PHÁT HIỆN TẤN CÔNG DDOS ĐỐI KHÁNG BẰNG MÔ HÌNH GAN VỚI BỘ PHÂN BIỆT KÉP (GAN-DD)

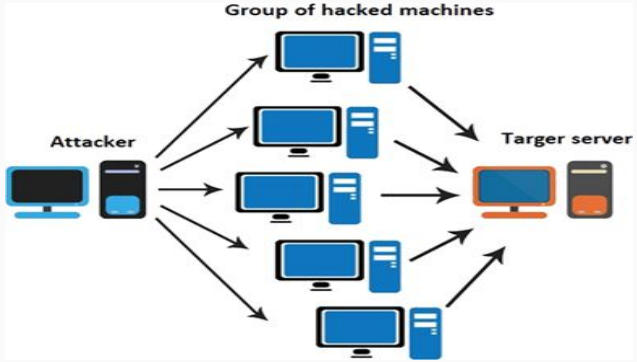
Kiều Hồng Khang - 240201042

Tóm tắt

- Lớp: CS2205.FEB2025
- Link Github của nhóm:
- Link YouTube video:

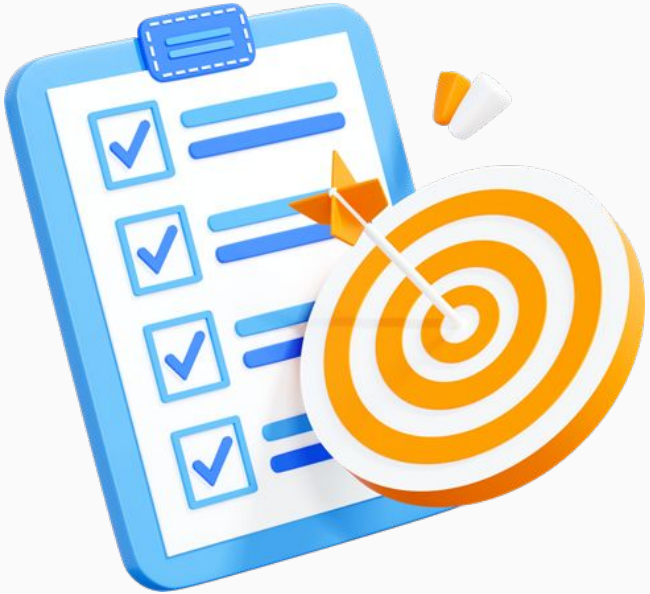
Kiều Hồng Khang

Giới thiệu



- Sự gia tăng về tần suất, cường độ và độ phức tạp của cuộc tấn công DDoS.
- Hạn chế về huấn luyện, thu thập dữ liệu, đánh giá và kiểm tra của các phương pháp ML và DL.
- Tấn công DDoS với lưu lượng tấn công đối nghịch là một kỹ thuật tiên tiến.
- GANDD là giải pháp dựa trên GAN với thiết kế gồm bộ phân biệt đối xử kép giúp cải thiện khả năng phát hiện tấn công DDoS.

Mục tiêu

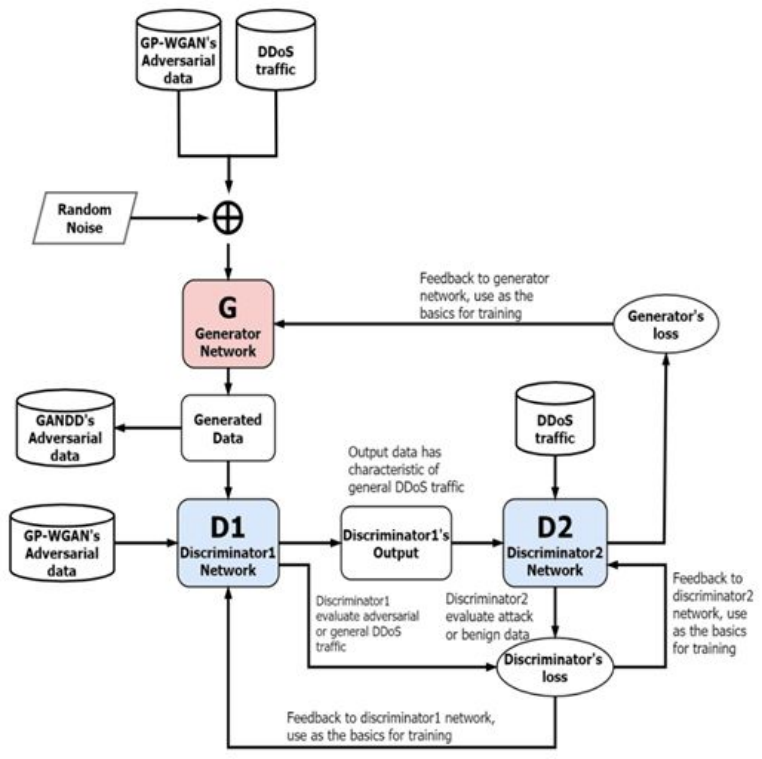


- Phát triển mô hình GAN-DD phát hiện DDoS đối kháng với độ chính xác cao.
- Đánh giá hiệu quả mô hình trên dữ liệu thực và dữ liệu bị nhiễu.
- Đề xuất hướng triển khai GAN-DD trong hệ thống mạng thực tế.

Nội dung và Phương pháp

Nội dung

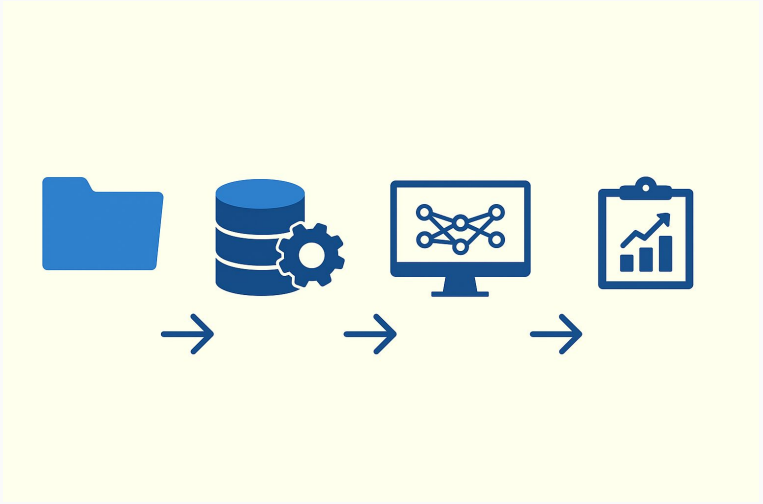
- Khảo sát các phương pháp phát hiện tấn công DDoS truyền thống.
- Tìm hiểu mô hình GANDD.
- Ứng dụng GANDD vào phát hiện tấn công DDoS.
- Đánh giá hiệu quả của GANDD.
- Phân tích thách thức và giải pháp.



Nội dung và Phương pháp

Phương pháp

- Tiền xử lý dữ liệu
- Xây dựng mô hình GAN-DD
- Huấn luyện mô hình
- Đánh giá hiệu quả
- Phân tích kết quả



Kết quả dự kiến

Việc ứng dụng GANDD (Generative Adversarial Networks with Dual Discriminators) vào phát hiện tấn công DDoS mang lại nhiều kết quả mong đợi bao gồm:

- Phát triển mô hình GAN-DD có khả năng phát hiện hiệu quả các cuộc tấn công DDoS, kể cả khi dữ liệu bị nhiễu đối kháng.
- Đạt độ chính xác trên 90%, F1-score ≥ 85% trên tập dữ liệu thực nghiệm.
- Hiệu quả mô hình vượt trội so với các phương pháp truyền thống và các biến thể GAN cơ bản.
- Đề xuất giải pháp triển khai mô hình trong môi trường thực tế, đảm bảo hiệu suất và khả năng ứng dụng.

Tài liệu tham khảo

[1]. Goodfellow, I.J.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; Warde-Farley, D.; Ozair, S.; Courville, A.; Bengio, Y. Generative adversarial networks. In Proceedings of the 27th International Conference on Neural Information Processing Systems, Montreal, QC, Canada, 8–13 December 2014; Volume 2, 2672–2680.

[2]. Gulrajani, I.; Ahmed, F.; Arjovsky, M.; Dumoulin, V.; Courville, A.C. Improved training of Wasserstein GANs. In Proceedings of the 31st International Conference on Neural Information Processing Systems, Long Beach, CA, USA, 4–9 December 2017; 5769–5779

[3]. Nguyen, T.D.; Le, T.; Vu, H.; Phung, D. Dual Discriminator Generative Adversarial Nets. In Proceedings of the Advances in Neural Information Processing Systems 30, Long Beach, CA, USA, 4–9 December 2017; pp. 2667–2677.

[4]. Zhang, X.; Zhao, Y.; Zhang, H. Dual-discriminator GAN: A GAN way of profile face recognition. In Proceedings of the 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), Dalian, China, 27–29 June 2020; 162–166

[5] Chin-Shiuh Shieh, Thanh-Tuan Nguyen, Wan-Wei Lin, Yong-Lin Huang, Mong-Fong Horng, Tsair-Fwu Lee, Denis Miu: Detection of Adversarial DDoS Attacks Using Generative Adversarial Networks with Dual Discriminators. Symmetry 14(1): 66 (2022). DOI: 10.3390/sym14010066