KỸ THUẬT LỪA DỐI VÀ TĂNG CƯỜNG DỮ LIỆU DỰA TRÊN CYCLEGAN CHO PHÁT HIỆN TẤN CÔNG TRONG MẠNG KHẢ LẬP TRÌNH

CAO BÁ KIỆT - 230202008

Tóm tắt

- Lớp: CS2205.CH181
- Link Github: https://github.com/CaoBaKietIT/PP-NCKH
- Link YouTube video: https://youtu.be/4mmJs8gIEZQ
- Ảnh + Họ và Tên: Cao Bá Kiệt
- Tổng số slides không vượt quá 10

Giới thiệu

- IDS học máy giúp phát hiện các cuộc tấn công mới với độ chính xác cao
- Vấn đề:
  - Thiếu nguồn dữ liệu để huấn luyện
  - Dữ liệu bị mất cân bằng giữa dữ liệu bình thường và dữ liệu độc hại
- Giải pháp:
  - Ứng dụng Cyber Deception trên mạng SDN để thu thập dữ liệu và thiết lập phòng thủ chủ động - phát hiện và chuyển hướng lưu lượng khi phát hiện tấn công, thu thập các IOCs, chiến thuật, kỹ thuật tấn công mới.
  - Sử dụng mô hình CycleGAN sinh dữ liệu độc hại để tái huấn luyện IDS và so sách với IDS ban đầu được huấn luyện dựa trên tập dữ liệu CICIDS2017

Mục tiêu

- Xây dựng, đánh giá Imbalanced-IDS với bộ dữ liệu CICIDS2017.
- Xây dựng mô hình CycleGAN để chuyển đổi dữ liệu bình thường sang dữ liệu độc hại trên tập dữ liệu CICIDS2017 và tái huấn luyện IDS (CycleGAN IDS)
- So sánh CycleGAN IDS với Imbalanced IDS
- Triển khai hệ thống bẫy trong mạng khả lập trình

Nội dung và Phương pháp

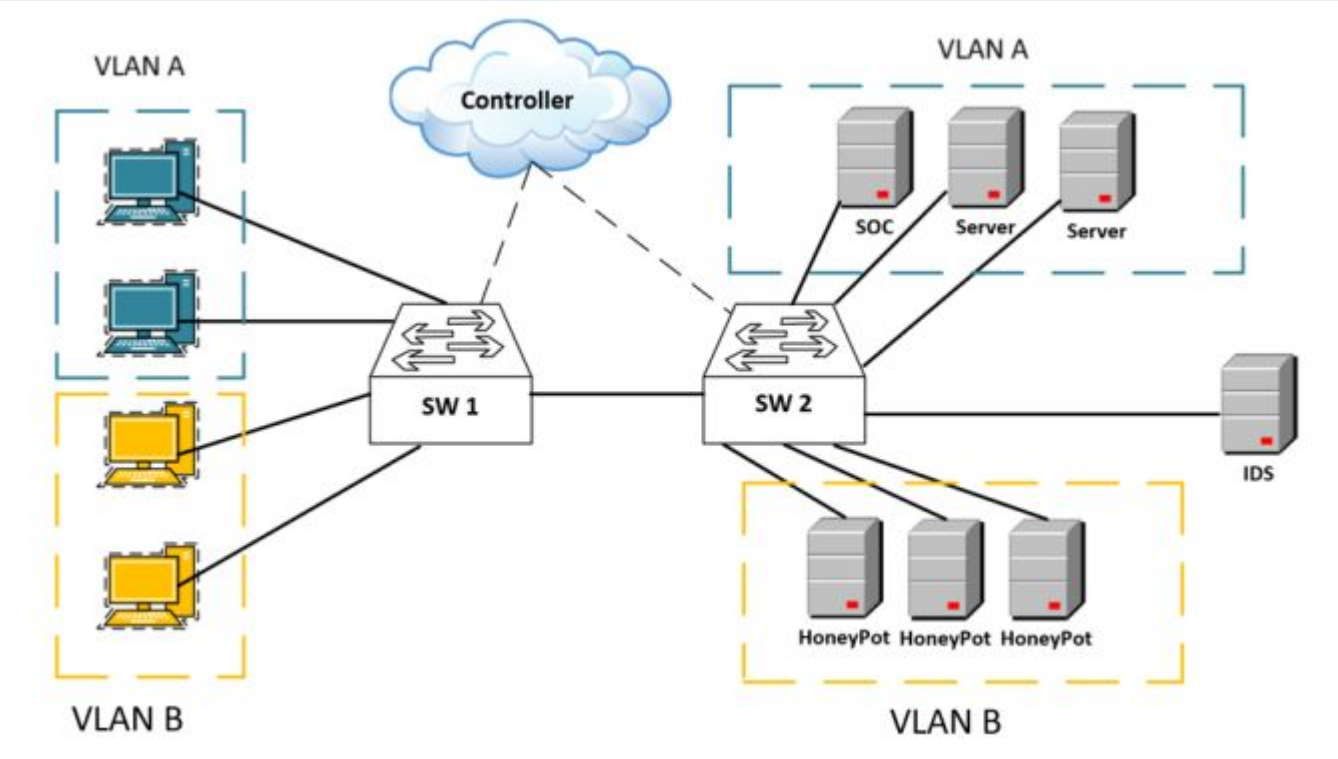
Nội dung 1: Hệ thống phát hiện xâm nhập dựa trên phương pháp học máy

Nội dung 2: Tìm hiểu về Neural Network, Generative Adversarial Network (GAN) và Cycle Adversarial Network (CycleGAN)

Nội dung 3: Xây dựng hệ thống Cyber deception trong mạng khả lập trình

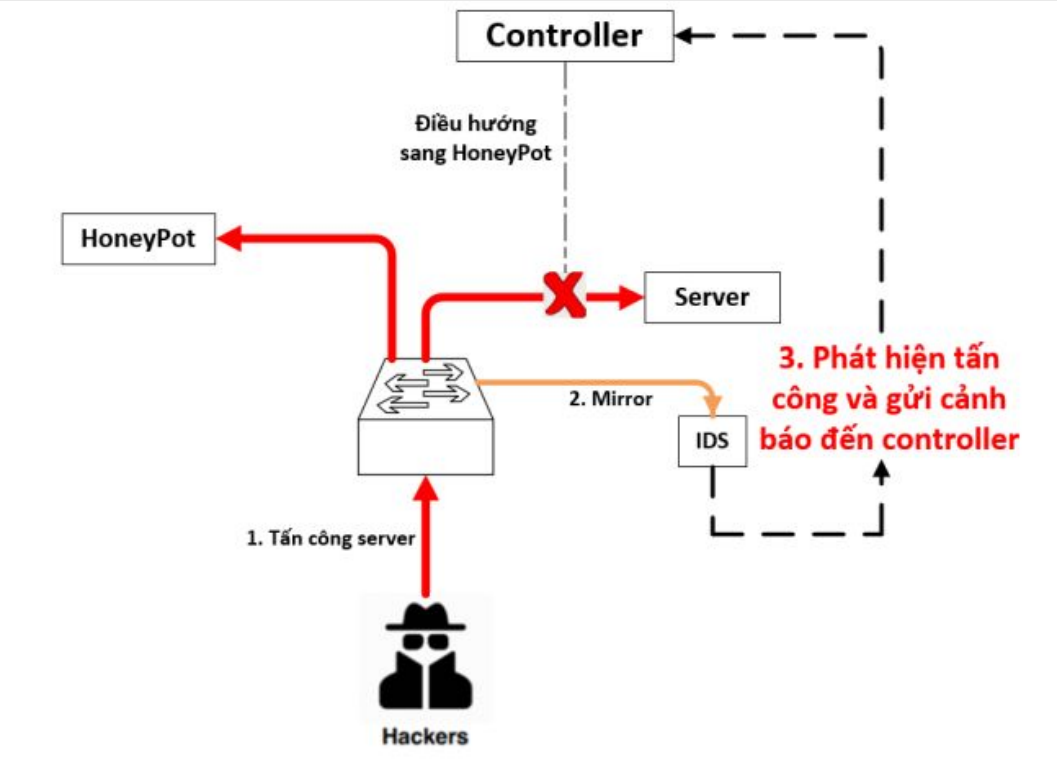
Nội dung 4: Tăng cường dữ liệu dựa trên Cyclegan cho phát hiện tấn công.

Nội dung và Phương pháp



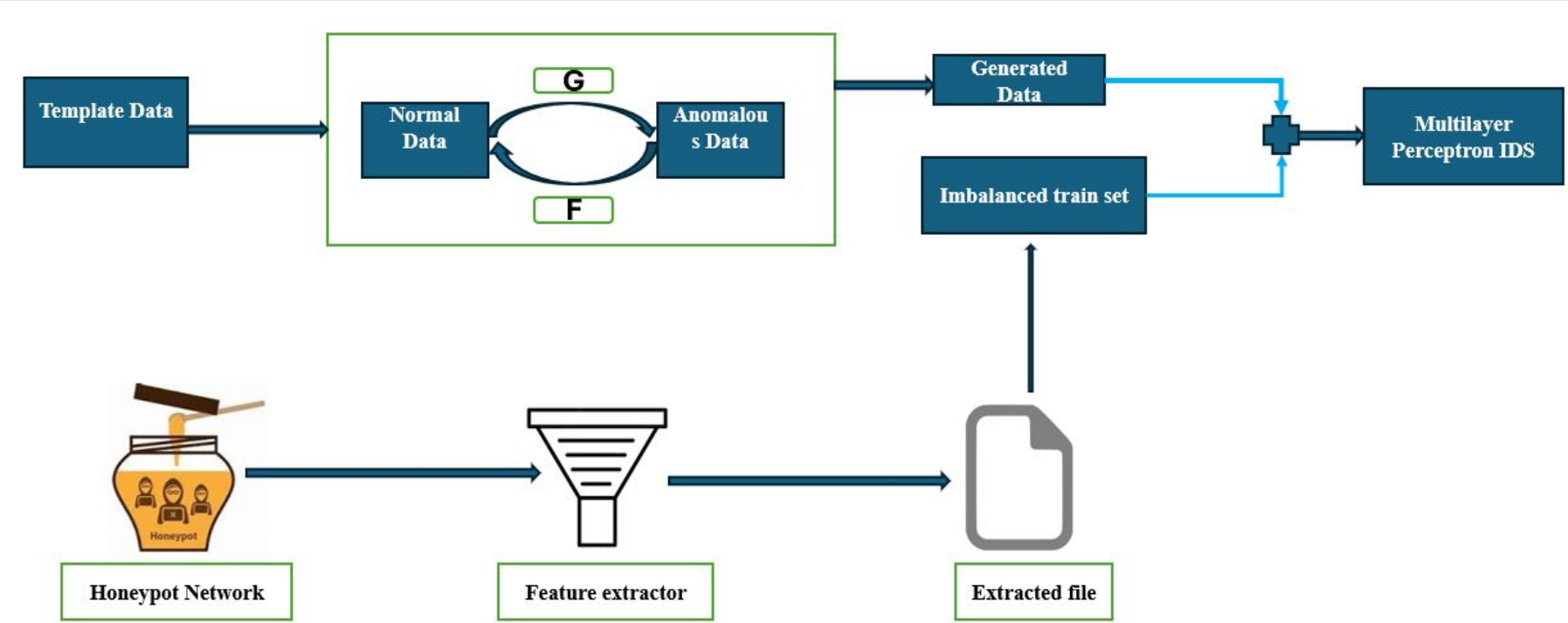
Sơ đồ hệ thống Cyber Deception trong mạng khả lập trình (SDN)

Nội dung và Phương pháp



Luồng hoạt động của hệ thống Cyber Deception trong mạng SDN

Nội dung và Phương pháp



Mô hình thiết kế kết hợp Cyber Deception với CycleGAN để tái huấn luyện IDS

Kết quả dự kiến

- Triển khai IDS dựa trên phương pháp học máy
- Triển khai Cyber Deception trong mạng khả lập trình để đánh lừa kẻ tấn công, từ đó thu thập được các IOCs, các chiến thuật, chiến lược và dữ liệu tấn công nhằm xây dựng hệ thống phòng thủ chủ động, dữ liệu tấn công làm cơ sở để tái huấn luyện mô hình để củng cố khả năng phát hiện tấn công.
- Model CycleGAN có khả năng sinh dữ liệu độc hại để vượt mặt IDS và tái huấn luyện IDS.

Tài liệu tham khảo

[1] Trung Thanh Bui, “SOFTWARE DEFINED NETWORKING – CÔNG NGHỆ MỚI LÀM THAY ĐỔI CẤU TRÚC MẠNG”, 2006.

[2] E. Al-Shaer, J. Wei, K. W. Hamlen, C. Wang, “Autonomous Cyber Deception”, pages 102-119, 2018.

[3] W. Han, Z. Zhao, A. Doupe et al., “HoneyMix: Toward SDN-based Intelligent Honeynet”, 2016.

[4] C. Wang and Z. Lu, “Cyber Deception: Overview and the Road Ahead”, 2018.

[5] Z. Li, Z. Qin, K. Huang, X. Yang and S. Ye, "Intrusion Detection Using Convolutional Neural Networks for Representation Learning," in International Conference on Neural Information Processing ICONIP, 2017.

[6] Tang T.A., McLernon D., Mhamdi L., Zaidi S.A.R., Ghogho M., “Intrusion Detection in SDN-Based Networks: Deep Recurrent Neural Network Approach,” in Advanced Sciences and Technologies for Security Applications, volume Deep Learning Applications for Cyber Security, Springer, Cham, 2019.