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

Índice de contenido

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 existentes[1]:

- **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.

[1]Esta 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).

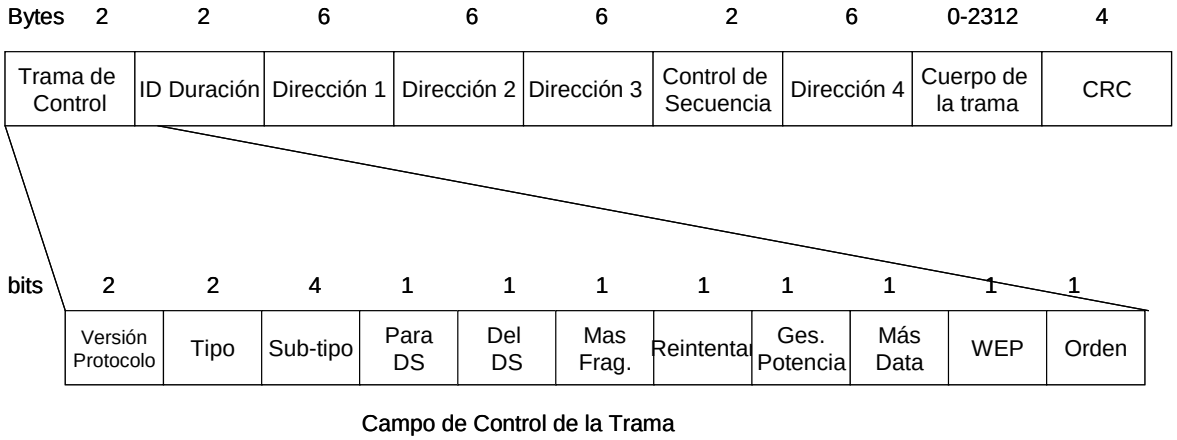


Figura 1: Formato de una PDU (trama) de la capa MAC.

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

lspci

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

Interface   Chipset           Driver
wlan0       Atheros AR2425    ath5k - [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

Paso 4 - Activar tarjeta wlan0

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

Paso 5 - Habilitar la tarjeta en modo monitor

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

Paso 1 - Verificar que esté en modo monitor

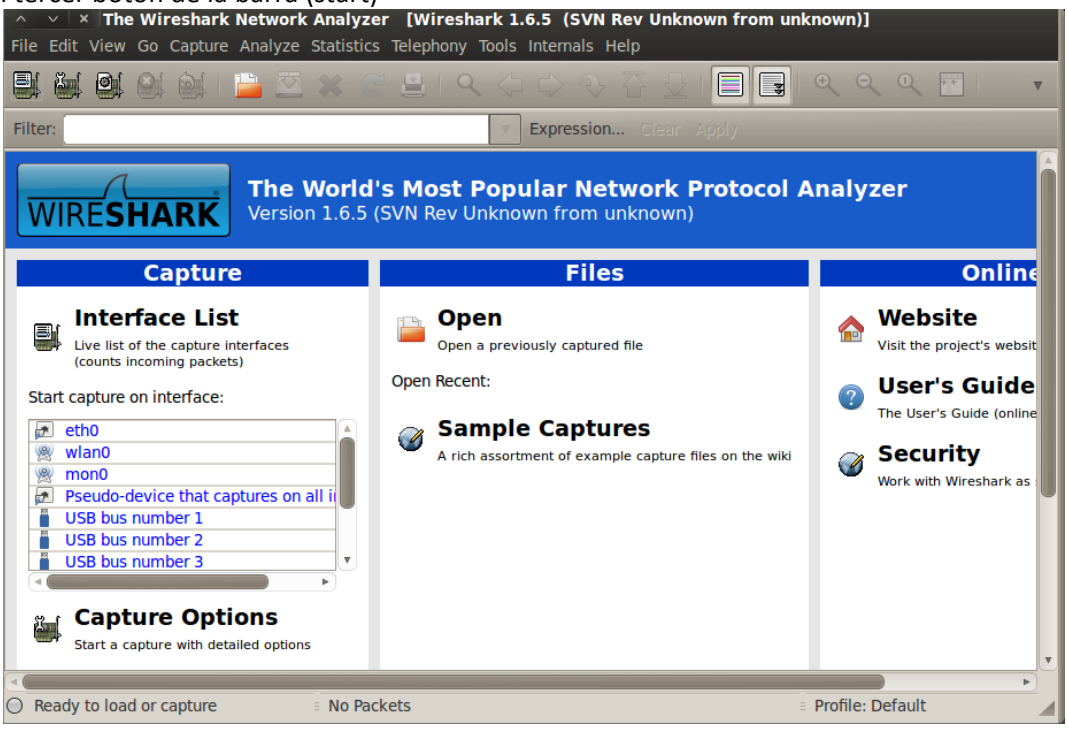
```
root@bt:~# airmon-ng

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
```

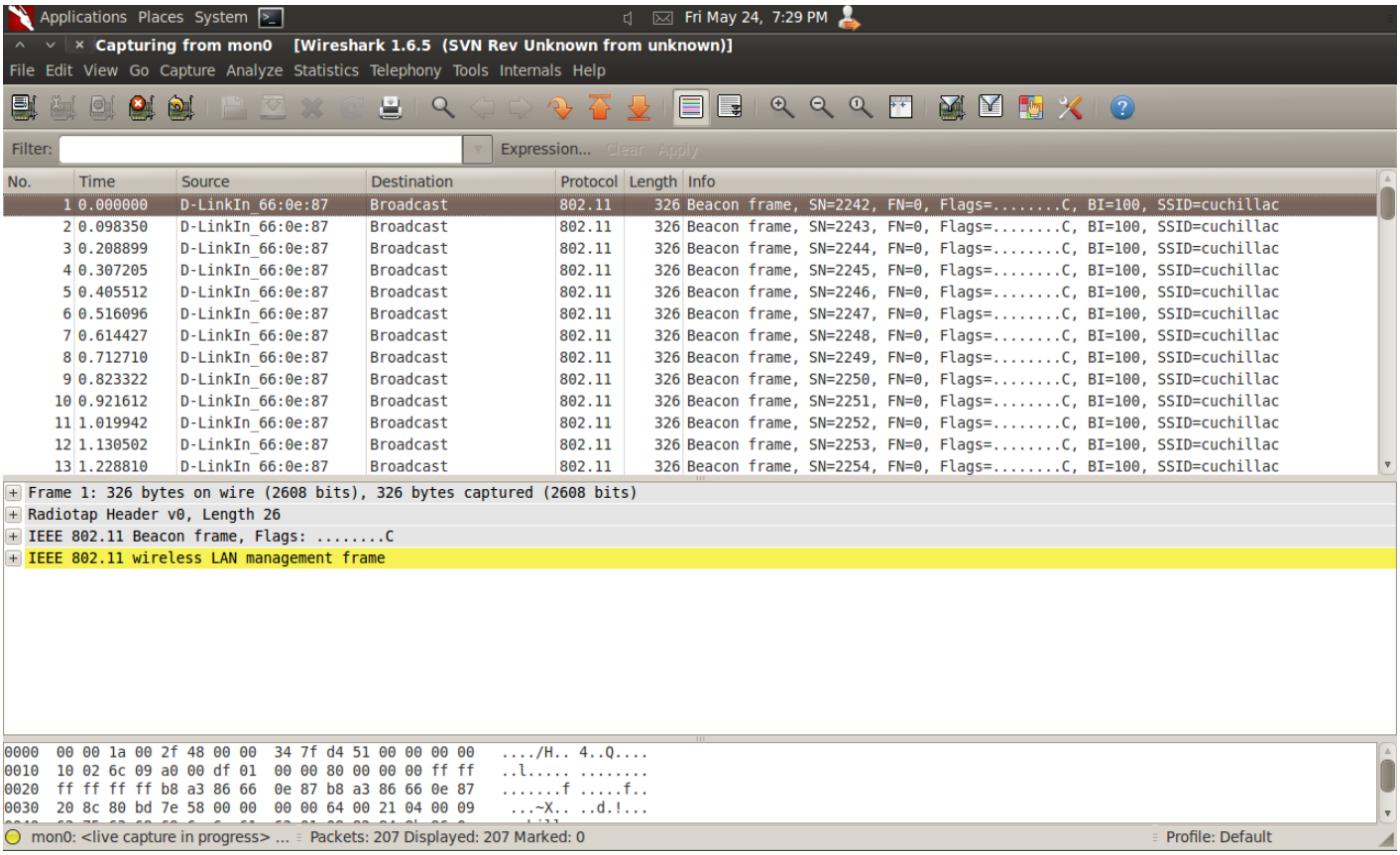
Paso 2 - Iniciar Wireshark

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)



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.



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`

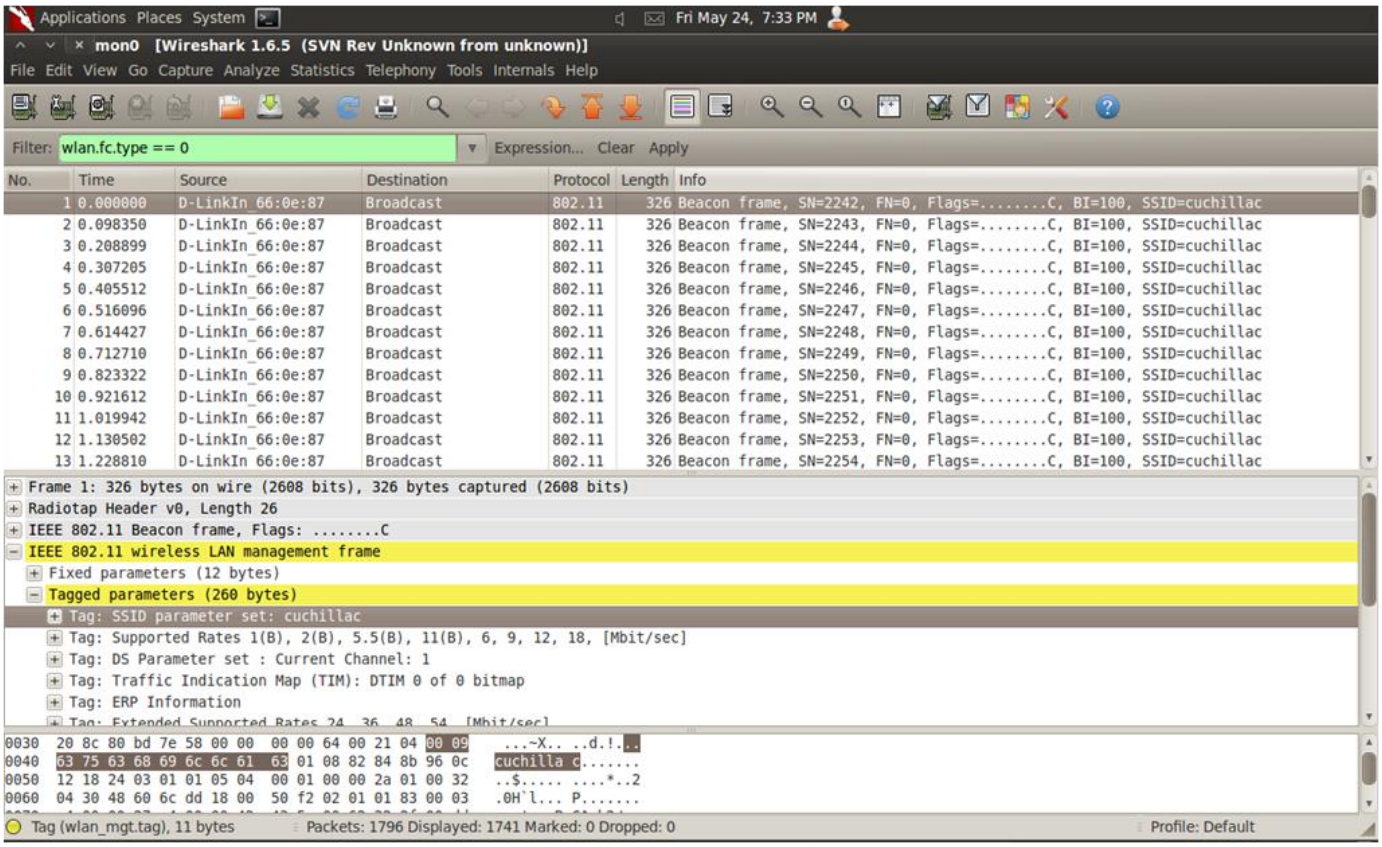
Para tramas de control
`wlan.fc.type == 1`

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.



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

Applications Places System Fri May 24, 7:34 PM

mon0 [Wireshark 1.6.5 (SVN Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.fc.type == 1 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	54.848731		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
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 v0, 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   ..../H.. ...T....
0010  10 02 6c 09 a0 00 a5 02  00 00 c4 00 64 00 30 69   ..l..... ....d.0i
0020  4b af 68 83 29 8c 83 11                            K.h.)...
```

Frame (frame), 40 bytes Packets: 1796 Displayed: 55 Marked: 0 Dropped: 0 Profile: Default

Capturas para tramas de gestión y beacon

Applications Places System Fri May 24, 7:50 PM

Capturing from mon0 [Wireshark 1.6.5 (SVN Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: (wlan.fc.type == 0) && (wlan.fc.subtype == 8) Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
10	0.017475	D-LinkIn_66:0e:87	Broadcast	802.11	326	Beacon frame, SN=673, FN=0, Flags=.....C, BI=100, SSID=cuchillac
74	0.115768	D-LinkIn_66:0e:87	Broadcast	802.11	326	Beacon frame, SN=674, FN=0, Flags=.....C, BI=100, SSID=cuchillac
130	0.226360	D-LinkIn_66:0e:87	Broadcast	802.11	326	Beacon frame, SN=675, FN=0, Flags=.....C, BI=100, SSID=cuchillac
190	0.324664	D-LinkIn_66:0e:87	Broadcast	802.11	326	Beacon frame, SN=676, FN=0, Flags=.....C, BI=100, SSID=cuchillac
261	0.422980	D-LinkIn_66:0e:87	Broadcast	802.11	326	Beacon frame, SN=677, FN=0, Flags=.....C, BI=100, SSID=cuchillac
322	0.533571	D-LinkIn_66:0e:87	Broadcast	802.11	326	Beacon frame, SN=678, FN=0, Flags=.....C, BI=100, SSID=cuchillac
379	0.631866	D-LinkIn_66:0e:87	Broadcast	802.11	326	Beacon frame, SN=679, FN=0, Flags=.....C, BI=100, SSID=cuchillac
441	0.730168	D-LinkIn_66:0e:87	Broadcast	802.11	326	Beacon frame, SN=680, FN=0, Flags=.....C, BI=100, SSID=cuchillac
511	0.840761	D-LinkIn_66:0e:87	Broadcast	802.11	326	Beacon frame, SN=681, FN=0, Flags=.....C, BI=100, SSID=cuchillac
570	0.939064	D-LinkIn_66:0e:87	Broadcast	802.11	326	Beacon frame, SN=682, FN=0, Flags=.....C, BI=100, SSID=cuchillac
625	1.037405	D-LinkIn_66:0e:87	Broadcast	802.11	326	Beacon frame, SN=683, FN=0, Flags=.....C, BI=100, SSID=cuchillac
691	1.147980	D-LinkIn_66:0e:87	Broadcast	802.11	326	Beacon frame, SN=684, FN=0, Flags=.....C, BI=100, SSID=cuchillac
747	1.246287	D-LinkIn_66:0e:87	Broadcast	802.11	326	Beacon frame, SN=685, FN=0, Flags=.....C, BI=100, SSID=cuchillac

```
Frame 10: 326 bytes on wire (2608 bits), 326 bytes captured (2608 bits)
Radiotap Header v0, Length 26
IEEE 802.11 Beacon frame, Flags: .....C
    Type/Subtype: Beacon frame (0x08)
  Frame Control: 0x0080 (Normal)
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: D-LinkIn_66:0e:87 (b8:a3:86:66:0e:87)
    BSS Id: D-LinkIn_66:0e:87 (b8:a3:86:66:0e:87)
    Fragment number: 0
    Sequence number: 673
  Frame check sequence: 0x958b4bdc [correct]

0000  00 00 1a 00 2f 48 00 00  62 ba 3c 93 00 00 00 00   ..../H.. b.<.....
0010  10 02 6c 09 a0 00 dc 01  00 00 80 00 00 00 ff ff   ..l..... ........
0020  ff ff ff ff b8 a3 86 66  0e 87 b8 a3 86 66 0e 87   .......f .....f..
0030  10 2a 80 2d eb 99 00 00  00 00 64 00 21 04 00 09   .*.-.... ..d.!...
```

mon0: <live capture in progress> ... Packets: 4907 Displayed: 1701 Marked: 0 Profile: Default

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  CH  MB   ENC  CIPHER AUTH ESSID
B8:A3:86:66:0E:87  -46     1028      129    0   1  54e. OPN              cuchillac

 BSSID              STATION            PWR   Rate Lost   Frames Probe
 B8:A3:86:66:0E:87  A0:0B:BA:39:00:5D  -27   54   -54      0      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 Places System Fri May 24, 8:00 PM

mon0 [Wireshark 1.6.5 (SVN Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.bssid == b8:a3:86:66:0e:87 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
2	0.002115	192.168.0.100	184.107.178.90	TCP	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	TCP	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 bytes on wire (2608 bits), 326 bytes captured (2608 bits)
+ Radiotap Header v0, Length 26
- IEEE 802.11 Beacon frame, Flags: .....C
    Type/Subtype: Beacon frame (0x08)
  + Frame Control: 0x0080 (Normal)
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: D-LinkIn_66:0e:87 (b8:a3:86:66:0e:87)
    BSS Id: D-LinkIn_66:0e:87 (b8:a3:86:66:0e:87)
    Fragment number: 0
    Sequence number: 673
  + Frame check sequence: 0x958b4bdc [correct]
```

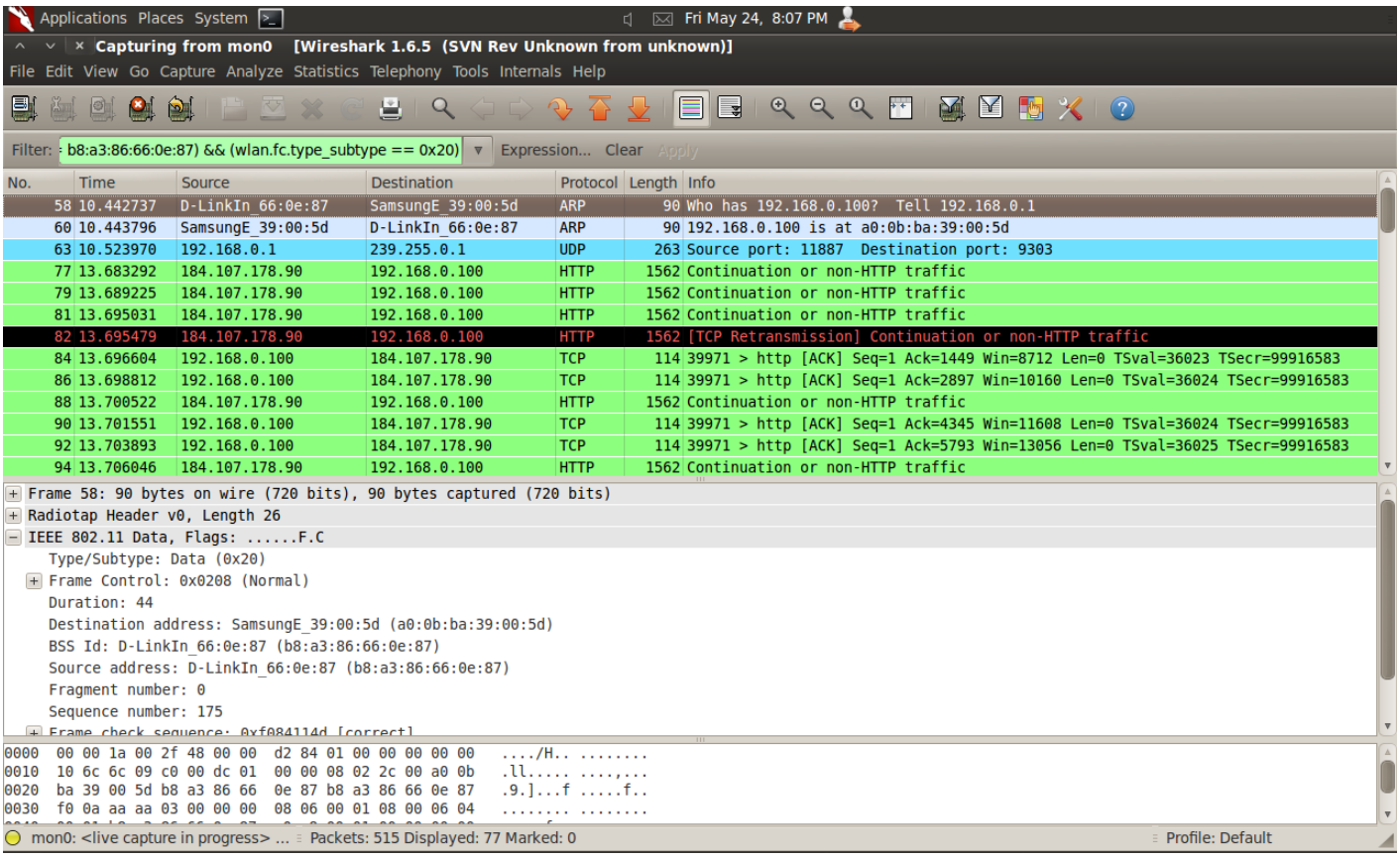
```
0000  00 00 1a 00 2f 48 00 00  62 ba 3c 93 00 00 00 00   ..../H.. b.<.....
0010  10 02 6c 09 a0 00 dc 01  00 00 80 00 00 00 ff ff   ..l..... ........
0020  ff ff ff ff b8 a3 86 66  0e 87 b8 a3 86 66 0e 87   .......f .....f..
0030  10 2a 80 2d eb 99 00 00  00 00 64 00 21 04 00 09   .*.-.... ..d.!...
```

Ready to load or capture | Packets: 8372 Displayed: 5307 Marked: 0 Dropped: 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)
```



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 Inyectar tráfico

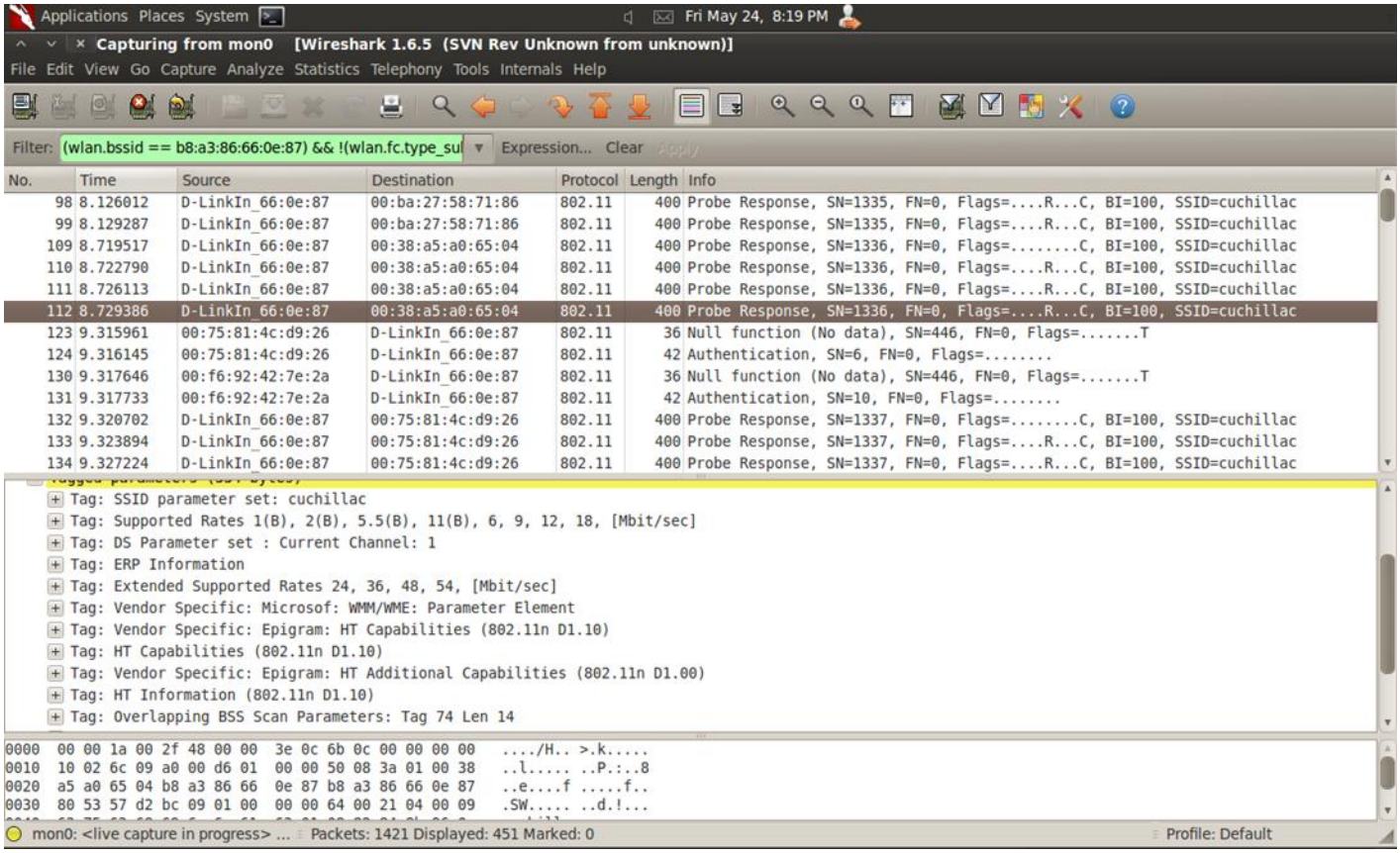
Abra una consola de comandos y digite la siguiente instrucción, una vez presionado la tecla “enter” regrese a la ventana del Wireshark para ver la captura, si regresa a la sesión de comandos debe visualizar que se realizado la inyección de manera satisfactoria.

```
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:

```
root@bt:~# iwconfig mon0 channel 1
```



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.