Các kỹ thuật hack mạng Wireless

I. Keywords

Trong phần này sẽ nói sơ lược về các yếu tố cơ bản về mạng Wireless hoặc LAN(Local Area Network) nói chung.

Phần này sẽ giải thích : Sniffing, Spoofing, SSIDs, Làm sao xác định SSID,WEP, từ chối dịch vụ bằng cách làm nhiễu hoặc làm giả wireless để dụ victim truy cập.

1. Giới thiệu sơ lược:

Mạng Wireless phát gói tin bằng tần số vô tuyến(RF) hoặc bước sóng quang hoặc (Optical Wavelengths) và các dòng laptop có thể bắt được.

Điều tồi tệ, là attacker có thể tạo một package mới mà wireless stations chấp nhận là hợp pháp.

1. Tổng quan Wireless Lan:

Wireless Lan có cách thức gần giống TCP/IP.

IEEE 802.11 được đề cập ở đây([www.ieee802.org/11/](http://www.ieee802.org/11/)) được phát triển bởi IEEE là giao thức giữa wireless client và AP hoặc giữa 2 wireless client. IEEE phải được xác thực bởi giao thức mạng(MAC- Medium Address Control) và Lớp Vật Lý(Physical Layer) IEEE 802.11 được nằm trong tầng 1(Physical) và tầng 2(Data Link) của OSI model. Có nhiều giao thức IEEE 802.11 : 802.11a/b/g

2.1 Trạm (Station) và Điểm Truy Cập(Access Point):

Trạm: là tầng lớp vật lý cung cấp mạng kết nối giữa trạng này với trạm khác bằng sóng vô tuyến. Cụ thể trạm là 1 cái USB Wireless. 1 cái laptop có card wireless.

Điểm truy cập: là 1 cái trạm(station) là một nơi để cung cấp frame để phân tán đến các trạm khác.Bản thân điểm truy cập(AP) là một thể loại được kết nối bởi dây(wire) đến LAN.

Chú ý :Trạm thu, AP phát.

2.2 Kênh(Channel):

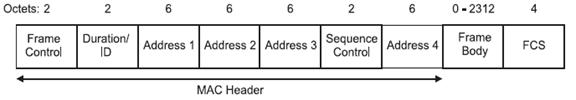
Các trạm liên kết với nhau sử dụng tần số vô tuyến (RF) giữa 2.4 - 2.5GHz.

2 Mạng dây cùng chung các kênh lân cận có thể can thiệp với nhau **(lưu ý điều này)**

2.3 Wire Equivalent Privacy(WEP)

WEP là 1 cái khóa chia sẽ đươc mã hóa các package trao đổi giữa trạm(station) và điểm truy cập(AP).

2.4 Frames



Có 3 loại:

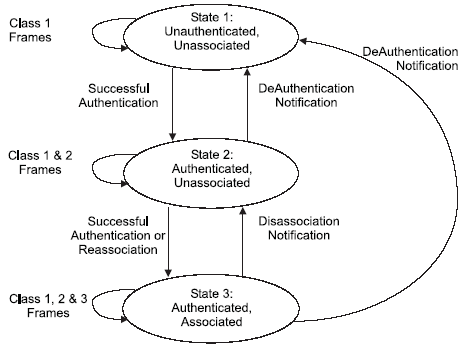
+ Management Frame:

+ Control Frame: Điều khiển phân tán.

+ Data Frame: Đóng gói tầng lớp OSI Model: Bao gồm địa chỉ MAC nguồn, MAC đích, BSSID, TCP/IP diagram, payload : WEP mã hóa

2.5 Authentication

Authentication được cung cấp xác thực từ trạm (station) và điểm kết nối(AP). Tất cả trạm được xác thực mà không có bất kỳ kiểm tra. Một trạm A gửi một frame quản lý Authentication bao gồm Xác nhận A, trạm B, Trạm B gửi lại frame rằng xác nhận A, địa chỉ tới A. Share key Authentication sử dụng để trao đổi giữa máy trạm và AP.



2.6 Beacon Frame

Beacon Frame được AP phát ra nhầm mục địch các trạm nhận được wifi hiện tại

Beacon gồm : SSID(tên Wireless), capabilities, và các thông tin khác.

2.7 Association

Dữ liệu truyền giữa AP(Điểm truy cập) và station(máy trạm) sau khi Association(xác thực). Tất cả APs(các điểm truy cập) phát ra Beacon frames nhiều lần mỗi giây. Trạm sẽ chọn để associated(xác thực) với AP(điểm truy cập) dựa trên signed strength(độ mạnh dấu hiệu). Station có thể không có tên Wireless (SSID).

Có 2 bước để xác thực 1AP tới 1 trạm.

Bước 1: 1 trạm lắng nghe tất cả Beacons frame mà chưa unauthenticated(chưa cấp quyền) và unassociated(chưa xác thực). Trạm sẽ chọn BSS(Basic Server Set) để join(thêm vào). AP and station xác thực lẫn nhau bằng cách trao đổi các Authentication management frames. Bây giờ thì client Authenticated, nhưng chưa ác thực ( unassociated)

Bước 2: Trạm gửi Association frame. AP phản hồi và gửi lại bao gồm Association ID đến máy trạm. Bây giờ máy trạm đã xác thực và cấp quyền.

1. Wireless Network Sniffing
2. Sniffing là gì?

Sniffing là việc lắng nghe trên network. Bắt các gói tin(package) và lưu một bản copy lên attacker. Mục đích chính là lấy thông tin.

Sniffing

1. Passive Scanning

Scanning là hành động sniffing bằng cách bật nhiều ật các kênh truyền radio của thiết bị wireless card. Điều này sẽ không phát hiện sự hiển diện của Scanning.

1. Detection of SSID
2. Wireless Spoofing
3. Wireless Network Probing
4. Những điểm yếu AP(Access Point)
5. Từ chối dịch vụ
6. Tấn công Man-in-the-Middle
7. War-Driving