**Mục lục**

1. [KIẾN THỨC LÝ THUYẾT 3](file:///C:\Users\Acer\Downloads\Bài-thực-hành-6_Phạm-Bá-Tú_B19DCAT164.docx#_bookmark0)
   1. [Tìm hiểu khái quát về các hệ thống phát hiện tấn công, xâm nhập 3](file:///C:\Users\Acer\Downloads\Bài-thực-hành-6_Phạm-Bá-Tú_B19DCAT164.docx#_bookmark1)
   2. [Kiến trúc của một hệ thống IDS 3](file:///C:\Users\Acer\Downloads\Bài-thực-hành-6_Phạm-Bá-Tú_B19DCAT164.docx#_bookmark2)
   3. [Phân loại các hệ thống phát hiện xâm nhập, các kỹ thuật phát hiện xâm nhập. 3](file:///C:\Users\Acer\Downloads\Bài-thực-hành-6_Phạm-Bá-Tú_B19DCAT164.docx#_bookmark3)
   4. [Các kỹ thuật phát hiện xâm nhập 4](file:///C:\Users\Acer\Downloads\Bài-thực-hành-6_Phạm-Bá-Tú_B19DCAT164.docx#_bookmark4)
   5. [Tìm hiều về kiến trúc và chức năng của một số hệ thống phát hiện tấn công, xâm nhập 5](file:///C:\Users\Acer\Downloads\Bài-thực-hành-6_Phạm-Bá-Tú_B19DCAT164.docx#_bookmark5)
2. [BÁO CÁO THỰC HÀNH 6](file:///C:\Users\Acer\Downloads\Bài-thực-hành-6_Phạm-Bá-Tú_B19DCAT164.docx#_bookmark6)

[Bước 1: 6](file:///C:\Users\Acer\Downloads\Bài-thực-hành-6_Phạm-Bá-Tú_B19DCAT164.docx#_bookmark7)

[Bước 2 7](file:///C:\Users\Acer\Downloads\Bài-thực-hành-6_Phạm-Bá-Tú_B19DCAT164.docx#_bookmark8)

[Bước 3 9](file:///C:\Users\Acer\Downloads\Bài-thực-hành-6_Phạm-Bá-Tú_B19DCAT164.docx#_bookmark9)

Bước 4 1

## **KIẾN THỨC LÝ THUYẾT**

##### **Tìm hiểu khái quát về các hệ thống phát hiện tấn công, xâm nhập**

###### Khái quát:

* + - Xâm nhập là tập các hành động nhằm thỏa hiệp với mục tiêu an toàn( tính bảo mật, toàn vẹn và sẵn dùng) của tài nguyên hoặc máy tính.
    - Các hệ thống tấn công xâm nhập (IDS) là một lớp phòng vệ quan trọng trong các lớp giải pháp đảm bảo an toàn cho hệ thống thông tin và mạng theo mô hình phòng thủ có chiều sâu.
    - Hệ thống tấn công, xâm nhập IDS có nhiệm vụ chính là:
      * Giám sát lưu lượng mạng hoặc các hành vi trên một hệ thống để nhận dạng các dấu hiệu của tấn công, xâm nhập.
      * Khi phát hiện các hành vi tấn công, xâm nhập thì gi logs các hành vi này cho phân tích bổ sung sau này.
      * Gửi thông báo cho người quản trị về các hành vi tấn công, xâm nhập đát phát hiện được.
      * Thông thường hệ thống IDS thường kết nối vào các bộ định tuyến, card mạng và chủ yếu làm nhiệm vụ giám sát và cảnh bảo, không có khả năng chủ động ngăn chặn tấn công, xâm nhập.

##### **Kiến trúc của một hệ thống IDS**

* Hệ thống cảm biến: thu thập những sự kiện liên quan đến an ninh hệ thống.
* Hệ thống phân tích: phát hiện tấn công và các hành vi đáng nghi dựa trên hệ thống cảm biến.
* Không gian lưu trữ: lưu trữ các sự kiện và kết quả phân tích.
* Giao diện điều khiển: để cài đặt hệ thống IDS, cập nhật các trạng thái bảo mật và kiểm tra các sự kiện/bản ghi từ hệ thống phân tích.

##### **Phân loại các hệ thống phát hiện xâm nhập, các kỹ thuật phát hiện xâm nhập.**

Các hệ thống phát hiện 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;

IDS – Intrusion Detection System: hệ thống phát hiện tấn công, xâm nhập.

###### **Phân loại theo nguồn dữ liệu**:

* Hệ thống phát hiện xâm nhập mạng (NIDS – Network-based IDS):phân tích lưu lượng mạng để phát hiện tấn công, xâm nhập cho cả mạng hoặc một phần mạng. Trong một sơ đồ mạng, NIDS được bố trí để giám sát phát hiện xâm nhập tại cổng vào và cho từng phân đoạn mạng.
* Hệ thống phát hiện xâm nhập cho host (HIDS – Host-based IDS):phân tích các sự kiện xảy ra trong hệ thống/dịch vụ để phát hiện tấn công, xâm nhập cho hệ thống đó.

##### **Các kỹ thuật phát hiện xâm nhập**

Được chia làm hai kỹ thuật chính: Phát hiện xâm nhập dựa trên chữ ký và phát hiện xâm nhập dựa trên các bất thường.

*- Phát hiện xâm nhập dựa trên chữ ký:* trước hết cần xây dựng csdl các chữ kí, hoặc các dấu hiện của các loại tấn công xâm nhập đã biêt. Hầu hết các chữ kí, dấu hiệu được nhận dạng và mã hóa thủ công và dạng thường gặp là các luật phát hiện. bước tiếp theo là sử dụng csdl các chữ ký để giám sát các hành vi của hệ thông hoặc mạng, cảnh báo nếu phát hiện chữ kí của tấn công.

- Ưu điểm lớn nhất của phát hiện xâm nhập dựa trên chữ ký là có khả năng phát hiện các tấn công, xâm nhập đã biết một cách hiệu quả. Ngoài ra, phương pháp này cho tốc độ xử lý cao, đồng thời yêu cầu tài nguyên tính toán tương đối thấp. Nhờ vậy, các hệ thống phát hiện xâm nhập dựa trên chữ ký đƣợc ứng dụng rộng rãi trong thực tế. Tuy nhiên, nhược điểm chính của phương pháp này là không có khả năng phát hiện các tấn công, xâm nhập mới, do chữ ký của chúng chưa tồn tại trong cơ sở dữ liệu các chữ ký.

Hơn nữa, nó cũng đòi hỏi nhiều công sức xây dựng và cập nhật cơ sở dữ liệu chữ ký, dấu hiệu của các tấn công, xâm nhập.

*-Phát hiện xâm nhập dựa trên bất thường:* Phát hiện xâm nhập dựa trên bất thường (Anomaly intrusion detection) dựa trên giả thiết: các hành vi tấn công, xâm nhập thường có quan hệ chặt chẽ với các hành vi bất thường. Quá trình xây dựng và triển khai một hệ thống phát hiện xâm nhập dựa trên bất thƣờng gồm 2 giai đoạn: là huấn luyện và là phát hiện.

-Giai đoạn huấn luyện: Hồ sơ (profile) của đối tƣợng trong chế độ làm việc bình thường được xây dựng. Để thực hiện giai đoạn huấn luyện này, cần giám sát đối tƣợng trong một khoảng thời gian đủ dài để thu thập đƣợc đầy đủ dữ liệu mô tả các hành vi của đối tượng trong điều kiện bình thường làm dữ liệu huấn luyện. Tiếp theo, thực hiện huấn luyện dữ liệu để xây dựng mô hình phát hiện, hay hồ sơ của đối tượng.

-Giai đoạn đoạn phát hiện: Thực hiện giám sát hành vi hiện tại của hệ thống và cảnh báo nếu có khác biệt rõ nét giữa hành vi hiện tại và các hành vi lưu trong hồ sơ của đối tượng.

-Ưu điểm của phát hiện xâm nhập dựa trên bất thường là có tiềm năng phát hiện các loại tấn công, xâm nhập mới mà không yêu cầu biết trước thông tin về chúng. Tuy nhiên, phương pháp này có tỷ lệ cảnh báo sai tƣơng đối cao so với phương pháp phát hiện dựa trên chữ ký. Điều này làm giảm khả năng ứng dụng thực tế của phát hiện xâm nhập dựa trên bất thường. Ngoài ra, nó cũng tiêu tốn nhiều tài nguyên hệ thống cho việc xây dựng hồ sơ đối tượng và phân tích hành vi hiện tại

##### **Tìm hiều về kiến trúc và chức năng của một số hệ thống phát hiện tấn công, xâm nhập**

**Snort**

Snort là một NIDS được Martin Roesh phát triển dưới mô hình mã nguồn mở. Tuy Snort miễn phí nhưng nó lại có rất nhiều tính năng tuyệt vời mà không phải sản phẩm thương mại nào cũng có thể có được. Nó được tạo ra bởi Cisco. Hệ thống có thể được chạy ở ba chế độ khác nhau và có thể thực hiện các chiến lược phòng thủ, vì vậy nó là một hệ thống ngăn chặn xâm nhập cũng như một hệ thống phát hiện xâm nhập.

###### **Kiến trúc:**

Snort bao gồm nhiều thành phần, với mỗi phần có một chức năng riêng. Các phần chính đó là:

* Môđun giải mã gói tin (Packet Decoder)
* Môđun tiền xử lý (Preprocessors)
* Môđun phát hiện (Detection Engine)
* Môđun log và cảnh báo (Logging and Alerting System)
* Môđun kết xuất thông tin (Output Module)

-Kiến trúc của Snort được mô tả trong hình sau:

Diagram

Description automatically generated

Khi Snort hoạt động nó sẽ thực hiện việc lắng nghe và thu bắt tất cả các gói tin nào di chuyển qua nó. Các gói tin sau khi bị bắt được đưa vào Môđun Giải mã gói tin. Tiếp theo gói tin sẽ được đưa vào môđun Tiền xử lý, rồi môđun Phát hiện. Tại đây tùy theo việc có phát hiện được xâm nhập hay không mà gói tin có thể được bỏ qua để lưu thông tiếp hoặc được đưa vào môđun Log và cảnh báo để xử lý. Khi các cảnh báo được xác định môđun Kết xuất thông tin sẽ thực hiện việc đưa cảnh báo ra theo đúng định dạng mong muốn.

# BÁO CÁO THỰC HÀNH

**1. Chuẩn bị môi trường, công cụ**

- 01 máy tính (máy thật hoặc máy ảo) chạy Linux với RAM tối thiểu 2GB,10GB đĩa cứng có kết nối mạng (LAN hoặc Internet).

- 01 máy tính (máy thật hoặc máy ảo) chạy Kali Linux (bản 2021 trở lên).

- Bộ phần mềm Snort tải tại https://www.snort.org/downloads

**2. Các bước thực hiện**

**a. Cài đặt và cấu hình Snort**

- Kiểm tra địa chỉ IP của máy tính Kali Linux và máy tính Ubuntu

Địa chỉ IP máy tính Ubuntu

Text

Description automatically generated

Địa chỉ IP máy tính Kali Linux

Text

Description automatically generated

Tiến hành cài đặt Snort

sudo apt-get update

sudo apt-get upgrade

sudo apt-get install snort\*

Text

Description automatically generated

Nhấn Y để tiếp tục

* Cấu hình Snort

Text

Description automatically generated

* Kiểm tra snort đã cài đặt thành công hay chưa

snort –V

Text

Description automatically generated

b. 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

Chỉnh sửa luật trong Snort

*cd /etc/snort/rules/*

*ls*

Text

Description automatically generated

*sudo nano scan.rules*

Tìm tới dòng msg: SCAN nmap XMAS”, đánh dấu # ở đầu dòng

Graphical user interface, text

Description automatically generated

Hiển thị thông điệp khi phát hiện có các gói ping gửi đến

*sudo nano local.rules*

Thêm dòng sau vào cuối file:

alert icmp any any -> 192.168.146.131 any (msg: “dangxuanhai052\_Snort

dectected ping packets are sending”; sid: 1000001;)

Text

Description automatically generated

Tại máy cài Snort ta gõ lệnh sau:

*cd*

*sudo snort -A console -q -i ens33 -c /etc/snort/snort.conf*

**

*Trên máy Kali, ta tiến hành ping*

*ping 192.168.146.131*

*Text

Description automatically generated*

Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.

Text

Description automatically generated

- Phát hiện các gói tin rà quét từ bất kỳ một máy nào gửi đến máy chạy Snort trên cổng 80.

Tương tự như trên, ta cấu hình file local.rules để hiển thị thông báo khi phát hiện có các gói tin trên cổng 80

Thêm dòng sau vào cuối file:

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 80 (msg: “dangxuanhai052\_Snort detected packets scanning on gate 80”; sid: 1001002; rev: 1;)

Text

Description automatically generated

Nếu ảnh trên không được thì sẽ thêm như ảnh bên dưới

Text

Description automatically generated

Trước tiên phải kích hoạt firewall và cổng 80 trên máy Snort

Text

Description automatically generated

Tại máy cài Snort ta gõ lệnh sau:

*cd*

*sudo snort -A console -q -i ens33 -c /etc/snort/snort.conf*



Trên máy Kali ta gõ lệnh sau

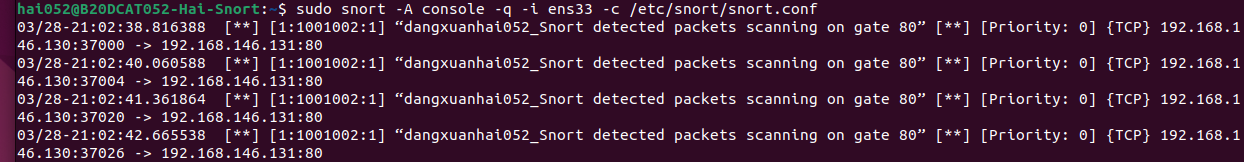
*sudo –i (chuyển sang root)*

*nmap 192.168.146.131 (dùng nmap để rà quét Snort)*

Text

Description automatically generated

Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort

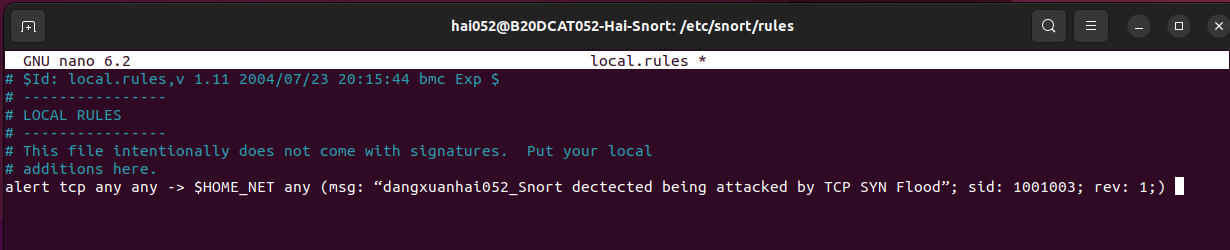


- Sử dụng công cụ hping3 để tấn công TCP SYN Flood máy Snort

Tương tự như trên, ta cấu hình file local.rules để hiển thị thông báo khi phát hiện đang bị tấn công TCP SYN Flood

Thêm dòng sau vào cuối file

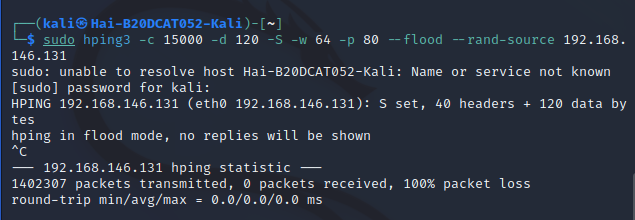
alert tcp any any -> $HOME\_NET any (msg: “dangxuanhai052\_Snort dectected being attacked by TCP SYN Flood”; sid: 1001003; rev: 1;)



Tại máy cài Snort ta gõ lệnh sau:

*Cd*

*sudo snort -A console -q -i ens33 -c /etc/snort/snort.conf*

**

Trên máy Snort kiểm tra kết quả phát hiện trên giao diện terminal hoặc log của Snort.

*Text

Description automatically generated*

1. **Tổng kết**

Qua bài báo cáo trên, chúng ta đã cùng nhau tìm hiểu khái quát về hệ thống phát hiện tấn công xâm nhập (IDS), phân loại các hệ thống phát hiện xâm nhập và các kỹ thuật phát hiện xâm nhập. Ngoài ra, chúng ta cũng tìm hiểu về kiến trúc và tính năng của một số hệ thống phát hiện tấn công, xâm nhập như Snort, OSSEC, Suricata, Wazuh. Bài thực hành cũng cung cấp một số kĩ năng cài đặt Snort, tạo các luật trong Snort để phát hiện các gói tin ping từ một máy khác gửi đến Snort, phát hiện các gói tin rà quét từ bất kì một máy nào gửi đến Snort trên cổng 80, cấu hình Snort để thông báo về một cuộc tấn công TCP.