Análisis de los Sistemas de Ataque y Protección en redes inalámbricas Wi Fi, bajo el Sistema Operativo Linux.

Yacchirema E. Ana M.[1], Alulema F. Darwin O.[2], Aguilar S. Darwin L.[3]

RESUMEN

Este artículo describe la preparación de una red inalámbrica Wi Fi en producción, con los sistemas de detección de intrusos Snort y Kismet; para su posterior evaluación bajo ataques. A través de pruebas de penetración con Backtrack 5 R3, usando sus herramientas Fern WiFi Cracker y Ettercap, para proceder a monitorear las respuestas de reacción de los IDSs, como son sus “alertas”.

Una vez culminados los ataques, los resultados son objeto de análisis, tanto del tráfico capturado por los sistemas gracias a Wireshark, así como la descripción del ataque de sus alertas; para así determinar las características de respuesta de Snort y Kismet; además se deducen recomendaciones mínimas de seguridad, dirigidas tanto a los administradores de la red y los clientes; para evitar inconvenientes con los atacantes.

Palabras clave: Wi Fi, Snort, Kismet, Ataques, Backtrack.

[1] Ana M. Yacchirema E. Carrera de Ingeniería Electrónica, Redes y Comunicación de Datos, Universidad de las Fuerzas Armadas ESPE, Sangolquí-Ecuador. (e-mail: anita89_23@hotmail.com).

[2] Darwin O. Alulema F. Departamento de Eléctrica y Electrónica, Universidad de las Fuerzas Armadas ESPE, Sangolquí-Ecuador. (e-mail:darwinalulema@gmail.com).

[3] Darwin L. Aguilar S. Departamento de Eléctrica y Electrónica, Universidad de las Fuerzas Armadas ESPE, Sangolquí-Ecuador. (e-mail: dlaguilar@espe.edu.ec).

ABSTRACT

This article describes the preparation of a WiFi wireless network in production, with Snort and Kismet intrusion detection systems; for further evaluation under attacks. Through Penetration Testing with Backtrack 5 R3, using its Fern WiFi Cracker and Ettercap tools, to proceed to monitor the responses of reaction of IDSs, such as their "alerts".

Once culminated attacks, the results are analyzed both captured traffic for the systems by Wireshark, and the description of the attack of their alerts, in order to determine the response characteristics of Snort and Kismet, also deduce minimum security recommendations, addressing both network administrators and clients, to avoid problems with the attackers.

Key Words: Wi Fi, Snort, Kismet, Attacks, Backtrack.

I. INTRODUCCIÓN

Las redes inalámbricas Wi Fi en la actualidad son parte importante de la infraestructura de red, porque brinda la comodidad y libertad de cables, que ha impulsado su uso y desarrollo.

La comunidad tecnológica se ha preocupado de sus dos grandes debilidades, velocidad y seguridad, desarrollando algoritmos y protocolos criptográficos que permitan brindar más protección a la información, sin dejar de lado la optimización del tiempo en su procesamiento que afecte las aplicaciones actuales en tiempo real y QoS.

El aire como medio de comunicación es muy sensible a los atacantes, pese a los

esfuerzos de la IEEE y la Alianza Wi Fi, siguen apareciendo técnicas y herramientas que están logrando vulnerar las seguridades en las redes inalámbricas.

Más allá del software y hardware, el factor humano de la organización jugará un papel decisivo, llevando buenas prácticas de seguridad y un personal técnico proactivo, tomando el papel de un hacker más.

II. PROTOCOLOS DE SEGURIDAD 802.11

Según el IEEE802.11 [1], existen dos tipos de algoritmos:

-Previo RSNA (Asociación de red de seguridad robusta): autenticaciones débiles como WEP y sistema abierto(nula autenticación) .

- RSNA: protocolos más robustos.

Tabla.1. Protocolos de Seguridad 802.11

Previo-RSNA	RSNA
Autenticación Sistema abierto(el cliente solicita y se acepta)	***TKIP***(incluye MIC para la integridad, IV mejorado, contador de secuencia TSC)
WEP(débil clave, bajo mecanismos de inyección se llega adivinar la clave, IV débil, CRC32)	***CCMP***(802.11i lo considera obligatorio, AES, CBC-MAC)
	BIP(CMAC, trabaja con la MIC para las tramas de gestión "MME")
	SAE(intercambio de clave maestra de par sabio PMK)
	802.1x(trabaja mediante la comunicación de un solicitante, un AP autenticador y un servidor de autenticación)
	WPA(usa TKIP, MIC, modo personal y empresarial)
	WPA2(implementación 802.11i)

- **Ataques en las redes 802.11**

Los atacantes de las redes inalámbricas no necesitan subir más allá de la capa de enlace de datos para atacar; porque su punto más débil es el medio de comunicación susceptible a captura e interceptación. Una vez logrado el objetivo del atacante pueden actuar activamente sobre la información incluso seguir escalando en el acceso a la red. Los ataques más comunes son:

Tabla.2. Ataques en las redes inalámbricas

Ataque	Funcionamiento
Craqueo de Mecanismos de encriptación y autenticación	Usado principalmente en WEP, son algoritmos de adivinanza de la clave, Ataques FMS.
Ataques de Vigilancia	Captura de datos de la WLAN en el medio, Eavesdropping ó sniffing, que conllevan a personas a ubicar WLANs (wardriving), y marcar su tipo de seguridad (Walkchalking).
DoS	Dejar fuera servicio a un cliente o AP legítimo. Ej: envío de tramas de des autenticación, envío de canal ocupado, inundación de solicitudes de autenticación.
Ataque AP Masquerading ó Evil Twin	APs intrusos que copian la configuración de APs legítimos, para engañar a clientes cercanos a él.
MAC Spoofing	Disfraza la MAC original, con otra legítima en la WLAN.
ARP Poisoning/Man in the Middle	Envío de respuestas ARP colocando la MAC de otro equipo en lugar de un legítimo, así logra ubicarse el atacante en la mitad de una comunicación (man in the middle).
Ataques de diccionario y fuerza bruta	Prueba y error adivinando la clave desde un conjunto de claves (diccionario) ó generando aleatoriamente (fuerza bruta).

III. SISTEMAS DE DETECCIÓN DE INTRUSOS

Los sistemas de detección de intrusos son sistemas que permiten monitorear el tráfico de un host o red en busca de tráfico anómalo y si lo considera como ataque emite alertas.

Los sistemas de detección de intrusos a evaluar son:

-**SNORT:** es un sistema de detección y prevención de intrusos de red (IDS/IPS) desarrollado por Sourcefire. Combinando los beneficios de la inspección basada en firmas, protocolo y anomalías. [3]

-KISMET: Es un detector de redes inalámbricas 802.11, sniffer e IDS que puede detectar ataques en la capa de enlace de datos y red, trabaja con tarjetas inalámbricas que soporten el modo monitoreo para observar el tráfico 802.11 en sus estándares a, b, g y n, según permita el controlador y hardware de la tarjeta. [4]

IV. BENCHMARKS

Son las técnicas con las que se evalúa la función y rendimiento de un sistema, a continuación se enumeran algunos de las metodologías y técnicas para evaluar la seguridad informática:

-Como técnicas de evaluación de seguridad se aplica las pruebas de penetración y análisis de vulnerabilidades.

-Por su lado las metodologías de pruebas de seguridad permiten direccionar las necesidades de evaluación de seguridad, destacar debilidades, definir características claves y beneficios de los sistemas. Ej:

OSSTMM (Open Source Security Testing Methodology Manual) que define grupos claves de procesos (Alcance, Canal, Índice y Vector), que corresponden a la recolección de datos en pruebas, tipo de comunicación, Clasificación de las pruebas según los objetivos, análisis de objetivos.

ISSAF (Information systems Security Assessment Framework) que define dos enfoques; el técnico correspondiente a las reglas y procedimientos a seguir en la evaluación, el administrativo consiguiendo mejores prácticas y compromiso de la organización a lo largo de las pruebas.

- **Backtrack 5 R3**

Es una herramienta de software libre, muy reconocida en el medio de auditorías de seguridad; posee un conjunto de herramientas muy útiles al momento de evaluar redes inalámbricas.

En el existe una gran cantidad de herramientas entre las que se destaca aircrack, airmong; incluso herramientas gráficas, que brindan una interfaz agradable y fácil de usar; siendo objeto importante en esta evaluación como son: Fern Wi Fi Cracker y ettercap.

Fig.1. Despliegue de las opciones de WLAN Exploitation

V. PROCESO DE EVALUACIÓN

Se asume el proceso que se define de las metodologías mencionadas anteriormente en el siguiente procedimiento:

1. Preparar el escenario y poner en marcha los sistemas a evaluar (Snort y Kismet).
2. Realizar las pruebas (atacar con Backtrack 5 R3).
3. Recolección de datos (alarmas, capturas, informes emitidos por los sistemas).
4. Clasificación de los datos y su consecuente análisis.
5. Determinación de resultados de la evaluación (determinación de características de respuesta de los IDSs).
6. En este punto final, gracias a todo el proceso y principalmente los resultados, se procede a emitir recomendaciones mínimas de seguridad; documentadas por escrito en un informe, tanto para el administrador de red como para los clientes.

VI. PREPARACIÓN DEL ESCENARIO

Componentes de la topología de pruebas:

La topología de pruebas en producción está conformada principalmente por un Wireless Fortigate 100D; quien realiza la función de controlador inalámbrico; usa el sistema de distribución (DS) de la red de la organización para conectarse a los APs (FortiAPs); quienes emiten los SSIDs que han sido definidos en la administración de la controladora con sus respectivos permisos de acceso.
El controlador inalámbrico posee tres conexiones hacia el firewall de la organización: los puertos con IP 10.200.10.2 , 10.200.11.2 y 10.200.11.3. El primero permite a los clientes de determinados perfiles; el acceso a la LAN de la organización, el segundo permite la conexión al proveedor de internet 1 a través del firewall y el último permite la conexión a internet; igualmente del proveedor 1, para los invitados a la red inalámbrica de la organización (fig.3).
Adicional posee una conexión independiente del firewall hacia un proveedor de internet 2 (puerto 200.31.26.154).
Se configura un SSID “Pruebas” para la evaluación, con seguridad WPA Personal, para evitar inconvenientes con el resto de SSIDs en producción, se escoge un FortiAP de la organización y se indica a través del controlador que transmita el SSID de pruebas.

Con objeto de las pruebas se colocaron los siguientes equipos:

-Se coloca un equipo con sistema operativo Ubuntu 12.0.4; con Snort y Kismet instalados según indicaciones de sus páginas web oficiales [4][5].
-Se conecta una tarjeta D-Link DWA125 A3 para las pruebas con Kismet y para Snort se coloca un switch(configurado port mirroring) entre el FortiAP y el switch de acceso, debido a que al ejecutarse sobre la tarjeta inalámbrica en modo monitor, no se podía decodificar el tráfico generado; DLT IEEE802.11 127 como se aprecia en la Fig. 2.

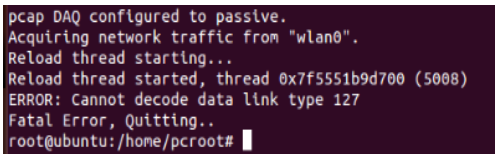


Fig.2. Error de lectura con la tarjeta inalámbrica en modo monitor en Snort

-Se ubica dos clientes con tarjetas inalámbricas con dirección MAC=70:F3:95:39:A4:97 cliente A, MAC= 00:21:6B:32:DB:C2 cliente B.

-Se sitúa la máquina atacante, con sistema operativo Backtrack 5 R3 [6], con dos tarjetas USB inalámbricas D-Link DWA125 A2 y Anera Adapter.

Las tarjetas utilizadas en esta evaluación permiten principalmente su configuración en modo monitor, y en el caso especial de Bactrack 5 R3 se utilizó dos tarjetas porque la D Link no funcionaba bien con Ettercap; entonces se optó por una adicional. En la tabla 3 se encuentra una descripción de las tajetas inalámbricas utilizadas.

Tabla.3. Características de las tarjetas inalámbricas USB para las pruebas

Tarjeta	**Características**
D-Link DWA125 ver. A2	Chip Ralink RT3070, potencia Tx 17dbm
D-Link DWA125 ver A3	Chip Ralink RT5370, potencia Tx 17dbm
Anera adapter 802.11 b/g/n	Chip Realtek RTL8192CU, antena externa de 2dbi

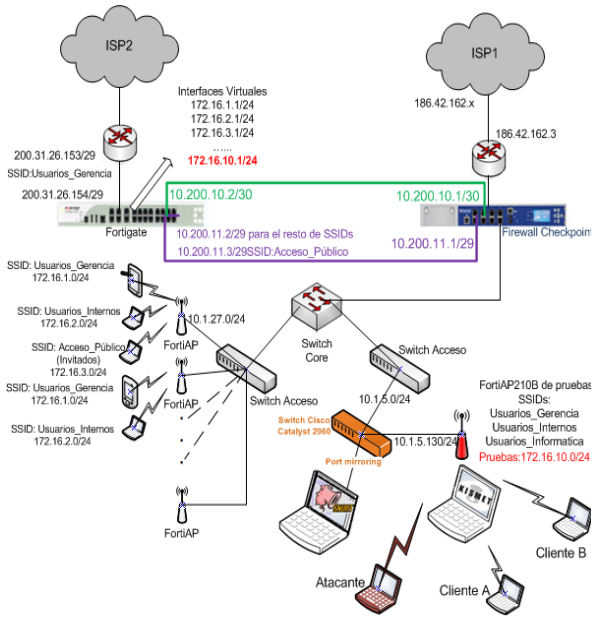


Fig.3. Topología de pruebas

El direccionamiento queda definido según las siguientes tablas:

Tabla.4. Direccionamiento IP del Fortigate

Direccionamiento IP del Fortigate	
Interfaz **Dirección/Máscara**	**Descripción**
Wan1 200.31.26.154/29	Salida hacia el internet de la red de Gerencia.
port1 10.200.11.2/29	Salida hacia el internet controlada por el firewall Checkpoint del resto de SSIDs.
port1 ***IP Secundaria*** 10.200.11.3/29	Salida hacia el internet controlada por el firewall Checkpoint para la red acceso_invitados
port2 10.200.10.2/30	Puerto de acceso a la red LAN, para los SSIDs que así lo necesiten.
Virtual10 172.16.10.1 / 24	Acceso a la WLAN de Pruebas.
Otras Interfaces virtuales (TotalSSID=11) 172.16.0.1- 172.16.0.9/24	Accesos a las diferentes WLANs configuradas según los perfiles y permisos necesarios solicitados; al fin de este proyecto existen 11 SSIDs.

Tabla.5. Direccionamiento IP del FortiAP de pruebas

Direccionamiento IP del FortiAP de pruebas	
Interfaz **Dirección/Máscara**	**Descripción**
Eth0 10.1.5.130/255.255.255.0	IP asignada en la red 10.1.5.0/24 a través de la cual se une a la infraestructura de la red de la organización
SSID Pruebas 172.16.10.0/255.255.255.0	SSID Pruebas
Otros SSID Usuarios _Gerencia 172.16.1.0/255.255.255.0 Usuarios_Informática 172.16.6.0/255.255.255.0 Usuarios_Internos 172.16.2.0/255.255.255.0	Otros SSIDs que también permiten el acceso autorizado el FortiAP de pruebas
Su Gateway en la red LAN	10.1.5.254
Su Fortigate configurado	10.200.10.2

VII. GENERACIÓN DE ATAQUES

En Backtrack existen herramientas de ataque hacia las redes inalámbricas, que se ejecutan a través de comandos realizados por el atacante, pero de manera especial existen herramientas con cómodas interfaces de usuario que facilitan el proceso de ataque; por ello se ha escogido las herramientas Fern WiFi Cracker y Ettercap.

Adicional en una WLAN lo que principalmente buscan los atacantes es acceso a la red para seguir escalando en privilegios y accesos, o interceptar información que es de su interés. Con obtener la clave se tiene acceso a la red y a los permisos que ella tenga definidos, con colocarse en la mitad de una comunicación se puede acceder a la información de intercambio de un cliente objetivo; para lograr estas metas Fern WiFi Cracker (crackeo de claves) y Ettercap (hombre en el medio a través de ARP Poisoning) encajan bien.

Los ataques detallados a continuación se realizaron tanto en ejecución de Snort como de Kismet.

- **Ataques con Fern Wi Fi Cracker**

Primero se ejecuta en el terminal de Backtrack airmon-ng e iwlist wlan (# de interfaz asignado) scan, el primero con objeto de verificar funcionamiento en modo monitor y el segundo con objeto de comprobar el alcance al objetivo, escaneando los SSIDs inalámbricos en el ambiente.

Fern WiFi Cracker al ejecutarse (ingresando al menú de WLAN Exploitation: *Applications/BackTrack/Exploitation Tools/Wireless Exploitation Tools/WLAN Exploitation*); presenta una ventana como se indica en la fig.4; en donde indica que se seleccione la interfaz atacante para colocarla en modo monitor y el inicio del escaneo.

Fig.4. Interfaz principal de Fern WiFi Cracker

La herramienta procede a escanear y una vez finalizado este proceso, indica al usuario un resumen de lo que ha logrado obtener de su sniffing en el ambiente. En la fig.5 muestra información de lo que consiguió en WLANs con WPA; resaltando el SSID objeto de pruebas.

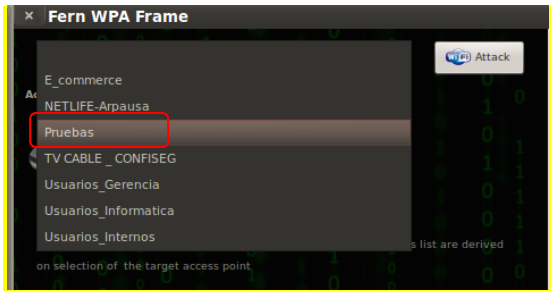


Fig.5. Lista de redes con WPA en Fern WiFi Cracker

Seleccionando el SSID de pruebas la herramienta despliega información detallada sobre el mismo y el proceso de ataques a seguir para conseguir su objetivo, de alcanzar la clave de acceso, fig.6:

a. Sondea el punto de acceso en busca de por lo menos un cliente conectado; caso contrario la herramienta no puede cumplir con los ataques.

b. Realiza una desautenticación al cliente (DoS DEAUTH) para proceder a capturar su handshake.

c. Comienza a intentar autenticarse con las posibles claves en el diccionario.

Fig.6. Proceso de ataque en Fern Wi Fi Cracker

Para el punto c mencionado anteriormente se desprende la necesidad de un diccionario; con el que se realizará el ataque; en este caso como Backtrack está bajo evaluación se usa un diccionario del mismo (*Fyle System/pentest/passwords/wordlists/rockyou.txt*).

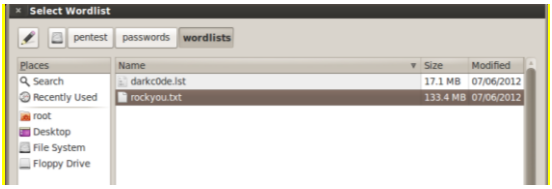


Fig.7.Selección del diccionario

Una vez que empieza el ataque la herramienta capturó al cliente B con MAC: 00:21:6B:32:DB:C2, fig.6, pero lastimosamente el diccionario brindado por Backtrack, no pudo localizar la clave que fue configurada, por no encontrarse dentro del mismo.

- **Ataques con ettercap**

Ettercap permitirá realizar los ataques Man in the Middle, a través de ARP Poisoning; como método para acceder a la información de un cliente objetivo, ó del sistema con el que se comunica.

En el directorio *Applications/Privilege Escalation/Protocol Analysis/Network sniffers/Ettercap-gtk* se puede acceder a ejecutar ettercap; en el cual se debe seleccionar la opción Uniffied Sniffing, porque el atacante se encuentra en el mismo medio donde fluye la comunicación.

Fig.8. Ventana Principal de ettercap

Ettercap pide el ingreso de la interfaz con la cual trabajará con los ataques; y sigue el siguiente proceso:

a . Al inicio de su ejecución comienza desplegando los equipos conectados en la WLAN en la "host list", luego se debe seleccionar de esta lista los objetivos del ataque, que son los clientes A y B; así el atacante podrá acceder a la información entre los clientes y estos no perderán conexión ni al internet, ni a sus permisos de perfil; porque no se ha intervenido en el AP; permaneciendo desapercibido por los clientes y el AP.

b. Se indica el tipo de ataque con el que se procederá a interceptar la comunicación; Mitm(man in the middle) y la técnica con lo cual lo logrará; en la presente evaluación se usó ARP Poisoning, debido a que el medio favorece este tipo de ataque, fig.9.

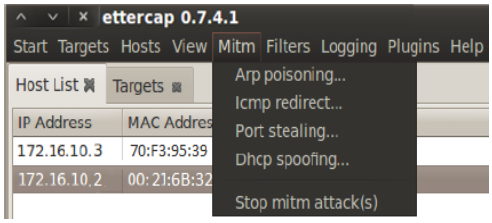
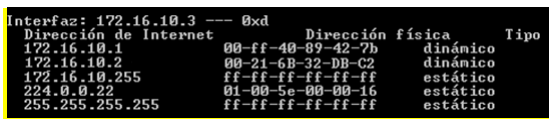
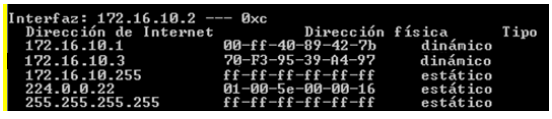


Fig.9. Selección de objetivos y tipo de Mitm

Por último se comprueba si fue efectivo el ataque revisando las tablas ARP de los clientes (comando *arp -a*) y como se puede ver en la fig.10. el cliente A (IP=172.16.10.2, MAC=70:F3:95:39:A4:97) y B (IP=172.16.10.3, MAC=00:21:6B:32:DB:C2); tienen respectivamente la MAC del atacante (48:02:2A:6F:FE:B5); lo que prueba que se ha logrado envenenar las tablas.





(a)

```
Interfaz: 172.16.10.3 --- 0xd
  Dirección de Internet         Dirección física      Tipo
  172.16.10.1           00-ff-40-89-42-7b     dinámico
  172.16.10.2           48-02-2A-6F-FE-B5     dinámico
  172.16.10.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático
```

```
Interfaz: 172.16.10.2 --- 0xc
  Dirección de Internet         Dirección física      Tipo
  172.16.10.1           00-ff-40-89-42-7b     dinámico
  172.16.10.3           48-02-2A-6F-FE-B5     dinámico
  172.16.10.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático
```

(b)

Fig.10. (a) Tabla ARP Cliente A y B antes del ataque MITM (b) Tablas ARP Cliente Ay B después del ataque MITM

VIII. RESULTADOS OBTENIDOS

A. Resultados obtenidos en Snort

Resultados: Al ingresar a la página de snortreport se puede apreciar que no generó ningún tipo de alerta sobre los ataques que tuvieron efecto.

Análisis: No se pudo obtener resultados a través de Snort, porque su ubicación dificultó la detección de ataques; puesto que no estaba en el medio donde ocurrían las anomalías producidas por Fern Wi Fi Cracker. Por el lado de los ataques con ettercap, como se lo realizó entre clientes tampoco hubo la activación de alertas por el hecho de que este tráfico nunca pasó por la comunicación FortiAP-Fortigate.

Fig.11. Despliegue de resultados de Snortreport

B. Resultados obtenidos en Kismet

- **Frente a los ataques con Fern Wi Fi Cracker**

Gracias a los archivos .pcapdump generado por Kismet y a través de un despliegue de información en Wireshark, se tomó un archivo de 11.7 Mb denominado kismet-2013-12-04-09-59-09-1; en el que se puede apreciar: que existió un 17,85% de tráfico perteneciente al SSID Pruebas, con una importante cantidad de tramas de desautenticación (303) que resalta de los demás SSIDs, fig.12; en la fig.13 se despliega la información sobre el tráfico en el SSID de pruebas; así resulta un importante tráfico que corresponde al 78,54% a la MAC del FortiAP, 20,14% MAC del BSSID, 84,66% MAC del cliente B atacado. Porcentajes con referencia tanto a las instancias en las que tomaron el papel de origen ó destino.

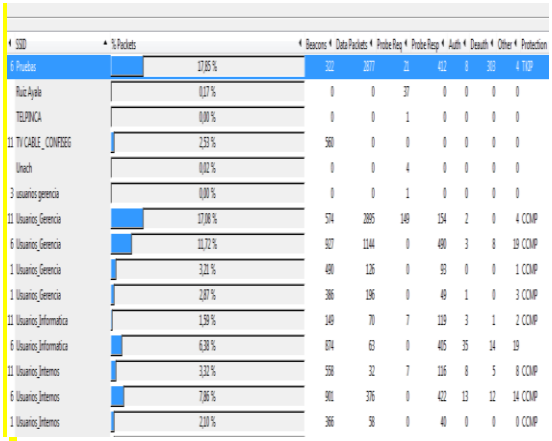


Fig.12. Porcentajes de tráfico capturado

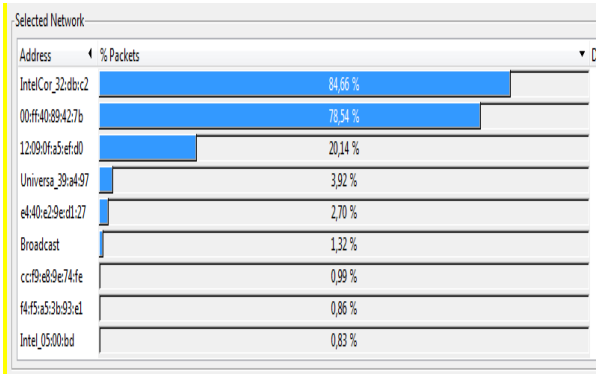


Fig.13. Porcentajes de tráfico en el SSID Pruebas

También generó alertas que se almacenaron en el archivo .alert en el cual se generaron en total 11 alertas correspondiente al tráfico mencionado anteriormente, de las cuales 5 corresponden al SSID de pruebas, que corresponden al tipo DEAUTHFLOOD, PROBENOJOIN Y ADHOCCONFLICT.

Análisis: De los datos obtenidos gracias a Kismet durante los ataques con Fern WiFi Cracker, principalmente de las alarmas se determina:

-La primera alerta generada definida de tipo PROBENOJOIN se generó debido a que se generó varias solicitudes probe, que corresponden a la ejecución del *iwlist*, en las pruebas de las tarjetas de ataque. Por lo tanto corresponde al primer verdadero positivo en su operación.

-La segunda y última alerta de tipo DEAUTHFLOOD corresponde a la desautenticación generada hacia el cliente B por parte Wi Fi Cracker; definiendo así su segundo verdadero positivo. Gracias a la gráfica de flujo de Wireshark se ilustra de mejor manera la acción del ataque, tanto la desautenticación generada con el supuesto origen el BSSID (fig.14) y el cliente(fig.15); para así evitar que intervenga en los intentos de autenticación.

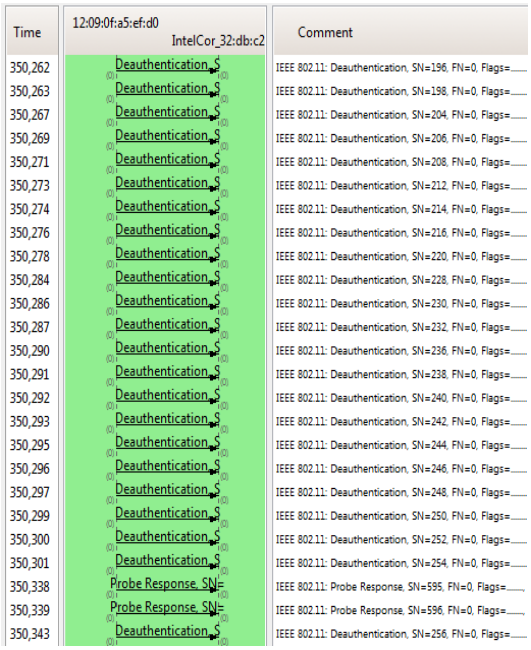


Fig.14 Desautenticación BSSID=>Cliente B

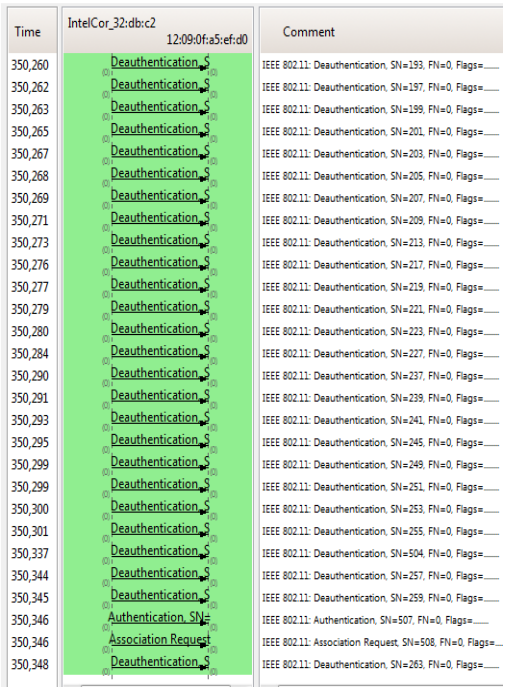


Fig.15. Desautenticación Cliente B=>BSSID

-Cuando logra desautenticar al cliente comienza el ataque de diccionario; mantiene desautenticado al cliente B y envía solicitudes de autenticación, en la fig.16 se puede apreciar el flujo de tramas de autenticación.

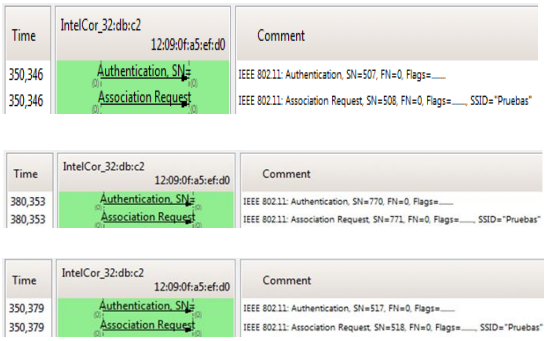


Fig.16. Flujo de tramas de autenticación (ataque diccionario)

-Por último se emitió dos alertas del tipo ADHOCCONFLICT, a través de Wireshark se puede determinar en el tráfico tramas beacons y probe responses con la MAC del AP, pero al mismo tiempo con los campos To DS y From DS con el valor de 0; que indica una comunicación ADHOC, que más bien corresponde al comportamiento normal que existe en la comunicación entre el FortiAP y el Fortigate, quien es el que realmente da acceso al DS; por ello caen dentro de los falsos positivos.

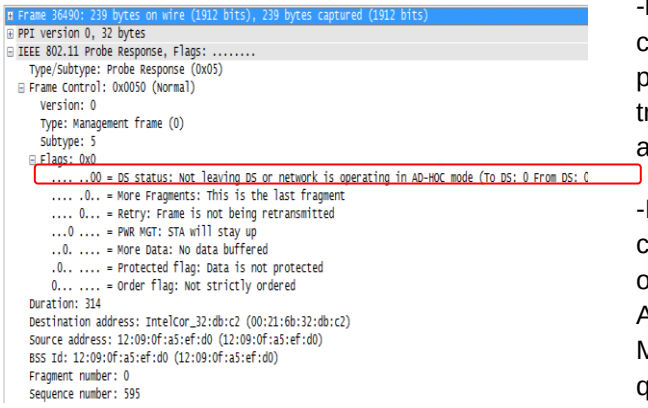


Fig.17. ejemplo de tramas que generan el ADHCOCONFLICT

- **Frente a los ataques con Ettercap**

Lastimosamente no existió evidencia ni en la captura de tráfico ni alertas acerca del ataque provocado por Ettercap; adicional sólo generó alertas con respecto a otros SSIDs del tipo ADHOCCONFLICT que se debe al comportamiento normal Fortigate-FortiAP explicado anteriormente.

IX. DETERMINACIÓN DE CARACTERÍSTICAS DE RESPUESTA DE LOS IDSs

- **Snort**

-Es una herramienta que se ha especializado más en ataques a las capas superiores, que en el campo de las redes inalámbricas después del análisis queda claramente definido una calidad de respuesta pésimo (no generó ninguna alerta).

- **Kismet**

-De un total de 15 alertas generadas tanto en los ataques con Fern WiFi Cracker y ettercap, 5 correspondieron al SSID de pruebas; después del análisis quedó al descubierto 3 alertas como verdaderos positivos (DEAUTHFLOOD, PROBENOJOIN) y 2 alertas como falsos positivos (ADHOCCOFLICT) lo que da un total del 60% de verdaderos positivos y un 40 % de falsas alertas, porcentajes aceptables de respuesta.

-kismet aporta a más de las alertas con capturas de tráfico .pcapdump; en donde se puede correlacionar el tiempo indicado en las tramas capturadas y la hora indicada en las alertas en el archivo .alert.

-Las alertas tienen un formato claro y muy conciso de lo que posiblemente está ocurriendo (Hora, Día, Año, BSSID, Tipo de Alerta, Dirección MAC Destino, Dirección MAC Fuente y una corta descripción de lo que supuestamente puede estar sucediendo).

X. MEDIDAS MÍNIMAS DE SEGURIDAD WIFI SEGÚN LOS RESULTADOS OBTENIDOS

Tabla.5. Recomendaciones mínimas de seguridad

Recomendaciones	
Clientes	Tener un antivirus y firewall instalados y actualizados.
	Tener con contraseña el inicio de sesión al equipo, evitar el acceso ilegítimo a su información como sus contraseñas a sus SSIDs.
	Reportar intermitencias, lentitud o desconexiones al administrador de red.
	No tener anotado la clave en lugares visibles.
AP	Debe ubicarse en un sitio donde no se encuentre con algún tipo de interferencia.
	Debe ubicarse en un lugar fuera del alcance de usuarios o extraños a la organización.
Controlador Inalámbrico	Configuración conforme a políticas de seguridad y acceso.
	En WPA+TKIP clave mínima de 10 a 15 caracteres alfanuméricos.
	Número máximo de intentos de autenticación y cambio constante de la clave compartida.
	Implementar filtrado MAC, evitando DHCP, ó de preferencia en organizaciones grandes como la de prueba un servidor RADIUS

XI. CONCLUSIONES

- Las técnicas de ataque enfocadas hacia las redes inalámbricas, apuntan sus esfuerzos principalmente a las capas física y enlace de datos, porque las circunstancias favorecen este hecho; los atacantes no van más allá en las capas superiores de la arquitectura de red, si pueden aprovechar capas inferiores frágiles.

-Los benchmarks son medios importantes de evaluación de la seguridad informática; permitiendo seguir un debido proceso hacia la obtención de resultados.

-Backtrack posee un importante arsenal para evaluar redes inalámbricas, incluso cómodas herramientas con interfaz gráfica que facilitan aún más el accionar de los atacantes; tal es el caso de Fern Wi Fi Cracker y ettercap.

- Fern WiFi Cracker está atado a la utilización de un buen diccionario para conseguir vulnerar WPA y WPA2; por su lado kismet generó alertas casi en el acto sobre casi todos ataques generados con Fern, pero lastimosamente no pudo definir alertas al resto de ataques generados (ettercap y ataques de diccionario).

-Snort lamentablemente no generó reacción alguna frente a los ataques, por su falta de decodificadores que le imposibilitaron estar en el medio, en el cual se generaron los ataques a Wi Fi.

-Kismet obtuvo un 60% de verdaderos positivos y un 40% de falsas alarmas que representan porcentajes aceptables de detección.

-Es recomendable trabajar con tarjetas inalámbricas que permitan la inhabilitación del salto de canal, para poder enfocar el IDS aun sólo SSID y evitar como en el presente escenario de pruebas se analice el tráfico y emita alarmas de otros SSIDs.

-Se recomienda integrar la funcionalidad de Snort y kismet, a través de las interfaces virtuales TUN/TAP presentes en Kismet, que permitan a kismet aumentar su detección a capas superiores y a Snort en el área de las redes inalámbricas Wi Fi.

XII. REFERENCIAS

[1] IEEE802.11 (2012**).** Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. [En línea]. Disponible en*:*

http://standards.ieee.org/getieee802/download/802.11-2012.pdf [2013, 01 de febrero].

[2] Hsiao, H., Mohsen, G. (2006). Next Generation Wireless Systems and Networks. Estados Unidos: John Wiley & Sons. Ltd.

[3] Sourcefire Team, (2013). Snort. Disponible en: http://www.snort.org [2013, 01 de noviembre].

[4] Roesch, M., Green, C. y Sourcefire, Inc. (2013). Snort's User Guide 2.9.5. [En línea]. Disponible en: http://www.snort.org [2013, 01 de noviembre].

[5] Kershaw, M. (2011). Kismet. [En línea]. *Disponible en:* http://www.kismetwireless.net/documentation.shtml [2013, 15 de octubre].

[6] Back|track-linux.org. (2013). BackTrack Linux-Penetration Testing Distribution. [En línea]. Disponible en: http://www.backtrack-linux.org/ [2013, 31 de noviembre].

XIII. BIOGRAFÍAS

- **Ana M. Yaccchirema E.**

Nació el 23 de Septiembre de 1989. Se graduó como bachiller especialidad físico matemático en el Colegio Nacional "Juan de Salinas" Sangolquí-Ecuador, donde obtuvo la distinción de Mejor Graduado período 2006-2007. Entre el 2007 y 2012 estudió la carrera de Ingeniería Electrónica, Redes y Comunicación de Datos en la Universidad de las Fuerzas Armadas ESPE, realizó su proyecto de grado sobre "Análisis de los Sistemas de Ataque y Protección en Redes Inalámbricas Wi Fi, bajo el Sistema Operativo Linux".

- **Darwin O. Alulema F.**

Nació el 28 de Septiembre de 1982, obtuvo el título de Ing. Electrónico en la Universidad de las Fuerzas Armadas ESPE en el 2005, el de Master en Teleinformática y Redes de Computadoras en la UTE en el 2008, sus áreas de interés son la programación de Tecnologías de Software para Electrónica empleando Java.

- **Darwin L. Aguilar S.**

Obtuvo su grado de bachiller en la Unidad Educativa Eduardo Valdivieso en 1993, el de Ing. Electrónico y Telecomunicaciones en la Universidad de las Fuerzas Armadas ESPE en el 2001, un diplomado en Gestión de Enseñanza Universitaria, Magister en Redes de Comunicación. Sus áreas de interés son las redes inalámbricas, network on the chip, televisión digital y la telefonía IP.