NGHIÊN CỨU NÂNG CAO HIỆU QUẢ PHÁT HIỆN THÂM NHẬP MẠNG THEO PHƯƠNG PHÁP THỐNG KÊ BẤT THƯỜNG

Giảng viên hướng dẫn: ts. Nguyễn ĐẠI THỌ
sinh viên: Vũ TRUNG TRIỆU

Nội dung

- Mục đích của đề tài
- Các dạng tấn công thâm nhập mạng
- Phương pháp phát hiện thâm nhập McPAD
- Thử nghiệm McPAD với một số dạng tấn công
- Kết luận

Mục đích của đề tài

- Tìm hiểu về phương pháp phát hiện thâm nhập dựa trên thống kê bất thường McPAD.
- Thử nghiệm McPAD với các dạng tấn công.

Các dạng tấn công thâm nhập mạng

- Tấn công Shellcode
- Tấn công Generic
- Tấn công CLET
- Tấn công Polymorphic Blending (PBAs)
- Tấn công sử dụng Rookit-malware
- Tấn công sử dụng công cụ metasploit

Tấn công shellcode

- Với tấn công Shellcode, kẻ tấn công sẽ cố gắng để tiêm mã độc hại và thực thi bằng cách khai thác một lỗ hổng trên máy mục tiêu.
- Có thể bị phát hiện bởi hệ thống phát hiện xâm nhập dựa trên thống kê bất thường.

Tấn công generic

- Đây là dạng tấn công tổng hợp bao gồm như:
  - Tấn công DoS (Denial-of-Service),
  - Tấn công URL decoding error
  - Tấn công rò rỉ dữ liệu.
  - Tấn công Shellcode

Tấn công CLET

- CLET là công cụ tạo cơ chế đa hình.
- Thêm đệm các byte vào payload tấn công sao cho sự phân bố giống với phân bố byte của một payload thông thường.
- Các shellcode mã hóa trong CLET sử dụng XOR.

Tấn công Polymorphic Blending (PBAs)

- Sử dụng cơ chế đa hình để trốn tránh dựa trên chữ ký IDS.
- Sử dụng phương pháp "*blending*" rải các packet tấn công lên những giá trị byte khác nhau với sự sắp xếp phù hợp sao cho tránh được sự phát hiện của IDS phát hiện dựa trên hành vi bất thường.

Tấn công sử dụng Rootkit-malware

- Rootkit là một dạng phần mềm độc hại (malware)
- Ẩn dấu mã độc hại, ngụy trang cho nó vô hình với người dùng.
- Tạo cửa hậu cho kẻ tấn công trên máy tính mục tiêu

Tấn công sử dụng metasploit

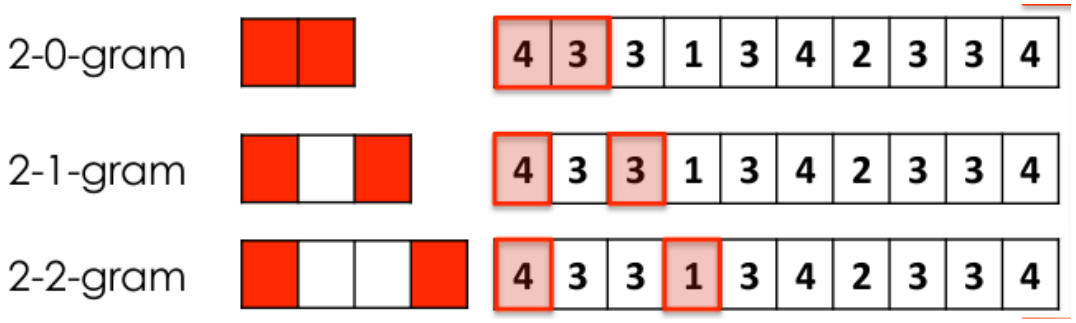
- Metasploit Framework là môi trường kiểm tra, và khai thác các lỗ hổng phần mềm, hệ điều hành.
- Metasploit cập nhật nhanh các mã khai thác trong cơ sở dữ liệu của nó, ngay cả khi là với những lỗ hổng vừa công bố.

Phương pháp phát hiện thâm nhập McPAD

- McPAD viết tắt của Multiple-Classifier Payload-base Anomaly Detector.
- Sử dụng phương pháp phát hiện thâm nhập dựa trên thống kê bất thường.
- Trước đó, PAYL đã sử dụng kĩ thuật phân tích n-gram. Tuy nhiên khi n > 2, số lượng đặc trưng có thể có là > 256^2

Phương pháp phát hiện thâm nhập McPAD

- McPAD sử dụng phương pháp phân tích 2v-gram.
- Trích chọn đặc trưng , tái tạo thông tin trình tự payload
- Giảm kích thước payload



Thử nghiệm McPAD với một số dạng tấn công

- Tấn công shellcode
- Tấn công generic
- Tấn công CLET
- Tấn công Polymorphic Blending (PBAs)
- Tấn công sử dụng Rookit-malware
- Tấn công sử dụng công cụ metasploit

Thử nghiệm các dạng tấn công với tỉ lệ false positive mong muốn là: 0.001%, 0.005%, 0.01%, 0.05%, 0.1%, 0.2%, 0.5%, 1%, 2%, 5%.

Thử nghiệm McPAD với một số dạng tấn công

Shellcode	Generic	CLET	Rookit-malware	Metasploit
0.967742	0.737864078	0.99747	0.798319328	0.798319328
0.967742	0.757281553	1	0.936134454	0.936134454
0.967742	0.737864078	0.99874	0.556302521	0.556302521
0.967742	0.854368932	1	0.821848739	0.821848739
0.967742	0.810679612	1	0.907563025	0.907563025
0.967742	0.854368932	0.95652	0.878991597	0.878991597
0.967742	0.917475728	1	0.803697479	0.803697479
0.967742	0.849514563	1	0.981512605	0.981512605
0.967742	0.967741936	0.95652	0.94789916	0.94789916
0.967742	0.844660194	0.95652	0.91092437	0.91092437

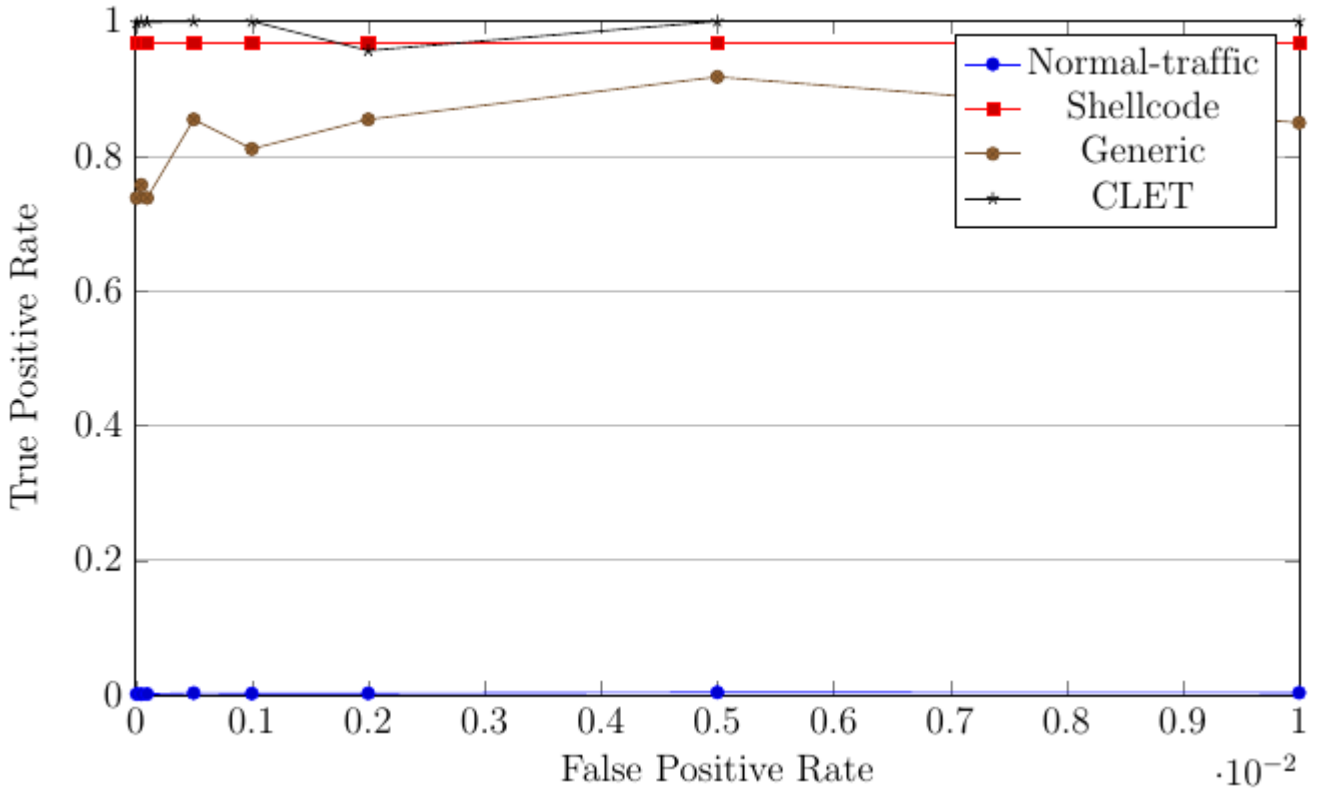
Thử nghiệm McPAD với một số dạng tấn công

Tỉ lệ phát hiện tấn công PBA.

2-gram	4-gram	12-gram	2-all-gram
0.2786726804	0.2557165862	0.8801932367	0.569823435
0.3244201031	0.5423510467	0.9996779388	0.6709470305
0.2780283505	0.4892109501	0.9971014493	0.9219903692
0.3244201031	0.5423510467	0.9996779388	0.6709470305
0.3337628866	0.5246376812	1	0.7990369181
0.3244201031	0.5423510467	0.9996779388	0.6709470305
0.3244201031	0.5423510467	0.9996779388	0.6709470305
0.2728737113	0.4837359098	0.998389694	0.6054574639
0.4951675258	0.5465378422	1	0.9990369181
0.2728737113	0.5342995169	0.9996779388	0.8112359551

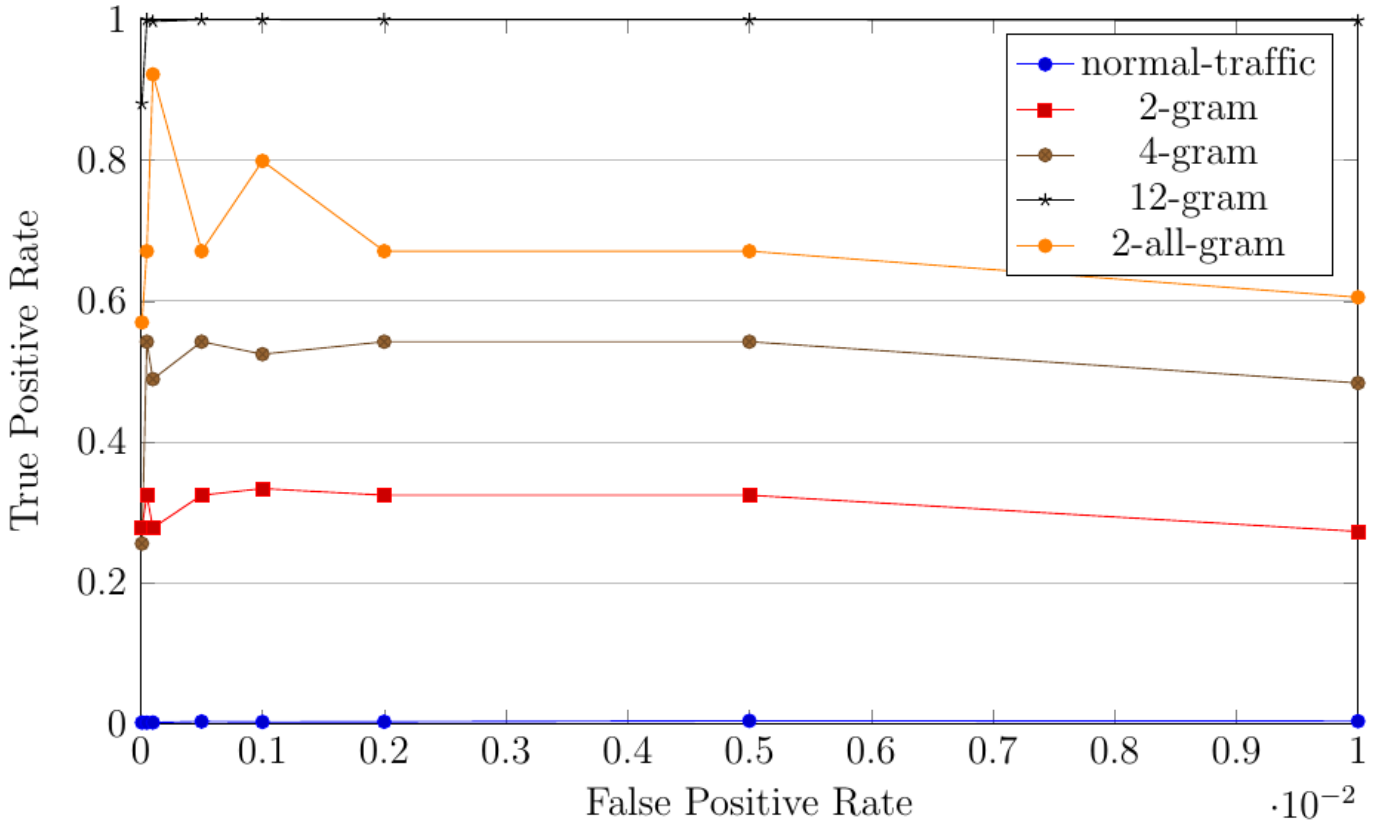
Thử nghiệm McPAD với một số dạng tấn công

Đường cong ROC cho tấn công Shellcode, Generic, CLET



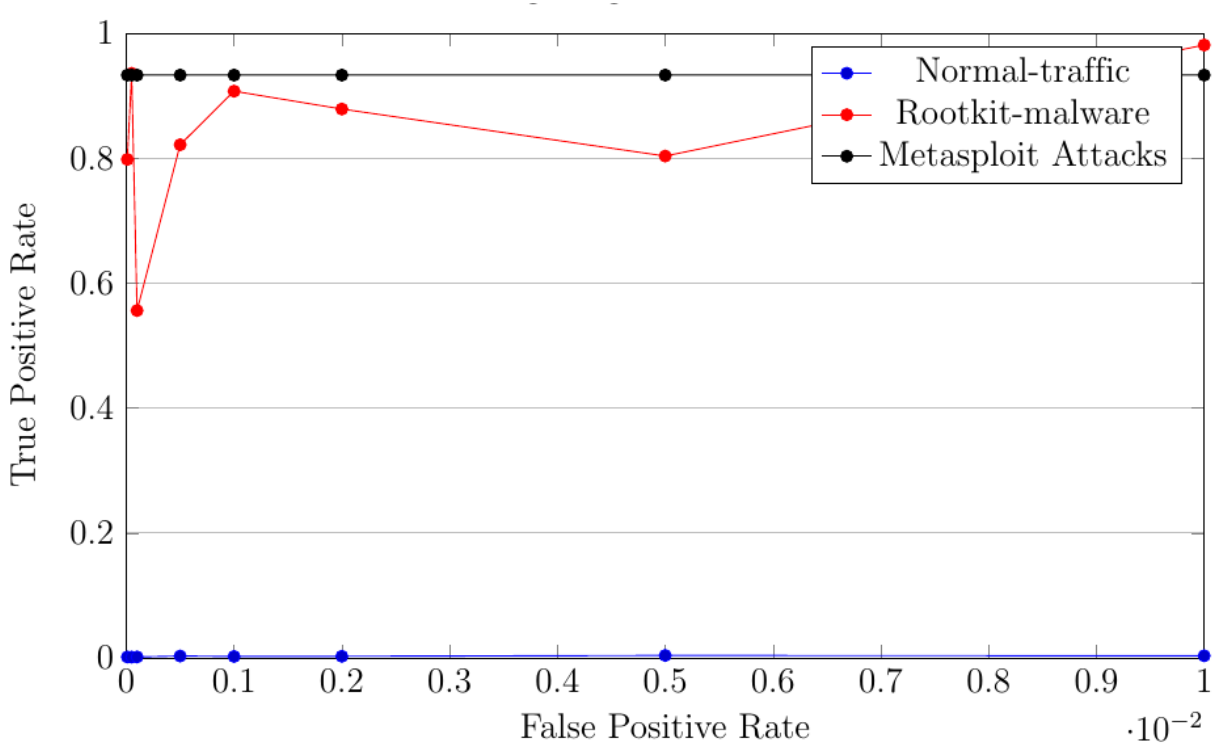
Thử nghiệm McPAD với một số dạng tấn công

- Đường cong ROC cho tấn công PBAs



Thử nghiệm McPAD với một số dạng tấn công

•Đường cong ROC cho tấn công sử dụng Rootkit-malware, công cụ metasploit



Kết luận

- Đã thử nghiệm McPAD với nhiều dạng tấn công và kết quả cho tỉ lệ phát hiện tốt, đặc biệt rất chính xác trong phát hiện tấn công dạng shellcode, đa hình CLET.
- Có thể phát hiện các cuộc tấn công vào các lỗ hổng mới.
- Tuy nhiên,McPAD tỉ lệ phát hiện một số tấn công PBA còn thấp.

Cảm ơn thầy cô và các bạn đã lắng nghe