Môn học: Phương pháp học máy trong an toàn thông tin

TOPIC : PROPOSAL FOR PROJECT

Nhóm: G06

1. THÔNG TIN CHUNG:

Lớp: NT522.N21.ATCL

STT	Họ và tên	MSSV
1	Đỗ Quang Thắng	20521893
2	Nguyễn Đoàn Thiên Cung	20521146
3	Vũ Trọng Nghĩa	20520651

2. TABLE OF CONTENTS:

1.So sánh 2 bài báo 1
2. Xây dựng proposal 4

SO SÁNH BÀI BÁO KHOA HỌC

	Adv-Bot: Realistic Adversarial Botnet Attacks against Network Intrusion Detection Systems	Crafting Adversarial Example to Bypass Flow-&ML- based Botnet Detector via RL
Mục tiêu &phương pháp nghiên cứu	tập trung vào phát triển một phương pháp phát hiện botnet mới dựa trên các tính năng học máy có thể đạt được hiệu suất.	tập trung vào phân tích cách tạo ra các ví dụ thử nghiệm tấn công bằng cách sử dụng học tăng cường để đánh lừa các máy chủ phát hiện botnet dựa trên luồng và máy học.
ứng dụng	có thể được ứng dụng để phát triển các phương pháp phát hiện mối đe dọa mạng mới và cải thiện hiệu suất của hệ thống phát hiện	có thể được ứng dụng để phát triển các phương pháp tấn công mới và cải thiện khả năng phát hiện mối đe dọa mạng.
Ưu điểm	có thể đạt được hiệu suất cao hơn so với các phương pháp truyền thống.	sử dụng học tăng cường để tạo ra các ví dụ thử nghiệm tấn công, giúp đánh lừa các máy chủ phát hiện botnet dựa trên luồng và máy học tăng khả năng phát hiện các mối đe dọa.
Nhược điểm	tập trung vào việc phát triển phương pháp phát hiện botnet mới, nhưng không đề cập đến các phương pháp tấn công.	tập trung vào việc phát triển phương pháp tấn công, nhưng không đề cập đến các phương pháp đối phó.
Method	đề xuất một thuật toán đối nghịch để tạo ra lưu lượng truy cập botnet đối nghịch có thể trốn tránh sự phát hiện bởi các hệ thống phát hiện xâm nhập dựa trên mạng máy học (NIDS).	tăng cường học (RL) để bỏ qua các máy dò botnet dựa trên máy học (ML). Tác giả đào tạo một agent RL để sửa đổi luồng lưu lượng truy cập botnet theo cách tránh bị phát hiện mà không ảnh hưởng đến chức năng của botnet.

Đánh giá	thuật toán được đề xuất đã có thể tạo ra lưu lượng truy cập botnet đối thủ hợp lệ có thể trốn phát hiện bởi các hệ thống phát hiện xâm nhập dựa trên mạng học (NIDS) dựa trên máy học trong một thiết lập blackbox	có hiệu quả trong việc trốn tránh phát hiện mà không sửa đổi mã nguồn botnet hoặc ảnh hưởng đến tiện ích botnet.

- Sau khi so sánh nhóm em đã chọn bài "Crafting Adversarial Example to Bypass Flow-&ML- based Botnet Detector via RL" vì ưu điểm sau :

- Hiệu quả: Sử dụng kỹ thuật Reinforcement Learning có thể giúp tạo ra các tấn công Adversarial Example hiệu quả hơn. Với việc sử dụng kỹ thuật này, các tấn công Adversarial Example có thể được tạo ra nhanh hơn và đạt được mức độ độc hại cao hơn.

- Tính toán: Việc tạo ra các tấn công Adversarial Example thực tế trong bài báo thứ nhất đòi hỏi nhiều thời gian và công sức tính toán. Sử dụng kỹ thuật Reinforcement Learning có thể giúp tiết kiệm thời gian và công sức tính toán.

- Kiểm soát: Việc tạo ra các tấn công Adversarial Example thực tế có thể gây ra những tác động không mong muốn đến hệ thống nghiên cứu. Sử dụng kỹ thuật Reinforcement Learning có thể giúp kiểm soát rủi ro và giảm thiểu các tác động không mong muốn đến hệ thống.

- Khả năng tái sử dụng: Các tấn công Adversarial Example được tạo ra bằng kỹ thuật Reinforcement Learning có thể được tái sử dụng cho nhiều mục đích khác nhau, trong khi các tấn công Adversarial Example thực tế thường chỉ có thể được sử dụng cho một mục đích cụ thể.

PROPOSAL

Crafting Adversarial Example to Bypass Flow-&ML- based Botnet Detector via RL

Xác định vấn đề	Phương pháp phát hiện Botnet phổ biến hiện nay là sử dụng kỹ thuật luồng dữ liệu (Flow-based) kết hợp với các thuật toán học máy (Machine Learning). Tuy nhiên, các phương pháp này cũng đang đối mặt với những vấn đề về độ chính xác và tính phức tạp. Bài báo này đề xuất xây dựng mẫu đối kháng để vượt qua hệ thống phát hiện Botnet dựa trên Luồng dữ liệu và học máy thông qua Học tăng cường (Reinforcement Learning).
Mục tiêu nghiên cứu:	Sử dụng kỹ thuật Học tăng cường (Reinforcement Learning) để xây dựng mẫu tin đối kháng, làm giảm độ chính xác của hệ thống phát hiện Botnet dựa trên Luồng dữ liệu và Học máy.
Kế hoạch thực hiện	- Tìm hiểu nền tảng về hệ thống phát hiện Botnet dựa trên Luồng dữ liệu và Học máy, cũng như các vấn đề liên quan tác giả đề cập trong bài báo. - Tìm hiểu về kỹ thuật Học tăng cường và cách áp dụng kỹ thuật này vào xây dựng mẫu đối kháng. - Chọn mô hình Học tăng cường phù hợp và thiết kế quá trình học tăng cường. - Thực nghiệm và đánh giá hiệu quả của các mẫu đối kháng được tạo ra.
Phương pháp dự kiến demo	- Thiết lập môi trường thực nghiệm với các máy tính chứa bot, máy chủ điều khiển và hệ thống phát hiện Botnet, trong đó sử dụng các thuật toán học máy và phương pháp luồng để phân tích dữ liệu. - Huấn luyện mô hình học tăng cường để tạo ra các mẫu đối kháng. - Sử dụng các mẫu đối kháng cho hệ thống phát hiện Botnet và đánh giá hiệu quả của chúng.

	- Trình bày kết quả thực nghiệm và đề xuất giải pháp cải tiến hệ thống phát hiện Botnet trước các mẫu đối kháng.