HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BÀI BÁO CÁO THỰC HÀNH SỐ 6

MÔN THỰC TẬP CƠ SỞ

Tên sinh viên: Ninh Chí Hướng

Mã sinh viên: B20DCAT094

Giảng viên hướng dẫn: Th.s Ninh Thị Thu Trang

HÀ NỘI, THÁNG 3/2023

Table of Contents

Bài 6 : Cài đặt cấu hình HIDS/NIDS

I.Cơ sở lý thuyết

Khi Internet và các mạng nội bộ càng ngày càng phổ biến, thách thức của các vấn đề xâm nhập mạng trái phép đã buộc các tổ chức phải bổ sung thêm hệ thống để kiểm tra các lỗ hổng về bảo mật CNTT. Một trong những hệ thống được những người quan tâm đến bảo mật nhắc đến nhiều nhất là hệ thống phát hiện xâm nhập (IDS). Bài viết này chúng tôi sẽ giới thiệu cho các bạn về IDS, cụ thể là vấn đề tổng quan về một số loại tấn công có thể phát hiện, triệu chứng khi bị tấn công và nhiệm vụ của IDS, các kiến trúc khác nhau và những khái niệm trong lĩnh vực này.

1.1 IDS là gì?

IDS (Intrusion Detection Systems - Hệ thống phát hiện xâm nhập) là thiết bị hoặc phần mềm có nhiệm vụ giám sát traffic mạng, các hành vi đáng ngờ và cảnh báo cho admin hệ thống. Mục đích của IDS là phát hiện và ngăn ngừa các hành động phá hoại bảo mật hệ thống, hoặc những hành động trong tiến trình tấn công như dò tìm, quét các cổng. IDS cũng có thể phân biệt giữa những cuộ tấn công nội bộ (từ chính nhân viên hoặc khách hàng trong tổ chức) và tấn công bên ngoài (từ hacker). Trong một số trường hợp, IDS có thể phản ứng lại với các traffic bất thường/độc hại bằng cách chặn người dùng hoặc địa chỉ IP nguồn truy cập mạng.

1.2 Công nghệ IPS là gì?

Hệ thống phòng chống xâm nhập liên tục giám sát lưu lượng mạng, đặc biệt là ở các gói riêng lẻ, để tìm kiếm bất kỳ cuộc tấn công nguy hiểm nào có thể xảy ra. Nó thu thập thông tin về các gói tin này và báo cáo cho quản trị viên hệ thống, nhưng nó cũng thực hiện những động thái phòng ngừa của riêng mình. Nếu phát hiện phần mềm độc hại tiềm ẩn hoặc loại tấn công khác, IPS sẽ chặn các gói đó truy cập vào mạng.

IPS cũng có thể thực hiện các bước khác, chẳng hạn như đóng những lỗ hổng bảo mật của hệ thống có thể bị khai thác liên tục. IPS có thể đóng các điểm truy cập vào mạng, cũng như cấu hình tường lửa thứ cấp để phát hiện những loại tấn công này trong tương lai, bổ sung thêm các lớp bảo mật cho hệ thống phòng thủ của mạng.

Phân loại

- Dựa trên phạm vi giám sát, IDS được chia thành 2 loại:
    - **Network-based IDS (NIDS):** Là những IDS giám sát trên toàn bộ mạng. Nguồn thông tin chủ yếu của NIDS là các gói dữ liệu đang lưu thông trên mạng. NIDS thường được lắp đặt tại ngõ vào của mạng, có thể đứng trước hoặc sau tường lửa.
    - **Host-based IDS (HIDS):** Là những IDS giám sát hoạt động của từng máy tính riêng biệt. Do vậy, nguồn thông tin chủ yếu của HIDS ngòai

lưu lượng dữ liệu đến và đi từ máy chủ còn có hệ thống dữ liệu nhật ký hệ thống (system log) và kiểm tra hệ thống (system audit).

- Dựa trên kỹ thuật phát hiện, IDS cũng được chia thành 2 loại:
  - **Signature-based IDS:** Signature-based IDS phát hiện xâm nhập dựa trên dấu hiệu của hành vi xâm nhập, thông qua phân tích lưu lượng mạng và log hệ thống. Kỹ thuật này đòi hỏi phải duy trì một cơ sở dữ liệu về các dấu hiệu xâm nhập (signature database), và cơ sở dữ liệu này phải được cập nhật thường xuyên mỗi khi có một hình thức hoặc kỹ thuật xâm nhập mới.
  - **Anomaly-based IDS:** phát hiện xâm nhập bằng cách so sánh (mang tính thống kê) các hành vi hiện tại với hoạt động bình thường của hệ thống để phát hiện các bất thường (anomaly) có thể là dấu hiệu của xâm nhập. Ví dụ, trong điều kiện bình thường, lưu lượng trên một giao tiếp mạng của server là vào khỏang 25% băng thông cực đại của giao tiếp. Nếu tại một thời điểm nào đó, lưu lượng này đột ngột tăng lên đến 50% hoặc hơn nữa, thì có thể giả định rằng server đang bị tấn công DoS. Để hoạt động chính xác, các IDS loại này phải thực hiện một quá trình "học", tức là giám sát hoạt động của hệ thống trong điều kiện bình thường để ghi nhận các thông số hoạt động, đây là cơ sở để phát hiện các bất thường về sau.

1.3 Suricata là gì

Suricata là một công cụ Giám sát An ninh mạng, IPS và Network IDS hiệu suất cao. Nó là mã nguồn mở và được sở hữu bởi một tổ chức phi lợi nhuận do cộng đồng điều hành, Tổ chức Bảo mật Thông tin Mở (OISF). Suricata được phát triển bởi OISF.

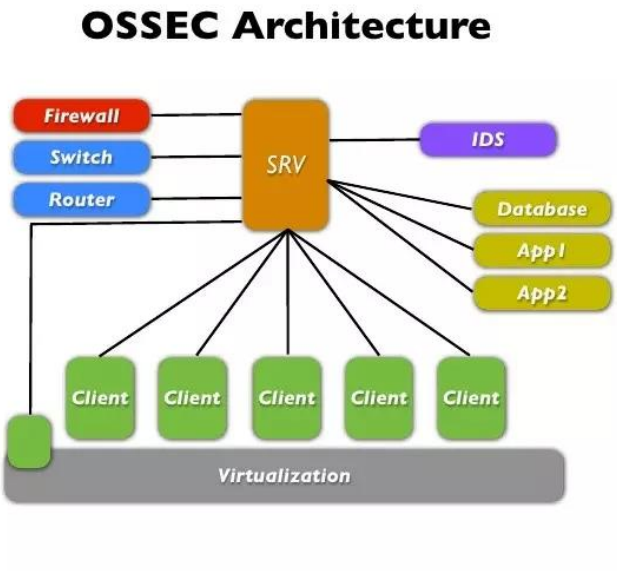
1.4 Zeek

Zeek được trình bày như một công cụ để hỗ trợ quản lý ứng phó sự cố an ninh . Nó hoạt động bằng cách bổ sung dựa trên chữ ký các công cụ để tìm và theo dõi các sự kiện mạng phức tạp. Nó được đặc trưng bằng cách cung cấp phản hồi nhanh, ngoài việc sử dụng nhiều luồng và giao thức. Nó không chỉ giúp xác định các sự kiện bảo mật, mà còn nhằm mục đích tạo điều kiện khắc phục sự cố.

1.5 OSSEC

OSSEC là hệ thống phát hiện xâm nhập dựa trên host (HIDS) dựa trên log mã nguồn mở, miễn phí, đa nền tảng có thể mở rộng và có nhiều cơ chế bảo mật khác nhau. OSSEC có thể phát hiện xâm nhập bằng cả chữ ký hoặc dấu hiệu bất thường. Các dấu hiệu bình thường và bất thường được mô tả trong bộ luật của OSSEC. OSSEC có một công cụ phân tích và tương quan mạnh mẽ, tích hợp giám sát và phân tích log, kiểm tra tính toàn vẹn của file, kiểm tra registry của Windows, thực thi chính

sách tập trung, giám sát chính sách, phát hiện rootkit, cảnh báo thời gian thực và phản ứng một cách chủ động cuộc tấn công đang diễn ra. Các hành động này cũng có thể được định nghĩa trước bằng luật trong OSSEC để OSSEC hoạt động theo ý muốn của người quản trị. Ngoài việc được triển khai như một HIDS, nó thường được sử dụng như một công cụ phân tích log, theo dõi và phân tích các bản ghi lại, IDS, các máy chủ Web và các bản ghi xác thực. OSSEC chạy trên hầu hết các hệ điều hành, bao gồm Linux, OpenBSD, FreeBSD, Mac OS X, Sun Solaris và Microsoft Windows. OSSEC còn có thể được tích hợp trong trong các hệ thống bảo mật lớn hơn là SIEM (Security information and event management). OSSEC chỉ có thể cài đặt trên Windows với tư cách là một agent.



1.6 Wazuh

Wazuh là nền tảng mã nguồn mở hợp nhất của XDR và SIEM. Nó miễn phí và có hơn 10 triệu lượt tải xuống hàng năm. Wazuh có các agent được triển khai trên các endpoint cần giám sát. Agent sẽ thu thập dữ liệu sự kiện bảo mật (security event) từ các endpoint được giám sát và chuyển tiếp chúng đến máy chủ Wazuh để phân tích log, phân tích tương quan và đưa ra cảnh báo.

Wazuh có sẵn một số mô-đun giúp nâng cao tình hình bảo mật tổng thể của một tổ chức. Dưới đây là một số mô-đun Wazuh có liên quan.

- Kiểm kê hệ thống (System inventory)
- Phát hiện lỗ hổng bảo mật (Vulnerability detector)
- Đánh giá cấu hình bảo mật (SCA)

- Phát hiện và ứng phó với mối đe dọa

II.Thực hành

2.1. Tải, cài đặt Snort và chạy thử Snort.

```
root@B20DCAT094-NInhChiHuong-Snort:~# apt install -y snort
```

```
root@B20DCAT094-NInhChiHuong-Snort:~# snort --v

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11
```

Kiểm tra log của Snort để đảm bảo Snort hoạt động bình thường.

```
root@B20DCAT094-NInhChiHuong-Snort:/# tail -f /var/log/snort/snort.alert.fast
03/16-07:53:13.858947  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Net
work Scan] [Priority: 3] {UDP} 192.168.14.1:61833 -> 239.255.255.250:1900
03/16-07:53:14.860841  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Net
work Scan] [Priority: 3] {UDP} 192.168.14.1:61833 -> 239.255.255.250:1900
03/16-07:55:11.848800  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Net
work Scan] [Priority: 3] {UDP} 192.168.14.1:56381 -> 239.255.255.250:1900
03/16-07:55:12.858732  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Net
work Scan] [Priority: 3] {UDP} 192.168.14.1:56381 -> 239.255.255.250:1900
03/16-07:55:13.871011  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Net
work Scan] [Priority: 3] {UDP} 192.168.14.1:56381 -> 239.255.255.250:1900
03/16-07:55:14.879402  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Net
work Scan] [Priority: 3] {UDP} 192.168.14.1:56381 -> 239.255.255.250:1900
03/16-07:57:11.881911  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Net
work Scan] [Priority: 3] {UDP} 192.168.14.1:56201 -> 239.255.255.250:1900
03/16-07:57:12.885730  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Net
work Scan] [Priority: 3] {UDP} 192.168.14.1:56201 -> 239.255.255.250:1900
03/16-07:57:13.894956  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Net
work Scan] [Priority: 3] {UDP} 192.168.14.1:56201 -> 239.255.255.250:1900
03/16-07:57:14.910633  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Net
work Scan] [Priority: 3] {UDP} 192.168.14.1:56201 -> 239.255.255.250:1900
```

2.2.Tạo các luật Snort

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

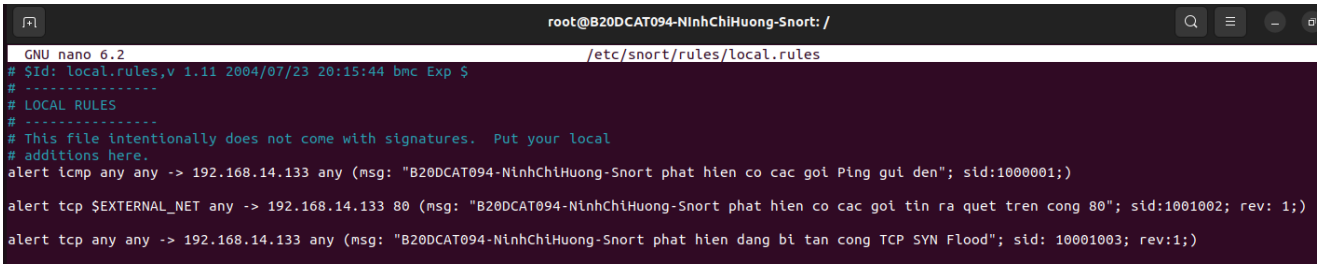
80. Hiển thị thông điệp khi phát hiện: “<Mã SV-Tên SV>-Snort phát hiện có các gói tin

rà quét trên cổng 80.”

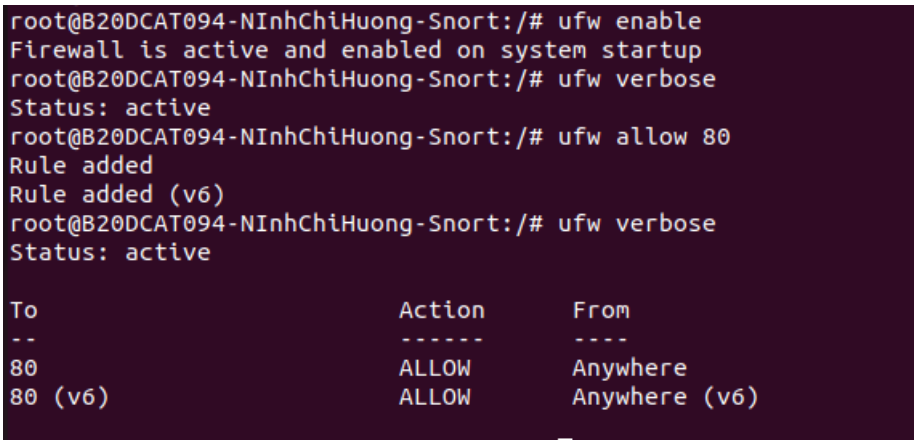
+ Phát hiện tấn công TCP SYN Flood từ bất kỳ một máy nào gửi đến máy chạy Snort. Hiển

thị thông điệp khi phát hiện: “<Mã SV-Tên SV>-Snort phát hiện đang bị tấn công TCP

SYN Flood.”



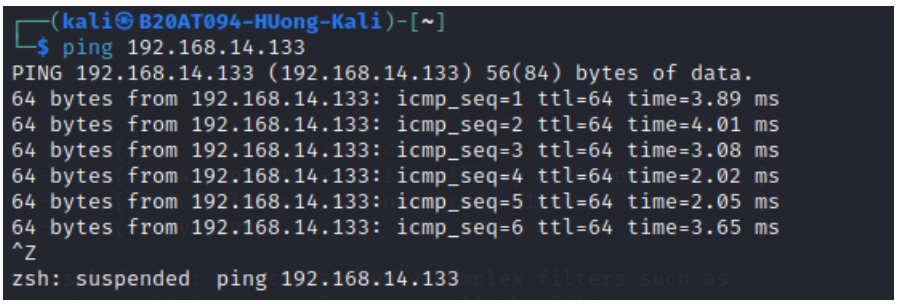
Cho phép gói tin vượt tường lửa

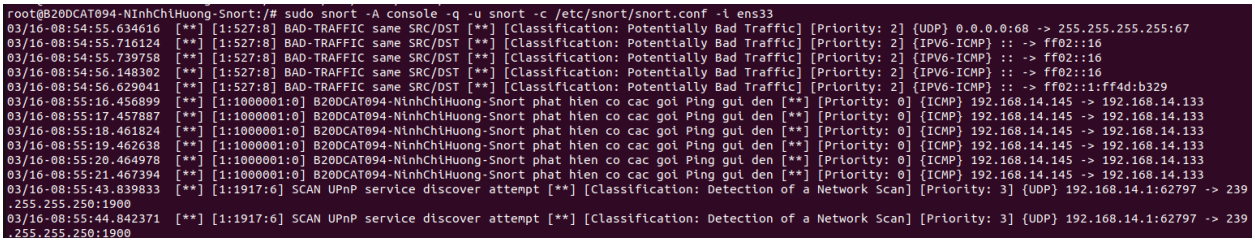


2.3. thực thi tấn công và phát hiện sử dụng Snort

+ 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.

```
┌──(kali㉿B20AT094-HUong-Kali)-[~]
└─$ nmap -sV -p80 -A 192.168.14.133
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-16 02:25 EDT
Nmap scan report for 192.168.14.133
Host is up (0.0028s latency).

PORT   STATE  SERVICE VERSION
80/tcp closed http

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```

```
root@B20DCAT094-NInhChiHuong-Snort:/# snort -A console -q -u snort -c /etc/snort/snort.conf -i ens33
03/16-16:09:14.640243  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 192.168.14.145:60882 -
> 192.168.14.133:80
03/16-16:09:14.640243  [**] [1:1001002:1] B20DCAT094-NinhChiHuong-Snort phat hien co cac goi tin ra quet tren cong 80 [**] [Priority: 0] {TCP} 192.168.14.145:608
82 -> 192.168.14.133:80
03/16-16:09:15.052882  [**] [1:1000001:0] B20DCAT094-NinhChiHuong-Snort phat hien co cac goi Ping gui den [**] [Priority: 0] {ICMP} 192.168.14.145 -> 192.168.14.
133
03/16-16:09:15.078444  [**] [1:1000001:0] B20DCAT094-NinhChiHuong-Snort phat hien co cac goi Ping gui den [**] [Priority: 0] {ICMP} 192.168.14.145 -> 192.168.14.
133
03/16-16:09:15.130560  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 192.168.14.145:41241 -
> 192.168.14.133:80
03/16-16:09:15.130560  [**] [1:1001002:1] B20DCAT094-NinhChiHuong-Snort phat hien co cac goi tin ra quet tren cong 80 [**] [Priority: 0] {TCP} 192.168.14.145:412
41 -> 192.168.14.133:80
03/16-16:09:15.155827  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 192.168.14.145:41242 -
> 192.168.14.133:80
03/16-16:09:15.155827  [**] [1:1001002:1] B20DCAT094-NinhChiHuong-Snort phat hien co cac goi tin ra quet tren cong 80 [**] [Priority: 0] {TCP} 192.168.14.145:412
```

+ 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.

```
┌──(root㉿B20AT094-HUong-Kali)-[~]
└─# hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.14.133

HPING 192.168.14.133 (eth0 192.168.14.133): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
82: ^C
--- 192.168.14.133 hping statistic ---
51105 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
03/16-13:35:18.568344  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 52.144.203.40:45793 -> 192.168.14.133:82
03/16-13:35:18.568347  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 138.7.119.38:45794 -> 192.168.14.133:82
03/16-13:35:18.568348  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 238.86.124.20:45795 -> 192.168.14.133:82
03/16-13:35:18.568350  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 68.169.197.46:45796 -> 192.168.14.133:82
03/16-13:35:18.568351  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 179.244.242.14:45797 -> 192.168.14.133:82
03/16-13:35:18.568353  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 84.228.20.56:45798 -> 192.168.14.133:82
03/16-13:35:18.568634  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 151.212.7.67:45799 -> 192.168.14.133:82
03/16-13:35:18.568636  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 115.24.135.169:45800 -> 192.168.14.133:82
03/16-13:35:18.569269  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 24.120.186.2:45801 -> 192.168.14.133:82
03/16-13:35:18.569274  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 48.220.135.144:45802 -> 192.168.14.133:82
03/16-13:35:18.569518  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 93.196.226.41:45803 -> 192.168.14.133:82
03/16-13:35:18.569521  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 81.54.101.136:45804 -> 192.168.14.133:82
03/16-13:35:18.569870  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 10.85.48.138:45805 -> 192.168.14.133:82
03/16-13:35:18.569874  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 118.67.84.118:45806 -> 192.168.14.133:82
03/16-13:35:18.570290  [**] [1:10001003:1] B20DCAT094-NinhChiHuong-Snort phat hien dang bi tan cong TCP SYN Flood [**] [Priority: 0] {TCP} 37.24.76.122:45807 -> 192.168.14.133:82
```

Tài liệu tham khảo

+ Chương 5, Giáo trình Cơ sở an toàn thông tin, Học viện Công nghệ BVCT, 2020.

+ Suricata: https://suricata.io/documentation/

+ Snort: https://www.snort.org/#documents

+ OSSEC: https://www.ossec.net/docs/

+ Wazuh: https://documentation.wazuh.com/current/index.html