

## Môn học: INT13147 - Thực tập cơ sở

### Bài thực hành số 6 - Cài đặt cấu hình HIDS/NIDS

#### 1. Mục đích

- Luyện tập việc cài đặt và vận hành các hệ thống phát hiện xâm nhập cho host (HIDS) và cho mạng (NIDS).
- Luyện tập việc tạo và chỉnh sửa các luật phát hiện tấn công, xâm nhập cho các hệ thống phát hiện xâm nhập thông dụng.

#### 2. Nội dung thực hành

##### 2.1 Tìm hiểu 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.
- 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...
- Một số 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>

##### 2.2 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>

##### 2.3 Các bước thực hiện

- Bước 1: 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.
- Bước 2: Tải, cài đặt Snort và chạy thử Snort. Kiểm tra log của Snort để đảm bảo Snort hoạt động bình thường.
- Bước 3: 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. Hiện 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. Hiện 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. Hiện thị thông điệp khi phát hiện: "<Mã SV-Tên SV>-Snort phát hiện đang bị tấn công TCP SYN Flood."
- Bước 4: 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.

#### 2.4 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 kẻ trên (hiển thị trên giao diện terminal hoặc log của Snort).

### 3. Các yêu cầu với báo cáo bài thực hành

Báo cáo bài thực hành cần có đầy đủ các nội dung/thành phần sau:

- Trang bìa (ghi rõ môn học, bài thực hành, mã sv và họ và tên.
- Trình bày vắn tắt về Snort (sơ đồ khối, các thành phần, luật) trong 1-2 trang.
- Ảnh chụp màn hình tất cả các bước thực hiện trong mục 2.3. Lưu ý ảnh màn hình phải có đầy đủ các thông tin về máy tấn công, máy phát hiện (Mã SV-Tên SV) và các cảnh báo phát hiện.
- Các ảnh chụp màn hình cần theo đúng thứ tự các bước trong mục 2.3.
- Bài nộp ở dạng file pdf, tên file ví dụ như: Bài thực hành 6\_Họ tên\_Mã sinh viên.pdf