Đại học Quốc gia Thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO

Môn học: IDPS

Kỳ báo cáo: First proposal (Session 0)

Tên chủ đề: First proposal

GV: Vũ Đức Lý

Ngày báo cáo: 23/9/2023

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn
2	Nguyễn Bùi Kim Ngân	20520648	20520648@gm.uit.edu.vn
3	Nguyễn Bình Thục Trâm	20520815	20520815@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	Mục tiêu của project	100%	
2	Lý do chọn project	100%	
3	Phương thức làm project	100%	
4	Kết quả mong đợi	100%	

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Tên đề tài: Thực nghiệm các tool IDPS dựa trên kịch bản tấn công và thực hiện đánh giá

Các tool dự kiến: (chọn 2 tool cho đồ án cuối kỳ)

- Snort
- Suricata
- Zeek
- Wazzuh
- Security Onion

1. Mục tiêu của project

Mục tiêu của dự án là thực nghiệm và đánh giá các công cụ Intrusion Detection and Prevention System (IDPS) dựa trên các kịch bản tấn công như:

- (Mutation) Malware
- DOS/DDOS
- Exploitation
- Monitor app (user behavior)
- Malicious traffic

Mục tiêu cụ thể bao gồm:

- Xác định hiệu suất của các công cụ IDPS trong việc phát hiện và ngăn chặn các loại tấn công khác nhau.
- Đánh giá tính năng, khả năng linh hoạt và tích hợp của mỗi công cụ IDPS.
- So sánh và xác định ưu điểm và hạn chế của từng công cụ IDPS trong ngữ cảnh các kịch bản tấn công đã chọn.

2. Lý do chọn project

Lý do chọn project:

- Nâng cao hiểu biết về IDPS: Dự án này được lựa chọn để cung cấp một cái nhìn sâu hơn vào tính năng và hiệu suất của các công cụ IDPS, giúp nâng cao hiểu biết về cách chúng hoạt động và cách chúng có thể bảo vệ mạng.
- Cập nhật kiến thức về tấn công mạng: Bằng cách thực nghiệm các kịch bản tấn công đa dạng, dự án này giúp cập nhật kiến thức về các mối đe dọa mạng mới nhất và cách chúng tác động lên hệ thống.

- Tăng cường khả năng bảo mật: Hiểu rõ cách hoạt động của các công cụ IDPS và khả năng của chúng trong việc phát hiện và ngăn chặn tấn công, từ đó giúp cải thiện khả năng bảo mật cho mạng và hệ thống.

3. Phương thức làm project

Phương pháp thực hiện:

- Lựa chọn công cụ IDPS: Chọn các công cụ IDPS phổ biến và đáng quan tâm để thực hiện các thử nghiệm dựa trên kịch bản tấn công đã nêu.
- Thiết kế môi trường thử nghiệm: Xây dựng môi trường thử nghiệm chứa các thành phần mạng và ứng dụng để phù hợp với mỗi kịch bản tấn công.
- Triển khai kịch bản tấn công và công cụ IDPS: Triển khai các kịch bản tấn công đã nêu và cấu hình các công cụ IDPS tương ứng để phát hiện và ngăn chặn tấn công.
- Thu thập dữ liệu và đánh giá: Tiến hành thực nghiệm, thu thập dữ liệu về hiệu suất của các công cụ IDPS và đánh giá theo các tiêu chí đã đề ra.

4. Kết quả mong đợi

Kết quả mong đợi:

- Đánh giá hiệu suất: Mong đợi thu được một đánh giá chính xác về khả năng phát hiện và ngăn chặn của mỗi công cụ IDPS đối với các kịch bản tấn công đã chọn.
- So sánh tính năng và linh hoạt: Đánh giá và so sánh tính năng, khả năng linh hoạt và tích hợp của các công cụ IDPS để xác định ưu điểm và hạn chế của mỗi công cụ.
- Đề xuất cải tiến: Dựa trên kết quả thu được, đề xuất cải tiến cho từng công cụ IDPS và phương pháp triển khai để nâng cao hiệu suất và tính linh hoạt.

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

  *Ví dụ: [*NT101.K11.ANTT*]-Session1_Group3.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT