# Proyecto “Rompiendo el código”

Barros, Maximiliano – Ceballos Escribano, Carlos Maximiliano
Durante, Albertina – García, Mauro Javier
Martínez Blanquier, Matías Ezequiel – Peralta, Flavio Marcelo
Vittar, Pablo Andrés – Wallace, Patricio Gabriel

*Laboratorio de Sistemas - Departamento de Ingeniería en Sistemas de Información*
*Universidad Tecnológica Nacional - Facultad Regional Córdoba*
*labsis@bbs.frc.utn.edu.ar*

## Abstract

*“Es una práctica, cuyo objetivo es demostrar la vulnerabilidad de una red inalámbrica protegida bajo encriptación WEP. Para ello se utiliza una suite de aplicaciones, provistas por una distribución especial del sistema operativo Linux, en formato Live CD, orientada al safe-networking. Consiste en el desarrollo de un procedimiento para implementar una red inalámbrica de transmisión de datos encriptados, los cuales son capturados y procesados para, mediante la aplicación de algoritmos de desencriptación, obtener la clave de seguridad de la red”.*

**Palabras Clave**

Seguridad wifi, redes inalámbricas, aircrack, airodump, aireplay, vulnerabilidad encriptación wep, paquetes IVs, safe-networking, desencriptar clave, rompiendo el código, GIROS LabSis, FRC – UTN, configuración interfaz de red, WifiWay.

## Introducción

El énfasis de la sociedad en la mejora de las comunicaciones, ha llevado a las ciencias de la informática, al desarrollo de tecnologías cada vez más sofisticadas, a velocidades cada vez superiores. Sin embargo, el avance de la tecnología no se acompaña por el avance en el conocimiento de los usuarios, en cuanto a los peligros que esto conlleva. Esto nos lleva a plantearnos el objetivo de demostrar en forma de práctica para los alumnos, las vulnerabilidades que pueden encontrarse en una red de comunicación inalámbrica, implementada sin los cuidados necesarios.

Si bien este trabajo es desarrollado con fines educativos, esta problemática puede tener graves consecuencias ya sea para una simple red doméstica, como para una red empresarial, y es de importancia que quienes hagan uso de esta tecnología, sepan tomar los recaudos necesarios. En base a esto desglosamos a la problemática en conceptos básicos vistos en la cátedra, para abarcar la misma y comprenderla, con el fin de buscar caminos que lleven a generar conciencia social.

## Elementos del trabajo y metodología

Para verificar y poder demostrar los riesgos que presenta una red inalámbrica bajo encriptación wep es necesario seguir el siguiente proceso:

a) Investigación: investigar sobre los conceptos básicos de redes, tales como el armado de la red, access point, paquetes, manejo de la suite aircrack-ng por consola bajo el sistema operativo Linux. Por otra parte la investigación recae en advertir los puntos vulnerables del sistema de encriptación wep, que nos permitirá llevar a cabo nuestro objetivo.

b) Desarrollo de la práctica: Herramientas a utilizar: Suite Aircrack-ng específicamente de WifiWay.

Pasos a realizar:

**1)** En primer lugar, se monta una red inalámbrica, se configura el router con el protocolo de seguridad WEP y se introduce una clave.

**2)** Se conectan un par de máquinas clientes al router, para ello deben contar con placas de red inalámbricas previamente instaladas ya sea por el puerto pci o externas usb. Estos equipos están dedicados a realizar solicitudes de eco ICMP, para ello se introduce en la línea de comandos,

ping IP_ROUTER -t -l 65000

El objetivo principal de estas dos máquinas es generar tráfico en la red así se logra capturar paquetes que contengan la clave para poder finalmente desencriptarla. Para ello se ejecuta el comando de solicitud de eco ICMP al router en aproximadamente diez ventanas de consola en ambos equipos.

**3)** Dos máquinas, equipadas con placas de red inalámbrica, ejecutan el cd WifiWay, el cual consiste en un Linux booteable que contiene una serie de herramientas y utilidades relacionadas con las redes inalámbricas. De todas ellas, en estas máquinas se utiliza Aireplay-ng.

Para la utilización de este programa es necesario verificar el tipo de placa de red (Broadcom no soporta esta herramienta y la mayoría de las placas solo pueden realizar una tarea a la vez, es decir, inyectar o capturar, salvo placas atheros en las cuales si se puede realizar más de una actividad a la vez). Una vez inicializado el Wifiway se ingresa con el entorno grafico deseado acorde a la computadora en la que se esta trabajando, y lo demás se trabaja por consola.
En primer lugar, ejecutamos en línea de comandos (en ambos equipos),

(a) ifconfig wlan0 down

(b) iwconfig wlan0 mode monitor channel 1
(c) ifconfig wlan0 up

En (a) se desactiva la interfaz wlan0, la cual es la que se va a utilizar para inyectar paquetes. Luego (b) se configura la interfaz wlan0 en modo monitor y se la coloca en el canal 1 para inyectar los respectivos paquetes. Concluyendo con la configuración de la interfaz, en (c) es activada para comenzar a funcionar.

*<u>Aclaración:</u> En esta experiencia se utiliza la interfaz wlan0, puede utilizarse otra, para ello ejecutar en consola ipconfig y allí aparecen los nombres de las interfaces de red. También es posible utilizar otro canal, para ello ver en la configuración del router.*

**4)** Una vez configurada la interfaz wlan0 en ambas máquinas, se introduce en la línea de comandos,

aireplay-ng -3 -b MAC_ACCESPOINT -h MAC_ORIGEN -x 1024 wlan0

El objetivo de estas máquinas es inyectar paquetes al punto de acceso (router). Aireplay-ng es el programa que permite realizar esta tarea, la opción -3 indica que el ataque a realizar es la inyección de paquetes, la opción -b indica que a continuación se va a introducir la dirección IP del punto de acceso al cual se le va a inyectar paquetes, la opción -h indica que a continuación se introduce la MAC de la placa de red de la máquina que inyecta, -x establece la cantidad de paquetes a inyectar por segundo, en este caso 1024 paquetes por segundo, y wlan0 es la interfaz que se utiliza, previamente configurada en modo monitor y por el canal adecuado.

**5)** En otra máquina, se realiza la captura de paquetes que circulan por la red. Los paquetes que son útiles para obtener la clave son los IVs. Para lograr capturarlos se utiliza la herramienta Airodump-ng del cd booteable WifiWay.

Se introduce en consola,

airodump-ng -w RUTA_AL_ARCHIVO_DE_CAPTURA --bssid MAC wlan0

Al utilizar airodump-ng la línea de comandos a utilizar que nos permitirán escuchar el envío de paquetes y capturar aquellos de tipo IVs que son los que poseen la clave a obtener. Mediante la opción –w le indicamos la ruta en la cual se guardaran los paquetes, es importante que se cambie la ruta si se desea guardar esta información para ser reutilizada porque la ruta en la que se guarda por defecto es el directorio de conexión y al estar booteando desde el cd los archivos se guardaran de forma virtual y se perderán al apagar la computadora. La opción –bssid es un filtro por el cual nosotros solo almacenaremos de la MAC que le ingresemos los paquetes IVs y por ultimo wlan0 es la interfaz sobre la cual se está trabajando.

**6)** En la misma máquina en la que se realiza la captura de paquetes IVS, se realiza el desencriptado de los paquetes para conseguir la clave WEP de la red inalámbrica, para lo cual se ejecuta en consola la siguiente línea de comandos,

aricrack-ng -a 1 -n 64 RUTA_AL_ARCHIVO_DE_CAPTURA.cap

Una vez alcanzado el mínimo de paquetes necesarios de acuerdo al tamaño de la clave (en nuestro caso la clave era de 64 bits de manera que necesitamos) se ejecuta el comando aircrack-ng. La opción –a nos permite ingresar el ataque en este caso 1que nos permite descifrar la clave entre los paquetes obtenidos. La opción –n nos permite que se pruebe únicamente con claves de 64 bits en vez de 128 bits que es la que se verifica por defecto.

## Resultados

Con este proyecto pretendemos mostrar a través de una práctica la inseguridad que presenta la encriptación wep implementada en una red inalámbrica.

## Discusión

La hipótesis a verificar abarca la vulnerabilidad de las redes inalámbricas de encriptación wep ¿Son realmente seguras una red inalámbrica con encriptación wep? ¿Es demostrable mediante una práctica esta inquietud para alguna cátedra?

## Conclusión

Las Redes inalámbricas llegaron para no irse nunca, pero como todo lo que sucede en el ámbito cibernético, primero llega la tecnología y muy atrás la seguridad de la misma. Debido a esto es fundamental hacer una demostración de este tipo para certificar que se debe tener sumo cuidado con respecto a qué tipo de encriptación utilizar para dar seguridad a la red.

Teniendo las herramientas necesarias acompañado de los conceptos basados en redes de información es visible que este tipo de encriptación es fácilmente vulnerable. Cumpliendo así nuestro objetivo concientizar, afianzar conocimientos dictados en la cátedra con una práctica que capta la atención del alumno debido a que representa una innovación tecnológica en desarrollo bastante usada en la actualidad, y mostrar que este tipo de encriptación no es la recomendable al momento de realizar un trabajo que necesite seriedad y privacidad.

## Agradecimientos

Agradecemos a nuestras familias por permitirnos desarrollar nuestros estudios brindándonos su constante apoyo.

Al Laboratorio de Sistemas de la UTN - FRC por permitir el desarrollo de esta práctica y a todos sus integrantes por la buena atención y disposición.

Al Ing. Fabián Gibellini, Ing. Marcelo Marciszack por darnos la oportunidad de ser parte del laboratorio y crecer como futuros profesionales.

Al Ing. Mario Groppo por facilitarnos el acceso y utilización de los recursos Laboratorio de Redes.

## Referencias

[1] Cecilia B. Sánchez, José L. Galoppo, José R. Pastor, Nelly B. Ríos, *Redes de Información*, quinta edición, Universitas Editorial Científica Universitaria, Córdoba, Argentina, 2006.

[2] Behrouz A. Forouzan, *Transmición de datos y redes de comunicaciones*, cuarta edición, Editorial Mc Graw – Hill, Madrid 2007.

[3] Guillaume Lehembre, "Seguridad Wi-Fi – WEP, WPA y WPA2", www.hakin9.org , 2006, pp. 1-15.

## Datos de Contacto

Barros, Maximiliano
el_maxi_@hotmail.com;
Ceballos Escribano, Maximiliano Carlos
escribano_maxi13@hotmail.com;
Durante, Albertina
alberakd@gmail.com;
García, Mauro Javier
mau_pro07@hotmail.com;
Martínez Blanquier, Matías Ezequiel
matias1690@gmail.com;
Peralta, Flavio Marcelo
flaperalta8@gmail.com;
Vittar, Pablo
vittar_73@hotmail.com;
Wallace, Patricio Gabriel
mcwallace830@gmail.com;
Ing. Fabián Alejandro Gibellini
Laboratorio de Sistemas
Departamento de Sistemas
Universidad Tecnológica Nacional
Facultad Córdoba
Cruz Roja y Ualdislao Frías S/N-Ciudad Universitaria
Córdoba – Argentina

fgibellini@bbs.frc.utn.edu.ar
tel: 4686385 – int 127-3