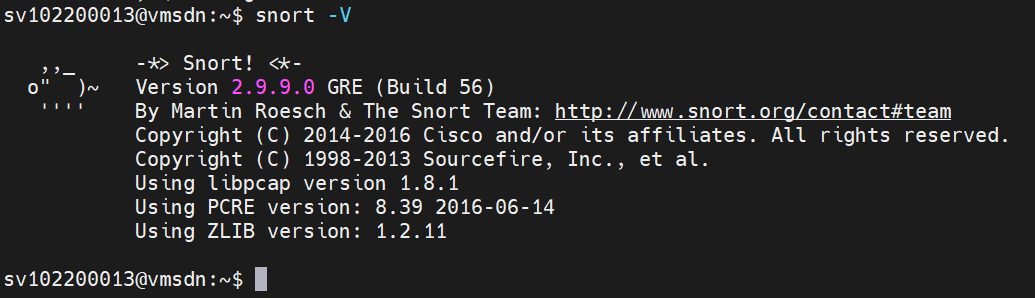
Đảm bảo Snort đã được cài đặt bằng lệnh sau:

Để kiểm tra thông tin các giao diện mạng, sử dụng lệnh:A screenshot of a computer screen

Description automatically generated

Chạy Snort để hiển thị các tiêu đề lớp 2:

A screenshot of a computer

Description automatically generated

**Mục tiêu:**

Thiết lập mạng SDN với 5 host, trong đó h5 sẽ dùng Snort để bắt và phân tích lưu lượng từ h4. Các host h1, h2, và h3 sẽ thực hiện tấn công DoS vào h4, và h5 sẽ phát hiện cuộc tấn công thông qua luật Snort.

**1. Cấu hình mạng**

Thiết lập mạng với 5 host kết nối tới một switch, switch này kết nối với bộ điều khiển SDN Floodlight:

bash

Sao chép mã

$ sudo mn --topo single5 --controller=remote,ip=127.0.0.1,port=6653

Lệnh này sẽ khởi động một mạng với 5 host kết nối tới một switch, và switch này kết nối với bộ điều khiển từ xa tại địa chỉ IP 127.0.0.1 và cổng 6653.

**2. Cài đặt và kiểm tra Snort**

Đảm bảo Snort được cài đặt và hoạt động:

bash

Sao chép mã

$ snort -V

Kiểm tra phiên bản Snort.

**3. Cấu hình Snort để bắt gói tin**

Snort có thể chạy với các chế độ khác nhau để bắt gói tin và ghi lại lưu lượng:

* Để chạy Snort và hiển thị các gói tin tầng 2:

bash

Sao chép mã

$ sudo snort -vd

* Để chạy với cấu hình snort.conf và lưu log:

bash

Sao chép mã

$ sudo snort -v -c /etc/snort/snort.conf

Tạo thư mục log và chạy Snort để ghi log:

bash

Sao chép mã

$ mkdir log

$ sudo snort -d -c /etc/snort/snort.conf -l ./log

**4. Cấu hình Snort phát hiện tấn công DoS**

Thêm một luật vào file mylocal.rules để phát hiện tấn công DoS qua ICMP:

bash

Sao chép mã

alert icmp any any -> any any (threshold: type both, track by\_dst, count 70, seconds 10; msg: "DoS by ICMP detected"; sid:1001;)

Lệnh này sẽ phát hiện khi có hơn 70 gói tin ICMP trong vòng 10 giây.

**5. Bắt lưu lượng từ h4 bằng h5**

Cấu hình Snort để h5 bắt lưu lượng từ h4:

bash

Sao chép mã

mininet> s1 ovs-vsctl -- set Bridge "s1" mirrors=@m -- --id=@s1-eth4 get Port s1-eth4 -- --id=@s1-eth5 get Port s1-eth5 -- --id=@m create Mirror name=e4toe5 select-dst-port=@s1-eth4 output-port=@s1-eth5

Lệnh này sẽ mirror lưu lượng của h4 sang h5. Sau đó, mở terminal cho h5 và chạy Snort:

bash

Sao chép mã

mininet> xterm h5

h5> snort -i eth0 -v -c $HOME/snort/snort.conf &

**6. Thực hiện tấn công DoS**

Dùng h1 để thực hiện tấn công ping flood vào h4:

bash

Sao chép mã

mininet> h1 ping -f h4

Kết quả của cuộc tấn công sẽ được ghi nhận trong file log của Snort tại /var/log/snort/alert với thông điệp "DoS by ICMP detected".

**7. Kiểm tra kết quả**

Mở file log của Snort để kiểm tra kết quả phát hiện tấn công:

bash

Sao chép mã

$ sudo cat ./log/snort.log.<timestamp>