

Crack Wifi trong 10 phút

Việc các attacker có thể xâm nhập vào các mạng wifi của tổ chức, thông qua việc crack khóa mã hóa truy cập vào wifi access point. Cho dù các công nghệ mã hóa mạng không dây hiện nay là rất mạnh như *Wired Equivalent Privacy* (WEP) và *Wi-Fi Protected Access* (WPA và WPA-2). Nhưng với những chương trình và thiết bị chuyên dụng, attacker có thể thực hiện thành công ý định của mình. Dưới đây là một trong những demo sử dụng AirPcap (USB 2.0 Wireless Capture Adapter – card bắt tín hiệu wifi) và chương trình Cain & Abel, một công cụ chuyên dụng để bắt gói trên mạng kể Wired hay wireless, sau đó tiến hành crack password, với nhiều phương thức khác nhau. Tất cả các setup được tiến hành trên Windows.

Chuẩn bị:

1. Card AirPcap Tx



AirPcap là một trong những thiết bị chuyên dùng để bắt và phân tích các tín hiệu của mạng không dây (của hãng Cace Technologies) theo các chuẩn hiện nay WLAN (802.11b/g). Thông thường Cace cung cấp bộ công cụ tích hợp bao gồm card AirPcap, và tool bắt gói tin như Wireshark (tên mới của công cụ Ethereal nổi tiếng). Thông qua card AirPcap (dò và bắt tín hiệu wifi, sóng radio) Wireshark tiến hành phân tích các thông tin thu thập được về wifi Protocols và các tín hiệu radio.

Trong demo này, không sử dụng Wireshark, việc thu thập, phân tích và giải mã các khóa mã hóa, thu được từ tín hiệu wifi, tiến hành thông qua một tool khác cũng cực mạnh là: Cain and Abel

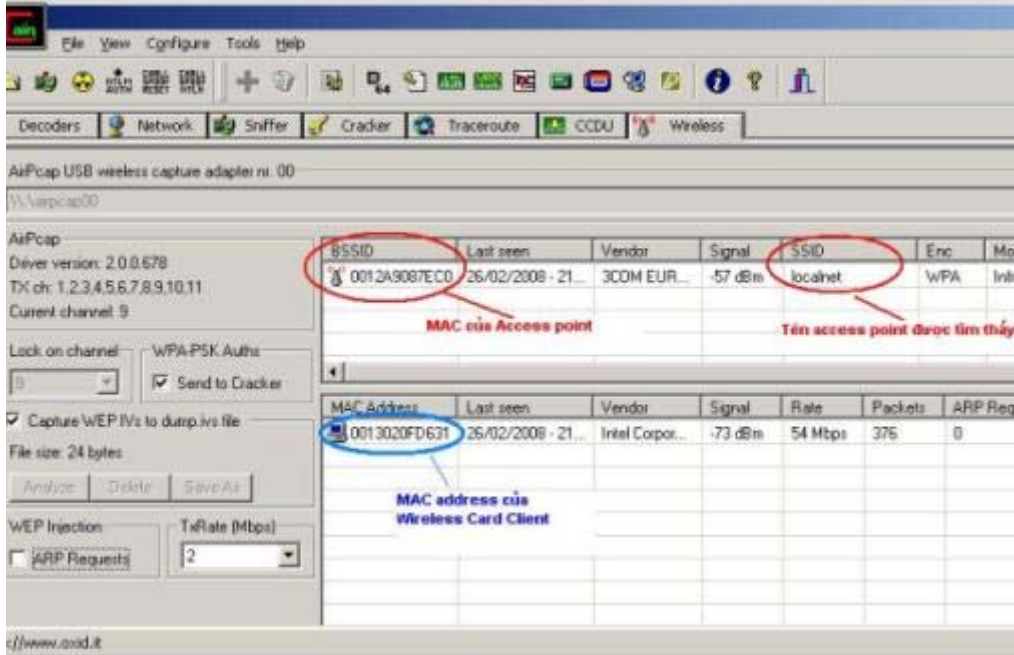
Tiến hành cài Airpcap drivers kèm theo CD, sau khi setup driver xong, gắn Airpcap adapter vào USB slot.

Chú ý: Tín hiệu thu phát của Wireless card hoặc Airpcap bao giờ cũng yếu hơn Access point. Đặt laptop gắn Airpcap, càng gần khu vực Wifi Access point phát sóng bao nhiêu, tín hiệu gửi và nhận với Access point càng "rõ nét"...

2. Chương trình Cain and Abel

Có lẽ người dùng UNIX rất buồn vì một công cụ mạnh và miễn phí như Cain and Abel lại chỉ chạy trên nền Windows. Một công cụ chuyên bắt gói tin và crack các password đã mã hóa. Sử dụng các phương thức tấn công khá phổ biến để crack pass, bao gồm: Dictionary attack, Brute-Force và Cryptanalysis...

Download tại Softpedia



Một Wifi Access point đã được phát hiện kèm theo MAC add và SSID của nó

Lưu ý:

Trước khi tiến hành bơm vào thông số ARP giả mạo (ARP injections/ARP spoofing), AirPcap sẽ phải tiến hành bắt được ít nhất một ARP request (để tìm MAC address thật) của bất kì wireless Client nào đang connect vào access point (wireless card của attacker hoặc các Clients hợp pháp khác..) đang kết nối với Wifi access point. Sau khi bắt ARP request, Cain & Abel sẽ tiến hành gửi một ARP request giả mạo (với MAC address vừa có được), và thiết lập duy trì với Wifi Access point trong suốt quá trình Access Point “nhả” IVs packets. Nếu vì bất kì lí do nào đó MAC address của Client không duy trì kết nối với Access point, thì Access Point sẽ gửi một thông điệp từ chối “DeAuthentication” và các gói IVs sẽ không được tiếp tục cung cấp.

Phải đảm bảo thu thập được trên 250,000 IVs (Initialization Vectors, số lượng các packet đồng bộ giữa AirPcap/Clients và wifi access point, thì Cain and Abel mới có thể tiến hành crack WEP key. Thông thường, không một ai đủ kiên nhẫn ngồi chờ IVs được kích hoạt đủ số lượng, cho nên hầu hết các Wep Crack tool hiện nay (Cain & Abel, Aircrack-ng, Aircrack-PTW, đều áp dụng kĩ thuật Packet Injection (hoặc deauth & ARP re-injection, thông qua các ARP request). Injection tác động làm Wifi Access Point, phải gửi lại các packet đã được lựa chọn, một cách nhanh hơn, khiến trong thời gian ngắn đã có đủ số lượng IVs cần thiết.

cho giải mã Wep key 128 bits. Chắc chắn rằng, thời gian chờ đủ IVs, cho đến khi có thể tiến hành crack Wep key, là..mệt mỏi !

Nếu phân tích về lý thuyết thì rất nhiều thứ còn phải đề cập, vì bạn phải hiểu về cấu trúc TCP/IP, Networking, Raw Socket, Packet header Injection, các chuẩn mã hóa Wireless như WEP hay WPA, WPA-2... Nếu cần phải hiểu rõ quy trình Sniff & crack wep-key, thì bạn nên dùng một công cụ, sử dụng command để đi từ đầu đến cuối, ví dụ như Aircrack-ng hoặc Aircrack-PTW, như đã giới thiệu ở trên.

Ở các công cụ này, việc dò tìm được tiến hành từng bước:

- Detect Access point (tìm được MAC address Access point, SSID name..)
- Send MAC address giả mạo, để tạo và duy trì kết nối với Access point (fake MAC)
- Thu thập Wep IVs packets, càng nhiều càng tốt (Wep 128 bits, phải trên 250.000 packets)
- Và cuối cùng là chạy chương trình để crack capture file, tìm wep key.

Nhưng tóm lại, với Aircap adapter đã setup kèm theo Driver và Cain & Abel, thì bạn mất không quá 10' để crack Wep key (128 bits).

Công việc chính của bạn, là chỉ nhìn vào giao diện đang vận hành của Cain & Abel, theo dõi số lượng Unique WEP IVs packets, đạt ngưỡng trên 250.000 packets. Sau đó đó nhấn nút giải mã với Korek's Wep hay PTW attack.

Korek's WEP Attack

Keys tested: 50
 WEP Key Length: 128 bits
 Initial part of the key (Hex):
 WEP IVs: 1702528
 Fudge Factor: 2
 Last KB Brute-Force: last key byte
 Keyspace:
 alfa-numeric keys only
 BCD hex digits only

Korek's Attacks

A_u15 A_u13_2 A_s5_2 A_u5_2 A_s3 A_4_u5_2
 A_s13 A_u13_3 A_s5_3 A_u5_3 A_4_s13 A_neg
 A_u13_1 A_s5_1 A_u5_1 A_u5_4 A_4_u5_1

KB	Depth	Byte (vote)	
0	0/ 1	6C(277)47(13)21(12)97(12)05(0)F0(0)	l
1	0/ 1	6F(280)8B(27)13(24)CC(15)9C(12)9D(8)	o
2	0/ 1	63(249)58(15)86(15)28(15)9F(12)39(0)	c
3	0/ 1	61(235)47(28)B8(28)36(24)01(15)D0(15)	a
4	0/ 1	6C(196)B5(24)99(15)68(13)8D(13)57(12)	l
5	0/ 1	6E(314)3E(45)41(28)D2(24)18(15)40(15)	n
6	0/ 1	65(186)8E(27)C9(25)5A(15)7D(13)E3(13)	e
7	0/ 1	74(272)5B(39)31(28)CC(25)0B(15)EC(13)	t
8	0/ 1	6B(110)18(26)B2(15)06(15)61(15)4D(13)	k
9	0/ 1	65(684)64(24)D4(15)EB(15)12(15)F6(15)	e
10	0/ 1	79(280)2D(30)01(30)31(28)77(24)F0(15)	y
11	0/ 1	30(326)7B(81)0E(41)1C(39)A5(28)19(24)	0

WEP Key found !
 ASCII: localnetkey00
 Hex: 6C6F63616C6E65746B65793030

Start Exit

Attack tìm wep key với Korek's

 *Video crack Wep Key với Aircap và Cain & Abel*

Network Security Articles 2008 - www.Nis.com.vn