ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC
CÔNG NGHỆ THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc Lập - Tự Do - Hạnh Phúc

ĐĂNG KÝ ĐỀ TÀI KHÓA LUẬN TỐT NGHIỆP

TÊN ĐỀ TÀI: TRIỂN KHAI HONEYPOT KẾT HỢP VỚI DEEP LEARNING ĐỂ MÔ PHỎNG HÀNH VI MÁY CHỦ

TÊN ĐỀ TÀI TIẾNG ANH: HONEYPOT IMPLEMENTATION BASED ON DEEP LEARNING TO SIMULATE SERVER BEHAVIOR

Cán bộ hướng dẫn:

Thời gian thực hiện: Từ ngày …/2024 đến ngày …/2024.

Sinh viên thực hiện:

Nguyễn Hoàng Thảo Quyên - 230202014 **Lớp:** CS2205.CH181

Email: quyennht.18@grad.uit.edu.vn **Điện thoại:**

Nội dung đề tài:

Giới thiệu:

Trong thế giới công nghệ ngày nay, với sự phát triển không ngừng của công nghệ internet, mối đe dọa về an ninh mạng ngày càng trở nên nghiêm trọng và phức tạp hơn bao giờ hết. Để bảo vệ mạng lưới của khỏi các cuộc tấn công mạng, các chuyên gia an ninh đang ngày càng quan tâm đến việc sử dụng honeypot - một công cụ mạng được thiết kế để thu hút và ghi lại các cuộc tấn công mạng.

HoneyPots tương tác cấp thấp là loại đơn giản nhất trong các loại honeypot và không mang lại nhiều nguy cơ tiềm ẩn như các loại tương tác cấp cao nhưng chúng lại dễ bị phát hiện bởi nhiều đặc trưng. Điều này sẽ làm giảm hiệu quả trong việc thu thập thông tin về các hành vi tấn công của tin tặc do chúng thường khoog chứa thông tin nên ít hấp dẫn.

Một trong các đặc trưng để phát hiện honetpot tương tác cấp thấp là khả năng tương tác thấp hơn nhiều so với các loại tương tác cấp cao, chúng gần như không thể phản hồi hoặc tương tác với kẻ tấn công một cách linh hoạt. Để giả quyết vấn đề này, chúng tôi đề xuất một mô hình máy học để xây dựng honeypot tương tác cấp thấp một cách thông minh hơn. Mô hình này sẽ được huấn luyện để mô phỏng phản hồi từ máy chủ một cách chân thực, tự động phản hồi và tương tác với các câu lệnh nhận được từ kẻ tấn công.

Bằng cách sử dụng kỹ thuật học máy, honeypot sẽ học từ dữ liệu thực tế thu thập được và tự động điều chỉnh phản hồi của mình, từ đó làm chúng trở nên khó phát hiện hơn. Điều này sẽ nâng cao khả năng thu thập thông tin và phát hiện các mẫu tấn công mới một cách hiệu quả, đồng thời giảm thiểu nguy cơ bị phát hiện dẫn đến giảm hiệu suất của honeypot.

Mô hình học máy này có thể được áp dụng để cải thiện tính bảo mật của hệ thống mạng và nâng cao khả năng phòng thủ chống lại các cuộc tấn công trực tuyến. Đồng thời, nó cũng đem lại lợi ích trong việc nghiên cứu và phát triển các giải pháp an ninh mạng tiên tiến hơn trong tương lai.

Input: các câu lệnh linux được nhập vào từ bàn phím.

Output: phản hồi giống như máy chủ thật, bao gồm việc mô phỏng các tiến trình hệ thống, các sự kiện hệ thống…

Mục tiêu:

- Xây dựng một mô hình mô phỏng hành vi, giới hạn là một máy chủ web, cho honeypot sử dụng thuật toán GAN và RNN. Sử dụng thuật toán Generative Adversarial Network (GAN) để tạo ra các mẫu dữ liệu phản hồi chân thực từ máy chủ. Áp dụng Recurrent Neural Network (RNN)

để mô phỏng các tương tác theo thời gian, phản hồi các câu lệnh của kẻ tấn công một cách liên tục và hợp lý.

- Sử dụng dữ liệu từ nhiều nguồn khác nhau để huấn luyện mô hình máy học này, giúp tăng tính chân thực và hiệu quả của honeypot. Thu thập dữ liệu tấn công mạng từ các nguồn khác nhau bao gồm log server, các cơ sở dữ liệu công cộng về các cuộc tấn công mạng, và các hệ thống honeypot hiện có. Kết hợp và tiền xử lý dữ liệu để tạo ra một bộ dữ liệu huấn luyện đa dạng và phong phú, giúp mô hình học được các hành vi tấn công thực tế và phản hồi một cách chính xác.
- Xây dựng một honeypot áp dụng mô hình mô phỏng đã huấn luyện. Tích hợp mô hình mô phỏng đã được huấn luyện vào hệ thống honeypot. Đảm bảo honeypot có khả năng phản hồi các cuộc tấn công một cách chân thực, bao gồm mô phỏng các tiến trình hệ thống và sự kiện hệ thống giống như một máy chủ web thật. Kiểm thử và đánh giá hiệu suất của honeypot trong việc thu hút và ghi lại các cuộc tấn công, đảm bảo rằng honeypot có thể thu thập thông tin hữu ích về các hành vi tấn công mới một cách hiệu quả.

Phạm vi:

- Dữ liệu được thu thập từ máy chủ sẽ bao gồm cấu hình hệ thống, các tiến trình của các máy chủ thật, các dữ liệu từ syslog để biết được các phản hồi của máy chủ thực đến các câu lệnh nhận vào.
- Máy chủ honeypot sẽ được giới hạn là một máy chủ web nên sẽ nhận thêm các dữ liệu về gói tin mạng như HTTP, HTTPS, DNS.

Đối tượng:

- Sử dụng thuật toán GAN và RNN để tạo mô hình và sử dụng trong đề tài này.

Nội dung:

- Tổng hợp tất cả các dữ liệu thành ba bộ chính để huấn luyện, kiểm tra và xác thực.

- Nghiên cứu các thuật toán học sâu GAN VÀ RNN, xây dựng mô hình học máy, huấn luyện mô hình để xác định độ đo của từng mô hình trên tập dữ liệu.
- Chọn dùng các bộ dữ liệu như Syslog Dataset, HTTP Archive,… để huấn luyện cấu hình hệ thống và các bộ dữ liệu như Apache HTTP Server Logs, Nginx HTTP Server Logs, … để huấn luyện về các gói tin mạng.
- Huấn luyện mô hình theo các bộ dữ liệu trên và đánh giá hệ thống.
- Xây dựng honeypot từ mô hình và chạy thử trên môi trường thực tế.

Phương pháp:

- Nghiên cứu các thuật toán tự sinh câu lệnh và phản hồi của máy Linux như BART-GAN, CodeGAN, LLM-GAN, GPT-3, Linux Command Transformer, Neural Command Prompt, Linux Command Response Prediction, GAN-based Linux Command Generation …
- Huấn luyện mô hình học sâu đã nghiên cứu, đánh giá kết quả.
- Dựng honeypot mã nguồn mở trong môi trường thử nghiệm và tìm cách áp dụng mô hình vừa huấn luyện vào hoặc tạo một honeypot mới từ mô hình.

Kết quả dự kiến:

- Một mô hình học sâu có khả năng phản hồi lại các câu lệnh với mức độ chân thực đạt yêu cầu.
- Một honeypot áp dụng mô hình máy học đã huấn luyện với các thông số đạt yêu cầu có thể phân tích các loại tấn công theo mẫu tấn công và phản hồi dựa theo kết quả phân tích.
- Báo cáo các phương pháp và kỹ thuật của mô hình máy học đã phát triển được. Kết quả thực nghiệm, đánh giá, so sánh với các phương pháp khác.

Tài liệu tham khảo:

[1] Siniosoglou, I., Efstathopoulos, G., Pliatsios, D., Moscholios, I. D., Sarigiannidis, A., Sakellari, G., … Sarigiannidis, P. (2020). NeuralPot: An Industrial Honeypot Implementation Based On Deep Neural Networks. 2020 IEEE Symposium on Computers and Communications (ISCC). doi:10.1109/iscc50000.2020.9219712

[2] Fan, W., Du, Z., Smith-Creasey, M., & Fernandez, D. (2019). HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design. IEEE Journal on Selected Areas in Communications, 1–1. doi:10.1109/jsac.2019.2894307

[3] Jiang, K., & Zheng, H. (2020). Design and Implementation of A Machine Learning Enhanced Web Honeypot System. 2020 13th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI). doi:10.1109/cisp-bmei51763.2020.9263640

[4] Mehta, V., Bahadur, P., Kapoor, M., Singh, P., & Rajpoot, S. (2015). Threat prediction using honeypot and machine learning. 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE). doi:10.1109/ablaze.2015.7155011

[5] Matin, I. M. M., & Rahardjo, B. (2020). The Use of Honeypot in Machine Learning Based on Malware Detection: A Review. 2020 8th International Conference on Cyber and IT Service Management (CITSM). doi:10.1109/citsm50537.2020.9268794

Kế hoạch thực hiện:

+ Tuần 1 - 6: Tìm và chọn các bộ dữ liệu phù hợp với mô hình, chia thành ba bộ. Nghiên cứu mô hình GAN và RNN sử dụng trong đề tài.

Kết quả dự kiến:

- Tài liệu chi tiết cấu trúc các mô hình sử dụng.
- Các bộ dữ liệu được sử dụng để huấn luyện mô hình.

+ Tuần 7 - 12: Huấn luyện thuật toán, ghi chép lại kết quả kèm đánh giá và so sánh.

Kết quả dự kiến:

- Bảng kết quả đánh giá và theo dõi thực nghiệm của thuật toán đã phát triển dựa trên các bộ dữ liệu đã chọn.

+ Tuần 13 - 16: Tìm hiểu các loại honeypot và lựa chọn một honeypot phù hợp để xây dựng chương trình demo trên môi trường thử nghiệm, đồng thời áp dụng các mô hình máy học đã huấn luyện vào chương trình này; hoặc tự dựng một honeypot dựa vào các mã nguồn mở, và áp dụng mô hình đã huấn luyện vào.

Kết quả dự kiến:

- Tài liệu chi tiết cấu trúc mô hình honeypot sử dụng trong đề tài.
- Chương trình honeypot đang chạy đã áp dụng mô hình.

Xác nhận của CBHD (Ký tên và ghi rõ họ tên)	**TP. HCM, ngày….tháng …..năm 2024** **Sinh viên** (Ký tên và ghi rõ họ tên)