Báo cáo bài thực hành số 6

Môn học

Thực tập cơ sở

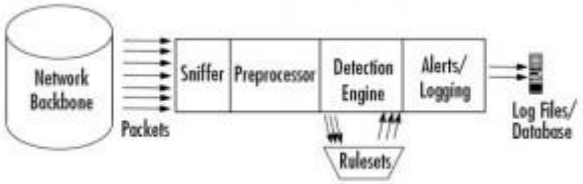
Giảng viên : Hoàng Xuân Dậu

Họ tên : Nguyễn Minh Phương

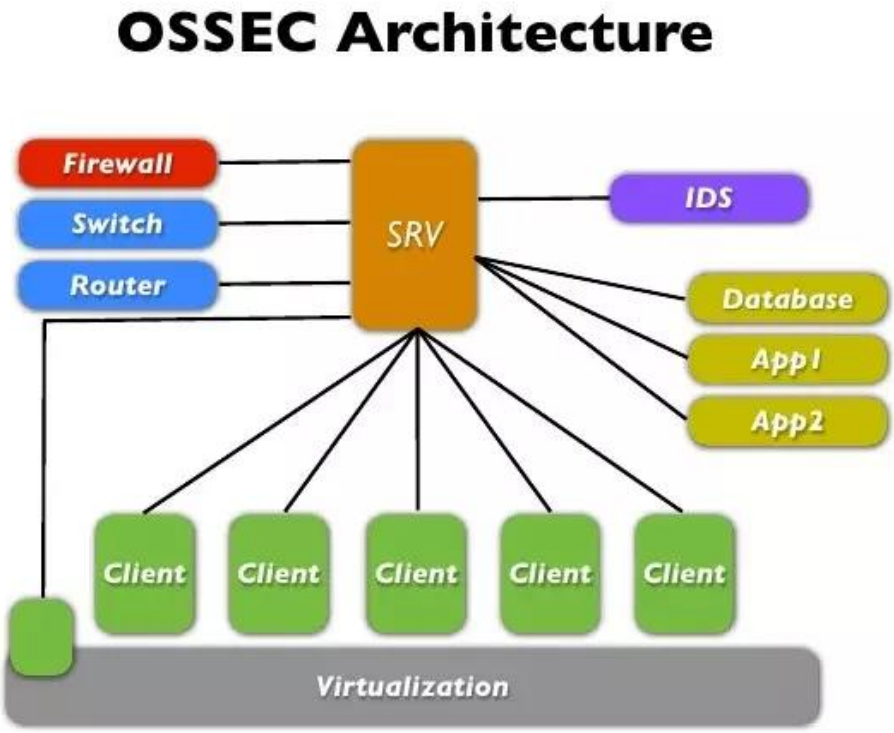
Mã SV: B19DCAT141

I. Lý thuyết :

- Tìm hiểu khái quát về các hệ thống phát hiện tấn công, xâm nhập, phân loại các hệ thống phát hiện xâm nhập, các kỹ thuật phát hiện xâm nhập.
    - Hệ thống phát hiện tấn công, xâm nhập
        - Hệ thống phát hiện xâm nhập (Intrusion Detection System – IDS) là hệ thống phần cứng hoặc phần mềm có chức năng giám sát lưu thông mạng, tự động theo dõi các sự kiện xảy ra trên hệ thống máy tính, phân tích để phát hiện ra các vấn đề liên quan đến an ninh, bảo mật và đưa ra cảnh báo cho nhà quản trị.
        - Các hệ thống phát hiện tấn công, xâm nhập (IDS) thường được sử dụng như một lớp phòng vệ quan trọng trong các lớp giải pháp đảm bảo an toàn cho hệ thống thông tin và mạng.
    - Phân loại IDS (hệ thống phát hiện xâm nhập)
        - **NIDS**: hệ thống phát hiện xâm nhập mạng. Hệ thống sẽ tập hợp gói tin để phân tích sâu bên trong mà không làm thay đổi cấu trúc gói tin. NIDS có thể là phần mềm triển khai trên server hoặc dạng thiết bị tích hợp appliance.
        - **HIDS**: hệ thống phát hiện xâm nhập host. Theo dõi các hoạt động bất thường trên các host riêng biệt. HIDS được cài đặt trực tiếp trên các máy (host) cần theo dõi.
    - Kỹ thuật phát hiện xâm nhập
        - Phát hiện xâm nhập dựa trên chữ ký: Giám sát sát các hành vi của hệ thống, và cảnh báo nếu phát hiện chữ ký của tấn công, xâm nhập.
        - Phát hiện xâm nhập dựa trên bất thường: Giám sát hành vi hiện tại của hệ thống và cảnh báo nếu có khác biệt rõ nét giữa hành vi hiện tại và hồ sơ của đối tượng.
- Tìm hiểu về kiến trúc và tính năng của một số hệ thống phát hiện tấn công, xâm nhập, như Snort, Suricata, Zeek, OSSEC, Wazuh...
    - Snort
        - Kiến trúc: Snort bao gồm nhiều thành phần, mỗi phần có một chức năng riêng biệt.
            - Module giải mã gói tin (packet decoder)
            - Module tiền xử lý (preprocessors)
            - Module phát hiện (detection engine)
            - Module log và cảnh báo(logging and alerting system)
            - Module kết xuất thông tin (output module)
        - Kiến trúc của Snort được thể hiện qua mô hình sau:



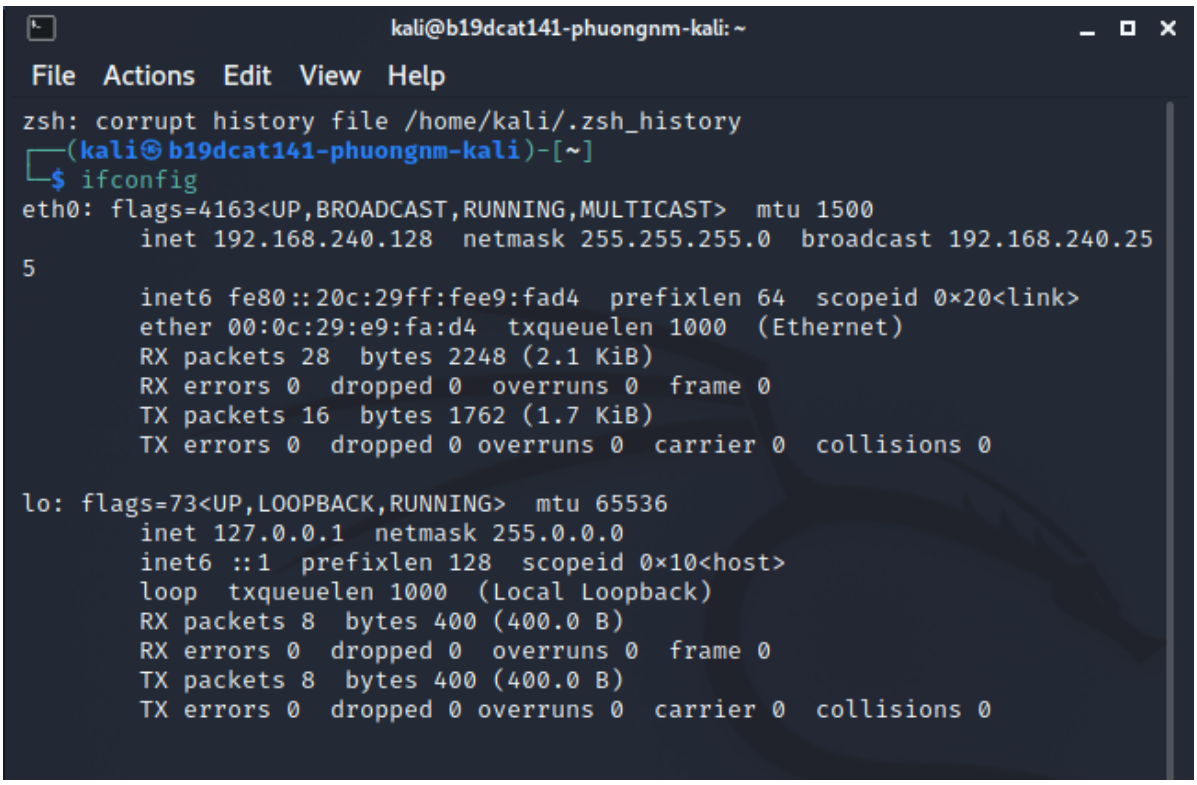
- OSSEC
  - Kiến trúc OSSEC được thiết kế theo mô hình client – server, gồm 2 thành phần chính là OSSEC server và OSSEC agent.

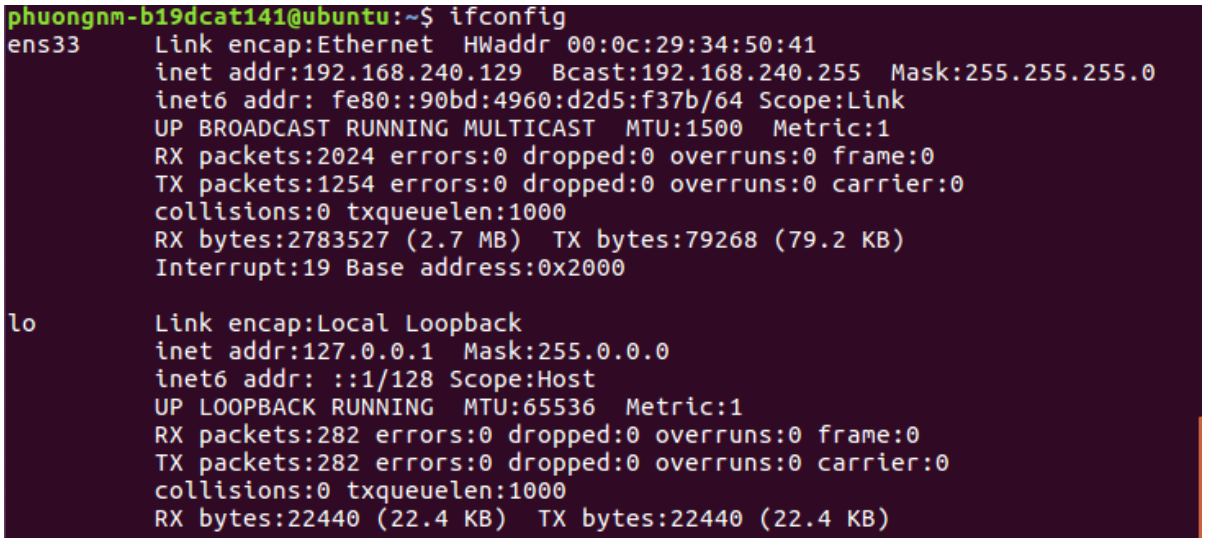


  - Tính năng
    - Theo dõi và phân tích các log
    - Kiểm tra tính toàn vẹn của file
    - Giám sát Registry
    - Phát hiện Rootkit
    - Phản ứng chủ động

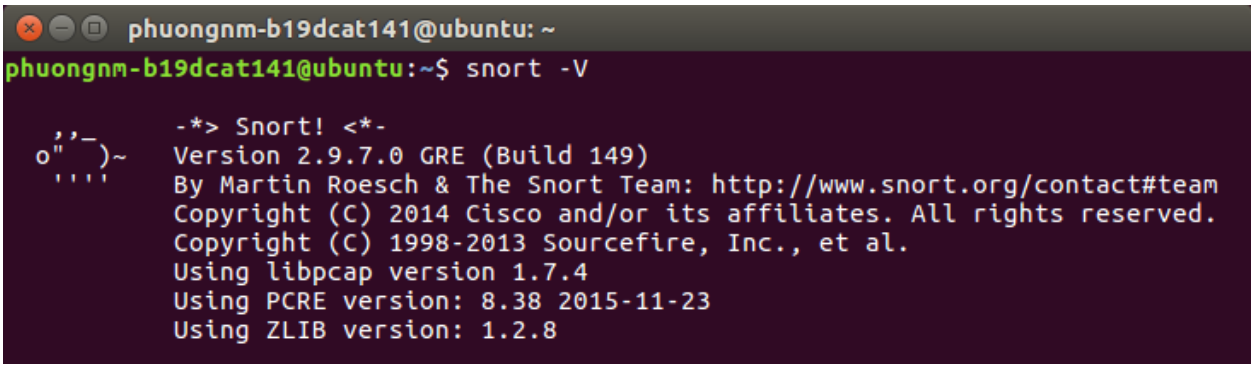
II. Thực hành :

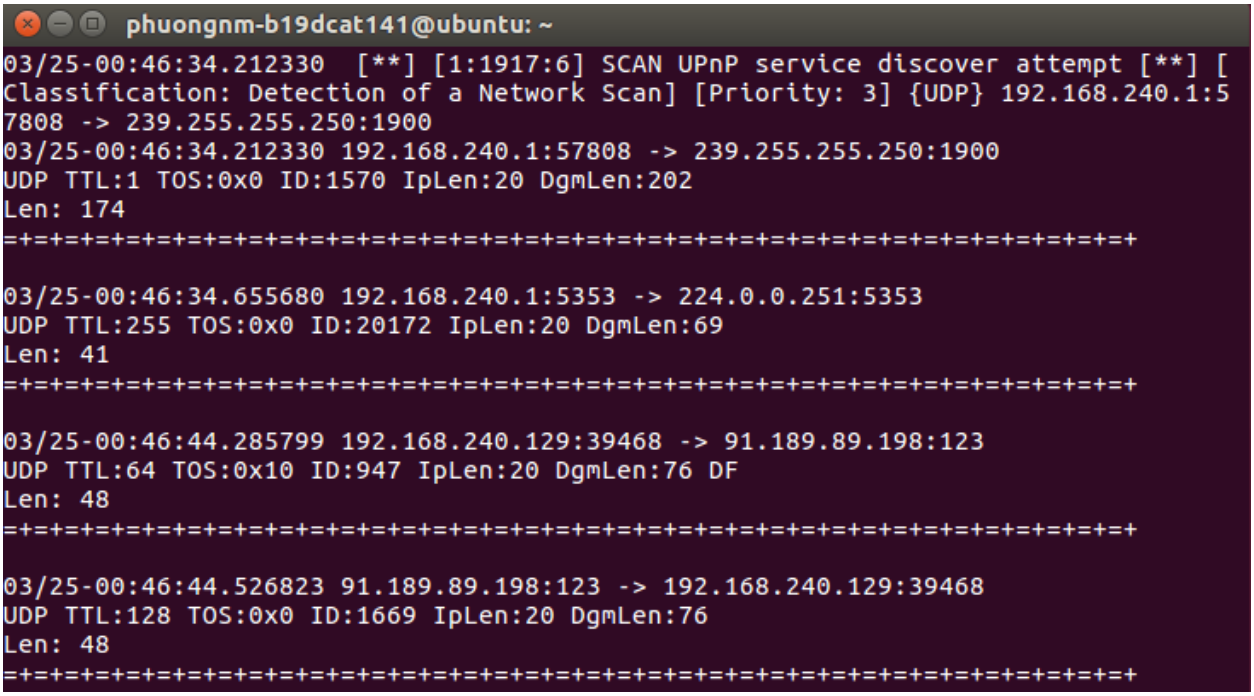
- Chuẩn bị các máy tính như mô tả trong mục 2.2. Máy Kali Linux được đổi tên thành <Mã SV-Tên SV>-Kali và máy cài Snort thành <Mã SV-Tên SV>-Snort. Các máy có địa chỉ IP và kết nối mạng LAN



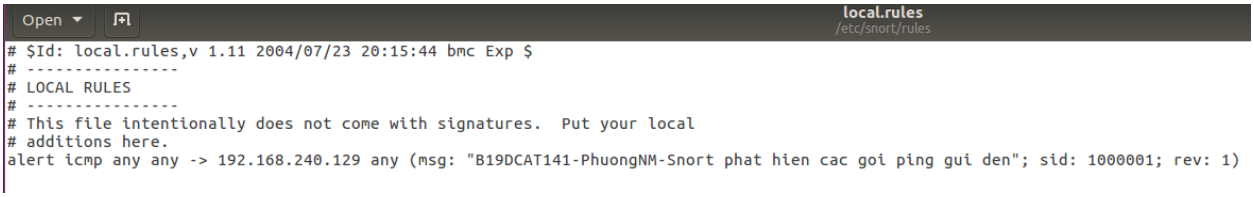


- Tải, cài đặt Snort và chạy thử Snort. Kiểm tra log của Snort để đảm bảo Snort hoạt động bình thường

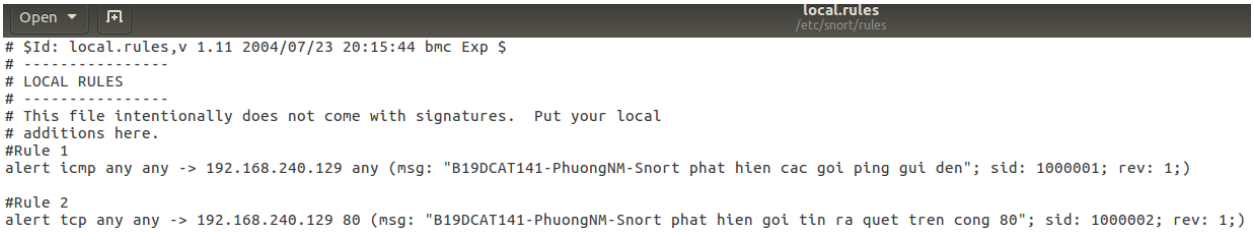

phuongnm-b19dcat141@ubuntu: ~
phuongnm-b19dcat141@ubuntu:~$ snort -V
-*> Snort! <*-
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.7.4
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.8


phuongnm-b19dcat141@ubuntu: ~
03/25-00:46:34.212330 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.240.1:5
7808 -> 239.255.255.250:1900
03/25-00:46:34.212330 192.168.240.1:57808 -> 239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:1570 IpLen:20 DgmLen:202
Len: 174
03/25-00:46:34.655680 192.168.240.1:5353 -> 224.0.0.251:5353
UDP TTL:255 TOS:0x0 ID:20172 IpLen:20 DgmLen:69
Len: 41
03/25-00:46:44.285799 192.168.240.129:39468 -> 91.189.89.198:123
UDP TTL:64 TOS:0x10 ID:947 IpLen:20 DgmLen:76 DF
Len: 48
03/25-00:46:44.526823 91.189.89.198:123 -> 192.168.240.129:39468
UDP TTL:128 TOS:0x0 ID:1669 IpLen:20 DgmLen:76
Len: 48

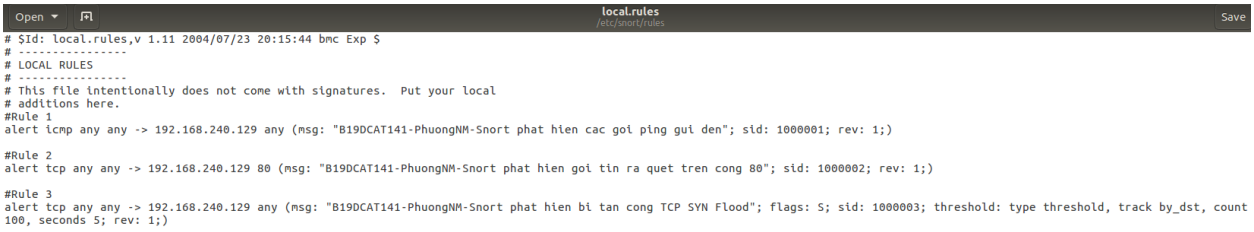
- Tạo các luật Snort để phát hiện 3 dạng rà quét, tấn công hệ thống:
  + Phát hiện các gói tin ping từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiển thị thông điệp khi phát hiện: “<Mã SV-Tên SV>-Snort phát hiện có các gói Ping gửi đến.”



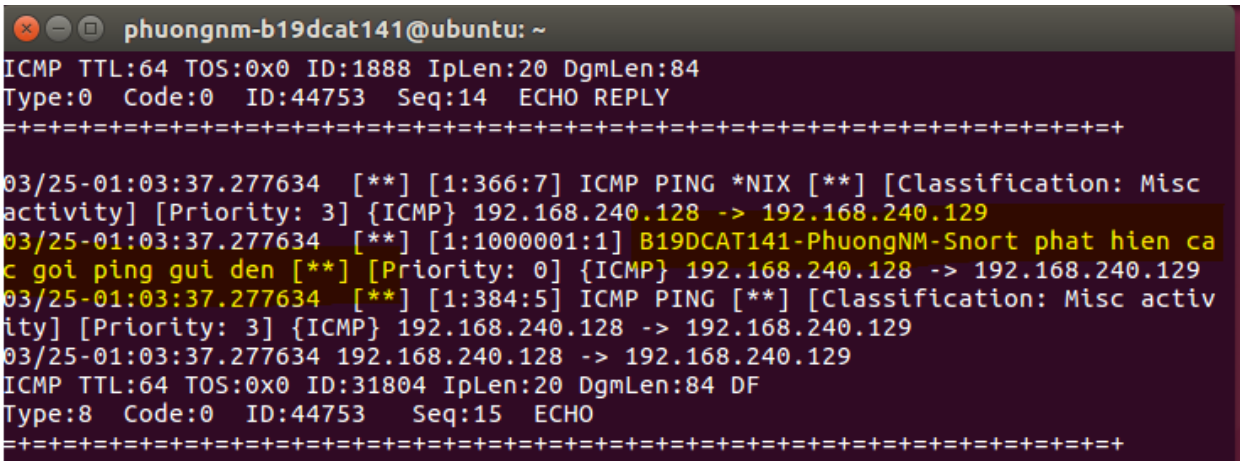
  + Phát hiện các gói tin rà quét từ bất kỳ một máy nào gửi đến máy chạy Snort trên cổng 80. Hiển thị thông điệp khi phát hiện: “<Mã SV-Tên SV>-Snort phát hiện có các gói tin rà quét trên cổng 80.”



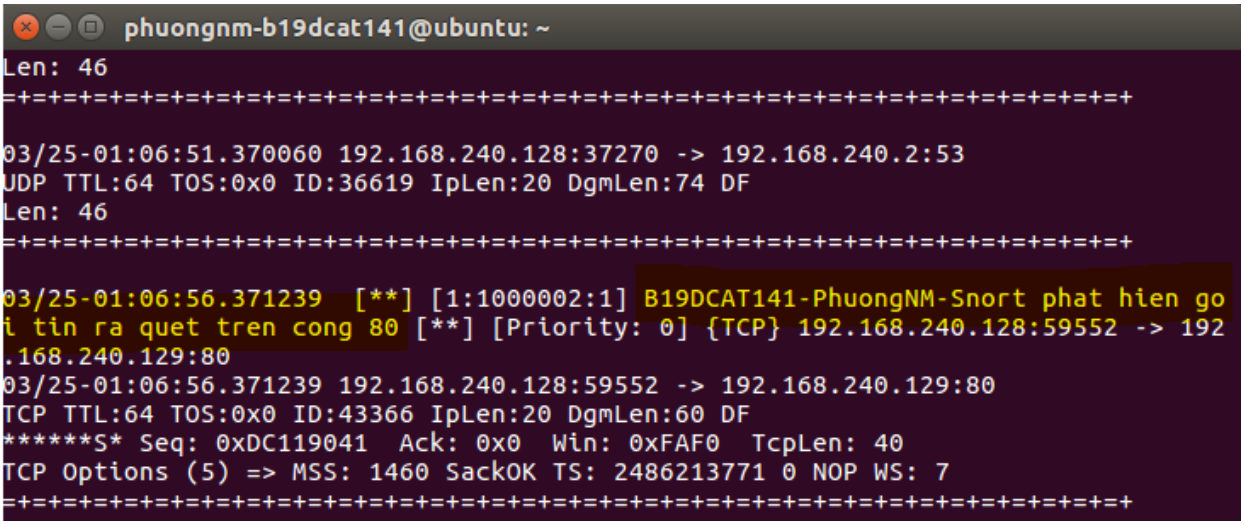
  + Phát hiện tấn công TCP SYN Flood từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiển thị thông điệp khi phát hiện: “<Mã SV-Tên SV>-Snort phát hiện đang bị tấn công TCP SYN Flood.”



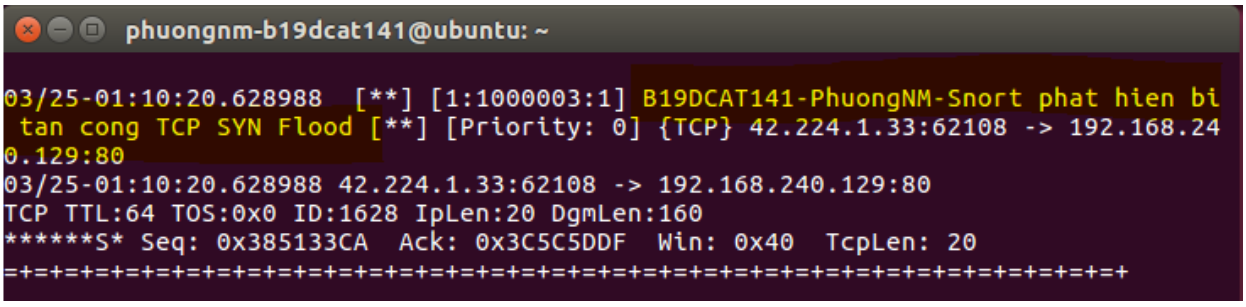
- Thực thi tấn công và phát hiện sử dụng Snort
  + Từ máy Kali, sử dụng lệnh ping để ping máy Snort. Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.



+ Từ máy Kali, sử dụng công cụ nmap để rà quét máy Snort (dùng lệnh: nmap -sV -p80 -A <địa chỉ IP máy Snort>). Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.



+ Từ máy Kali, sử dụng công cụ hping3 để tấn công TCP SYN Flood máy Snort (dùng lệnh: hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source <địa chỉ IP máy Snort>). Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.



III. Kết quả cần đạt :

- Hệ thống phát hiện xâm nhập Snort hoạt động ổn định.
- Các luật mới được tạo và lưu vào trong file luật của Snort.
- Snort phát hiện thành công các rà quét tấn công kể trên (hiển thị trên giao diện terminal hoặc log của Snort).