DETECTION OF ADVERSARIAL DDOS ATTACKS USING GENERATIVE ADVERSARIAL NETWORKS WITH DUAL DISCRIMINATORS (GANDD)

NGUYỄN THÀNH TÂM - 230201053

[1] Trường ĐH Công Nghệ Thông Tin [2] University of Information Technology HCMC, Vietnam [3] National Institute of Informatics

What ?

Ứng dụng mô hình GANvới Bộ phân biệt đối xử kép (GANDD) để phát hiện các cuộc tấn công DDoS, trong đó:

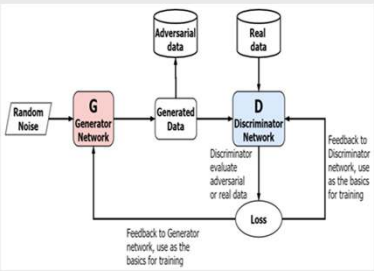
- Nghiên cứu và phát triển mô hình GANDD..
- Đánh giá hiệu quả của mô hình GANDD
- So sánh hiệu quả của mô hình GANDD với các phương pháp phát hiện tấn công DDoS truyền thống.

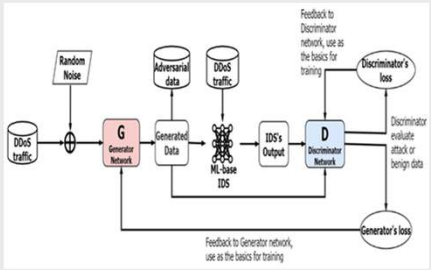
Why ?

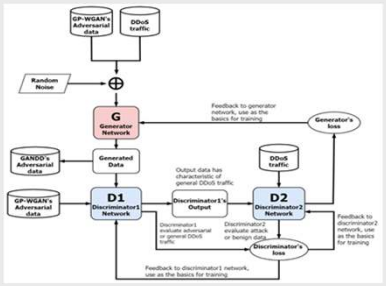
- Các cuộc tấn công DDoS đang ngày càng gia tăng về tần suất, cường độ và độ phức tạp.
- Phương pháp ML,DL hạn chế về huấn luyện, thu thập dữ liệu, đánh giá và kiểm tra.
- GANDD khả năng học hỏi từ các mẫu dữ liệu phức tạp và phân biệt lưu lượng truy cập bình thường khỏi lưu lượng truy cập tấn công DDoS đối ngjich một cách hiệu quả.

Overview

Mô hình GAN → Mô hình GP-WGAN → Mô hình GANDD





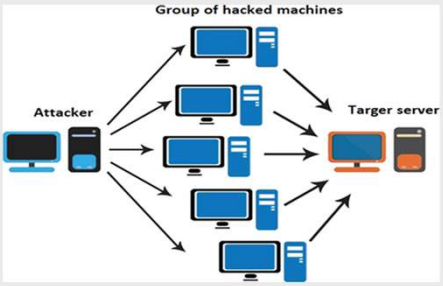


Description

1. Tìm hiểu các phương pháp phát hiện tấn công DDoS truyền thống

Phân tích so sánh ưu và nhược điểm của các phương pháp phát hiện tấn công DDoS hiện có theo:

- Phát hiện dựa trên quy tắc.
- Phát hiện dựa trên thống kê
- Phát hiện dựa trên máy học.



2. Tìm hiểu mô hình GANDD

Kiến trúc và nguyên tắc hoạt động của mô hình GANDD

Ứng dụng GANDD vào phát hiện tấn công DDoS theo phương pháp:

- Thu thập dữ liệu: Thu thập dữ liệu lưu lượng truy cập mạng và dữ liệu tấn công DDoS từ các nguồn khác nhau
- Xử lý dữ liệu: Làm sạch, chuyển đổi và chuẩn hóa dữ liệu để đảm bảo chất lượng dữ liệu phù hợp cho việc huấn luyện mô hình
- Huấn luyện mô hình GANDD: Thiết lập cấu trúc mô hình, chọn thuật toán tối ưu hóa và huấn luyện mô hình GANDD

3. Triển khai mô hình GANDD

- Triển khai mô hình GANDD: Triển khai mô hình GANDD vào hệ thống phát hiện tấn công DDoS thực tế.
- Đánh giá mô hình GANDD:đánh giá để đánh giá hiệu quả phát hiện tấn công DDoS của mô hình GANDD, bao gồm tính chính xác, độ nhạy và độ đặc trưng.
- Phân tích thách thức và giải pháp: Xác định các thách thức khi ứng dụng GANDD vào phát hiện tấn công DDoS

NII

NGUYỄN THÀNH TÂM – University of Information Technology HCMC, Vietnam
TEL : 0916173031 Email : tamngt.18@grad.uit.edu.vn