**TÌM HIỂU VÀ XÂY DỰNG HỆ THỐNG PHÁT HIỆN XÂM NHẬP MẠNG IDS SỬ DỤNG MACHINE LEARNING**

|  |  |  |
| --- | --- | --- |
|  | ***Sinh viên thực hiện chính:*** | **Nguyễn Thắng Lợi** |
| ***Ngày, tháng, năm sinh:*** | 29/01/2004 |
| ***Thành viên đề tài:*** | Nguyễn Văn Trường, Lê Anh Khoa, Nguyễn Trí Dũng, Nguyễn Thành Lộc |
| ***Giảng viên hướng dẫn*** | Th.S Nguyễn Thị Thanh Vân |
| ***Số điện thoại liên lạc:*** | 0901.27.78.26 |
| ***Địa chỉ email:*** | 22162023@student.hcmute.edu.vn |
|  |  |

**Tóm tắt nội dung đề tài:**

1. **Mục tiêu đề tài**

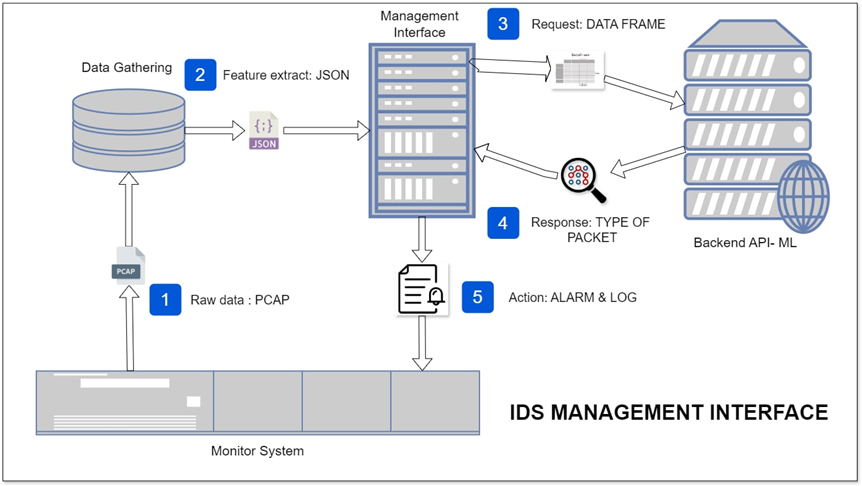
Hiện nay, lĩnh vực công nghệ thông tin đang phát triển nhanh chóng nhưng bên cạnh đó, ngày càng nhiều các cuộc tấn công mạng quy mô lớn xảy ra đòi hỏi các tổ chức, doanh nghiệp phải phát hiện kịp thời các cuộc tấn công để giảm thiểu tối đa thiệt hại mà các cuộc tấn công gây ra. Chúng em ấp ủ thực hiện một dự án “Tìm hiểu và xây dựng hệ thống phát hiện xâm nhập mạng IDS sử dụng Machine Learning”. Mục tiêu hướng tới là phân tích và thiết kế kiến trúc cho một hệ thống IDS tích hợp mô hình học máy, cách thức khai phá dữ liệu và huấn luyện cho mô hình học máy để tối ưu hóa khả năng nhận diện xâm nhập.

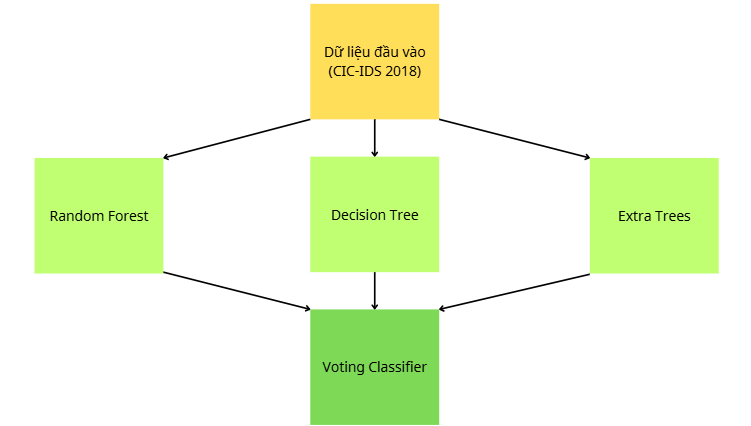
1. **Tính mới và tính sáng tạo**

Hệ thống phát hiện xâm nhập mạng đóng vai trò quan trọng trong các hệ thống hệ thống bảo mật để phát hiện và ngăn chặn kịp thời các cuộc tấn công. Cho đến nay, trên thế giới đã có nhiều nghiên cứu về việc áp dụng các công nghệ tiên tiến, đặc biệt là Machine Learning vào việc xây dựng các hệ thống phát hiện xâm nhập mạng. Tuy nhiên, việc nghiên cứu và ứng dụng Machine Learning vào hệ thống phát hiện xâm nhập mạng ở Việt Nam vẫn còn hạn chế chưa đáp ứng được nhu cầu bảo mật ngày càng cao. Do đó, nhóm đã tiến hành nghiên cứu và phát triển một hệ thống phát hiện xâm nhập mạng sử dụng Machine Learning trên bộ dữ liệu CIC-IDS 2018 để có thể góp phần nâng cao bảo mật cho các hệ thống bảo mật.

1. **Kết quả nghiên cứu**

Xây dựng hệ thống phát hiện xâm nhập mạng bao gồm các thành phần như: Bộ phận thu thập gói tin, bộ phận backend API-ML, bộ phận quản lý. Hoạt động kết hợp thu thập dữ liệu, xử lý đặc trưng, phân tích với Machine Learing và quản lý các phản hồi để đảm bảo an ninh mạng hiệu quả.

Hình 1. Sơ đồ hệ thống IDS nhóm đề xuất



*Hình 2.1 Các mô hình học máy dược sử dụng*

Kết hợp các thuật toán Decision Tree, Random Forest, Extra Trees vào một mô hình Voting Classifier để kết hợp dự đoán từ nhiều mô hình con, tạo ra một kết quả cuối cùng bằng cách lấy ý kiến đa số giúp tận dụng được điểm mạnh của từng mô hình, giảm thiểu nhược điểm riêng lẻ của chúng.

Bộ dữ liệu CIC-IDS 2018 được phát triển và cung cấp bởi Trung tâm An ninh mạng Canada (Canadian Institute for Cybersecurity - CIC) thuộc Đại học New Brunswick. Đây là một trong những tập dữ liệu tiêu chuẩn được sử dụng phổ biến trong nghiên cứu phát hiện xâm nhập mạng, với mục đích đánh giá hiệu suất của các hệ thống phát hiện xâm nhập dựa trên các kỹ thuật học máy và học sâu. Bộ dữ liệu CIC-IDS 2018 được xây dựng nhằm mô phỏng các kịch bản tấn công mạng phổ biến trong thực tế và cung cấp thông tin chi tiết về các hành vi của các loại tấn công, từ đó giúp phát triển và kiểm thử các thuật toán phát hiện xâm nhập.

Kết quả đạt được sau khi sử dụng mô hình học máy với bộ dữ liệu CIC-IDS-2018 đạt được độ chính xác trung bình khá cao

99,88%. Với các cuộc tấn công Dos/DDos đạt được kết quả cao nhất với 99,89% do sự đặc trưng về cuộc tấn công này khá rõ ràng. Còn với những loại tấn công khác (OtherAttacks) đạt kết quả khá thấp với

80% có thể bởi vì các cuộc tấn công này chưa rõ ràng và dễ bị nhầm lẫn với các cuộc tấn công khác nên đạt kết quả không cao. Nhưng tổng quan thì kết quả trung bình khá cao, ít khi bỏ sót các cuộc tấn công.

Bảng 1. Kết quả đạt được

|  |  |  |  |
| --- | --- | --- | --- |
| Classification | Precision (%) | recall (%) | f1-score (%) |
| Bot | 87.94 | 76.86 | 82.93 |
| BruteForce | 99.95 | 100 | 99.97 |
| DoS/DDoS | 99.85 | 99.92 | 99.89 |
| OtherAttacks | 100 | 66.67 | 80.00 |
| PortScan | 98.94 | 99.27 | 99.11 |
| WebAttacks | 99.05 | 97.20 | 98.12 |

1. **Đóng góp về mặt kinh tế-xã hội, giáo dục và đào tạo, an ninh quốc phòng và khả năng áp dụng thực tế**

Đề tài khi được áp dụng sẽ giúp tăng cường hiệu quả trong việc bảo vệ an ninh mạng trong việc phát hiện và xử lý kịp thời các cuộc tấn công, giúp cải thiện độ an toàn cho hệ thống thông tin tại các tổ chức, doanh nghiệp với tình hình tấn công mạng ngày càng gia tăng. Bên cạnh đó, hệ thống này cũng mang ý nghĩa thiết thực trong việc thúc đẩy ứng dụng công nghệ trí tuệ nhân tạo vào bảo mật, tạo nên môi trường bảo mật an toàn và bền vững. Và bài nghiên cứu này cũng có thể tài liệu cho sinh viên ngành an toàn thông tin nói riêng, công nghệ thông tin nói chung để góp phần nâng cao nhận thức, kiến thức về an toàn mạng.