
Aurora 3D Animation Maker

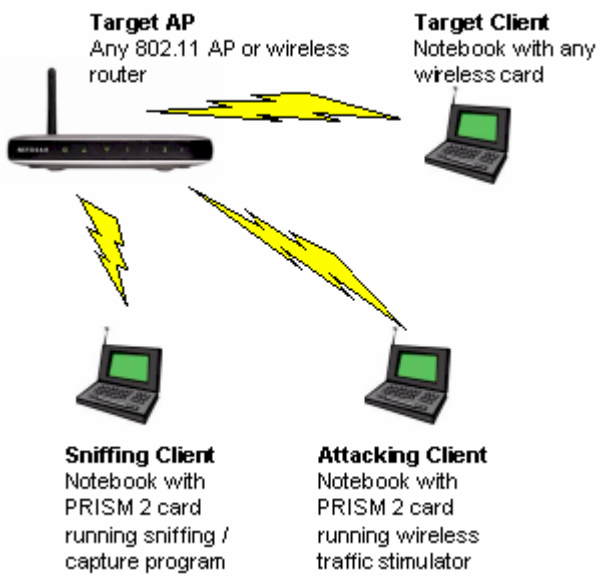
Kỹ thuật dò khóa WEP của mạng WiFi step by step

Hàng trăm và có thể là hàng nghìn bài báo viết về cách tấn công WEP, nhưng có bao nhiêu người thực sự có thể crack được WEP, những beginner thường nản lòng với những comand của nó và những loại card yêu cầu và những điều phức tạp hơn là không wen với môi trường linux. Trong phần này chúng tôi sẽ hướng dẫn từng bước cách hack WEP.

Bài đọc đầu tiên sẽ giúp các bạn xây dựng một mô hình mô phỏng và hướng dẫn lướt qua những phần của crack WEP, việc tiếp cận một cách tiêu chuẩn hóa và đa dạng để mà bạn có thể tập trung vào những công cụ crack WEP mà không bị cản trở bởi những lỗi hardware hay software.

Toàn bộ quá trình được làm với những software có sẵn và không yêu cầu những hardware đặc biệt chỉ một vài cái laptop với mấy cái card wireless là đủ.
Bài đầu tiên sẽ giúp bạn build một cái lab và hướng dẫn scanport của crac wep, sau hết, các bạn cần kiếm một cái document để tìm hiểu trước khi có thể crack nó
Bài hai sẽ mô tả cách kích hoạt thằng access point để tạo ra traffic và quá trình sử lí dữ liệu sau khi đã capture, sau hai bài này bạn có thể crack được wep key rùi đó.
Bài ba sẽ giúp chúng ta các skill bảo mật nhằm chống lại sự xâm nhập vào wireless.
Mặc dù WEP crack có thể làm được trên cùng một laptop nhưng lý tưởng nhất là bạn nên làm trên hai máy, một máy thực hiện tấn công để kích thích luồng data để đủ lượng data bắt được trong một thời gian ngắn, trong khi đó máy kia sẽ sniff hoặc capture luồng data do máy đầu tạo ra.

Thật ra bạn có thể sử dụng trên một máy với một wireless card, nhưng tui khuyên điều này không nên tại thời điểm mới bắt đầu, nó thường bắt gặp những nhầm lẫn trong những việc bạn đang làm, và tui nhận ra rằng những chương trình audit thường hay gặp một chút không ổn định khi dùng cách này.



chú ý rằng dùng một cái active attack và một cái passive capture sẽ làm tăng cơ hội thành công hơn, và tăng tốc độ quá trình crack bằng cách nó sẽ giúp sinh ra nhiều packet hơn là môi trường bình thường.
và đây là danh sách hardware cần thiết có trong lab của chúng ta:

wireless accesspoint: sẽ là đích ngắm của chúng ta..hehe..loại nào cũng được
môt laptop với một card wireless có thể sử dụng được: đây sẽ là máy target và không quan trọng cái chipset của thằng wireless card. Vì nó là máy thừa mà..hhihih
hai laptop có card wireless có chipset PRISM 2: một vài chương trình chẳng hạn như kismet có thể hỗ trợ đa dạng các loại wireless card, nhưng tui khuyên là nên dùng card có chipset được nói như trên, bạn có thể sử dụng những loại external có antennaes thì càng good, nhưng không có cũng chẳng sao(it's up to you).
Trong khi crack WEP key phải có những tool hack chứ..hihihi…tới đây thì các bạn tìm trên mạng nha Auditor security collection CD, hay ra mấy shop bán software tìm nha hoặc xài thằng BACK TRACK đây là phiên bản mới của thằng trên, link down ftp://mirror.switch.ch/mirror/backtrack/bt2final.iso
Việc set up đúng như lab của chúng ta thì rất là quan trọng, bởi vì bạn muốn điều khiển được môi trường bạn làm việc, bạn cũng nên nghĩ tới việc ngăn accident không thể lường trước được tới những access point của hàng xóm chứ đúng không nào, bởi vi trong phần hai một vài attack của chúng ta có thể kick off mấy thằng client của access point đó…hahah nguy hiểm thật, muốn đi tiếp chứ?

Bước đầu tiên là phải config cái lab đã, một target access point và cái thằng laptop dư thừa mình đã nói ở trên, cái access point được cấu hình security với WEP key mà chúng ta sẽ crack, security 64 bit, và nhớ đặt SSID.
Bạn nên note lại những cái bạn vừa cấu hình để sau này còn đối chứng chứ:

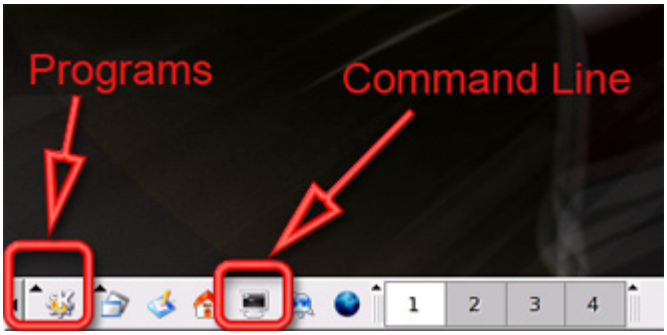
MAC address của ACP
SSID
CHANEL
KEY

Sau đó config thằng laptop dư thừa, kết nối bình thường tới thằng accesspoint,nhớ đăng nhập có key đàng hoàng nha.
Sau đó ghi lại cái MAC của thằng dư thừa này.
Tới đây thì mạng WLAN của mình đà được config
Bây giờ shutdown thằng dư thừa đó được rùi:
Đến đây chắc mình phải định nghĩa cho từng thằng laptop thui,sợ các bạn bị nhầm lẫn đó mà

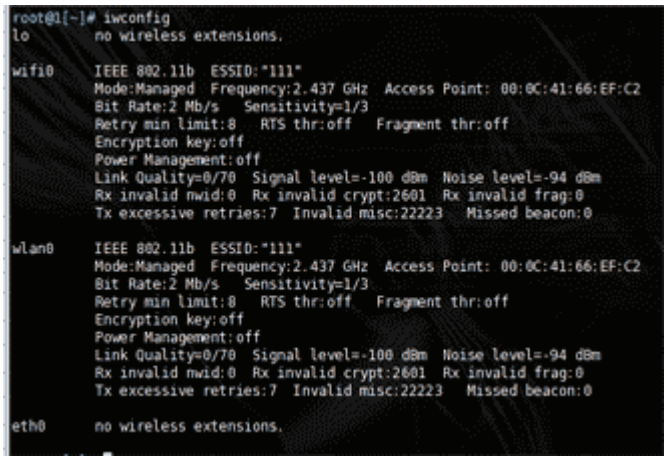
Mạng lab: WLAN
Thằng dư thừa: target computer
laptopA:
laptop B
accesspoint: target ACP

OK vào việc nào: (đi tiếp không)(đủ sức thì đi không đủ thì đừng đua nha)hiihiih
Đã đến lúc config laptopA và B để mà scan WLAN và sniff traffic tấn công để lấy luồng traffic
Trước tiên là cho cái disk hack vào boot from cd (ko bít các bạn có bít làm ko nhỉ) vào cmos chọn first là cd, nhớ là gắn card wireless vào nha
Sau khi đã điều chỉnh độ phân giải thích hợp từ auditor boot menu nó sẽ cài vào RAM
Và bạn sẽ ở màn hình như thế này đây:

hai biểu tượng quan trọng sẽ là program và commandline ở phía dưới bên trái màn hình

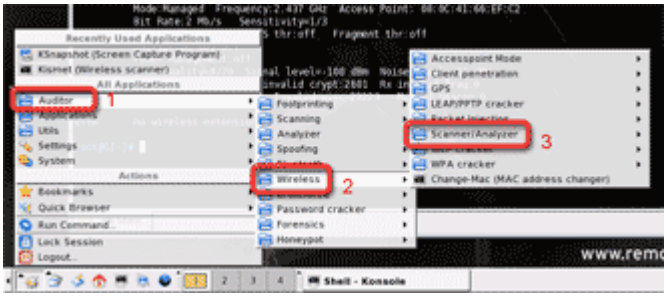


trước khi tiếp tục làm bạn nên chắc rằng wirelesscard đã gắn vào đúng và được config bằng auditor:
click vào biểu tượng command line rùi wuýnh nó….hihiihih
IWCONFIG

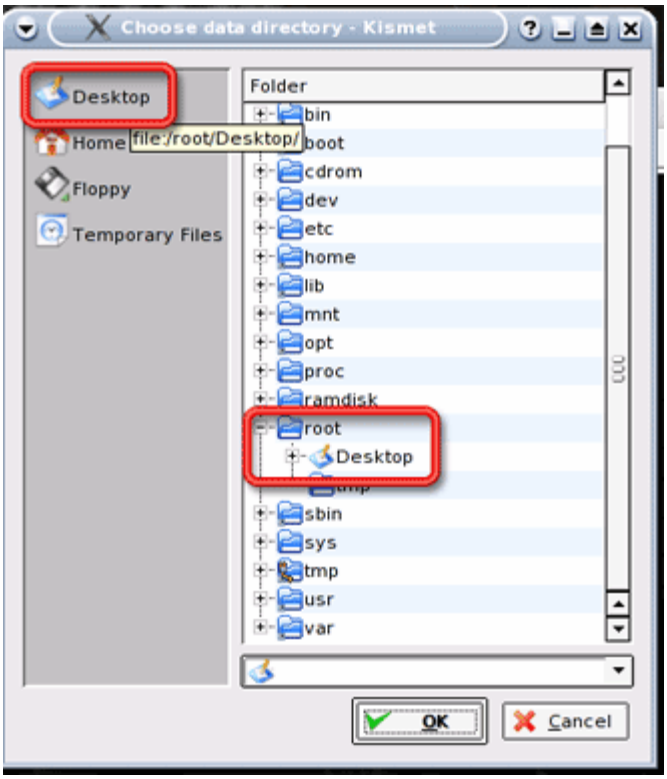


Trong số những thông tin mà auditor xổ ra hãy chú ý thông số wlan0 vậy là card có chipset PRISM – based card và auditor đã detect được card mạng của bạn rùi đó, bạn có thể cấu hình tương tự với laptopB, xong rùi shutdown …hihiihiiihi, vì bạn sẽ không cần nó cho đến phần hai, nơi mà bạn sẽ học làm sao để kick data cái traffic và sẽ capture bằng laptopA.Đã bắt đầu dùng kismet rùi (chiến đấu thui)
Đây là công cụ hữu ích để detect WLAN, ACP
Nó cũng capture traffic nhưng có một chương trình hay hơn đó là airodump một phần của aircrack, công cụ rất tốt trong công việc crack WEP cho nên chúng ta sẽ dùng và chắc rằng card wireless đang

làm hoạt động để scan wireless và capture traffic.
Vào program icon, sau đó auditor- wireless – scanner – analyzer – và cuối cùng là kismet

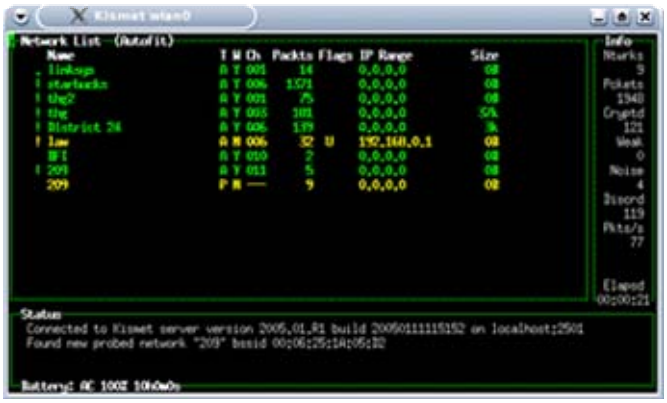


Thêm vào đó để scan mạng wireless, kismet sẽ capture dữ liệu vào một file để sau này phân tích, cho nên kismet yêu cầu nơi để lưu file đã được capture, click vào desktop và sau đó ok

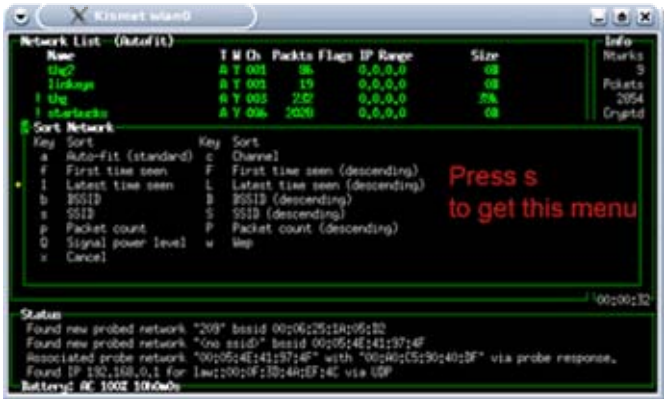


Kismet cũng yêu cầu một cái prefix cho file được capture, thay tên mặc định bằng capture.

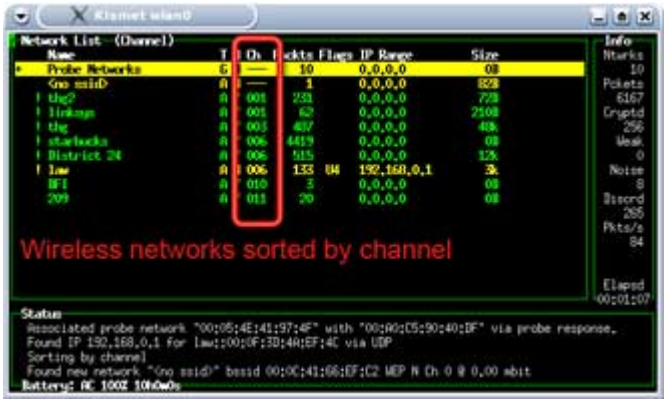
Khi kismet hoạt động nó sẽ liệt kê tất cả các mạng wireless trong một range, bao gồm cả target ACP bạn đã setup, channel (giống kênh đào áh),dưới cột CH column, những cái mà bạn ghi lúc nãy đó, check lại xem giống ko?.
Nếu kismet liệt kê nhiều ACP gần cái lab của bạn, thì nên chuyển cái lab ấy ra xa cái ACP của người ta một tí (đụng tới kẻo mang hoạ..hihihi).



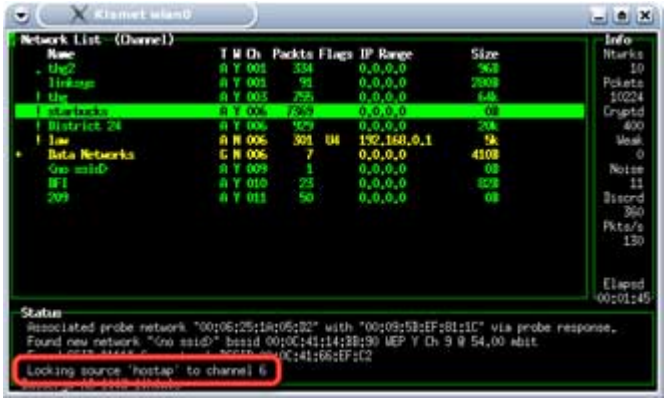
Trong khi kismet dang hoạt động bạn sẽ thấy số packet đang thay đổi cho tất cả các ACP ở bên phải màn hình.
Kismet hiện ra tổng số network được tìm thấy, số packet được capture và tổng số packet được encrypted, thậm chỉ cả những target computer đã tắt ngúm đi rùi, thì nó cũng được show ra những packet từ ACP (vì cứ khoảng vài giây thằng ACP sẽ phát ra đèn báo hiệu và nói (lạy ông tui ở bụi này…heheh).
Kismet hoạt động trong chế độ autofit nên sẽ không liệt kê đầy đủ các ACP theo thứ tự của nó, nhấn S để sort, ở đây bạn có thể xác định thứ tự sort, nó sẽ dễ nhìn hơn khi ta sort nó.
Nhấn C thì ACP sẽ theo channel



Kismet mặc định sẽ nhảy channel từ 1 tới 11(hiphop…hihi) dùng trỏ chuột để di chuyển highlight tới SSID của bạn và nhấn L kissmet sẽ khoá cái channel của SSID đó,



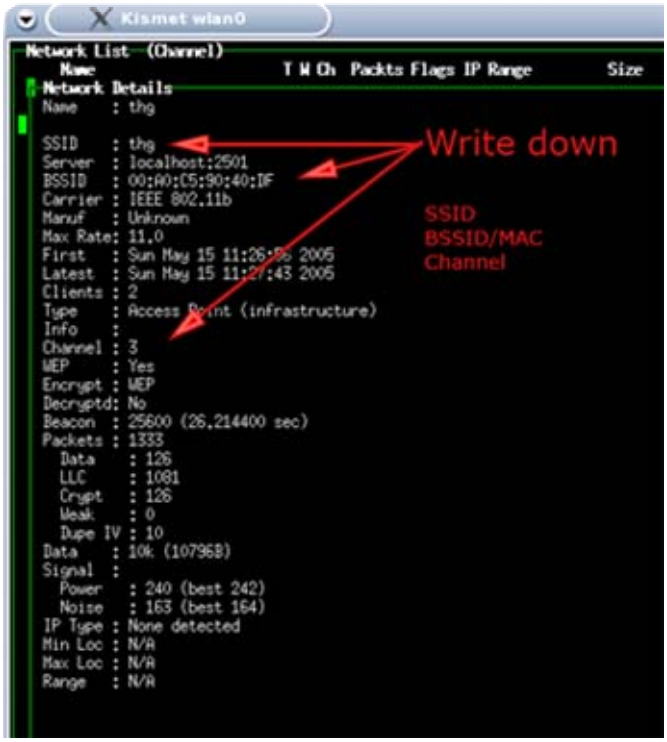
bạn sẽ chú ý rằng số packet của những ACP có thể vẫn tiếp tục tăng, điều này là bởi vì các channel sẽ gối lên nhau theo thứ tự.



Bây giờ một điều hợp lý là chúng ta biết kissmet đang hoạt động, chúng ta sẽ xem điều gì sẽ diễn ra khi máy target computer trên mạng bắt đầu trao chuyển thông tin,bắt đầu kết nối thằng dư thừa vào mạng trong khi vẫn scan kismet, khi thằng dư thừa boot vào window và kết nối với ACP bạn chú ý rằng một lượng dữ liệu được mã hoá nhanh chóng được kissmet capture, bạn sẽ dùng những gói này để attack trong phần hai.
Tại thời điểm này bạn đã biết cách cơ bản để tiếp cận với crack WEP, 1 ACP, 2 laptop sniff và attack đang hoạt động, và cũng wen với việc tìm đường vào của software trong disk auditor, dùng kismet để tìm ra range wireless.
Phần hai chúng ta sẽ dùng laptop B để kick cái WLAN sinh ra traffic và chúng ta sẽ capture và thực sự crack. Cho đến khi đó bạn đã thực sự quen với việc dùng kismet, tới WLAN và khám phá vài công cụ khác có trong disk auditor.

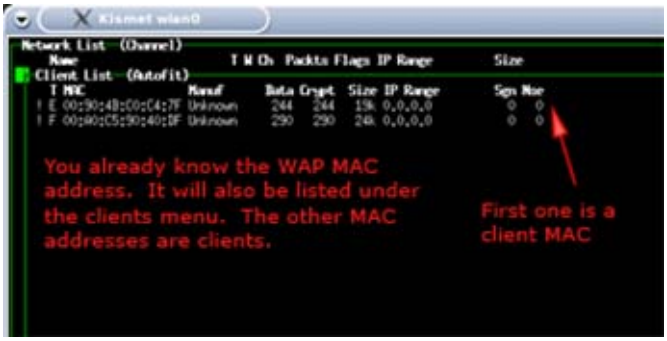
Phần hai:
ở phần một chúng ta đã chỉ ra cách basic để crack wep, config wlan và hai laptop sniff và attack.
Trong phần này chúng tôi sẽ hướng dẫn làm sao để dùng thêm những công cụ có trong auditor cd để capture traffic và dùng nó để crack wep, chúng tôi cũng hướng dẫn làm sao để deauthentication (chứng thực lại) và packetreplay để kick WLAN sinh ra traffic là một yếu tố chính để tiết kiệm thời gian crack
Tuy nhiên trước khi bắt đầu, chúng ta hãy làm một vài điểm cần chú ý mà có thể tiết kiệm thời gian và khả năng sử dụng những chương trình
Để sử dụng thành công, bạn cần có những căn bản về thuật ngữ network và những yếu tố căn bản, bạn cũng nên biết cách ping mạng, open command prompt và nhập những command, căn bản về linux thì càng tốt.
Những quy tắc yêu cầu về hardware đã được bàn về ở phần 1
Một mạng WLAN và một thằng dư thừa kết nối với ACP
Và điều quan trọng trong mô hình lab này là không được truy cập vào những ACP của người khác mà không được sự đồng ý của chủ
Cũng chý ý là điều này có thể thực hiện trên chỉ một laptop không nhất thiết là hai máy, nhưng để cho rõ ràng và tránh nhầm lẫn chúng ta nên sử dụng hai máy laptop.
4 tool chính dùng trong phần này là AIRODUMP, VOID11,AIRREPLAY VÀ AIRCRACK đều có trên disk auditor.
AIRODUMP : scan mạng wireless và capture packet vào một nơi nào đó
VOID11: sẽ deauthenticatiom (chứng thực lại) computer từ ACP , sẽ áp đặt cho chúng kết nối lại với ACP, tạo ARP request (lấy MAC)
AIRREPLAY: tóm cái ARP request rồi gửi lại tới thằng ACP
AIRCRACK: sẽ lấy những file capture được tạo ra bởi AIRODUMP
ở phần1: bạn đã sử dụng kismet để lấy những thông tin, bây giờ hãy ghi ra giấy để nhớ sau này còn xài.
MAC của ACP
MAC của thằng dư thừa

CHANNEL đang sử dụng của ACP
WEP KEY đã được set up trong ACP
Trong đời thực một vài người muốn break vào trong mạng wireless thông thường lấy những thông tin (MAC của ACP , channel của ACP, và target computer)
Những điều này gọi là "zero knowledge", nếu như kẻ tấn công có tất cả các thông tin cần thiết điều đó được gọi là cuộc tấn công "full knowledge" lúc đó không còn gì là thách thức đối với họ, chúng ta cứ cho rằng chúng ta không bít gì hết và mô tả làm sao để lấy những thông tin cần thiết.
Tìm MAC của ACP thì không có gì khó đối với chúng ta với việc xài thằng kismet, hãy làm tương tự như ở phần một tôi đã hướng dẫn, để lấy được SSID, MAC, và CHANNEL của ACP, vậy là những zero knowledge đã được chuyển qua tất cả các thông tin cần thiết để chạy crack WEP



có vài trường hợp người ta sử dụng giấu cái SSID không cho broadcash ra ngoài nhằm mục đích ngăn chặn một số phần mềm nhưng đối với kismet thì đừng có nằm mơ, nó sẽ liệt kê tất cả những thông tin mà nó capture được.

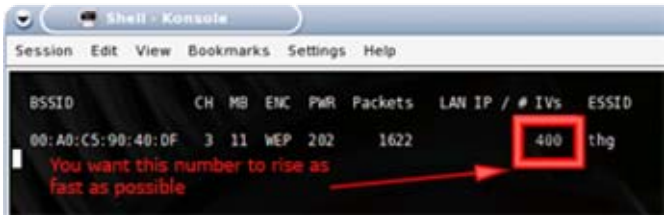
Tìm MAC của client:
Chúng ta cần một thông tin cuối cùng để bắt đầu quá trình crack, MAC của client kết nối với ACP, quay lai kismet nhấn Q để quay lại menu chính, sau đó nhấn shift + C để liệt kê danh sách MAC của client, MAC sẽ được liệt kê bên khung bên trái



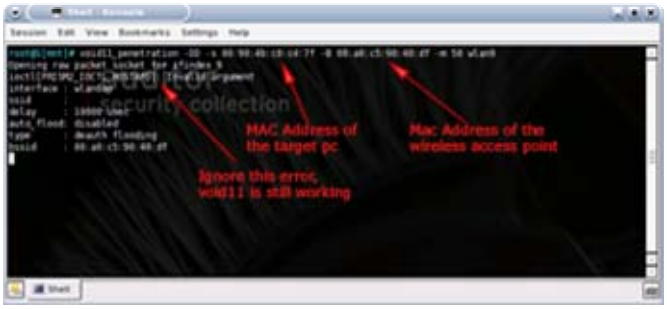
Nếu như bạn không thấy MAC của client thì phải chắc rằng cái thằng dư thừa đã kết nối tới ACP, nếu như không có thì không thể thực hiện các bước tiếp theo, vì lab của chúng ta cần có một client đã kết nối tới ACP.
Capture dữ liệu với AIRODUMP
Không cần nhắc đến tốc độ kinh khủng của nó, nhưng cũng cần phải có đủ packet để làm việc trong quá trình crack WEP, nó có tác dụng capture packet vào một file để sau này phục vụ cho AIRCRACK, chúng ta hãy xem chúng hoạt động như thế nào nhá.
Bạn có thể sử dụng laptop nào cũng được cả, nhưng trong lab này chúng ta sử dụng laptopA,
Mở airodump và gõ vào command sau:

Commands for setting up airodump
iwconfig wlan0 mode monitor
iwconfig wlan0 channel THECHANNELNUM
cd /ramdisk
airodump wlan0 cap

Hãy lưu ý rằng thay THECHANNELNUM=SỐ CHANNEL mà ACP bạn đang xài
/ramdisk là nơi data bị capture lưu
nếu như gần nơi bạn có các ACP khác nhưng nếu bạn muốn audit cái ACP của bạn, hãy thêm dòng lệnh như sau ở cuối command trên
airodump wlan0 cap1 MACADDRESSOFAP
điều này sẽ hướng dẫn AIRODUMP chỉ lưu những packet của target ACP
bạn có thể exit AIRODUMP bằng cách nhấn ctrl + C và nhấn ls –l sẽ liệt kê ra các file được lưu và chú ý phần đuôi file là .cab nếu capture thành công nó sẽ chỉ vài kb thôi
phần Ivs:



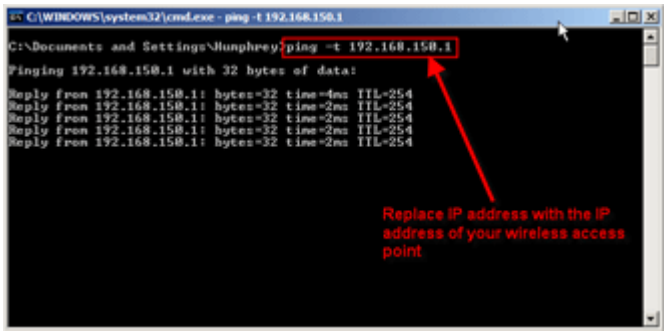
Trong khi AIRODUMP đang chạy, bạn sẽ thấy MAC của ACP được liệt ra ở BSSID phần bên trái, bạn cũng thấy packet count và Ivs count tăng lên, đây là điều thường diễn ra trong bất kì traffic nào thậm chí cả khi bạn không đang lướt web và nếu như bạn duyệt web hay email trên target computer thì bạn sẽ thấy ở mục IVs tăng lên, IVs là quan trọng nhất nó quyết định bạn có thể crack được hay không, thông thường thì thông số IVs trong khoảng 50.000 tới 200.000 cho 64bit và 200.000 tới 700.000 cho 128 bit.
Bạn cũng phải chú ý rằng ở chế độ traffic bình thường thì IVs không tăng nhanh nó có thể mất một giờ hay thậm chí cả ngày để capture đủ dữ liệu cho việc crack thành công, nhưng may thay chúng ta đã có một công cụ giúp ta làm tăng tốc độ này
Cách nhanh nhất để sinh ra nhiều packet là kick cho thằng WLAN luôn ở chế độ busy, chúng ta có thể thử bằng cách download file hoặc ping từ thằng target tới một địa chỉ nào đó
Vd: ping –t –l 5000 (ip nào đó)
Và tới đây thì VOID11 bắt đầu vào cuộc:
VOID11 được dùng để deauthenticate giữa target computer với ACP, để tạo ra traffic, target computer sẽ bị kick off ra khỏi mạng và tự động kết nối lại với ACP, trong quá trình kết nối lại thì traffic sẽ được sinh ra mà capture



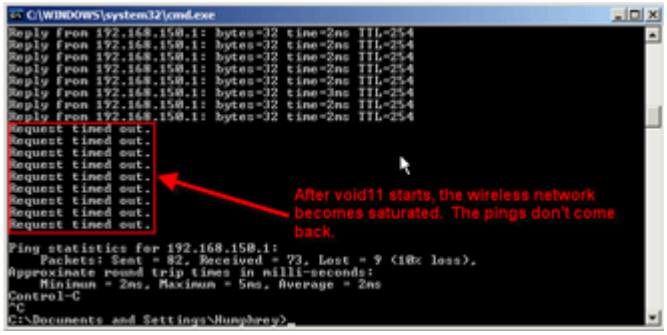
Bắt đầu với laptopB với auditor cd được cho vào,sau đó mở shell và đánh vào lệnh sau:

Commands for setting up a void11 deauth attack
switch-to-hostap
cardctl eject
cardctl insert
iwconfig wlan0 channel THECHANNELNUM
iwpriv wlan0 hostapd 1
iwconfig wlan0 mode master
void11_penetration -D -s MACOFSTATION -B MACOFAP wlan0

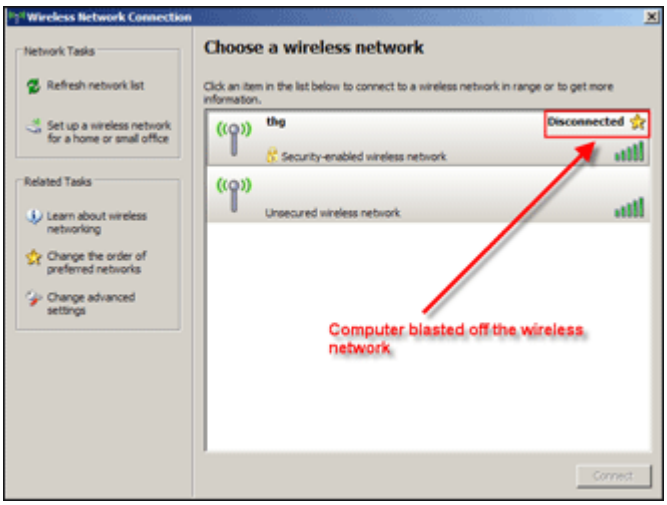
Chú ý thay THECHANNELNUM = kênh đang hoạt động trên ACP
MACOFSTATION là MAC của target client và MACOFAP là MAC của ACP
Trong quá trình chạy có thể VOID11 báo một thông báo lỗi nhưng bạn đừng bận tâm (không ăn nhằm gì tới hoà bình thế giới cả)
Trong khi laptopB đang chạy thì chúng ta hãy xem điều gì sẽ xảy ra trên máy target computer nha, mạng sẽ từ từ chậm xuống thậm chí ngừng hẳn, và vài giây sau sẽ bị ngắt lun ra khỏi mạng (ác quá ha)
Bạn có thể kiểm tra điều này bằng cách vẫn tiếp tục ping tới từ target tới ACP
Đây là trước khi chạy VOID11 trên máy laptopB



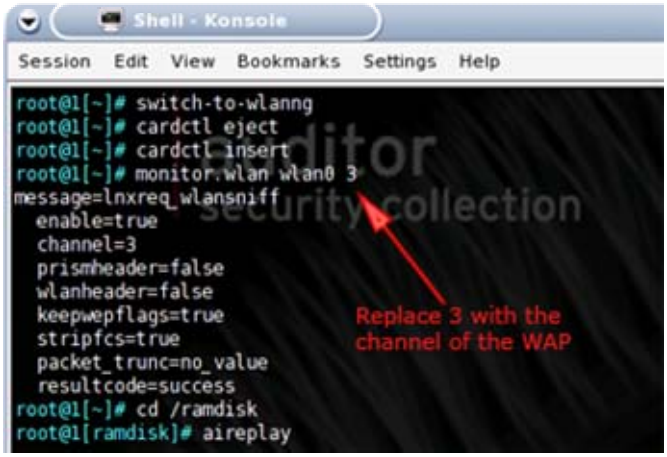
Và trong khi chạy VOID11,nếu bạn stop VOID11 thì ping sẽ trả lại bình thường



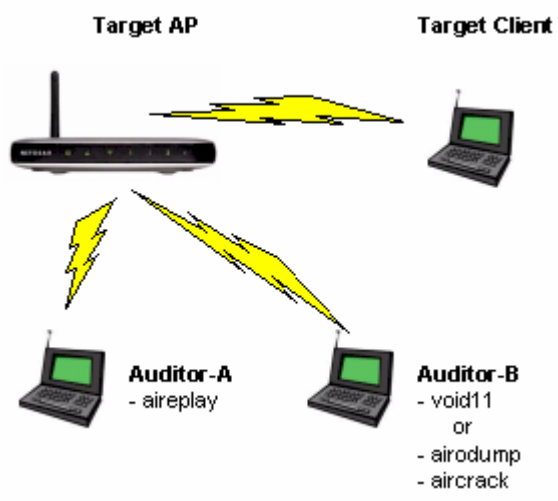
Và bạn có thể check một cách cụ thể trên property của card mạng wireless trên target



Và bạn hãy chú ý trên laptopA số IVs tăng lên rất nhanh trong vài giây từ 100 – 200, điều này xảy ra là vì quá trình kết nối lại của target và ACP
Packet repaly dựa vào AIRREPALY
Trong khi deauthentiace sinh ra traffic, nó thường không đủ tăng tốc quá trình làm cho IVs của chúng ta tăng nhanh, để tăng hữu hiệu tạo ra traffic chúng ta sẽ dùng tới một công cụ đó là replay attack, replay attack hoạt động dựa vào packet bắt được do target sinh ra, sau đó lừa client là nó đã nhận được packet và lặp lại packet một cách thường xuyên hơn bình thường.
Stop deauthenticate attack sau đó mở AIRREPLAY lên sử dụng những capture file, đó là những ARP request



Chúng ta hãy bắt đầu với tình trạng clean, nghĩa là restar hai laptop A,B. và hãy chú ý rằng laptopA chỉ chạy AIRREPLAY với mục đích kick traffic mạng và IVs nhằm tiết kiệm thời gian crack và laptopB đang sử dụng AIRODUMP, hay VOID11 và đang sử dụng AIRCRACK để phục vụ cho việc crack dựa vào những packet đã thu lượm được



Trước tiên chúng ta hãy khởi động AIREPLAY trên máy laptopA và nhập vào các command sau:
Commands to set up aireplay to listen for an ARP packet
switch-to-wlanng
cardctl eject
cardctl insert
monitor.wlan wlan0 THECHANNELNUM
cd /ramdisk

aireplay -i wlan0 -b MACADDRESSOFAP -m 68 -n 68 -d ff:ff:ff:ff:ff:ff

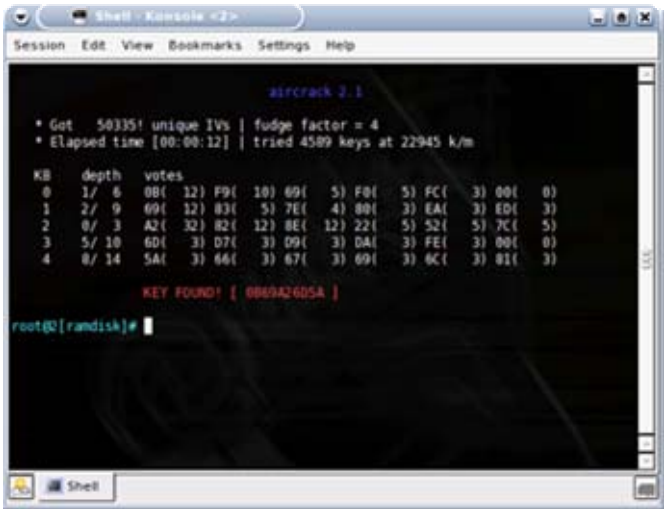
Chú ý switch-to-wlanng và monitor .wlan là những cái đã được tích hợp sẵn trong disk để đơn giàn hoá khi nhập command
thay thế THECHANNELNUM = số channel mà bạn tìm thấy được trong các bước trước
và MACADDRESSOFAP = MAC của ACP
nào bây giờ tới máy target computer bật nó lên kết nối với ACP sau đó sang máy laptopB bật VOID11 và quan sát, ta sẽ thấy rằng tín hiệu mạng của client từ từ giảm xuống và có khi mất hẳn, và bạn cũng thấy rằng AIREPLAY tăng lên rất nhanh, thỉnh thoảng AIREPLAY thông báo một packet tóm được và hỏi bạn có muốn replay nó không

Bạn sẽ muốn một packet match những tiêu chuẩn sau:
• FromDS - 0
• ToDS - 1
• BSSID - MAC Address of the Target AP
• Source MAC - MAC Address of the Target computer
• Destination MAC - FF:FF:FF:FF:FF:FF

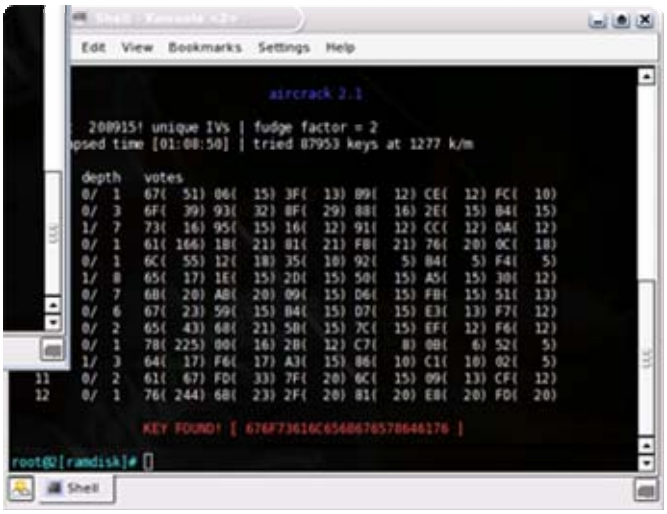
Nhấn chữ n cho sự không đồng ý và AIREPLAY sẽ resume lại và y để xác nhận nếu match những tiêu chuẩn trên để AIREPLAY sẽ chuyển từ chế độ capture sang chế độ replay, ngay lập tức quay trở lại laptopB và stop VOID11
Capture packet dựa vào deauthenticate được xem là phần gian xảo nhất trong phần crack. Trong khi nó tạo ra traffic, nưng nó tạo ra không được nhiều lắm trong quá trình client reconnect tới ACP, capture có thể phức tạp hơn tuỳ thuộc vào driver của card và hệ điều hành của client , VOID11 có thể dễ dàng áp đảo thằng client bằng với một deauthen packet thậm chí không có đủ thời gian để reconnect lại.
Thỉnh thoảng bạn có thể may mắn từ những packet đầu nhưng thỉnh thoảng bạn cũng phải đợi cho tới packet cần match
Trong command của AIREPLAY một tham số -d cho chế độ delay
Tại thời điểm này thì laptopA đang chạy AIREPLAY có số IVs tạm đủ cho chúng ta thực hiện việc cracking, stop VOID11 trên máy laptop B và bật AIRODUMP lên, đánh vào những command sau:
Starting up airodump after stopping void11
switch-to-wlanng
cardctl eject
cardctl insert
monitor.wlan wlan0 THECHANNELNUM
cd /ramdisk
airodump wlan0 cap1

chắc các bạn cũng đã biết làm như thề náo rồi đúng không, chỉ có dòng cuối nếu trong mạng bạn có nhiều mạng wireless thì bạn hãy gõ một command tại cuối dòng là
airodump wlan0 cap1 MACADDRESSOFAP
chắc lệnh trên bạn cũng hiểu phải không nào , mình đã giải thích nhiều rồi mà
sau khi AIRODUMP khởi động bạn sẽ thấy IVs tăng lên rất nhanh khoảng 200 /s, cám ơn AIREPLAY trên laptopA
trong khi AIRODUMP đang write IVs vào file ta hãy bắt đầu quá trình chạy AIRCRACK, ta có thể cho chạy song song, mở AIRCRACK và nhập command sau :
Starting aircrack
cd /ramdisk
aircrack -f FUDGEFACTOR -m MACADDRESSOFAP -n WEPKEYLENGTH -q 3 cap*.caplưu ý
FUDGEFACTOR là một số nguyên và mặc định là 2
MACADDRESSOFAP = MAC của ACP
WEPKEYLENGTH đọc chắc các bạn cũng hiểu là chiều dài bit của WEBKEY thông thường là 64 và 128

bạn có thể thay số 2 bằng một số nào đó lớn hơn nhưng sẽ làm quá trình chậm hơn, nhưng có kết quả chắc hơn, nó sẽ give up nếu như không tìm thấy 64 bit format
bạn có thể nhấn ctrl + C để stop và up arrow để resart lại lệnh vừa rồi của AIRCRACK, nó sẽ update packet và tham số -p cho quá trình multi process, thỉnh thoảng bạn sẽ được màn hình như sau:



chúng ta đã hoàn tất quá trình crack WEPKEY với 64bit chỉ trong vòng chưa tới 5 phút bao gồm quá trình scan và crack với AIRCRACK và kick traffic với AIREPLAY đang chạy, đôi khi bạn có thể crack khi IVs lên đến 25000 nhưng hầu hết là nên trên 100000 và 128 bit thì còn hơn nữa khoảng từ 150000 đến 700000, có nhiều IVs thì càng good cho việc crack, điều quan trọng là bạn phải điền vào lenghkey mà bạn muốn crack và không có công cụ nào cung cấp điều đó trong disk này, nên bạn nên thử cả hai 64 và 128



Và đây là lenghkey 128 bit. Bạn cũng nên có một máy có cấu hình mạnh cả cpu và một lượng khá về RAM, bạn cũng có thể tách riêng quá trình sử lý bằng cách lưu file capture vào một máy khác máy đó không cần phải kết nối vào mạng chỉ cần chạy AIRCRACK sử lý những packet mà AIRODUMP lượm về, hoặc có thể lưu trên thiết bị USB, chỉ việc mở command len và nhập command sau:

Saving capture files to USB flash drive
mkdir /mnt/usb
mount -t vfat /dev/uba1 /mnt/usb
copy /ramdisk/cap*.cap /mnt/usb
umount /mnt/usb

Kết luận:
bảo mật bằng wepkey không phải là phuong pháp tốt, “wired equivalent privacy”, chúng ta nên sử sụng chế độ bảo mật cao hơn là WPA2 “WIFI PROTEC ACCESS” version2

sau đây là summary commad:
Commands for setting up airodump
iwconfig wlan0 mode monitor
iwconfig wlan0 channel THECHANNELNUM
cd /ramdisk
airodump wlan0 cap
Commands for setting up a void11 deauth attack

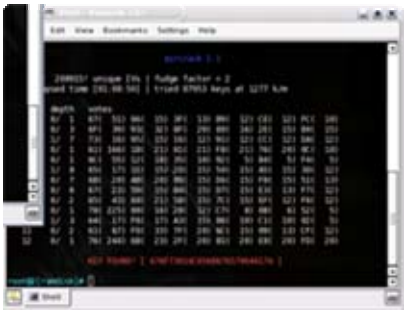
switch-to-hostap
cardctl eject
cardctl insert
iwconfig wlan0 channel THECHANNELNUM
iwpriv wlan0 hostapd 1
iwconfig wlan0 mode master

void11_penetration -D -s MACOFSTATION -B MACOFAP wlan0
Commands to set up aireplay to listen for an ARP packet
switch-to-wlanng
cardctl eject
cardctl insert
monitor.wlan wlan0 THECHANNELNUM
cd /ramdisk

aireplay -i wlan0 -b MACADDRESSOFAP -m 68 -n 68 -d ff:ff:ff:ff:ff:ff
Starting up airodump after stopping void11
switch-to-wlanng
cardctl eject
cardctl insert
monitor.wlan wlan0 THECHANNELNUM
cd /ramdisk
airodump wlan0 cap1
Starting aircrack
cd /ramdisk
aircrack -f FUDGEFACTOR -m MACADDRESSOFAP -n WEPKEYLENGTH -q 3 cap*.cap

Dò khóa WEP của mạng WiFi và cách bảo vệ

Friday, 20 June 2008 04:08



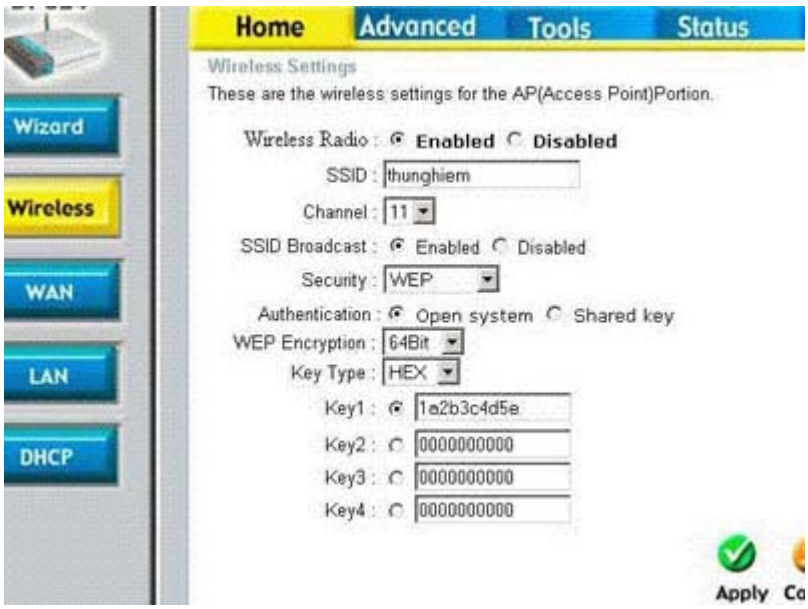
Hiện nay công nghệ mạng ko dây wifi đã khá phổ biến, được nhiều nơi sử dụng vì tính tiện dụng của nó, nhưng bên cạnh đó vấn đề bảo mật cho wifi cũng gây nhức đầu cho ko ít người, nhất là người dùng gia đình & ko chuyên. Bài viết này tôi xin đề cập đến khả năng dò khoá mã hoá WEP (wep key) của wifi và các giải pháp phòng chống.

Giới thiệu chung về wifi và WEP.

WIFI – WIreless FIdelity (thuật ngữ này hiện giờ vẫn còn đang gây tranh cãi vì nó chẳng có nghĩa gì cả) là một bộ giao thức cho thiết bị ko dây dựa trên chuẩn 802.11x bao gồm các Access Point và các thiết bị đầu cuối ko dây như pc card, usb card, wifi PDA… kết nối với nhau. Wifi sử dụng nhiều chuẩn mã hoá khác nhau nhằm bảo vệ tránh sự truy cập trái phép, vì tính đặc thù của kết nối ko dây là ko thể giới hạn về mặt vật lý truy cập đến đường truyền, bất cứ ai trong vùng phủ sóng đều có thể truy cập được, nên mã hoá là điều cần thiết đối với người sử dụng cần sự riêng tư, an toàn. Wifi hiện nay có 3 kiểu mã hoá chính gồm: WEP-Wired Equivalent Privacy , WPA-Wireless Protected Access và WPA2. WEP là kiểu mã hoá ra đời sớm nhất và được hỗ trợ phổ biến nhất bởi các nhà sx thiết bị wifi, đa số thiết bị wifi đều hỗ trợ wep sử dụng khoá mã hoá dài từ 40-128 bits. Gần đây nhiều người đã phát hiện ra điểm yếu trong phương thức mã hoá wep và đã đưa ra rất nhiều công cụ crack. Tuy nhiên cũng ko thể từ bỏ WEP ngay được vì nó đã được sử dụng phổ biến từ lâu, ko phải nhà sx thiết bị nào cũng kịp chuyển sang hỗ trợ các kiểu mã hoá khác với các thiết bị mà họ đã sx Vậy điểm yếu của WEP là ở đâu ? Do wep sử dụng phương thức mã hoá dòng (stream cipher), nó cần 1 cơ chế đảm bảo hai gói tin-packet giống nhau sau khi được mã hoá sẽ cho ra kết quả ko giống nhau nhằm tránh sự suy đoán của hacker. Nhằm đạt mục tiêu trên, một giá trị có tên IV (Initialization Vector) được sử dụng để cộng thêm với khoá của ta đưa vào, tạo ra khoá khác nhau sau mỗi lần mã hoá dữ liệu. IV là giá trị có độ dài 24 bit được thay đổi ngẫu nhiên theo từng gói dữ liệu, vì vậy thực tế wep key chúng ta được chỉ định chỉ còn 40bits với kiểu mã hoá 64bits và 104bit với kiểu 128bit trong các AP(access point), vì 24bit được dành cho việc tạo các IV này(các bạn thử để ý xem, khi nhập mật mã trong AP nếu chọn mã hoá 64bit ta chỉ có thể nhập được 5 ký tự nếu chọn mật mã kiểu string, hay 10 ký tự nếu chọn kiểu hexa, tương đương với 40bit). Do khi thiết bị gửi tạo ra IV 1 cách ngẫu nhiên nên bắt buộc phải được gửi đến thiết bị nhận ở dạng ko mã hoá trong header của gói tin, thiết bị nhận sẽ sử dụng IV & khoá để giải mã phần còn lại của gói dữ liệu. IV chính là điểm yếu trong mô hình mã hoá WEP, vì độ dài của IV là 24bits nên giá trị của IV khoảng hơn 16 triệu trường hợp, nếu cracker bắt giữ đủ 1 số lượng packet nào đó thì hoàn toàn có thể phân tích các IV này để đoán ra khoá-key mà nạn nhân đang sử dụng. Phần tiếp sau đây tôi sẽ mô tả mô hình mạng wifi thử nghiệm và cách thức để dò ra khoá mã.

Mô hình thử nghiệm và cách dò.

Mô hình thử nghiệm tôi giả lập là 1 mạng wifi giống thực tế bao gồm 1 AP hiệu DLink DI524 & 1 máy tính có card wifi, được gọi là AP & client “mục tiêu”, sử dụng kiểu mã hóa WEP 64bits với mật khẩu là 1a2b3c4d5e dạng hex (xem hình 1).



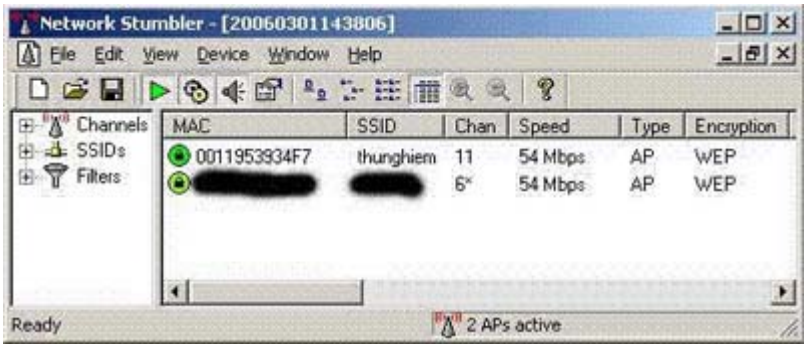
Hình 1: Giao diện Setup của AP thử nghiệm.

Công cụ crack tôi dùng bao gồm bộ chương trình phần mềm Aircrack 2.4 chạy trên linux, netstumbler, kismet, đĩa live cd linux, 1 máy laptop có 2 card wifi adapter hoặc 2 máy tính mỗi máy 1 card tương thích với aircrack.

Như người ta thường nói: biết người biết ta trăm trận trăm thắng, để crack mạng wifi mục tiêu, đầu tiên ta phải biết rõ mọi thông tin về mục tiêu như chính chủ nhân của nó vậy (tất nhiên chỉ có khóa mã là chưa biết thôi. Thế những thông tin cần biết là gì ?, đó là :

- SSID hoặc ESSID (Service Set IDentifier -hiểu nôm na là tên nhận diện của mạng, giống như tên workgroup của mạng LAN ngang hàng vậy), ở mô hình thử nghiệm này tôi đặt tên là thunghiem.
- Kênh – channel của mạng, ở đây tôi để là kênh 11.
- Kiểu mã hóa, ở đây là WEP 64 bit.
- Địa chỉ MAC address của AP & MAC card của máy mục tiêu.

Vậy dùng cái gì để thu thập những thông tin này ?. Đó là dùng NetStumbler (xem hình 2) chạy trên windows hoặc Kismet trên linux, netstumbler ko xem được MAC của client mục tiêu nên ta dùng kismet or chương trình airodump trong bộ công cụ aircrack để thu thập.



Hình 2: Dùng netstumbler để thu thập thông tin.

Sau khi thu thập đủ thông tin về mục tiêu, ta tiến hành sử dụng bộ aircrack. Aircrack là bộ công cụ nguồn mở chạy trên linux dùng để dò tìm khóa mã WEP/WPA rất mạnh được phát triển bởi Christophe Devine, có rất nhiều công cụ tương tự nhưng aircrack được ưa thích hơn cả vì mạnh & dễ dùng, tuy nhiên nó cũng hỗ trợ khá ít loại chipset wifi. Bộ aircrack có 3 công cụ chính ta sẽ dùng là:

- aireplay dùng để bơm-injection làm phát sinh thêm dữ liệu lưu thông trong mạng mục tiêu, đối với những mạng có quá ít dữ liệu lưu thông mạng ta phải dùng nó để làm giảm thời gian chờ đợi bắt giữ đủ số packet phục vụ cho việc dò tìm khóa. (hình ví dụ 3)

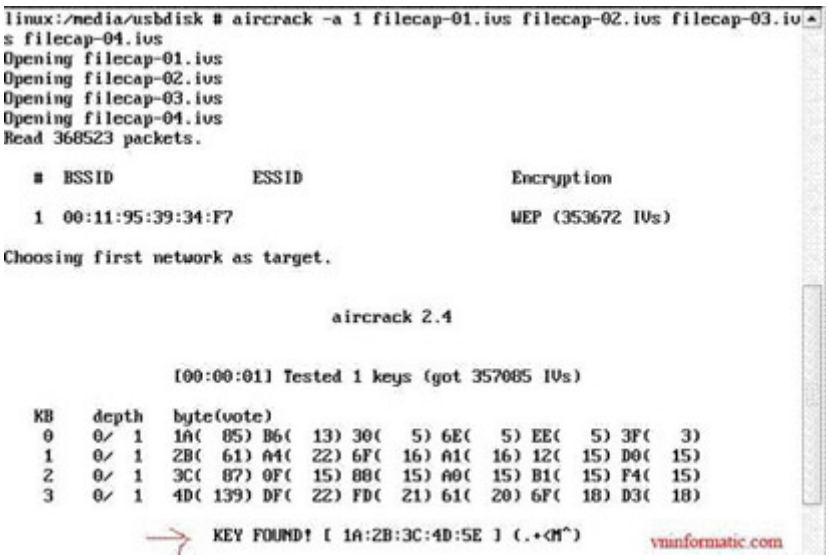
```
linux:/media/usbdisk # aireplay -0 10 -a 00:11:95:39:34:f7 eth1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
20:10:48  Sending DeAuth to broadcast -- BSSID: [00:11:95:39:34:F7]
20:10:50  Sending DeAuth to broadcast -- BSSID: [00:11:95:39:34:F7]
20:10:51  Sending DeAuth to broadcast -- BSSID: [00:11:95:39:34:F7]
20:10:52  Sending DeAuth to broadcast -- BSSID: [00:11:95:39:34:F7]
20:10:53  Sending DeAuth to broadcast -- BSSID: [00:11:95:39:34:F7]
20:10:54  Sending DeAuth to broadcast -- BSSID: [00:11:95:39:34:F7]
20:10:56  Sending DeAuth to broadcast -- BSSID: [00:11:95:39:34:F7]
20:10:57  Sending DeAuth to broadcast -- BSSID: [00:11:95:39:34:F7]
20:10:58  Sending DeAuth to broadcast -- BSSID: [00:11:95:39:34:F7]
20:10:59  Sending DeAuth to broadcast -- BSSID: [00:11:95:39:34:F7]
linux:/media/usbdisk # aireplay -3 -b 00:11:95:39:34:f7 -c 00:11:f5:ba:7f:2f eth
Please specify a source MAC (-h).
linux:/media/usbdisk # aireplay -3 -b 00:11:95:39:34:f7 -h 00:11:f5:ba:7f:2f eth
Saving ARP requests in replay_arp-0307-201324.cap
You must also start airodump to capture replies.
Read 991 packets (got 0 ARP requests), sent 0 packets...
linux:/media/usbdisk #
```

Hình 3: deauth client, giả dạng ARP & bơm dữ liệu để tăng lưu thông mạng

- airodump dùng để monitor và capture-bắt giữ packet mà AP đã phát ra, lưu lại thành file capture.(hình 4)

```
CH 11 ][ BAT  99% ][ GPS    0.000    0.000    0.000    0.00 ][ 2006-03-07 20:00

BSSID              PWR  Beacons    # Data  CH  MB  ENC   ESSID

00:11:95:39:34:F7   -1      171     28809  11  54. WEP   thunghiem

BSSID              STATION            PWR  Packets  Probes

00:11:95:39:34:F7  00:11:F5:BA:7F:2F   -1    29994
```

Hình 4: bắt các gói dữ liệu, dưới cột station là địa chỉ MAC của client- aircrack dùng để đọc file capture và dò tìm khóa.(hình 5)



Hình 5: dò tìm khóa bằng aircrack, chỉ có 1s là ra !!!

Tôi sẽ ko ghi cụ thể các dòng lệnh & tham số ra đây vì ta có thể dùng tham số help –h để biết cú pháp cụ thể. Nhưng đầu tiên ta phải đưa 2 card wifi của chúng ta qua chế độ "monitor mode", xem help của lệnh ifconfig & iwconfig để biết cách làm.
Vì mạng thử nghiệm của tôi có quá ít lưu thông mạng nên tôi sử dụng aireplay bơm các gói tin tới AP. Đại khái cách hoạt động của aireplay là gửi các gói tin deauthentication đến AP làm cho AP mất kết nối, "đá" client ra khỏi mạng (nhiều người thường dùng cách này để quấy phá mấy quán café wifi), client sẽ phải gởi các yêu cầu ARP request để kết nối lại với AP. Sau đó ta chạy aireplay với tham số khác cùng với đ/c MAC của client đã biết để giả dạng gửi các ARP request này liên tục tới AP, làm cho AP trả lời các yêu cầu này. Trong lúc chạy aireplay, ta chạy airodump để bắt giữ các gói tin trả lời từ AP có chứa IV (lưu ý aireplay & airodump phải chạy trên 2 card khác nhau, ko được cùng 1 card). Sau khi chạy airodump, theo dõi màn hình ta sẽ thấy số IV ở cột #Data sẽ tăng nhanh chóng cùng với sự tăng packet ở cột Beacons nếu ta đã chạy aireplay để bơm dữ liệu.
Tài liệu có nói rằng phải cần bắt khoảng dưới 500 ngàn IV để giải mã khóa 64bit & từ 500 ngàn IV trở lên để giải mã khóa 128bit, thực tế ở đây tôi chỉ cần hơn 300k IV là đã thành công. Khi thấy airodump đã capture được kha khá, ta cứ để nó chạy tiếp và mở 1 cửa sổ console khác và chạy aircrack để đọc các IV từ file mà airodump đã lưu để dò tìm khóa, tiến trình này rất nhanh thường ko mất quá 5s với máy P4 Mobile của tôi. Tổng thời gian để bơm dữ liệu & dò tìm khóa ko quá 1 tiếng, khá ấn tượng phải ko ?!.
Ngoài ra công cụ này còn có thể dò được cả khóa mã hóa bằng WPA, 1 phương thức an toàn và mạnh hơn WEP nhiều. Do thời gian có hạn nên tôi ko trình bày trong bài viết này.

Các phương pháp bảo mật cho mạng WiFi.

Phần này tôi sẽ trình bày các cách bảo mật cho mạng wifi, phân tích các mặt ưu nhược của từng cách, từ cách đơn giản đến phức tạp, tuy nhiên ai cũng có thể tự làm được hết. Chúng ta có thể áp dụng riêng lẻ từng cách hay kết hợp nhiều cách lại đều được.

- Tắt access point: khi xài xong or ko có nhu cầu sử dụng mạng nữa thì ta có thể tắt điện nó đi. Cách này nghe có vẻ cực đoan & buồn cười nhưng lại là cách hiệu quả 100%.
- Tắt chế độ SSID Broadcast: đa số các AP đều cho phép ta tắt chế độ này, nó làm cho tiện ích wireless

vậy nó cũng ko ngăn được 1 số ct scan mạnh khác như Kismet…
- Lọc địa chỉ MAC: AP đều có tính năng lọc MAC của các client kết nối vào, có 2 cách lọc là chỉ cho phép và chỉ cấm đ/c MAC nào đó. Cách này vẫn ko ngăn được những cao thủ tìm cách biết được đ/c MAC các client trong mạng của ta & dễ dàng giả dạng chúng thông qua thay đổi đ/c MAC của card mạng wifi.
- Mã hóa: WEP, WPA/WPA2 là những kiểu mã hóa thông dụng trong các AP, nếu AP của bạn chỉ hỗ trợ WEP thì hãy xài key dài nhất có thể (thường là 128bit), nếu có hỗ trợ WPA thì xài key tối thiểu 128bit or 256bit. Đa phần các AP có support WPA đều xài kiểu WPA-PSK (pre-shared key hoặc passphare key), WPA2 mã hóa thì an toàn hơn nữa nhưng phải cần thêm 1 server Radius nhằm mục đích xác thực. Chúng ta nên đặt khóa càng phức tạp càng tốt(bao gồm ký tự hoa thường, số & ký tự đặc biệt kết hợp lại), ko nên dùng những từ có nghĩa hay có trong từ điển, vì cracker vẫn dò được mã khóa WPA khi dùng tự điển dò theo kiểu brute force attack. Dùng cách này sẽ làm giảm tốc độ đường truyền giữa AP & client vì các thiết bị sẽ mất nhiều năng lực để giải/mã hóa kiểu phức tạp này.
- Dùng các kiểu xác thực người dùng, tường lửa, mã hóa dữ liệu trên đĩa & tập tin: các cách này sẽ ko ngăn được người khác dò ra khóa mã hóa wep/wpa. Nhưng nó ngăn họ ko xem cũng như can thiệp vô được những dữ liệu đang lưu thông & tài nguyên trên mạng của chúng ta.

Lời kết.

Qua bài viết này, chúng ta thấy 1 cách tương đối tổng quát về vấn đề bảo mật của mạng ko dây hiện nay. Chúng ta ko thể từ bỏ hoàn toàn được WEP vì hiện giờ rất nhiều thiết bị wifi hỗ trợ tốt cho nó. Nó cũng đã bộc lộ khá nhiều điểm yếu dễ bị khai thác. Nhưng cũng ko phải là thảm họa gì nếu chúng ta biết cách sử dụng kết hợp 1 vài cách phòng thủ phù hợp cho mạng wifi của chúng ta.
Với bài viết này tôi muốn giúp mọi người hiểu thêm về bảo mật mạng wifi. Tôi sẽ ko chịu trách nhiệm về bất cứ điều gì xảy ra nếu có ai đó sử dụng những thông tin trong bài này vào mục đích ko tốt khác, cũng như sẽ ko trả lời bất cứ câu hỏi nào liên quan tới dò tìm key.