ĐỀ CƯƠNG NGHIÊN CỨU

TÊN ĐỀ TÀI (IN HOA)

PHÁT HIỆN TẤN CÔNG MẠNG DỰA TRÊN PHƯƠNG PHÁP HỌC MÁY

TÊN ĐỀ TÀI TIẾNG ANH (IN HOA)

NETWORK INTRUSION DETECTION SYSTEMS USING MACHINE LEARNING PROJECT

TÓM TẮT

Ngày nay tình trạng các hoạt động tấn công xâm nhập mạng ngày càng gia tăng, các kẻ tấn công ngày càng tinh vi, nhiều hệ thống phát hiện xâm nhập (Network Intrusion Detection Systems) được phát triển nhằm phát hiện các hành vi bất thường, bằng cách dựa theo những quy tắc đã được thiết lập sẵn để kiểm tra các lưu lượng mạng đi vào bên trong hệ thống. Tuy nhiên nhiều hệ thống đều gặp phải các tình trạng như tạo ra rất nhiều cảnh báo, trong đó có các cảnh báo dương tính giả hoặc không phát hiện được các hành vi bất thường mới, các lưu lượng mạng tấn công chưa có signature trên hệ thống. Phương pháp thực hiện để cải tiến cho việc này là xây dựng mô hình máy học với thuật toán Cây quyết định (Decision Tree) bằng cách kiểm tra các lưu lượng mạng dựa trên những thuộc tính riêng biệt của một lưu lượng mạng đi vào bên trong hệ thống, từ đó đưa ra việc xác định lưu lượng tấn công hay là lưu lượng bình thường. Với mục tiêu khắc phục được những điểm yếu của mô hình NIDS truyền thống, giảm thiểu được những phát hiện sai lệch và tăng cường phát hiện được những cuộc tấn công mới hoặc xây dựng dựa trên những biến đổi từ các cuộc tấn công cũ. Việc hoàn thành tốt đề tài này sẽ góp phần tăng cường bảo mật cho các hệ thống, ngăn chặn được các hành vi xấu tổn hại đến tài nguyên cũng như các hệ thống quan trọng đang vận hành bên trong.

GIỚI THIỆU

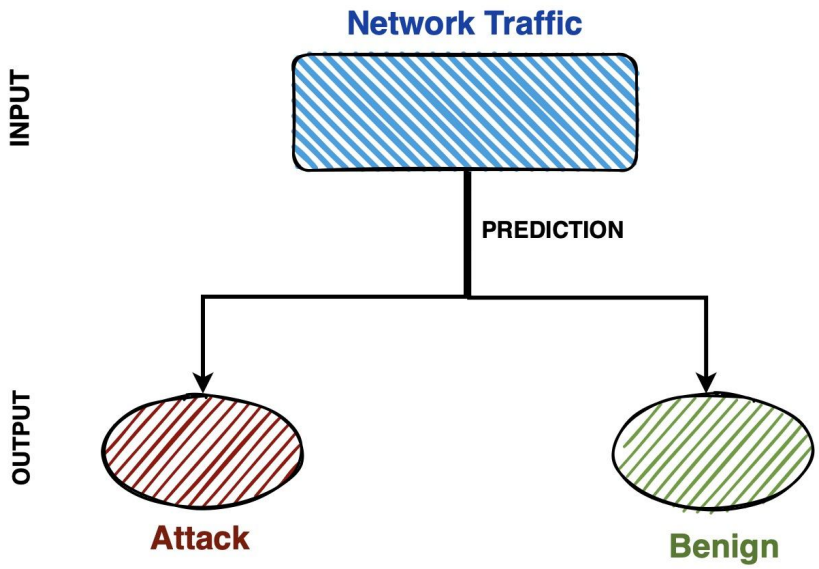
An ninh mạng ngày nay đối mặt với thách thức lớn từ sự ngày càng phức tạp của các mối đe dọa mạng cộng với việc sử dụng rộng rãi các thiết bị thông minh như điện

thoại thông minh, cửa thông minh, camera, ổ khóa,..) và quá trình cạnh tranh của các đơn vị sản xuất thúc đẩy nhanh quá trình sản xuất sản phẩm, cho ra đời những sản phẩm thiết bị sử dụng mạng nhưng không đảm bảo an toàn trên không gian mạng. Hơn thế nữa, các tấn công mạng không chỉ ngày càng tinh vi mà còn có khả năng biến đổi để tránh phát hiện từ các hệ thống an ninh truyền thống. Trong bối cảnh này, phương pháp học máy đã nổi lên như một công cụ quan trọng để nâng cao khả năng phát hiện các cuộc tấn công mạng không chỉ là đã tồn tại trước đó mà còn phát hiện các cuộc tấn công mới hoặc các cuộc tấn công tạo ra từ sự đột biến của các cuộc tấn công trước đó. Trong đề tài này là nghiên cứu và phát triển một hệ thống phát hiện tấn công mạng (Network Intrusion Detection System) sử dụng phương pháp học máy (Machine Learning). Điều này là cực kỳ quan trọng vì sự gia tăng về cả về số lượng và tính phức tạp của các tấn công mạng đặt ra thách thức lớn cho các hệ thống an ninh hiện đại. Vì vậy sự kết hợp giữa khả năng phân tích dữ liệu lớn và khả năng học máy có thể mang lại hiệu quả cao, làm tăng độ chính xác cho việc phát hiện một cuộc tấn công xâm nhập vào hệ thống .Hi vọng rằng đề tài nghiên cứu này không chỉ đóng góp vào lĩnh vực phát hiện tấn công mạng mà còn mở ra những triển vọng mới trong việc ứng dụng học máy trong an ninh mạng. Việc thành công của đề tài có thể mang lại lợi ích lớn cho cộng đồng an ninh mạng bằng cách cung cấp một công cụ hiệu quả và linh hoạt để giảm thiểu rủi ro từ các tấn công mạng.

Trong đề tài nghiên cứu này, áp dụng mô hình Decision Tree (Cây quyết định) thường được sử dụng trong bài toán phân loại và dự đoán.

Input: Dữ liệu đầu vào của bài toán này là các lưu lượng mạng thô đi vào bên trong hệ thống

Output: Kết quả xác định đó là lưu lượng “xấu” - lưu lượng tấn công xâm nhập hệ thống hoặc lưu lượng mạng “tốt” - lưu lượng bình thường.



MỤC TIÊU

- Nghiên cứu mô hình học máy Decision Tree và ứng dụng vào việc phát hiện tấn công mạng
- Xây dựng được hệ thống phát hiện xâm nhập mạng hiệu quả, có khả năng nhận diện và phân loại các loại tấn công mạng phổ biến, hành vi bất thường và các cuộc tấn công mạng chưa có signature, đồng thời giảm thiểu được tỉ lệ nhiễu (dương tính giả).
- Phát triển được mô hình đã có và có thể thực hiện khả năng học liên tục và tiến hóa trong thuật toán. Góp phần phát hiện nhanh những đợt tấn công mạng đã có sẵn và mới nhất.

NỘI DUNG VÀ PHƯƠNG PHÁP

1. **Nội dung:**

- Nội dung 1: Nắm rõ được những khái niệm về tấn công mạng, phương thức mà các công cụ NIDS phát hiện tấn công mạng, cách triển khai mô hình NIDS trong mô hình doanh nghiệp.
- Nội dung 2: Tìm hiểu về mô hình học máy. Tìm hiểu về cách hoạt động và Xây dựng cây quyết định (Decision Tree) từ thuật toán ID3
- Nội dung 3: Thu thập, lựa chọn tập Dataset phù hợp và đầy đủ với kiến trúc mô

hình học máy.

- Nội dung 4: Xây dựng và phát triển mô hình phát hiện tấn công mạng, quá trình cài đặt các node trong mô hình, xây dựng kiến trúc với khả năng thu thập dữ liệu và các thông tin có liên quan để phục vụ cho quá trình học máy và nâng cao tỉ lệ chính xác. Thực hiện training cho mô hình và tinh chỉnh các số liệu cho phù hợp.
- Nội dung 5: Dựa trên các kết quả từ môi trường thử nghiệm và môi trường thực tế, từ đó cho ra được những đánh giá thiết thực về mô hình nghiên cứu.

2. Phương pháp thực hiện

- Xây dựng một mô hình NIDS cơ bản có hiệu quả. Phát hiện được các cuộc tấn công cơ bản, đã có signature được công bố trên cộng động.
- Phân tích nghiên cứu về cấu trúc hoạt động của Decision Tree, tổng hợp các cách và thứ tự xây dựng. Các model của Decision Tree bao gồm CART, C4.5 và ID3. ID3 sẽ được áp dụng trong đề tài này bởi tính tiện dụng và hiệu quả.
- Trong thuật toán ID3 cần phải xác định thứ tự của các thuộc tính cần xem xét tại mỗi bước. Thứ tự của các thuộc tính được phân chia theo thuộc tính tốt nhất sẽ lần lượt được chọn ra dựa theo một tiêu chuẩn nào đó ví dụ 1 lưu lượng đến từ quốc gia lạ).
- Để đánh gía được chất lượng sau mỗi lần phân chia dữ liệu vào từng thuộc tính, ta thực hiện xem xét dữ liệu được đổ hòan toàn vào cùng một thuộc tính hay là dữ liệu bị phân chia lẫn vào nhau. Từ đó đưa ra được điểm cần điều chỉnh và tiến hành xây dựng node quyết định
- Bộ dữ liệu NSL-KDD tập hợp các bản ghi lưu lượng mạng được sử dụng trong dự án này. NSL-KDD datatset bao gồm có 4 tập dữ liệu con là DDTest+, KDDTest-21, KDDTrain+ và KDDTrain+_20Percent trong đó KDDTrain+ sẽ được ưu tiên dùng để huấn luyện mô hình và KDDTest+ dùng để kiểm tra.
- Huấn luyện mô hình trên bộ dữ liệu được chọn và so sánh kết quả.
- Xây dựng các cảnh báo phát hiện tấn công xâm nhập mạng và bỏ qua với những lưu lượng cho là bình thường.

3. Thời gian dự kiến

- Nội dung 1: Tìm hiểu về NIDS thực hiện trong 4 - 5 tuần
- Nội dung 2: Tìm hiểu về mô hình học máy và tích hợp vào NDIS thực hiện trong 4 - 5 tuần
- Nội dung 3: Xây dựng tập dữ liệu Dataset thực hiện trong 4 - 5 tuần
- Nội dung 4: Xây dựng mô hình, đào tạo, kiểm tra kết quả và tinh chỉnh thực hiện trong 6 tuần
- Nội dung 5: Kết luận, đánh giá kết quả thực hiện trong 2 tuần

KẾT QUẢ MONG ĐỢI

- Có thể thực hiện kết hợp xây dựng mô hình NIDS và học máy để phát hiện tấn công mạng
- Bộ dữ liệu sử dụng áp dụng tốt cho mô hình
- Có khả năng thu thập dữ liệu, học hỏi và tiến hóa phát hiện chính xác tấn công mạng
- Phát hiện tốt và nhanh chóng các cuộc tấn công mạng xảy ra
- Áp dụng được trong thực tiễn.

TÀI LIỆU THAM KHẢO

[1] Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., Ahmad, F.: Network intrusion detection system: a systematic study of machine learning and deep learning approaches. Trans. Emerg. Telecommun. Technol. 32(1), e4150 (2021)

[2] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., Hotho, A.: A survey of network-based intrusion detection data sets. Comput. Secur. 86, p. 147–167 (2019)

[3] Manghnani, T., Thirumaran, T.: Computational CBGSA – SVM model for network based intrusion detection system. In: Applications and Techniques in Information Security, pp. 185–191. Singapore (2019)

[4] Zhou, Y., Cheng, G., Jiang, S., Dai, M.: Building an efficient intrusion detection system based on feature selection and ensemble classifier. Comput. Netw. 174, 107247 (2020)

[5] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[6] https://github.com/shramos/Awesome-Cybersecurity-Datasets#network-traffic

[7] https://www.geeksforgeeks