3

Lab

# Viết rule trên Snort

Thực hành

**Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập**

**Lưu hành nội bộ**

# A. TỔNG QUAN

## A.1 Mục tiêu

- Tìm hiểu và viết các rule cho Snort (https://www.snort.org/documents#latest_rule_documents)
- Phân tích các luồng traffic trước và sau khi triển khai rule.

## A.2 Cài đặt môi trường

- Sử dụng môi trường đã cài đặt ở bài thực hành 02.

# B. THỰC HÀNH

Sinh viên thực hiện bài thực hành với những yêu cầu bên dưới.

## B.1 Viết rule cho Snort

**Yêu cầu 1.1** Ngăn chặn tấn công ICMP Flood

- Viết Snort rule thực hiện giới hạn gói ICMP đến máy *Victim*. Ngưỡng (threshold) là không quá 23 gói/5s.
- Sử dụng công cụ **hping3** trên máy *Attacker* để thực hiện tấn công.
- Kiểm tra kết quả trước và sau khi cài đặt rule.

**Yêu cầu 1.2** Chỉ cho phép truy cập đến các dịch vụ đang chạy trên Victim

- Sử dụng **nmap** quét các cổng đang mở trên máy *Victim*.
- Viết Snort rule chỉ cho phép các máy truy cập đến các port đang mở của máy Victim. Chặn tất cả các port còn lại.
- Sử dụng công cụ **telnet** hoặc **nmap** trên máy Attacker thực hiện tấn công.
- Kiểm tra kết quả trước và sau khi cài đặt rule.

**Yêu cầu 1.3** Ngăn chặn tấn công dò mật khẩu trên ứng dụng Web

- Truy cập vào ứng dụng web Mutillidae (/mutillidae/index.php?page=login.php) trên máy Victim. Viết Snort rule ngăn chặn tấn công dò mật khẩu đăng nhập trên ứng dụng web này. **Lưu ý**: chỉ chặn dò mật khẩu, ứng dụng web vẫn phải truy cập bình thường.
- Sử dụng công cụ **hydra** trên máy Attacker thực hiện tấn công.
- Kiểm tra kết quả trước và sau khi cài đặt rule.

**Yêu cầu 1.4** Ngăn chặn tấn các công Path Traversal

- Viết Snort rule ngăn chặn các tấn công Path Traversal[1].

[1] https://owasp.org/www-community/attacks/Path_Traversal

- Trên máy Attacker truy cập đến đường dẫn http://192.168.x.200/dvwa/ để thực hiện tấn công.
- Kiểm tra kết quả trước và sau khi thực hiện tấn công.

**Yêu cầu 1.5** Sinh viên tự xây dựng thêm 2 kịch bản tấn công và viết Snort rule để ngăn chặn tấn công

- Sinh viên tự xây dựng 2 kịch bản tấn công khác không liên quan đến tấn công DoS và tấn công web, sau đó, viết rule Snort để ngăn chặn tấn công.
- Thực hiện viết rule Snort, kiểm tra kết quả trước và sau khi tấn công giống như các yêu cầu phía trên.
- Điểm đánh giá tùy thuộc vào mức độ phức tạp của kịch bản.

## C. YÊU CẦU

– Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện **theo nhóm**.

**Hình thực báo cáo**

- Hình thức 1: Báo cáo tại lớp.
- Hình thức 2: Nộp báo cáo kết quả và nội dung chi tiết những việc (**Report**) mà nhóm đã tìm hiểu, thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả; giải thích cho quan sát (nếu có).

**Báo cáo:**

– File ***.PDF***, tập trung vào nội dung, không mô tả lý thuyết.

– Đặt tên theo định dạng: **[Mã lớp]-LabX_NhomY.PDF**.

*Ví dụ: [NT204.K11.ATTT]-Lab3_Nhom0.PDF.*

– Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với tên theo định dạng **[Mã lớp]-LabX_NhomY.ZIP**.

– Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**~HẾT~**