Crackear Redes WIFI :)

Aquí está el tutorial que tanto habíais estado esperando, ya no hay impedimento a la hora de navegar en cualquier lugar... en unos pocos pasos sencillos estaréis navegando :), si bien es cierto que a las herramientas aquí citadas se les puede sacar algo más de jugo...

Este tutorial está probado con una tarjeta IntelWireless MiniPCI B/G de las que lleva cualquier portatil centrino y bajo ubuntu

Si no tienes esta tarjeta tendrás que descargarte un driver compatible para poder ponerla en modo monitor (si es que lo hay para tu tarjeta) puedes consultarlo aqui http://patches.aircrack-ng.org/

Lo más efectivo y fácil, es que acudamos a nuestro amigo *Gestor de paquetes Synaptic* (Sistema / Administración / ...) y busquemos aircrack, marcamos todo y lo aplicamos. Has de tener todos los

repositorios

activos (En synaptic, pincha en CONFIGURACION / REPOSITORIOS / marcamos todas, le damos a cerrar y... en la pantalla principal pinchamos en el botón RECARGAR, una vez termine ya lo tendremos)

Lo primero pondremos nuestra tarjeta wifi en modo monitor, sobra decir que mientras se encuentre en dicho estado NO PODREMOS NAVEGAR...

Bien, siempre siendo root (sudo su) o usando sudo (que esto le gusta mucho a la gente de hacer) ponemos nuestra tarjeta en modo monitor

airmon-ng start eth1

A continuación ejecutamos airodump este "escuchará" el tráfico wifi que encuentre a su alrededor, y lo almacenará en el archivo que le indiquemos

airodump-ng eth1 (o el eth que tengamos wlan0, ath0...)

Con esto visualizamos las redes y el trafico que tienen actualmente, vemos datos como BSSID que es la mac de la victima, DATA es el tráfico, es MUY IMPORTANTE fijarse en esre dato, pues a mayor DATA, mayor posibilidades de hackear, ya que este método se basa en la desencriptación basada en la captura de tráfico

Vemos también su CH (Channel = Canal) los MB de su red, el tipo de ENC (encriptación) y el nombre del SSID (ahí lo llama ESSID)

Bien, como he dicho antes, elegimos a la victima por la cantidad de Beacons, y miramos su CH (Channel), entonces en funcion de eso, interrumpimos el script (ctrl+c)y tecleamos (ojo con ver en que directorio estamos, lo más recomendable, crearse una carpeta en home y meterse, ejecutar desde ahí todos los comandos ej. /home/kuroneko/):

airodump-ng -c X (canal_el_q_elijamos) -w narchivo (nombre_del_archivo) eth1 (o wlan0 o

Crackear Redes WIFI :)

ath0...)

el nombre del archivo sirve para ir guardando ahí el trafico :)

Abrimos NUEVA VENTANA (Nos será útil tener las 3 abiertas)

#aireplay-ng -3 -b XX:XX:XX:XX:XX:XX:Mac_de_la_victima) -h 00:11:22:33:44:55 (mac_ficti cia) eth1

*NOTA: Al ejecuta el comando airodump debajo de la lista de routers WIFI (se diferencian por tener un ESSID nombre del punto de acceso) hay una lista de clientes, la primera dirección MAC es del router al que estan contectados y la segunda es la suya propia, PODEMOS usar su MAC de MAC ficticia)

Abrimos NUEVA VENTANA

en nuestro directorio se nos abrá creado un archivo .cap o .ivs, dicho archivo guarda el tráfico generado por el canal elejido al cual estamos "escuchando", aireplay por su parte intenta autenticarse en la red

entonces escribiremos...

aircrack-ng -x -0 archivo-XX.ivs(nuestro_archivo_ivs)

El programa empezará entonces a probar miles de combinaciones, hasta hallar aquella que le de acceso a la red

Para los que aman la consola, es preferible realizar todo este proceso desde allí, pues, el consumo de CPU es muy elevado. Se pueden mantener 3 sesiones simultáneas usando las teclas ctrl+alt+F1, F2, F3... así cuantas quieras ;)

Suerte ;)

KuroNeko

Veamos una imagen el proceso...

Crackear Redes WIFI :)

http://www.youtube.com/watch?v=W-vHH09t2Zw