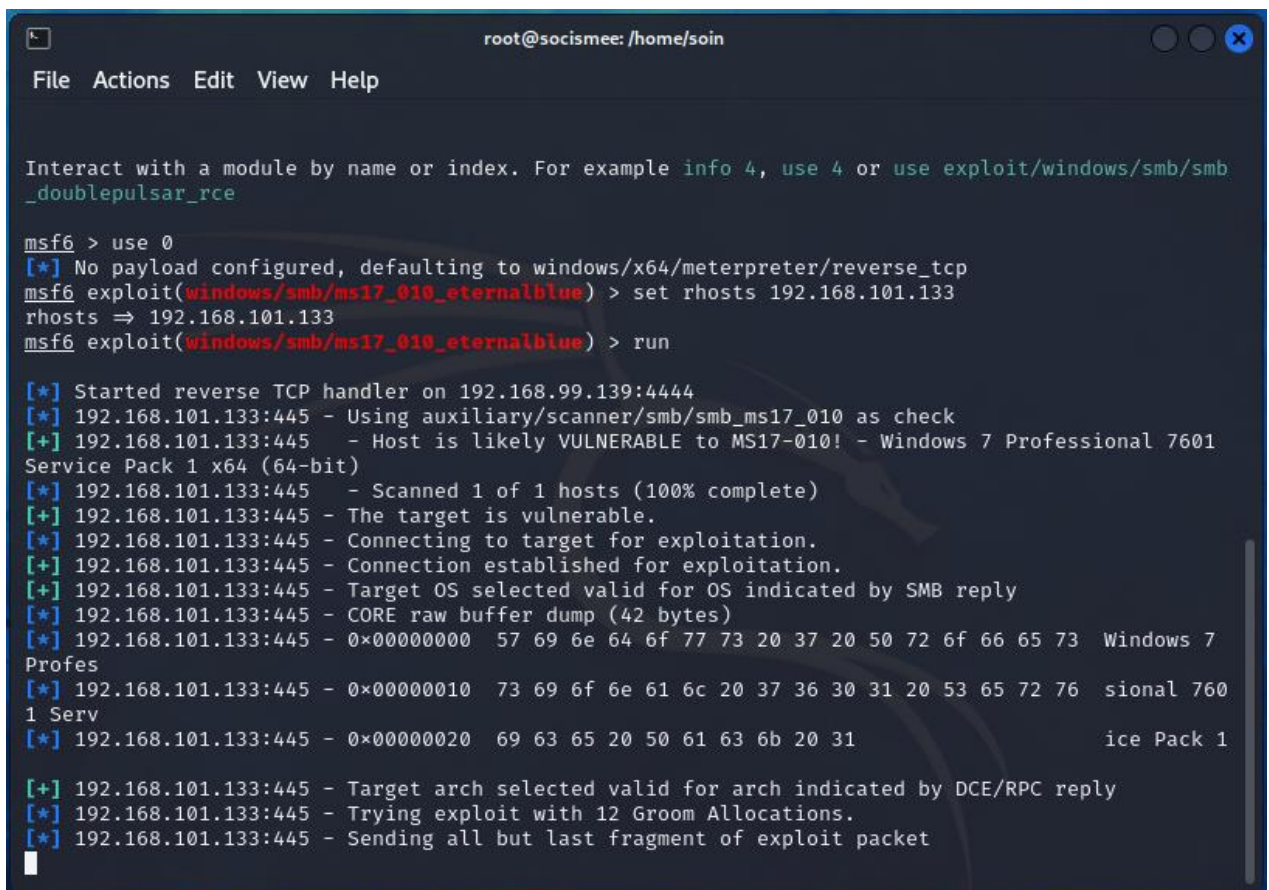
*signature\_severity*: Mức độ nghiêm trọng của lỗ hổng (cao - Major).

*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 chứa lỗ hổng ms17-010:



- Snort phát ra cảnh báo:

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☒ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

+

4 Entries in Active Log

| Date                | Action | Pri | Proto | Class                                  | Source IP      | SPort | Destination IP  | DPort | GID:SID | Description                                |
|---------------------|--------|-----|-------|--|----------------|-------|-----------------|-------|---------|--|
| 2024-06-12 01:07:10 |        | 1   | TCP   | Attempted Administrator Privilege Gain | 192.168.99.139 | 45287 | 192.168.101.134 | 445   | 1:1     | ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010 |
| 2024-06-12 01:07:10 |        | 1   | TCP   | Attempted Administrator Privilege Gain | 192.168.99.139 | 45287 | 192.168.101.134 | 445   | 1:1     | ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010 |
| 2024-06-12 01:06:23 |        | 1   | TCP   | Attempted Administrator Privilege Gain | 192.168.99.139 | 45653 | 192.168.101.134 | 445   | 1:1     | ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010 |
| 2024-06-12 01:06:23 |        | 1   | TCP   | Attempted Administrator Privilege Gain | 192.168.99.139 | 45653 | 192.168.101.134 | 445   | 1:1     | ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010 |

- Ta tiến hành ngăn chặn cuộc tấn công này:

Available Rule Categories

Category Selection:

custom.rules

Select the rule category to view and manage.

Defined Custom Rules

```
drop tcp any any -> any 445 (msg:"ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010"; flow:established,to_server; content:"|8006|")
```

- Cuộc tấn công đã bị ngăn chặn:

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☒ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

+

2 Entries in Active Log

| Date                | Action | Pri | Proto | Class                                  | Source IP      | SPort | Destination IP  | DPort | GID:SID | Description                                |
|---------------------|--------|-----|-------|--|----------------|-------|-----------------|-------|---------|--|
| 2024-06-12 01:11:12 |        | 1   | TCP   | Attempted Administrator Privilege Gain | 192.168.99.139 | 38875 | 192.168.101.134 | 445   | 1:1     | ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010 |
| 2024-06-12 01:11:12 |        | 1   | TCP   | Attempted Administrator Privilege Gain | 192.168.99.139 | 38875 | 192.168.101.134 | 445   | 1:1     | ET EXPLOIT ETERNALBLUE Exploit M2 MS17-010 |