Vulnerability Detection in Wireless Network 802.11i Through the Link Layer Analysis

Andrés S Troya, Jaime J Astudillo
Department of Electrical and Electronics, Universidad de las Fuerzas Armadas ESPE
Sangolquí- Ecuador
Email:{ astroya, jjastudillo1}@espe.edu.ec

Abstract— This article demonstrates the vulnerabilities of the 802.11i standard. We propose two lab scenarios capturing the management and control frames for analysis in Wireshark followed by a comparison of the advantages and disadvantages of each scenario in order to implement the best option in a real world setting. The first test scenario involves an access point with the capacity to have a Sniffer installed to monitor its network traffic. The second scenario is implemented with a regular AP, which uses an external adapter to capture the Management and Control frames. Both lab scenarios will provide us with valuable information through the Sniffers to detect weaknesses throughout the wireless network according to the 802.11i standard.

Keywords— 802.11i, Wireshark and AP

I. Introducción

Considerando la proliferación de redes inalámbricas, uno de los temas más destacados a considerar es el de la seguridad, cuyo objetivo principal es aislar los actos no deseables, y la prevención de actos potencialmente perjudiciales para la red, de forma que si se producen, hagan el menor efecto dañino posible. Entre las actividades más destacadas que se pueden efectuar para proteger estas redes están: la identificación y autenticación de usuarios, detección de intrusos de la red, análisis de riegos y clasificación de información presentes en la red. Hay que poner mayor énfasis en los factores que inciden dentro del comportamiento de la red, mediante el estudio de diferentes escenarios y del planteamiento de soluciones rápidas y efectivas para asegurar la integridad de los datos y confidencialidad de la red.

Este artículo se centra en la demostración de las vulnerabilidades en el estándar *802.11i* [1]. Se proponen dos escenarios de prueba que pueden realizar la captura de las tramas de gestión y control para el análisis en *Wireshark* [2]. Posterior, se hace una comparación para señalar cada una de las ventajas y desventajas de dichos escenarios con el fin de elegir la mejor opción que se podría aplicar en el mundo real. El primer escenario de prueba implica un punto de acceso con la capacidad de tener un *sniffer* instalado para monitorear el tráfico de la red; el segundo escenario se implementa con un *AP* regular, que utiliza un adaptador externo para capturar las tramas de gestión y de control. Ambos escenarios de prueba nos proporcionarán valiosa información a través del análisis de trafico para encontrar puntos débiles en la red inalámbrica bajo este estándar.

II. El escenario 802.11i

802.1x es un marco de estándares abiertos para autenticar las estaciones inalámbricas conocidos como suplicantes *(supplicants)* con un servidor de autenticación en la red cableada mediante un punto de acceso inalámbrico llamado autenticador *(authenticator)*. El servidor de autenticación conocido como *RADIUS (Remote Authentication Dial-In User Service)* mantiene registros detallados de los usuarios para limitar el acceso a la red de los no autorizados. Estos tres elementos conforman el escenario físico de este entandar.

En la figura que se muestra a continuación, se puede identificar estos tres dispositivos. El suplicantes *iPad (wifi addr: 28:6A:BA:EB:52:67)*, el autenticador *AP* (*wifi addr: 00:1B:B1:00:00:89)* y finalmente el servidor de autenticación *(FreeRADIUS)*. Además, el protocolo de autenticación que se implementa es *EAP-TLS.*

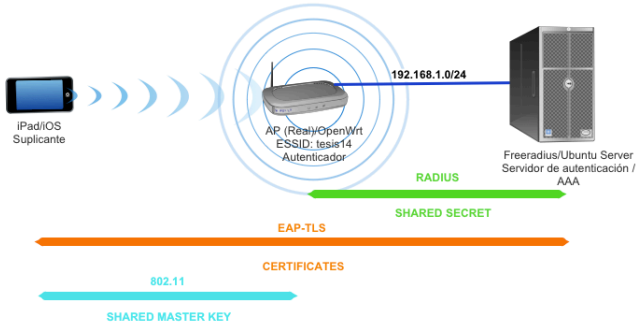

Figura. 1 Escenario 802.11i

Al establecer nuestro escenario de prueba bajo el estándar *802.11i*, se requiere de un protocolo de autenticación. EAP *(Extensible Authentication Protocol)* es el mecanismo oficial adoptado para la autenticación en las redes inalámbricas para las conexiones punto a punto en este modelo.

En los escenarios, se implementa la autenticación EAP-TLS *(EAP-Transport Layer Security)*. Esto debido a que el protocolo TLS, es considerado como uno de los más seguros dentro de los estándares de EAP disponibles en la actualidad.

El servidor RADIUS proporciona su certificado al cliente y solicita el certificado del cliente. El cliente, valida el certificado de servidor y responde con un mensaje de respuesta de EAP que contiene su certificado e inicia la negociación para las especificaciones de cifrado. Después

de validar el certificado del cliente, el servidor responde con las especificaciones de cifrado para la sesión.

OpenSSL es requerido para crear los certificados que permitan la autenticación mutua entre el usuario y el servidor RADIUS.

III. Escenarios de Prueba

Se preparan dos escenarios de prueba, esto con el objetivo de analizar la mejor forma de monitorear y capturar el trafico en una red. Se requiere de *sniffers* para poder estudiar las tramas que se envían en la red inalámbrica y así protegerla contra ataques. Sin embargo, la implementación de estos monitores puede ser mas conveniente que otra, es por eso que se presentan a continuación dos opciones:

A. Escenario 1: Implementado con AP Alix2d2 y Kismet integrado

En la búsqueda de un escenario que nos permita la facilidad de captura de paquetes, hemos considerado la implementación de una red 802.11i con un autenticador (AP) con tarjeta Alix2d2 [3]. Esta tarjeta tienen la capacidad de poder instalar un sistema operativo (OS) libre como OpenWrt [4] que permita instalar un detector de paquetes e intrusiones como es Kismet [5], ambos diseñados para Linux lo que permite su compatibilidad de funcionamiento.

Kismet para nuestro escenario de prueba es implementado bajo infraestructura Server/Drone. Esto quiere decir que el AP con Kismet funcionará como drone permitiéndole así capturar los paquetes y pasarlos a un servidor para su interpretación.

Figura. 2 Tarjeta Alix2d2

B. Escenario 2: Implementado con un AP y adaptador AirPcap Nx

En este escenario consideramos un Access Point que no permite la instalación de un sniffer en su OS. Por ende, se debe considerar la adquisición de un adaptador externo para el análisis de trafico inalámbrico. Se escogió las tarjetas AirPcap Nx [6] para cumplir con este propósito. Las tarjetas AirPcap se conectan por medio de un puerto USB para conectarse por ejemplo en una laptop. Una vez conectada, se capturan los paquetes son capturados a través de Wireshark, esto por cuanto los drivers de la tarjeta son 100% compatibles con este analizador de trafico.

Figura. 3 Adaptador AirPcap Nx

La siguiente tabla resume ventajas y desventajas de la implementación del escenario de prueba con AirPcap Nx o Alix2d2.

AirPcap Nx	Alix2d2	Características
	✓	Escalabilidad
	✓	Precio conveniente
✓		Monitoreo en tiempo real
✓	✓	Compatibilidad Wireshark
✓		Movilidad
	✓	Facilidad para la administración
	✓	Personalizable
✓		Estabilidad del dispositivo
✓		Adaptable a las redes existentes

Tabla. 1 AirPcap Nx vs Alix2d2

La tabla que se muestra a continuación presenta las características físicas de los equipos.

Características	Alix2d2	AirPcap Nx
Memoria interna	2 GB Expansible	No dispone
DRAM	256 MB DDR	No dispone
Frecuencia de trabajo.	2,4 GHz - 5 GHz	2,4 GHz - 5 GHz
Puertos Ethernet	2 puertos	No dispone
Alimentación de energía	Adaptador 12v 2A AC/DC	Energizado por puerto USB
Soporte de estándar.802.11	a/b/g	a/b/g/n
Soporte de estándar de encriptación	WEP, WPA, 802.1x, AES-CCM y TKIP.	WEP, WPA PSK WPA2 PSK.
Canales donde puede trabajar	13	13
Tipo de antena	5.5dBi Omnidireccional Antena Externa	5 dB
VSWR	<2.0	< 2.1

Tabla. 2 Características físicas

IV. Vulnerabilidades

Con el fin de realizar el estudio de vulnerabilidades es importante analizar las capacidades de cualquier hacker o adversario. A partir de la capa de enlace de una WLAN, existen tres posibles tipos de tramas que ya han sido analizadas en el escenario de prueba normal, estas son: Administración, Control y Datos. Como se demuestra a continuación, cualquier manipulación de estas tramas puede

comprometer la confidencialidad, integridad y autenticación.

Los diferentes ataques fueron realizados sobre los escenario que se ha expuesto. Estos escenarios de prueba se encuentra en un modelo de red de infraestructura bajo el estándar *802.11i* y un mecanismo de autenticación EAP-TLS considerado el más seguro y robusto en comparación a otros mecanismos EAP existentes. EAP-TLS se encuentra analizado a profundidad y no ha podido ser demostrado o evidenciado deficiencias graves dentro de el protocolo tales como vulnerabilidades a ataques MITM, esto gracias a su característica principal que, como norma para realizar la autenticación y el establecimiento del túnel cifrado, debe existir un intercambio de certificados digitales, es decir que, el servidor envía su certificado hacia el cliente y de forma reciproca, el cliente envía el certificado hacia el servidor. Cabe señalar que el certificado del cliente debe ser instalado previamente. Cada uno de los certificados debieron haber sido firmados por la misma entidad *(CA)*, de no ser así, serán rechazados y la conexión no será establecida. Si bien el proceso de autenticación de EAP-TLS lo define como el protocolo más seguro en la protección de confidencialidad y autenticación, sigue siendo vulnerable a ataques de denegación de servicios *(DoS)* [7].

El protocolo de autenticación TLS presenta una desventaja para la implementación ya que para redes de media o gran escala la instalación y distribución de los certificados se torna en un proceso tedioso y complicado.

El estándar 802.11i con EAP-TLS es vulnerables a los ataques DoS *(Denial – of - Service)*. El atacante de denegación de servicio es capaz de interrumpir la conexión legitima de suplicantes con el autenticador por medio de las características propias de las redes inalámbricas, un atacante por ejemplo puede denegar servicios mediante la falsificación de tramas de administración no protegidas como las de deautenticación, En este sección, se consideran ataques de *DoS* de uso frecuente que requieren un esfuerzo razonable y no elaborado por parte del adversario para su análisis.

A. Inundación EAPoL - Start

El protocolo *802.1x* comienza con una trama EAPOL-Start que es enviada por el cliente para iniciar la autenticación y continua con la respuesta del *AP* al enviar una trama EAP Request Identity. Un atacante interrumpirá el punto de acceso al inundarlo con tramas EAPoL – Start para agotar los recursos internos del mismo. Este ataque se puede lograr en *BT5* [8] al utilizar el siguiente comando:

>>root@bt:~# mdk3 mon0 x 0 –t (BSSID) –n (ESSID) –s (Speed - Paquetes/s) –c (CH)

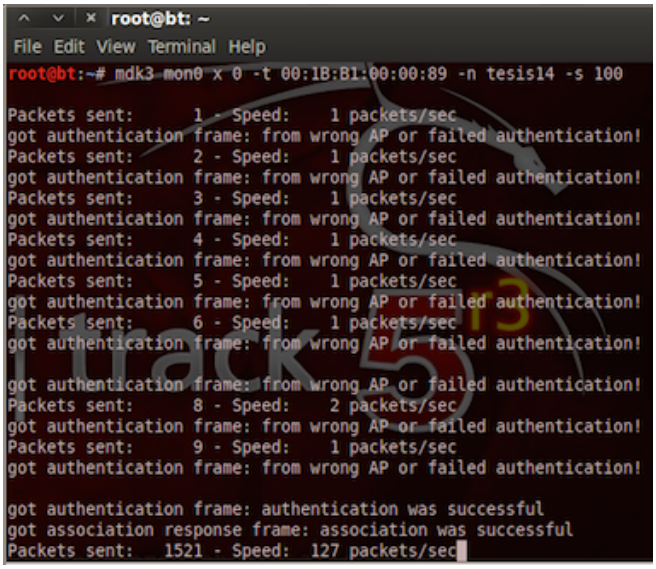

Figura. 4 mdk3 mon0 x

A continuación se observa la captura de las tramas tipo EAPOL – Start generadas a través de *Wireshark* con el objetivo de agotar los recursos del *AP* y obligar a este equipo su reseteo. Se evidencia en el "Source", la creación de direcciones MAC aleatorias de suplicantes realizando peticiones de tramas EAPOL – Start al punto de acceso.

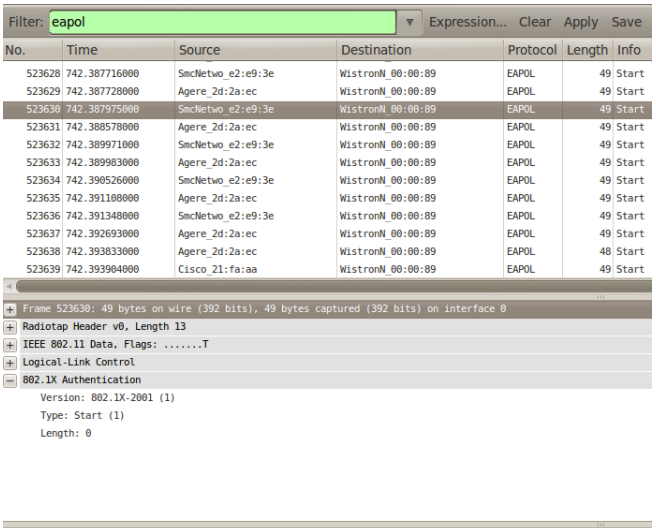

Figura. 5 Wireshark: Inundación EAPoL - Start

B. Inundación Authentication

En el Access Point, cada cliente tiene su estado almacenado en la tabla de asociación. Este estado, tiene un limite de tamaño. Una forma de ataque *DoS* es inundar esta tabla de asociación al crear de forma aleatoria varias tramas de Authentication Request desde MAC ficticias hacia el AP. El punto de acceso al no poder verificar todas estas solicitudes alcanzara su limite y al hacerlo, no podrá autenticar clientes legítimos. Este ataque se lo realiza con el siguiente comando:

>>root@bt:~# mdk3 mon0 a 0 –t (BSSID) –n (ESSID) –s (Speed - Paquetes/s) –c (CH)

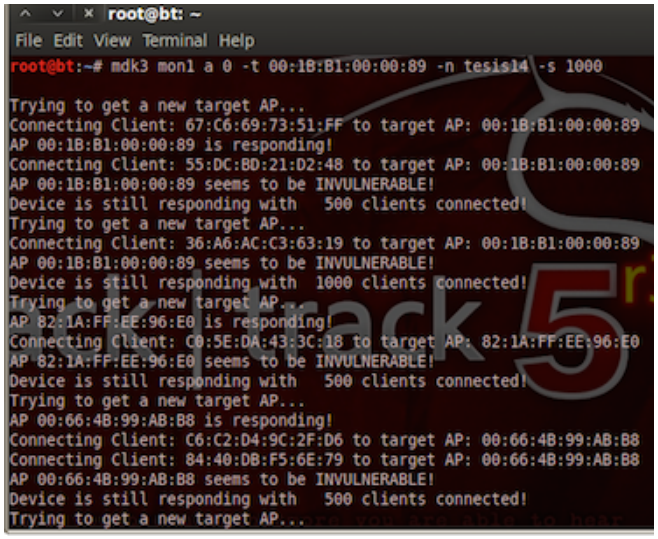

Figura. 6 mdk3 mon1 a

En Wireshark se aprecia la captura de las tramas de clientes con MAC aleatorias solicitando un Authentication Request al AP. Nuevos intentos de autenticación con usuarios legítimos al punto de acceso no fueron exitosos después de este ataque.

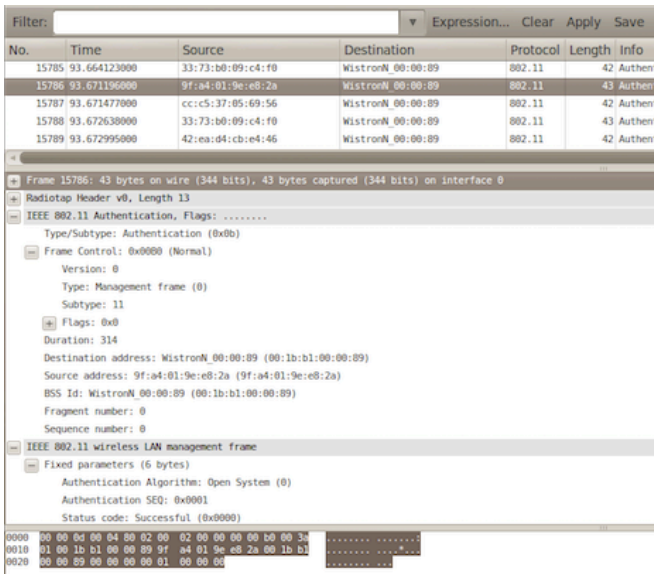

Figura. 7 Wireshark: Inundación Authentication

Los ataques de inundación *EAPoL – Start* y *Authentication* son ejemplos de denegación de servicio contra el autenticador. Además, la inundación de *Authentication* es manipulación de la trama de administración.

C. Inundación CTS/RTS

El estándar 802.11 establece tramas de control como *Request to Send* y *Clear to Send* para minimizar la posibilidad de colisiones al existir envió de tramas extensas. En la siguiente figura se puede ver el como funciona.

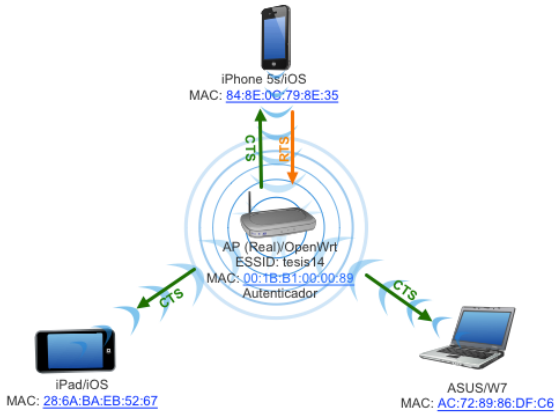

Figura. 8 CTS/RTS

En el caso en que el cliente (iPhone 5s) quiera realizar el envió al *AP* de una trama extensa primero envía una petición de RTS para reservar el canal con el fin de evitar así las colisiones. Entonces el punto de acceso responde con una trama CTS que reserva el canal por el tiempo que dure el envío. La trama CTS a su vez, se enviará a los demás clientes (iPad y ASUS) dejándolos saber que solo el iPhone 5s puede trasmitir por ese tiempo.

Teniendo este concepto claro, la inundación de CTS por parte de un atacante impulsa a otros dispositivos inalámbricos que comparten la red WiFi a frenar su trasmisión hasta que el adversario deje de transmitir las tramas CTS.

Para realizar este ataque, en BT5 se descarga la herramienta necesaria *framespam* [9].

El "file" es un archivo .txt (trama CTS.txt) donde se ingresa la trama CTS que se va a enviar. La trama Clear to Send es:

Figura. 9 Trama CTS

En el archivo .txt únicamente la información de la trama: \0304\0\0\0175\01\02\03\04\05\06

Se ignora el FCS (Frame Check Sequence) debido a que se calcula por el hardware antes de enviarse.

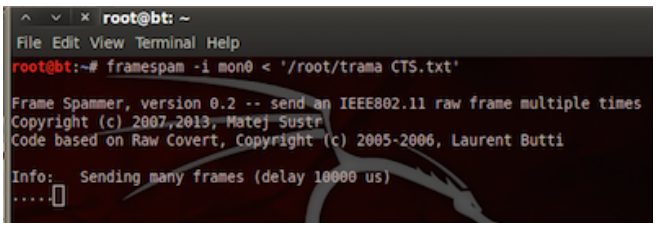

Figura. 10 CTS/RTS

Este ataque se ve en Wireshark como se muestra en la siguiente figura:

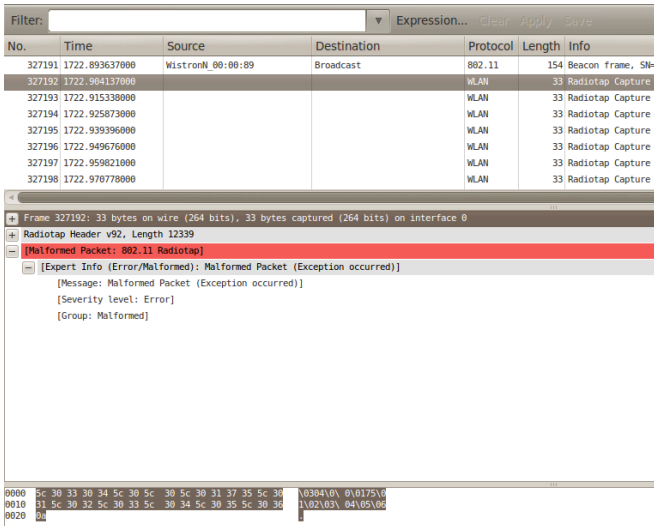

Figura. 11 Wireshark: Inundación CTS

Esta inundación deja la red atacada totalmente sin respuesta, tanto el cliente como el *AP* dejan de trasmitir.

D. Ataque de Interferencia

Al implementar un AP falso, el mejorar los niveles de potencia nos da una ventaja sobre el AP legitimo, esto por cuanto se amplia el área de cobertura y atrae la conexión o asociación de clientes legítimos con nuestro AP (Falso).

Se inicia el AP falso al iniciar el hostapd en *BT5*

>>root@bt:~# hostapd hostapd-2.0/hostapd/hostapd.conf

El archivo *hostapd.conf* ya esta pre configurado con toda la información que obtuvimos de esnifar la red para simular ser el *AP* real, es decir, mismo ESSID (tesis14), etc. Como el punto de acceso falso tiene mejores niveles de potencia. los clientes o suplicantes van a tender a conectarse con este equipo, logrando así un ataque exitoso de *DoS*.

En la siguiente figura se evidencia los clientes legítimos y AP (Real) conectados.

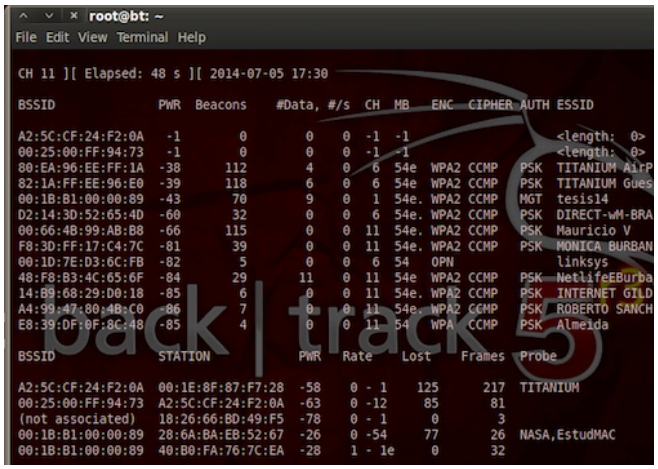

Figura. 12 AP (Real) y clientes legítimos asociados

Ahora se muestra en la figura los clientes legítimos que se asocian en el AP falso (wifi addr: 00:80:48:77:01:CE) debido al ataque de interferencia.

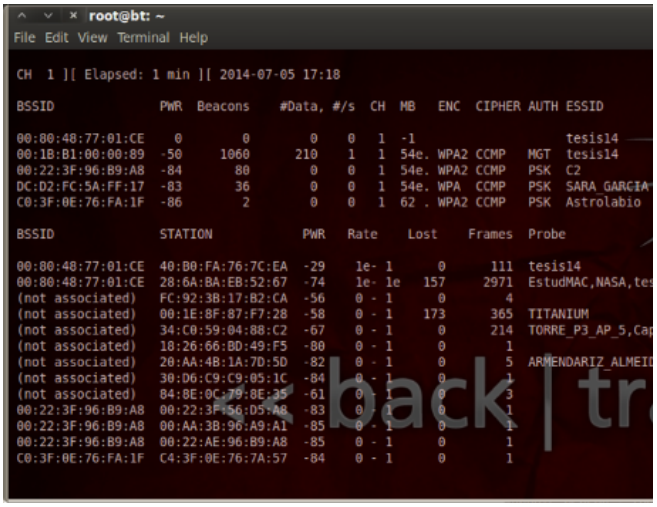

Figura. 13 AP (Falso) y clientes legítimos asociados

Los ataques de Inundación CTS/RTS e interferencia son ejemplos de denegación de servicio contra la infraestructura. Además, la inundación de CTS/RTS es manipulación de la trama de control.

E. Inundación Deauthentication

Este ataque tiene como objetivo desvincular al cliente del punto de acceso. Este ataque se vulnera la red con los siguientes comandos:

Para crear un DoS generalizado que desautentique todos los usuarios del AP se pone:

>>root@bt:~# aireply-ng -0 5 –a (BSSID) mon0

Esto se muestra en la siguiente figura:

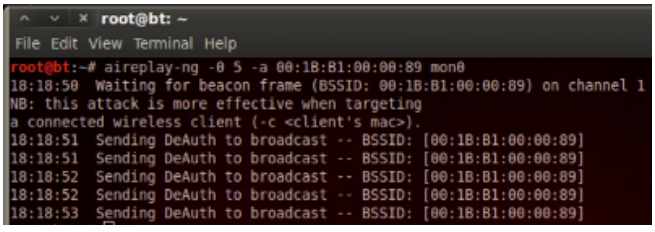

Figura. 14 Deauthentication todos los usuarios

En Wireshark se puede ver las tramas suplantadas con la dirección MAC del Access Point para desautenticar todos los clientes.

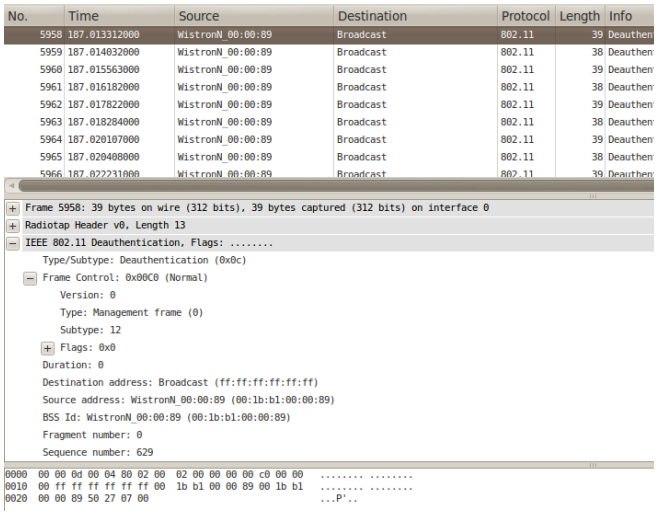

Figura. 15 Wireshark: Inundación Deauthentication

En el caso en que de pretenda desautenticar un solo cliente del AP con el fin de realizar un ataque *DoS* se hace uso del siguiente comando:

>>root@bt:~# aireply-ng -0 5 –a (BSSID) –c (MAC STATON) mon0

En la siguiente figura se puede ver la ejecución de este comando.

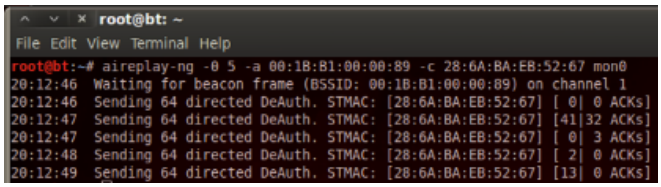

Figura. 16 Deauthentication usuario especifico

A continuación se puede visualizar la des autenticación de un único usuario en Wireshark:

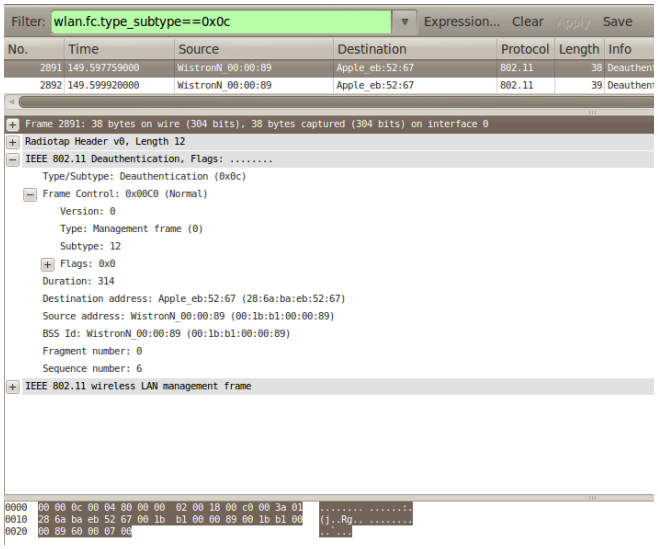

Figura. 17 Wireshark: Inundación Deauthentication usuario especifico

El ataques de desautenticación es un ejemplo de denegación de servicio contra el cliente manipulando la trama de administración.

V. Análisis de Resultados

Al completar la evaluación de los escenarios de prueba, se determinó que para un ambiente administrable, el *AP* con Kismet incorporado es el mas optimo, pero requiere la adquisición de estos equipos para cada uno de sus puntos de acceso, mientras que al utilizar las tarjetas AirPcap Nx estas se adaptan al entorno de red existente.

Las capturas de trafico en ambos casos son compatibles para su análisis en Wireshark. Sin embargo, el monitoreo con AirPcap de las tramas se lo realiza en tiempo real a diferencia que con las tarjetas Alix2d2 únicamente la captura se realiza en tiempo real.

El análisis de los paquetes capturados por los dos escenarios son los mismos, por lo que su implementación en el mundo real no va a estar basada en esta información sino mas bien en la configuración de red que se tenga en base a las ventajas y desventajas del diseño de cada una.

El protocolo de autenticación EAP-TLS crea un túnel seguro entre el servidor de autenticación y el suplicante, esto por cuanto se requiere la instalación de certificados validos en ambos partes para establecer confianza con la autoridad de certificación *(CA)*. Esto garantiza la inefectividad de ataques como MITM *(men in the middle)* o enmascaramiento de *AP* maliciosos para la obtención de las credenciales por medio de fuerza bruta utilizando ataques con diccionarios.

El método de EAP-TLS presenta una vulnerabilidad en el caso en que no se instale los certificados tanto en el servidor como en el cliente. Esto lo se detectó en dispositivos iOS, sucede cuando el cliente no tiene instalado el certificado y se requiere establecer la conexión por medio del protocolo de autenticación EAP. En la negociación del túnel en el paso 13 de la Figura. 108, se realiza la negociación y el equipo al no contar con los certificados instalados opta por el método PEAP, el mismo que es vulnerable a ataques de MITM, enmascaramiento de AP malicioso y ataques de fuerza bruta con diccionario, que permitirá obtener las credenciales del usuario, y posterior el ingreso a la red.

El estándar 802.11i es vulnerable a los ataques de denegación de servicio *(DoS)* debido a que las tramas de administración y control viajan por el medio sin encriptación, esto deja las tramas susceptibles a un usuario malicioso que las pueda usar para su conveniencia.

Referencias

- [1] I. Overview, N. Cam-winget, and C. Systems, “IEEE 802.11i.” [Online]. Available: http://csrc.nist.gov/archive/wireless/S10_802.11i Overview-jw1.pdf.
- [2] “Wireshark.” [Online]. Available: http://www.wireshark.ch/en/.
- [3] “Alix2d2.” [Online]. Available: http://linitx.com/product/alix-2d2-system-board-lx800-256mb-ram-2-lan-2-minipci-usb/12568.
- [4] “OpenWrt.” [Online]. Available: https://openwrt.org/.
- [5] “Kismet.” [Online]. Available: https://www.kismetwireless.net/.

- [6] U. S. B. W. Adapter and E. A. Support, “AirPcap Nx.” [Online]. Available: http://www.cacetech.com/documents/AirPcap Nx Datasheet.pdf.
- [7] “Ataques DoS.” [Online]. Available: http://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/7-2/wIPS_Configuration/Guide/wIPS_72/msecg_appA_wIPS.html.
- [8] “BackTrack.” [Online]. Available: http://www.backtrack-linux.org/downloads/.
- [9] “framespam.” [Online]. Available: http://matej.sustr.sk/code/framespam/framespam.en.html.