NÂNG CAO KHẢ NĂNG ĐÁNH LỪA CỦA HONEYPOT ỨNG DỤNG MÔ HÌNH HỌC TĂNG CƯỜNG DỰA TRÊN LÝ THUYẾT TRÒ CHƠI

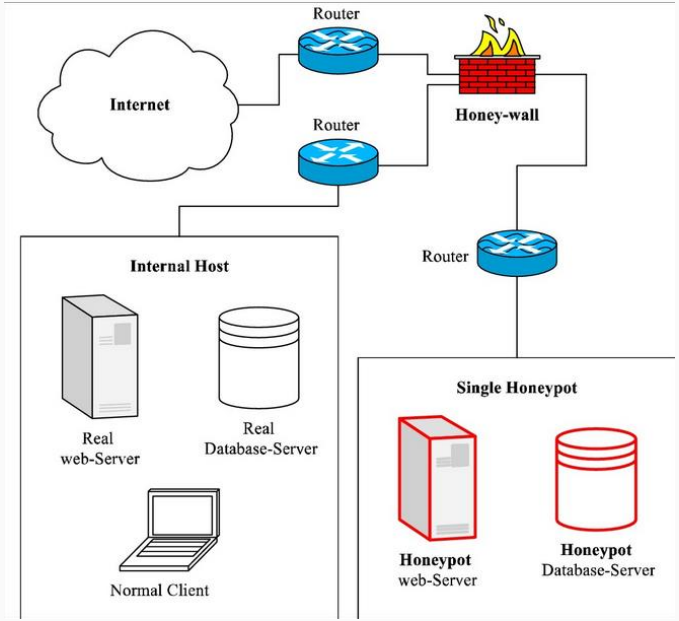
Bùi Chí Trung - 230202019

Tóm tắt

- Lớp: CS2205.CH181
- Link Github: https://github.com/trungbc2711/CS2205.CH181
- Link YouTube video: https://youtu.be/1-tERS5xS_o
- Bùi Chí Trung

Giới thiệu

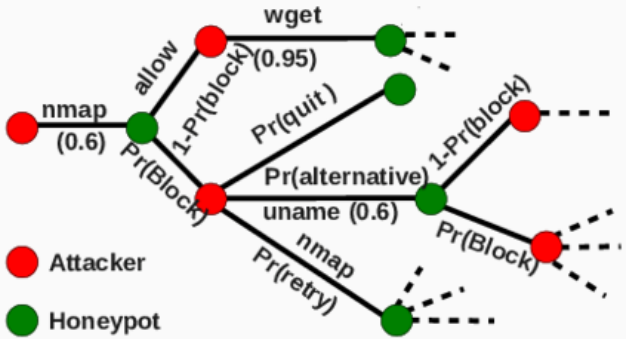
Honeypot là một giải pháp nổi bật trong Defensive Deception, mô phỏng hệ thống thật để thu hút kẻ tấn công.

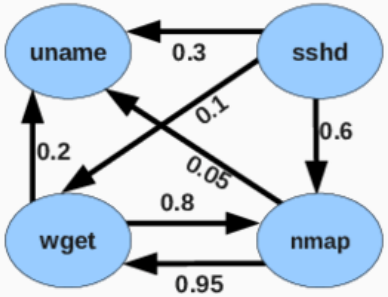


Làm sao để những phản hồi của hệ thống honeypot với những tương tác của kẻ tấn công đảm bảo hai yếu tố: thông tin phản hồi là giả mạo và phải giống thông tin thật nhất có thể?

Giới thiệu

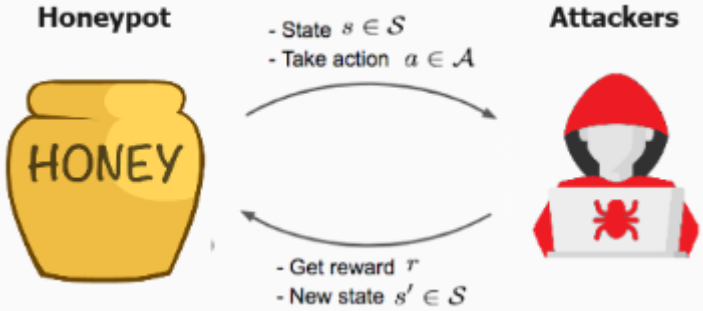
Lý thuyết trò chơi (Game Theory) là mô hình toán học có khả năng phân tích nhiều tình huống có thể xảy ra trước khi xác định hướng hành động thích hợp.





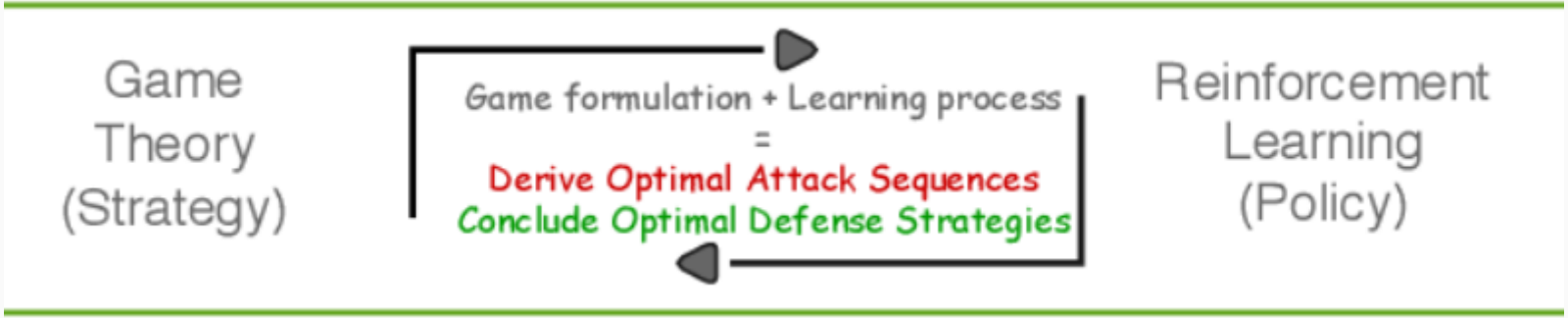
Giới thiệu

Mô hình học tăng cường (Reinforcement Learning) là một phương pháp học máy, trong đó một agent học cách tương tác với môi trường nhằm tối đa hóa một hàm mục tiêu dài hạn thông qua việc nhận thưởng hoặc phạt.

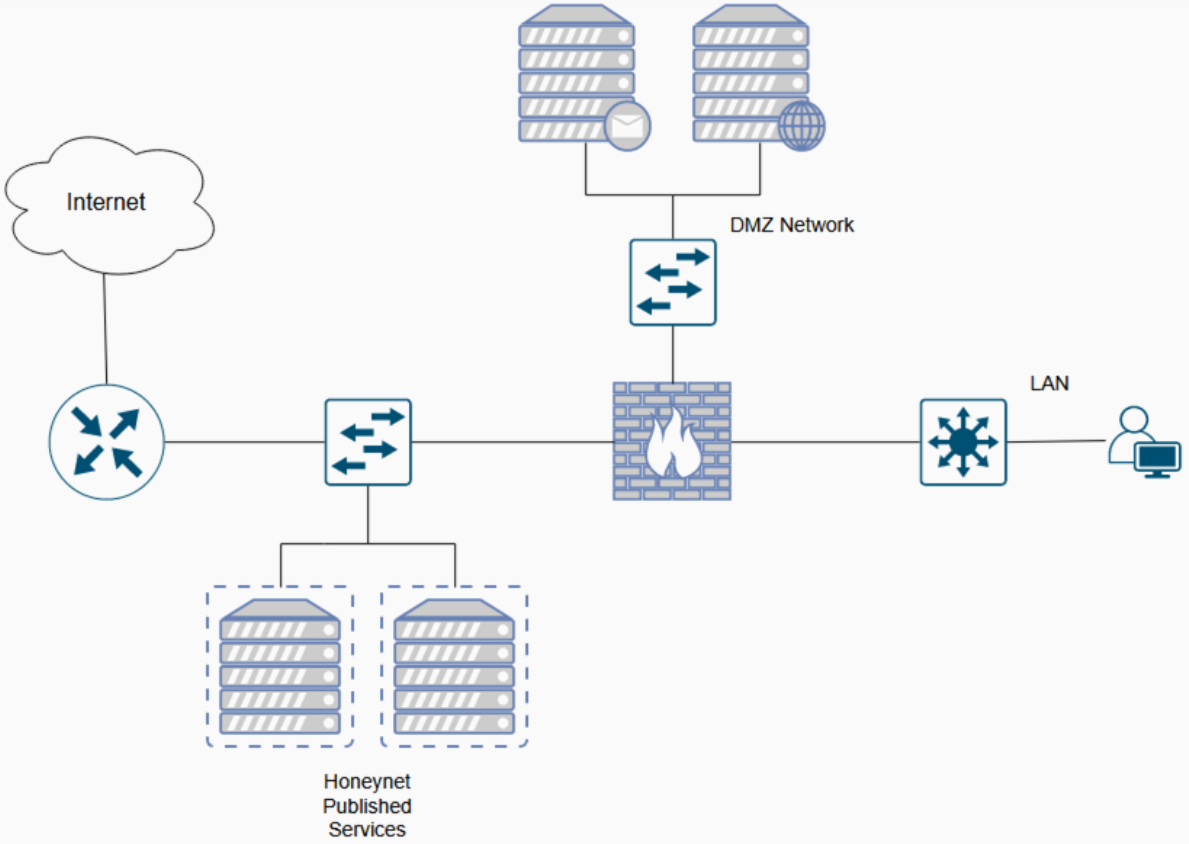


Mục tiêu

- Xây dựng thành công mô hình Reinforcement Learning dựa trên Game Theory có khả năng phân tích tương tác, hành vi của kẻ tấn công.
- Tích hợp mô hình vào hệ thống thật để mô hình tự học các tương tác bên ngoài môi trường lab.



Mục tiêu



Nội dung và Phương pháp

- Nội dung 1: Tìm hiểu về các khái niệm, cấu trúc, phương thức hoạt động và cách tạo ra mô hình Game Theory và Reinforcement Learning.
- Nội dung 2: Tạo ra bộ dữ liệu để huấn luyện mô hình.
- Nội dung 3: Xây dựng và huấn luyện thành công mô hình Reinforcement Learning dựa trên Game Theory.
- Nội dung 4: Đánh giá hiệu suất của mô hình trong môi trường phòng thí nghiệm.
- Nội dung 5: Tiếp lục huấn luyện và đánh giá mô hình trong môi trường thật nhằm kiểm tra tính thực tiễn của đề tài.

Kết quả dự kiến

Hệ thống honeypot đóng giả Web Application Server:

- Tích hợp mô hình Reinforcement Learning dựa trên Game Theory.
- Khả năng phản hồi nhanh những thông tin giả mạo nhưng chân thật.
- Cung cấp dự đoán về hành động, chiến lược của kẻ tấn công cho quản trị viên.
- Có thể ứng dụng vào các môi trường hệ thống công nghiệp.

Tài liệu tham khảo

[1]. Amir Javadpour, Forough Ja'fari, Tarik Taleb, Mohammad Shojafar, Chafika Benzaid; "A comprehensive survey on cyber deception techniques to improve honeypot performance"; Computers & Security 140(4):103792.

[2]. Xiannuan Liang, Yang Xiao; "Game Theory for Network Security"; IEEE Communications Surveys & Tutorials 15(1):472-486.

[3]. Li Zhang, Vrizlynn.L.L. Thing; "Three decades of deception techniques in active cyber defense - Retrospect and outlook"; Computers & Security 106(3):102288.

[4]. Mu Zhu, Ahmed H. Anwar, Zelin Wan, Jin-Hee Cho, Charles Kamhoua, Munindar P. Singh; "A Survey of Defensive Deception: Approaches Using Game Theory and Machine Learning"; IEEE Communications Surveys & Tutorials PP(99):1-1.