THÔNG TIN CHUNG CỦA BÁO CÁO

- Link YouTube video của báo cáo (tối đa 5 phút):
  (ví dụ: https://www.youtube.com/watch?v=AWq7uw-36Ng)
- Link slides (dạng .pdf đặt trên Github):
  (ví dụ: https://github.com/mynameuit/CS2205.APR2023/TenDeTai.pdf)
- *Mỗi thành viên của nhóm điền thông tin vào một dòng theo mẫu bên dưới*
- *Sau đó điền vào Đề cương nghiên cứu (tối đa 5 trang), rồi chọn Turn in*

• Họ và Tên: Đặng Công Vinh
• MSSV: 220201021
 
	• Lớp: CS2205.APR2023
	• Tự đánh giá (điểm tổng kết môn): 8.5/10
	• Số buổi vắng: 1
	• Số câu hỏi QT cá nhân: 3
	• Số câu hỏi QT của cả nhóm: 15
	• Link Github: https://github.com/mynameuit/CS2205.APR2023/
	• Mô tả công việc và đóng góp của cá nhân cho kết quả của nhóm:
	  ○ Lên ý tưởng cho đề tài cần nghiên cứu
	  ○ Viết đề cương nghiên cứu, slide, poster
	  ○ Làm video YouTube

ĐỀ CƯƠNG NGHIÊN CỨU

TÊN ĐỀ TÀI (IN HOA)

NGHIÊN CỨU GIẢI PHÁP PHÁT HIỆN SỚM TẤN CÔNG DDOS DỰA CÁC THUẬT TOÁN MÁY HỌC

TÊN ĐỀ TÀI TIẾNG ANH (IN HOA)

STUDYING A SOLUTION FOR EARLY DETECTION OF DDOS ATTACKS BASED ON MACHINE LEARNING ALGORITHMS

TÓM TẮT *(Tối đa 400 từ)*

Đề xuất xây dựng hệ thống hoạt động như một cảm biến có thể được cài đặt ở bất kỳ đâu trên mạng và thực hiện phân loại lưu lượng truy cập trực tuyến. Sử dụng các kỹ thuật về học máy cơ bản để phát hiện xâm nhập bất thường mạng và các kỹ thuật giảm chiều dữ liệu để loại bỏ các đặc trưng không có nhiều ý nghĩa trong việc phát hiện bất thường là một bài toán mở cần được quan tâm nghiên cứu để tăng hiệu quả dự báo, giảm độ phức tạp tính toán, giảm khả

năng overfitting của mô hình. Mục tiêu chính của hệ thống đề xuất là giảm thời gian tính toán giúp phát hiện sớm tấn công nhưng vẫn đảm bảo độ chính xác của việc phát hiện bất thường.

GIỚI THIỆU *(Tối đa 1 trang A4)*

Thách thức lớn nhất trong việc chống lại DDoS là việc phải phát hiện sớm các cuộc tấn công và giảm thiểu tấn công nhanh nhất có thể. Câu hỏi đặt ra là "Làm thế nào để xây dựng phương pháp có thể phát hiện các cuộc tấn công DDoS nhưng tương thích với IPS - Intrusion prevention system, hạ tầng mạng hiện hữu và không yêu cầu nâng cấp phần mềm hoặc phần cứng".

Trong nghiên cứu này, tác giả đề xuất xây dựng hệ thống hoạt động như một cảm biến có thể được cài đặt ở bất kỳ đâu trên mạng và phân loại lưu lượng truy cập trực tuyến bằng chiến lược dựa trên các thuật toán học máy (Machine Learning) giúp phân loại các mẫu lưu lượng ngẫu nhiên được thu thập trên các thiết bị mạng thông qua giao thức truyền phát. Cụ thể:

- ☐ **Input**: Sử dụng các kỹ thuật về học máy cơ bản để phát hiện xâm nhập bất thường mạng (DDoS) và các kỹ thuật giảm chiều dữ liệu để loại bỏ các đặc trưng không có nhiều ý nghĩa trong việc phát hiện bất thường.
- ☐ **Output**: Giảm thời gian tính toán giúp phát hiện sớm tấn công nhưng vẫn đảm bảo độ chính xác của việc phát hiện bất thường.

MỤC TIÊU

(Viết trong vòng 3 mục tiêu, lưu ý về tính khả thi và có thể đánh giá được)

Nghiên cứu và đề xuất xây dựng hệ thống hoạt động như một cảm biến có thể được cài đặt ở bất kỳ đâu trên mạng và thực hiện phân loại lưu lượng truy cập trực tuyến như: Sử dụng các kỹ thuật về học máy cơ bản để phát hiện xâm nhập bất thường mạng và các kỹ thuật giảm chiều dữ liệu để loại bỏ các đặc trưng không có nhiều ý nghĩa trong việc phát hiện bất thường nhằm giảm thời gian tính toán giúp phát hiện sớm tấn công nhưng vẫn đảm bảo độ chính xác của việc phát hiện bất thường.

PHẠM VI

Sử dụng các kỹ thuật về học máy cơ bản (Machine Learning) để phát hiện xâm nhập bất thường mạng (DDoS) và các kỹ thuật giảm chiều dữ liệu để loại bỏ các đặc trưng không có nhiều ý nghĩa trong việc phát hiện bất thường.

ĐỐI TƯỢNG

Mô hình sử dụng thuật toán KNN (K-nearest neighbor) kết hợp với các kỹ thuật giảm chiều dữ liệu để loại bỏ các đặc trưng không có nhiều ý nghĩa trong việc phát hiện bất thường.

NỘI DUNG VÀ PHƯƠNG PHÁP

(Viết nội dung và phương pháp thực hiện để đạt được các mục tiêu đã nêu)

Nội dung:

➢ Tìm hiểu các thuật toán máy học có thể ứng dụng trong việc phát hiện tấn công DDoS hoặc dùng trong một số hệ thống phát hiện xâm nhập như [3]-[11]: K-nearest neighbor (KNN), Random Forests (RF), AdaBoost, Support Vector Machine (SVM).

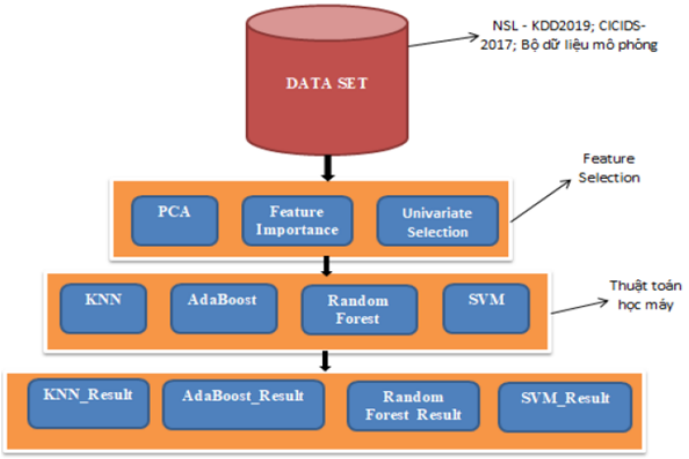
➢ Tìm hiểu các kỹ thuật giảm chiều dữ liệu: Principal Component Analysis (PCA), Feature Importance, Univariate Selection.

➢ Đề xuất phương pháp, kỹ thuật giảm chiều dữ liệu xử lý các dữ liệu đầu vào, các giải thuật học máy để phát hiện các cuộc tấn công nhờ vào khả năng phân loại của chúng để áp dụng vào hệ thống phát hiện xâm nhập mạng (IDS) [12].

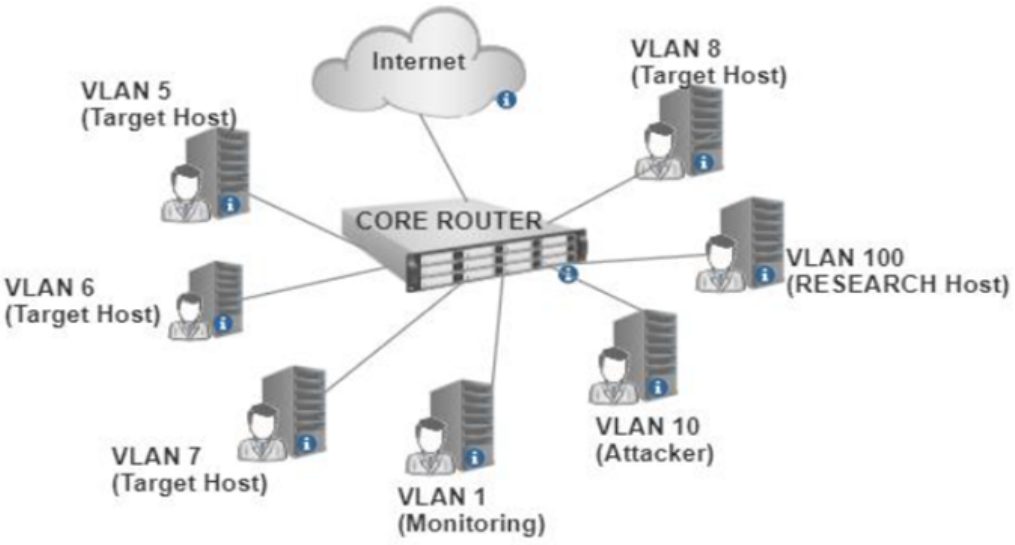
➢ Giả lập mô hình phát hiện tấn công, xây dựng bộ dữ liệu sử dụng huấn luyện để minh họa, đánh giá được tính hiệu quả của hệ thống.

Phương pháp:

❖ Xây dựng và đề xuất mô hình phát hiện tấn công sử dụng kết hợp giải thuật học máy và kỹ thuật giảm chiều dữ liệu.



❖ Giải lập môi trường mạng, xây dựng bộ dữ liệu sử dụng huấn luyện và thiết lập kịch bản tấn công để kiểm thử, đánh giá được tính hiệu quả của hệ thống.



➔ *Đối với thuật toán máy học*: Sử dụng phương pháp Rescaling sử dụng MiMaxScaler có sẵn trong thư viện sklearn; Sử dụng các kỹ thuật giảm chiều dữ liệu xử lý các dữ liệu đầu vào; Sử dụng các giải thuật học máy để phát hiện các cuộc tấn công nhờ vào khả năng phân loại của chúng.

➔ *Đối với Hệ thống IDS*: Bộ dữ liệu chữ ký Signature Dataset (SDS) phát hiện xâm nhập dựa trên chữ ký; Sử dụng kỹ thuật Recursive Feature Elimination with Cross Validation để lựa chọn các đặc trưng quan trọng, sau đó huấn luyện qua thuật toán Random Forest.

KẾT QUẢ MONG ĐỢI

(Viết kết quả phù hợp với mục tiêu đặt ra, trên cơ sở nội dung nghiên cứu ở trên)

★ Chứng minh được thuật toán KNN sẽ phù hợp sau khi được huấn luyện bởi bộ dữ liệu đã giảm chiều dữ liệu, thời gian thực hiện nhanh hơn hẳn và vẫn cho ra được hệ thống có độ chính xác tương đối cao.

★ Phương pháp giảm chiều dữ liệu giúp cho mô hình phát hiện xâm nhập mạng áp dụng các thuật toán học máy cơ bản đạt được mục tiêu đề ra của nghiên cứu. Thời gian thực thi càng ngắn thì càng sớm phát hiện được tấn công, đảm bảo được độ chính xác khi phân loại tấn công.

TÀI LIỆU THAM KHẢO *(Định dạng DBLP)*

[1] Y. Cao, "Understanding Internet DDoS Mitigation from Academic and Industrial Perspectives," IEEE Acess, vol. 6, pp. 66641-66648, 2018.

[2] B. Sunny, "D-FACE: An anomaly based distributed approach for early detection of DDoS attacks," Journal of Network and Computer Applications, vol. 111, pp. 49-63, 2018.

[3] H. HadianJazi, "Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling," Journal of Computer Networks, vol. 121, pp. 25-36, 2017.

[4] N. Muraleedharan and B. Janet, "A deep learning based HTTP slow DoS classification approach using flow data," ICT Express, vol. 7, no. 2, pp. 210-214, 2021.

[5] Y. Zhen, "A systematic literature review of methods and datasets for anomaly-based network intrusion detection," Journal of Computers & Security, vol. 116C, pp. 1-10, 2022.

[6] E. Alhajjar, "Adversarial machine learning in Network Intrusion Detection Systems," Expert Systems with Applications, vol. 186, pp. 1-10, 2021. [7] Y. Gu, "Multiple-Features-Based Semisupervised Clustering DDoS Detection Method," Mathematical Problems in Engineering, vol. 2017, pp. 1-10, 2017.

[8] K. Saravanan, "Detection mechanism for distributed denial of service (DDoS) attacks for anomaly detection system," Journal of Theoretical and Applied information Technology, vol. 60, pp. 174-178, 2014.

[9] Y. Liao and R. V. Vemuri, "Use of K-Nearest Neighbor classifier for intrusion detection," Computers & Security, vol. 21, no. 5, pp. 439-448, 2002.

[10] M. Aamir and S. M. A. Zaidi, "Clustering based semi-supervised machine learning for DDoS attack classification," Journal of King Saud University - Computer and Information Sciences, vol. 33, no. 4, pp. 436-446, 2021.

[11] F. A. F. Silveira, A. M. B. Junior, G. V. Solar, and L. F. Silveira, "Smart Detection: An Online Approach for DoS/DDoS Attack," Security and

Communication Networks, vol. 2019, pp. 1-15, 2019.
[12] J. Long, "TR-IDS: Anomaly-Based Intrusion Detection through Text-Convolutional Neural Network and Random Forest," Security and Communication Networks, vol. 2018, no. 1, pp. 1-9, 2018.
[13] A. Maraj, “Testing of network security systems through DoS attacks,” in Embedded Computing (MECO), 6th Mediterranean Conference on IEEE, pp. 368-373, 2017.
[14] T. T. Tran and H. H. Le, “Study technique to limit bandwidth spending from DDoS attacks,” Dalat University Journal of Science, vol. 7, pp. 52-61, 2020.
[15] H. H. Le, “Improve network security system in Vietnam using reverse method,” TNU Journal of Science and Technology, vol. 225, no. 09, pp. 125-133, 2020.
[16] H. H. Le, “Study to applying Blockchain technology for preventing of spam email,” TNU - Journal of Science and Technology, vol. 208, no. 15, pp. 161-167, 2019.
[17] H. H. Le, “Study the method of implementation of Border Gateway Protocol on IPv4 and IPv6 infrastructure by analysis and evaluate of some properties affecting protocol performance,” TNU Journal of Science and Technology, vol. 226, no. 11, pp. 149-157, 2021.

Kế hoạch thực hiện:

Kế hoạch thực hiện	Nội dung và kết quả mong muốn đạt được
Từ 1/07/2023 đến 8/07/2023	Mô tả chi tiết các thuật toán máy học có thể ứng dụng trong việc phát hiện tấn công DDoS hoặc dùng trong một số hệ thống phát hiện xâm nhập như: K-nearest neighbor (KNN), Random Forests (RF), AdaBoost, Support Vector Machine (SVM).

Từ 9/07/2023 đến 15/07/2023	Mô tả chi tiết các kỹ thuật giảm chiều dữ liệu: Principal Component Analysis (PCA), Feature Importance, Univariate Selection.
Từ 16/07/2023 đến 31/07/2023	Mô tả chi tiết: - Phương pháp, kỹ thuật giảm chiều dữ liệu xử lý các dữ liệu đầu vào, các giải thuật học máy để phát hiện các cuộc tấn công nhờ vào khả năng phân loại của chúng để áp dụng vào hệ thống phát hiện xâm nhập mạng (IDS). - Mô hình phát hiện tấn công, xây dựng bộ dữ liệu sử dụng huấn luyện để minh họa.
Từ 1/08/2023 đến 15/08/2023	- Huấn luyện dựa trên dữ liệu đã thu thập, ghi chép lại kết quả kèm đánh giá và so sánh. - Báo cáo kết quả thực hiện và nộp đề tài nghiên cứu.