BÁO CÁO CUỐI KỲ Nhóm 7 2023-2024

NT330.021.ANTT

An Toàn Mạng Không Dây

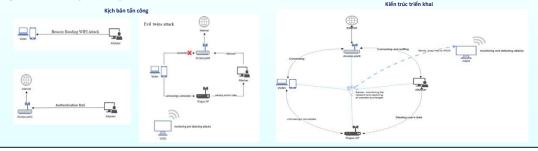


Tìm hiểu và Xây dựng thử nghiệm hệ thống WIDS

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 nhằm 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 kip thời phát hiện và ngặn chặn cuộc tấn công mạng không dây. Trong để tài này, nhóm sẽ chi 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.



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 WFP/WPA/WPS



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



- + 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

Results

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

8550 M.O.S.X.D.D	Printey WAZ WA	Clokes : CCCP	Auth : PSK	ESSED in mang-acid
	Channel : 1	Speed : 11 %5		
85510 : 91:10:55:34:0C:F5	Privacy MPAZ MPA	Cloker : COMP	Ann : PSK	ESSED : mang-actif
Client : # client	Channel : 11	Speed : 11 %		
855TD : 00:29:54:23:28:00	Privacy : MPAZ MPA	Cloter : COP	Auto : PSK	ESS30 : mang-act6
Client : # client		Speed : 11 HI	Pares : 29	
85510 45:56:00:44:04:53	Princey MPA2 MPA	Eigher : COMP	Auto : PSK	ESSID : mang-acid
Client : 0 client	Chevrel : 10	Speed : 11 HB		
BSSS : 80:30:87:47:40:48	Princey WHAT WAS	Cipher : COP	Auth : PSK	ESSED : mang-actif
		Speed : 11 H	Fower : 89	
85577 DE: 88:56:16:2A:16	Privacy : WAZ WA	Clipher : COP	Aum : PSK	ESSED : mang-act6
Client : 0 client	Chinnel: 7	Speed : 11 16	Power in 88	
85533 : 85:50:28:88:16:77	Privacy : MPA2 MPA	Cloker : COM	Auch : PSK	ESSED : mang-actif
ESST : 80:48:40:17:44:18	Frincy : NEAZ NEA	Cipher : COMP	Avo : PSK	ESSSO : mang-act3
	Channel : 11	Speed : 11 NO	Page 1 52	
85533 BD:51:32:8F:4A:85	Privacy MPA2 MPA	Eigher COMP	Auto : PSK	ESSID : mang-act3
	Channel : 2	Speed : 11 10	Power : 13	
85510 SS: 87:46:CE:80:48	Princey MAZ MPR	Clipher : COMP	Auch PSK	ESSED : mang-act3
	Channel : 12	Speed : 11 HE	Power 1 38	
85510 B:16:49:30:33:41	Princip MAZ MPS	Cloter : COP	Auto PSK	ESSED : mang-act1
Client : 0 client	Chartel : 5	Speed : 11 NO		
8550 : 79:5° X:FF:5°:44	Privacy MPA2 MPA	Clokes : COP	Auch PSX	ESSID : mang-act3
Client : 0 client	Channel : 18	Speed : 11 NG	FORES C 50	
\$315 BA:65:90:C1:FA:C3	Privacy : MPA2 MPA	Cipher : COMP	Auth : PSK	85500 : mang-act3
Client : 0 client	Overeal = 14	Speed : 11 HG		
05525 : 08:40:85:88:96:0E	Privacy : MAZ MA	Cloker : COM	Auth : PSK	\$5500 mang-act3
Client : # client		Speed 11 HE	France C 29	

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.

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





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.



KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG @Trường ĐH Công nghệ Thông tin - ĐHQG-HCM