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):

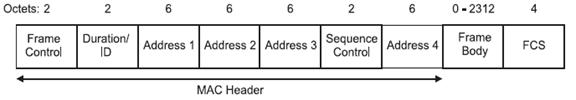
Các trạm liên kết với nhau sử dụng tần số vô tuyến (RF) giữa 2.4 - 2.5GHz.

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:

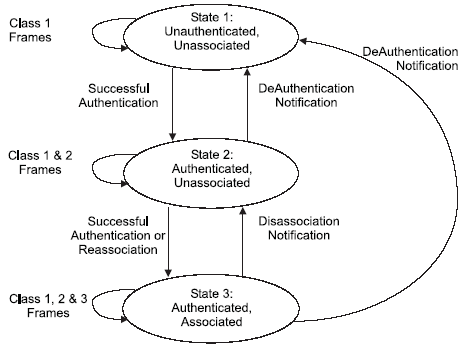
+ Management Frame:

+ 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

Attacker có thể phát hiện SSID ò một network thông thường. Vì Attacker dựa vào Beacon, Association Request.

Nhưng với trường hợp AP chỉnh lại SSID dưới dạng ẩn danh (người ngoài không nhìn thấy được). Do vậy Beacon frames bằng rỗng. Và rõ ràng là người ngoài cuộc sẽ không nhìn thấy đc WLAN.

Với trường hợp Beacon không tắt. Thì rõ rang attacker có thể thấy được mạng bằng cách passive scanning.

Với trường hợp khó hơn là Beacon trả về SSID rỗng, Thì attacker lắng nghe Associate Request từ máy trạm và Associate Response từ AP.

Vì cả 2 đều có thông tin chính xác SSID. Nếu máy trạm muốn vào trong(join) AP. Nó phải gửi Probe Requests ở tất cả channels và lắng nghe Probe Responses bao gồm SSID từ ÁP. Attacker sẽ đợi chờ để sniff Probe Response và có thể lấy được SSID

Với trường hợp Beacon tắt hoàn toàn. Attacker có thể sniffing từ Associate request. Attacker có thể chọn để lấy được probe request bằng cách tiêm vào frames mà anh ấy đã tạo. Sau đó lắng nghe phản hồi và phân tích SSID.

Các cách trên có thể sẽ khó khăn nếu không đánh lừa được người bị hại

1. Thu thập Frames cho việc Cracking WEP

Attacker sẽ sniff một số lượng lớn frames từ BSS. Các frames này đều dùng chung 1 khóa. Sau khi thu thạp frames, Attacker sẽ mã hóa bằng cách sử dùng “mathematically-week” IVs. Sẽ nhận được vào việc thu thập từ vài giờ đến vài ngày phụ thuộc vào độ bận rộn của WLAN như thế nào.

Hoặc Attacker cần 1 danh sách pass hoặc brute đều có thể crack đc.

1. Phát hiện người sniffer

Việc phát hiện người sniffer wireless, hoặc radio-slien trong network dường như là không thể.

1. Wireless Spoofing

Spoofing là một dạng tấn công giả mạo IP, network hay một dạng mà attacker muốn lấy cắp. Nó gần giống với Man In The Middle

Có một vài kỹ thuật tấn công spoofing(giả mạo) trong wire(mạng có dây) và cả wireless(mạng không dây) networks. Người tấn công sẽ tạo một cái frame mà truyền tất cả các thông tin bao gồm địa chỉ hoặc xác thực của nạn nhân với 1 cách thức hợp pháp nhưng giá trị đó là ảo.

Kẻ tấn công thu thập thông tin của victim thông qua sniffing

4.1 MAC Address Spoofing

Kẻ tấn công thông thường mong muốn dấu mình nhưng các hành động thăm dò như inject frame(tiêm vào/ chèn vào frame) rằng được quản lý bởi hệ thống administrator. Kẻ tấn công sẽ làm giả MAC Address của inject frame mà thiết bị sẽ không phát hiện.

Các APs thông thường kiểm soát truy cập bởi sự cho phép chỉ ở máy trạm mà biết được MAC addresses. Hoặc là Attacker làm giả MAC Address hợp pháp trong inject frame mà anh ấy tạo ra.

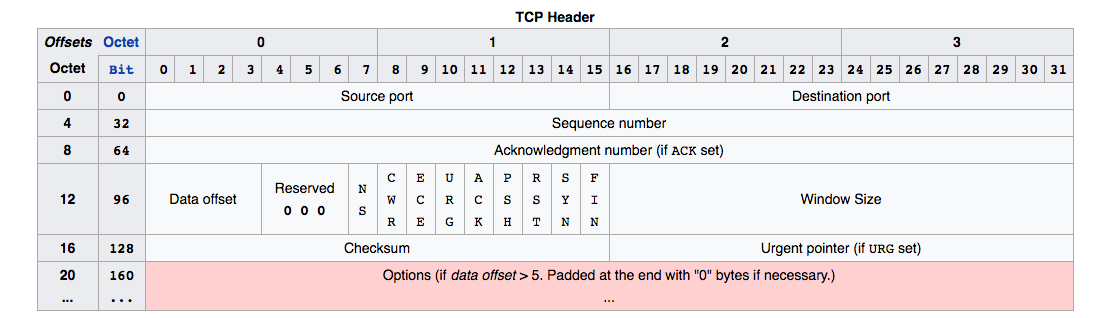
Với các AP mà không sử dụng đến lọc Mac Address thì Attacker không cần giả mạo

Attacker có thể dùng phần mềm để tùy ý giả mạo MAC Address. Trong 1 khoảng giây Attacker có thể thay đổi MAC lên đến ngàn lần.

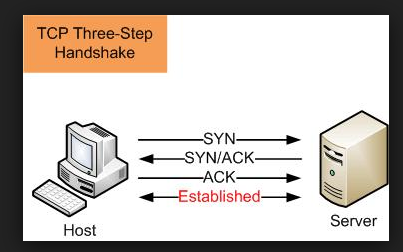
4.2 IP Spoofing

Đây là phương thức giả mạo IP được sử dụng nhiều nhất nhằm mục đích giao tiếp và truyền đạt file theo dựa vào sự tin tưởng của Victim

Cách thức:



Đầu tiên: Giả sử Victim muốn giao tiếp với router(192.168.1.1).



Host sẽ gửi SYN đến Server SYN.

Server sẽ gửi lại SYN/ACK tới Host.

Trước khi Host gửi lại ACK.

Thì ở đây về phía Attacker sẽ giả mạo IP Host rồi gửi ACK tới Server.

Lúc này Server tưởng Attacker là Host. Nên thiết lập kết nối ở Attacker và Server.

4.3 Frame Spoofing

Khi mà Frame được giả mạo địa chỉ nguồn. Nó không thể nhận dạng trừ khi địa chỉ đó hầu như không tồn tại.

1. Wireless Network Probing
   1. Nhận dạng SSID

Thông thường thì SSID enable cho các client thấy được thông tin của mạng.

Nhưng với số trường hợp đặc biệt thì SSID chỉ cho thấy với các MAC Address mà AP đã cài đặt. Attacker sẽ không kiên nhẫn đợi chờ lắng nghe các Probe Request, Associate Request. Attacker sẽ tiêm vào Probe Request frame bao gồm địa chỉ Mac giả.

Nhưng cũng có trường hợp AP sẽ disable sự phản hồi của Probe Request rằng nó bao gồm SSID. Trong trường hợp này, Attacker sẽ xác định máy trạm và gửi cho máy trạm Disassociation frame giả. Và rõ rang Attacker phải làm giả AP để victim tưởng đó là thât. Máy trạm sẽ gửi lại Reassociation Request tới Attacker. Và Attacker sẽ lấy được SSID.

* 1. Nhận dạng APs và máy trạm
  2. Nhận dạng sự thăm dò

Nhận dạng sự thăm dò là có thể. Frames mà attacker tiêm vào có thể được lắng nghe bởi intrusion detection systems (IDS). Và có GPS-enabled rằng nó có thể xác định tọa độ người thăm dò

1. Những điểm yếu AP(Access Point)
2. Từ chối dịch vụ
3. Tấn công Man-in-the-Middle
4. War-Driving