Revista Nexos Científicos
Julio –Diciembre 2018 pp. 21-27
Volumen 2, Número 2
Fecha de recepción: octubre 2018
ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: noviembre 2018

Vulnerar la seguridad WPA y WPA2 con AIRCRAK

Naranjo Kerly [1]; Salazar Martha[2]

[1] Universidad Tecnológica Israel-Departamento de Ciencias de la Ingeniería –Carrera de Sistemas, Quito, Ecuador, k.erly5@hotmail.com
[2] Universidad Tecnológica Israel-Departamento de Ciencias de la Ingeniería –Carrera de Sistemas, Quito, Ecuador, msalarzar@uisrael.edu.ec

Resumen: El presente trabajo es realizado para analizar las vulnerabilidades a las que están expuestas las redes inalámbricas de alta velocidad conocidas comúnmente como Redes WI-FI, así como los métodos que brindan cierto grado de seguridad a estas redes. Los diferentes métodos de seguridad que pueden ser aplicados a redes inalámbricas se tratan en el segundo capítulo; estos medios son: autenticación de usuario, encriptación, lista de control de acceso o filtrado de direcciones MAC, WEP y WPA. A continuación, se describen las vulnerabilidades de las redes WI-FI, se definen las características de los diferentes tipos de ataques a los que las redes están sujetos, además se enumeran los problemas concretos que pueden volver insegura una red inalámbrica.

Palabras clave: Redes, WI-FI, Ataques, Vulnerabilidades.

Violate WPA and WPA2 security with AIRCRACK

Abstract: This work is carried out to analyze the vulnerabilities to which high-speed wireless networks commonly known as WI-FI Networks are exposed, as well as the methods that provide a certain degree of security to these networks. The different security methods that can be applied to wireless networks are covered in the second chapter; These means are: user authentication, encryption, access control list or MAC address filtering, WEP and WPA. Next, the vulnerabilities of WI-FI networks are described, the characteristics of the different types of attacks to which the networks are subject are defined, and the specific problems that can make a wireless network insecure are listed.

Keywords: Networks, WI-FI, Attacks, Vulnerabilities

1. INTRODUCCIÓN

La mayoría de los problemas de seguridad son causados intencionalmente por gente maliciosa que intenta ganar algo o hacer daño a alguien, los cuales pueden provenir tanto de gente externa o de miembros internos de la empresa. Najera-Gutierrez, G., & Ansari, J. A. (2018).
La seguridad, por tanto, implica ser más competente que adversarios a menudo inteligentes y dedicados. Ramachandran, V., & Buchanan, C. (2015)

Las redes inalámbricas de área local (WLAN) tienen un papel cada vez mas importante en las comunicaciones del mundo de hoy. Acosta-López, A., Melo-Monroy, E. Y., & Linares-Murcia, P. A. (2018)
Debido a su facilidad de instalación y conexión, se han convertido en una excelente alternativa para ofrecer conectividad en lugares donde resulta inconveniente o imposible brindar servicio con una red alambrada, pero al mismo tiempo han generado una serie de amenazas que atentan contra la seguridad de las redes.

1. Estudiante de ingeniería en Sistemas, k.erly5@hotmail.com
2. Master Universitario en Ingeniería Matemática y Computación, msalarzar@uisrael.edu.ec

ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: noviembre 2018

Aspectos generales de las WLAN

El acceso sin necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es tan fácil, que cualquier equipo que se encuentre a 100 metros o menos de un punto de acceso, podría ingresar a la red inalámbrica. Roy, D., Moazzami, K., & Singh, R. (2007)
Durante el transcurrir del tiempo y con el fin de mejorar la seguridad, velocidad y cubrimiento, aparecen diferentes estando res para las WLAN, desarrollados por la IEEE, como son 802.11 a, 802 .11 b, 802.11 e, 802.1 11, 802.11 g, 802 .1 1 h Y 802 .1 1 i

Problemas encontrados

El rango de las redes WLAN con frecuencia es de algunos cientos de metros, pero intrusos pueden aprovechar esta situación para hacer de los suyos.

Por ejemplo, el 7 de septiembre del 2001, el IEEE declaró que WEP era inseguro, por lo cual en los últimos años se generó WPA (WI-FI Protected Access) y WPA2 (WI-FI Protected Access 2). WPA2 está basado en el nuevo estándar 802.11 i. WPA, por ser una versión previa, no incluye todas las características del IEEE 802.11 i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11 i.

Kali Linux

Kali Linux es una distribución de Linux basada en Debian destinada a pruebas avanzadas de penetración y auditoría de seguridad, contiene varios cientos de herramientas orientadas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa. Kali Linux está desarrollado, financiado y mantenido por Offensive Security, una empresa líder en capacitación en seguridad de la información. Meyer, U., & Wetzel, S. (2004)

Kali Linux fue lanzado el 13 de marzo de 2013 como una reconstrucción completa de BackTrack Linux, cumpliendo completamente con los estándares de desarrollo de Debian. Diehl, M. WEP Vulnerability Testing.

Herramientas Kali Linux

Aircrack-ng: Aircrack-ng es un programa de descifrado de claves 802.11 WEP y WPA-PSK que puede recuperar claves una vez que se han capturado suficientes paquetes de datos. Implementa el ataque estándar de FMS junto con algunas optimizaciones como los ataques KoreK, así como el nuevo ataque de PTW, lo que hace que el ataque sea mucho más rápido en comparación con otras herramientas de craqueo WEP. Lyon, G. F. (2009)

Aireplay-ng: Aireplay-ng está incluido en el paquete aircrack-ng y se usa para inyectar cuadros inalámbricos, su función principal es generar tráfico para su posterior uso en aircrack-ng para descifrar claves WEP y WPA-PSK. Aireplay-ng tiene muchos ataques que pueden desautenticar a los clientes inalámbricos con el fin de capturar los datos de protocolo de enlace WPA, autenticaciones falsas, repetición de paquetes interactivos, inyección de solicitud ARP hecha a mano y reinyección de solicitudes ARP.

2. METODOLOGÍA

Detección de vulnerabilidades

En conjunto con lo expuesto en el presente documento, se procede se realizar un ataque WPA / WPA 2 a las redes inalámbricas.

En primer lugar se procede a la preparación del entorno. Los ataques mencionados se los realizará en el sistema operativo Kali Linux. Para su instalación, seguir los siguientes pasos.

Descargar la imagen ISO de Kali Linux de la página oficial https://www.kali.org/downloads/.

Revista Nexos Científicos
Julio –Diciembre 2018 pp. 21-27
Volumen 2, Número 2
Fecha de recepción: octubre 2018
ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: noviembre 2018

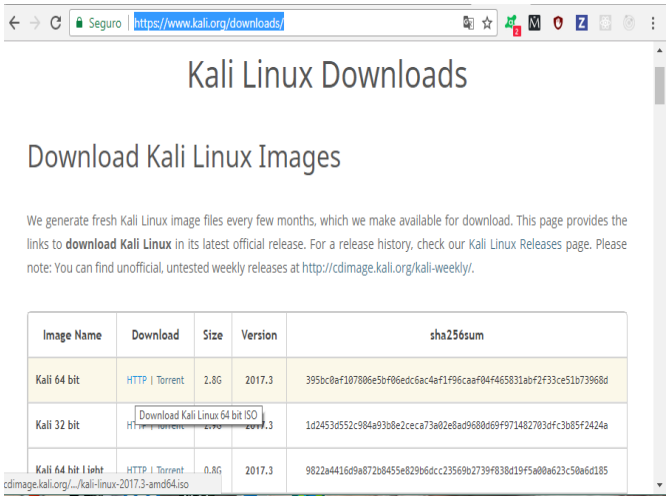


Ilustración 1 Página de descarga Kali Linux
Fuente: Autores Naranjo Kerly

Cargar el sistema operativo en un dispositivo USB. Se recomienda usar Rufus o Lili Linux para el booteo del USB.

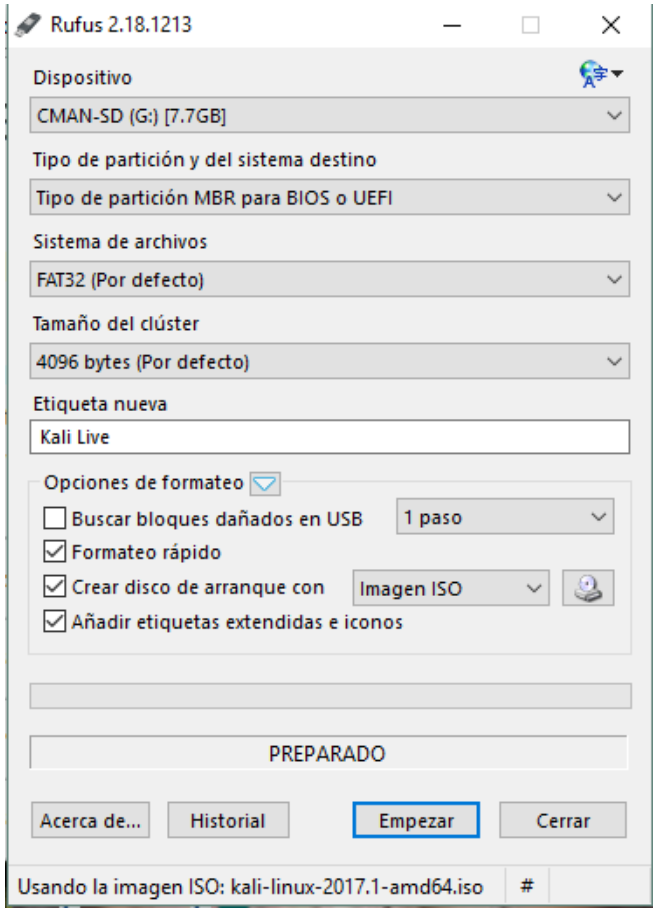


Ilustración 2 Bootear el sistema operativo
Fuente: Autores Naranjo Kerly

Entrar la BIOS de la computadora donde se pretende instalar Kali Linux y seleccionar el arranque desde el dispositivo USB. García Dueñas, M. (2010)

Ilustración 3 BIOS del ordenador
Fuente: Autores Naranjo Kerly

Una vez arrancado desde el dispositivo USB, en la primera interfaz que muestra Kali Linux seleccionar el modo Live.

Ilustración 4 Interfaz inicial de Kali Linux
Fuente: Autores Naranjo Kerly

3. RESULTADOS Y DISCUSIÓN

Descifrar claves WPA y WPA2

Este proceso consiste en enviar un ataque al router víctima y desconectar un dispositivo conectado a la red de la víctima. Cuando el dispositivo vuelva a conectarse, interceptar el ingreso de la contraseña y generar el WPA Handshake, que es la contraseña encriptada de la víctima. Introducir un diccionario personalizado generado con Kali Linux y comparar palabra por palabra con la contraseña encriptada obtenida. Muñoz Villa, D. G. (2006)

Revista Nexos Científicos
Julio –Diciembre 2018 pp. 21-27
Volumen 2, Número 2
Fecha de recepción: octubre 2018
ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: noviembre 2018

Una vez que se encuentra la contraseña se puede utilizar la red a la que se realizó el ataque.

Procedimiento

1. Crear un diccionario personalizado con Kali Linux para una víctima predeterminada en base a información (nombre, fecha de nacimiento, equipo de futbol, número de cédula) que se obtiene de la misma. Lashkari, A. H., Danesh, M. M. S., & Samadi, B. (2009)

   Iniciar una terminal en Kali Linux y ejecutar el siguiente comando para crear el diccionario, el cual contendrá 100000000 líneas o combinaciones entre números del 0 al 9.

```
# crunch min max (simbolos) –o
diccionario.lst
```

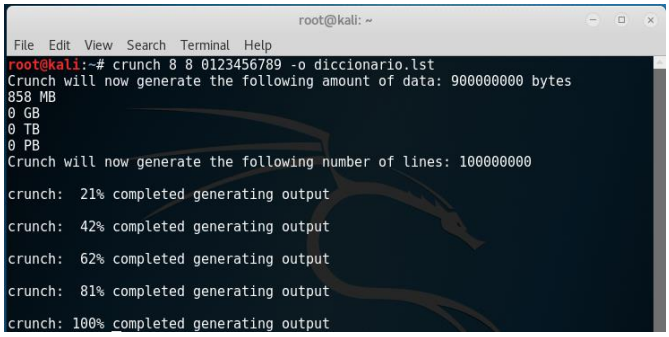


Ilustración 5 Crear un diccionario
Fuente: Autores Naranjo Kerly

2. En una nueva terminal ejecutar el comando **airmon-ng** para listar las interfaces de red inalámbrica instaladas en el ordenador.

```
# airmon-ng
```

Ilustración 6 Listar las interfaces de red
Fuente: Autores Naranjo Kerly

3. Configurar la placa de red en modo monitor para poder realizar el proceso de hackeo de contraseña.

```
# ifconfig wlan0 down
# iwconfig wlan0 mode monitor
# ifconfig wlan0 up
# airmon-ng start wlan0
```

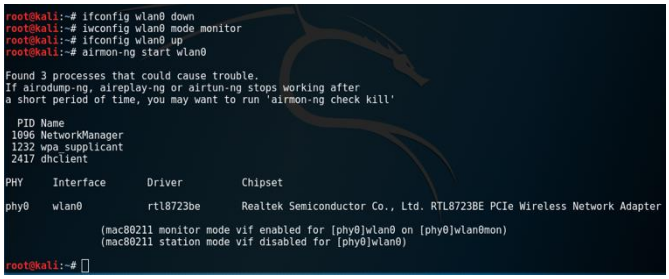


Ilustración 7 Configurar la placa en modo monitor
Fuente: Autores Naranjo Kerly

4. Mostrar la tabla del estado de los dispositivos WLan detectados, con el comando:

```
# airodump-ng mon0
```

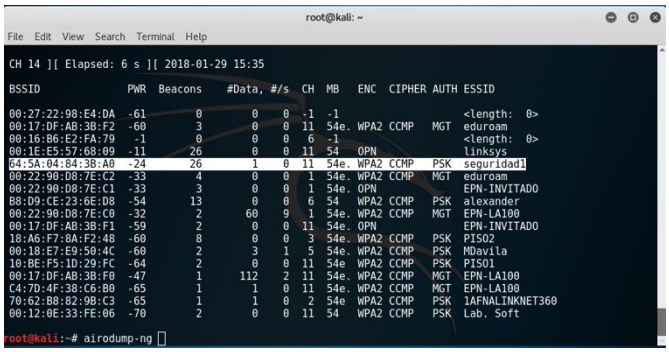
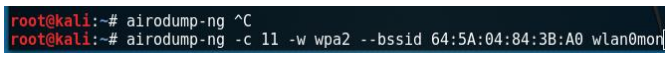


Ilustración 8 Tabla de dispositivos WLAN
Fuente: Autores Naranjo Kerly

La sección resaltada en color blanco muestra la victima escogida para la demostración del presente ataque.

5. Identificar el ESSID de la víctima y con el siguiente comando filtrar únicamente la red de interés y las estaciones conectadas a la misma.

```
# airodump-ng –c canal –w
nombre_archivo –bssid MACVictima
interfaz
```



Revista Nexos Científicos
Julio –Diciembre 2018 pp. 21-27
Volumen 2, Número 2
Fecha de recepción: octubre 2018

ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: noviembre 2018

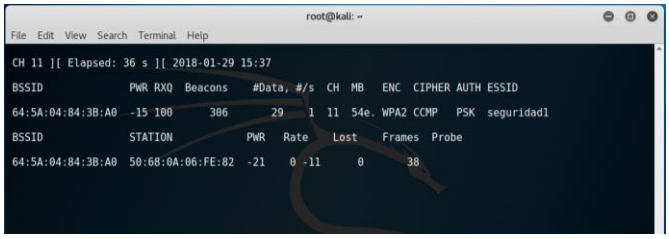


Ilustración 9 Detalle de la red victima
Fuente: Autores Naranjo Kerly

6. Finalmente, el comando **aircrack-ng** permite recorrer el diccionario hasta encontrar la clave de la víctima.

```
# aircrack-ng –w diccionario – b la MAC_víctima
```

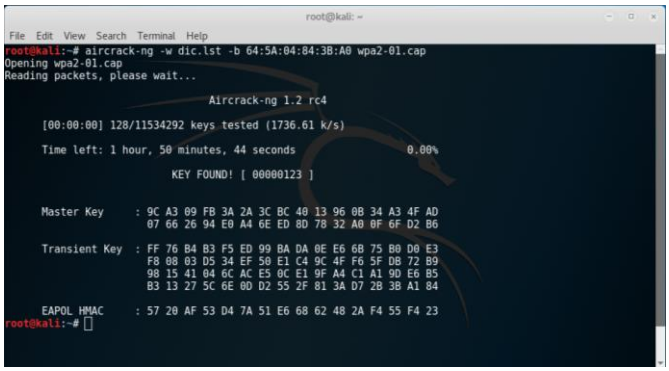


Ilustración 20 Clave de la victima encontrada
Fuente: Autores Naranjo Kerly

Mapeo de puertos

El mapeo de puertos consiste en escanear los puertos y estados de cada de uno de ellos para una red WLAN específica. Para realizar este proceso se utiliza la herramienta NMAP de Kali Linux, la cual sirve para hacer auditorias de seguridad de los puertos, siendo lo principal la tabla de estados, estos pueden ser:

- **Closed:** Cerrado
- **Open:** Abierto
- **Filtred:** Filtrado
- **Unfiltred:** No Filtrado

Procedimiento

1. Detectar que la herramienta NMAP se encuentre instalada en el ordenador con Kali Linux desde donde se pretende realizar el mapeo.

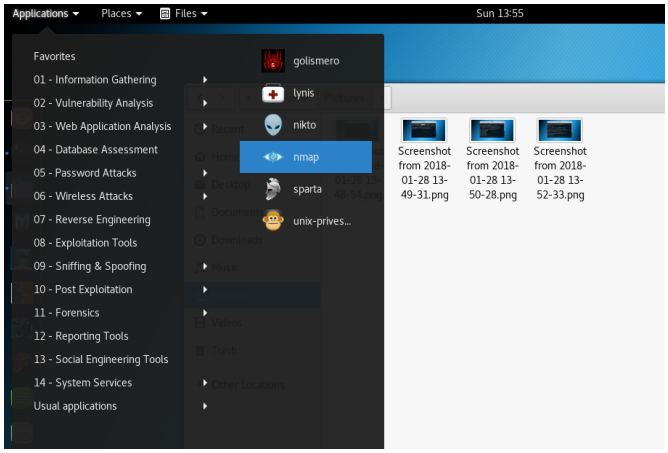


Ilustración 31 Herramienta NMAP en Kali Linux
Fuente: Autores Naranjo Kerly

2. Identificar la dirección IP a la que se quiere escanear los puertos.

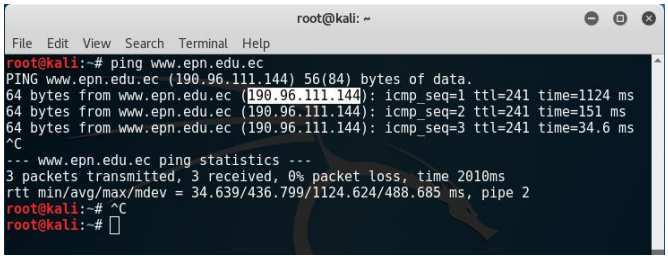


Ilustración 42 Direcciones IP víctimas
Fuente: Autores Naranjo Kerly

3. En una terminal de Kali Linux ejecutar el comando nmap -p [puertos] [host] para listar la tabla de puertos y sus estados.

```
# nmap -p [puertos] [host]
```

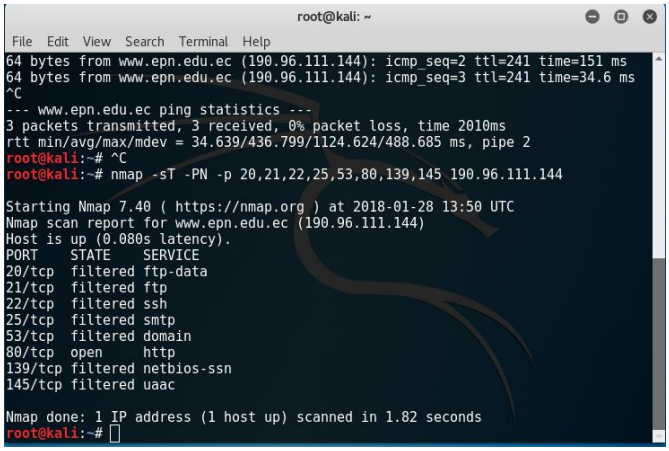


Ilustración 53 Tabla de puertos y estados
Fuente: Autores Naranjo Kerly

ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: noviembre 2018

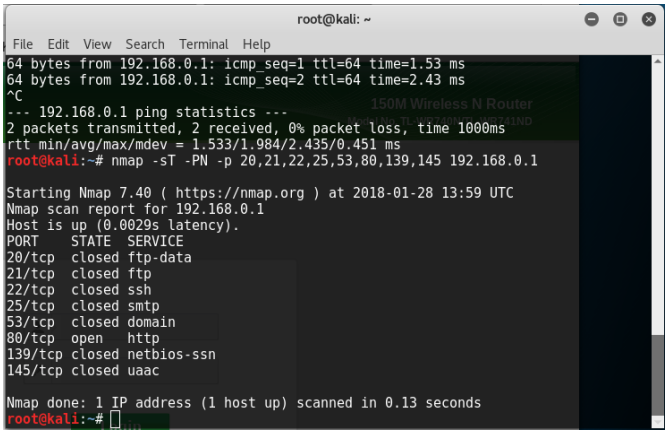


Ilustración 64 Tabla de puertos y estados
Fuente: Autores Naranjo Kerly

4. CONCLUSIONES

- Las redes inalámbricas presentan muchas vulnerabilidades.

- Las principales ventajas de las redes WI-FI son la movilidad que ofrecen a los usuarios, ya que no los ata a un punto en específico, y también la facilidad de acceso a redes abiertas e inclusive redes semiseguras o seguras utilizando los permisos necesarios.

- Los software o sistemas operativos como Kali Linux, son desarrollados para atacar las vulnerabilidades de las redes WLAN, con el objetivo de fortalecer la red luego de identificar la debilidad.

- Para mejorar la seguridad de las redes WLAN, existen las herramientas de modos de autentificación del sistema abierto y de llave compartida, el Identificador del Juego de Servicios (Service Set Identifier-SSID), WEP, WPA, WPA2, filtrado de direcciones MAC, VPN s y protección mediante 802.1x.

- La tecnología inalámbrica es el sueño de todo espía: datos gratuitos sin tener que hacer nada.

- Un intruso puede colocar un equipo inalámbrico para que grabe todo lo que oiga, evadiendo de esta manera los firewal ls de la compañía. Por ello es importante tener muy en cuenta las protecciones con los equipos inalámbricos (portátiles, acces point, etc) que se encuentren dentro de la compañía.

- Existen prácticas bien conocidas para localizar redes inalámbricas: el warchalking y el wardriving.

- WLAN es una tecnología podríamos decir que "nueva", pero en este corto periodo de vida la evolución constante que ha tenido, y que sigue teniendo, hará que el número de usuarios domésticos y empresarial siga aumentando.

- Los tipos de ataques que puede sufrir una red WI-FI pueden ser pasivos o activos; en el caso MITM el intruso solamente husmea la red para obtener información, en el segundo caso la situación es más delicado ya que el intruso puede alterar la información o inclusive puede impedir que un usuario autorizado haga uso de la red.

REFERENCIAS

Najera-Gutierrez, G., & Ansari, J. A. (2018). *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux*. Packt Publishing Ltd.

Ramachandran, V., & Buchanan, C. (2015). Kali Linux Wireless Penetration Testing: Beginner's Guide. Packt Publishing Ltd.

Acosta-López, A., Melo-Monroy, E. Y., & Linares-Murcia, P. A. (2018). Evaluación da seguridad en protocolo de rad inalambrico WPA2-PSK usando las herramientas Linset y Aircrack-ng. Revista Facultad de Ingenieria, 27(47), 71-79.

Diehl, M. WEP Vulnerability Testing.

Roy, D., Moazzami, K., & Singh, R. (2007). ARP Spoofing and Man in the Middle attack using Ettercap. School of Computer Science, University of Windsor, Canada.

Meyer, U., & Wetzel, S. (2004, October). A man-in-the-middle attack on UMTS. In Proceedings of the

ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: noviembre 2018

3rd ACM workshop on Wireless security (pp. 90-97).

Lyon, G. F. (2009). Nmap network scanning: The official Nmap project guide to network discovery and security scanning. Insecure.

Muñoz Villa, D. G. (2006). Seguridad en redes WLAN (Bachelor's thesis).

García Dueñas, M. (2010). Seguridad en WLAN 802.11: evaluación de las contramedidas para combatir el ataque de falsificación (Bachelor's thesis, Universidad Politècnica de Catalunya).

Lashkari, A. H., Danesh, M. M. S., & Samadi, B. (2009, August). A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i). In 2009 2nd IEEE International Conference on Computer Science and Information Technology (pp. 48-52). IEEE.