

TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA CÔNG NGHỆ THÔNG TIN

Tel. (84-511) 736 949, Fax. (84-511) 842 771

Website: itf.ud.edu.vn, E-mail: cntt@edu.ud.vn



BÁO CÁO ĐỒ ÁN
CƠ SỞ NGÀNH MẠNG

Đánh chặn các cuộc tấn công từ Attacker trên Wireless

Giảng Viên : ThS. Trần Hồ Thủy Tiên

Sinh Viên : Lê Việt Tri

LỚP : 13T.CLC

ĐÀ NẴNG, 12/2016

LỜI NÓI ĐẦU

Đồ án cơ sở ngành mạng là một trong những đồ án chuyên ngành của khoa công nghệ thông tin. Nó cung cấp cho em rất nhiều kiến thức về lập trình cơ sở,đặt biệt là những kiến thức về mạng. Qua bài đồ án này đã giúp em nắm vững thêm kiến thức cơ bản thầy cô hướng dẫn và định hướng để em hoàn thành chủ đề đồ án. Xin cảm ơn thầy Nguyễn Văn Nguyên đã nhiệt tình giảng dạy và hướng dẫn em hoàn thành đồ án này cũng như các thầy cô khác trong khoa đã giảng dạy chúng em trong những học kỳ vừa qua.

Em đã cố gắng rất nhiều,nhưng có lẽ không tránh khỏi thiếu sót,mong các thầy cô và các bạn giúp đỡ.

Trong đồ án này em đã xin phép trọ để thực thi các cuộc tấn công vào ngày 27/12/2016.

Đồ án không mang tính gây hư hỏng, lấy trộm thông tin vào mục đích xấu trên các thiết bị.

Đà Nẵng, ngày 27 tháng 12 năm 2016

Sinh viên thực hiện : Lê Việt Tri

Nhóm 13.14-Lớp 13T.CLC-Khoa CNTT

Đại Học Bách Khoa Đà Nẵng

NHẬN XÉT GIÁO VIÊN

[illegible]

Mục lục

LỜI NÓI ĐẦU	2
Chương 1. Giới thiệu cơ bản về Wireless	6
1. Giới thiệu sơ lược:.....	6
2. Tổng quan Wireless Lan:	6
2.1 Trạm (Station) và Điểm Truy Cập(Access Point):	6
2.2 Kênh(Channel):.....	6
2.3 Wire Equivalent Privacy(WEP).....	6
2.4 Frames.....	7
2.5 Authentication.....	7
2.6 Beacon Frame	8
2.7 Association.....	8
3. Wireless Network Sniffing.....	8
3.1 Sniffing là gì?.....	8
3.2 Passive Scanning.....	8
3.3 Detection of SSID	8
3.4 Thu thập Frames cho việc Cracking WEP.....	9
3.5 Phát hiện người sniffer.....	9
4. Wireless Spoofing	9
4.1 MAC Address Spoofing.....	9
4.2 IP Spoofing	11
4.3 Frame Spoofing.....	12
5. Wireless Network Probing	12
5.1 Nhận dạng SSID	12
5.2 Nhận dạng APs và máy trạm	12
5.3 Nhận dạng sự thăm dò	12
6. Những điểm yếu AP(Access Point)	12
6.1 Chống lại bộ lọc MAC.....	12
6.2 Trojan AP.....	12
7. Từ chối dịch vụ (Denial of Service)	13
7.1 Jamming the Air Waves.....	13
7.2 Làm tràn Associations	13
7.3 Forged Dissociation	13
7.4 Forged Deauthentication.....	13
8. Tấn công Man-in-the-Middle.....	13
8.1 Wireless MITM.....	13
8.3 Session Hijacking.....	13
9 Công cụ hỗ trợ.....	14
Chương 2. THUẬT TOÁN	15
1. Phân tích yêu cầu đề tài.....	15
2. Hướng giải quyết.....	17
2.1. Dấu SSID	17
2.2. MAC Filter.....	17
2.3. Đặt Password	17
2.4. Trang bị kiến thức.....	17
Chương 3 KẾT QUẢ CHƯƠNG TRÌNH.....	18
1. WifePhisher.....	18

Step 1: Khởi động chương trình.....	19
Step 2: Liệt kê các SSID xung quanh bắt được(nhờ vào Beacon).....	19
Step 3: Chọn các phương thức giả tạo web:	19
Step 4: Đợi chờ Victim	20
2. Wireshark : Bắt gói tin (package).....	24
3. Ettercap	25
4. Phương pháp giải quyết:	25
4.1. Chủ động:.....	25
MAC Filter.....	25
Disable SSID.....	25
Enable FireWall	26
4.2. Bị động:.....	26
Chương 4 KẾT LUẬN.....	26
1. Đạt được.....	26
2. Chưa đạt được.....	26
3. Hướng phát triển	26
Chương 5 PHỤ LỤC.....	27
1. Tài liệu tham khảo.....	27
2. Website tham khảo.....	27
3. Hệ điều hành hỗ trợ.....	27
4. Code	27

Chương 1. Giới thiệu cơ bản về Wireless

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.

2. 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/) 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 trạm 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):

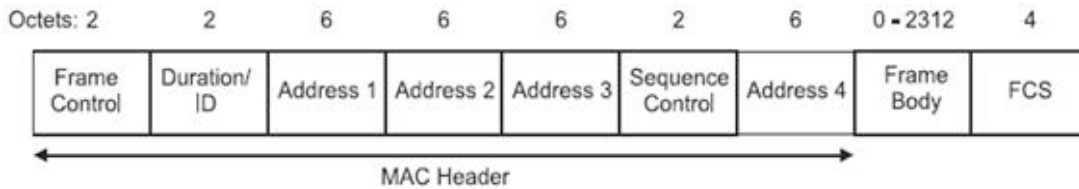
Các trạm liên kết với nhau sử dụng tần số vô tuyến (RF) giữa 2.4 - 2.5GHz.

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 sẻ được mã hóa các package trao đổi giữa trạm(station) và điểm truy cập(AP).

2.4 Frames



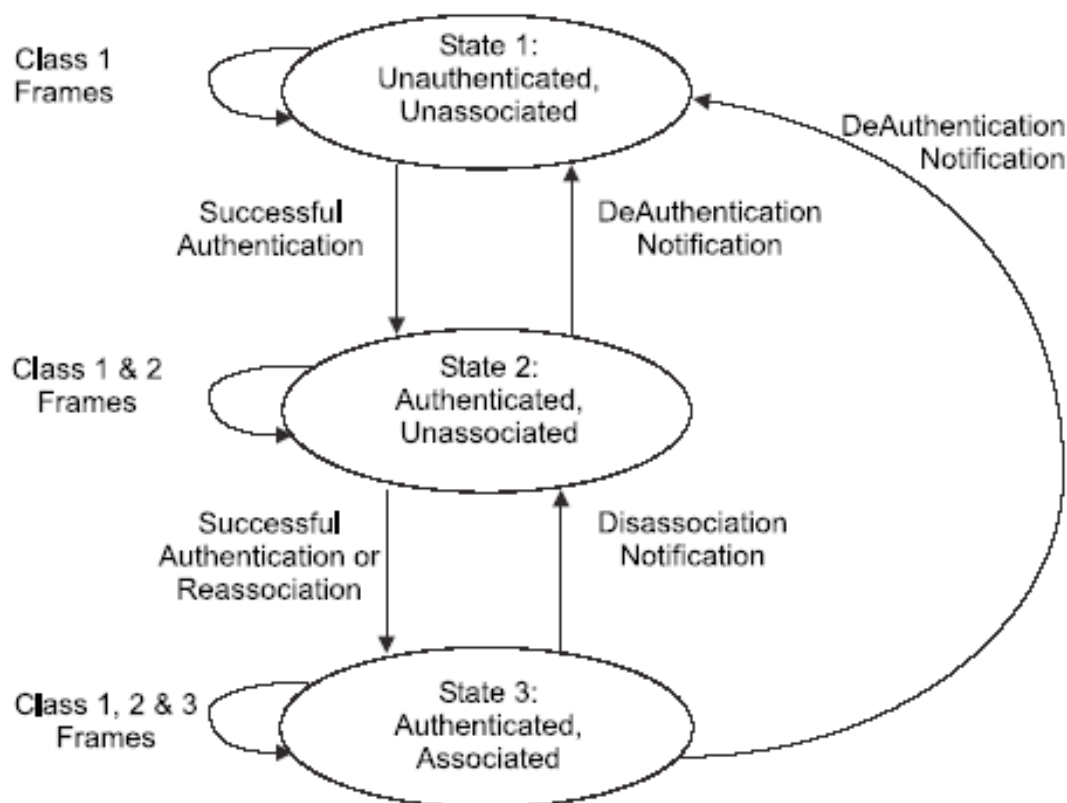
Hình 2.4: Cấu trúc Frames

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.



Hình 2.5: Cấp quyền cho station

2.6 Beacon Frame

Beacon Frame được AP phát ra nhằm mục đích 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 xác 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.

3. Wireless Network Sniffing

3.1 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.

3.2 Passive Scanning

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

3.3 Detection of SSID

Attacker có thể phát hiện SSID ở 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 ràng 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 AP. 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

3.4 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 thập frames, Attacker sẽ mã hóa bằng cách sử dụng “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.

3.5 Phát hiện người sniffer

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

4. 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.

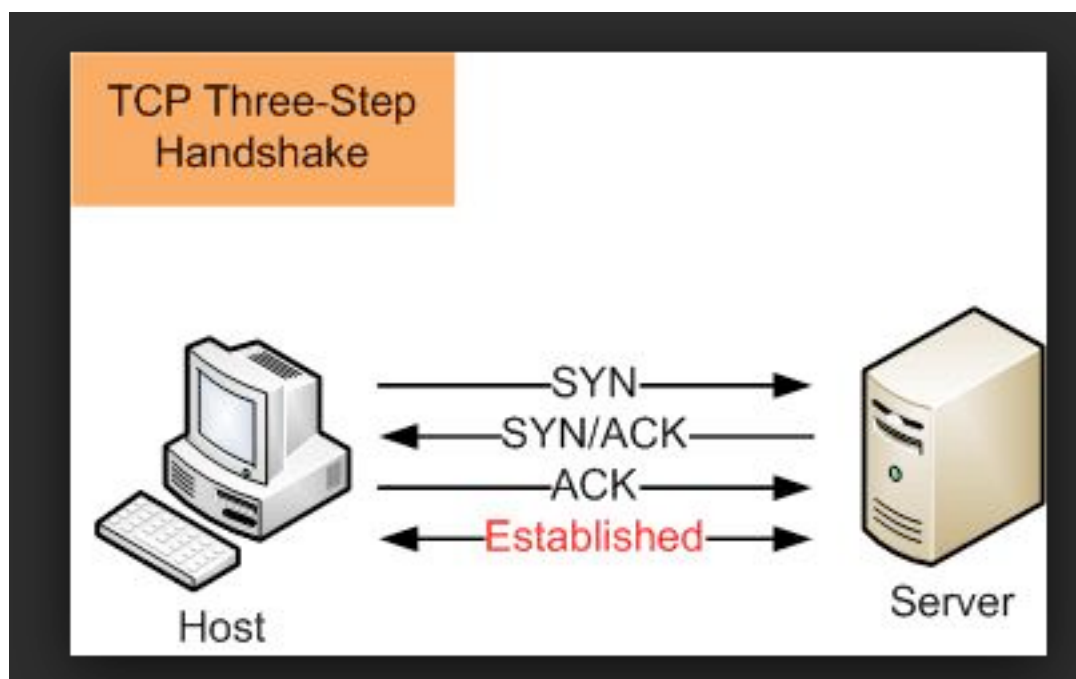
4.2 IP Spoofing

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

TCP Header																																	
Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0			N	C	E	U	A	P	R	S	F	Window Size															
	S								W	C	R	C	S	S	Y	I																	
	R								E	G	K	H	T	N	N																		
16	128	Checksum																Urgent pointer (if URG set)															
20	160	Options (if <i>data offset</i> > 5. Padded at the end with "0" bytes if necessary.)																															
...																															

Hình 4.2.1: TCP Header

Cách thức:



Hình 4.2.2: Giao tiếp Host và Server

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.

5. Wireless Network Probing

5.1 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 ràng Attacker phải làm giả AP để victim tưởng đó là thật. Máy trạm sẽ gửi lại Reassociation Request tới Attacker. Và Attacker sẽ lấy được SSID.

5.2 Nhận dạng APs và máy trạm

5.3 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

6. Những điểm yếu AP(Access Point)

6.1 Chống lại bộ lọc MAC

Các AP thông thường đều cấp phát quyền truy cập chỉ những MAC đã được đăng ký. Điều này thật dễ dàng với attacker chỉ cần sử dụng một chương trình có thể thay đổi MAC của attacker và kèm theo đó là lắng nghe MAC từ các máy nội bộ

6.2 Trojan AP

Khi attacker vào được wifi của bạn. Thì attacker dễ dàng lấy thông tin như password, id ... Cách thức này có thể gọi Man In The Middle (MITM). Mà victim khó có thể nhận ra.

Diễn hình đó là phần mềm : HostAP (<http://hostap.epitest.fi/>).

7. Từ chối dịch vụ (Denial of Service)

DoS là cách thức tấn công làm tê liệt hệ thống. Trong mạng wireless networks, DoS khó có thể ngừng cuộc tấn công này và nạn nhân khó có thể nhận ra đó có cuộc tấn công.

7.1 Jamming the Air Waves

Attacker có thể gỡ bỏ một số lượng lớn thiết bị bằng cách làm nhiễu sóng RF.

Dẫn đến không thể truy cập được các victim.

Cách khắc phục : RF proofing the surrounding environment.

7.2 Làm tràn Associations

Theo chuẩn IEEE 802.11 tối đa được 2007 associations đồng thời. Và các associations khác sẽ bị hủy. Attacker có thể gửi đồng thời vượt quá tiêu chuẩn với các MAC khác nhau.

Cách khắc phục : Bật chế độ MAC filtering (Bộ lọc MAC)

7.3 Forged Dissociation

Attacker gửi một Dissociation frame giả mà được chèn MAC Address victim.

Mục đích làm victim không kết nối mạng được. Rõ ràng thì khi victim không kết nối lại được thì victim sẽ gửi lại một Reassociation frame nhưng điều đó không có nghĩa là sẽ kết nối lại. Bởi vì attacker liên tục gửi gói Dissociation trong một khoảng thời gian buộc Victim không thể kết nối mạng

7.4 Forged Deauthentication

8. Tấn công Man-in-the-Middle

8.1 Wireless MITM

Attacker sẽ cần tới 2 card wireless. Một là dùng để giả danh AP. Cái còn lại dùng để deauthentication tới máy trạm. Buộc máy trạm kết nối tới AP mà attacker giả danh.

Lúc này thì MITM thành công. Attacker có thể đánh cắp thông tin từ nạn nhân.

8.2 ARP Poisoning

ARP : Address Resolution Protocol. Là phương thức giao tiếp giữa 2 máy trao đổi trên Ethernet.

Phương thức giao tiếp ARP dựa vào các gói ARP request và ARP response nhằm nhận biết lẫn nhau.

Nhưng AP không có xác minh, do vậy Attacker sử dụng ARP poisoning làm MITM để đánh cắp thông tin.

Có thể sử dụng phần mềm Ettercap để đánh cắp .

8.3 Session Hijacking

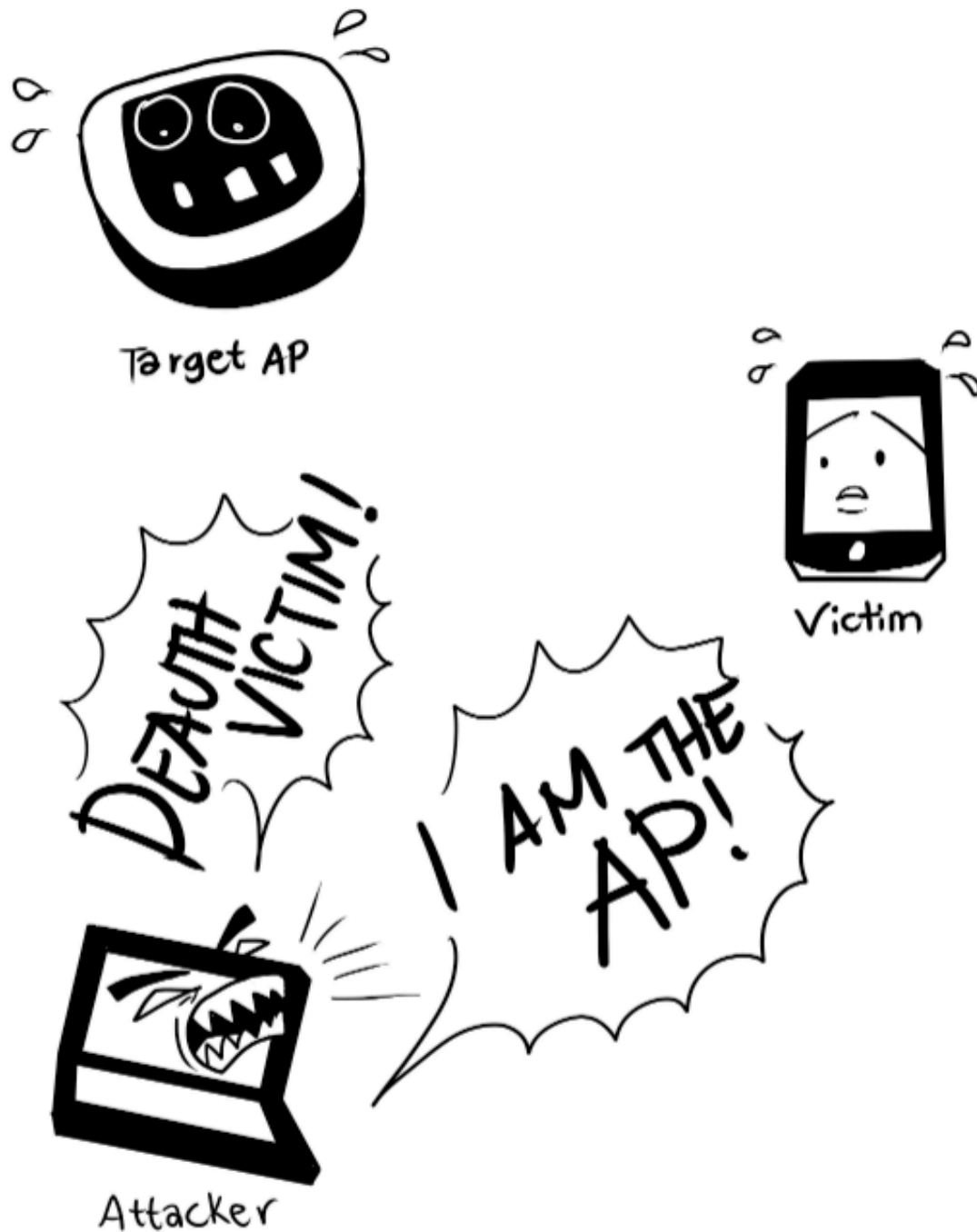
Đầu tiên attacker sẽ DoS victim. Victim sẽ bị ngắt kết nối. Tiếp tục attacker sẽ giả mạo MAC Address. Sau đó sử dụng các quyền mà victim có được.

9 Công cụ hỗ trợ

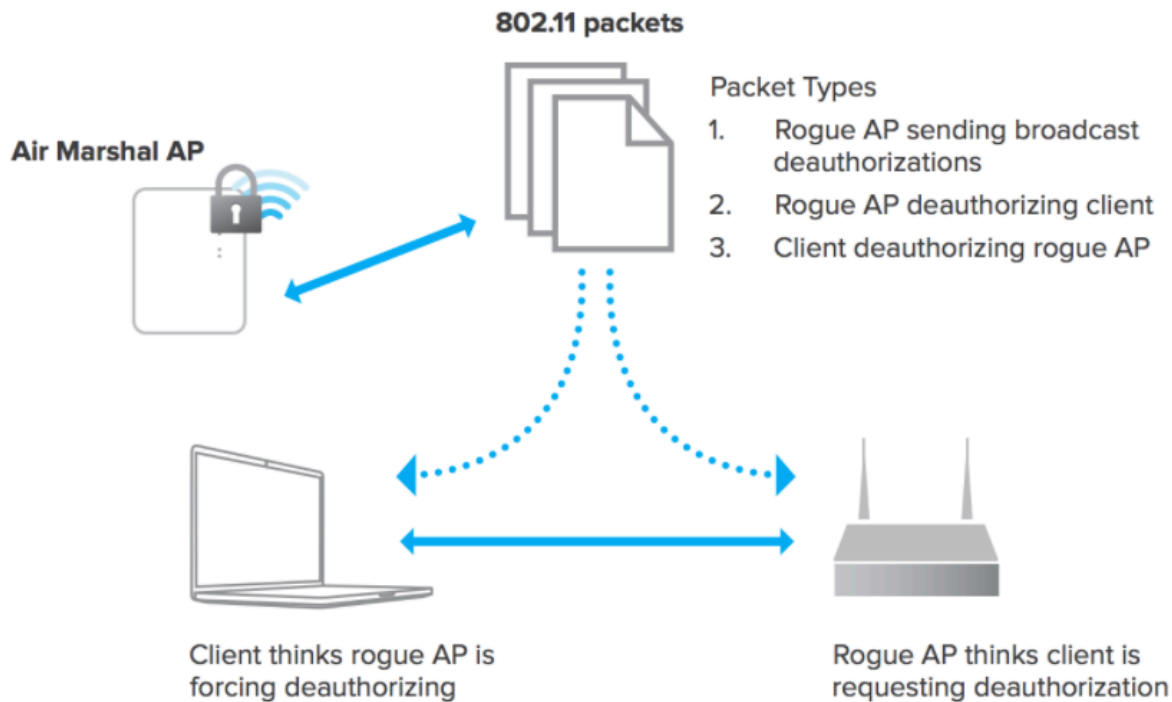
- 9.1** AirJack
- 9.2** AirSnort
- 9.3** Ethereal
- 9.4** FakeAP
- 9.5** HostAP
- 9.6** Kismet
- 9.7** WEPcrack
- 9.8** Wellenreiter
- 9.9** Stumb Vector

Chương 2. THUẬT TOÁN

1. Phân tích yêu cầu đề tài.



Nguồn Ảnh : Wifisphier – Giải thích cách tấn công
Hình 2.1.1 Mô tả cách tấn công Wifi (Dễ hiểu)



Nguồn : documentation.meraki.com

Hình 2.1.2 Mô tả cách tấn công từ AP giả

Dựa vào các lỗ hổng ở phía Wireless như dễ dàng làm giả AP hay chặn các đường truyền từ các station đến AP.

Hay đơn thuần là Attacker có thể làm giả MAC victim. Điều đó có nghĩa các quyền mà victim nói đến AP đều thông qua attacker. Nếu Attacker kết hợp thêm deassociate tới victim

Trong phần này tôi sẽ giải quyết vấn đề chặn các cuộc tấn DoS từ phía attacker

2. Hướng giải quyết.

Cách tốt nhất để bảo vệ các cuộc tấn công

- + Ẩu SSID
- + MAC Filter
- + Đặt Password
- + Trang bị kiến thức cho người dùng

2.1. Ẩu SSID

Trong phần setting của router có mục ẩn SSID. Chỉ cần bật nó lên. Điều này giúp Attacker không nhận ra Wireless của mình.

2.2. MAC Filter

Chỉ lọc những máy mà mình tin tưởng vào trong danh sách. Mục này cũng có trong router.

2.3. Đặt Password

Chúng ta nên đặt Pass có độ dài >16 và mật khẩu không nên liên quan tới vấn đề gì.

Vì attacker có thể crack > 4500passwords/s

Lời khuyên nên hàng tháng đổi 1 lần.

2.4. Trang bị kiến thức

Mọi cuộc tấn công từ Attacker sẽ không thành công nếu người dùng được trang bị kiến thức nền tảng.

Thứ nhất: Nếu người dùng bỗng dưng mất mạng. Điều đó không có nghĩa là mạng lag. Điều chắc chắn ở đây là đường truyền có vấn đề. Có thể là do một Attacker gửi gói tin deassociate làm người dùng không thể kết nối mạng gốc được.

Thứ hai: Phải cảnh giác với Wireless cùng tên nhưng không có mật khẩu.

Thứ ba: Sử dụng tường lửa để phòng chống ARP Poisoning.

Thường xuyên track dòng dữ liệu trao đổi để kiểm tra.

Nếu có trường hợp nào lạ nên báo công an bởi vì nhược điểm của phương thức tấn công này là có thể định vị được GPS của kẻ tấn công.

Thông thường code được viết dưới dạng python vì python có khả năng triển khai tốt hơn các ngôn ngữ khác.

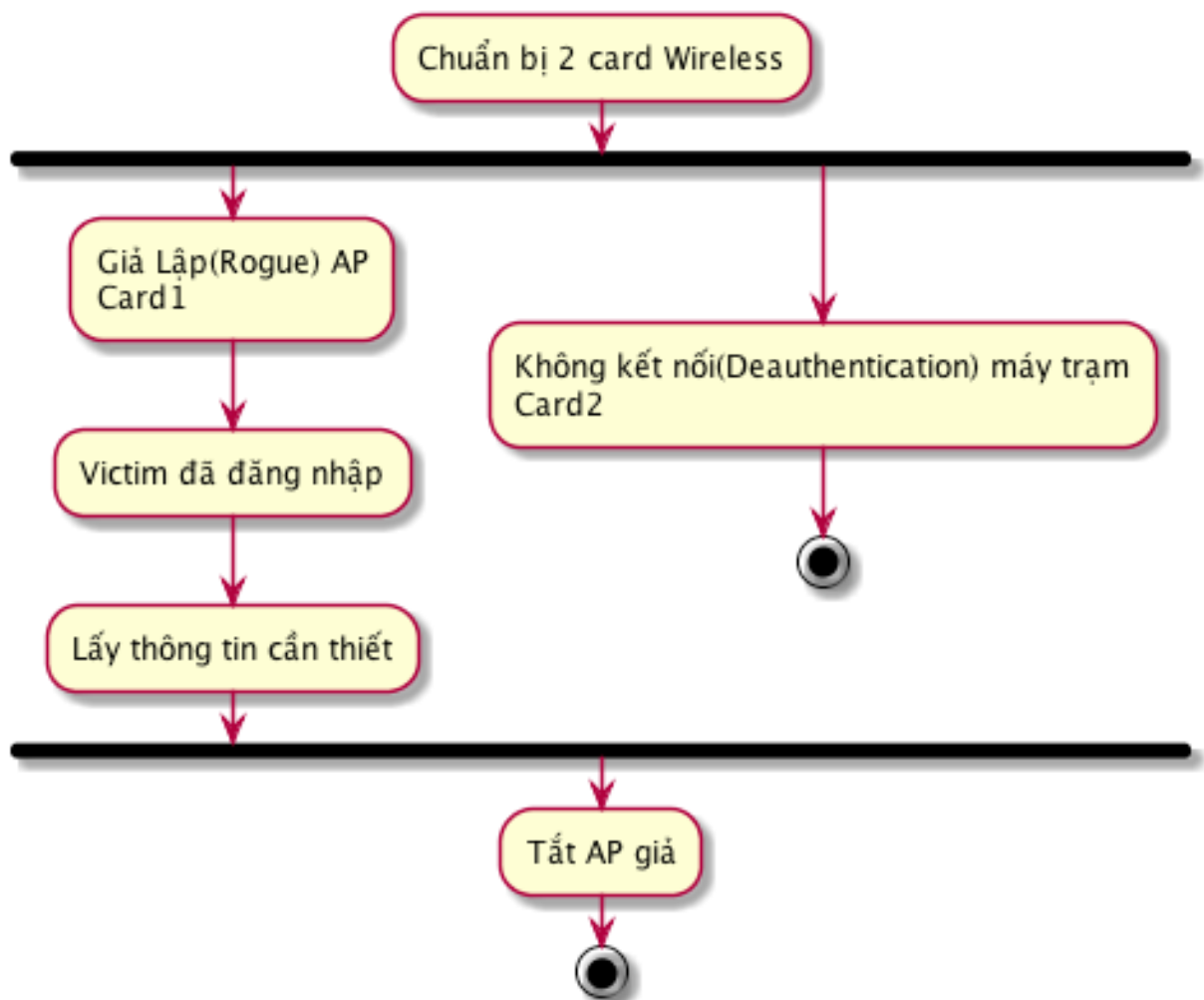
Ở đây tôi có dùng tool Wireshark để bắt các package

Và sử dụng wifiphiser để tạo AP giả và deauthenticate station

Ethercap ở đây tôi dùng để sử dụng ARP Poisoning và bắt các gói http protocol

Chương 3 KẾT QUẢ CHƯƠNG TRÌNH

1. WifePhisher



Step 1: Khởi động chương trình

```
→ wifiphisher git:(master) sudo wifiphisher
[sudo] password for zaku:
[*] Starting Wifiphisher 1.2GIT at 2016-12-27 12:48
[+] Selecting wlan1 interface for the deauthentication attack
[+] Selecting wlan0 interface for creating the rogue Access Point
[*] Cleared leases, started DHCP, set up iptables
□
```

Sử dụng 2 card wireless :

1. Giả lập AP
2. deauthentication attack (Ngừng cung cấp connect giữa máy trạm và AP)

Step 2: Liệt kê các SSID xung quanh bắt được(nhờ vào Beacon)

```
[+] Ctrl-C at any time to copy an access point from below
num ch  ESSID            BSSID            Mô tả bả gner      vendor
-----
1 - 5   Nguyen Luong Bang - 70:d9:31         - WPA2/WPA         - Cambridge In
2 - 5   tro 1                - 98:de:d0         - WPA2/WPA         - Nova
3 - 5   tro 2                - c4:e9:84         - WPA2             - Tp-link Techn
4 - 7   hTu                  - a0:65:18         - WPA2/WPA         - Vnpt Techno
5 - 11   a 44A370             - c8:3a:35         - WPA              - Tenda Techno
6 - 11   567890               - c8:3a:35         - OPEN             - Tenda Techno
7 - 11   danang               - a8:58:40         - WPA2/WPA         - Cambridge In
8 - 11   Hoa                  - a8:58:40         - WPA2/WPA         - Cambridge In
□
```

Lưu ý: Ở đây các phương thức WPA dễ dàng crack được
Với WPA2 thì bảo mật cao hơn
Tôi sẽ cố gắng tận công :Nguyễn Luong Bang

Step 3: Chọn các phương thức giả tạo web:

```
Available Phishing Scenarios:
1 - Network Manager Connect
    Imitates the behavior of the network manager. This template shows Chrome's "Connection Failed" page a
    and MAC OS are supported.
2 - Firmware Upgrade Page
    A router configuration page without logos or brands asking for WPA/WPA2 password due to a firmware up
3 - OAuth Login Page
    A free Wi-Fi Service asking for Facebook credentials to authenticate using OAuth
4 - Browser Plugin Update
    A generic browser plugin update page that can be used to serve payloads to the victims.

[+] Choose the [num] of the scenario you wish to use: [ ]
```

Step 4: Đợi chờ Victim

```
DHCP Leases:
1420616741 60:21:c0:8c [REDACTED] 10.0.0.58 android [REDACTED] *

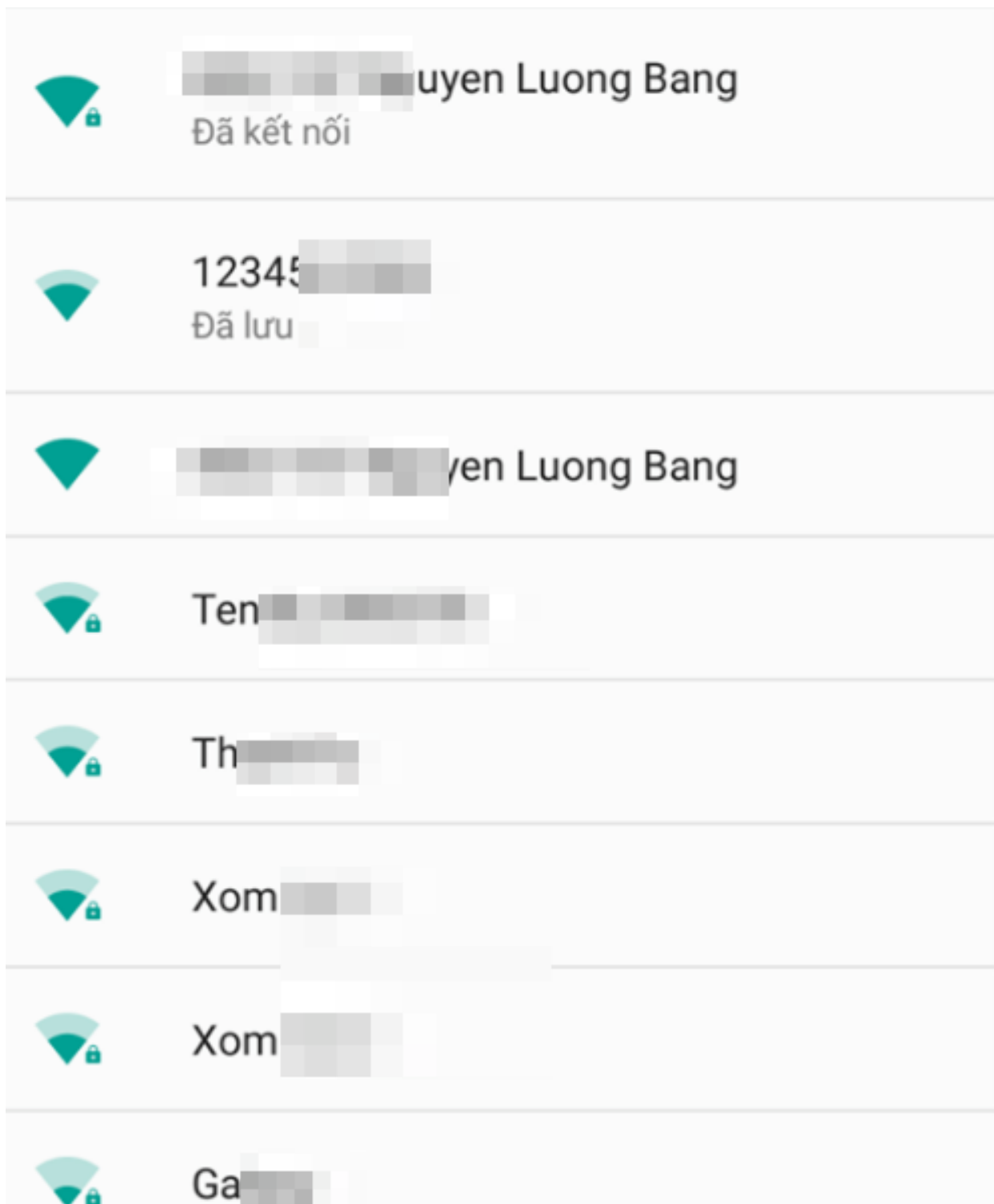
HTTP requests:
[*] GET 10.0.0.58
[*] GET 10.0.0.58
```

Chú ý:

Ở đây chúng ta thấy có victim là android với chỉ số mac 60:21:c0:8c...

Phía dưới là HTTP requests là web mà Attacker giả lập để dụ victim truy cập

Hình ảnh Victim truy cập:



Chúng ta thấy được : Có tới 2 cái wifi ...Nguyễn Lương Bằng

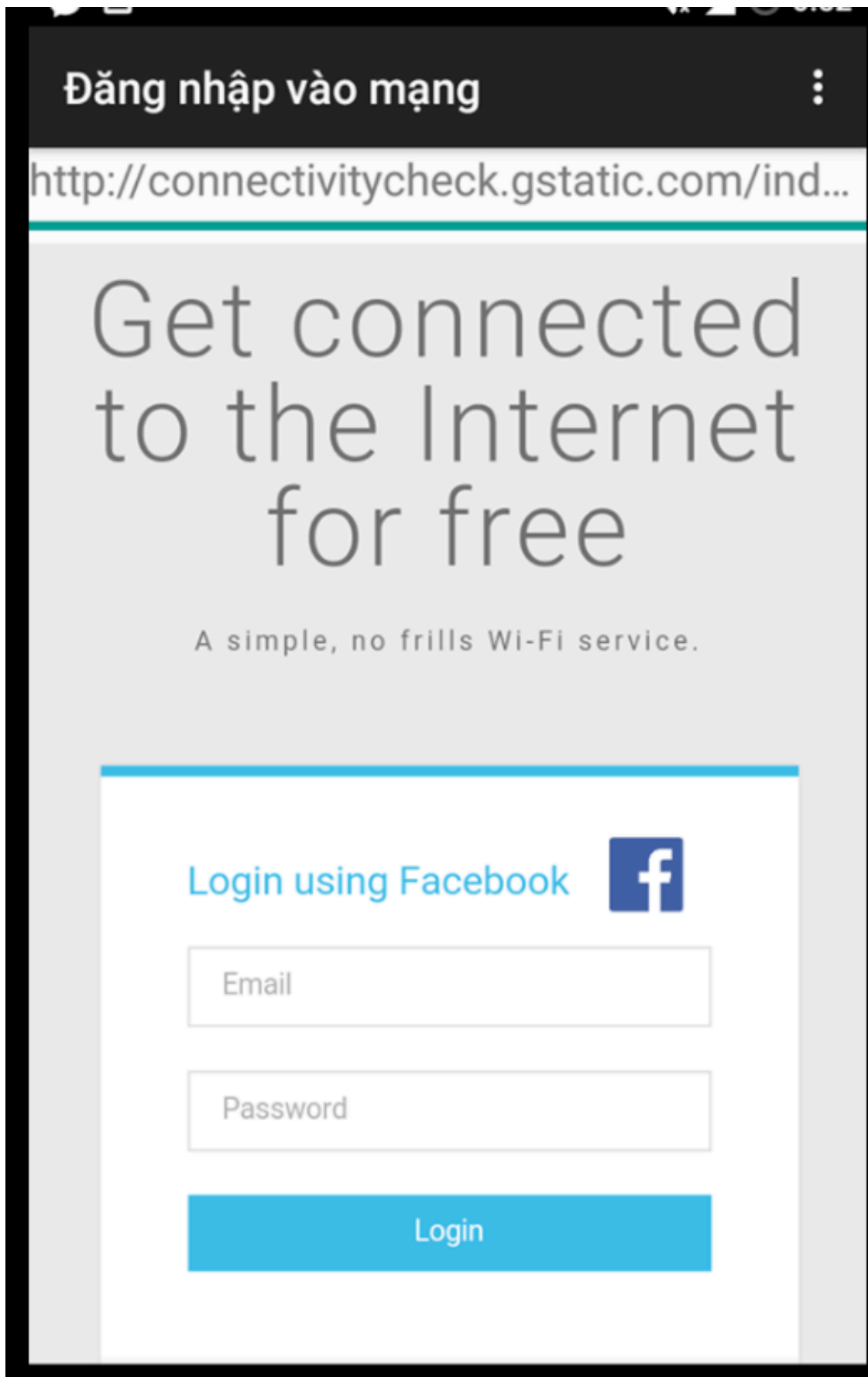
Một cái có password: AP thật

Cái còn lại không có password: AP giả

Victim sẽ không thể kết nối với AP thật bởi vì Attacker đã gửi liên tục file deauthentication cho victim với AP là giả

Nếu Victim có bật chế độ tự động truy cập wireless thì có thể sẽ tự động vào AP giả. Và bất chợt victim sẽ hiện thị các trang web mà wifiphiser có thể giả lập. Ở đây wifiphiser sử dụng Apache

Hình ảnh tiếp theo:



Thật sự rất dễ dàng mất Password phải không nào nếu lơ là.

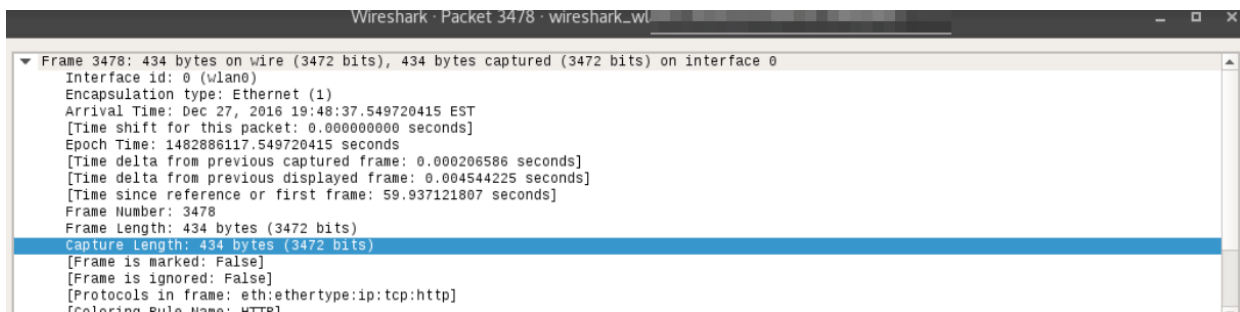
Tiếp theo attacker sẽ lấy được password và id.(web http)

Attacker sẽ shutdown AP lập tức để cung cấp mạng cho victim.

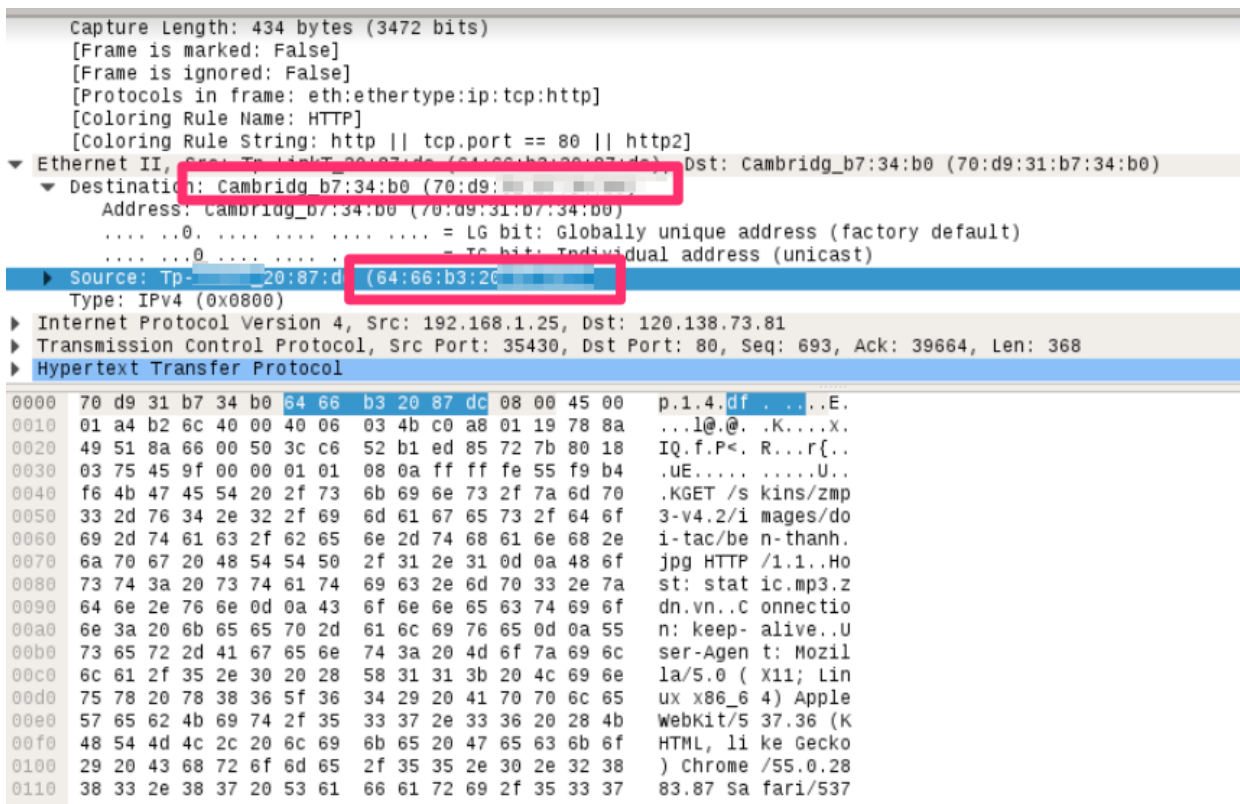
Và victim cảm thấy bình thường

2. Wireshark : Bắc giới tin (package)

Thông tin một package:



Bao gồm MAC Nguồn, MAC đến



3. Ettercap

4. Phương pháp giải quyết:

4.1.Chủ động:

MAC Filter

Enable Mac Filter ☐

Mac Address

Mac Filter Mode White ▾

Add

Default Policy Deny ▾

Mode	Mac Address	Delete
White	28:ba	Delete

SaveRefresh

Disable SSID

Enable SSID Disable ▾




SSID Broadcast Enable ▾

SSID Isolate Disable ▾

Enable WPS Enable ▾

WPS Mode PBC ▾

Enable FireWall

Remote Telnet Enabled	<input checked="" type="checkbox"/>
Remote Https Enabled	<input checked="" type="checkbox"/>
Request Attrack Protect	Enable 
Redirect Attrack Protect	Enable 
Land Attrack Protect	Enable 

4.2.Bị động:

Người dùng phải cảnh giác với mạng Lag Giật
Thông báo với công an nếu gặp trường hợp 2 APs.
Phải cảnh giác cực kỳ với các trang http

Chương 4 KẾT LUẬN

1. Đạt được.

Đã thử các cuộc tấn công Attacker
Đã thành công các cách bảo vệ APs
Đã dùng các tool : Wireshark, Ettercap, Wifiphiser, Aircrack

2. Chưa đạt được.

Chưa thử DoS bằng cách giả IP

3. Hướng phát triển

Thử nghiệm các phương pháp DoS và tìm cách bảo vệ

Chương 5 PHỤ LỤC

1. Tài liệu tham khảo

2. Website tham khảo

<http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm>
<http://airccse.org/journal/nsa/0511ijnsa12.pdf>

3. Hệ điều hành hỗ trợ

Kali Linux

4. Code

4.1 Scan AP

Main

```
if __name__ == "__main__":
    signal.signal(signal.SIGINT, signal_handler)
    usage()
    parameters = {sys.argv[1]:sys.argv[2]}
    if "mon" not in str(parameters["-i"]):
        newiface = setup_monitor(parameters["-i"])
    else:
        newiface = str(parameters["-i"])
    init_process()
    print "Sniffing on interface " + str(newiface) + "...\\n"
    sniff(iface=newiface, prn=PacketHandler, store=0)
```

Nhằm mục đích phát hiện AP giả. Với địa chỉ MAC giả khác với địa chỉ MAC gốc

PacketHandler

```
def PacketHandler(pkt) :
    # pkt.show()
    if pkt.haslayer(Dot11) :
        if pkt.type == 0 and pkt.subtype == 8 :
            if pkt.addr2 not in ap_list :
                ap_list.append(pkt.addr2)
                print "BEACON: AP MAC: %s with SSID: %s " %(pkt.addr2, pkt.info)
    if pkt.haslayer(Dot11ProbeReq):
        if pkt.addr2 not in ap_list:
            # ap_list.append(pkt.addr2)
            print "PROBE:SUB_TYPE:"+str(pkt.subtype) +" AP MAC: %s with SSID: %s " %(pkt.addr2, pkt.info)
```

4.2 Đếm số IP nhận và đi từ packet

```
def PacketHandler(pkt):
    # global stations
    if pkt.haslayer(IP):
        pckt_src=pkt[IP].src
        pckt_dst=pkt[IP].dst
        pckt_ttl=pkt[IP].ttl
        stationSrcs.append(pckt_src)
        stationDecs.append(pckt_dst)
        # if pckt_src not in stations:
        #     stations.append(pckt_src)
        # print "Packet: %s is going to %s and has ttl val
        stationSrcTimes= collections.Counter(stationSrcs)
        stationDecTimes= collections.Counter(stationDecs)
        print "SRC=> "+ str(stationSrcTimes)
        print "DEC=> "+ str(stationDecTimes)
    if __name__ == "__main__":
        # sniff(prn=lambda x:x.sprintf("{IP:%IP.src% -> %IP.ds
        sniff(prn=PacketHandler)
```

Hạn chế ngăn chặn tấn công DoS