BÁO CÁO CUỐI KỲ
Nhóm 7
2023-2024

NT330.O21.ANTT
An Toàn Mạng Không Dây

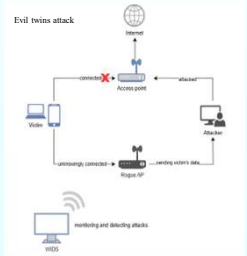
Tìm hiểu và Xây dựng thử nghiệm hệ thống WIDS

Nguyễn Lê Thảo Ngọc , Hồ Công Long
University of Information Technology

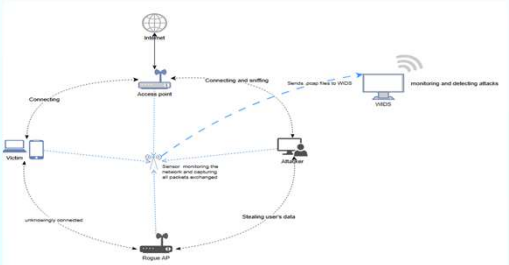
INTRODUCTION

Ngày nay với sự phát triển mạnh mẽ của công nghệ, mạng Wifi (đặc biệt là chuẩn 802.11) đã và đang trở thành thành phần không thể thiếu trong cuộc sống hàng ngày của con người. Sự ứng dụng rộng rãi này khiến mạng Wifi trở thành đối tượng hấp dẫn bị nhiều kẻ xấu nhắm tới nhằm khai thác thông tin và dữ liệu người dùng một cách trái phép, do đó chúng cần phải thực hiện các biện bảo vệ thích hợp như là sử dụng hệ thống WIDS hoặc WIPS nhằm kịp thời phát hiện và ngăn chặn cuộc tấn công mạng không dây. Trong đề tài này, nhóm sẽ chỉ làm việc với mạng không dây sử dụng giao thức mã hoá WPA2 để tái hiện lại các cuộc tấn công đơn giản và biểu diễn khả năng phát hiện cuộc tấn công của hệ thống WIDS mà nhóm triển khai.

Kịch bản tấn công



Kiến trúc triển khai

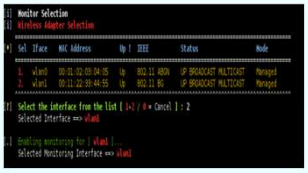


Method

Nhóm sử dụng phần mềm WIDS mã nguồn mở tại (1) để triển khai hệ thống WIDS và thực hiện một số chỉnh sửa để chạy trên Python3 và môi trường Kali Linux

Hệ thống WIDS này sẽ sniff các lưu lượng truy cập trong môi trường mạng không dây để phát hiện các tín hiệu đáng ngờ như các gói tấn công WEP/WPA/WPS.

Phần mềm này sẽ quét thông tin các interface có trên máy là WIDS server rồi yêu cầu chúng ta chọn interface để tiến hành thu thập và giám sát lưu lượng mạng



Purpose

+ Phát hiện các gói tin deauthentication được gửi hàng loạt đến Client hoặc Access point với số lượng không hợp lý

+ Phát hiện sự thay đổi AP mà Client kết nối tới

+ Phát hiện lưu lượng giao tiếp không hợp lý giữa Client và AP

+ Phát hiện nhiều gói tin được gửi liên tục đến Access point bằng địa chỉ MAC broadcast

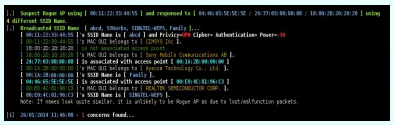
(1) https://github.com/SYWorks/wireless-ids.git

Results

Sau khi thực hiện tấn công Beacon flood, WIDS phát hiện rất nhiều mạng wifi giả.

Sau khi thực hiện tấn công Authentication attack, WIDS phát hiện xuất ra thông báo cảnh báo về cuộc tấn công.

Tạo access point giả rồi tấn công Evil twins. WIDS xuất ra thông báo về Access point giả này với các đặc điểm bất thường của nó.



Conclusions

Trong đồ án này, chúng em đã nghiên cứu và phát triển một hệ thống phát hiện xâm nhập không dây (WIDS) nhằm tăng cường bảo mật cho mạng không dây. Mục tiêu chính của đồ án là xây dựng một hệ thống có khả năng phát hiện các cuộc tấn công phổ biến trong mạng không dây và đưa ra các cảnh báo kịp thời.

Kết quả thực nghiệm cho hệ thống WIDS của chúng em có thể phát hiện hiệu quả các loại tấn công như tấn công giả mạo (spoofing), tấn công từ chối dịch vụ (DoS),... Hệ thống sử dụng các phương pháp phát hiện dựa trên chữ ký và quy tắc để phân tích và nhận diện các hoạt động bất thường trong mạng.