Guía No. 1 – Pruebas básicas en tarjeta WIFI para pruebas de seguridad

Índice de contenido

Guía No. 1 – Pruebas básicas en tarjeta WIFI para pruebas de seguridad	1
Información de apoyo a la práctica	2
A. Tipos de equipos para estas prácticas	2
B. Tipos de trama	2
1. Tramas de Control	2
2. Tramas de Datos	2
3. Tramas de Gestión (managemet)	3
Tramas de la Capa MAC	3
Fase 1 – Configuración básica de la tarjeta	6
Paso1 - Definir contraseña del root	6
Paso 2 – Identificar valores de la tarjeta WIFI	6
Paso 3 - Cambiar MAC address de la tarjeta WIFI	7
Paso 4 - Activar tarjeta wlan0	7
Paso 5 - Habilitar la tarjeta en modo monitor	8
Fase II – Pruebas de captura de paquetes	9
Prueba 1 – Captura de tráfico	9
Paso 1 - Verificar que esté en modo monitor	9
Paso 2 - Iniciar Wireshark	9
Prueba 2 – Escaneo para Infraestructura (AP)	13
Paso 1 – Prueba de sniffing AP (escaneo de un AP)	13
Paso 2 - Definir canal para el escaneo	13
Paso 3 - Observar captura de tramas en Wireshark seleccionando un determinado canal	13
Prueba 3 – Inyección de tráfico a un AP	15
Paso 0 – Detener los airdump-ng si hubiera alguno corriendo	15
Paso 1 – Utilizar Wireshark para monitorear tramas	15
Paso 2 Inyectar tráfico	16
Tarea	17
Bibliografía	17

Información de apoyo a la práctica

A. Tipos de equipos para estas prácticas

1. Un Punto de Acceso es un aparato que permite conectar estaciones inalámbricas entre sí o incluso estaciones inalámbricas con estaciones por cable.

También un Punto de acceso puede comunicarse con otros puntos de acceso extendiendo la zona inalámbrica o creando un perímetro inalámbrico más grande, es lo que se conoce con el nombre de WDS.

2. Una estación inalámbrica es un dispositivo que puede comunicarse con un punto de acceso y por consiguiente, con el resto de estaciones inalámbricas o con estaciones con cable.

También una estación inalámbrica puede comunicarse directamente con otra sin necesidad de punto de acceso, es lo que conocemos como comunicación ad-hoc.

B. Tipos de trama

1. Tramas de Control

A continuación se describen las tramas de control existentes¹:

- **Request-To-Send (RTS)**: alerta al destino y a otras estaciones sobre transmisión de trama al destino.
- Clear ToSend (CTS): es enviado por el destino. Garantiza permiso para enviar trama de datos.
- Acknowledgment (ACK): es un reconocimiento a la data precedente, trama de gestión o trama PS-Poll. Indica que la trama fue recibida correctamente.
- **Powersave poll (PS-Poll):** requiere que el AP transmita una trama almacenada para una estación que estaba en modo power-save.
- Contention-free (CF)-end: anuncia el fin de un período libre de contención.
- **CF-end + CF-ack:** es un reconocimiento de un CF-end. Libera a la estación de las restricciones asociadas a un período libre de contención.

2. Tramas de Datos

Hay 8 tipos de tramas de datos que se describen a continuación:

- Data: solo contiene data del usuario.
- **Data+CF-Ack:** contienen data y reconoce una trama de data recibida previamente.
- **Data+CF-Poll:** usado por un punto de coordinación para enviar data a un usuario móvil y para requerirle que envíe data que pude estar disponible en su almacenamiento.
- Data+Ack+CF-Poll: combina las funciones de las dos tramas anteriores.
- Las restantes tipos de tramas no transportan data. Tres de estas tienen la misma funcionalidad que las anteriores pero no transportan data.

¹Esta información la tomé del documento "Redes de Área Local y Personal Inalámbricas: 802.11 (Parte I)"elaborado por la Profesora Agregado Maria Elena Villapol de la Universidad Central de Venezuela, Facultad de Ciencias para un Postgrado en Ciencias de la Computación.

• La última trama es **NullFunction** que no tiene data, ni polls, ni ack. Ella solo transporta el bit de gestión de potencia para indicar que la estación está cambiando a un estado de operación en baja potencia.

3. Tramas de Gestión (managemet)

Las tramas de gestión se describen a continuación:

- **Requerimiento de asociación**: enviado por una estación a un AP para requerir una asociación con este BSS.
- **Respuesta de la asociación**: retornado por el AP a la estación para indicar la aceptación o no del requerimiento de asociación.
- **Requerimiento de asociación**: enviado por una estación cuando se mueve de un BSS a otro y requiere hacer una asociación con el AP en el nuevo BSS.
- Respuesta de la reasociación: respuesta a un requerimiento de reasociación.
- **Requerimiento de probe:** usado para obtener información de otra estación o AP. Usado para localizar un BSS.
- **Respuesta del probe**: respuesta a un requerimiento de probe.
- **Beacon**: se transmite periódicamente para permitir que las estaciones móviles localicen e identifiquen a un BSS.
- Anuncio del mensaje de indicación de tráfico: permite a una estación móvil alertar a otra sobre la existencia de tramas almacenadas que están esperando para ser enviadas a ella.
- **Dis asociación:** usado por una estación móvil para terminar una asociación.
- Autenticación: se utilizan múltiples tramas para la autenticación de una estación a otra.
- **Des autenticación**: es enviado por un estación a otra para indicar que se ha terminado una comunicación segura.

Tramas de la Capa MAC

A continuación se describe el formato de las unidades de datos de protocolo (PDUs) intercambiadas entre entidades de la capa MAC (Ver Ilustración 10).





Figura 1: Formato de una PDU (trama) de la capa MAC.

El campo de control de la trama incluye los siguientes campos:

- Versión del protocolo: actualmente 0
- Tipo: identifica el tipo de trama
- Subtipo: indica el subtipo de trama
- Para DS: es colocado en 1 en todas las tramas destinadas al DS (Ver Tabla 1)

• **Del DS**: es colocado en 1 en las tramas que salen del DS (Ver Tabla 1).

Valores de Para DS/Del DS	Significado
Para DS = 0	Tramas enviadas de una estación a otra
Del DS = 0	dentro del mismo IBSS.
Para DS = 1	Tramas de datos destinadas a un DS.
Del DS = 0	
Para DS = 0	Tramas de datos que salen de un DS.
Del DS = 1	
Para DS = 1	Tramas de un sistema de DS inalámbrico
Del DS = 1	distribuidas de un AP a otro.

Tabla 1: Significado de los valores Para DS/Del DS

- **Campo de más fragmento**: indica si éste es la trama de una MSDU fragmentada.
- Reintentar: si está en 1 indica si la trama es una retransmisión.
- **Campo de gestión de potencia:** indica el estado en que se encuentra una estación después de una terminación de una secuencia de intercambio de trama exitosa. Es uno si la estación está en el modo de power-save y en 0 si está en modo activo.
- Más data: indica si hay más MSDUs almacenados para la estación.
- Wired Equivalente Privacy (WEP): si está en 1 indica si el cuerpo de la trama fue procesado por el algoritmo de WEP.
- Orden: si está en 1 indica si las tramas deben estar estrictamente ordenadas.

C – Tipos de herramientas utilizadas.

Para esta práctica se utilizará BT 5r3 y Kali 1.0.5

Sin embargo cualquier versión de BT 5.X y Kali 1.X estará bien. Tambien es posible utilizar las distros Wifiway 3.4 y wifislax 4.6

• Si utiliza Kali, seleccione la opción "Live"



• Si utiliza BackTrack, seleccione la opción "BackTrack Text" y luego digite startx



Fase 1 – Configuración básica de la tarjeta.

El objetivo de esta fase es asignar contraseña al usuario root de nuestro sistema operativo si no lo tuviera (versión live por ejemplo) y cambiar el valor de la dirección MAC de nuestra WIFI, con ello podremos realizar un ataque seguro al evitar que nuestra verdadera MAC sea detectada y poder ubicar en las lecturas de tramas nuestra propia MAC

Paso1 - Definir contraseña del root

root@bt:~# passwd root

Enter new UNIX password: **toor** Retype new UNIX password: **toor** passwd: password updated successfully

Paso 2 - Identificar valores de la tarjeta WIFI

2.1 Identificar si el SO ha reconocido la WIFI

- Si es una WIFI por USB digite lsusb
 - Si es una WIFI integrada digite

Ispci

2.2 Verifique si se reconoce la WIFI

ifconfig

2.3 Identifique la dirección MAC de la WIFI

wlan0 Link encap:Ethernet HWaddr 0a:23:b0:40:a0:11
 UP BROADCAST MULTICAST MTU:1500 Metric:1
 RX packets:0 errors:0 dropped:0 overruns:0 frame:0
 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

Paso 3 - Cambiar MAC address de la tarjeta WIFI

3.1 Verificar id de tarjeta root@bt:~# airmon-ng

InterfaceChipsetDriverwlan0Atheros AR2425ath5k - [phy0]

3.2 Detener modo monitor root@bt:~# airmon-ng stop wlan0

Interface Chipset Driver wlan0 Atheros AR2425 ath5k - [phy0] (monitor mode disabled)

3.3 Detener wlan0 root@bt:~# ifconfig wlan0 down

3.4 Cambiar tarjeta por una MAC más fácil de visualizar Nota: Tenga en cuenta que si están en el laboratorio las Wireless no deberán tener el mismo valor

root@bt:~# macchanger --mac 00:11:22:00:11:22 wlan0

```
Current MAC: 00:24:2b:06:8c:15 (Dlink Corporation)
Faked MAC: 00:11:22:00:11:22 (Cimsys Inc)
```

Nota: En la distro de Kali aparece la identificación del valor permanente de la MAC de la WIFI

<u>Paso 4 - Activar tarjeta wlan0</u>

4.1 Active la tarjeta wlan0 root@bt:~# ifconfig wlan0 up

4.2 Verifique que aparezca la tarjeta wlan0 root@bt:~# ifconfig wlan0

wlan0 Link encap:Ethernet HWaddr 00:11:22:00:11:22 UP BROADCAST MULTICAST MTU:1500 Metric:1 RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

4.3 Verifique que la dirección MAC haya sido cambiada

<u>Paso 5 - Habilitar la tarjeta en modo monitor</u>

5.1 Habilite el modo monitor

root@bt:~# airmon-ng start wlan0

Interface Chipset Driver wlan0 Atheros AR2425 ath5k - [phy0] (monitor mode enabled on mon0)

4.3 Verifique que exista el objeto monitor mon0

mon0	Link encap:UNSPEC HWaddr 00-24-2B-06-8C-15-00-00-00-00-00-00-00-00-00-00
	UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
	RX packets:1477 errors:0 dropped:0 overruns:0 frame:0
	TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
	collisions:0 txqueuelen:1000
	RX bytes:433111 (433.1 KB) TX bytes:0 (0.0 B)
wlan0	Link encap:Ethernet HWaddr 00:11:22:00:11:22 UP BROADCAST MULTICAST MTU:1500 Metric:1 RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

Fase II – Pruebas de captura de paquetes.

El objetivo de esta sección es verificar que la tarjeta WIFI es capaz de capturar todos los tipos de paquetes en una comunicación WIFI, inyectar tráfico de manera satisfactoria Si las pruebas fueran infructuosas se deberá conseguir otra tarjeta WIFI o intentar agregar un módulo que le permita la captura de paquetes. (Es más efectiva la primera opción)

Para esta sección es necesario que haya una computadora, tabet o teléfono celular conectado al AP, de manera que nuestro equipo con Backtrack o Kali pueda monitorear el tráfico en la red de manera silenciosa. Por lo cual no se deberá asociar el BT o Kaly con el AP.

Prueba 1 - Captura de tráfico

<u>Paso 1 - Verificar que esté en modo monitor</u> root@bt:~# airmon-ng

Interface Chipset Driver wlan0 Atheros AR2425 ath5k - [phy0]

Nota: si no existiera mon0, se debe crear monitor mon0 (vea la Fase 1 de esta guía) root@bt:~# airmon-ngstart wlan0

Paso 2 - Iniciar Wireshark

- 2.1 Presionar las teclas: Alt + F2
- 2.2 Digitar en minúsculas: wireshark
- 2.3 En la primera columna seleccionar: mon0
- 2.4 Presione el tercer botón de la barra (start)

 ~ × The Wireshark Network Analyze File Edit View Go Capture Analyze Statistics 	er [Wireshark 1.6.5 (SVN Rev Unknown from unk 5 Telephony Tools Internals Help	(nown)]
en en en en i 📮 🖂 🗙 e	· 밀 · 옥 수 수 수 집 모 · 티로)	
Filter:	Texpression Clear Apply	
WIRESHARK Version 1.6.5 (SVN Rev Unknown from unknown)	Analyzer
Capture	Files	Online
Interface List Live list of the capture interfaces (counts incoming packets) Start capture on interface: eth0 wilan0 Pseudo-device that captures on all i USB bus number 1 USB bus number 2 USB bus number 3	Open a previously captured file Open Recent: Image: Sample Captures A rich assortment of example capture files on the wiki	 Website Visit the project's websit User's Guide The User's Guide (online Security Work with Wireshark as
Capture Options Start a capture with detailed options	kets =	▼ Profile: Default

Nota: en BT el wireshark es la versión 1.6.5 en Kali es la versión 1.8.5

Cuando se inicie la captura se observarán los paquetes que están viajando en el medio.

A 🖌	oplications Pla	ces System 🚬		4	🖂 Fri May 2	24, 7:29	PM 👗					E
~ v	× Capturi	ng from mon0 [Wiresh	ark 1.6.5 (SVN Rev Unk	nown from u	nknown)]							
File E	dit View Go	Capture Analyze Statistics	Telephony Tools Internals	; Help								
	i 0 🎒		🖱 🛃 I 🔍 🗘 🎝 🤇	▶ 🚡 👱		÷	Q Q	++	🏹 🗹 🎦 :	× I 🕐		
Filter:			Expression	ion Clear								
No.	Time	Source	Destination	Protocol Leng	gth Info			_				
	1 0.000000	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon	frame,	SN=2242,	FN=0,	Flags=	C, BI=100,	SSID=cuchillac	
	2 0.098350	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon	frame,	SN=2243,	FN=0,	Flags=	C, BI=100,	SSID=cuchillac	
	3 0.208899	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon	frame,	SN=2244,	FN=0,	Flags=	C, BI=100,	SSID=cuchillac	
	4 0.307205	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon	frame,	SN=2245,	FN=0,	Flags=	C, BI=100,	SSID=cuchillac	
	5 0.405512	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon	frame,	SN=2246,	FN=0,	Flags=	C, BI=100,	SSID=cuchillac	
	6 0.516096	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon	frame,	SN=2247,	FN=0,	Flags=	C, BI=100,	, SSID=cuchillac	
	7 0.614427	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon	frame,	SN=2248,	FN=0,	Flags=	C, BI=100,	, SSID=cuchillac	
	8 0.712710	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon	frame,	SN=2249,	FN=0,	Flags=	C, BI=100,	, SSID=cuchillac	
	9 0.823322	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon	frame,	SN=2250,	FN=0,	Flags=	C, BI=100,	, SSID=cuchillac	
	10 0.921612	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon	frame,	SN=2251,	FN=0,	Flags=	C, BI=100,	, SSID=cuchillac	
	11 1.019942	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon	frame,	SN=2252,	FN=0,	Flags=	C, BI=100,	, SSID=cuchillac	
	12 1.130502	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon	frame,	SN=2253,	FN=0,	Flags=	C, BI=100,	SSID=cuchillac	
	13 1.228810	D-LinkIn 66:0e:87	Broadcast	802.11	326 Beacon	frame,	SN=2254,	FN=0,	Flags=	C, BI=100,	, SSID=cuchillac	v
+ Fra	me 1: 326 by	tes on wire (2608 bits)	, 326 bytes captured (2	608 bits)								
+ Rad	iotap Header	v0, Length 26										
+ IEE	E 802.11 Bea	con frame, Flags:	C									
+ IEE	E 802.11 wir	eless LAN management f	rame									
0000	00 00 la 00	2f 48 00 00 34 7f d4	51 00 00 00 00/H.	. 4Q								
0010	10 02 6c 09	a0 00 df 01 00 00 80	00 00 00 ff ffl									
0020	20 8c 80 bd	Do as oo oo 00 87 Do 7e 58 aa aa aa aa aa aa	as 80 00 0e 87 aa 21 a4 aa a9 ~ ~ Y									
0050	20 00 00 00											
💛 mo	n0: <live captu<="" th=""><th>ire in progress> 🗉 Packet</th><th>s: 207 Displayed: 207 Marke</th><th>d: 0</th><th></th><th></th><th></th><th></th><th></th><th></th><th>Profile: Default</th><th></th></live>	ire in progress> 🗉 Packet	s: 207 Displayed: 207 Marke	d: 0							Profile: Default	

2.5 Detenga la captura de paquetes

Presione el cuarto botón (con x en color rojo)

2.6 Verificar filtros de tramas

Recordando de la teoría (primera sección de esta guía) Para poder determinar los tipos de tramas en 802.11, es recomendable utilizar los filtros de Wireshark

Los filtros los colocamos en la primera caja de texto de la parte superior de Wireshark

Utilice los siguientes filtros

Para tramas de management (de gestión) wlan.fc.type == 0

Para tramas de control
wlan.fc.type == 1

Para tramas de datos wlan.fc.type == 2

Otro filtro interesante es el filtro para los beacon

(wlan.fc.type == 0) && (wlan.fc.subtype == 8)

Utilice los filtros para comprobar que su tarjeta WIFI puede capturar las tramas anteriores.

A.	plications Dia	cos Ouston 🗐		14-10	- Ed May 24 7.2				
Ap	plications Pla	ces System		q	Fn May 24, 7:3.	3 PM 🍝			
^ ×	× mon0 [Wireshark 1.6.5 (SVN	Rev Unknown from	unknown)]					
File E	dit View Go	Capture Analyze Statistic	ts Telephony Tools I	nternals Help					
		🗟 ڬ 🗶 🕯	े 🖉 🗧	୍ର 🔖 🚡 👱	I 3 4	० ० 🖻	🏽 🗹 🔝 🔀	2	_
Filter:	wlan.fc.type =	== 0	V E	Expression Clear	Apply				
No.	Time	Source	Destination	Protocol Len	gth Info				-
	1 0.000000	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon frame,	SN=2242, FN=0	, Flags=C, B	I=100, SSID=cuchillac	
	2 0.098350	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon frame,	SN=2243, FN=0	, Flags=C, B	I=100, SSID=cuchillac	
	3 0.208899	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon frame,	SN=2244, FN=0	, Flags=C, B	I=100, SSID=cuchillac	
	4 0.307205	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon frame,	SN=2245, FN=0	, Flags=C, B	I=100, SSID=cuchillac	
	5 0.405512	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon frame,	SN=2246, FN=0	, Flags=C, B	I=100, SSID=cuchillac	
	6 0.516096	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon frame,	SN=2247, FN=0	, Flags=C, B	I=100, SSID=cuchillac	
	7 0.614427	D-LinkIn 66:0e:87	Broadcast	802.11	326 Beacon frame,	SN=2248, FN=0	, Flags=C, B	I=100, SSID=cuchillac	
	8 0.712710	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon frame,	SN=2249, FN=0	, Flags=C, B	I=100, SSID=cuchillac	
	9 0.823322	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon frame,	SN=2250, FN=0	, Flags=C, B	I=100, SSID=cuchillac	
	10 0.921612	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon frame,	SN=2251, FN=0	, Flags=C, B	I=100, SSID=cuchillac	
	11 1.019942	D-LinkIn 66:0e:87	Broadcast	802.11	326 Beacon frame,	SN=2252, FN=0	, Flags=C, B	I=100, SSID=cuchillac	
	12 1.130502	D-LinkIn 66:0e:87	Broadcast	802.11	326 Beacon frame,	SN=2253, FN=0	, Flags=C, B	I=100, SSID=cuchillac	
	13 1.228810	D-LinkIn 66:0e:87	Broadcast	802.11	326 Beacon frame,	SN=2254, FN=0	, Flags=C, B	I=100, SSID=cuchillac	*
+ Fran	ne 1: 326 by	tes on wire (2608 bits), 326 bytes captu	red (2608 bits)					4
+ Rad	iotap Header	v0, Length 26							
+ IEE	E 802.11 Bea	con frame, Flags:	C						
- IEE	E 802.11 wir	eless LAN management f	rame						
E F	ixed paramet	ers (12 bytes)							
T	agged parame	ters (260 bytes)							100
9	Tag: SSID p	parameter set: cuchill	ac						
	Tag: Suppor	rted Rates 1(B), 2(B),	5.5(B), 11(B), 6,	9, 12, 18, [Mbit	/sec]				
6	Tag: DS Par	rameter set : Current	Channel: 1						
(iii	Tag: Traffi	ic Indication Map (TIM): DTIM 0 of 0 bit	map					
6	Tag: ERP In	nformation							
(ii	Tag. Exten	ded Sunnorted Rates 24	36 48 54 [Mbi	t/secl	100				٣
0030	20 8c 80 bd	7e 58 00 00 00 00 64	00 21 04 00 09	~Xd.!					
0040	63 75 63 68	69 6c 6c 61 63 01 08	82 84 8b 96 0c	uchilla c					
0050	12 18 24 03	01 01 05 04 00 01 00	00 2a 01 00 32 .	*2					
0000	04 30 48 60	00 00 18 00 50 12 02	01 01 03 00 03 .	Un L P					
🔘 Tag	(wlan_mgt.tag), 11 bytes Packe	ets: 1796 Displayed: 17	741 Marked: 0 Droppe	ed: 0			Profile: Default	1

Busque una trama cuyo origen sea un AP y el destino Broadcast

Expanda la sección: IEEE 802.11 wireless LAN management frame

Expanda la sección: Tagged parameters

Observe toda la información del AP: SSID, rates, canal, tipo de encriptación, vendedor, etc.

Analice la información provista por una captura de paquetes tipo datos.

Para la trama de datos

Busque una trama del AP (origen) hacia un cliente WIFI (destino), que contenga en info "Probe Response" Expanda a sección: IEEE 802.11 Probe Response, Observe el fabricante, la MAC address y el BSS Id

Nota: posteriormente necesitará conocer el bssid (nombre del AP). Para esta guía el bssid es: b8:a3:86:66:0e:87 y el ssid es cuchillac

× x mon0 [Wireshark 1.6.5 (SVN Rev Unknown from unknown)] File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help Wan.fc.type == 1
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2" Image: Colspan="2">File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help Image: Colspan="2">Image: Colspan="2">Image: Colspan="2" Image: Colspan="2">File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help Image: Colspan="2">Image: Colspan="2" Image: Colspan="2">Expression Clear Apply No. Time Source Destination Protocol Length Info 640 50.637133 Rim af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C Colspan="2">Colspan="2" 651 51.339295 Rim af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C Colspan="2">Colspan="2" 662 52.040933 Rim af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C Colspan="2">Colspan="2">Colspan="2" 662 52.444947 Rim af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C Colspan="2">Colspan="2" 663 54.146872 Rim af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C Colspa="2">Colspa="2" Colspan="2" <tr< td=""></tr<>
Image:
Filter. Wan.fc.type == 1 v Expression Clear Apply No. Time Source Destination Protocol Length Info 640 50.637133 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 651 51.339295 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 662 52.040933 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 673 52.741639 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 682 53.444947 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 693 54.146872 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 704 54.584731 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 715 55.55602 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C <td< th=""></td<>
No. Time Source Destination Protocol Length Info 640 50.637133 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 651 51.339295 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 662 52.040933 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 673 52.741639 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 682 53.444947 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 693 54.146872 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 714 54.848731 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 715 55.55002 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 715 55.551029 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 727 56.252564 Rim_af:68:83 (RA) 802.11 40
640 50.637133 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 651 51.339295 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 662 52.040933 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 673 52.741639 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 682 53.444947 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 693 54.146872 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 704 54.848731 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 715 55.550602 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 716 55.551029 Rimaf:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 727 56.252564 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 738 56.954444 Rim_af:68:83 (RA)
651 51.339295 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 662 52.040933 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 673 52.741639 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 682 53.444947 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 693 54.146872 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 704 54.848731 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 715 55.550602 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 716 55.551029 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 727 56.252564 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 738 56.954444 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 749 57.656268 Rim_af:68:83 (R
662 52.040933 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 673 52.741639 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 682 53.444947 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 693 54.146872 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 704 54.848731 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 715 55.550602 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 716 55.551029 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 727 56.252564 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 738 56.954444 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 749 57.656268 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 749 57.656268 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 749 57.656268 <t< td=""></t<>
673 52.741639 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 682 53.444947 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 693 54.146872 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 704 54.848731 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 715 55.550602 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 716 55.551029 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 727 56.252564 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 738 56.954444 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 749 57.656268 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 749 57.656268 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 759 58.358165 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 759 58.358165 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 759 58.358165 Ri
682 53.444947 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 693 54.146872 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 704 54.848731 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 715 55.550602 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 716 55.551029 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 727 56.252564 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 738 56.954444 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 749 57.656268 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 749 57.656268 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 759 58.358165 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C
693 54.146872 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 704 54.848731 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 715 55.550602 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 716 55.551029 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 727 56.252564 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 738 56.954444 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 749 57.656268 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 749 57.656268 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 759 58.358165 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C
704 54.848731 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 715 55.550602 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 716 55.551029 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 727 56.252564 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 738 56.954444 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 749 57.655268 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 759 58.358165 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C
715 55.550602 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 716 55.551029 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 727 56.252564 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 738 56.954444 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 749 57.0556268 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 759 58.358.165 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C
716 55.551029 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 727 56.252564 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 738 56.954444 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 749 57.0556268 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 759 58.358.165 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C
727 56.252564 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 738 56.954444 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 749 57.656268 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 759 57.656268 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C
738 56.95444 Rim_af:68:83 RA 802.11 40 Clear-to-send, Flags=C 749 57.656268 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C 759 58.358165 Bim af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C
749 57.656268 Rim_af:68:83 (RA) 802.11 40 Clear-to-send, Flags=C
759 58 358165 Rim af:68:83 (RA) 802.11 40 Clear-to-send Flags= C
🖝 Frame 640: 40 bytes on wire (320 bits), 40 bytes captured (320 bits)
💌 Radiotap Header νθ, Length 26
IEEE 802.11 Clear-to-send, Flags:C
Type/Subtype: Clear-to-send (0x1c)
🖶 Frame Control: 0x00C4 (Normal)
Duration: 100
Receiver address: Rim_af:68:83 (30:69:4b:af:68:83)
😸 Frame check sequence: 0x298c8311 [correct]
0000 00 00 1a 00 2f 48 00 00 e2 f5 d8 54 00 00 00 00/HT
⊖ Frame (frame), 40 bytes ■ Packets: 1796 Displayed: 55 Marked: 0 Dropped: 0 ■ Profile: Default

Capturas para tramas de gestión y beacon

App	lications Pla	aces System 🔄		۵	🖂 Fri May 24,	7:50 PM 💄					
~ v	× Capturi	ng from mon0 [Wires	hark 1.6.5 (SVN Re	v Unknown from	unknown)]						
File Edi	t View Go	Capture Analyze Statistic	s Telephony Tools II	nternals Help							
EN St.	E BI OI		0.4	0 7 4		• • •			/ 6		
			= ~ ~			440			• •		
Filter:	wlan.fc.type	== 0) && (wlan.fc.subtype	e == 8) v E	expression Clear							
No.	Time	Source	Destination	Protocol Le	ngth Info						
16	0.017475	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon fr	ame, SN=673	, FN=0,	Flags=C,	BI=100,	SSID=cuchillac	
74	0.115768	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon fr	ame, SN=674	, FN=0,	Flags=C,	BI=100,	SSID=cuchillac	
130	0.226360	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon fr	ame, SN=675	, FN=0,	Flags=C,	BI=100,	SSID=cuchillac	
196	0.324664	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon fr	ame, SN=676	, FN=0,	Flags=C,	BI=100,	SSID=cuchillac	
261	0.422980	D-LinkIn 66:0e:87	Broadcast	802.11	326 Beacon fr	ame, SN=677	, FN=0,	Flags=C,	BI=100,	SSID=cuchillac	
322	0.533571	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon fr	ame, SN=678	, FN=0,	Flags=C,	BI=100,	SSID=cuchillac	
379	0.631866	D-LinkIn 66:0e:87	Broadcast	802.11	326 Beacon fr	ame, SN=679	, FN=Θ,	Flags=C,	BI=100,	SSID=cuchillac	
441	0.730168	D-LinkIn 66:0e:87	Broadcast	802.11	326 Beacon fr	ame, SN=680	, FN=0,	Flags=C,	BI=100,	SSID=cuchillac	
511	0.840761	D-LinkIn 66:0e:87	Broadcast	802.11	326 Beacon fr	ame, SN=681	, FN=0,	Flags=C,	BI=100,	SSID=cuchillac	
576	0.939064	D-LinkIn 66:0e:87	Broadcast	802.11	326 Beacon fr	ame, SN=682	, FN=0,	Flags=C,	BI=100,	SSID=cuchillac	
625	1.037405	D-LinkIn 66:0e:87	Broadcast	802.11	326 Beacon fr	ame, SN=683	, FN=0,	Flags=C,	BI=100,	SSID=cuchillac	
691	1.147980	D-LinkIn 66:0e:87	Broadcast	802.11	326 Beacon fr	ame, SN=684	, FN=0,	Flags=C,	BI=100,	SSID=cuchillac	
747	1.246287	D-LinkIn 66:0e:87	Broadcast	802.11	326 Beacon fr	ame, SN=685	, FN=0,	Flags=C,	BI=100,	SSID=cuchillac	
+ Frame	10: 326 b	oytes on wire (2608 bit	s), 326 bytes capt	ured (2608 bits)							4
+ Radio	tap Header	v0, Length 26									
- IEEE	802.11 Bea	con frame, Flags:	c								
Ty	pe/Subtype	: Beacon frame (0x08)									
+ Fr	ame Control	l: 0x0080 (Normal)									
Du	ration: 0										
De	stination a	address: Broadcast (ff:	:ff:ff:ff:ff:ff)								
So	urce addres	ss: D-LinkIn 66:0e:87	(b8:a3:86:66:0e:87)								
BS	S Id: D-Lin	nkIn 66:0e:87 (b8:a3:86	5:66:0e:87)								
Fra	agment numb	ber: 0									
Se	quence numb	ber: 673									
a Fr	ame check	sequence Av958h4bdc [/	correct]								*
0000 00	00 1a 00	2f 48 00 00 62 ba 3c	93 00 00 00 00 .	/H b.<	•						A
0010 10	02 6c 09	a0 00 dc 01 00 00 80	00 00 00 ff ff .	.1							
0020 f	f ff ff ff	b8 a3 86 66 0e 87 b8	a3 86 66 0e 87 .	ff.	2						
0030 10	J 2a 80 2d	eb 99 00 00 00 00 64	00 21 04 00 09 .	*d.!							
😑 mon(: <live captu<="" td=""><td>ure in progress> Packe</td><td>ets: 4907 Displayed: 17</td><td>01 Marked: 0</td><td></td><td></td><td></td><td></td><td></td><td>Profile: Default</td><td>1</td></live>	ure in progress> Packe	ets: 4907 Displayed: 17	01 Marked: 0						Profile: Default	1

Prueba 2 - Escaneo para Infraestructura (AP)

Paso 1 - Prueba de sniffing AP (escaneo de un AP)

Con este paso se determinará si la tarjeta WIFI puede trabajar en modo promiscuo, sino se puede trabajar en modo promiscuo y capturar paquetes se deberá utilizar una Tarjeta WI-FI que si lo haga

Digite el siguiente comando para escanear todas las frecuencias

root@bt:~#airodump-ng --bssid b8:a3:86:66:0e:87 mon0

C CH 7][Elapsed: 8 mins][2013-05-24 20:08

BSSID	PWR	Beacons	#Data,	#/s	СН	MB	ENC	CIPHER	AUTH	ESSID
B8:A3:86:66:0E:87	-46	1028	129	0	1	54e.	OPN			cuchillac
DCCID		TON	סשס	Da	+ 0 1	I o o t	Examo	a Droha		
B8:A3:86:66:0E:87	A0:0	B:BA:39:00:	<u>5D</u> -27	ка 54	.tei -	-54	frame 0	s probe 110)	

Una vez terminada el escaneo obtendremos la potencia, canal, MB, tipo de encriptación (por ejemplo WPA2, WPA, WEP, OPN) tipo de cifrado (TKIP, ""), tipo de autenticación (PSK, ""), ssid del AP

Paso 2 - Definir canal para el escaneo

Para concentrar el escaneo en un solo canal definimos el canal en el cual opera el AP Nota: para el siguiente comando se deberá utilizar el canal correspondiente a su propio AP, ya que para esta guía se utilizó el canal 1.

root@bt:~# iwconfig mon0 channel 1

root@bt:~# iwconfig mon0

```
mon0 IEEE 802.11bg Mode:Monitor Frequency:2.417 GHz Tx-Power=20 dBm
Retry long limit:7 RTS thr:off Fragment thr:off
Power Management:on
```

Paso 3 - Observar captura de tramas en Wireshark seleccionando un determinado canal

3.1 Para filtrar sólo las tramas del AP que nos interesa

Utilizaremos el siguiente filtro

wlan.bssid == b8:a3:86:66:0e:87

Tomamos en cuenta que para esta guía la MAC para el SSID es B8:A3:86:66:0e:87

Applications Plac	ces System 🚬		C	🛭 🖂 Fri May 24, 8:00 PM 💄
× mon0 [Wireshark 1.6.5 (SVN R	ev Unknown from u	nknown)]	
File Edit View Go	Capture Analyze Statistics	Telephony Tools Inte	ernals Help	
	🏽 🗎 👱 🗶 C	। ९ 🔶 🗧	> 🕹 🚡	👱 🗐 🕞 । ବ୍ ବ୍ ବ୍ 🖭 🎆 🝸 🍢 🏹 । 😨
Filter: wlan.bssid ==	= b8:a3:86:66:0e:87		pression Cle	ear Apply
No. Time	Source	Destination	Protocol	Length Info
2 0.002115	192.168.0.100	184.107.178.90	ТСР	114 43798 > http [ACK] Seq=1 Ack=1 Win=41216 Len=0 TSval=4294962008 TSecr=99638536
4 0.005429	184.107.178.90	192.168.0.100	HTTP	1502 Continuation or non-HTTP traffic
6 0.010988	184.107.178.90	192.168.0.100	HTTP	1502 Continuation or non-HTTP traffic
8 0.012757	192.168.0.100	184.107.178.90	ТСР	114 39632 > http [ACK] Seq=1 Ack=2801 Win=40668 Len=0 TSval=4294962010 TSecr=996385
10 0.017475	D-LinkIn_66:0e:87	Broadcast	802.11	326 Beacon frame, SN=673, FN=0, Flags=C, BI=100, SSID=cuchillac
11 0.017815	184.107.178.90	192.168.0.100	HTTP	1502 Continuation or non-HTTP traffic
13 0.021895	184.107.178.90	192.168.0.100	HTTP	1502 Continuation or non-HTTP traffic
15 0.023431	192.168.0.100	184.107.178.90	TCP	114 39632 > http [ACK] Seq=1 Ack=5601 Win=40668 Len=0 TSval=4294962011 TSecr=996385
17 0.027389	184.107.178.90	192.168.0.100	HTTP	1502 Continuation or non-HTTP traffic
19 0.032842	184.107.178.90	192.168.0.100	HTTP	1502 Continuation or non-HTTP traffic
20 0.033231	184.107.178.90	192.168.0.100	HTTP	1502 [TCP Retransmission] Continuation or non-HTTP traffic
22 0.034909	192.168.0.100	184.107.178.90	TCP	114 39632 > http [ACK] Seq=1 Ack=8401 Win=40668 Len=0 TSval=4294962012 TSecr=996385
24 0.038296	184.107.178.90	192.168.0.100	HTTP	1502 Continuation or non-HTTP traffic
+ Frame 10: 326 by	ytes on wire (2608 bits), 326 bytes captur	ed (2608 bit	ts)
+ Radiotap Header	v0, Length 26			
IEEE 802.11 Beac	con frame, Flags:	C		
Type/Subtype:	Beacon frame (0x08)			
+ Frame Control	: 0x0080 (Normal)			
Duration: 0				
Destination a	ddress: Broadcast (ff:f	f:ff:ff:ff)		
Source addres	s: D-LinkIn_66:0e:87 (b	8:a3:86:66:0e:87)		
BSS Id: D-Lin	kIn_66:0e:87 (b8:a3:86:	66:0e:87)		
Fragment numb	er: 0			
Sequence numb	er: 673			
+ Frame check s	equence: Ax958h4hdc [co	rrectl		
0000 00 00 la 00 1	2f 48 00 00 62 ba 3c 9	3 00 00 00 00	/H b.<	
0010 10 02 6c 09 a	a0 00 dc 01 00 00 80 0	0 00 00 ff ff]	ا	4
0020 11 11 11 11 11 1	eb 99 00 00 00 00 87 08 a	0 21 04 00 09 *		
Ready to load or ca	apture Packets	: 8372 Displayed: 5307	/ Marked: 0 Dro	opped: 0 🛛 Profile: Default

3.2 Para visualizar paquetes de datos entre AP y cliente

Dependiendo de la cantidad de AP que existan cerca de nuestro AP destino la cantidad de tramas de beacon será mayor, para filtrar paquetes en donde haya información relacionada con datos de los protocolos, utilizamos el siguiente filtro:

(wlan.bssid == b8:a3:86:66:0e:87) && (wlan.fc.type_subtype == 0x20)

A	pplications Plac	es System 🚬		(🛭 🖂 Fri May 24, 8:07 PM 💄	Ξ				
~ `	× Capturin	g from mon0 [Wiresh	ark 1.6.5 (SVN Rev Ur	known fro	m unknown)]					
File E	File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help									
	i ei 🔐	<mark>≥ 11 ≥</mark> × 6	1 2 Q (\$ \$		👱 । 🗐 📑 । ବ୍ ବ୍ ବ୍ 🖭 । 🎆 🗹 ங 🗶 । 😨					
Filter:	b8:a3:86:66:0e	e:87) && (wlan.fc.type_subt	ype == 0x20) 🔻 Expre	ssion Cle	rar Apply					
No.	Time	Source	Destination	Protocol	Length Info					
	58 10.442737	D-LinkIn 66:0e:87	SamsungE 39:00:5d	ARP	90 Who has 192.168.0.100? Tell 192.168.0.1					
	60 10.443796	SamsungE 39:00:5d	D-LinkIn 66:0e:87	ARP	90 192.168.0.100 is at a0:0b:ba:39:00:5d	U				
	63 10.523970	192.168.0.1	239.255.0.1	UDP	263 Source port: 11887 Destination port: 9303					
	77 13.683292	184.107.178.90	192.168.0.100	HTTP	1562 Continuation or non-HTTP traffic					
	79 13.689225	184.107.178.90	192.168.0.100	HTTP	1562 Continuation or non-HTTP traffic					
	81 13.695031	184.107.178.90	192.168.0.100	HTTP	1562 Continuation or non-HTTP traffic					
	82 13.695479	184.107.178.90	192.168.0.100	HTTP	1562 [TCP Retransmission] Continuation or non-HTTP traffic					
	84 13.696604	192.168.0.100	184.107.178.90	TCP	114 39971 > http [ACK] Seq=1 Ack=1449 Win=8712 Len=0 TSval=36023 TSecr=99916583					
	86 13.698812	192.168.0.100	184.107.178.90	TCP	114 39971 > http [ACK] Seq=1 Ack=2897 Win=10160 Len=0 TSval=36024 TSecr=99916583					
	88 13.700522	184.107.178.90	192.168.0.100	HTTP	1562 Continuation or non-HTTP traffic					
	90 13.701551	192.168.0.100	184.107.178.90	TCP	114 39971 > http [ACK] Seq=1 Ack=4345 Win=11608 Len=0 TSval=36024 TSecr=99916583					
	92 13.703893	192.168.0.100	184.107.178.90	TCP	114 39971 > http [ACK] Seq=1 Ack=5793 Win=13056 Len=0 TSval=36025 TSecr=99916583					
	94 13.706046	184.107.178.90	192.168.0.100	HTTP	1562 Continuation or non-HTTP traffic	▼				
+ Fra	me 58: 90 byt	es on wire (720 bits),	90 bytes captured (7	20 bits)						
+ Rad	liotap Header	v0, Length 26								
- IEE	E 802.11 Data	, Flags:F.C								
-	Type/Subtype:	Data (0x20)								
+	Frame Control:	0x0208 (Normal)								
1	Duration: 44									
1	Destination ad	dress: SamsungE_39:00:	5d (a0:0b:ba:39:00:50)						
1	BSS Id: D-Link	In 66:0e:87 (b8:a3:86	66:0e:87)							
	Source address	: D-LinkIn_66:0e:87 (b	08:a3:86:66:0e:87)							
1	Fragment numbe	er: 0								
	Sequence numbe	er: 175								
+	Frame check se	onuence: AvfA84114d [co	rrectl							
0000	00 00 1a 00 2	f 48 00 00 d2 84 01 0	0 00 00 00 00/	Н						
0010	10 6c 6c 09 c	0 00 dc 01 00 00 08 0	2 2c 00 a0 0b .ll	,						
0020	ba 39 00 50 b	18 a 3 86 66 98 87 68 a	13 80 66 96 87 .9.].	Ti	I					
0030				· · · · · · · · · · · · · · · · · · ·						
🔵 ma	on0: <live captur<="" td=""><td>e in progress> 🗉 Packet</td><td>s: 515 Displayed: 77 Mark</td><td>ed: 0</td><td>🗉 Profile: Default</td><td>1</td></live>	e in progress> 🗉 Packet	s: 515 Displayed: 77 Mark	ed: 0	🗉 Profile: Default	1				

Prueba 3 - Inyección de tráfico a un AP

En esta prueba se utilizará el Wireshark para monitorear el tráfico inyectado por la herramienta aireplay-ng

Paso 0 - Detener los airdump-ng si hubiera alguno corriendo

Es decir; se debe finalizar cualquier proceso que se estuviera ejecutando en alguna consola de texto de Backtract o Kali que haya abierto.

Paso 1 - Utilizar Wireshark para monitorear tramas.

1.1 Abrir el Wireshark

1.2 Ejecutar Wireshark y escanear tramas asociadas al AP

Para evitar visualizar tramas de beacon (las cuales no nos dejarían observar la inyección de una forma fácil), utilizaremos el siguiente filtro. Tenga en cuenta que necesitará conocer la dirección MAC del AP o BSSID

(wlan.bssid == b8:a3:86:66:0e:87) && !(wlan.fc.type subtype == 0x08)

El Wireshark comenzará a escanear

Paso 2 Invectar tráfico

Abra una consola de comandos y digite la siguiente instrucción, una vez presionado la tecla "enter" regrese a la ventana del Wireshark para ver la captura, si regresa a la sesión de comandos debe visualizar que se realizado la inyección de manera satisfactoria.

root@bt:~# aireplay-ng -9 -e cuchillac -a b8:a3:86:66:0e:87 mon0

```
20:18:52 Waiting for beacon frame (BSSID: B8:A3:86:66:0E:87) on channel 1
20:18:52 Trying broadcast probe requests...
20:18:52 Injection is working!
20:18:54 Found 1 AP
20:18:54 Trying directed probe requests...
20:18:54 B8:A3:86:66:0E:87 - channel: 1 - 'cuchillac'
20:18:55 Ping (min/avg/max): 1.277ms/17.248ms/24.355ms Power: -35.13
20:18:55 30/30: 100%
```

Con la opción -9 indica que aireplay-ng hará inyección de paquetes (30 de forma predeterminada) Con –e se define el SSID Con –a se define la dirección MAC del AP

Nota: Si llega necesitar definir el canal utilice el siguiente comando:

X	Applications Pla	ces System 🔄		ſ	1 🖂 Fri May 24, 8:19 PM 袅	1
~	V × Capturir	ng from mon0 [Wires	hark 1.6.5 (SVN Rev U	nknown fro	m unknown)]	
File	Edit View Go	Capture Analyze Statistic	cs Telephony Tools Interr	als Help		
	M (M (M)		े 🚊 🔍 🧔 🖓	∿	👱 🗐 🖬 ଏ ଏ ଏ 🖾 😹 🗹 🔝 🗶 😰	
Filte	en: (wlan.bssid =:	= b8:a3:86:66:0e:87) && !(wlan.fc.type_su	ession Cle	ar Apply	
No.	Time	Source	Destination	Protocol	Length Info	
	98 8.126012	D-LinkIn_66:0e:87	00:ba:27:58:71:86	802.11	400 Probe Response, SN=1335, FN=0, Flags=RC, BI=100, SSID=cuchillac	
	99 8.129287	D-LinkIn_66:0e:87	00:ba:27:58:71:86	802.11	400 Probe Response, SN=1335, FN=0, Flags=RC, BI=100, SSID=cuchillac	
	109 8.719517	D-LinkIn_66:0e:87	00:38:a5:a0:65:04	802.11	400 Probe Response, SN=1336, FN=0, Flags=C, BI=100, SSID=cuchillac	
	110 8.722790	D-LinkIn_66:0e:87	00:38:a5:a0:65:04	802.11	400 Probe Response, SN=1336, FN=0, Flags=RC, BI=100, SSID=cuchillac	
	111 8.726113	D-LinkIn_66:0e:87	00:38:a5:a0:65:04	802.11	400 Probe Response, SN=1336, FN=0, Flags=RC, BI=100, SSID=cuchillac	
	112 8.729386	D-LinkIn_66:0e:87	00:38:a5:a0:65:04	802.11	400 Probe Response, SN=1336, FN=0, Flags=RC, BI=100, SSID=cuchillac	
	123 9.315961	00:75:81:4c:d9:26	D-LinkIn_66:0e:87	802.11	36 Null function (No data), SN=446, FN=0, Flags=T	
	124 9.316145	00:75:81:4c:d9:26	D-LinkIn_66:0e:87	802.11	42 Authentication, SN=6, FN=0, Flags=	
	130 9.317646	00:f6:92:42:7e:2a	D-LinkIn_66:0e:87	802.11	36 Null function (No data), SN=446, FN=0, Flags=T	
	131 9.317733	00:f6:92:42:7e:2a	D-LinkIn_66:0e:87	802.11	42 Authentication, SN=10, FN=0, Flags=	
	132 9.320702	D-LinkIn_66:0e:87	00:75:81:4c:d9:26	802.11	400 Probe Response, SN=1337, FN=0, Flags=C, BI=100, SSID=cuchillac	
	133 9.323894	D-LinkIn_66:0e:87	00:75:81:4c:d9:26	802.11	400 Probe Response, SN=1337, FN=0, Flags=RC, BI=100, SSID=cuchillac	
	134 9.327224	D-LinkIn_66:0e:87	00:75:81:4c:d9:26	802.11	400 Probe Response, SN=1337, FN=0, Flags=RC, BI=100, SSID=cuchillac	Ŧ
Ulic	Togy CCTD	cere (eer eycee)				
	Tag: SSID p	stad Patas 1(P) 2(P)	5 5 (P) 11 (P) 6 0	10 10 [M	hit/cocl	
	Tag: Suppor	red Rates 1(b), 2(b),	(happel, 1	12, 10, [1	bit/sec]	
	Tag: DS Fai	formation	channet: 1			(3)
	Tag: Exten	led Supported Rates 24	36 48 54 [Mbit/ce	1		
	Tag: Vendor	Specific: Microsof:	WMM/WME: Darameter Ele	ment		
	+ Tag: Vendor	Specific: Enigram: H	T Canabilities (802 11	n D1 10)		_
	+ Tag: HT Car	abilities (802 11n D1	10)			
	+ Tag: Vendor	Specific: Enigram: H	IT Additional Canabilit	ies (802 1	10 01 00)	
	+ Tag: HT Inf	formation (802 11n D1	10)	105 (002.1	11 01:007	
	Tag: Overla	anning RSS Scan Parame	ters: Tag 74 Len 14			
	- rug. over et	spping 055 Scan rarance	icers, rug /4 cen 14	MA		•
0000	00 00 la 00	2f 48 00 00 3e 0c 6b	0c 00 00 00 00	/H >.k		A
0010	10 02 6c 09	a0 00 d6 01 00 00 50	08 3a 01 00 38l.	P.:	8 F	
0030	80 53 57 d2	bc 09 01 00 00 00 64	00 21 04 00 09 .SW.			
On	non0: <live captu<="" td=""><td>re in progress> Packet</td><td>ets: 1421 Displayed: 451 Ma</td><td>arked: 0</td><td>Profile: Default</td><td></td></live>	re in progress> Packet	ets: 1421 Displayed: 451 Ma	arked: 0	Profile: Default	
	inter anve cupto	ie in progresse in a rucky	ton a new orophayed. Hor in		- Hone bedde	10

root@bt:~# iwconfig mon0 channel 1

Guía de pruebas de penetración en redes WIFI – Elaborada por Ing. Víctor Cuchillac - Página 16 de 17

Tarea

Investigue las siguientes herramientas:

- wireshark
- airmon-ng
- airplay-ng
- airodump-ng

Bibliografía

La información en la sección B "Tipos de tramas" fue tomada del documento "Redes de Área Local y Personal Inalámbricas: 802.11 (Parte I)" elaborado por la Profesora Agregado Maria Elena Villapol de la Universidad Central de Venezuela, Facultad de Ciencias para un Postgrado en Ciencias de la Computación.