Universidad Técnica

Federico Santa María.

Vulnerabilidad de redes de Wi-Fi

Integrantes:

Emilio Henríquez Bustos 2643035-6

Ricardo Valencia Luna 2930036-4

Gonzalo Sanchez Vargas 29300

Resumen.

La masificación de las redes wifi durante los últimos años y la gran cantidad de información que circula a través de ellas nos obliga a entender como funcionan los mecanismos que protegen dicha información de personas que pueden hacer mal uso de esta.

Existen distintos tipos de cifrado para proteger la información, cada uno de estos con distintas características y unos más seguros que otros. Es necesario tener un amplio conocimiento sobre las debilidades de cada sistema para así tomar una buena decisión a la hora de instalar una red wifi.

Los cifrados de información en redes wifi mas conocidos son WEP, WPA y WPA2. El primero fue WEP, un sistema basado en el algoritmo RC4 pero implementado pobremente. Luego nace WPA para hacer frente a los problemas de WEP y por ultimo se invento WPA2 y sus variantes.

Introducción.

En este trabajo se presenta información detallada sobre los sistemas de cifrado de información de redes wifi mas conocidos. Se presenta también información sobre las principales debilidades de cada sistema de forma teórica y también de forma practica mediante una demostración.

Encriptación WEP.

La encriptación WEP (Wireless Equivalent Privacy) es un sistema de cifrado de información para redes wifi. Fue incluido en el sistema IEEE 802.11.

Esta encriptación se basa en el algoritmo de cifrado RC4, el cual fue desechado inmediatamente por los criptógrafos por proveer muy poca seguridad.

Existe la encriptación WEP de 64 y 128 bits.

¿Cómo funciona la encriptación WEP?

Primero se genera un keystream con la clave WEP (generada por el usuario), un vector de inicialización y en algunos casos la dirección MAC del host que transmite la información. Luego de obtener el keystream se realiza la operación lógica xor entre este y la información que se desea transmitir. La diferencia entre WEP de 64 y 128 bits radica en el largo de la clave WEP. En el caso de WEP de 64 bits el keystream se compone de una clave wep de 16 bits mientras que en WEP de 128 bits la clave WEP es de 104 bits. Por otro lado el vector de inicialización tiene un largo de 24 bits en ambos casos. El keystream debe ser distinto para cada paquete que se desea enviar. Como la clave WEP es generada por el usuario y es fija se utiliza el vector de inicialización para generar keystreams distintos. Para que el host receptor pueda traducir el mensaje cifrado requiere saber el keystream. Para lograr esto se transmite el vector de inicialización sin cifrar en el mensaje cifrado.

Debilidades

La principal debilidad de la encriptación WEP es la mala implementación del vector de inicialización:

-Es enviado sin cifrar

-Es de tamaño fijo. Al ser un número de 24 bits tiene alrededor de 16,7 millones de valores posibles, es decir, después de un tiempo se utilizaran todos sus valores y se tendrán que repetir lo cual para los criptógrafos es una falencia enorme.

-Como el vector de inicialización tiene un rango de valores fijos, si la clave wep no es cambiada los keystreams también se comenzaran a repetir.

Para entender el problema de la reutilización de vectores de keystreams se puede mirar de un enfoque más matemático. Primero se capturan paquetes hasta que se encuentren dos que utilicen el mismo vector de inicialización (Recordar que este vector de inicialización se transmite como texto plano):

C1=información1(x)keystream(clave wep, VI) (primer mensaje cifrado)

C2=información2(x)keystream(clave wep, VI) (segundo mensaje cifrado)

Luego se realiza la operación xor entre ambos

C1(x)C2=informacion1(x)informacion2

Se observa que si los keystream son los mismos en ambos mensajes al realizar la operación xor entre ellos el keystream desaparece.

WPA

Creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado). Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros).

La Alianza Wi-Fi WPA previsto como una medida intermedia para ocupar el lugar de WEP mientras se preparaba 802.11i.

WPA fue diseñado para utilizar un servidor de autenticación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario (a través del protocolo 802.1i). Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión; sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida ([PSK] - Pre-Shared Key) para usuarios de casa o pequeña oficina. La información es cifrada utilizando el algoritmo RC4 (debido a que WPA no elimina el proceso de cifrado WEP, sólo lo fortalece), con una clave de 128 bits y un vector de inicialización de 48 bits.

Una de las mejoras sobre WEP, es la implementación del Protocolo de Integridad de Clave Temporal (TKIP - Temporal Key Integrity Protocol), que cambia claves dinámicamente a medida que el sistema es utilizado. Cuando esto se combina con un vector de inicialización (IV) mucho más grande, evita los ataques de recuperación]].

Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a Redes inalámbricas sea mucho más difícil. El algoritmo Michael fue el más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas más viejas; sin embargo es suceptible a ataques. Para limitar este riesgo, las Redes WPA se desconectan durante 60 segundos al detectar dos intentos de ataque durante 1 minuto.

WPA incluye protección contra ataques de "repetición" (replay attacks), ya que incluye un contador de tramas. WPA también incluye una comprobación de integridad del mensaje. Esto está diseñado para evitar que un atacante pueda capturar, modificar y / o reenvío de paquetes de datos.

WPA2

WPA2 ha sustituido a WPA, WPA2 requiere de pruebas y certificación por la Alianza Wi-Fi. La certificación se inició en septiembre de 2004. Del 13 de marzo de 2006, la certificación WPA2 es obligatoria para todos los nuevos dispositivos para llevar la marca Wi-Fi.

Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocólo WPA2 que utiliza el algoritmo de encripatción AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de Seguridad del gobierno de USA - FIPS140-2. "WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público. Los productos que son certificados para WPA2 le dan a los gerentes de TI la Seguridad que la tecnología cumple con estándares de interoperatividad" declaró Frank Hazlik Managing Director de la Wi-Fi Alliance. Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i

Está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de “migración”, no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i (El estándar 802.11i fue ratificado en Junio de 2004).

WPA2 es la segunda generación de WPA y está actualmente disponible en los AP más modernos del mercado. WPA2 no se creó para afrontar ninguna de las limitaciones de WPA, y es compatible con los productos anteriores que son compatibles con WPA. La principal diferencia entre WPA original y WPA2 es que la segunda necesita el estándar avanzado de cifrado (AES) para el cifrado de los datos, mientras que WPA original emplea TKIP.

El único añadido de WPA2 sobre WPA es la preautentificacióny la PMK (Pairwise Master Key) que ayuda a los dispositivos cuando hacen roaming y cambian de punto de acceso.

Conclusiones.

-Muchas personas entienden el hackeo de redes wifi como la obtención de las claves para obtener internet gratis pero es un tema mucho mas delicado. Si se logra hackear una red wifi esta en peligro toda la información que circula a través de ella: Información sobre cuentas bancarias, cuentas privadas, conversaciones, etc…

-Si bien la encriptación WEP es débil y fácilmente vulnerable no es recomendable tener una red wifi sin encriptación. Es recomendable siempre usar al menos WEP

-Con este tema logramos entender como funcionan los distintos tipos de cifrados para las seguridades WEP, WPA y WPA2. Como ha evolucionado la seguridad de las redes inalámbricas y como es posible vulnerar estas mismas.

WEP demostró ser la mas vulnerable, ya que solo se requiere captar los paquetes de la red que se desea atacar y luego por fuerza bruta ingresamos estos a Aircrak para forzar, mediante una serie de combinaciones de caracteres, la aparición de la contraseña de la red víctima.

Para el caso de WPA y WPA2 requiere captar el handshake de los usuarios que se conectan a la red, ya que son estos los que tienen la contraseña que se quiere descubrir. Una vez obtenido el handshake usamos diccionarios específicos para forzar el descubrimiento de la clave.

Ningún tipo de encriptación es infalible y por ello se recomienda cambiar nuestras contraseñas 1 vez al mes como mínimo con el fin de evitar el ingreso de intrusos en nuestra red.

Referencias.

-Wired Equivalent Privacy (WEP) | Wikipedia.org:

http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

-Understanding WEP weakness | dummies.com:

http://www.dummies.com/how-to/content/understanding-wep-weaknesses.html

-Vector de inicialización | Wikipedia.org:

http://es.wikipedia.org/wiki/Vector_de_inicializaci%C3%B3n

-WEP weakness and plaintext recovery | etutorials.org:

http://etutorials.org/Networking/Wireless+lan+security/Chapter+6.+Wireless+Vulnerabilities/WEP+Keystream+and+Plaintext+Recovery/

-Vulnerabilidades del cifrado WEP | wiki.elhacker.net:

http://wiki.elhacker.net/seguridad-wireless/introduccion/vulnerabilidades-del-cifrado-wep

Anexo.

Demostración de hackeo WEP en Windows

El proceso se divide en 2 partes:

1) **Captura de paquetes de AP seleccionado**, realizado con el ***Commview for WIFI v6.3***

2) **Descifrado de la clave WEP de los paquetes capturados**, realizado con ***Aircrack-ng GUI.exe***

Aircrack-ng GUI.exe utiliza ***interface grafica*** por lo que agiliza el trabajo, aunque dentro del paquete de Aircrack está el ***Aircrack-ng.exe*** que trabaja en modo TEXTO y que se usa en la consola de comandos DOS, el cual NO usaremos.

1) PROCESO DE CAPTURA DE PAQUETES UTILIZANDO COMMVIEW FOR WIFI

Arrancamos el programa y

- Pulsamos ***PLAY*** (debe aparecer en celeste si esta todo OK)
- En la ventana que aparece Pulsamos ***Iniciar Exploración*** (esto buscara los AP que recibimos)
- Comienzan a aparecer los AP separados en sus canales , ***Seleccionas un AP*** y en el recuadro superior a ***Iniciar Exploración,*** te **aparecerá toda la información de ese AP**, aquí es importante que observe ***si es un AP y si tiene clave WEP***, entonces puede seleccionarlo para capturar sus paquetes en los cuales buscar la clave WEP, digo esto porque también pueden aparecer AP, **SIN CLAVE WEP** o sea son de libre acceso por lo que será inútil capturar sus paquetes dado que no hay encriptación en ellos. Aquí puede probar, que al seleccionar otros AP va cambiando el ***CANAL,*** justo encima del botón ***Capturar*** o sea que ***la captura se hace por canales*** y ***en cada canal pueden haber muchos AP, es necesario saber esto porque luego al aplicar el Aircrack-ng GUI.exe*** vera que tendrá que elegir cual AP seleccionar de todos los que hay en ese canal, esto es muy beneficioso porque con la misma

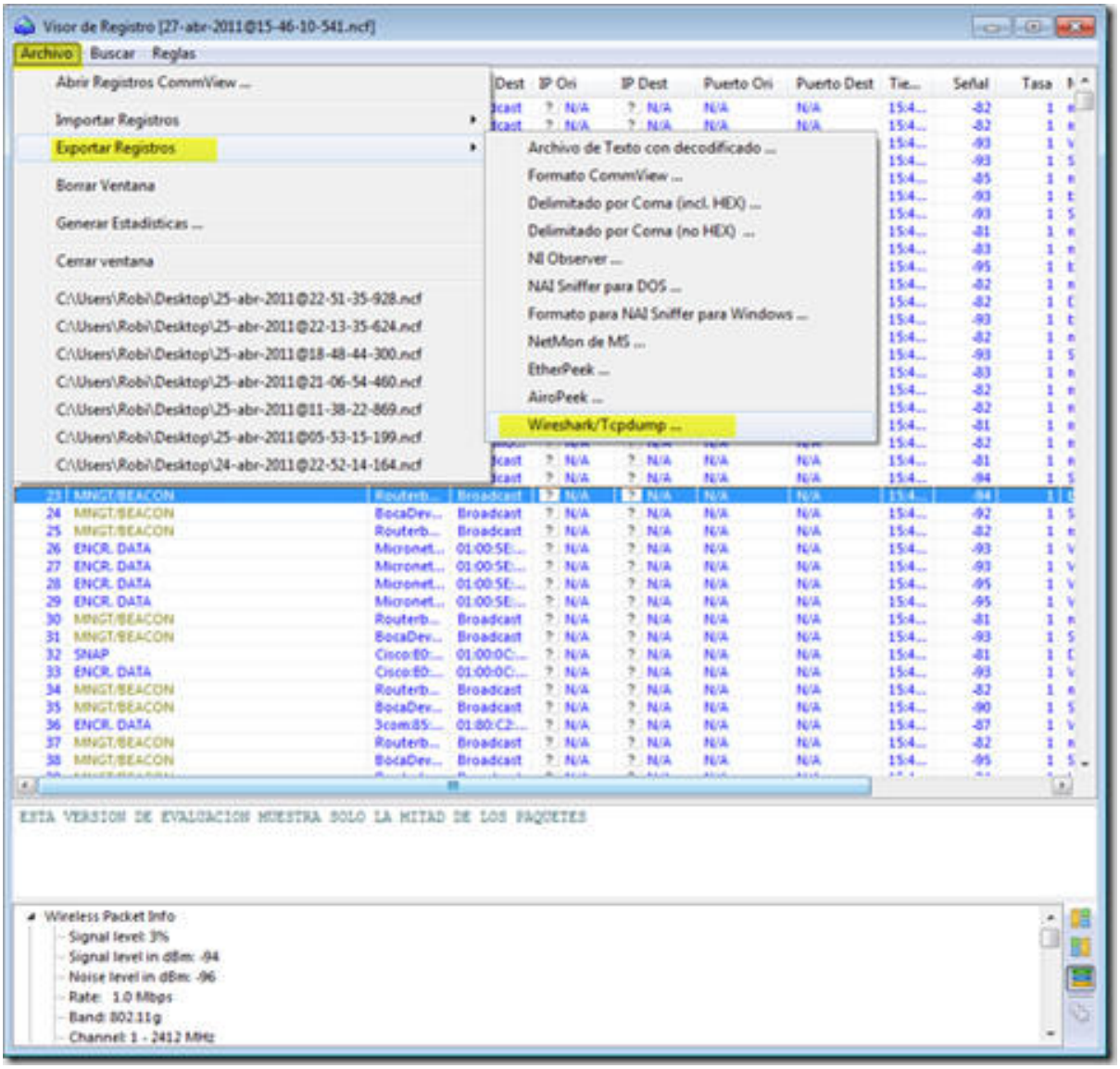
captura podemos buscar la clave WEP de distintos AP volviendo a ejecutar el ***Aircrack-ng GUI.exe*** y seleccionando otro AP.

- Ya con un AP seleccionado Pulsamos ***Capturar ,*** se cerrara la ventana y aparecerá la ventana principal del programa en la pestaña ***Nodos,*** el valor de captura en la columna ***Paquetes*** de debe incrementar cuanto mas rápido mejor y lo mismo para la pestaña ***Canales*** la columna ***Encriptación***. Si eligió el directorio de salida el ***desktop o escritorio,*** aparecerá al cabo de unos minutos y esto depende del trafico, el primer icono fichero de captura con un nombre asignado automáticamente por ***Commview for WIFI,*** este fichero de captura se ira incrementando en tamaño hasta llegar al tamaño máximo de configuración que le dimos ***(***ver en pestaña ***Registro*** o en ingles ***Logging, era*** de 90 MB) y comenzara otro nuevo y así por horas hasta que cortemos la captura. ***RECOMIENDO NO CORTAR LA CAPTURA HASTA ENCONTRAR LA CLAVE*** porque podemos estar ejecutando ***Aircrack-ng GUI.exe*** (cuando ya tengamos mas de 5 o 6 ficheros de captura) para ver si ya encontramos la clave mientras se esta capturando.

Atención: esto no se puede hacer si no convertimos el formato de salida de estos ficheros de

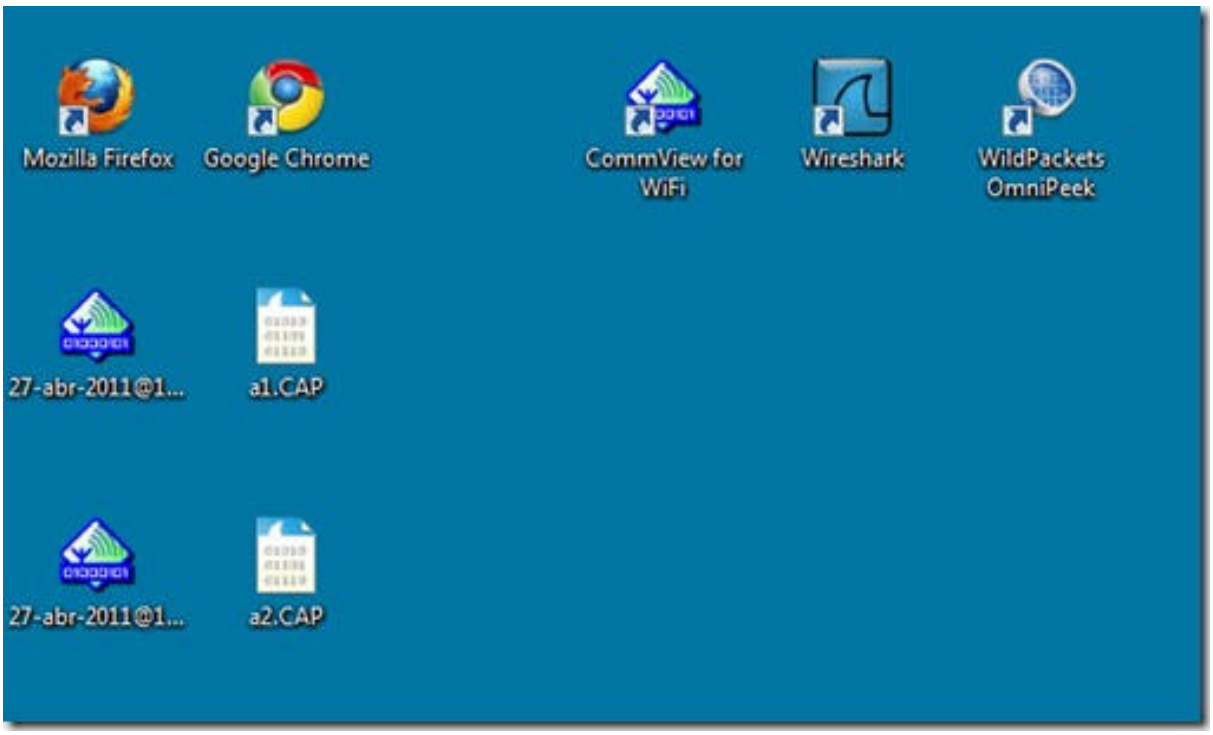
captura (.ncf) a un formato que lea ***Aircrack-ng GUI.exe.***

- ***CONVERTIR el formato del fichero de captura de Commview for WIFI .ncf al formato .cap que puede leer Aircrack-ng GUI.exe.*** Esto se hace simplemente haciendo doble click sobre el primer fichero de captura de Commview for WIFI .cnf, aparecerá una ventana del fichero, mostrando parte de su contenido, a nosotros solo nos interesa pulsar en ***Archivo\Exportar Registros\Wireshark /Tcdump*** aparecerá una ventana donde le damos un nombre (SIN EXTENCION .CAP) por ej. A1. Esto lo hacemos por cada fichero capturado por ***Commview for WIFI*** (.ncf) y ahora tendremos una secuencia de ficheros A1, A2, A3, …. todos con extensión .cap listos para ser tratados con ***Aircrack-ng GUI.exe.***



Así irá quedando el escritorio con los ficheros del Commview y los convertidos a **.cap**. Cuidado con confundir el icono del programa Commview con iconos de los ficheros de captura del Commview.

Ya estamos listos para usar ***Aircrack-ng GUI.exe*** y encontrar la clave WEP



2) PROCESO DE HACKEO DE LA CLAVE WEP CON Aircrack-ng GUI.exe

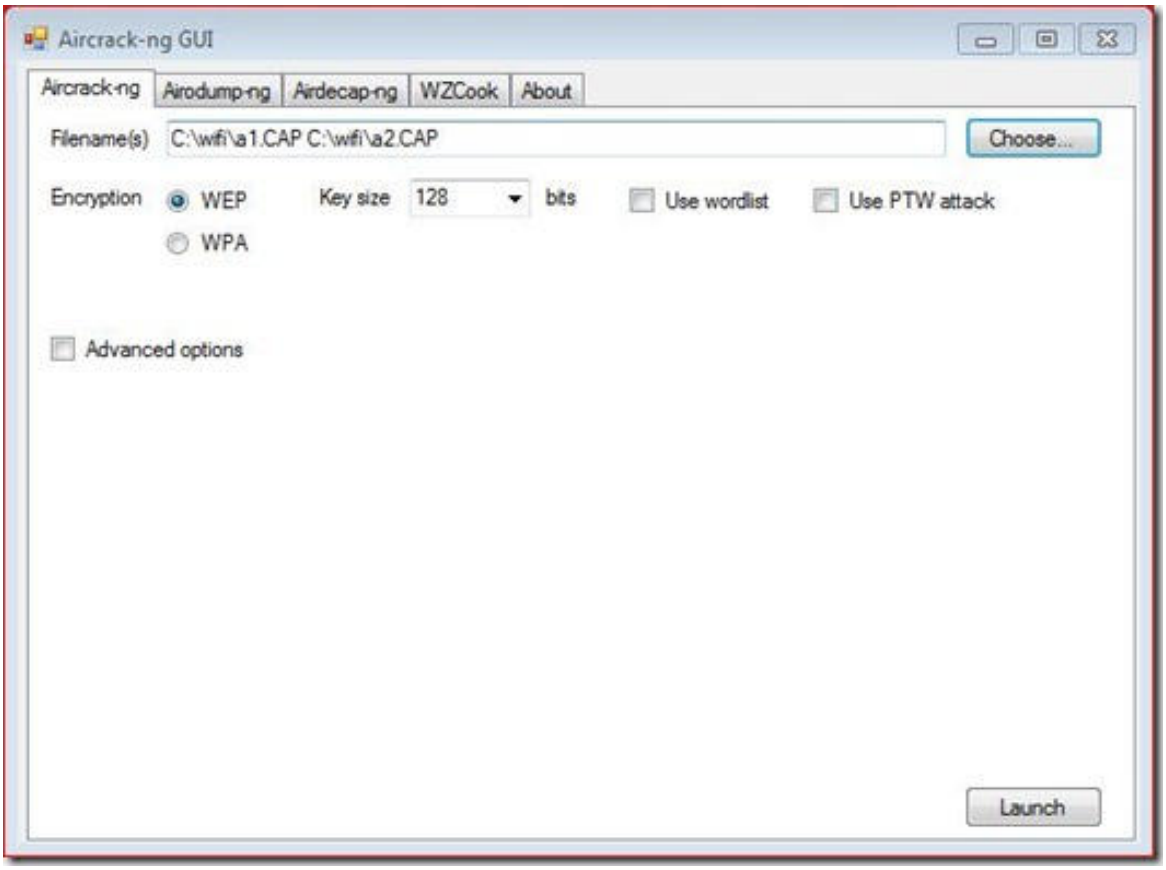
Este procedimiento se ejecuta directamente con ***Aircrack-ng GUI.exe*** donde lo tenga:

1. Creamos un directorio para nuestro proceso por ej. en **C:*WIFI***
2. Copiamos **TODO el contenido del directorio BIN del Aircrack descomprimido** y lo pegamos en **C:*WIFI***
3. Vamos al escritorio cortamos y copiamos todos los ficheros **.cap** y los pegamos en **C:*WIFI***

Con el Explorer de Windows vamos a **C:*WIFI*** y ejecutamos **Aircrack-ng GUI.exe** (con doble click),

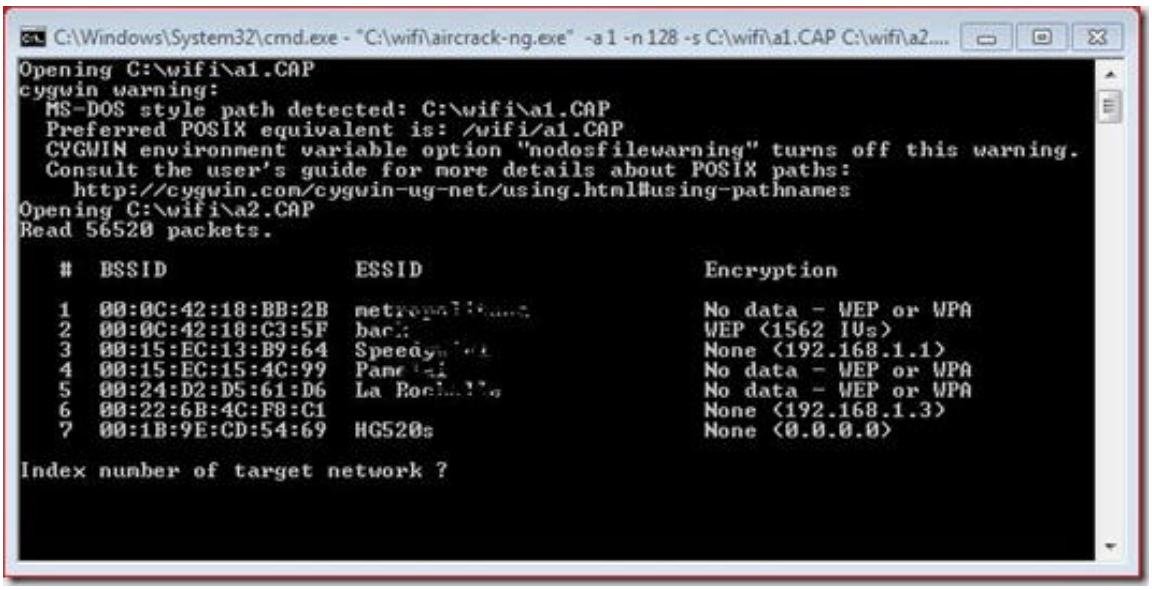
Pulsas en el botón ***Choose*** (elegir), seleccionamos **TODOS *los ficheros .cap del directorio C:\WIFI*** (***es un error seleccionar uno por uno para analizar)*** y no modifique nada (todo como sale en el grafico) solo mire la ***key size*** que esté en **128 bits**, que es la mas usada en este momento, hace unos años era la de 64 bits y en muchos tutoriales todavía aparece

esta configuración, por lo que es imposible que encuentre una clave de 128 bits si pone 64 bits, pero actualmente a nadie se le ocurre poner claves de 64bits, además si pone 128 bits puedes encontrar una de 64bits, pero no al revés.



Ahora verá el botón ***Launch*** (lanzar la ejecución) en el rincón derecho inferior de la ventana, **pulse en él**,

Este es el proceso de descifrar la clave WEP, es muy rápido al contrario de la captura y dura solo unos segundos, pero si el canal que elegimos para la captura tenia varios AP el programa nos mostrara una ventana donde nos pedirá que elijamos el AP, introduciendo 1,2,3,4 etc. según donde aparezca el AP que nosotros queremos Hackear la clave.



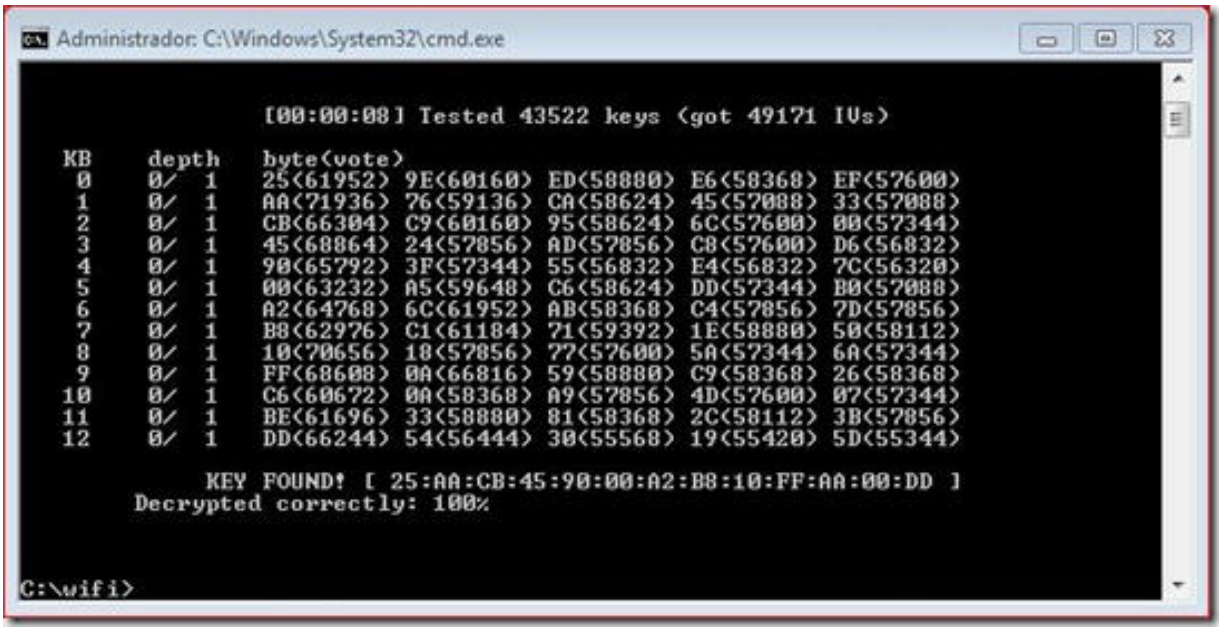
Aquí es importante resaltar que el AP debe mostrar que tiene IVs en la columna ***Encryption***, en este caso el numero 2 tiene 1562 IVs y es el único en el que se podrá buscar la clave WEP, así que ponemos 2 y pulsamos ENTER, recién ahora está el Aircrack trabajando descifrando la clave WEP.

<u>Si NO encuentra la clave WEP:</u>

1. Cerramos ***Aircrack-ng GUI.exe*** y ***dejamos que sigua capturando paquetes*** el ***Commview For WIFI***,
2. Cuando tengamos varios ficheros mas, los convertimos al formato .cap y los agregamos a los ficheros .cap que ya teníamos en el directorio c:\WIFI,
3. Ejecutamos ***Aircrack-ng GUI.exe*** borramos todos los nombres que aparecen en ***filenames*** a lado del botón ***Choose,*** porque sino se duplicaran los nombres de los que ya estaban antes, seleccionamos **TODOS** los ficheros .cap y luego click en ***Launch,*** si no encontró la clave volvemos a punto 1

<u>Si encuentra la clave WEP:</u>

Aparecerá una ventana como esta (la cual es un resultado de otras capturas donde si encontramos la clave de un AP con 50000 IVs) donde dirá KEY FOUND! ……



La clave esta formada por pares de 2 cifras hexadecimales separados por ":" varia la longitud de pares según la clave sea de 64, 128, 152, 256, 512 bits.

64 BITS ==> 10 CARACTERES O 5 PARES HEXADECIMALES

128 BITS ==> 26 CARACTERES O 13 PARES HEXADECIMALES

152 BITS ==> 32 CARACTERES O 16 PARES HEXADECIMALES

Para obtener la clave final debemos sacarle el doble punto y esa es la clave final a introducir cuando pulsemos para conectarnos a un punto de acceso. por ej..

KEY FOUND! [1B:56:EE:4B:CF:75:1A:70:D1:A0:C1:ED:12]

Quedará así:

1B56EE4BCF751A70D1A0C1ED12

Tiene 13 pares o sea es una clave de 128 bits

Ahora podemos parar y cerrar Commview for WIFI v6.3