HỆ THỐNG PHÁT HIỆN XÂM NHẬP TỰ ĐỘNG PHỤC HỒI CHO MÔI TRƯỜNG ĐIỆN TOÁN ĐÁM MÂY

AUTONOMOUS SELF-HEALING IDS FOR CLOUD COMPUTING ENVIRONMENTS

GVHD: PGS.TS Lê Đình Duy

Phạm Xuân Bách - 240202002

Tóm tắt

- Lớp: CS2205.CH183
- Link Github của nhóm: https://github.com/pxuanbach/Final_Project-CS2205.CH183
- Link YouTube video: https://youtu.be/Zg83WqP_3N8
- Phạm Xuân Bách

Giới thiệu

- Điện toán đám mây phát triển mạnh mẽ với các mô hình IaaS, PaaS, SaaS. Tuy nhiên, các mối đe dọa an ninh mạng ngày càng tinh vi.
- Hệ thống phát hiện xâm nhập (IDS) hỗ trợ giám sát an ninh mạng nhưng gặp hạn chế: **tỷ lệ cảnh báo sai cao, phản ứng chậm, thiếu cơ chế tự phục hồi**.
- Giải pháp đề xuất: IDS tự động phục hồi ứng dụng Machine Learning (ML) & Deep Learning (DL) để phát hiện chính xác tấn công, đưa ra phản ứng nhanh và tự điều chỉnh hệ thống bằng học tăng cường (Reinforcement Learning), sẽ được huấn luyện trên bộ dữ liệu CICIDS2017.

Mục tiêu

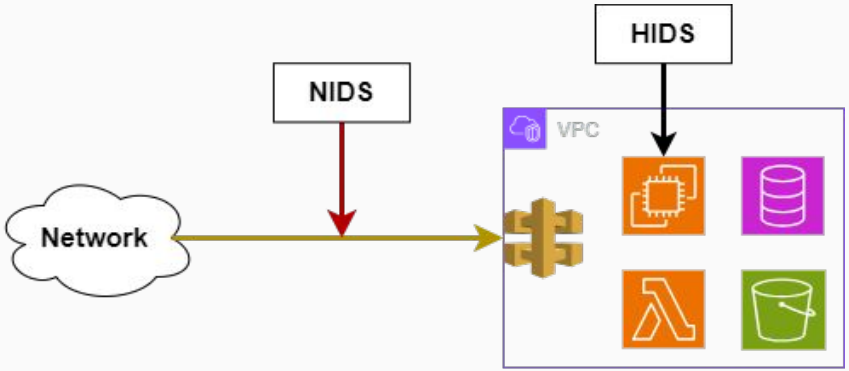
- **Phát triển mô hình IDS tự phục hồi** có khả năng phát hiện tấn công mạng có độ chính xác cao và tự động khôi phục hệ thống mà không cần sự can thiệp của con người.
- **Ứng dụng các kỹ thuật học máy và học sâu** để nâng cao khả năng phát hiện bất thường và phân loại mối đe dọa với độ chính xác cao hơn IDS truyền thống.
- **Phân tích tác động của IDS tự phục hồi** lên hiệu suất hệ thống đám mây, bao gồm chi phí tính toán, mức độ tiêu thụ tài nguyên, độ trễ hệ thống và mức độ ảnh hưởng đến dịch vụ.

Nội dung và Phương pháp

Nội dung 1: Tìm hiểu về các kiến thức nền tảng và các nghiên cứu hiện có của hệ thống phát hiện xâm nhập tự phục hồi

Khảo sát, phân tích các nghiên cứu hiện có về chủ đề IDS tự phục hồi:

- Hệ thống lại các thuật toán ML/DL **đã được sử dụng và kết quả đánh giá** (độ chính xác, tỷ lệ cảnh báo sai).
- Khảo sát các bộ dữ liệu **được sử dụng để huấn luyện** các mô hình ML/DL.
- Tìm hiểu thuật toán **học tăng cường** để đưa ra quyết định tự phục hồi cho hệ thống.



Hình 1. *Hệ thống phát hiện xâm nhập trên môi trường điện toán đám mây*

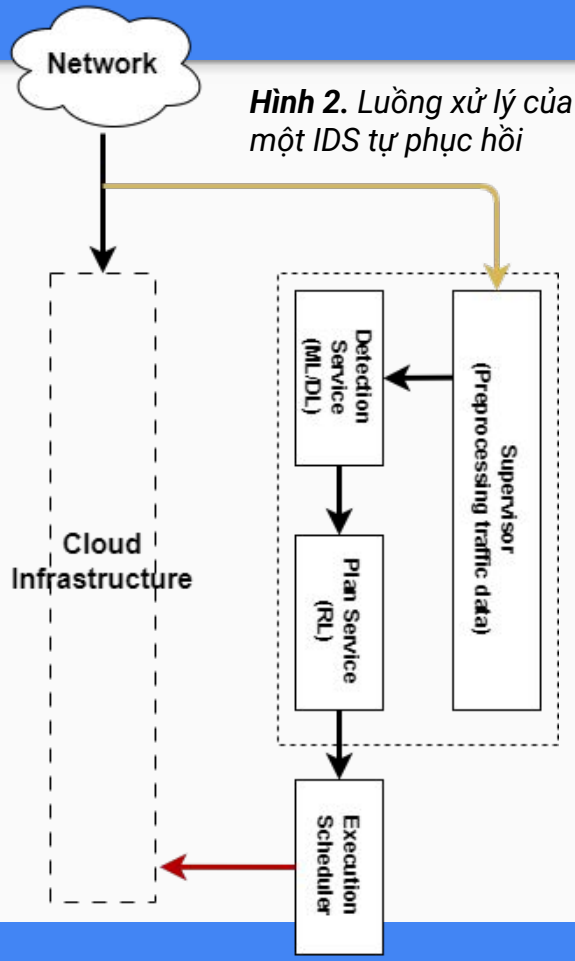
Nội dung và Phương pháp

Nội dung 2: Thiết kế IDS tự phục hồi ứng dụng Machine Learning (ML) và Deep Learning (DL)

Nghiên cứu này đề xuất hệ thống sẽ bao gồm ba thành phần chính:

- **Phát hiện tấn công**: ML/DL nhận diện bất thường, phát hiện tấn công chưa từng thấy.
- **Phân loại mối đe dọa**: DL giúp giảm cảnh báo sai, nâng cao độ chính xác IDS.
- **Cơ chế tự phục hồi**: RL giúp cô lập tấn công, điều chỉnh firewall, khôi phục hệ thống.

Thuật toán đề xuất: **RF, SVM, RNNs, LSTM**.



Hình 2. *Luồng xử lý của một IDS tự phục hồi*

Nội dung và Phương pháp

Nội dung 3: Phương pháp thực hiện

Bộ dữ liệu: Sử dụng **CICIDS2017**, gồm 3 triệu bản ghi, 80 thuộc tính, mô phỏng nhiều loại tấn công: Brute Force, DoS, DDoS, Botnet, SQL Injection, XSS, PortScan...

Tiền xử lý dữ liệu: chuẩn hóa dữ liệu, chia thành các tập để huấn luyện, kiểm thử và đánh giá.

Đánh giá hiệu suất:

- Độ chính xác: Accuracy, Precision, Recall, F1-score.
- Thời gian phản ứng khi bị tấn công.
- Tài nguyên hệ thống: CPU, RAM so với IDS truyền thống.
- Tỷ lệ tự phục hồi thành công.

Kết quả dự kiến

- Tài liệu cung cấp báo cáo về một IDS có khả năng tự phục hồi ứng dụng ML/DL.
- Đưa ra các đánh giá thực nghiệm và so sánh với các IDS hiện có.

Tài liệu tham khảo

[1]. Zamani, Mahdi and Movahedi, Mahnush. (2013). Machine learning techniques for intrusion detection. arXiv preprint arXiv:1312.2177.

[2]. Khraisat, Ansam and Gondal, Iqbal and Vamplew, Peter and Kamruzzaman, Joarder. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2, 1--22.

[3]. Sharafaldin, Iman and Lashkari, Arash Habibi and Ghorbani, Ali A and others. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp, 1, 108--116.

[4]. Ahmed, Nisher and Hossain, Md Emran and Rishad, SSI and Mohiuddin, Arafath Bin and Sarkar, Md Imran and Hossain, Zakir. (2023). Leveraging Reinforcement Learning for Autonomous Cloud Management and Self-Healing Systems. JURIHUM: Jurnal Inovasi Dan Humaniora, 1, 678--689.

Tài liệu tham khảo

[5]. Dai, Wenbin and Riliskis, Laurynas and Wang, Peng and Vyatkin, Valeriy and Guan, Xinping. (2018). A cloud-based decision support system for self-healing in distributed automation systems using fault tree analysis. IEEE Transactions on Industrial Informatics, 14, 989--1000.

[6]. Kushal, Sauharda, Shanmugam, Bharanidharan, Sundaram, Jawahar, & Thennadil, Suresh. (2024). Self-healing hybrid intrusion detection system: an ensemble machine learning approach. Discover Artificial Intelligence, 4, 28.