


THÔNG TIN CHUNG CỦA BÁO CÁO

<ul style="list-style-type: none">• Họ và Tên: Bùi Chí Trung• MSSV: 230202019 	<ul style="list-style-type: none">• Lớp: CS2205.CH181• Tự đánh giá (điểm tổng kết môn): 8.0/10• Số buổi vắng: 1• Số câu hỏi QT cá nhân: 5• Link Github: https://github.com/trungbc2711/CS2205.CH181• Link Youtube: https://youtu.be/1-tERS5xS_o
---	---

ĐỀ CƯƠNG NGHIÊN CỨU

TÊN ĐỀ TÀI (IN HOA)

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

TÊN ĐỀ TÀI TIẾNG ANH (IN HOA)

ENHANCING THE DECEPTIVE CAPABILITIES OF HONEYPOT USING GAME THEORY-BASED REINFORCEMENT LEARNING MODEL

TÓM TẮT

Phòng thủ chủ động là một phương pháp đầy hứa hẹn trong an ninh mạng, khác biệt so với phòng thủ truyền thống. Defensive Deception là một kỹ thuật phổ biến trong phòng thủ chủ động, giúp người phòng thủ dự đoán và đánh lừa kẻ tấn công bằng cách dẫn chúng vào hệ thống bẫy để theo dõi và hiểu rõ chiến lược của chúng. Honeypot, một giải pháp nổi bật trong Defensive Deception, mô phỏng hệ thống thật để thu thập thông tin chi tiết về các kỹ thuật và chiến lược tấn công. Dù hiệu quả, honeypot đòi hỏi sự quản lý cẩn thận để đảm bảo phản hồi giả mạo nhưng chân thật. Lý thuyết Trò chơi và mô hình Học tăng cường đã được áp dụng trong hai thập kỷ qua để giải quyết các vấn đề này, cho phép phân tích nhiều tình huống và hỗ trợ ra quyết định. Đề tài này đề xuất một mô hình Học tăng cường dựa trên Lý thuyết Trò chơi, với hệ thống honeypot và kẻ tấn công là hai người chơi. Mô hình này phân tích tương tác của kẻ tấn công để đưa ra phản hồi giả mạo nhưng chân thật, đồng thời dự đoán hành động tiếp theo của kẻ tấn công và đề xuất đối sách phù hợp. Ngoài ra, tính thực tiễn của đề tài cũng sẽ được xem xét.

GIỚI THIỆU

Phương thức đánh lừa trong phòng thủ (Defensive Deception) là một trong số những phương thức được triển khai phổ biến khi nhắc đến phòng thủ chủ động. Thông qua Defensive Deception, người phòng thủ có thể đoán trước được hành động của kẻ tấn công; đánh lừa hoặc thu hút kẻ tấn công vào một hệ thống bẫy có sẵn nhằm theo dõi và

tìm ra chiến lược tấn công. Honeypot là một trong những giải pháp nổi bật hoạt động trên lý thuyết này bằng cách mô phỏng lại hệ thống thật. Các honeypot có tính tương tác cao thường được triển khai nhằm cung cấp một môi trường thực tế mô phỏng chặt chẽ các hệ thống và dịch vụ. Chúng tạo điều kiện cho sự tương tác sâu rộng với những kẻ tấn công, khiến chúng trở nên hiệu quả trong việc thu thập thông tin chuyên sâu về các kỹ thuật và chiến lược tấn công [1]. Tuy nhiên, sự phức tạp của chúng đòi hỏi phải có sự quản lý cẩn thận. Một trong số đó là 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. Có thể thấy được, cuộc đối đầu giữa hệ phòng thủ và những kẻ tấn công là một trò chơi chiến lược. Trong suốt hai thập kỷ vừa qua, vô số phương pháp dựa trên Lý thuyết Trò chơi (Game Theory) đã được nhiều nhà nghiên cứu đề xuất nhằm giải quyết vấn đề kể trên [3]. Một mô hình dựa trên Game Theory có khả năng phân tích nhiều tình huống có thể xảy ra (lên tới hàng trăm nghìn) trước khi xác định hướng hành động thích hợp [2]. Điều này có thể nâng cao đáng kể quá trình ra quyết định của người quản trị. Bên cạnh áp dụng Game Theory, một vài mô hình học tăng cường (Reinforcement Learning) cũng đã được áp dụng để giải quyết vấn đề của honeypot. Tuy nhiên, mỗi mô hình đều có ưu nhược điểm của riêng nó. Với Reinforcement Learning là sự khó khăn trong việc khó khăn trong việc tổng quát hóa kiến thức học được từ một môi trường cụ thể sang các môi trường khác. Còn với Game Theory là quá trừu tượng và không áp dụng trực tiếp được vào các tình huống thực tế, đặc biệt khi các yếu tố con người và cảm xúc đóng vai trò quan trọng. Trong đề tài này, một mô hình học tăng cường (Reinforcement Learning) xây dựng dựa trên Game Theory với hệ thống honeypot và kẻ tấn công là hai người chơi. Khi kết hợp mô hình học tăng cường và mô hình lý thuyết trò chơi, hệ thống có khả năng học từ kinh nghiệm để tối ưu hóa quyết định và tương tác linh hoạt với môi trường động. Bằng cách phân tích những tương tác của kẻ tấn công, mô hình có thể đưa ra các thông tin phản hồi tới kẻ tấn công, đảm bảo hai thuộc tính giả mạo và độ chân thật cao. Ngoài ra, nó cũng có thể dự đoán hành vi của đối thủ dựa trên mô hình trò chơi, và sử dụng thông tin này để đưa ra chiến lược gia cố hệ thống mạng.

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 và đưa ra được các phản hồi đảm bảo tính giả mạo và độ chân thật cao, cũng như cung cấp cho quản trị viên thông tin dự đoán về nước đi tiếp của kẻ tấn công trong phạm vi các cuộc tấn công nằm trong dataset.
- Tích hợp mô hình vào một hệ honeypot nhằm nhận được những tương tác trong môi trường thật, với mong đợi mô hình có hiệu suất không quá chênh lệch khi so với môi trường phòng thí nghiệm.

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.

Phương pháp: Tìm đến các công cụ tìm kiếm, các bài báo khoa học/bài viết liên quan cũng như sử dụng các công cụ hỗ trợ AI như chatGPT, Gemini, ...

Nội dung 2: Tạo ra bộ dữ liệu để huấn luyện mô hình.

Phương pháp: Tìm hiểu về các chiến lược tấn công phổ biến thông qua các framework tiêu chuẩn như ATT&CK, Cyber Kill Chain, ..., sau đó chuẩn hóa các thông số để có thể đưa vào mô hình huấn luyện.

Nội dung 3: Xây dựng và huấn luyện thành công mô hình Reinforcement Learning dựa trên Game Theory.

Phương pháp: Mô hình sẽ được cung cấp các thuộc tính của vùng mạng cần được bảo vệ và được huấn luyện các dấu hiệu, chiến lược của các cuộc tấn công đã được định nghĩa trong bộ dữ liệu với mục đích kiểm tra tính khả thi của đề tài.

Nội dung 4: Đánh giá hiệu suất của mô hình trong môi trường phòng thí nghiệm.

Phương pháp: Mời một số chuyên gia trong lĩnh vực Penetrating Attack tấn công thử vào hệ thống có tích hợp mô hình sử dụng các kỹ thuật, phương pháp đã được định nghĩa trong bộ dữ liệu dùng trong quá trình huấn luyện. Các tiêu chí đánh giá dự kiến bao gồm: Thời gian người tấn công nhận ra đây không phải hệ thống thật, Các loại dữ

liệu hệ thống Honeypot trích xuất ra để sử dụng, Độ tối ưu tài nguyên khi tích hợp mô hình vào hệ thống Honeypot.

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.

Phương pháp: Mời một số chuyên gia trong lĩnh vực Penetrating Attack thực hiện các cuộc tấn công vào hệ thống có tích hợp mô hình đang đóng giả là một Web Application Server nhưng không ràng buộc về các kỹ thuật sử dụng. Các tiêu chí đánh giá gồm những mục trong nội dung 4 và thêm hai tiêu chí là: Độ phức tạp của cuộc tấn công và Cách hệ thống honeypot ảnh hưởng đến chiến thuật của người tấn công.

KẾT QUẢ MONG ĐỢI

Sau khi thực hiện hành công tất cả nội dung đã đề ra ở trên, kì vọng đặt ra ở đề tài sẽ thu được thành phẩm là một hệ thống honeypot đóng giả Web Application Server được tích hợp mô hình Reinforcement Learning, có khả năng phản hồi nhanh những thông tin giả mạo nhưng đầy tính chân thật với từng tương tác của kẻ tấn công nhằm dẫn dắt kẻ tấn công ra khỏi tài sản có giá trị cao trong hệ thống mạng. Ngoài ra cũng cung cấp thêm cho quản trị viên hệ thống dự đoán về những hành động, chiến lược có thể được kẻ tấn công sử dụng tiếp theo giúp quản trị viên có thể đưa ra các quyết sách gia cố hệ thống phù hợp. Một yếu tố cũng không thể không xét đến chính là việc mô hình này có thể được 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; May 2024.
- [2]. Xiannuan Liang, Yang Xiao; “Game Theory for Network Security”; IEEE Communications Surveys & Tutorials 15(1):472-486; 12 July 2012.
- [3]. Li Zhang, Vrizlynn.L.L. Thing; “Three decades of deception techniques in active cyber defense - Retrospect and outlook”; Computers & Security 106(3):102288; July 2021.

[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; 06 August 2021.