Universidad Central "Marta Abreu" de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

Propuesta de Configuración de Seguridad en la Red WiFi del Proveedor de Servicios ETECSA en Villa Clara

Tesis presentada en opción al Título Académico de Máster en Telemática.

Maestría de Telemática

Autor: *Ing. Anabel Sánchez Arcia*

Tutor: *MsC. Ing. Manuel Oliver Domínguez*

Santa Clara

2016

Hago constar que el presente trabajo fue realizado en la Universidad Central "Marta Abreu" de las Villas como parte de la culminación de los estudios de Maestría en Telemática autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

_____
Firma del Autor

Los abajo firmantes, certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

_____
Firma del Tutor

_____
Firma del Jefe de Dpto.
Donde se defiende el trabajo

_____
Firma del Responsable de
Información Científico-Técnica

No hay perfección sin esfuerzo. Los mediocres jamás cosechan rosas por temor a las espinas.

José Ingenieros.

A mis padres que con su amor, esfuerzo y dedicación han ayudado a formarme como profesional y además por ser las personas que más quiero en el mundo.

A mis abuelos por depositar en mí toda su confianza y darme todo su cariño.

A mi tía, a mi primo Eriel, a su esposa Ludaymy y a mi sobrino Julito.

A toda mi familia.

A mi novio Erick que me ha apoyado para que pudiera dedicarle tiempo a mi vida profesional.

A todas mis amigas y amigos.

A todas aquellas personas que de una forma u otra tuvieron que ver con mi formación durante estos años.

A todos, Gracias.

A mi familia.

Resumen

En el presente trabajo se propone una arquitectura y configuración segura a la Red WiFi de la Empresa de Telecomunicaciones de Cuba ETECSA, la cual brinda el servicio de conectividad a Internet en Villa Clara. Para lograr este diseño de red se analizan los aspectos teóricos más importantes relacionados con las Intrusiones de Seguridad Informática en redes inalámbricas a nivel mundial, y, en función de las principales vulnerabilidades que presenta esta red se realiza la propuesta.

En el trabajo se describen los aspectos más relevantes de los distintos estándares, métodos y configuraciones de seguridad de las redes inalámbricas WiFi, examinando su funcionamiento, ventajas e inconvenientes, niveles de seguridad ofrecidos, implementación y tendencias. Se especifican los principales entornos donde son aplicables, las soluciones más importantes aportadas y se exponen las vulnerabilidades de cada una de estos diseños.

Se hace un estudio de las debilidades que presenta la red WiFi de Etecsa en Villa Clara, con las cuales se puede inhabilitar el funcionamiento del servicio, provocar que el sistema no responda como es debido ante alguna intrusión o aprovecharse de estas debilidades para evitar pagar el servicio. Se realiza además un análisis de los principales ataques a estas redes y como evitar los mismos.

Por lo que se propone una arquitectura de red WiFi utilizando el estándar 802.11i que proporciona seguridad al sistema y a los clientes y que elimina las vulnerabilidades de la red actual. Además se propone insertar un Sistema de Detección de Intrusos con la utilización de la herramienta Alien Vault OSSIM, la cual es capaz de alertar en tiempo real los eventos anómalos que ocurran en la red. Comprobando así que la configuración de seguridad propuesta es la más conveniente por las propias características que presenta esta red y por el tipo de servicio que se brinda. Este trabajo se puede tomar como referencia para la implementación de redes WiFi en otras ciudades.

Índice

Introducción

La seguridad en redes de computadoras ha pasado de ser una simple cuestión de estudio teórico a una difícil tarea diaria que consume tiempo y recursos en la actualidad. Las redes de computadoras ganan terreno y su seguridad se convierte en una tarea de todos los profesionales del mundo de la informática.

Existen varias tecnologías que brindan acceso a Internet, una de las más usadas es la inalámbrica debido lo rápida de su la instalación y que permiten una alta movilidad. En los últimos años esta tecnología ha evolucionado mucho por su facilidad de implementación, su bajo costo (en relación a las redes cableadas como las tecnologías xDSL (*Digital Subscriber Line*)) al permitir un gran margen de movimiento al cliente.

En las redes inalámbricas, la seguridad juega un rol mucho más decisivo, debido a la exposición del medio de transmisión, por lo que se necesitan implementar mecanismos que garanticen la autenticidad, la confidencialidad de la información y la estabilidad del servicio ofrecido.

En las redes inalámbricas utilizadas para brindar servicio de conectividad a Internet es muy importante la estabilidad, a partir de esta consideración, los clientes escogerán o no esta vía de conexión, las pérdidas económicas por no tener esto presente pueden ser numerosas. De ahí la importancia de contar con mecanismos eficientes de seguridad que el proveedor de servicios Etecsa pueda implementar para poner en explotación este tipo de redes.

El servicio de conectividad a Internet por medio de la red de acceso WiFi que brinda la Empresa de Telecomunicaciones de Cuba tiene ciertas características; cualquier dispositivo con la norma 802.11 debe conectarse a la red, los dispositivos que se van a conectar a estas redes son propiedad del cliente por lo que constantemente estos pueden cambiar, la forma de conexión debe ser sencilla para el cliente, por lo que no se pueden implementar medidas de seguridad que impliquen configuraciones complejas en los equipos terminales, la forma de cobro del servicio es por tiempo de conectividad, ya sea por tarjetas o por cuentas pre pagadas, estas tarjetas o cuentas deben poder utilizarse desde cualquier punto de

conectividad de la empresa de Etecsa ya sea en salas de navegación o en la propia red inalámbrica WiFi.

Los mecanismos de seguridad que se pueden aplicar para proteger redes inalámbricas varían según el nivel de seguridad requerido, el tipo de servicio deseado y el coste de gestión y mantenimiento de las soluciones adoptadas. Los organismos normativos (IEEE, IETF) han desarrollado protocolos de seguridad para proteger redes inalámbricas, los más utilizados son WEP, WPA, WPA2 e IEEE 802.1x, dichos protocolos se encuentran en la capa de enlace del modelo OSI, en dicha capa se encuentra los protocolos que diferencian una red inalámbrica WiFi del resto de las redes. A estas redes inalámbricas se le pueden implementar el resto de los protocolos de seguridad igual que a las redes cableadas, en el nivel de red se pueden utilizar soluciones VPN e IPsec, en la capa de transporte SSL/TLS y en el nivel de aplicación SSH y HTTPS. Existen además otros tipos de herramientas que se pueden utilizar para brindar seguridad como son los Firewall y los IDS (Sistemas de Detección de Intrusos).

El principal problema encontrado es precisamente la carencia de una plataforma para la detección temprana de anomalías en la red de manera que se pueda detectar y contener a tiempo ataques de negación de servicio, envenenamiento de la red, propagación de virus, robo de identidades, entre otros usos indebidos.

Existe una gran variedad de estándares de protocolos que implementan en alguna medida seguridad en redes, también se cuenta con numerosas herramientas y aplicaciones para estos fines. Diseñar una red inalámbrica segura solo puede ser posible a través de un análisis detallado de los distintos protocolos, herramientas y aplicaciones, además del funcionamiento de los principales servicios y sus vulnerabilidades.

Para la solución de este problema surgen las siguientes interrogantes:

- ¿Cuáles son los principales estándares y protocolos de seguridad en redes inalámbricas?

- ¿Cuáles son las vulnerabilidades existentes en la red inalámbrica desplegada actualmente?
- ¿Cuáles son las principales plataformas de detección de anomalías existentes en el mercado?
- ¿Qué características deberá tener la configuración de seguridad de la red inalámbrica para brindar servicio de conectividad a Internet?
- ¿Qué beneficios brindará la configuración de seguridad propuesta para dicha red?

Por ello, el objetivo general es Proponer una configuración de seguridad a la red inalámbrica WiFi de la Empresa de Telecomunicaciones de Cuba Etecsa en Villa Clara, para lo cual se han propuesto las siguientes tareas específicas:

- Estudio de los principales estándares, métodos y herramientas que brindan seguridad en redes inalámbricas.
- Estudio de las principales plataformas de detección de anomalías que existen en el mercado.
- Análisis de las principales vulnerabilidades de la red WiFi que ofrece servicio de conectividad a Internet.
- Elaboración de una propuesta de seguridad que proporcione integridad y confidencialidad de la información que viaje por esta red.
- Elaboración de una propuesta de seguridad que detecte las anomalías en esta red.

Este trabajo se ha estructurado en: introducción, desarrollo, compuesto de tres capítulos, conclusiones, recomendaciones, referencias bibliográficas, glosario de términos y anexos. A continuación se describe brevemente el contenido de los diferentes capítulos.

Capítulo1: Análisis y Evaluación de las principales soluciones de seguridad.

Este capítulo aborda el estado del arte de los estándares y mecanismos de seguridad de las redes inalámbricas y puntualiza algunas herramientas de ataques a estas redes que atentan contra la seguridad de las mismas. Se hace énfasis en el análisis y evaluación de las principales configuraciones, diseños y métodos de seguridad a este tipo de redes, sus

ventajas y desventajas, así como los niveles de seguridad ofrecidos por cada uno. Además se evalúan distintas herramientas de detección y aviso de posibles ataques a la red.

Capítulo2: Características de la Red WiFi de Etecsa en Villa Clara.

En este capítulo se describirá la arquitectura y funcionamiento de la red WiFi de Etecsa, los mapas de cobertura de dicha red, la cantidad de usuarios que se conectan, la forma de cobro del servicio, la accesibilidad a la red y el equipamiento que la soporta. Se identificarán las vulnerabilidades de seguridad que presenta la red y la necesidad de una herramienta capaz de alertar ante un evento anómalo en el comportamiento de la misma.

Capítulo3: Evaluación y análisis de la arquitectura de seguridad propuesta para la red WiFi de Etecsa.

En este capítulo se realizarán pruebas que demuestran las vulnerabilidades de la red WiFi de Etecsa. Para evitar la ocurrencia de acciones que exploten estas debilidades se propone un diseño que garantice una mayor seguridad a la red y a los clientes. En el capítulo se describe la arquitectura escogida especificando cada una de las ventajas alcanzadas. Además se propone una herramienta que permite detectar, avisar y actuar ante ataques o intentos de intrusión en la red.

Capítulo 1 Análisis y Evaluación de las principales soluciones de seguridad.

1.1 Introducción

Con el desarrollo de Internet y el aumento del número de clientes potenciales que esta conecta son cada vez son más altos los volúmenes de información que se manejan como resultado de operaciones de distintos países que en muchas ocasiones intercambian datos privados entre sí. Esto, unido a la expansión de la conectividad, hace que la seguridad se convierta en una tarea de todos los profesionales del mundo de la informática y las comunicaciones.

Una de las tecnologías más usadas para acceder a Internet es la inalámbrica. Durante los últimos años su evolución no ha cesado. La facilidad de implementación y el bajo costo en relación a las redes cableadas ha impulsado el incremento en la demanda de redes inalámbricas por parte de los usuarios del sector tanto privado como comercial.

Entre las redes de acceso más utilizadas se encuentran las redes de alcance local o WLAN, dentro de estas redes locales un tipo comúnmente usado son las redes WiFi, presentadas comercialmente como *Wireless Fidelity*[1]. En estos momentos la mayoría de los equipos terminales (*laptops, tables, smartphone*) vienen con una tarjeta integrada WiFi. Existen además varios dispositivos que permiten a las PC de mesa que éstas puedan tener una tarjeta de red WiFi, lo que ha ayudado en gran medida al crecimiento y expansión en el uso de estas redes en todo el mundo.

La seguridad siempre ha sido uno de los factores más delicados a tomar en cuenta al momento de diseñar un sistema de comunicaciones y más aún cuando se ofrece un servicio público. Las redes WiFi son un caso muy particular porque los datos viajan a través de un medio totalmente inseguro, lo que da origen a la necesidad de crear un sistema de seguridad específico para este tipo de tecnología. Debido a lo inseguro del medio de transmisión, se necesitan implementar mecanismos que garanticen la autenticidad y confidencialidad de la información, y la estabilidad del servicio que se brinda por estas redes.

En la actualidad la mayoría de redes WiFi no cuentan con un sistema de autentificación seguro que garantice que la información no pueda ser accedida ni modificada por usuarios no autorizados[2]. Cada vez aparecen herramientas de ataque más sofisticadas que atentan contra el buen funcionamiento de la red, ya sea generando ataques de negación de servicio o evitando pagar por el uso del mismo, por lo que es importante contar con un sistema de seguridad capaz de detectar, informar y detener amenazas o intrusión a los recursos de la red por usuarios no autorizados, y, además proteger la información de los clientes que circula en la red[3].

En las redes inalámbricas WiFi utilizadas para brindar servicio de conectividad a Internet es muy importante la estabilidad de las mismas, a partir de esta consideración, los clientes escogerán o no esta vía de conectividad, las pérdidas económicas por este concepto pueden ser numerosas[4]. De ahí la importancia de mecanismos eficientes de seguridad que el proveedor de servicios necesita implementar para poner en explotación este tipo de redes.

Los mecanismos de seguridad que se pueden aplicar para proteger redes inalámbricas varían según el nivel de seguridad requerido, el tipo de servicio deseado y el coste de gestión y mantenimiento de las soluciones adoptadas.

En este capítulo se abordará lo referente a los distintos métodos de seguridad específicos para redes inalámbricas, en los que se determinarán sus ventajas y vulnerabilidades. Se estudiarán herramientas que permiten detectar y contener a tiempo ataques y eventos anómalos en la red. Además se realizará una revisión actual de los principales ataques a los que pueden ser sometidas las redes inalámbricas WiFi.

1.2 Métodos de Seguridad

El canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse peligroso. Cualquiera podría estar escuchando la información transmitida (ataques pasivos), inyectando nuevos paquetes o modificando los ya existentes (ataques activos)[1]. Las mismas precauciones que se tiene para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

Para dar solución a estos problemas han surgido varios mecanismos de seguridad que se verán a continuación.

1.2.1 Filtrado de direcciones MAC

El filtrado de direcciones MAC consiste en suministrar a cada punto de acceso un listado con las direcciones de los equipos que están autorizados a conectarse. La ventaja principal es por tanto que ningún equipo, como por ejemplo un equipo malicioso, que no esté incluido en la lista de direcciones no podrá conectarse[1][5][6].

Este método de control de acceso está muy extendido por su facilidad de configuración. Se basa en realizar dicho control mediante la comprobación de la dirección MAC de nivel 2 o nivel de trama. Su implantación es muy sencilla, ya que sólo se necesita declarar en el punto de acceso o en un servidor aparte las direcciones MAC que están autorizadas para conectarse a la WLAN (*Wireless Local Area Network*) [6].

Este sistema de autenticación tiene varios problemas. El primero es que si los usuarios no son fijos o hay usuarios itinerantes, el alta y la baja de las direcciones provocan carga de gestión y por consiguiente peligro de dejar alguna entrada de la lista "olvidada". Otro de los problemas es lo fácil que resulta cambiar la dirección MAC de un dispositivo, lo que hace que resulte muy sencillo sustituirla por una válida, y por tanto, que este método de autenticación resulte muy vulnerable. Uno de los métodos de ataque más común consiste en escuchar el tráfico que pasa por la WLAN y guardar direcciones MAC válidas, para que en el momento que alguna de ellas quede libre, sustituir ésta por la dirección MAC del dispositivo cliente. De todo esto se deduce que este método de autenticación resulta ineficiente[7].

1.2.2 Protocolo de seguridad WEP

WEP (*Wired Equivalente Privacy*) es el algoritmo opcional de seguridad para ofrecer protección a las redes inalámbricas incluido en la primera versión del IEEE 802.11[1]. El estándar 802.11 ofrece mecanismos de seguridad mediante procesos de autenticación y de cifrado[8]. En el modo *Ad Hoc* la autenticación puede realizarse mediante un sistema

abierto o mediante un sistema de clave compartida. Un punto de acceso que reciba una petición podrá conceder autorización a cualquier estación o solo a aquellas que estén permitidas. Por lo que en un sistema de clave compartida tan solo aquellas estaciones que posean una llave cifrada serán autenticadas[1][5][9][10].

El algoritmo de encriptación de WEP es el siguiente (Fig. 1.1):

1. Se calcula un CRC (Control de Redundancia Cíclica) de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, *Integrity Check Value*).
2. Se concatena la clave secreta a continuación del IV (*Initial Vector*) formando el *Seed*.
3. El PRNG (*Pseudo-Random Number Generator*) de RC4 genera una secuencia de caracteres pseudos aleatorios (*keystream*), a partir del *Seed*, de la misma longitud que los bits obtenidos en el punto 1.
4. Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.
5. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos de la trama IEEE 802.11. El algoritmo para descifrar es similar al anterior.

Debido a que el otro extremo conocerá el IV y la clave secreta, tendrá entonces el *Seed* y con ello podrá generar el *keystream*. Realizando el XOR entre los datos recibidos y el *keystream* se obtendrá el mensaje sin cifrar (datos y CRC-32)[11]. A continuación se comprobara que el CRC-32 es correcto.

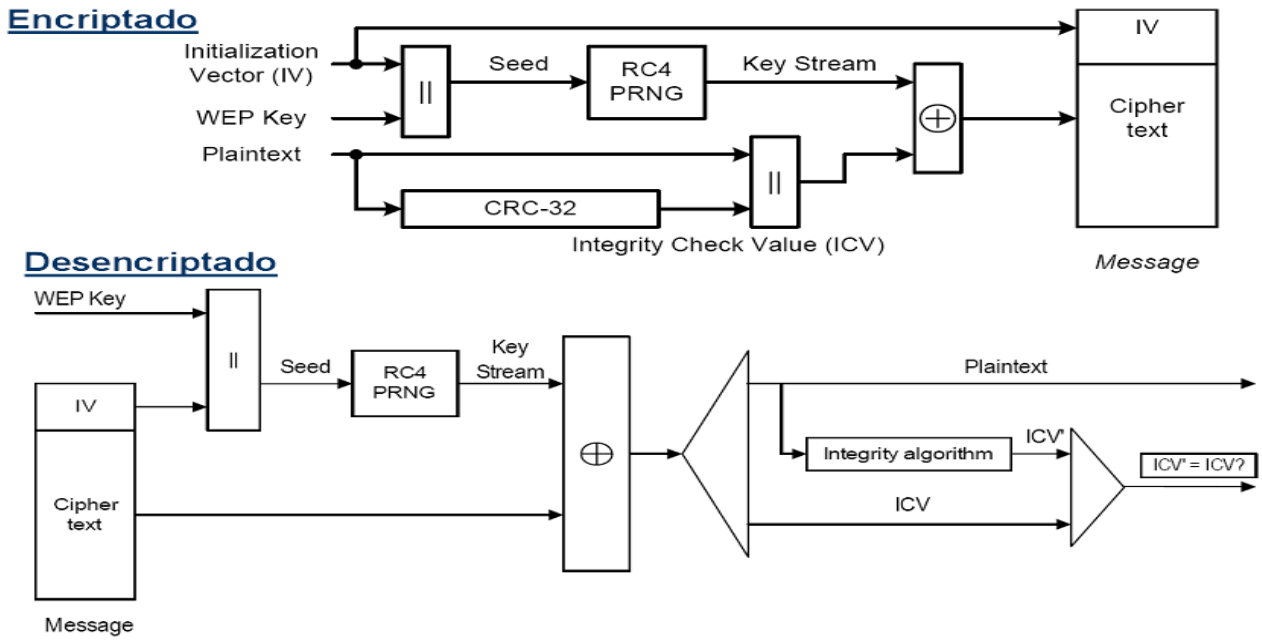


Fig. 1.1 Proceso de encriptado y desencriptado del protocolo WEP.

Este esquema de encriptación fue incluido en el estándar 802.11 y desde entonces ha sido ampliamente criticado, debido a sus más que demostradas debilidades[7]. Está basado en clave simétrica, por lo que tanto el cliente como la estación base deben conocer la clave a utilizar. El tamaño de ésta puede ser de 40 ó 104 bits, y se completa con un vector de inicialización de 24 bits. Precisamente, este corto vector ha sido uno de los principales puntos débiles de este esquema. La encriptación se basa en el algoritmo RC4, y utiliza un algoritmo de integridad CRC32 que genera un ICV independiente de la clave utilizada, lo que también ha ocasionado vulnerabilidades a nivel de seguridad[1].

El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un incremento en las tareas de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de las ocasiones que la clave se cambie poco o nunca.

El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Como el IV viaja en cada trama es sencillo de interceptar por un posible atacante, siendo esto otra vulnerabilidad del sistema[1][12].

1.2.3 Portal WEB Cautivo

Este sistema de control de acceso necesita un servidor que realice el control de la conexión al exterior. Con este método de autenticación, el cliente consigue conectarse a la red WiFi sin problemas, e incluso se le asigna una IP, pero sin capacidad de comunicarse fuera del entorno que se haya previamente definido[4]. Cuando el cliente intenta establecer comunicación con una página Web externa, automáticamente es redirigido a un portal cautivo en el cual puede autenticarse. Una vez hecho, ya sea con un simple usuario/clave o previo pago de una tarjeta de conexión o incluso con una tarjeta de crédito, el usuario consigue conectividad a Internet durante el tiempo establecido[13].

Esto se debe a que el navegador es una herramienta muy extendida, la mayoría de dispositivos con acceso WiFi tienen un navegador, y su utilización resulta muy natural para los usuarios, permitiendo así mismo el pago del servicio (conexión a Internet) de una manera fácil. La arquitectura del sistema está formada por los punto de acceso, un sistema de acceso que controla las conexiones al exterior, y un portal Web para poder autenticar a los usuarios (Fig. 1.2). Este portal puede estar situado en el mismo dispositivo que controla las conexiones o puede instalarse en un servidor Web aparte. En todos los sistemas en los que hay una fase de comprobación de credenciales (acceso vía Web, EAP-TTLS,...) hay un servidor de autenticación que bien chequea dichas credenciales contra alguna base centralizada de usuarios o bien delega la autenticación a un segundo mecanismo con chequeo de credenciales (por ejemplo un servidor POP de correo).

Como desventaja de este sistema de autenticación se tiene que la comunicación va sin ningún tipo de encriptación por lo que es susceptible de ser escuchada por cualquier estación en el alcance de la WiFi, de ahí que se recomiende el complementar este sistema de acceso con algún sistema que asegure el contenido de la comunicación como son IPSec, SSL, SSH, etc[5][7].

Fig. 1.2. Sistema de Autenticación Portal Cautivo.

1.2.4 802.1X

Es un estándar de control de acceso al medio, con lo que a diferencia de otros sistemas, como el del portal cautivo, en este caso el cliente no tiene una conexión efectiva con acceso al medio hasta que no se haya autenticado satisfactoriamente[1][13][14].

1.4.1 Arquitectura de 802.1x

La arquitectura de 802.1x está relacionada con tres elementos fundamentalmente (Fig.1.3):

1.) El cliente o suplicante 802.1x. Este es un terminal que desea usar los recursos ofrecidos por una red de comunicaciones.

2.) El autenticador o controlador. Este sistema controla los puertos para acceder a la red. Este puede ser un switch en una red cableada o un punto de acceso en una red inalámbrica. El flujo de datos del cliente 802.1x es dividido en dos clases de tramas:

- La trama usada por EAP (*Extensible Authentication Protocol*)[15][16].
- El resto de las tramas son bloqueadas cuando el Puerto está en el estado “no autorizado”. Si exitosamente en el proceso de autenticación el puerto pasa al

estado "autenticado" entonces todas las tramas pasan libremente, significando acceso a los usuarios a todos los servicios[1].

3.) El servidor de autenticación, típicamente RADIUS (*Remote Authentication Dial-In User Service*)[17]. Este es el responsable de realizar el proceso de autenticación con el cliente 802.1x[18]. El autenticador tiene dos puertos: un puerto no controlado el cual no hace control de tráfico, y un puerto controlado que permite (o no) pasar paquetes de usuarios autenticados.

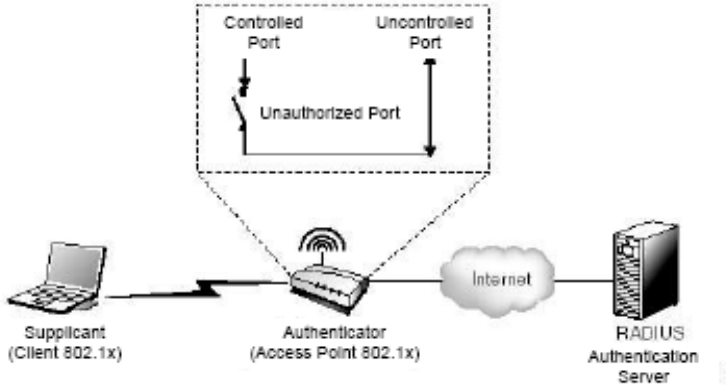


Fig. 1.3.Arquitectura de 802.1x.

1.4.2 Autenticación por Puerto

El estándar 802.1x define un control de acceso a la red basado en puertos. Esta función es para autenticar y autorizar equipos sujetados de la red local. En las redes inalámbricas IEEE 802.11, un puerto es una asociación entre una estación y un punto de acceso. El puerto controlado se comporta como un switch con dos estados. En el estado "no autorizado", solamente las tramas dedicadas a la autenticación EAP no son bloqueadas. En el estado "autorizado", los flujos de información pasan libremente[1].

El estándar 802.1x define las técnicas de encapsulación usadas para transportar paquetes EAP entre el puerto cliente 802.1x y el puerto del punto de acceso o switch[15]. Estos puertos son llamados PAE (*Port Access Entity*).EAP es un componente fundamental del estándar 802.1X, y surgió como mejora del método de autenticación empleado en PPP (*Point to Point Protocol*), y que sirve de base sobre la que implementar diferentes modos de paso de credenciales (normalmente usuario/contraseña), tales como: PAP, MS-CHAP,

MD5, etc., lo que le ha dado gran flexibilidad y se ha convertido en uno de los aspectos a los que debe gran parte de su éxito[16]. Dentro del 802.1x se define la encapsulación de EAP en tramas Ethernet sobre una LAN, llamado EAPOL (EAP sobre LAN). En el protocolo EAP, intervienen tres tipos de elementos: el cliente que solicita acceso, el autenticador que sirve de enlace entre el cliente y el servidor de autenticación, que en el caso de redes WiFi es el punto de acceso, y el servidor de autenticación que es el que realiza la comprobación de credenciales como podría ser un servidor RADIUS. EAPoL indica el comienzo y el final de la sesión de autenticación con el mensaje de notificación EAPOL-START y EAPOL-LOGOFF[15][16].

En el estado autorizado, el puerto controla la duración de la sesión, significando el tiempo restante que considere el cliente autenticado sin preguntar por la re autenticación, usando la variable del período de re autenticación (reAuthPeriod), valor por defecto 3,600 s. Típicamente, el punto de acceso retransmite las tramas EAP perdidas cada 30s. Mientras tanto, el cliente 802.1x retransmite la trama EAPOL-START no reconocida cada 30 s por un mensaje EAP-REQUEST IDENTITY.

1.4.3 Proceso de autenticación de 802.1x

En redes inalámbricas, el protocolo EAP es usado en un modo transparente entre la estación y el servidor de autenticación a través de un punto de acceso[1][2]. Este es primero encapsulado en tramas EAPoLen el protocolo RADIUS, el cual es transportado sobre IP. Básicamente, la inserción de un terminal inalámbrico en un ambiente 802.1x ocurre como sigue:

1 Primero la estación se autentica, entonces consigue asociarse con un punto de acceso, el cual es identificado por un SSID (cadena de caracteres de 32 bit).
2 Para comenzar la autenticación, el cliente difunde una trama EAPOL-START cada 30 segundos, el mismo solicita conexión al punto de acceso que filtra todo el tráfico menos el correspondiente al protocolo EAPOL.
3 El punto de acceso se percata de que hay un nuevo cliente pidiendo acceso y le envía una solicitud de identificación enviando un mensaje REQUEST.IDENTITY-EAP al cliente 802.1x, el cual en la vuelta produce una respuesta EAP-

RESPONSE.IDENTITY conteniendo la identidad del terminal inalámbrico (EAP-ID).

4 El punto de acceso envía a la dirección IP del servidor de autenticación el mensaje EAP-RESPONSE.IDENTITY encapsulado en una solicitud RADIUS.

5 Los mensajes de preguntas y respuestas EAP son cambiados entre el servidor RADIUS y el cliente 802.1x, el punto de acceso juega solamente el rol pasivo.

6 El servidor RADIUS indica el éxito o el fracaso de este procedimiento a través de un mensaje EAP-SUCCESS o EAP-FAILURE. Basado en esta información, el puerto transita al estado "autorizado" o "no autorizado".

7 Al final del proceso de autenticación el mensaje RADIUS ACCESS-ACCEPT causa una transición de estado del puerto a "autorizado". El mensaje RADIUS ACCESS-REJECT fuerza el puerto en cuestión al estado "no autorizado". El puerto retiene este estado durante una sesión de autenticación.

8 En casos donde la autenticación es exitosa, el cliente y el servidor de autenticación 802.1x calculan una clave de sesión, nombrada llave única (*Unicast Key*). En el ambiente Microsoft este valor es un par de llaves 2x32 bytes[19]. .El servidor de autenticación envía este al punto de acceso en el atributo MS-MPPE-SEND-KEY y MS-MPPE-RECV-KEY del mensaje de acceso aceptado RADIUS.

9 El punto de acceso entonces selecciona una llave de encriptación, nombrada llave Global, a la asociación de seguridad con el cliente 802.1x. El último es encriptado y señalado con la llave de sesión recibida desde el servidor RADIUS y entonces entregado al cliente 802.1x en una trama EAPOL-KEY.

El proceso de autenticación se muestra en la figura 1.4.

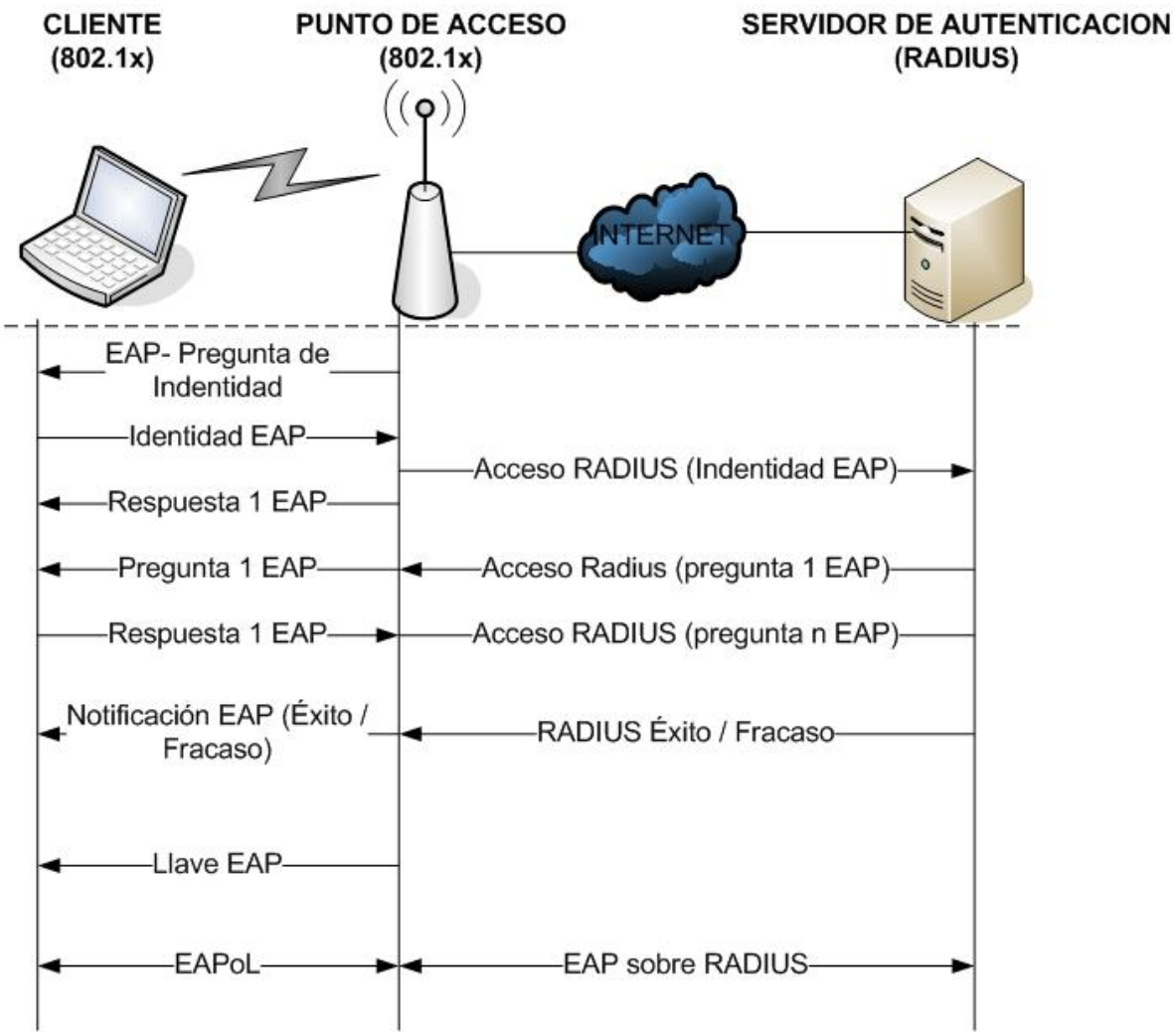


Fig. 1.4. Proceso de autenticación 802.1x.

En EAP los mensajes son trasmitidos en claro, además de no requerirse ningún tipo de autenticación por parte del servidor ni del cliente, lo que supone una clara vulnerabilidad a nivel de seguridad (más aún en entornos inalámbricos)[15][20]. Como mejoras al protocolo, se han incluido variantes que crean canales seguros entre el cliente y el servidor de autenticación: EAP-TLS, EAP-PEAP, y EAP-TTLS. EAP-TLS se trata de una variante de EAP en la cual se realiza una negociación SSL (*Secure Sockets Layer*) con autenticación basada en certificado, tanto por parte del cliente como del servidor. Tanto en el caso de EAP-PEAP como de EAP-TTLS, la conexión segura se realiza a partir exclusivamente del certificado del servidor (sería el equivalente a HTTPS en Web). En el caso de TLS (*Transport Layer Security*), las credenciales corresponden al certificado de cliente, mientras

que en el de PEAP y TTLS éstas son comunicadas utilizando uno de los métodos ya comentados: MS-CHAP, PAP, etc. A nivel de usuario, en el primer caso (TLS) basta con tener el certificado de cliente instalado, mientras que en los otros (PEAP y TTLS) tendría que proporcionar las credenciales, por lo general un usuario/contraseña[21].

Otra de las ventajas que incluye 802.1x es la posibilidad de generar, de manera dinámica y en la fase de autenticación, las claves que permitirán una conexión segura entre cliente y punto de acceso. Es decir, el servidor de autenticación genera una clave que es distribuida de manera segura al cliente y al punto de acceso, para que utilizando el esquema de encriptación convenido, cifren toda la comunicación hasta el cierre de la sesión. Esto hace que no haya una única clave que tenga que ser conocida por todos los clientes que acceden a la red, sino que se genera y distribuye de manera automática en el momento de la autenticación. IEEE 802.1x no constituye una alternativa al cifrado sino que solo contempla un marco para la autenticación y la distribución de claves, por lo que debe ser usado junto a una técnica de cifrado[7].

Llevar a cabo este proceso permite reducir la inseguridad de las redes inalámbricas porque:

1 Proporciona acceso controlado: Todo usuario que quiera acceder al recurso debe identificarse.
2 Permite autorizar el uso: A parte de saber quién intenta acceder a un recurso, se puede hacer un control de qué acciones puede ejecutar un usuario.
3 Permite el registro de actividades: Permite llevar *logs* o registros sobre cuál es el comportamiento de los usuarios en la red, y tener datos estadísticos que orienten la toma de decisiones para desempeñar una mejor gestión de la red.

Estos tres aspectos corresponden a tres palabras claves: Autentificación, Autorización y Contabilidad, conocidos también como servicios AAA, por su nombre en inglés: *Authentication, Authorization and Accounting*[22] (ver Epígrafe 1.3).

1.2.5 Protocolo de Seguridad WPA

WPA (*Wire Protect Access*) implementa la mayoría de lo que conforma el estándar IEEE 802.11i y fue diseñado para funcionar con todos los dispositivos de redes inalámbricas, excepto con los puntos de acceso de primera generación. Los datos utilizan el algoritmo RC4 con una clave de 128 bits y un vector de inicialización de 48 bits. Una de las mejoras más sobresalientes sobre su predecesor (WEP) es TKIP (*Temporal Key Integrity Protocol*, o Protocolo de integridad de clave temporal), el cual consiste en el cambio dinámico de clave mientras se utiliza el sistema. Además de proporcionar autenticación y cifrado WPA proporciona mejor integridad de la carga útil. WPA utiliza un Código de Integridad de Mensaje (MIC o *Message Integrity Code*). El Código de Integridad de Mensaje de WPA incluye un mecanismo que contrarresta los intentos de ataque para vulnerar TKIP y bloques temporales[1][9][23][24].

Características de WPA

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación[23][24].WPA incluye las siguientes tecnologías:

- IEEE 802.1X. Estándar para proporcionar un control de acceso en redes basadas en puertos. Los clientes tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA como puede ser RADIUS. Si la autorización es positiva, entonces el punto de acceso abre el puerto.
- EAP[15]. Es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad, WPA lo utiliza entre el cliente y el servidor RADIUS.
- TKIP (*Temporal Key Integrity Protocol*), es el protocolo encargado de la generación de la clave para cada trama.
- MIC (*Message Integrity Code*) es el código que verifica la integridad de los datos de las tramas.

WPA puede funcionar en dos modos:

- Con servidor AAA, RADIUS normalmente. Este es el modo indicado para las empresas o redes públicas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad[24].
- Con clave inicial compartida (PSK). Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos[7].

1.2.6 Protocolo WPA2

WPA2 es el nombre dado por la WiFi Alliance a la segunda fase del estándar IEEE 802.11i. La seguridad es mucho más fuerte y robusta en comparación con el protocolo WPA. WPA2 ya no se basa en un parche temporal sobre el algoritmo RC4 sino que utiliza el algoritmo de encriptación AES (*Advanced Encryption Standard*)[25]. Dicho algoritmo requiere un hardware mucho más robusto que los anteriores protocolos por lo que algunos puntos de acceso antiguos no pueden utilizar dicho protocolo. La implementación de protección que se aplica en el estándar de seguridad WiFi 802.11a se conoce con el acrónimo CCMP (*Counter Mode with CBC-MAC Protocol*) y está basada en el algoritmo AES[25]. El cifrado que se utiliza es un cifrado simétrico de 128 bits y el vector de inicialización tiene una longitud igual que en el WPA, es decir de 48 bits[1][9][23].

AES se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (*Counter-Mode /Cipher Block Chaining /Message Authentication Code Protocol*) en lugar de los códigos MIC. Otra mejora respecto a WPA es que WPA2 incluye soporte no sólo para el modo BSS sino también para el modo IBSS (redes *ad-hoc*)[25][26].

El protocolo CCMP usa el modo de operación CCM, el cual combina el comercio del modo CTR (*Counter Mode*) para confidencialidad y CBC-MAC (*Cipher Block Chaining-*

Message Authentication Code) para autenticación e integridad. CCM asegura la integridad del campo de datos del MSDU y también ciertas partes seleccionadas de la cabecera MAC. En CCMP, todos los tratamientos AES usan una llave y una longitud de bloqueo de 128 bits. CCM usa la misma llave temporal para CTR y CBC-MAC. Normalmente, el uso de la misma llave para varias funciones introduce un defecto de seguridad. Este no es el caso porque el IV es diferente para el modo CTR y CBC-MAC. Todos los valores en el cálculo del CBC-MAC son aleatorios, donde la probabilidad de colisión es muy débil. A pesar de todo, si hay una colisión, solamente el MIC cifrado es afectado, y no puede ser deducida la información. El protocolo CCM es un modo generado que puede ser usado con cualquier algoritmo de encriptación orientado a bloques[1].

1.2.7 VPN

La VPN (*Virtual Private Network*) es una herramienta para proteger las comunicaciones. Las VPN crean un túnel criptográfico entre 2 puntos determinados, utilizando para esto encriptación mediante el protocolo IPSEC. La aplicación de las VPN a ambientes WiFi surgen cuando se empezó a tomar conciencia de la fragilidad en la seguridad debido a las carencias y fallos de WEP, donde en algunos sectores se difundió su uso con el fin de mejorar y reforzar la encriptación. Básicamente lo que hace la VPN es crear un túnel entre el cliente y el servidor, quedando de esta manera protegida la conexión con IPSec, el cual es un método de encriptación muy robusto pero implica configurar los equipos terminales con esta herramienta.

1.2.8 Mecanismos de seguridad del nivel de transporte y aplicación

Los protocolos SSL (*Secure Socket Layer*) y TLS (*Transport Layer Security*) son protocolos que proporcionan comunicaciones seguras en Internet, ambos son muy parecidos. SSL fue diseñado por Netscape en 1996 y, aunque no es un protocolo estandarizado por el IETF, éste lo estandarizó en 1999 con ligeras modificaciones, aunque el protocolo funcionaba de la misma manera[21]. SSL/TLS permite la autenticación tanto de cliente como servidor, usando claves públicas y certificados digitales y proporciona comunicación segura mediante el cifrado de la información entre emisor y receptor.

SSL/TLS funciona por encima del protocolo de transporte (normalmente TCP) y por debajo de los protocolos de aplicación. Este protocolo está muy extendido para realizar actividades de comercio electrónico como transferencias bancarias, venta y compra en línea, entre otras. SSL/TLS se compone de cuatro protocolos. Estos protocolos funcionan de manera idéntica en SSL y en TLS, pero incorporan algunos detalles en TLS para su mejor funcionamiento[21] (Figura 1.5).

- Protocolo de Registro (*Record Protocol)*: encapsula los protocolos de nivel más alto y construye un canal de comunicaciones seguro. Se podría decir que es un protocolo de transporte.
- Protocolo de saludo (*Handshake Protocol*): se encarga de gestionar la negociación de los algoritmos de cifrado y la autenticación entre cliente y servidor. Define las claves de sesión utilizadas para cifrar. Se podría decir que es un protocolo de autenticación.
- Protocolo de cambio de cifrado (*Change Cipher Spec Protocol*): es un mensaje de un byte para notificar cambios en la estrategia de cifrado.
- Protocolo de alerta (*Alert Protocol*): señaliza alertas y errores en la sesión establecida.

Existen multitud de implementaciones del protocolo, tanto comerciales como de libre distribución siendo una de las más populares la biblioteca OpenSSL. SSL es capaz de trabajar con la mayoría de los protocolos que trabajan sobre TCP de tal manera que tiene asignado un número de puertos por defecto, por ejemplo el protocolo HTTP sobre SSL ha sido denominado HTTPS y tiene como puerto el 443.

SSL se basa en un esquema de clave pública para el intercambio de claves de sesión. En primer lugar el cliente y el servidor intercambian una clave de suficiente longitud mediante un algoritmo de cifrado asimétrico, como RSA o Diffie-Hellman, utilizando certificados. Mediante esa clave se establece un canal seguro, utilizando para ello un algoritmo simétrico previamente negociado. Los mensajes al ser transmitidos, se fragmentan en bloques, se comprimen y se les aplica un algoritmo hash para obtener un resumen (*Message Authentication Codes*) del mensaje para asegurar la integridad.

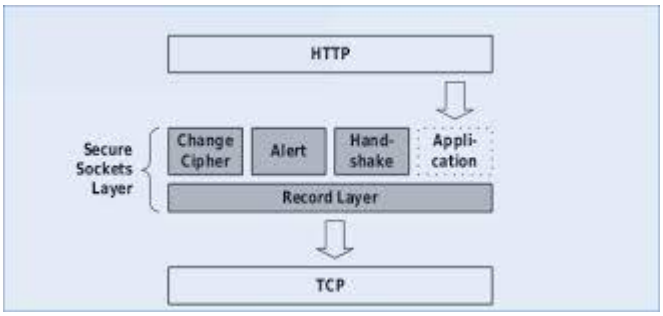


Fig. 1.5. Protocolo SSL/TLS.

1.2.9 Sistema de Detección de Intrusos (IDS)

El área de las auditorias de seguridad y detección de intrusiones se va siendo más indispensable cada día. Estas tecnologías no solo identifican y rastrean intrusiones, sino que mejoran la estabilidad y confianza de otros mecanismos de seguridad del sistema que monitorizan. Estos sistemas surgen en los años 80 y desde entonces han aparecido una enorme variedad de propuestas que intentan dar solución a estos problemas[3][27][28].

Un sistema de detección de intrusos (o IDS de sus siglas en inglés *Intrusion Detection System*) es un programa usado para detectar accesos no autorizados a una computadora o a una red. La detección de intrusos es el área aplicada de la seguridad informática encargada de informar de eventos que puedan tener lugar en un sistema informático y pueda ser considerado, por unas u otras razones, como parte de un intento de intrusión. Un intruso puede actuar de diferentes maneras como puede ser el acceso a un sistema, la ejecución de programas no autorizados o el ataque a una red informática[3].

El IDS suele tener sensores virtuales (por ejemplo, un *sniffer* de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

El funcionamiento de esta herramienta se basa en el análisis del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos

sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El IDS no sólo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento.[28][3]

Normalmente esta herramienta se integra con un firewall. El detector de intrusos es incapaz de detener los ataques por sí solo, excepto los que trabajan conjuntamente en un dispositivo de puerta de enlace con funcionalidad de firewall, convirtiéndose en una herramienta muy poderosa ya que se une la inteligencia del IDS y el poder de bloqueo del firewall, al ser el punto donde forzosamente deben pasar los paquetes y pueden ser bloqueados antes de penetrar en la red.

Los IDS suelen disponer de una base de datos de "firmas" de ataques conocidos. Dichas firmas permiten al IDS distinguir entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque o intento del mismo.

Tanto el IDS como los cortafuegos están relacionados con seguridad en redes de información, un IDS difiere de un cortafuegos. Un cortafuego limita el acceso entre redes, para prevenir una intrusión, pero no determina un ataque que pueda estar ocurriendo internamente en la red. Un IDS, evalúa una intrusión cuando esta toma lugar, y genera una alarma. Un IDS además observa ataques que se originan dentro del sistema. Este normalmente se consigue examinando comunicaciones, e identificando mediante heurística, o patrones (conocidos como firmas), ataques comunes ya clasificados, y toma una acción para alertar a un operador.

Un IDS usa alguna de las dos siguientes técnicas para determinar que un ataque se encuentra en curso[28][3]:

- Heurística

Un IDS basado en heurística, determina actividad normal de red, como el orden de ancho de banda usado, protocolos, puertos y dispositivos que generalmente se interconectan, y alerta a un administrador o usuario cuando este varía de aquel considerado como normal, clasificándolo como anómalo.

- Patrón

Un IDS basado en patrones, analiza paquetes en la red, y los compara con patrones de ataques conocidos, y pre configurados. Estos patrones se denominan firmas. Debido a esta técnica, existe un periodo de tiempo entre el descubrimiento del ataque y su patrón, hasta que este es finalmente configurado en un IDS. Durante este tiempo, el IDS será incapaz de identificar el ataque.

Los IDS tienen varias funcionalidades:

- Alertar en tiempo real eventos sospechosos.
- Visualización del tráfico en una sesión TCP.
- Visualización de tráfico en contenido binario.
- Detección de códigos malignos.
- Detección de virus.

1.2.9.1 Principales IDS

Uno de los sistemas de detección de intrusos es el de Cisco, conocido formalmente por Cisco *NetRanger*, es una solución para detectar, prevenir y reaccionar contra actividades no autorizadas a través de la red. Cisco Secure IDS incluye dos componentes: Sensor y Director. Las "herramientas" de red de alta velocidad *Cisco Secure IDS Sensors* analizan el contenido y el contexto de los paquetes individuales para determinar si se autoriza su tráfico. Si se detecta una intrusión, como por ejemplo un ataque de pruebas SATAN (*System Administrators Tool for Analyzing Networks*), un barrido de pings, los sensores de Cisco Secure IDS detectan el uso incorrecto en tiempo real, pueden enviar alarmas a una consola de gestión de *Cisco Secure IDS Director* para la representación geográfica y sacan al agresor de la red. Dado que el sistema *Cisco Secure IDS* incorpora funciones de respuesta pro-activas en Sensor, mediante la modificación de las listas de control de acceso (ACL) de los enrutadores Cisco, se puede configurar el sistema para rechazar o eliminar automáticamente ciertas conexiones. Esta característica puede ser temporal o, si se desea, se puede mantener indefinidamente. El resto del tráfico de la red funcionará normalmente: sólo se eliminará de forma rápida y eficaz el tráfico no autorizado de los usuarios internos o

de los intrusos externos. Así se consigue que los operadores de seguridad tengan un poder de actuación sobre toda la red para detener rápidamente la utilización inadecuada de la misma o el acceso de intrusos a la red[29].

Otro de los sistemas de detección de intrusiones de tiempo real, basados en red, es el Bro, el cual monitoriza de forma pasiva el tráfico de red. Su diseño está dividido en un motor de eventos que reduce el flujo de tráfico de red filtrado, a una serie de eventos de alto nivel. Por otro lado usa un intérprete de guiones de políticas de seguridad del sistema. Este sistema no solo es capaz de detectar ataques realizados a través del tramo de red que monitoriza, sino que también contempla la posibilidad de ser en sí mismo un potencial objetivo de ataques, para lo cual cuenta con mecanismos específicos para su detección y defensa. Es capaz de reconocer ataques como los de sobrecarga, cuyo objetivo central es el de sobrepasar la capacidad de proceso del detector, ataques de caída, los que provocan fallos en el monitor, o lo dejan sin recursos de sistema. Y por último los de subterfugio, los cuales intentan engañar al monitor mediante el envío de paquetes TCP con sumas de control inválidas o paquetes IP cuyo TTL es suficiente para llegar al monitor, pero no para llegar a su destino. Para ampliar su grado de efectividad Bro, cuenta además con capacidades de proceso específico de algunas aplicaciones de red, tales como *Finger*, FTP, *Portmapper*, *Ident*, *Telnet* y *Rlogin*. Se distribuye bajo una licencia tipo BSD[3].

El sistema STAT, portado a redes UNIX bajo el nombre de USTAT, fue creado en la universidad de California y usa diagramas de transiciones de estados que representan ataques conocidos para la detección de usos indebidos. Los diagramas de transición que se muestran en la figura, son la representación gráfica de escenarios de intrusión. Este sistema usa grafos para identificar ataques. Su paso por cada uno de los estados, depende de que se cumplan o no las características especificadas en cada estado.

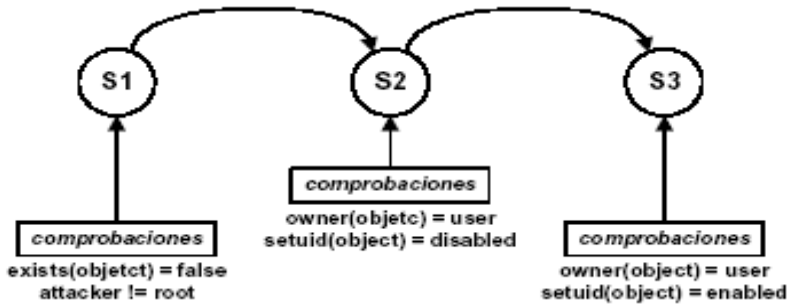


Figura 1.6 Diagrama de Transición de estados

En la figura los nodos son representativos de los estados y los arcos de transiciones. Estos diagramas facilitan la asociación entre los estados y muestran la evolución del intruso desde que entra al sistema, con privilegios limitados, hasta que llega a obtener el control del sistema. Los estados del diagrama indican situaciones particulares de un sistema, a las que se puede llegar de distintas maneras. De forma que varios atacantes puedan coincidir en el mismo estado habiendo realizado diferentes acciones. El estado inicial es representado por el sistema antes de ser comprometido, la intrusión se produce cuando se llega al último estado del diagrama. Si una acción determinada no lleva a ningún estado en concreto, el sistema devuelve al usuario al estado más cercano en que estaba. Sin embargo si llevan al usuario al estado final de un diagrama entonces el sistema envía una alarma al responsable de seguridad con las acciones tomadas en la última transición[3].

Dentro de las ventajas del sistema STAT podemos mencionar que los diagramas de transición permiten hacer una representación a alto nivel de escenarios de penetración, aspectos que no presentan los sistemas vistos anteriormente. Las transiciones ofrecen además una serie de patrones que conforman un ataque. Los diagramas de estado por su parte establecen la forma más sencilla de definir un ataque de modo que el motor de análisis puede usar variantes del mismo para identificar ataques similares. Este sistema es capaz de detectar ataques coordinados y lentos identificados en un diagrama.

Dentro de los aspectos negativos de este sistema tenemos que los diagramas de transición y las firmas o patrones son creados a mano, como en la mayoría de los sistemas. El lenguaje que usa para describir los ataques es muy limitado y en ocasiones resulta insuficiente para recrear ataques más complejos. Mientras que el análisis de algunos estados puede requerir

más datos del objetivo, por parte del motor lo que reduce considerablemente el rendimiento del sistema. De modo que las limitaciones de este sistema hacen que no pueda detectar algunos ataques comunes por lo que se hace necesario el uso de motores de análisis adicionales.

Uno de los sistemas de detección de intrusiones más populares es el Snort. Soporta algunas funciones de detección de anomalías, aunque es un detector de intrusiones de red basado en reglas. Es una herramienta basada en software libre y es capaz de realizar análisis de tráfico en tiempo real. Este sistema tiene la ventaja de funcionar bajo gran variedad de plataformas (Linux, OpenBSD, FreeBSD, NetBSD, Solaris, SunOS, HP-UX, AIX, IRIX, Tru64, Mac OS X Server, Win32). Está basado en las librerías *libpcap*, de modo que soporta cualquier plataforma que acepte las mismas[30].

Snort realiza análisis de protocolos, búsqueda y comparación de contenidos, y puede detectar gran variedad de ataques y sondeos, tales como desbordamientos de *buffer*, escaneo sigiloso de puertos (*stealth port scans*), ataques CGI, sondeos SMB, intentos de identificación de sistema operativo (*OS finger printing*), entre otros[3][30].

Este programa utiliza un lenguaje flexible de reglas para describir el tráfico de red que debe recoger o dejar pasar, además de un motor de detección que usa una arquitectura de *plugins* modular. Este sistema tiene también capacidades de alarma en tiempo real, y soporta diversos mecanismos de alarma, a través de *syslog* y un fichero especifico, sockets UNIX y mensajes *WinPopup* a clientes Windows. Puede usarse como rastreador de paquetes *sniffer*, de forma similar al *Tcpdump*, como registrador de paquetes, útil para la depuración de tráfico de red, y como detector de intrusiones de red[30].

Otro de los sistemas de detección de intrusos más utilizados hoyes el OSSIM (*Open Source Security Information Management*), el cual es una colección de herramientas que ayudan a la seguridad en la red, detección de intrusos y prevención. Es una herramienta que ofrece administración de eventos de seguridad mediante un motor de correlación y una colección detallada de herramientas de código abierto.

Alien Vault USM ofrece un excelente rendimiento, administración, reportes y soporte técnico respecto a OSSIM. Una característica clave que OSSIM no posee pero que su versión comercial sí, es el *Logger*, el cual es una base de datos adicional para propósitos forenses.

El sistema OSSIM ofrece diversas características:

- Detección de bajo nivel y en tiempo real de amenazas conocidas y actividad anómala.
- Envíos de forma automática.
- Auditoría de redes, equipos y políticas.
- Análisis de comportamiento de la red y situaciones.
- Administración de logs.
- Inteligencia que mejora la efectividad de la detección de amenazas.
- Análisis de seguridad orientado a riesgos.
- Reportes técnicos y administrativos.
- Una arquitectura de alto rendimiento escalable.

Se compone por un número de detectores y monitores dispersos por la red. Se encargan de realizar la detección y generación de alertas que posteriormente enviarán la información al sistema central para la recolección y correlación de los diferentes eventos. Los sensores se despliegan para el monitoreo de la actividad de la red.

Normalmente incluyen:

- Monitores y detectores pasivos de bajo nivel que recolectan datos buscando patrones.
- Analizadores que de forma activa buscan vulnerabilidades en la red.
- Agente de OSSIM que reciben datos desde equipos de red (routers, firewalls, etc.), comunican y envían sus eventos al servidor principal.

Una configuración típica de sensor OSSIM posee las siguientes funciones:

- IDS (Suricata/Snort).
- Analizador de Vulnerabilidades (OpenVAS/Nessus).
- Detector de Anomalías (p0f, Prads, arpwatch).

1.3 Autenticación, Autorización y Contabilización (AAA)

En seguridad informática, el acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: Autenticación, Autorización y Contabilización (*Authentication, Authorization and Accounting*). La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados. AAA se combina a veces con auditoria, convirtiéndose entonces en AAAA. Los protocolos AAA fueron una de las soluciones propuestas a los problemas de control de acceso presentados desde el nacimiento de Internet para prestar los servicios AAA anteriormente comentados[22][31][32].

Autenticación

La autenticación es el proceso por el que una entidad prueba su identidad ante otra. Normalmente la primera entidad es un cliente (usuario, ordenador, etc) y la segunda un servidor (ordenador). La Autenticación se consigue mediante la presentación de una propuesta de identidad (un nombre de usuario) y la demostración de estar en posesión de las credenciales que permiten comprobarla. Ejemplos posibles de estas credenciales son las contraseñas, los testigos de un sólo uso (*one-time tokens*), los certificados digitales, o los números de teléfono en la identificación de llamadas. Los protocolos de autenticación digital modernos permiten demostrar la posesión de las credenciales requeridas sin necesidad de transmitirlas por la red[22].

Autorización

Autorización se refiere a la concesión de privilegios específicos (incluyendo "ninguno") a una entidad o usuario basándose en su identidad (autenticada), los privilegios que solicita, y el estado actual del sistema. Las autorizaciones pueden también estar basadas en restricciones, tales como restricciones horarias, sobre la localización de la entidad solicitante, la prohibición de realizar *logins* múltiples simultáneos del mismo usuario, etc.

La mayor parte de las veces el privilegio concedido consiste en el uso de un determinado tipo de servicio. Ejemplos de tipos de servicio son filtrado de direcciones IP, asignación de direcciones, asignación de rutas, asignación de parámetros de calidad de servicio, asignación de ancho de banda, y cifrado entre otras[32].

Contabilización

La Contabilización se refiere al seguimiento del consumo de los recursos de red por los usuarios. Esta información puede usarse posteriormente para la administración, planificación, facturación, u otros propósitos. La contabilización en tiempo real es aquella en la que los datos generados se entregan al mismo tiempo que se produce el consumo de los recursos. En contraposición la contabilización por lotes ("*batch accounting*") consiste en la grabación de los datos de consumo para su entrega en algún momento posterior. La información típica que un proceso de contabilización registra es la identidad del usuario, el tipo de servicio que se le proporciona, cuando comenzó a usarlo, y cuando terminó[32].

Existen varios protocolos que realizan estas tres funciones:

- TACACS - Corresponde al protocolo pionero que suplió la carencia de servicios AAA. Actualmente ha caído en desuso y, su creador, CISCO, le retiró el soporte.
- TACACS+ - Este protocolo entró para reemplazar a TACACS, aunque hoy en día todavía se usa, sólo es implementado en una pequeña porción del mercado, debido al poco dinamismo de las soluciones comerciales.
- RADIUS – Protocolo desarrollado por *Livingston Enterprises*, se convirtió en un estándar de la IETF, se ha mantenido vigente a través de muchas aplicaciones que implementan el protocolo y siguen siendo actualizadas y mejoradas[33][17][34][19].
- DIAMETER – Protocolo que pretende mejorar la especificación de RADIUS y proveer nuevas funcionalidades. Sin embargo, su calidad de “estándar en construcción” o “borrador”, no ha facilitado el desarrollo de aplicaciones que lo implementen, ocasionando que su incursión en ambientes de producción sea mínima.

Otros protocolos utilizados en combinación con los protocolos usados en AAA son los siguientes:

- PPP
- EAP
- LDAP

1.3.1 Protocolo RADIUS

RADIUS *(Remote Authentication Dial-In User Service)*. Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza los puertos 1812 y 1813 UDP para establecer sus conexiones (para autentificar/autorizar y contabilizar, respectivamente)[33].

Cuando se realiza la conexión con un ISP (*Internet Service Provider*) mediante módem xDSL, *Ethernet* o WiFi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo *Network Access Server* (NAS) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP y otros parámetros como L2TP, etc. RADIUS consta de tres componentes: un protocolo con un formato de trama que utiliza el protocolo de datagramas de usuario (UDP), un servidor y un cliente (Fig. 1.6)[33][34].

Fig. 1.6. Componentes del protocolo Radius.

Los paquetes que se envían a través de la red manejan un formato propio del protocolo RADIUS, los mismos que contienen un campo denominado código que indica el tipo de paquete, como se muestra en la siguiente tabla:

TABLA 1. CAMPOS DEL PAQUETE RADIUS

VALOR	NOMBRE DEL CAMPO	DESCRIPCIÓN
1	Access-Request	Cliente: Petición de acceso
2	Access-Accept	Servidor: Petición aceptada
3	Access-Reject	Servidor: Petición rechazada
4	Accounting-Request	Cliente: Petición de registro
5	Accounting-Response	Servidor: Respuesta de registro
11	Access-Challenge	Servidor: Desafío para autenticación
12	Status-Server	Reservado (Experimental)
13	Status-Client	Reservado (Experimental)
255	Reserved	Reservado

Principales características:

- Funciona bajo el modelo cliente-servidor[33].

- Ofrece nivel limitado de seguridad en la red ya que aunque las comunicaciones entre el cliente y el servidor son validadas mediante un secreto compartido que no se envía por la red, solo se encripta la clave del usuario en los paquetes de solicitudes de acceso desde el cliente al servidor, utilizando el método de encriptación MD5. El resto del paquete no está encriptado pudiendo ser objeto de captura el nombre de usuario, servicios autorizados y la contabilización de estos.
- Los servidores RADIUS soportan varios esquemas de autentificación de usuario como: EAP, PAP y CHAP y soportan varios orígenes de información como: una base de datos del sistema (*/etc/passwd*), o una base de datos interna (del propio servidor RADIUS), mecanismos PAM y otros como *Active Directory*, LDAP y Kerberos.
- Capacidad para el manejo de sesiones, notificando inicio/cierre de conexión, lo que permite que al usuario se le pueda determinar su consumo y facturar en consecuencia; esta constituye una de las características fundamentales de este protocolo, los datos se pueden utilizar con propósitos estadísticos.
- El protocolo RADIUS ofrece una base de datos central donde almacenar toda la información del usuario de marcado. Todos los servidores de acceso a redes compatibles con RADIUS pueden utilizar esta base de datos.
- Un servidor RADIUS puede actuar como *proxy* a otros servidores RADIUS u a otro tipo de servidores de autentificación.
- RADIUS soporta dos lenguajes, uno construido internamente tipo C llamado *Rewrite* u otro llamado *Schema* que requiere *Guile versión 1.4* o mayor. Este le permite al administrador escribir sus propios métodos de autentificación y contabilidad.
- Opera en la capa 2 del modelo OSI con el uso del protocolo 802.1x. Ya que la autentificación de la Capa 2 opera en el nivel local, se evita que los intrusos utilicen la red física sin autentificarse[33].
- Algunos servidores usan el puerto UDP 1645 para mensajes de autentificación y, el puerto 1646, para mensajes de contabilización. Esto último debido a que son los puertos que se usaron inicialmente para este tipo de servicio.

Este estándar trae las siguientes ventajas:

- Alto nivel de seguridad porque puede usar nombres de usuarios y contraseñas o certificados de usuario.
- Cifrado más seguro.
- Autentificación y cohesión a la WLAN transparentes.
- Autentificación por separado de usuarios y de equipos.
- Bajo costo de red.
- Alto rendimiento porque el cifrado se lleva a cabo en el *hardware* de la WLAN y no en el procesador del equipo cliente.
- Sus clientes tan sólo tienen que implementar el protocolo de comunicación con RADIUS y no todas las posibilidades de AAA existentes (PAP, CHAP, LDAP, Kerberos, mySQL, etc.).
- En su comunicación con el cliente RADIUS, nunca se transmiten las contraseñas directamente por la red, ni siquiera al usar PAP, sino que usa algoritmos para ocultar las contraseñas como MD5.

Un servidor RADIUS puede ser implementado en las plataformas más populares: Linux, Microsoft Windows y SUN/SOLARIS. El software utilizado RADIUS ha sido compilado y probado en:

- Linux (todas las versiones)
- FreeBSD
- NetBSD
- Solaris

1.4 Ataques a las redes WiFi

Las redes inalámbricas son sensibles a un grupo de ataques que toman ventajas por las características del medio físico de estas redes para la comunicación entre los dispositivos. Los ataques a redes WiFi más comunes que se han podido identificar son los siguientes:

1.4.1. Romper claves WEP

Por las propias características que presenta WEP es un protocolo inseguro. Hay principalmente dos métodos de romper la seguridad en este protocolo y por consiguiente obtener su clave, mediante fuerza bruta y mediante descifrado. El método de fuerza bruta consiste tan solo en ir probando una tras otra posibles combinaciones de claves hasta dar con la correcta. Este método además de poder ser poco efectivo es muy lento. El otro método, el descifrado, averigua la clave aplicando el proceso de descifrado a un conjunto de paquetes capturados previamente. Para capturar estos paquetes se suele inyectar paquetes ARP con el fin de que se genere movimiento de tráfico en la red y poder así hacer una mayor captura de paquetes[1][9].

Para ejecutar lo antes expuesto existe varias herramientas entre las más conocidas es la familia de Aircrack[9][35].

- AIRODUMP-NG: Se usa para capturar los datos transmitidos a través de las ondas WiFi (IV de los paquetes WEP), muestra todas las redes WiFi a su alcance, con su *Bssid, essid,* potencia, canal, tipo de encriptación, etc.

- AIREPLAY-NG: Esta herramienta es la que se usa para lanzar los distintos ataques, como son los siguientes:

Ataque 0. Sirve para des autenticar a un cliente conectado al AP que se está atacando. Esto es especialmente útil cuando la red tiene cifrado WPA, ya que se lograra que el cliente se tenga que volver a autentificar y podremos capturar el *handshake.*

Ataque 1. Autentificación falsa. Este ataque se utiliza cuando no hay un cliente legítimo conectado a la red. De esta forma se crea un cliente falso que se asociará al AP y así poder lanzar los ataques correspondientes. Es indispensable para lanzar los ataques 2, 3 y 4.

Ataque 2. Reinyección interactiva de paquetes. Este ataque permite elegir el paquete que se va a re inyectar al AP.

Ataque 3. Inyección de paquetes ARP Automáticamente. Este ataque es el más efectivo, cuando hay un cliente legitimo conectado, una vez se lanza el ataque la aplicación intentará conseguir un paquete ARP y cuando lo consiga, empezará a re inyectárselo al AP generando así un tráfico que permitirá subir los IVs a una velocidad frenética.

Ataque 4. Este es un ataque por saturación al enrutador víctima, en la actualidad es poco efectivo, ya que los enrutadores identifican el ataque y no lanzan paquetes de respuesta. Pero cuando el AP es vulnerable se consigue obtener la clave WEP de una manera relativamente rápida.

- AIRCRACK-NG: Se utiliza para des encriptar los paquetes capturados y así obtener la clave de la red WiFi. Para ello se le indica el archivo, dicho archivo es capturado previamente con airodump-ng, y comenzará el proceso de descifrado.

Otras herramientas para des encriptar WEP son: Airoscript, GOYScript WEP, Airlin, Minidwep-gtk, las cuales funcionan automáticamente sin ejecución de ningún comando, lo que las hace sencillas para cualquier atacante[9][36].

1.4.2. Romper claves WPA, WPA2

La ruptura de claves WPA se basa en dos pasos, capturar el *handshake* y el *crackeo* mediante diccionario[37][10][18]. Cada vez que un cliente se conecta a una red con cifrado WPA, envía un paquete-saludo, o *Handshake* al AP al que se va a conectar, donde este paquete saludo contiene la contraseña encriptada que se desea obtener. El *handshake* solo se puede capturar exclusivamente cuando un cliente se conecta al punto de acceso. Por tanto se abren dos posibilidades, esperar pacientemente a que el cliente se desconecte y se vuelva a conectar, o bien, forzar la desconexión del cliente utilizando un ataque de des autenticación. Una vez obtenido el *handshake* se *crackea* éste mediante un diccionario[9][23][24].

Existen varias herramientas para realizar estos ataques como pueden ser[24]:

- *Linset: Linset* es una herramienta que utiliza técnicas de descifrado de contraseñas en tiempo real en los enrutadores y puntos de acceso víctimas sin utilizar diccionarios de claves pre configuradas para ello. El funcionamiento es el siguiente:
  1. Escanea la red en busca de puntos de acceso para conectarse y muestra una lista de todos los encontrados.
  2. Lanza un *handshake* a la red seleccionada.
  3. Crea un falso punto de acceso con el mismo SSID que la red víctima.
  4. Realiza un ataque DoS contra los clientes conectados a la red seleccionada a la espera de que se bloquee la conexión e intenten conectarse de nuevo, esta vez al falso punto de acceso.
  5. Se monta automáticamente un servidor DHCP y cuando los clientes se conectan al punto de acceso falso se les muestra una web donde se solicita la contraseña.
  6. Cuando se envía la contraseña a la web falsa esta se compara con el *handshake* enviado anteriormente para ver si es correcta.
  7. Si la clave es correcta se finaliza el ataque DoS, el punto de acceso y el DHCP de manera que el usuario vuelve a conectarse automáticamente de nuevo al punto de acceso original.
  8. Un *script* limpia todos los datos generados del sistema atacante para no dejar rastro de la actividad a la vez que ningún archivo temporal pueda influir en la conexión pirata.

- *WifiPhishing*: El ataque es una mezcla de ingeniería social (el método más común de ataque), con una sencilla aplicación. La aplicación requiere de Kali Linux y dos interfaces de red, una que sea capaz de inyección. Lo que la aplicación hace, es, básicamente clonar y replicar a un punto de acceso familiar de la víctima, mientras que simultáneamente se bloquea el acceso al enrutador original. Con Wifiphisher, se le hace creer a la persona que está teniendo problemas de autentificación, al obligar a todos los clientes conectados al punto de acceso original a desconectarse. Cuando un usuario conectado al punto de acceso no autorizado intenta abrir una página web, el punto de acceso mostrara una página de *phishing* en lugar de pedir al usuario su contraseña inalámbrica. La página de *phishing* predeterminada

proporcionada por la herramienta se disfraza de una página de configuración del enrutador que indica que una actualización de *firmware* está disponible para el dispositivo por lo que se requiere la contraseña WPA para iniciar el proceso de actualización.

Al hacerse pasar por el enrutador original (enviando incluso una página falsa preguntando por la contraseña), los incautos usuarios simplemente ingresan la contraseña falsa al router, proporcionándosela voluntariamente a esta réplica maligna. Y una vez que se obtiene la contraseña original, este "gemelo diabólico" puede seguir operando como intermediario de conexión (entre el punto de acceso original y los clientes), interceptando todo el tráfico que transita por ahí. Por lo que es útil para el robo de contraseñas e información.

Wifiphisher, es una herramienta de seguridad que monta rápidamente ataques automatizados de *phishing* contra redes WPA, con el fin de obtener la contraseña secreta. Es un ataque de ingeniería social que a diferencia de otros métodos no incluye ninguna fuerza bruta. La herramienta no aprovecha ninguna nueva vulnerabilidad, sino que combina métodos conocidos para automatizar un ataque WiFi.

- *Goyscrip*t WPA: *Script* para capturar *handshake*, a esta herramienta se le selecciona la interfaz que se va a usar en modo monitor. Una vez seleccionada el *script* lanzara airodump-ng para escanear solo las redes con cifrado WPA, y mostrará la lista de redes disponibles. Cuando se elija la red, comenzará el ataque de des autentificación para capturar automáticamente el *handshake*. Cuando lo consiga pasará automáticamente aircrack-ng con 3 diccionarios que tiene ya cargados[23][35].

- *BrutusHack: BrutusHack* es un *script*, para pasar diccionarios con los parámetros pre-configurados a un *handshake*, previamente capturado. En esta herramienta tenemos varios modelos de diccionario preconcebidos, para distintas redes o distintos tipos de diccionarios.

- *Goyscript* DIC: *Script* parecido al anterior con 4 diccionarios ya creados. La herramienta detecta automáticamente los *handshake* capturados con *Goyscript* WPA

- *StrinGenerator*: Generador de diccionarios, para atacar *handshake* de redes WPA.

1.4.3. Escuchas/Sniffing

El objetivo de las escuchas es monitorizar la red con el fin de capturar información sensible como por ejemplo, la dirección MAC o IP origen y destino, contraseñas, claves, identificadores de usuario, etc. Las escuchas se consideran un paso previoa ataques posteriores, como por ejemplo la inyección y modificación de paquetes sin necesidad de descifrar claves[23][35][38]. No obstante para que un dispositivo tenga la capacidad de llevar a cabo escuchas de red debe tener instalada o integrada una tarjeta WLAN que actué en modo promiscuo o en modo monitor, ya que estos modos de operación permiten recibir todo el tráfico que circula por la red. Adicionalmente es necesario utilizar un software *sniffer*, como pueden ser:

- Wireshark
- Fiddler
- WinPcap
- Free IP Scanner
- SoftPerfect Network Scanner
- IP Sniffer
- Find MAC Address
- Angry IP Scanner

1.4.4. Denegación de servicio, clases principales.

Los ataques DoS (Denegación de servicio) son uno de los tipos más sencillos de llevar a cabo y a la vez uno de los más complicados de contrarrestar. La DoS consiste básicamente

en enviar un gran número de peticiones a un servidor de manera que los usuarios legítimos del servicio no puedan acceder a esos recursos[9].

Los principales ataques DoS son los siguientes:

- Ataque de inundación de buffer o *Buffer Overflow*
- Ataque de inundación de SYN o SYN *Flood*
- Ataque Teardrop
- Ping de la muerte
- Ataque de inundación ICMP
- Ataque *Smurf*

1.4.5. Denegación de servicio por saturación de ruido

El objetivo principal que persigue el atacante con este ataque es imposibilitar la comunicación del usuario con el punto de acceso a través de la degradación de la señal. Para conseguir degradar la señal el atacante no podrá distanciar el punto de acceso del usuario y ni tampoco podrá ir interponiendo obstáculos entre ambos. Sin embargo una señal WiFi se puede ver afectada por 3 factores principalmente: distancia, obstáculos e interferencias. Por tanto lo que hará el atacante será debilitar la señal mediante interferencias, provocadas éstas por una cantidad intensa de ruido[4][39].

1.4.6. Denegación de servicio por torrente de autenticaciones

Para que se pueda dar este ataque se deben cumplir 2 condiciones, que se utilice el estándar 802.1x y el servidor RADIUS, y además que cada usuario que quiera acceder tenga que autenticarse previamente. Básicamente consiste en el envío masivo y simultaneo de peticiones falsas por parte de un atacante, consiguiendo así que el servidor RADIUS se mantenga ocupado con este atacante y tenga que denegar por consiguiente el servicio a los otros usuarios (puesto que no podrá atenderlos)[2][9].

1.4.7. Ataques Spoofing

Un ataque de *Spoofing* tiene como función el suplantar validadores, credenciales o identificadores estáticos, es decir parámetros que permanecen invariables antes, durante y después de la concesión de un privilegio, una autenticación, etc. Varios de estos valores son por ejemplo las direcciones IP, direcciones MAC, nombre de dominio, nombres de recursos compartidos y direcciones de correo electrónico. Una forma de ejecutar este ataque es a través de redefinir la dirección física o MAC de la interfaz inalámbrica por una dirección MAC valida dentro del sistema atacado. Para hacer esto basta con emplear un *sniffer* que permita (ataque pasivo) capturar alguna MAC valida en el sistema, con el fin de suplantar posteriormente la dirección MAC capturada. Cabe decir que para utilizar dicha dirección MAC se tendrá que esperar a que el usuario propietario de la MAC se desconecte, aunque también se puede ejecutar un ataque DoS contra él con el fin de expulsarlo de la red[9].

1.4.8. Ataque Hombre en el medio

El ataque hombre en el medio (*Man in the Middle* (MITH)) está basado en *Spoofing y* consiste en interponerse entre dos sistemas. En este ataque, un atacante intercepta y modifica los datos de la comunicación para así suplantar la identidad de las entidades implicadas en la comunicación. Puede escuchar todos los mensajes intercambiados entre las partes e incluso modificarlos y volver a enviarlos, implicando esto que los extremos sigan creyendo que se están comunicando con el extremo legítimo. Los entornos que operan sobre las redes locales facilitan la captura y redirección de sesiones ya que una estación inalámbrica que transmite no es capaz de detectar presencia alguna de estaciones adyacentes con la misma MAC o IP[40].

1.4.9. Secuestro de sesiones /Hijacking

Hijacking es una amenaza de seguridad que al igual que MITH se vale del *Spoofing*, aunque en este caso se intentará tomar una conexión existente entre dos dispositivos de usuario. Tras monitorizar la red el atacante puede generar tráfico que parezca venir de una de las partes constituyentes de la comunicación, robando así la sesión de los usuarios correspondientes[9][36].

1.5 Conclusiones parciales del capítulo

Sin lugar a dudas el área de las redes de datos y de la conectividad ha sido una de las que más ha evolucionado en los últimos tiempos. Este proceso como todos no ha estado libre de malas intenciones por parte de personas inescrupulosas que buscando beneficios económicos o simplemente fama han creado una serie de técnicas y ataques para violar la seguridad de los estándares existentes. En respuesta a esto los especialistas e ingenieros han creado mejores productos. Este ciclo de ataques y mejoras ha llevado el mundo del WiFi a un estado considerado estable en estos momentos. Se puede afirmar que las soluciones WiFi se encuentran en un punto en que su despliegue y explotación puede realizarse de forma segura si se utilizan los productos y las configuraciones adecuadas.

Nuestro país ha visto el potencial de estas redes y ha apostado en ellas como una forma de aumentar los índices de acceso a internet de la población.

En el siguiente capítulo se aborda el tema específicamente para la provincia de Villa Clara.

Capítulo 2 Características de la Red WiFi de Etecsa en Villa Clara

2.1 Introducción

La Empresa de Telecomunicaciones de Cuba S.A. (ETECSA) ofrece servicio de conectividad a Internet utilizando para esto diferentes tecnologías de acceso. Entre las tecnologías más empleadas están las que van sobre redes de cobre como xDSL (*Digital Subscriber Line*), con una gran estabilidad y calidad de servicio. Otras que se están introduciendo son las que viajan a través de fibra óptica como son FTTN (*fiber to the node*), FTTC (*fiber to the cabinet*), FTTH (*fiber to the home*) con la arquitectura GPON (*Gigabit-capable Passive Optical Networks*).Estas tecnologías alcanzan altas velocidades, xDSL con 24 Mbps de bajada y 6 Mbps de subida y GPON con 2.488 Gbps de bajada y 1.244 Gbps de subida, además son redes altamente seguras por su condición de acceso alambrado, por lo que un intruso para acceder a dichas redes tiene que interceptarlas físicamente.

Otra de las redes por la que se brinda este servicio son las redes de acceso inalámbricas con la tecnología WiFi. Dicho servicio ha sido de gran aceptación en el mercado por las ventajas que ofrece a los clientes, alta velocidad, movilidad y uso de una gran variedad de dispositivos (teléfonos inteligentes, tabletas, laptops, PC con tarjetas de red inalámbricas y todo equipo terminal con WiFi). Una de las ventajas para el operador es su fácil implementación técnica y cobertura en áreas relativamente grandes usando para esto poco equipamiento, lo que abarata el costo del servicio.

A pesar de las ventajas de esta red inalámbrica la misma también presenta inconvenientes, uno de los más importantes es su inseguridad debido a que la señal puede ser fácilmente interceptada.

En este capítulo se describirá la arquitectura y funcionamiento de la red WiFi de Etecsa, los mapas de cobertura de dicha red, la cantidad de usuarios que se conectan, la forma de cobro del servicio, la accesibilidad a la red y el equipamiento que la soporta. Se identificarán las

vulnerabilidades de seguridad que presenta la red y la necesidad de una herramienta capaz de alertar ante un evento anómalo en el comportamiento de la misma.

2.2 Arquitectura actual de la red WiFi de Etecsa

Actualmente la red WiFi de la Empresa de Telecomunicaciones de Cuba S.A. está compuesta por:

1. Equipo terminal: Dispositivo propiedad del cliente que cumpla con la norma IEEE 802.11 a/b/g/n.
2. Punto de acceso (AP): Antena para interiores o exteriores con la norma IEEE802.11a/b/g/n, utilizada únicamente para la conexión física de los equipos terminales con la red.
3. Controlador de acceso (AC): Controlador de acceso a la red, encargado de que todos los usuarios se autentiquen antes de concederles el acceso a Internet.
4. Portal web cautivo: Pagina web utilizada para que el cliente se autentique, dicho portal se encuentra en un servidor distante del controlador de acceso.
5. Servidor AAA con protocolo RADIUS: servidor que guarda los permisos de acceso y la contabilidad de los usuarios (usuario, contraseña, saldo existente).

En la figura 2.1 se muestra la arquitectura de dicha red.

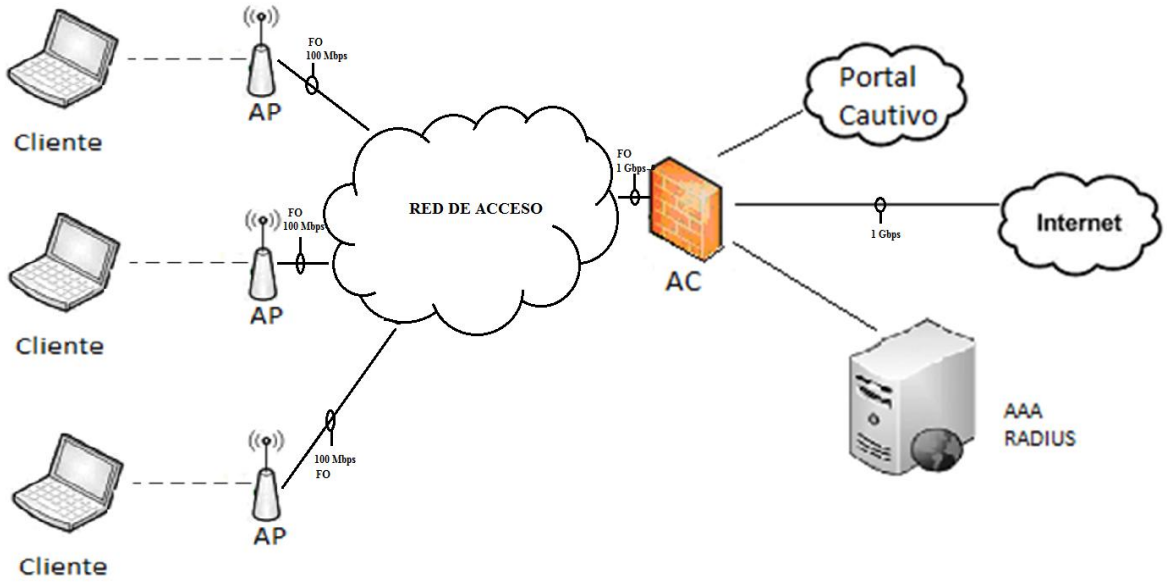


Fig. 2.1. Arquitectura actual de la red WIFI.

En la estructura antes mostrada cada AP está interconectado a una red de acceso a 100 Mbps, todos los elemento de la red de acceso se encuentran interconectados por medio de fibra óptica a 1 Gbps. A esta red de acceso está enlazado el controlador de acceso con una velocidad de conexión también a 1 Gbps. El controlador de acceso tiene conexión con el portal web cautivo, el servidor RADIUS e Internet. Toda la red entre los AP y el AC se encuentra a nivel de enlace del Modelo OSI, por lo que no existe ningún equipamiento de las capas superiores en esa porción de la red.

Este portal cautivo anteriormente mencionado se encuentra en un servidor externo al elemento de control AC. En esta configuración el AP no implementa ningún mecanismo de protección a los datos que circulan entre el cliente y él, solo ofrece la posibilidad de acceso físico a la red.

2.3 Proceso de conexión a la red

En esta arquitectura el cliente se conectará al AP libre de autenticación y libre de cualquier proceso de encriptación. El proceso de conexión, autenticación y desconexión se muestra en la figura 2.2.

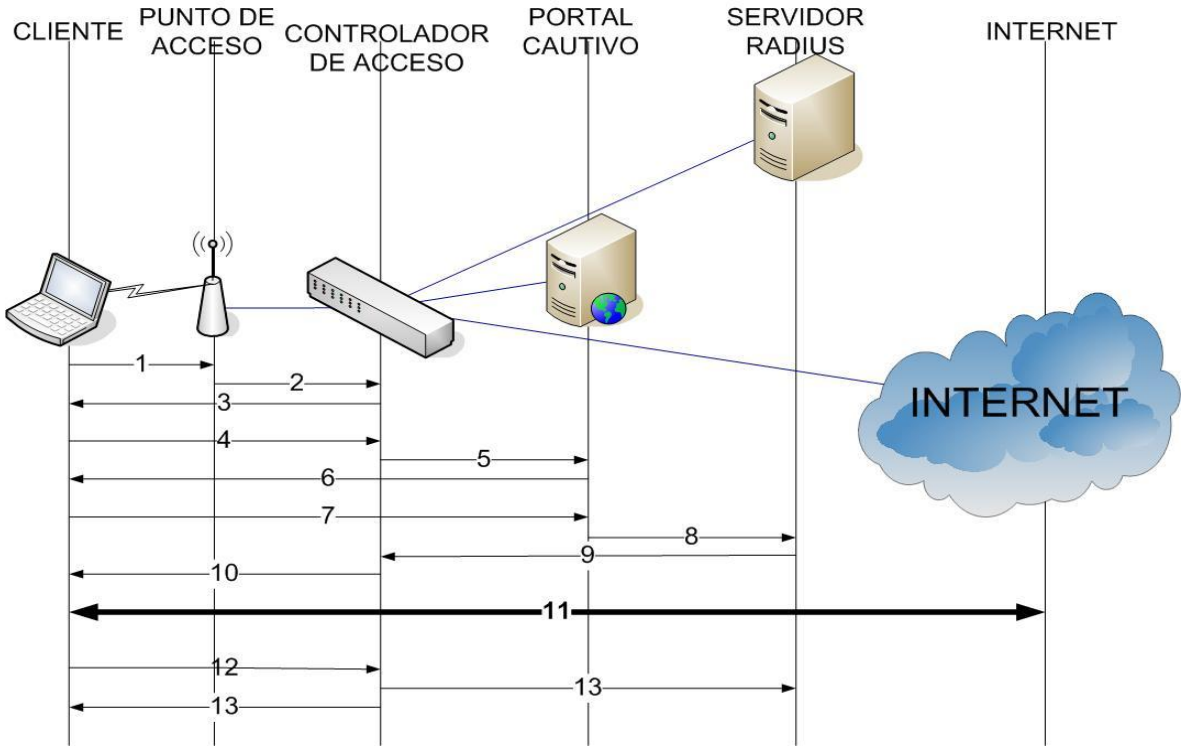


Fig. 2.2 Proceso de autenticación.

Proceso de conexión, autenticación y desconexión:

1. El cliente solicita conectarse a la antena escogiendo el SSID de la misma.
2. La antena recibe la petición y le envía al AC una solicitud DHCP del cliente.
3. El AC recibe la solicitud de dirección IP y le asigna una libre del rango.
4. El cliente abre un navegador web y hace una petición de navegación (Ejemplo: www.google.com).
5. El AC re direcciona la solicitud de navegación al portal web cautivo.
6. El portal cautivo muestra una petición de usuario y contraseña, por lo que el cliente es obligado a autenticarse para poder realizar una navegación exitosa.
7. El cliente envía los datos usuario y contraseña mediante el portal cautivo.
8. El portal cautivo envía los datos de usuario y contraseña introducidos por el cliente al servidor RADIUS.
9. El servidor RADIUS comprueba los datos introducidos por el cliente contra su base de datos. Si esta autenticación es denegada por el servidor, el navegador le devuelve al cliente una respuesta de negación de acceso por las causas encontradas (Ejemplo: error de usuario/contraseña, límite de tiempo en 0, etc.) y como consecuencia el cliente no puede llevar a cabo dicha navegación. En caso contrario, si la autenticación que realiza el cliente en el portal Web es aceptada por el servidor RADIUS, éste le envía al AC la contabilidad de la cuenta (saldo inicial y saldo restante).
10. El AC le muestra al cliente el saldo actual de su cuenta y el saldo restante. A partir de aquí el AC mientras dure la conexión es el encargado de actualizar dicha contabilidad.
11. Conexión a Internet establecida.
12. El cliente solicita la desconexión (ejecutando: LOGOUT, http://1.1.1.1 o apagando la antena WiFi del equipo terminal).
13. El AC le reenvía al servidor RADIUS el estado final contable en que quedó dicha cuenta y al cliente le envía una confirmación de desconexión.

2.4 Cobertura de la red WiFi de Etecsa

El servicio de acceso a Internet por medio de una red WiFi surge en la provincia en el año 2012 donde se escogió el Hotel Iberostar Ensenachos como lugar para una prueba piloto, a partir de ahí se fue incrementando el servicio en las instalaciones turísticas de la provincia de las cadenas hoteleras Gaviota, Cubanacan e Islazul, por lo que en estas instalaciones es donde mayor alcance de cobertura se ha alcanzado. En la zona de Cayo Santa María existe una cobertura WiFi en todos los hoteles (15 instalaciones), también en hoteles de la ciudad como son el Hotel Barcelona en Remedios y los Hoteles América y Santa Clara Libre en la ciudad de Santa Clara, además se comenzó el servicio en este año en lugares abiertos como los parques principales de Remedios y Santa Clara.

En la figura 2.3 se muestra el mapa de Santa Clara con los lugares de presencia en la ciudad. En los anexos 1 y 2 se muestran los mapas de cobertura de Cayo Santa María y Remedios respectivamente.

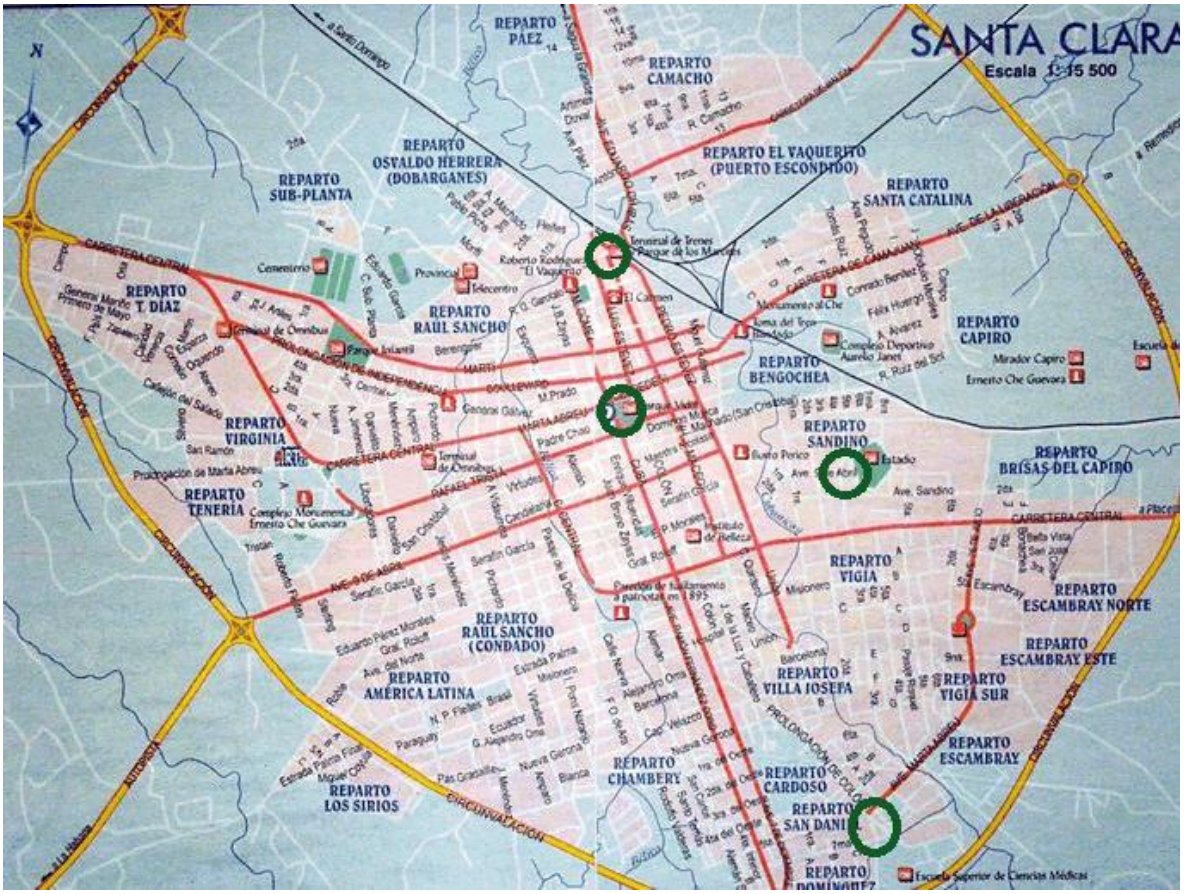


Fig. 2.3 Zonas WiFi en la ciudad de Santa Clara.

2.5 Características del servicio de acceso a Internet

Las características básicas del servicio son:

- Servicio prepago.
- El cobro es por tiempo de conexión.
- La navegación corresponde a una "Cuenta de Acceso" y puede tener alcance nacional o internacional.
- El servicio permanente puede ser recargado y el servicio temporal es "No recargable".
- La "Cuenta de Correo", es creada a voluntad del usuario y tiene alcance, nacional o internacional, según el servicio que elija previamente el usuario.

La "Cuenta de Acceso" es la que le permite al usuario acceder a la navegación, puede tener alcance nacional o internacional. Siempre es pre pagado y puede ser "recargable" o "No recargable". Identificada por dos atributos básicos el "nombre de usuario" y la "contraseña", no siendo estos los únicos que se le configuran.

Las cuentas permanentes recargables son mediante la activación de una cuenta de acceso (contrato), previo registro del usuario. Sus características son:

- Se activa con un saldo inicial mínimo.
- Modalidad prepago.
- Recargable.
- Ciclo de vida dependiente de la validez del saldo depositado mediante recarga el que se adiciona al disponible.
- La política de acceso a la navegación será implementada por tiempo.

El contrato de la Cuenta de Acceso Recargable (CAR) se identificada por los siguientes datos (atributos):

- Contrato: Documento legal que se entregará al usuario que contrate cualquier modalidad del servicio permanente.

- Número de contrato: Es el número que genera automáticamente GESNAUTA en el momento que el usuario contrata el servicio.
- Saldo Inicial Mínimo (recarga inicial): Es el dinero en efectivo que abona obligatoriamente el usuario en el momento de la contratación del servicio, con este saldo queda pre pagada y recargada la cuenta del usuario por primera vez. Este saldo tiene un período de validez que mantiene activa la cuenta de acceso. Las opciones de saldo dependen de la modalidad del servicio contratado y este podrá ser superior al fijado para cada modalidad.
- Nombre de usuario (login de acceso): Es el nombre que el usuario tendrá la opción de elegir, siendo único por servicio. Una vez ejecutada la acción de provisión del servicio no podrá ser cambiado por el usuario. Internamente en el InfoX-AAA se maneja un número de serie que se relaciona con el nombre de usuario.
- Nombre de Dominio: describe el alcance de la cuenta de acceso para la navegación y es definido y suministrado por ETECSA:
- navegación con alcance internacional–dominio @nauta.com.cu
- navegación con alcance nacional - dominio@nauta.co.cu
- Contraseña (password de acceso):Cadena de caracteres generada de forma automática por el *Módulo de Ventas*, cumpliendo los requisitos de *contraseña segura*. Se le entrega al usuario de forma impresa en texto claro formando parte del *contrato* (el sistema deberá cumplir con el requerimiento que solo se imprima una sola vez por cada contrato). El usuario tendrá la obligación, en la primera conexión, de cambiar la contraseña entregada, de lo contario no podrá acceder a la navegación. La contraseña que el usuario elija deberá cumplir con el requerimiento de *contraseña segura*.
- Fecha de activación CAR: Es el día (momento) en que se culmina el proceso de creación (comercialización) de la CAR al usuario. El usuario contrata el servicio y realiza obligatoriamente el depósito, en efectivo, de un *saldo inicial mínimo* equivalente a una recarga para un tiempo de conexión.
- Fecha de desactivación CAR: Es el período de tiempo máximo estipulado que transcurre entre una habilitación de saldo y otra. Se fija en “días naturales” y varía

en dependencia del saldo habilitado. Esta fecha coincide con la fecha de vencimiento del saldo (ya sea el *Saldo Inicial Mínimo* o el *Saldo de Recarga*).

- Fecha de expiración CAR (define el Ciclo de Vida de la CAR): Es el período de tiempo que se define para que el usuario realice la recarga obligatoria de lo contrario expira la cuenta de acceso, se define en días naturales: "330 días naturales posteriores a la fecha de desactivación de la CAR", es independiente del servicio contratado y del monto del último saldo de recarga depositado.

Al expirar la cuenta:

- El usuario pierde totalmente su cuenta de acceso, sin opciones de reintegro del saldo retenido. El sistema AAA libera la licencia y podrá generarse otra cuenta de acceso recargable.

Las cuentas temporales no recargables son aquellas que se adquieren mediante la compra de una tarjeta de acceso, sus características son:

- Modalidad prepago.
- Ciclo de vida 30 días posteriores a su primera conexión.
- La política de acceso a la navegación será implementada por tiempo.

Esta Cuenta de Acceso No Recargable (CAnR) es físicamente una tarjeta pre pagada con carácter "Temporal". Identificada por los siguientes datos (atributos):

- Número de Serie: Cadena de caracteres que se genera de forma automática y consecutiva y que diferencia una tarjeta de otra (es único por Tarjeta). Aparece impreso de forma visible en el reverso de la tarjeta que se comercializa.
- Nombre de usuario (*login* de acceso): Coincide con el número de serie de la tarjeta y es la cadena de caracteres que el usuario deberá teclear, junto con una contraseña, para acceder al servicio (es único por usuario). Aparece impreso de forma visible en el reverso de la tarjeta que adquiere el usuario.
- Nombre de Dominio: Describe el alcance de la cuenta de acceso, no será visible en la tarjeta y el usuario no lo tendrá que adicionar, pues el sistema lo deberá incluir

por defecto en el momento de la autenticación. Las cuentas de acceso no recargables siempre tendrán alcance internacional y utilizarán el dominio @nauta.com.cu

- Contraseña (password de acceso):El sistema la genera de manera automática (a cada tarjeta generada se le asocia una contraseña). Estará impresa en el reverso de la tarjeta de forma oculta bajo *scratch*.
- Fecha de activación CAnR: Es el día que se asocia el lote de tarjetas recibidos en el punto de venta al área de navegación a través del Módulo de Ventas.
- Fecha de expiración CAnR: Es el periodo de tiempo, 30 días "naturales"después de la primera conexión, que tiene el usuario para consumir el tiempo de acceso (1hora o 30 minutos) que viene referido en la tarjeta que adquiere, esta fecha es independiente al saldo que se prepaga por la tarjeta. A partir de aquí se libera la licencia en el AAA y puede ser generada nuevamente otra cuenta de acceso no recargable.

En la siguiente figura se muestra un ejemplo de una tarjeta pre pagada temporal.

Fig. 2.4 Tarjeta pre pagada de acceso a Internet.

2.6 Características del equipamiento utilizado en la red

El equipamiento utilizado en la red es de una gran variedad de marcas debido a que en algunos lugares los AP se encuentran en instalaciones hoteleras y son propiedad del lugar. Entrelasmarcas existentes en la red podemos mencionar Browan, Huawei, TP-LINK, Trendnet, Lobometrix, entre otras. En estos momentos existen dos sistemas para las redes inalámbricas implementadas, el sistema para las redes inalámbricas de terceros (en lugares

turísticos) y el sistema para las redes WiFi públicas (las implementadas en los parques principales de las ciudades). Las redes de terceros están compuestas fundamentalmente por equipamiento de la marca Browan y las redes públicas exclusivamente con equipamiento de la marca Huawei.

2.6.1. Access Point Exterior Browan modelo 2251

BW2251 es un punto de acceso para exteriores con un alto rendimiento y de ricas características. El AP es un dispositivo de alta potencia, robustez, resistente al agua, para ambientes exteriores, lo cual puede ayudar al operador a desplegar a gran escala la red inalámbrica. Puede ser controlado por un controlador de acceso inalámbrico con un sistema de autoconfiguración, el cual permite administrarlo centralmente, monitorearlo, provisión automática y auto configuración que reduce el despliegue, la administración y el costo de operación.

Características:

- Soporta servidor de administración para auto configuración
- Dos radios, soportando 802.11b/g/n y 802.11a/n (2.4GHz y 5GHz)
- Soporta protocolo de administraciónTR-069
- Soporta WPA/WPA2
- Soporta VLAN ID por BSSID - 'AP Virtual'
- Anti Interferencia con asignación dinámica de canales (*Dynamic Channel Allocation* (DCA))
- Privacidad Equivalente al Cable (*Wired Equivalent Privacy* (WEP))con clave de 64 o 128bits
- Soporta autenticación802.1x usando EAP-TLS, EAP-TTLS, PEAP y SIM
- ACL con control de acceso MAC, control de sesión, Nat/Pat
- QoS : ToS, DSCP
- *Isolation* en la capa 2 previniendo que clientes inalámbricos se comuniquen con otros.
- DHCP: servidor y cliente

- Autenticación por RADIUS y servidor Proxy
- Soporta simultáneamente 802.11b/g/n y 802.11a/n.
- Soporta abastecimiento integrado de energía IEE802.3 PoE de fácil instalación en varios ambientes que reduce el costo.

2.6.2. Controlador de acceso Browan modelo BG6020G

El controlador de acceso BROWAN modelo BG6020G es un dispositivo con alta capacidad de carga y conexiones de red flexible (puertos a 1Gbpsde fibra óptica y puertos Ethernet de cobre 10/100/1000Mbps). El BG6020G tiene varias funciones de servicio de Internet público, como son AAA, ruteo IP y funcionalidad VPN.

Funcionalidades de BG6020G:

- Múltiples métodos de autenticación: BG6020G soporta varios métodos de autenticación segura incluyendo el portal cautivo, 802.1x/EAP, autenticación MAC, y RADIUS. Cuando usa el método de portal cautivo, todos los usuarios y contraseñas son aseguradas sobre SSL. EAP puede ser usado directamente sobre 802.1x vía servidor RADIUS o residir la autenticación EAP sin el punto de acceso de la LAN inalámbrica.
- Contabilidad: para la facturación la información de contabilidad es reenviada instantáneamente, el volumen de transferencia de datos grabados por el BG6020G es en tiempo real. La información será reenviada a la red del operador central a través del servidor RADIUS. Se puede implementar una amplia variedad de planes de factura desde tiempo pre pagado, transferencia de datos pre pagada, suscriptores pos pago, pago por usuario y tarifa plana.
- Integración: BG6020G es completamente basado en interfaces y protocolos estándares, cumple con las recomendaciones de la WiFi Alliance, interoperable con servidores RADIUS y servidores Web. Por seguridad, las funciones AAA y el tráfico de administración del operador central de la red pueden ser tunelizados y encriptados por una VPN interna.

- Sin necesidad de configuración en el suscriptor: BG6020G hace que el acceso a Internet sea muy sencillo. Los suscriptores son re direccionados automáticamente a una web sin necesidad de configuración en la PC.
- Administración Remota: El BG6020G puede ser administrado vía SNMP, http(s), SSH o telnet, o vía puerto serie.
- Política de aislamiento (*isolation)* entre AP: De esta forma se limita la comunicación entre clientes de distintos APs.

Características:

- Autenticación de usuarios con UAM (*Universal Access Method*), 802.1x/EAPoLAN y MAC
- Cliente AAA RADIUS y servidor proxy con soporte EAP
- Soporta *Universal Address Translation* (UAT) y proxy web
- Compatible el *log-on* WISPr vía navegador web con SSL/TLS
- Soporta "lista blanca" (sitios web libres de costo o de autenticación)
- Soporta XML(interna o externa) para las páginas de bienvenida, *log-on* y *log-off*
- Re direccionamiento de correo electrónico
- Ruteo IP con IPSEC y PPTP pasando a través de NAT/NAPT
- Administración de ancho de banda por usuario mediante RADIUS
- Protocolos WAN: PPPoE, PPTP, clientes DHCP
- Funcionalidad de servidor DHCP o de redirigir las solicitudes a un servidor DHCP Relay.
- Cliente VPN: PPTP/MPPE, GRE
- Subred de administración para la administración remota de AP
- Soporta VLAN
- Soporta múltiples pools IP por LAN/VLAN
- Administración remota por SNMP v1, 2c, proxy SNMP, http(s), SSH, telnet, consola
- Mecanismo de N+1
- Más de 1000 usuarios concurrentes

2.6.3. Access Point Exterior Huawei modelo WA251DK

El AP Huawei modelo WA251DK-NE es un AP exterior de alto rendimiento:

- Cumple con los estándaresIEEE 802.11a/b/g/n.
- Usando antenas inteligentes integradas, el AP soporta 3x3 MIMO-OFDM y dos bandas de frecuencias: 2.4 GHz y 5GHz.
- Proporciona razones de más de 450 Mbps por cada módulo.
- Soporta switch PoE+ y/o adaptadores DC/PoE+.
- Es diseñado para proveedores de servicios de Internet (ISPs) y empresas desarrolladoras de grandes redes.
- La administración y mantenimiento del AP es simple, el WA251DK-NE automáticamente administra los canales y la frecuencia ajustando y soportando en servicio un rápido *roaming*.
- En exteriores el AP proporciona una alta potencia, soportando amplias áreas de cobertura y altas razones de transmisión.
- En el acceso a la red IP soporta varios protocolos incluyendo direcciones IP estáticas y Protocolo Dinámico de Configuración de Host (DHCP)
- Provee varias características de seguridad de red, como son defensa de DoS y DTLS (*Datagram Transport Layer Security*).
- Soporta sistemas abiertos de autenticación, incluyendo encriptación y varios métodos de autenticación como son Infraestructura de Autenticación y Privacidad deWLAN (WAPI), WEP, WPA y WPA2.
- Descubre automáticamente el controlador de acceso y levanta configuraciones cargadas por éste.
- Automáticamente ajusta canales y frecuencias para implementar balance de carga.
- Soporta *roaming* sin interrumpir el servicio.
- El AP soporta ser administrado por un AC y *plug-and-play*.
- Soporta monitoreo en tiempo real por un sistema de administración en red (NMS).

Funcionalidades del AP WA251DK

- Análisis del espectro y detección de interferencias: Escanea el espectro en el ambiente de su radio en tiempo real, detecta interferencia, identifica el tipo de

interferencia, y proporciona un reporte de alarma para visualizar la calidad de la red y mejorar la operación y mantenimiento de la red.

- Supresión de usuarios con baja razón de velocidad: coloca umbrales para reducir el tiempo de usuarios con baja razón de velocidad que son programadas y la duración en el cual los usuarios con baja razón ocupan recursos de interfaces inalámbricas. De esta forma, los restantes recursos de estas interfaces pueden ser asignados a usuarios de razones altas, haciendo uso completo de los recursos y mejorando la capacidad del sistema sin afectar usuarios de poca razón de velocidad.
- Navegación inteligente de bandas de frecuencia: Cuando una estación terminal(STA) doble banda es cubierto por un AP que trabaja en la banda de 2.4 GHz y un AP que trabaja en la banda de 5 GHz, el STA es asociado preferiblemente con el AP que trabaja en la banda de 5 GHz para aliviar el tráfico del AP que trabaja en la banda de 2.4 GHz. De esta forma, los recursos de las dos bandas son utilizados completamente.
- Balanceo de carga inteligente: Si múltiples APs cubren un STA, el AC decide a cual AP se conectará el STA, basándose en la carga de los AP, como es el número de STA asociados o el tráfico.
- Hotspot 2.0: apuntando a usuarios con celulares de alta gama, usa el estándar IEEE 802.11u para proporcionar seguridad en el acceso WiFi, aliviando el tráfico en la macro red, y aumentando la lealtad de los usuarios hacia los operadores. Soporta Hotspot 2.0-IEEE802.11u descubriendo redes automáticamente y seleccionándolas, utilizando autenticación WPA2 y 802.1X EAP.

2.6.4. Controlador de acceso Huawei modelo MAG9811

Las tecnologías IEEE 802.11 de redes de área local inalámbricas (WLAN) han sido ampliamente usadas en redes de área metropolitanas (MANs) y redes empresariales. El MAG9811 es un controlador de acceso desarrollado por Huawei. Este es aplicable a controlar el acceso de redes MAN empresariales proporcionando altas velocidades, seguridad, y fiabilidad de servicios WLAN. El MAG9811habilita grandes capacidades, altos rendimientos, alta fiabilidad, fácil instalación y mantenimiento.

El MAG9811 proporciona una variedad de rasgos de WLAN, incluyendo AP *plug-and-play*, administración de radio frecuencia, localización de suscriptor, balance de carga, administración de calidad de servicio de los AP, *roaming*, administración de suscriptores inalámbricos y defensa contra ataques.

Funcionalidades:

- Grandes Capacidades y alto rendimiento: Administra más de 4096 APs y soporta más de 96000 suscriptores concurrentes. Soporta *roaming* rápido para suscriptores WLAN.
- Fiabilidad de diseño de telecomunicaciones: la MPUs trabaja en modo 1+1. Redundancia en los componentes claves como los módulos de energía, los módulos de fan, relojes y bus de administración. Protección contra instalaciones de tarjetas en slot incorrectos. Redundancia 1:1 de los sistemas de energía con 2 *subrack* de AC o DC.

Funciones del sistema de mantenimiento y administración:

- Dos modos de autenticación de usuarios: autenticación local y autenticación RADIUS.
- Interfaces del sistema de administración dentro y fuera de la red (NMS).
- Operaciones simultaneas para múltiples usuarios.
- Interfaz de información en capa 2 y capa 3.
- Administración de alarmas críticas, clasificación de alarmas y filtrado de alarmas.
- Interfaz espejo: el MAG9811 proporciona la función de interfaz espejo para ver paquetes específicos por esta interfaz. Los paquetes supervisados ayudan en la ingeniería del mantenimiento y pueden ser analizados por los operadores de la red.
- Sistema de prueba y diagnóstico: el MAG9811 proporciona la función de habilitar un registro de informaciones sobre eventos claves, procesamiento de paquetes y estado de los servicios en un tiempo especificado. El MAG9811 proporciona además la función de detección y diagnóstico de traza. Cuando el sistema es reinicializado por defecto esta traza ayuda a localizar y rectificar la falla.

2.7 Vulnerabilidades de la red WiFi de Etecsa

Este diseño de red tiene grandes desventajas por la cantidad de vulnerabilidades que presenta en cuanto a protección de la red a ataques y en cuanto a la protección de los datos del cliente. Una de sus desventajas es que no implementa ningún mecanismo de seguridad e integridad de los datos entre el cliente y el AP, esta comunicación puede ser vista por un atacante que con alguna herramienta de escucha puede conocer la clave de un cliente y usarla sin pagar el servicio. Uno de los ataques a los que puede ser víctima es a ¨Man in the Middle. En este ataque un atacante intercepta y modifica los datos de la comunicación para así suplantar la identidad de las entidades implicadas en la comunicación. Puede escuchar todos los mensajes intercambiados entre las partes e incluso modificarlos y volver a enviarlos, implicando esto que los extremos sigan creyendo que se están comunicando con el extremo legítimo (Figura 2.5).

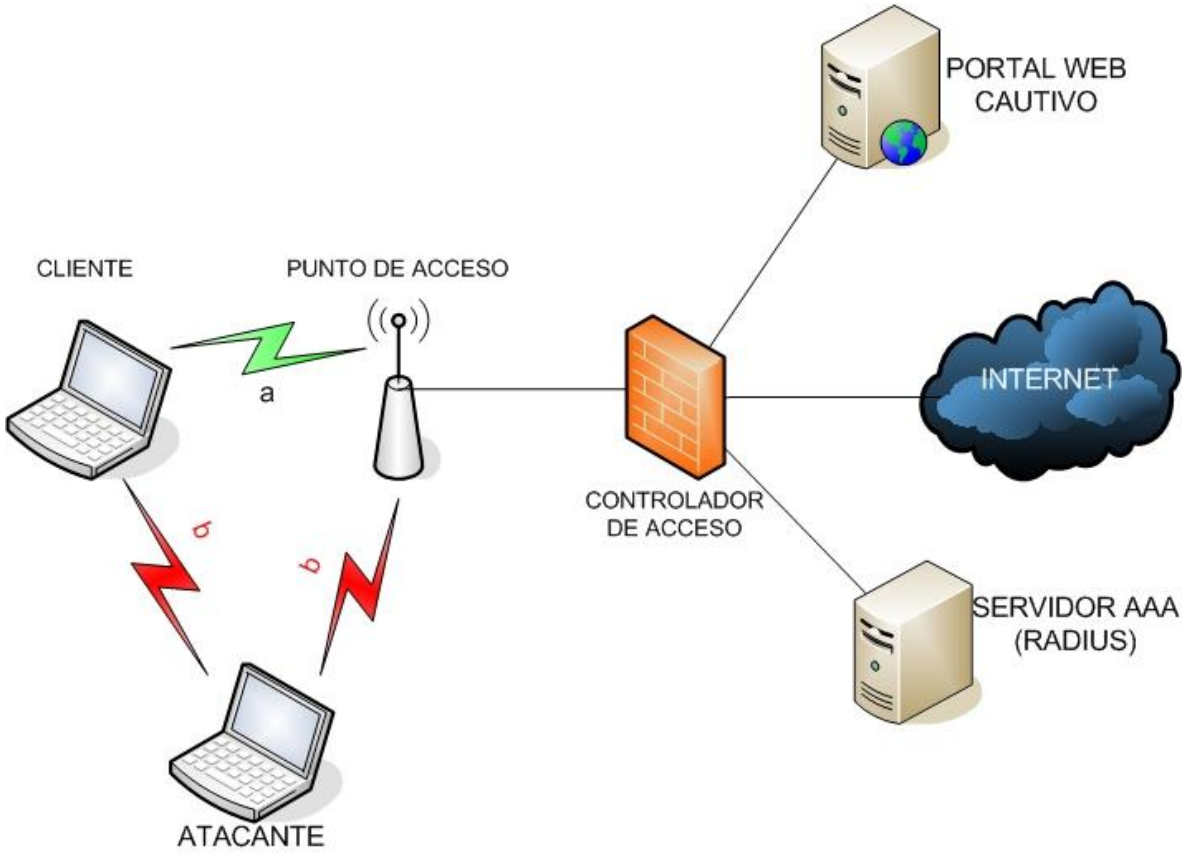


Fig. 2.5. Ataque MITH. a) Tráfico normal entre el cliente y el AP. b) Tráfico interceptado por el atacante.

Otra de las vulnerabilidades es que los clientes se conectan a la red a nivel IP libremente sin autenticación, esto les da la posibilidad de realizar ataques que para ser exitosos solo necesiten estar conectados a la red, si un atacante realiza un ataque sin haberse autenticado en la web queda impune, ya que el sistema no guarda trazas a nivel de conectividad. Como el cliente se conecta a la red sin autenticación el mismo puede que nunca abra un navegador web y sin embargo estar haciendo uso de la red con otro tipo de aplicaciones como lo son juegos en red, transferencia de ficheros, entre otras, todo esto sin pagar el servicio y saturando de trafico los recursos de la red (AP, AC, enlaces) (Figura 2.6).

Con la estructura existente se derrochan direcciones IP del rango de direcciones DHCP. Cuando el cliente se conecta a la antena adquiere una dirección IP que la mantiene mientras tenga el WiFi encendido de su dispositivo, aún cuando no esté navegando, esto ocurre muy a menudo puesto que la mayoría de los dispositivos vienen con conexión automática a la red inalámbrica. Esto provoca además un aumento en la red de tráfico de *broadcast* por usuarios que no están haciendo uso del sistema.

Uno de los ataques a los que está expuesta esta red es a ataques al servidor DHCP con herramientas como DHCP Ack Inyector que hacen un mal uso del protocolo DHCP (IP Spoofing Attacks, Discover DoS attacks, etc.).

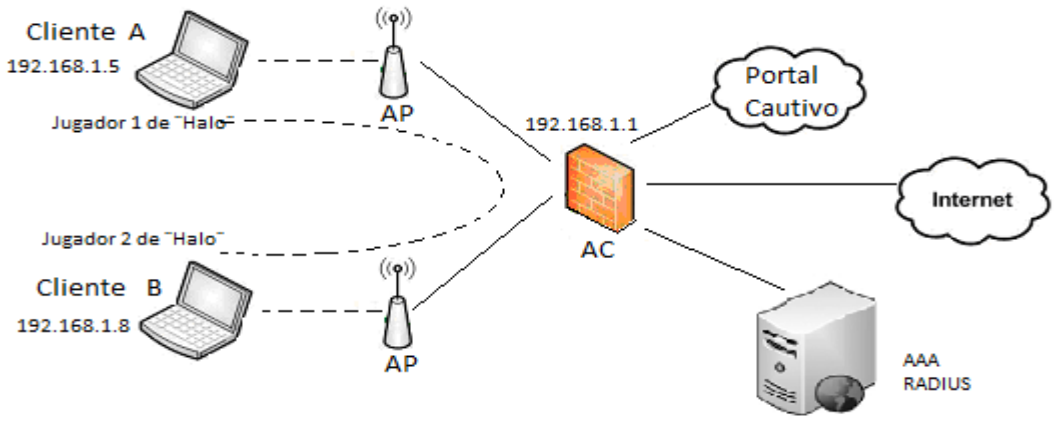


Fig. 2.6. Aplicaciones que corren sin autenticación.

Entre las vulnerabilidades de este sistema está que no se usa HTTPS con certificado de seguridad dado por una entidad certificadora. Al estar el portal sin certificado de seguridad

cualquier mal intencionado podría falsear el portal, hacer una copia del mismo y levantarlo en la red logrando que los clientes se autentiquen en el portal falso, esto podrían usarlo para robar contraseñas a los clientes.

2.8 Importancia y Necesidad de los Sistemas de Detección de Intrusos

La falta de conocimiento en torno a los sistemas de detección de intrusiones hace que en ocasiones sean malinterpretados, lo que genera confusiones con respecto a lo que realmente puede hacer y lo que no. A pesar de que son de gran ayuda en materia de seguridad, no son la solución definitiva a todos los problemas.

Los sistemas de detección cuentan con métodos para monitorizar y analizar tanto los eventos de sistema como el comportamiento de los usuarios, extrayendo los datos más relevantes de entre grandes cantidades de eventos de auditorías, lo que facilita considerablemente el trabajo del administrador o auditor de seguridad. Para lo que suelen usar diversos métodos como la reducción de auditoría, o técnicas de filtrado estadístico. En su mayoría proporcionando no sólo métodos para registrar su propia actividad, sino que permiten emitir informes sobre los eventos más importantes ocurridos en un determinado periodo de tiempo.

Brindan información continua sobre el estado del sistema, en algunos casos son capaces de crear un modelo inicial y compararlo con los cambios posteriores respecto a este invariable. En este aspecto se incluyen los casos en que se usan algoritmos de cifrado para determinar si ha habido cambios en el sistema de ficheros, denominados verificadores de integridad.
De forma limitada pueden establecer patrones de relación entre ataques o comportamientos similares, mostrados desde distintas máquinas para así determinar si el atacante es la misma persona o si se trata de un ataque coordinado.

Los IDS basados en la detección de usos indebidos, pueden reconocer ataques que coincidan con los patrones que almacenan en su base de conocimiento. Normalmente usan técnicas estadísticas para elaborar patrones de actividad y contrastarlos con la actividad

normal, detectando posibles anomalías. Aunque poco desarrollado en la práctica, este enfoque tiene ilimitadas posibilidades.

Los analizadores de vulnerabilidades, permiten comprobar la seguridad de la configuración de un sistema. En ocasiones esto se hace lanzando ataques conocidos contra el objetivo, para evaluar sus reacciones. Otra de las formas de descubrir vulnerabilidades consiste en repasar automáticamente la configuración del sistema, en busca de debilidades en las políticas de seguridad.

La mayoría de los productos de detección de intrusiones actuales usan mecanismos de análisis y registro en tiempo real. Comunican además alarmas a los responsables cuando se produce una intrusión. Las opciones para hacer esto son variadas, pudiéndose por ejemplo, registrar un evento de sistema, enviar una notificación vía correo electrónico o mensaje SMS, por solo mencionar algunos.

Las características de detección automática, así como contar con una interfaz fácil de usar hace que muchos IDSs, permitan incluso a usuarios no expertos en seguridad, mejorar de forma sensible la seguridad de sus sistemas. Debido a su sencillez de uso, proporcionan información sobre las políticas de seguridad por defecto así como métodos para corregir los posibles errores de configuración de forma automática.

Los niveles de seguridad y estabilidad que se brindan en la red WiFi de ETECSA son aceptables, sin embargo no existe la forma de detectar ataques provenientes de los usuarios internos hacia cualquier elemento de la red o incluso hacia otro usuario de la misma. Se pasa por alto todo tipo de información que se genera localmente como eventos de seguridad así como también los paquetes que se conmutan en nuestros segmentos de red. Debido a que resultan cantidades alarmantes y resulta imposible examinar por inspección manual. De donde se deduce la necesidad de implementar un sistema capaz de analizar cientos de miles de eventos de seguridad, y cientos de miles de paquetes de red para determinar posibles intrusiones a la seguridad de los sistemas en explotación.

2.9 Conclusiones parciales

El despliegue de una red WiFi es una realidad en la provincia de Villa Clara. Diariamente miles de usuarios aprovechan las ventajas y posibilidades de este servicio para comunicarse con sus familiares, mejorar su nivel profesional o simplemente por diversión.

El impacto ha sido enorme desde el punto de vista social.

Debido a que este proceso empezó casi desde cero el despliegue no ha estado libre de errores. El hecho de ser una tarea con recursos centralizados también ha limitado un poco la capacidad de innovar y de adaptarse a las condiciones específicas de los lugares por parte del personal de Etecsa de la provincia. Es por esto que se puede decir que persisten problemas e insatisfacciones que podrían ser eliminados o minimizados con el objetivo de lograr una red más eficiente, segura y cómoda para los usuarios. Estas propuestas se estarán tratando en el próximo capítulo.

Capitulo 3 Evaluación y análisis de una propuesta de arquitectura para la red WiFi de Etecsa

3.1. Introducción

Las redes públicas de acceso a Internet, en especial las inalámbricas, están expuestas a disímiles ataques, ataques que pueden explotar las vulnerabilidades propias del medio físico como también aquellos que buscan alterar el servicio en busca de beneficios propios. En las redes inalámbricas utilizadas para brindar este servicio es muy importante la estabilidad de las mismas, a partir de esta consideración, los clientes escogerán o no esta vía de conectividad, las pérdidas económicas por este concepto pueden ser numerosas. De ahí la importancia de mecanismos eficientes de seguridad que el Proveedor de Servicios Etecsa necesita implementar y así poder brindar un servicio con alta calidad.

Para darle solución a los problemas expuestos en el capítulo anterior de la red WiFi existente se propone una arquitectura y una configuración más segura, con lo que se pueden evitar ataques a la misma y proteger a los clientes legítimos de la empresa que hacen uso del servicio.

En este capítulo se realizarán pruebas que demuestran las vulnerabilidades de la red WiFi de Etecsa. Para evitar la ocurrencia de acciones que exploten estas debilidades se propone un diseño que garantice una mayor seguridad a la red y a los clientes. En el capítulo se describe la arquitectura escogida especificando cada una de las ventajas alcanzadas. Además se propone una herramienta que permita detectar, avisar y actuar ante ataques o intentos de intrusión en la red.

3.2. Vulnerabilidad Red Abierta

Entre las debilidades de la red existente está que no implementa ningún mecanismo de encriptación e integridad de los datos entre el cliente y el AP, esta comunicación se hace totalmente transparente, por lo que la información que circula en este segmento de red puede ser vista por otro cliente con un *sniffer* como Wireshark (Figura 3.1). Para poder

escuchar toda la información que circula por red WiFi se necesita una PC con una tarjeta de red inalámbrica que permita el modo monitor o promiscuo y un programa *sniffer* de red .

Entre las informaciones que un intruso puede obtener están las direcciones IP, direcciones MAC, nombre de dominio, nombres de recursos compartidos y direcciones de correo electrónico. Una forma de utilizar esta información por un atacante es cambiar la dirección física o MAC de la interfaz inalámbrica por una dirección MAC valida dentro del sistema atacado. Para hacer esto basta con capturar alguna MAC valida en el sistema, suplantarla dirección IP y MAC, realizar cualquier ataque al cliente verdadero para desconectarlo de la red y disfrutar de la conexión que tenía el cliente sin pagar el servicio. Para utilizar dicha dirección MAC se tendrá que esperar a que el usuario propietario de la MAC se desconecte, aunque también se puede ejecutar un ataque DoS contra él con el fin de expulsarlo de la red.

Como se puede ver en la figura 3.1, el *sniffer* muestra todos los datos de cada paquete que circula en la red. Para este ejemplo se capturó el tráfico con el programa Wireshark instalado en una laptop, se estableció la comunicación entre un teléfono y la antena WiFi, el teléfono obtuvo la IP 181.225.253.22 dada por la antena por medio del protocolo DHCP. Sin embargo toda esta comunicación entre el teléfono y la antena es escuchada por la laptop como muestra en la figura el paquete señalado en azul.

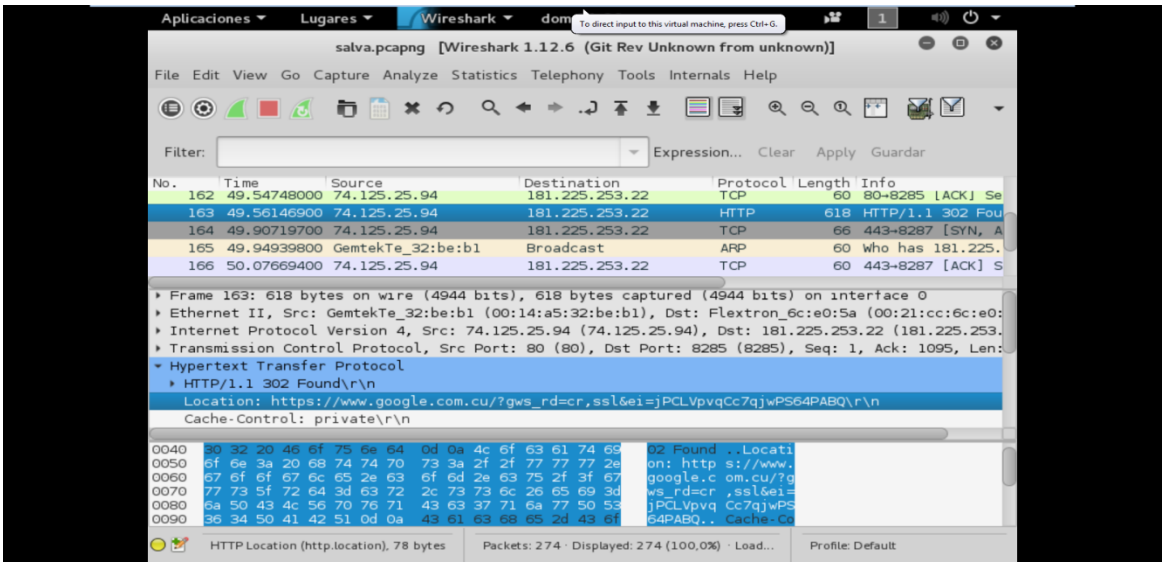


Fig. 3.1 Tráfico capturado por un *sniffer*.

3.3. Vulnerabilidad de suplantación

La ausencia de un certificado digital en la página de autenticación del sistema WiFi de Etecsa www.portalwifi-temas.nauta.cu puede ser aprovechada por atacantes, tanto para ataques de suplantación de los puntos de acceso como por la suplantación del portal en sí, simplemente con el objetivo de robar las contraseñas de acceso a la red.

Con las herramientas existentes en las redes es muy sencillo para un principiante suplantar o clonar una página web, la mayoría de estas herramientas son de rápida descarga y se encuentran gratis. Para la prueba se utilizara la herramienta Kali Linux la cual se puede encontrar en http://www.cdimage.kali.org. En el anexo 3 se muestran los pasos para clonar la página de autenticación del sistema WiFi de Etecsa.

Para suplantar la web www.portalwifi-temas.nauta.cu se utilizó la herramienta SET (*Social Engineering Toolkit*) que se encuentra dentro del paquete de Kali Linux. (Figura 3.2)

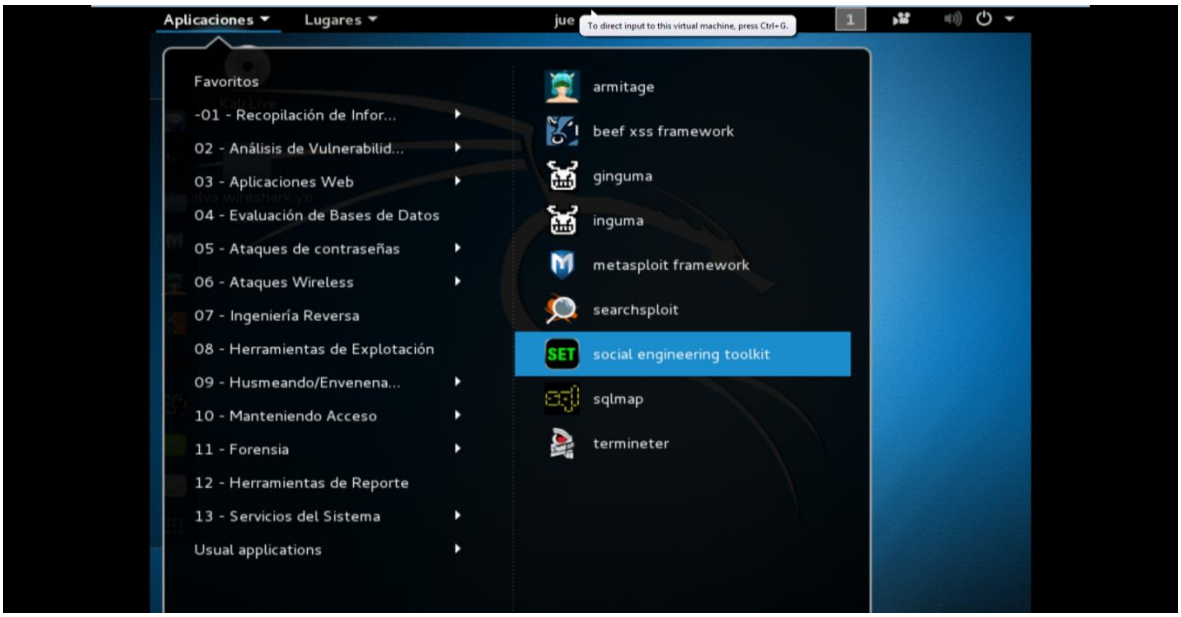


Fig. 3.2 Herramienta SET.

La PC que servirá de servidor web falso y en la que se va a instaurar el portal de autenticación clonado debe estar conectada a la red víctima, en este caso la dirección IP que obtuvo la PC es 181.225.253.3, dicha IP se configura como la IP donde va a radicar la web.

En la herramienta SET se copia la dirección de la página original para clonarla como se muestra en la siguiente figura.

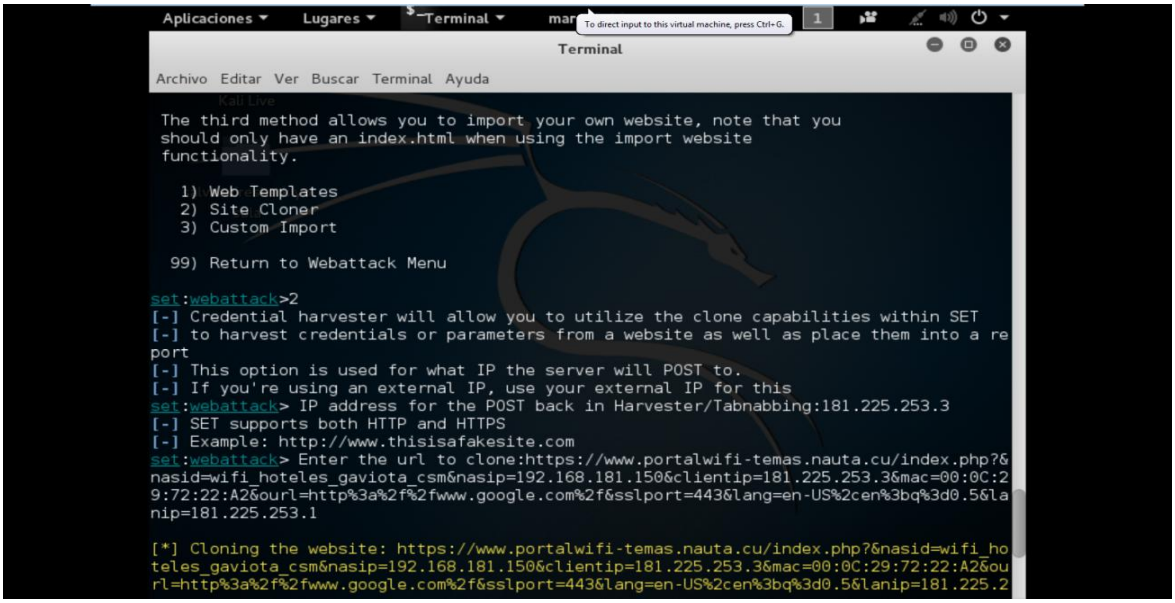


Fig.3.3 Selección de la página web a copiar.

Luego de tener la web clonada se necesita que los demás usuarios se conecten a la web falsa para que sea fructífero el robo de las cuentas. Una de las formas para que el resto de los clientes entren en la página simulada es realizar un ataque DNS *spoofing*, con este ataque se pretende que cuando un usuario realice una petición DNS la PC Kali le responda primero que el verdadero servidor DNS con la dirección IP de la web clonada.

Para realizar el ataque DNS *spoofing* se escogió la herramienta Ettercap que se encuentra dentro del paquete Kali Linux. Aprovechando que la web que se quiere clonar es un portal cautivo se crean en Ettercap los registros con las páginas más utilizadas por los clientes. Para este ejemplo se escogió www.google.com la cual está por defecto en la mayoría de los navegadores y el propio portal clonado. En la figura se expone un ejemplo de registros DNS modificados (Figura 3.4).

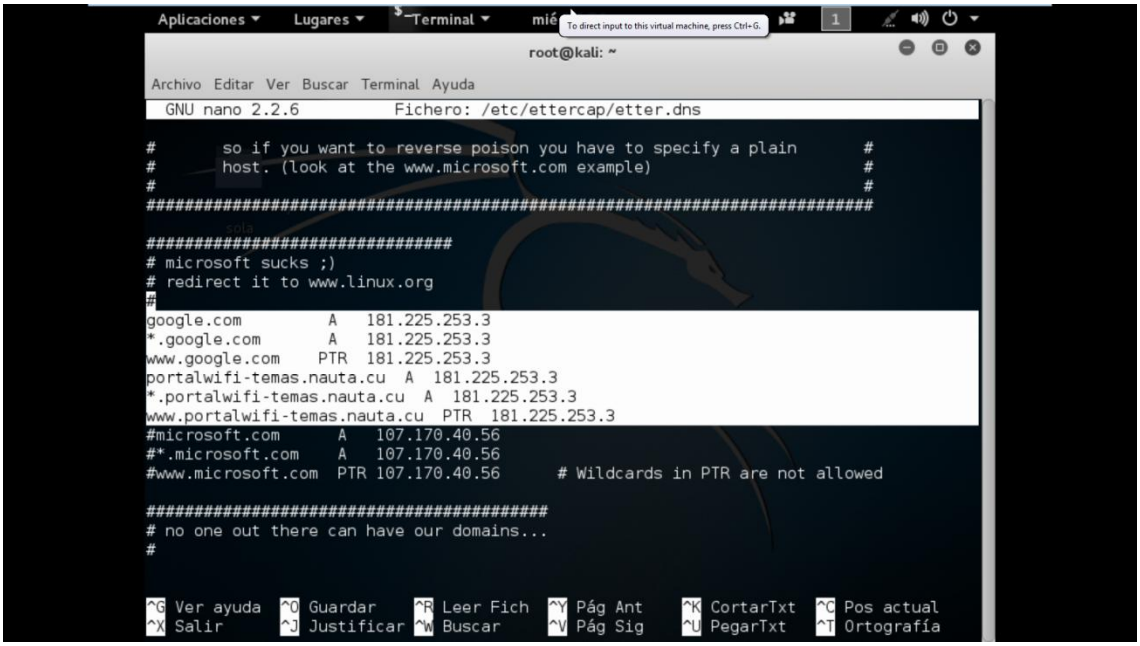


Fig. 3.4 Registros DNS modificados de Ettercap.

A partir de la ejecución del ataque *dns_spoof* de ettercap todos los clientes en dicha red que intenten acceder a www.google.com serán re direccionados al servidor web falso para que se autentique. Como la página original no tiene certificado digital el cliente está acostumbrado a acceder a una web con problemas de seguridad por lo que para el cliente no existe diferencia entre la página original y la falsa. (Figura 3.5)

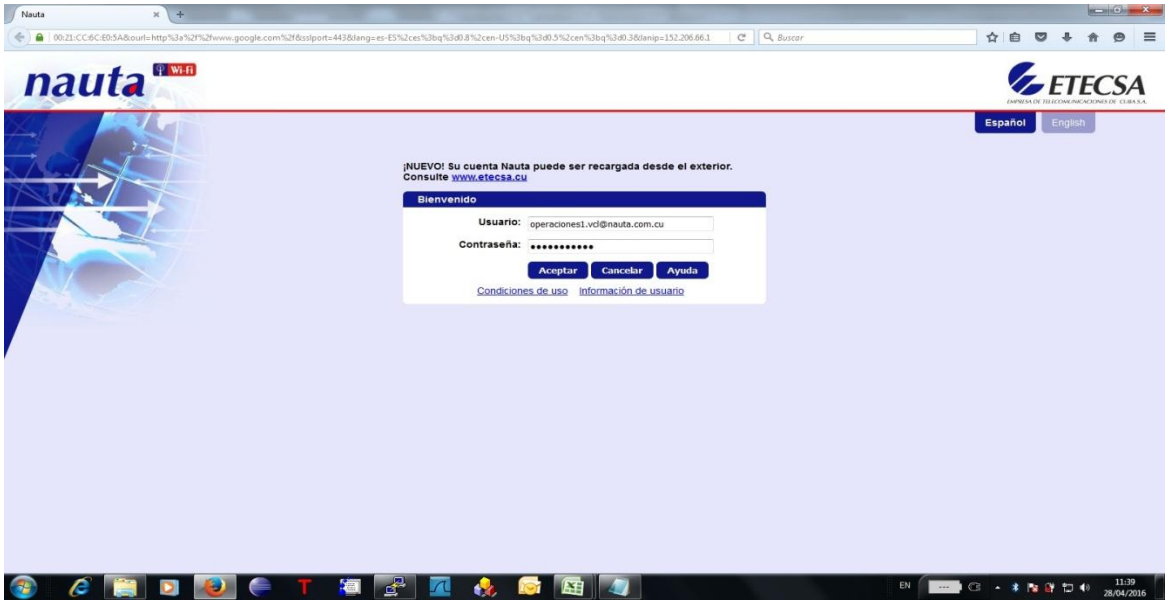


Fig. 3.5 Redireccionamiento a la web de autenticación falsa.

Cuando el cliente entra los datos en la web clonada se muestran en la PC Kali como se muestra en la figura siguiente.

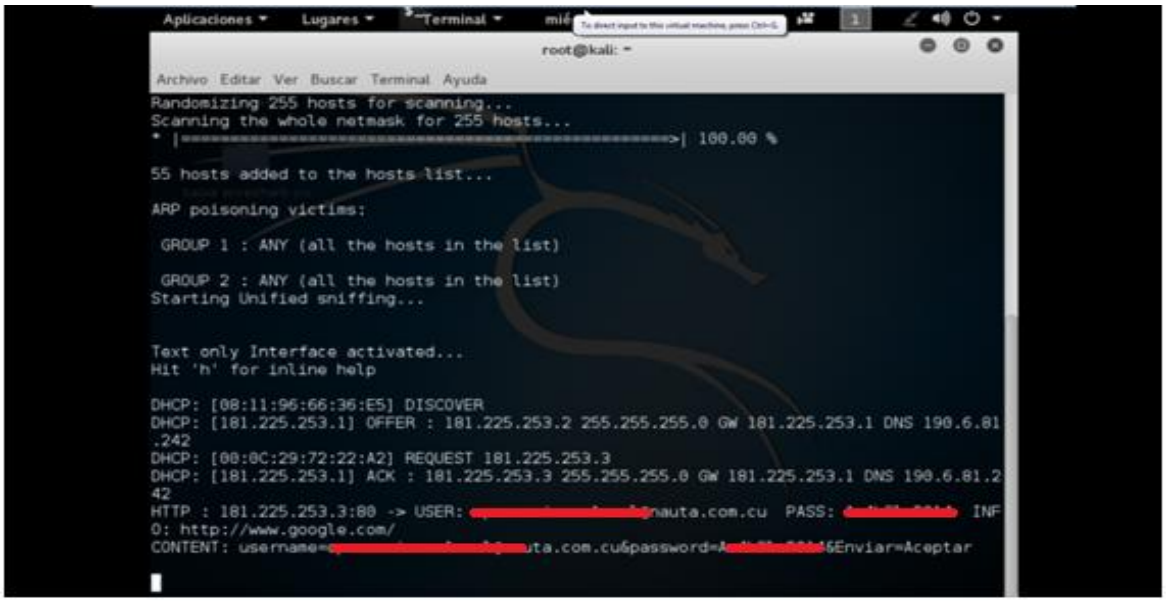


Fig. 3.6 Usuario y Contraseñas robadas.

Otra vía de redirigir el tráfico de los clientes al portal falso es duplicando el sistema, o sea, creando una antena WiFi con el mismo nombre que los AP originales, dicha antena WiFi puede ser un punto de acceso o creado en la misma PC. De esta forma el cliente se conecta al AP falso, obtiene una IP de este y es re direccionado a un portal físicamente idéntico al original. A partir de este punto la contraseña de la cuenta puede ser robada igual que en el ejemplo anterior.

Otra herramienta que se puede utilizar para suplantar el punto de acceso con un AP falso es Wifislax. Esta herramienta es muy sencilla de implementar, no necesita estar instalada en la PC, se puede ejecutar desde una memoria USB. Wifislax convierte la PC en un AP con el mismo SSID que la red que se va a duplicar (WIFI_ETECSA), el programa solo actúa como interceptor de la señal realizando un ataque de “hombre en el medio”. En la PC no se entregan direcciones IP por DHCP ni se falsifica el portal web cautivo, toda la comunicación se realiza entre el cliente y el sistema verdadero, el atacante solo escucha

toda la información que circula entre ambos extremos, conociendo así la contraseña de acceso del cliente.

Todo lo anteriormente descrito puede suceder sin que la gran mayoría de los clientes se den cuenta de la estafa a la que son objetos, en ambos casos el cliente solo ve la advertencia de un portal sin certificado, pero tanto la web autentica como la suplantada no poseen certificado digital, por lo que dicha advertencia no es suficiente.

3.4. Vulnerabilidad de red compartida

Para un proveedor de servicios que cobra por tiempo de conexión es importante garantizar que usuarios no autorizados no puedan revender el servicio compartiendo sus recursos de red. Compartir la conexión de la red provoca al proveedor que menos clientes paguen el servicio legítimamente, pero sobre todo el cliente que se conecta a través de otro cliente es el más afectado, paga por una conexión que no tiene garantizada una buena calidad de servicio, debido a que el proveedor garantiza por cliente una velocidad suficiente para acceder a cualquier servicio, pero a medida que sea compartida la misma se ve degradada.

Para compartir la red solo se necesita un equipo que admita la creación de un punto de acceso WiFi. Una de las formas de hacerlo sin programas es configurando la tarjeta de red inalámbrica de la PC como punto de acceso directamente por el ejecutor CMD, en el mismo elegimos el SSID y la contraseña, luego en la tarjeta de red elegimos la opción de uso compartido, permitiendo así que otros usuarios se conecten a través de la conexión a Internet del propio equipo (Figura 3.7).

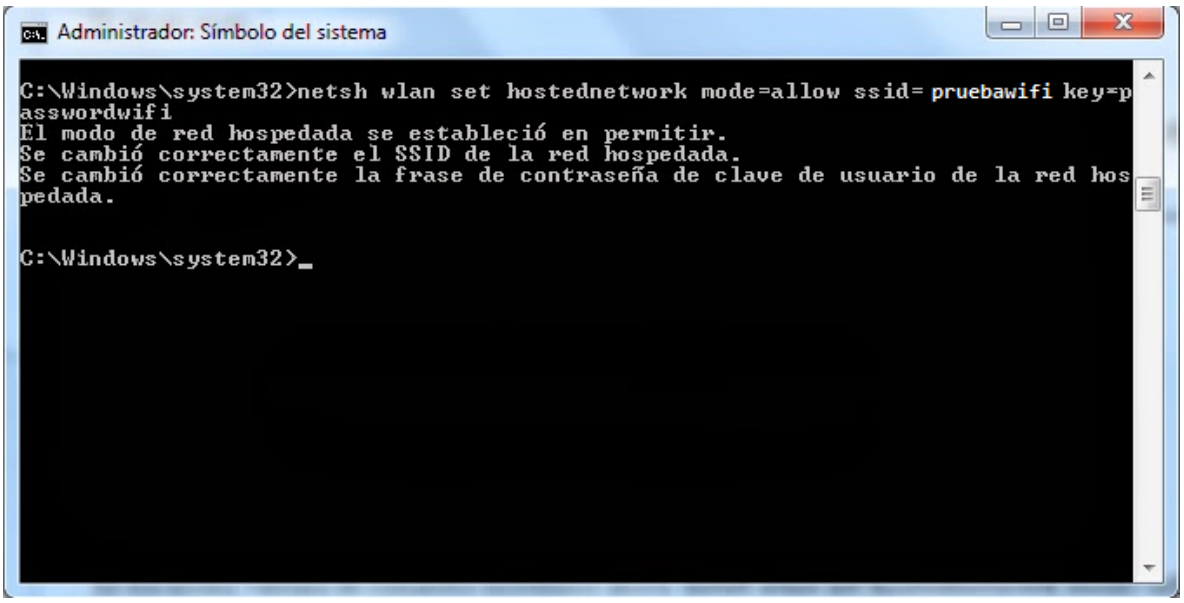


Fig. 3.7 Configuración de un punto de acceso en la PC.

Existen varias herramientas que permiten que usuarios sin ninguna experiencia en el área puedan compartir la red, entre ellas una de las más utilizadas es el Connectify (Figura 3.8). Por cada usuario la empresa de telecomunicaciones permite alcanzar un máximo de 1Mbps de velocidad, lo que depende de la congestión de la zona WiFi, lo que quiere decir que el cliente puede que no alcance 1Mbps. Si el cliente legítimo conecta a más clientes pasando a través de su tarjeta de red, dicha velocidad alcanzada por el cliente legítimo es dividida por todos los clientes conectados a través de él. Disminuyendo así la calidad del servicio para los clientes finales.

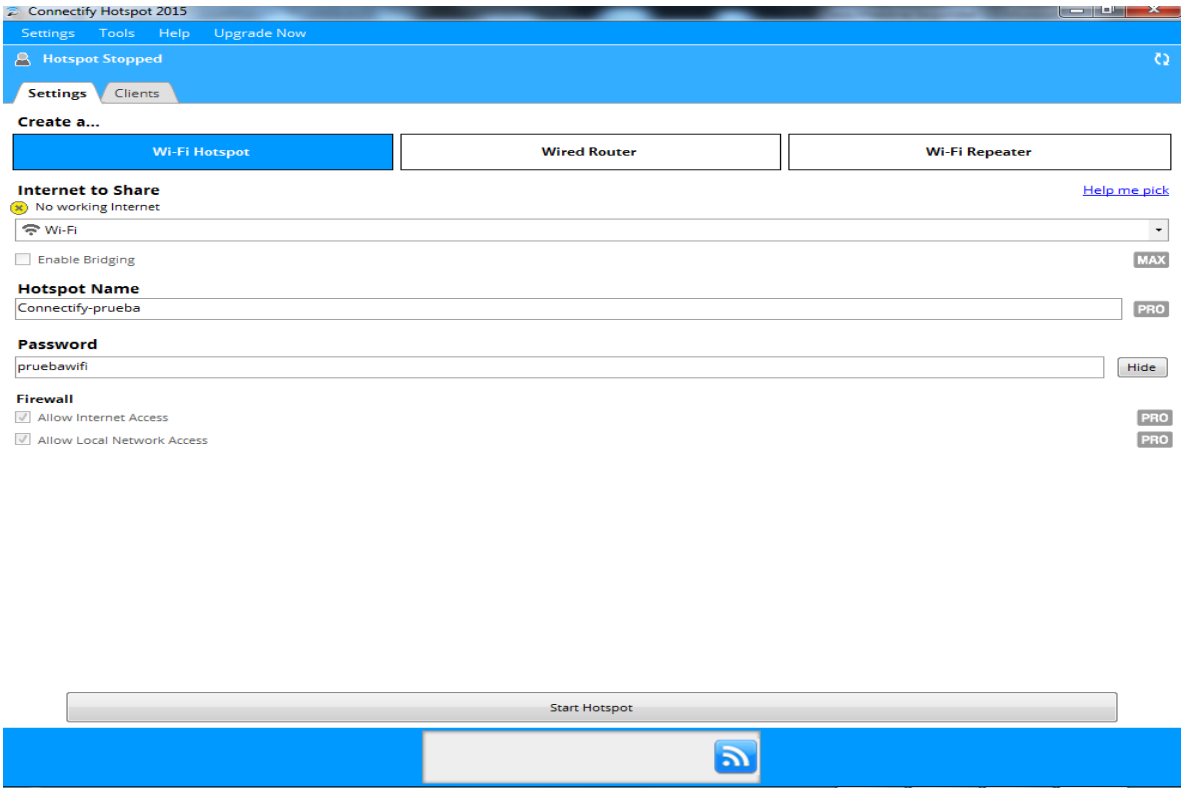


Fig. 3.8. Programa *Connectify* para compartir la red.

3.5. Vulnerabilidad de acceso mediante Túneles DNS

Los túneles DNS son muy utilizados para vulnerar la seguridad establecida, generalmente políticas de control de acceso, normalmente usado para evitar pagar el servicio de conexión. Los túneles DNS pueden ser útiles para las políticas de restricciones de protocolos, es decir, si no se puede usar ciertas aplicaciones o servicios como algún juego en línea. También para vulnerar los censuradores de alguna página Web específica, convirtiendo la PC en un Proxy Web sin restricciones que da acceso a todas las páginas Web accesibles, o a acceder transparentemente a Internet.

En el caso de la red WiFi de Etecsa son usados para violar la restricción de acceso, conectando al cliente a Internet sin la autenticación del mismo en el portal Web cautivo. Esto es posible ya que para el controlador de acceso el cliente solo está haciendo uso del protocolo DNS (Figura 3.9).Una de las formas de evitar los túneles DNS es la configuración de Listas de Control de Acceso (ACLs) que solo permitan el uso del protocolo DNS por los servidores DNS propios de la empresa de telecomunicaciones.

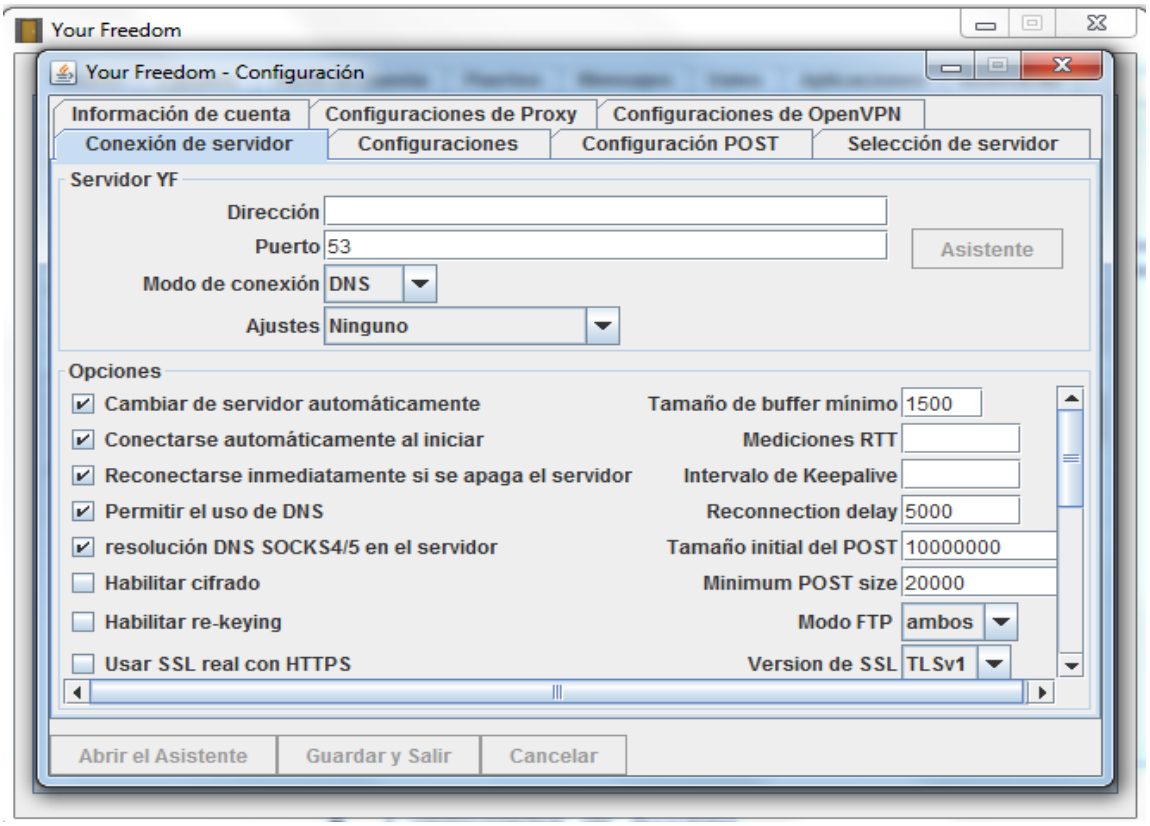


Fig. 3.9 Túnel DNS con el programa Your Freedom.

3.6. Propuesta de arquitectura de la red WiFi de Etecsa

3.6.1. Parte 1 – Propuesta de una arquitectura segura en el acceso a la redWiFi de Etecsa

Para eliminar las vulnerabilidades existentes relacionadas con el acceso a la red WiFi de Etecsa se propone la arquitectura mostrada en la figura 3.10, la cual está formada por:

- Cliente
- Punto de Acceso
- Controlador de Acceso
- Servidor RADIUS

Entre el cliente y el AP se escoge el protocolo de encriptación WPA2 (802.11i) en el modo empresarial contra un servidor AAA del tipo RADIUS. El Controlador de Acceso implementa el protocolo 802.1x para la autenticación en el sistema. El AC tiene un camino

conectado al servidor RADIUS para la autenticación y un camino hacia Internet al que solo tendrán conexión aquellos clientes a los cuales la autenticación haya sido exitosa, mientras el servidor RADIUS no envíe una respuesta de autenticación válida, el AC mantiene la conexión del puerto cerrada utilizando el protocolo 802.1x.

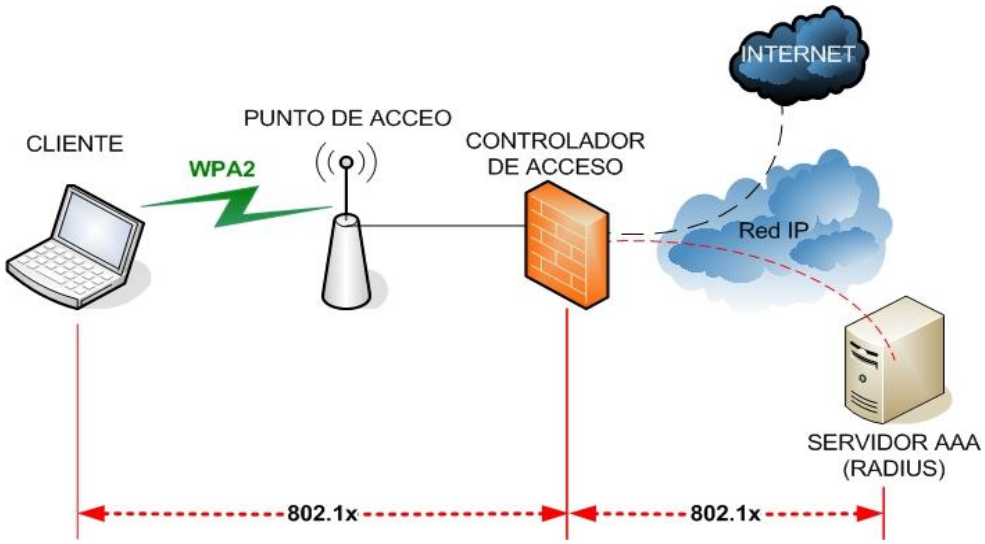


Fig. 3.10. Arquitectura de red propuesta.

3.6.1.1 Eliminación del portal cautivo

Una de las etapas que causa mayor incomodidad por parte de los usuarios es el proceso de autenticación en el portal cautivo. Eso pasa sobre todo con las personas que tiene una cuenta permanente y que acceden al servicio generalmente desde dispositivos móviles desde los cuales el uso del teclado no es algo tan simple como en una computadora portátil.

Dado que la política de la empresa Etecsa es que el número de cuentas permanentes se incremente, y, teniendo en cuenta que las credenciales de los usuarios no cambian tan frecuentemente, debería existir una variante en la cual los usuarios dueños de cuentas permanentes puedan conectarse a la red de forma más simple, o sea sin pasar por el portal cautivo.

Esto es posible usando el método de autentificación WPA2 *enterprise*.La implementación de este método no llevaría ninguna modificación en la infraestructura existente, básicamente se simplificaría (Figura 3.11).

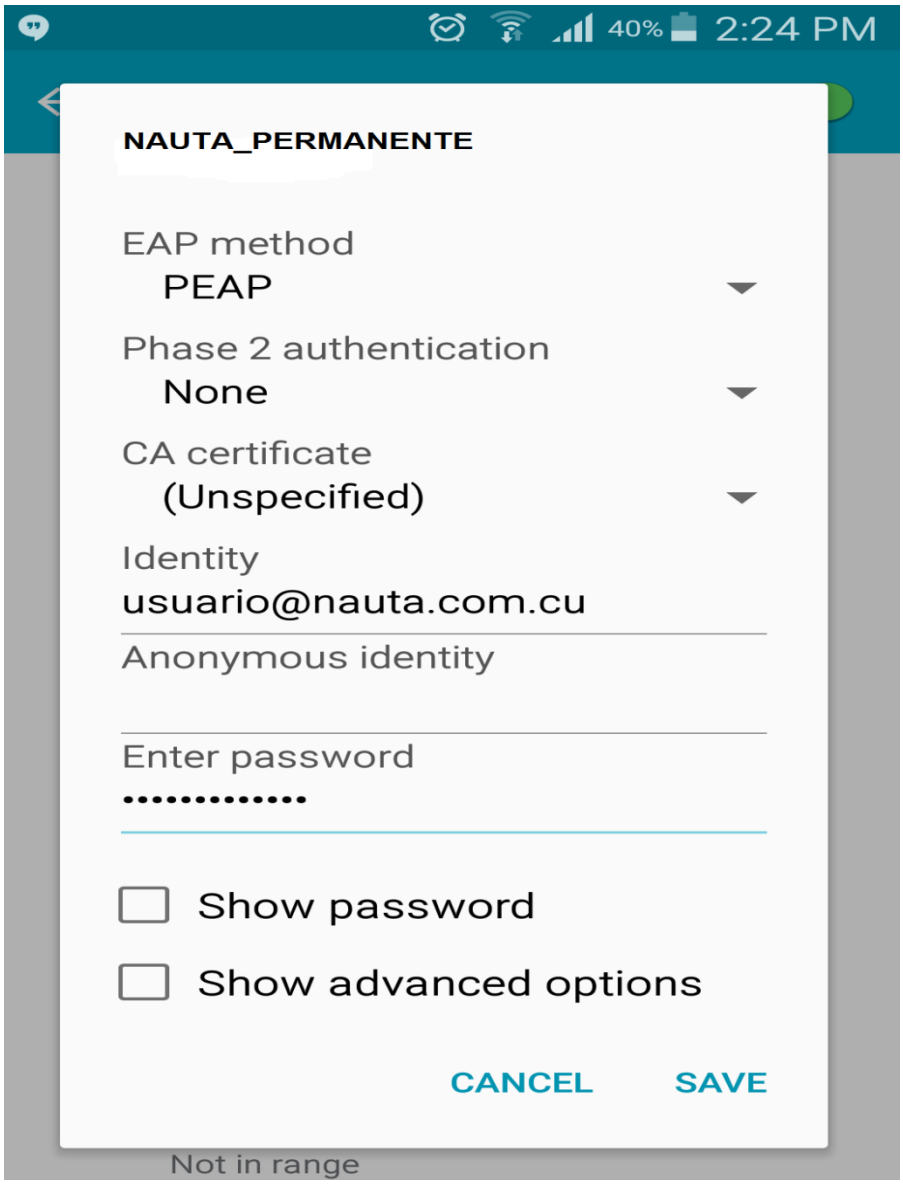


Fig. 3.11 Autenticación utilizando WPA 2 *Enterprise*.

Se podría hacer de forma gradual ya que en la mayoría de las zonas de acceso a la red WiFi de Etecsa se han instalado 3 puntos de acceso. Uno de ellos podría estar configurado con un SSID diferente como podría ser NAUTA_PERMANETE lo cual le indicaría a los usuarios

que es el que deben usar si desean tener una experiencia de conexión mucho más rápida y sencilla.

Al usar este método se podría lograr también una mayor seguridad en la transmisión de los datos y una mejor resistencia contra ataques de suplantación ya que nunca la contraseña sería enviada en texto plano como se hace con el portal cautivo.

3.6.1.2 Seguridad ofrecida por la configuración propuesta

La estructura propuesta elimina las vulnerabilidades en el acceso a la red descritas en la red inalámbrica actual:

- La comunicación entre el cliente y el AP es cifrada. Para lograr la integridad y autenticidad de los mensajes se propone el mecanismo de encriptación WPA2 (802.11i) empresarial, por su robustez ante los ataques y su dificultad para vulnerarlo, garantizando la protección de los datos entre el cliente y el AP.
- El sistema guarda trazas a nivel de conectividad. Con la utilización el protocolo 802.1x se obliga al cliente a autenticarse antes de conectarse a la red, de esta forma se hace posible que queden registradas las trazas por usuarios desde el momento en que se conectan a la red.
- Alta protección contra ataques de *spoofing.* Al estar la comunicación entre el AP y el cliente cifrada, el atacante no podrá conocer con un *sniffer* direcciones IP, direcciones MAC, nombre de dominio, nombres de recursos compartidos ni direcciones de correo electrónico.

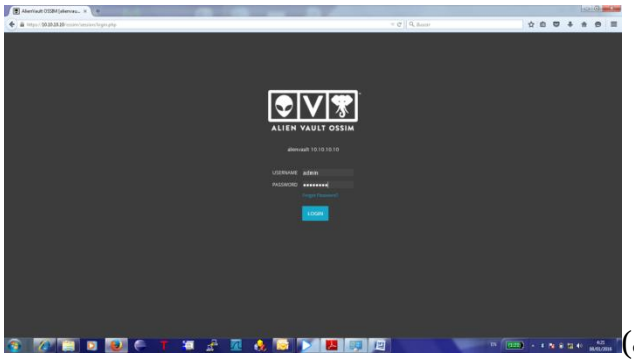
Elimina el robo de contraseñas por suplantación. Aunque un atacante inserte en la red un AP falso cuando el cliente se conecte al AP mandará la información cifrada y como el atacante no conoce la contraseña no podrá leer la información.

3.6.2. Parte 2 – Propuestade inserciónde un Sistema de Detección de Intrusos en la red WiFi

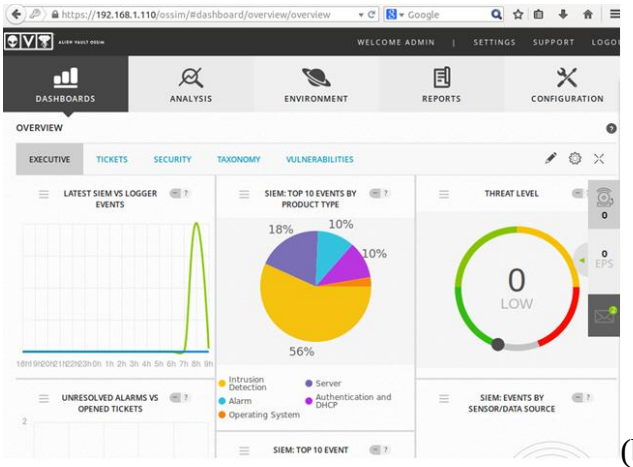
En toda red se necesitan mecanismos eficientes de seguridad que permitan la auditoria y el control de todo lo que este circulando en la misma. Para darle solución a los problemas de falta de registro en tiempo real del tráfico que circula, expuestos con anterioridad, se

propone insertar un IDS en la red WiFi, evitando ataques a la misma y proteger a los clientes que utilizan el servicio. Por las ventajas que ofrece y por ser libre de costo se escogió el IDS OSSIM como propuesta para su inserción en la red WiFi de Etecsa.

En la siguiente figura se muestra el OSSIM visto desde una web de gestión. Para ver los eventos de seguridad se abre un navegador web con la dirección IP, usuario y contraseñas del OSSIM, configurada en la instalación del mismo.



(a)



(b)

Fig. 3.12 Vista gráfica de OSSIM.

La arquitectura propuesta en la figura 3.13está formada por:

- Cliente
- Punto de Acceso
- Sistema de Detección de Intrusos OSSIM
- Controlador de Acceso

- Servidor RADIUS

El IDS insertado (OSSIM) a la red es el encargado de detectar ataques provenientes desde el exterior (Internet) y ataques provocados por otros usuarios internos de la red. Para que el IDS sea capaz de detectar estas intrusiones necesita que por su tarjeta de red circule todo el tráfico, por lo que la tarjeta necesita estar configurada en modo promiscuo.

Para que al IDS llegue todo el tráfico el mismo debe estar conectado a un puerto del *switch*capaz de ver todo el trafico de la red, esto se conoce como puerto espejo. El puerto espejo es utilizado con un *switch* de red para enviar copias de paquetes de red vistos en un puerto del switch (o una VLAN entera) a una conexión de red monitoreada en otro puerto del *switch*. El puerto espejo en un sistema de *switch* Cisco se refiere a un analizador de puertos del *switch* (*Switched Port Analyzer; SPAN*) algunas otras marcas usan otros nombres para esto, tal como *Roving Analysis Port* (RAP) en los *switches* 3Com.

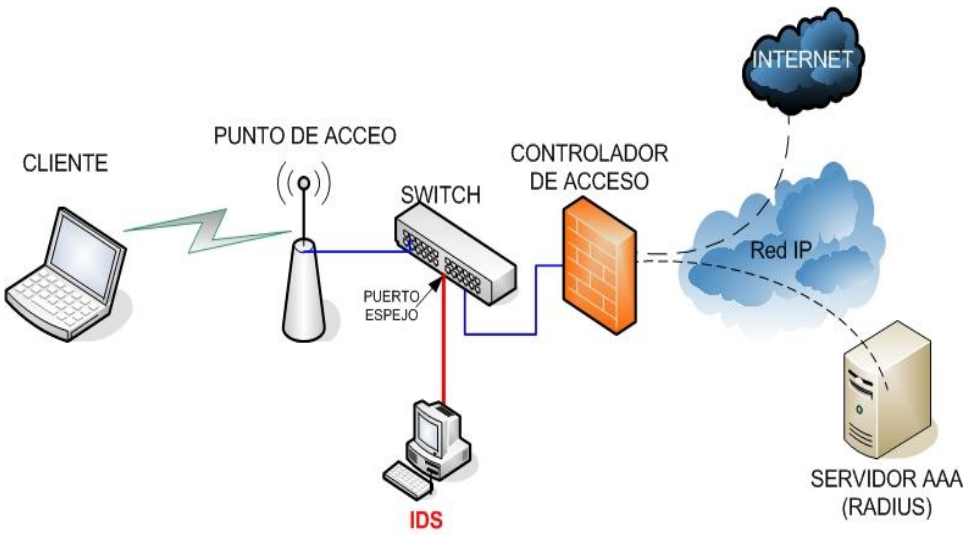


Fig. 3.13. Arquitectura de red propuesta con OSSIM.

Para generalizar la arquitectura descrita anteriormente se propone el OSSIM en una estructura de un solo servidor con múltiples sensores desplegados en varios sitios. Cada sensor es encargado de la recolección de eventos y monitoreo del sistema en el sitio en el que se encuentra. En esta configuración el monitor puede ser ubicado en una zona de la red

de gestión, atendido únicamente por los operadores de la red. Para disminuir los costos, dichos sensores se ubicarían solo en las zonas WiFi con mayor incidencia de ataques registrados.

3.6.2.1 Seguridad ofrecida por la configuración propuesta

Los IDS son un elemento fundamental en la infraestructura de seguridad de redes. En la configuración propuesta el IDS permite:

- Descubrir y castigar a un atacante y proveer información sobre las intrusiones que se están produciendo. Incluso cuando los IDS no son capaces de bloquear ataques, pueden recoger información relevante sobre éstos. Esta información puede, bajo ciertas circunstancias, ser utilizada como prueba en actuaciones legales. También se puede usar esta información para corregir fallos en la configuración de seguridad de los equipos. Como se muestra en la siguiente figura el IDS muestra los tipos de eventos ocurridos y los datos del mismo, MAC de la tarjeta de red, IP, fecha exacta en que ocurrió el evento, por lo que posibilita actuar como prueba de usos indebidos por un usuario de la red WiFi (Figura 3.13). Otra de las ventajas es que desde que el cliente se conecta a la red está siendo supervisado por el IDS, quedando trazas de todos los intentos de intrusión del mismo.
- Detectar preámbulos de ataques (normalmente pruebas de red y otras actividades). Un atacante puede examinar la red, sin embargo el IDS detectará estas pruebas, las identificará como sospechosas y podrá bloquear el acceso del atacante al sistema, avisando al administrador de la red de lo ocurrido para que tome las acciones pertinentes.

La estructura propuesta elimina las vulnerabilidades descritas en las redes inalámbricas mencionadas anteriormente. Una de sus principales ventajas es que permite analizar el tráfico en tiempo real y así evitar ataques de manera activa, esto lo puede realizar implementando reglas de seguridad en el IDS. Por lo que se puede detectar y contener a tiempo ataques de negación de servicio, envenenamiento de la red, propagación de virus,

robo de identidades, entre otros usos que el administrador de la red WiFi entienda malicioso. La edición de las reglas o políticas de seguridad en AlienVault OSSIM es uno de los elementos más importantes ya que define los eventos a monitorear, así como el comportamiento del sistema ante un evento generado, en función de las necesidades de la red WiFi. Las políticas permiten definir cómo el sistema procesa los eventos una vez que arriban al OSSIM, por lo que están compuestas por condiciones y consecuencias; las condiciones determinan qué eventos son procesados por la política, mientras que la segunda define qué pasará cuando los eventos coinciden con las condiciones especificadas. Las políticas pueden ser empleadas para filtrar eventos reduciendo el número de alarmas generadas, para enviar una notificación al personal de seguridad al producirse una alarma, o monitorear una dirección IP o puerto.

La posibilidad del IDS OSSIM de personalizar las alarmas, es decir, ante cualquier situación que el administrador de la red WiFi considere ser una nueva amenaza, puede ser configurada el mismo para que lo detecte y avise del evento ocurrido. Esto posibilita que ante nuevos ataques o intentos de evitar pagar el servicio se puedan modificar las reglas de detección del IDS, aún cuando no estén en la base de datos como ataques registrados.

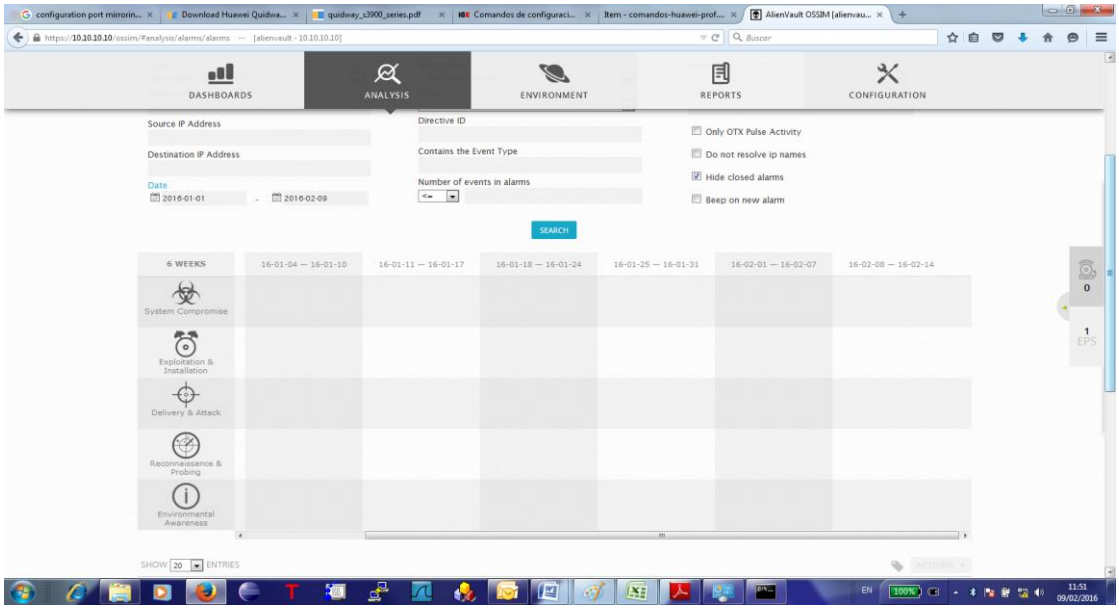


Fig. 3.14. Análisis de eventos ocurridos.

3.7. Ventajas y deficiencias de la propuesta de seguridad a la red WiFi de Etecsa

Las propuestas anteriormente mencionadas permiten ser empleadas de forma independiente o integradas, formando todo un sistema de protección al servicio y a la red WiFi. Dicha implementación permitiría en primer lugar proteger los datos de los clientes aumentando su confianza en el servicio que brinda la empresa. Entre las ventajas de la arquitectura se encuentran:

- Alta dificultad de descifrar por un intruso la información transmitida desde el cliente al punto de acceso y viceversa.
- Proceso de autenticación seguro.
- Detección de intentos de intrusión en la red.
- Evidencia de todas las acciones realizadas por un usuario en la red.

Al igual que otras arquitecturas de seguridad, esta propuesta también presenta debilidades. Entre los inconvenientes más significativos se encuentran:

- No todos los dispositivos que utilizan los clientes de la empresa tienen la funcionalidad de utilizar el protocolo EAP, los equipos más viejos no cuentan con esta característica.
- Para utilizar una conexión WPA2 Enterprise se necesita configurar en la PC o en el dispositivo del cliente la opción de permitir autenticación EAP. Lo cual constituye una limitación si se resalta que el servicio que se brinda por estas redes es público, y el mismo para lograr una mayor generalización del servicio necesita ser lo más sencillo posible para el cliente.
- La instalación de sensores de OSSIM distribuidos en los sitios WiFi eleva los costos de equipamiento y de operación de la red.
- Aquellos sitios WiFi que por su baja incidencia de ataques no se les instale un sensor OSSIM quedan expuestos a la ocurrencia de ataques sin quedar registros de los mismos, comportándose ese segmento como un punto ciego en la red.

3.8. Conclusiones parciales

El despliegue de la red WiFi en Villa Clara y de forma general en nuestro país ha sido un proceso que ha traído un cambio en la vida de la población. Son indudables las enormes facilidades que esta vía de comunicación representa para las familias cubanas. Pero como toda obra aun presenta defectos y problemas que pueden ser aprovechados por personas inescrupulosas para lograr beneficios para ellos a costa de la degradación del servicio o del robo de recursos ajenos. Hay opciones que se pueden hacer para mejorar esta situación y para detectar irregularidades. Algunas de estas opciones han sido tratadas en este capítulo y se encuentran agrupadas en dos grupos o tareas. La primera ha estado relacionada con el cambio en la conexión por parte del usuario y básicamente no implica inversiones solo reconfiguraciones de las facilidades existentes. La segunda está relacionada con la instalación de un mecanismo para la detección temprana de anormalidades en la red. Esta arquitectura permitiría detectar la mayoría de los intentos de desestabilización del servicio por parte de los usuarios y porque no también por parte desde el universo de internet contra los usuarios Nauta. No se debe olvidar que cuando nos conectamos al mundo el mundo también se conecta a nosotros.

Conclusiones

Como conclusiones del trabajo se tienen:

La arquitectura de red propuesta ofrece un servicio más fiable a los usuarios que utilicen estas redes para acceder a Internet, dicha propuesta elevará los niveles de protección del sistema y de los clientes.

En la actualidad los dispositivos (puntos de acceso, controlador de acceso) tienen la posibilidad técnica de encriptación WPA2 y de autenticación 802.1x, por lo que implementar esta propuesta no implicaría gastos adicionales para la explotación de estas redes WiFi en Etecsa.

Aunque en la actualidad aun existen clientes que utilizan dispositivos que no contemplan el protocolo EAP, dichos dispositivos son la minoría y la tendencia es el aumento del uso de dispositivos más modernos.

Los atacantes cada vez buscan herramientas más sofisticadas con el objetivo de realizar ataques exitosos, la ventaja con esta configuración de seguridad utilizando un IDS es que se podrá estar al tanto de los nuevos intentos de intromisión y se contará con reglas que identifiquen de forma automática a los atacantes facilitando así su neutralización.

Recomendaciones

Como recomendaciones se propone:

Implementar la propuesta de arquitectura segura para la red WiFi de Etecsa.

- Implementar el portal cautivo utilizando certificado digital en aquellos sitios en que no sea factible la propuesta anterior.

- Implementar una modalidad de conexión directa para los usuarios permanentes del servicio Nauta.

- Instalar y configurar los sensores en los sitios críticos de seguridad.

- Evaluar la posibilidad de configurar la utilidad de toma de decisiones del IDS de forma autónoma.

- Implementar un sistema de aviso por SMS con la detección de alertas de posible intrusión con afectación del servicio.

Referencias Bibliográficas

[1] H. Chaouchi, Wireless and Mobile Network Security, Londres: ISTE Ltd, 2009.

[2] S. Hewitt, "SECURITYIN NETWORKCONNECTEDPERFORMANCE ENVIRONMENTS," *Huddersfield,HD13DH,UnitedKingdom,* 2014.

[3] R. D. Pietro, Intrusion Detection Systems, Italia: Springer Science+Business Media, LLC., 2008.

[4] E. K. Attipoe, "End User's Perception about Security of the Public Wireless Network," *International Journal of Societal Applications of Computer Science,* vol. 2, no. 8, Agosto 2013.

[5] C. Morisset, "Formalization of Influencing in Information Security," *Computing Science, Claremont Tower, Claremont Road,* no. CS-TR-1423, 2014.

[6] A.Halim, "Studying the Performance of Secure IEEE 802.11g," *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS),* vol. 2, no. 1, 2014.

[7] B. Park, "A Study of Secure Communications in WiFi Networks," *Dept. Of Computer Science, Kyonggi Univ,* 2013.

[8] L. S. Y. Z. Xiangyun Zhou, Physical Layer Security in Wireless Communications, CRC Press, 2016.

[9] L. Kurup, "Comparative Study of Attacks on Security Protocols," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* vol. 3, no. 8, Agosto 2014.

[10] H. Reibold, WLAN Security kompakt: Praxiseinstieg in das Penetration Testing von drahtlosen Netzwerken, Brain-Media, 2015.

[11] A. Diab, Self-Organized Mobile Communication Technologies and Techniques for Network Optimization, IGI Global, 2016.

[12] A. M. Patel, "RAP Problems and Solutions in 802.11 Wireless LAN," *International Journal of Advance Research in Computer Science and Management Studies,* vol. 2, no. 1, 2014.

[13] M. M. Noor, "Current Threats of Wireless Networks," *Communication System and Network (iKohza) Research Group,* 2013.

[14] S. C. G. B. P. S. Koushik Sinha, Wireless Networks and Mobile Computing, CRC Press, 2016.

[15] B. Aboba, "Extensible Authentication Protocol (EAP)," *IETF,* Junio 2004.

[16] L. Blunk, "PPP Extensible Authentication Protocol (EAP)," *IETF,* Marzo 1998.

[17] C. Rigney, "RFC2865-Remote Authentication Dial In User Service (RADIUS)," *IETF,* Junio 2000.

[18] W. Osterhage, Wireless Security, CRC Press, 2016.

[19] G. Zorn, "Microsoft Vendor-specific RADIUS Attributes," *IETF,* 1999.

[20] S.-E. Zetterström, Basic Wifi-Hacking, LULU Press, 2015.

[21] T. Dierks, "The TLS Protocol," *IETF,* Enero 1999.

[22] B. Aboba, "RFC 3539-Authentication, Authorization and Accounting (AAA) Transport Profile," *IETF,* Junio 2003.

[23] S. Andrei, "WPA/WPA2 Password Security Testing using Graphics Processing Units," *Journal of Mobile, Embedded and Distributed Systems,* vol. 5, no. 4, 2013.

[24] AldoCassola, "A Practical, Targeted, and Stealthy Attack Against WPA Enterprise Authentication," 2013.

[25] K. Raeburn, "Advanced Encryption Standard (AES) Encryption for Kerberos 5," *RFC 3962,* 2005.

[26] J. A. R. P. d. Carvalh, "Laboratory Performance of Wi-Fi IEEE 802.11B,G WPA2 Point-to-Point Links: a Case Study," in *Proceedings of the world Congress on Engineering 2011*, Londres, 2011.

[27] M. Baldi, "A Physical Layer Secured Key Distribution Technique for IEEE 802.11g Wireless Networks," vol. 1, no. 1212.4991, 2012.

[28] R. Alder, How to Cheat at Configuring Open Source Security Tools, Elsevier,Inc., 2007.

[29] J. Burton, Cisco Security Professional's Guide to Secure Intrusion Detection Systems, Syngress Publishing,Inc., 2003.

[30] J. Babbin, Snort Cookbook, O'Reilly, 2005.

[31] C. d. Laat, "RFC2903-Generic AAA Architecture," Agosto 2000.

[32] C. Perkins, "RFC 3957 Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4," *IETF*, 2005.

[33] M. Chiba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)," *IETF,* Julio 2003.

[34] C. Rigney, "RFC2866-RADIUS Accounting," *IETF*, Junio 2000.

[35] F. Lanze, "Undesired Relatives: Protection Mechanisms Against The Evil Twin Attack in IEEE 802.11," 2013.

[36] T. Nguyen, "AN EFFICIENT SOLUTION FOR PREVENTING DIS'ING ATTACK ON 802.11 NETWORKS," *Journal of Engineering Technology and Education* , 2012.

[37] S. M. Bellovin, Thinking Security: Stopping Next Year's Hackers, Pearson Education, 2015.

[38] A. N. Sakib, "WPA 2 (Wi-Fi Protected Access 2) Security Enhancement:Analysis & Improvement," *Global Journal of Computer Science and Technology,* vol. 12, no. 6, Marzo 2012.

[39] J. Xiong, "SecureArray: Improving WiFi Security with Fine-Grained Physical-Layer Information," *Computer Science,* 2013.

[40] J. Milliken, "Development of Device Identity Using WiFi Layer 2 Management Frames for Combating Rogue APs," *Institute of Electronics, Communications and Information Technology (ECIT),* 2013.

[41] K. Raeburn, "Advanced Encryption Standard (AES) Encryption for Kerberos 5," *ISTF,* Febrero 2005.

[42] E. P. Calhoun, "Control and Provisioning of Wireless Access Points (CAPWAP)

Protocol Binding for IEEE 802.11," Marzo 2009.

[43] L. Deng, "Considerations for ALTO with network-deployed P2P caches," *IETF*, Julio 2013.

[44] M. A. Haque, "Performance of WiMAX over WiFi with Reliable QoS over Wireless Communication Network," *World Applied Programming,* vol. 1, no. 5, Diciembre 2011.

[45] A. N. Sakib, "Security Improvement of WPA 2 (Wi-Fi Protected Access 2)," *International Journal of Enginering Science and Technology (IJEST),* vol. 3, no. 1, Enero 2011.

[46] A. Salas, Los hombres que susurran a las máquinas: Hackers, espías e intrusos en tu ordenador, Grupo Planeta, 2015.

Glosario

AAA	*Authentication Authorization Accounting*
AC	*Access Control*
ACL	*Access Control List, Listas de Control de Acceso*
AES	*Advanced Encryption Standard*
AP	*Access Point*
CCPM	*Counter Mode with CBC-MAC Protocol*
CRC	*Control de Redundancia Cíclica*
EAP	*Extensible Authentication Protocol*
EAPoL	*EAP over LAN*
HTTPS	*HTTP sobre SSL*
IDS	*Intrusion Detection System*
IETF	*Internet Engineering Task Force*
IV	*Vector de Inicialización*
MIC	*Message Integrity Code*
RADIUS	*Remote Authentication Dial-In User Service*
SSL	*Secure Socket Layer*
TKIP	*Temporal Key Integrity Protocol, o Protocolo de integridad de clave temporal*
TLS	*Transport Layer Security*
VPN	*Virtual Private Network*
WEP	*Wired Equivalente Privacy*
WiFi	*Wireless Fidelity*
WLAN	*Wireless Local Area Network*
WPA	*Wired Protect Access*

Anexos

Anexo 1 Cobertura de red WiFi en Cayo Santa María.

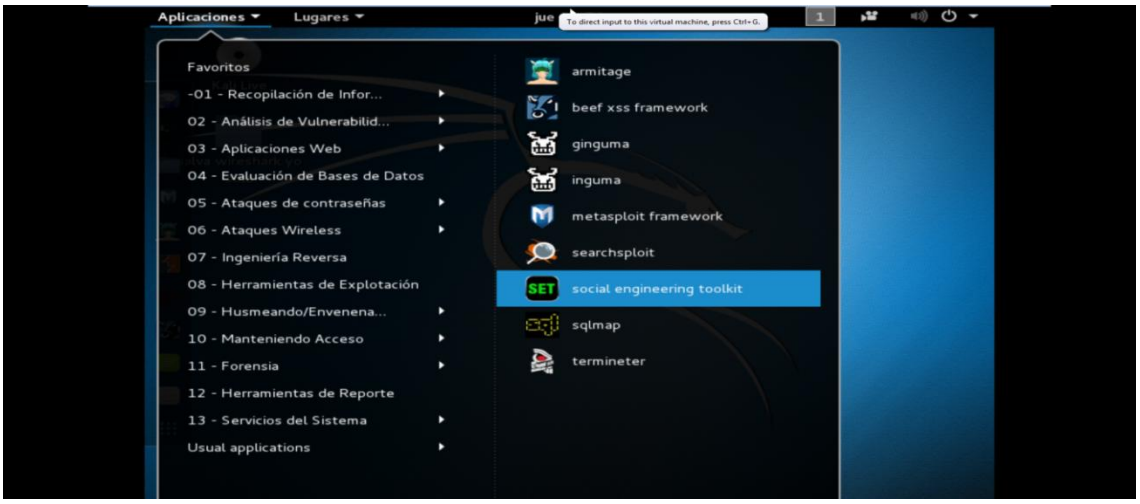
La red WiFi en los cayos del norte de la provincia de Villa Clara se encuentra en operación en los 15 hoteles ubicados en los cayos Las Brujas, Ensenachos y Cayo Santa María.

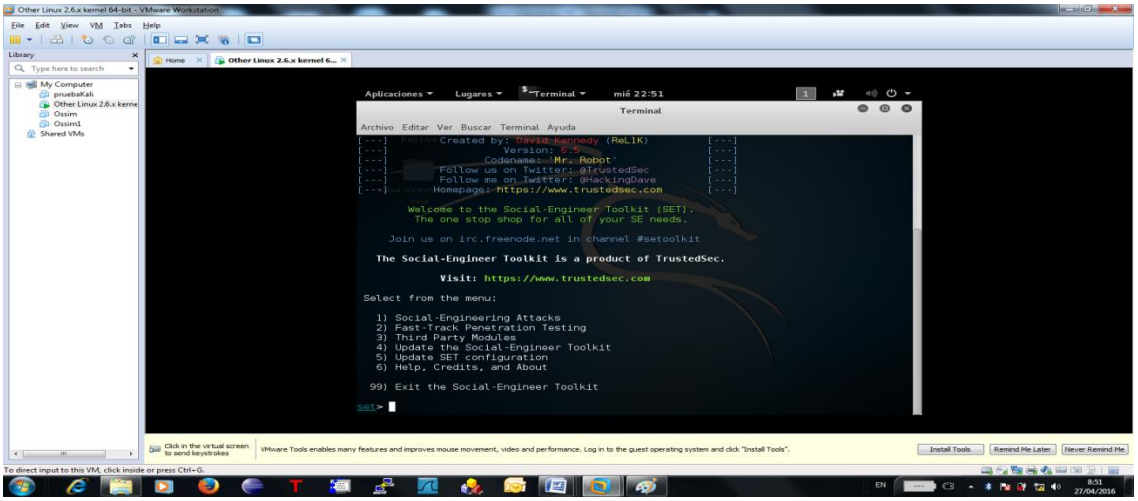
Anexo2 Cobertura de la red WiFi en la ciudad de Remedios.

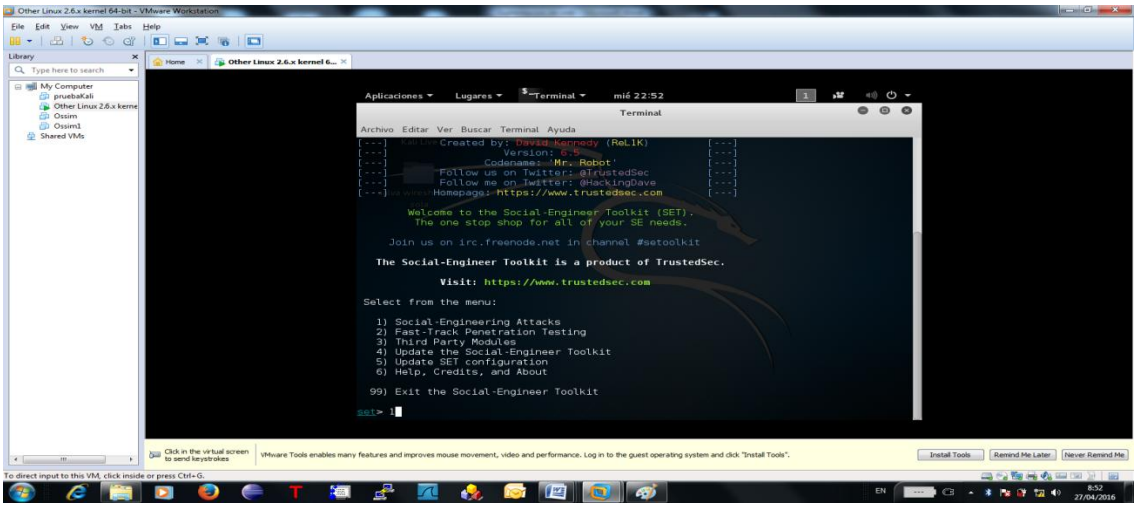
En la ciudad de Remedio la red WiFi de Etecsa brinda cobertura al parque Plaza Central y en las instalaciones hoteleras:

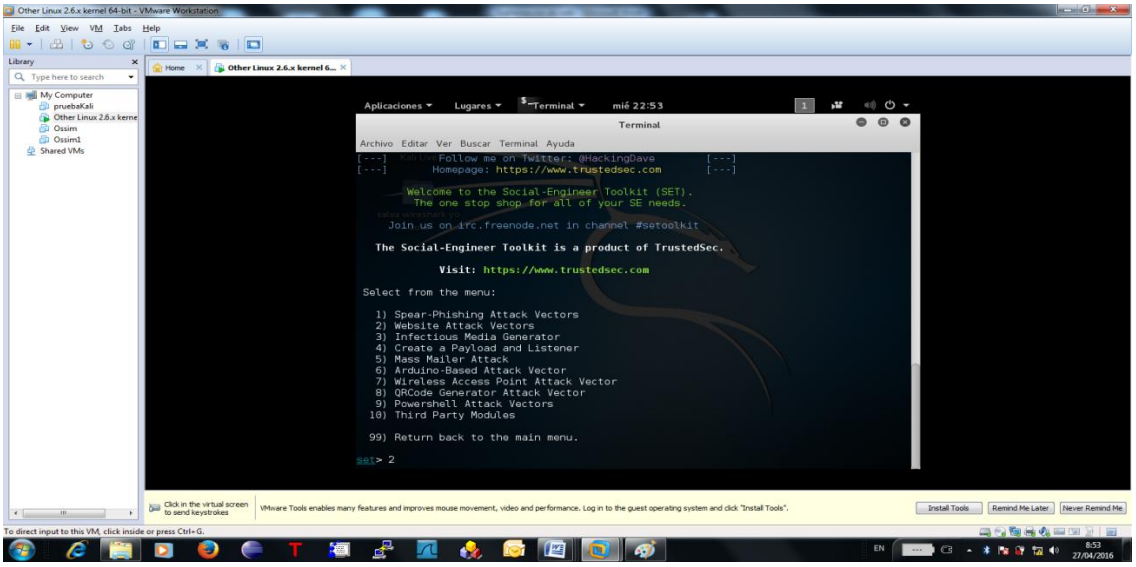
- Hotel Mascotte
- Hotel Camino del Príncipe
- Hotel Real
- Hotel Barcelona

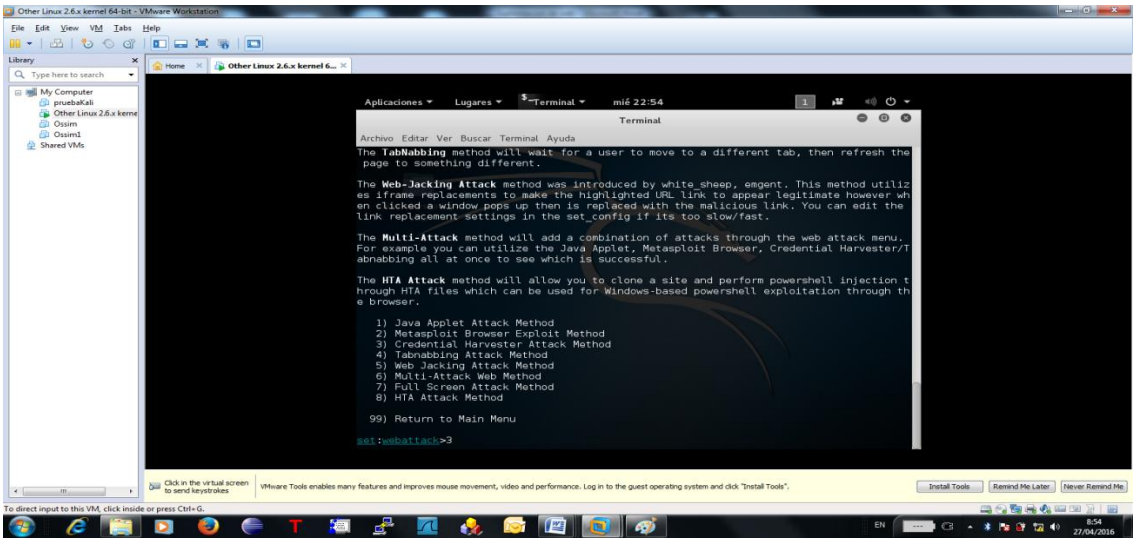
Anexo 3 Suplantación de una página web utilizando la herramienta SET (Social Engineering Toolkit).

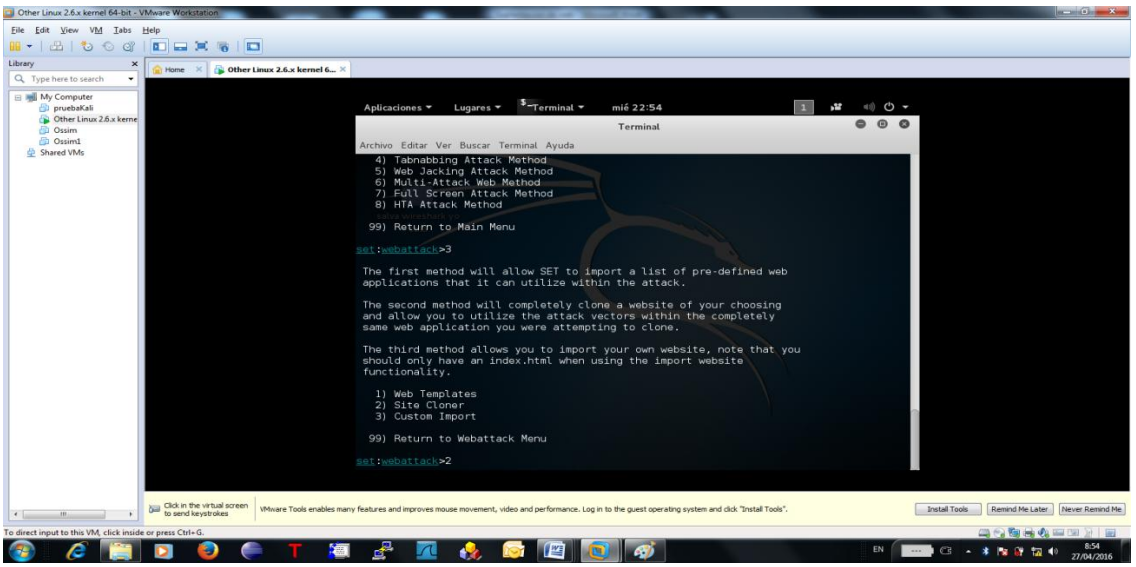


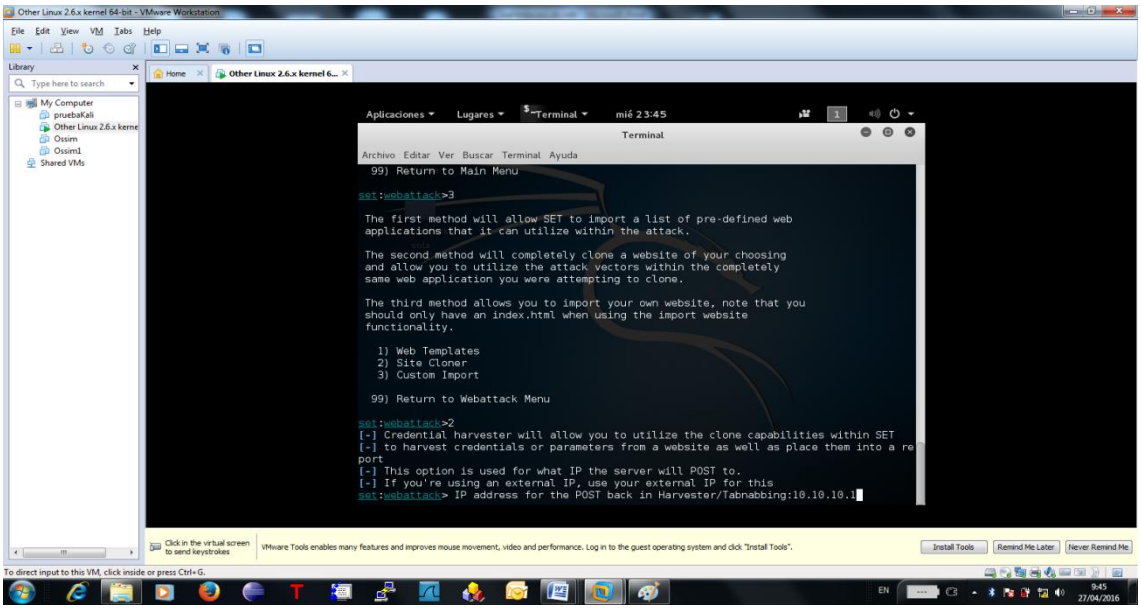


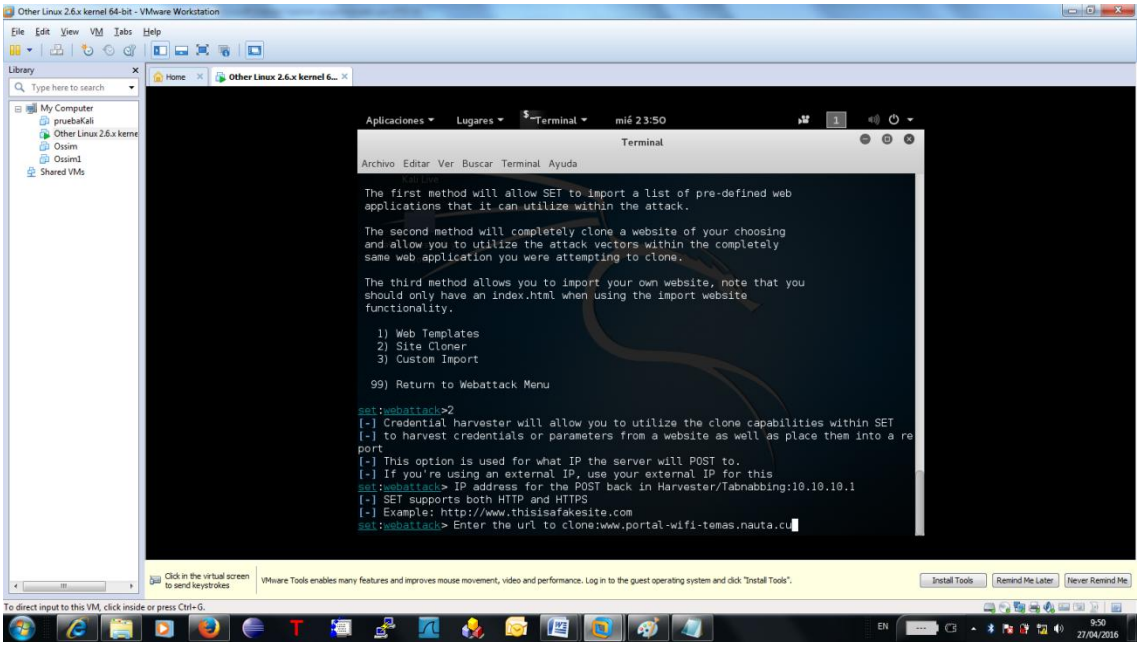



Other Linux 2.6.x kernel 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
pruebaKali
Other Linux 2.6.x kerne
Ossim
Ossim1
Shared VMs
Home
Other Linux 2.6.x kernel 6...
Aplicaciones Lugares Terminal mié 22:53
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2
Click in the virtual screen to send keystrokes
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".
Install Tools
Remind Me Later
Never Remind Me
To direct input to this VM, click inside or press Ctrl+G.
EN
8:53
27/04/2016


Other Linux 2.6.x kernel 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
pruebaKali
Other Linux 2.6.x kerne
Ossim
Ossim1
Shared VMs
Home
Other Linux 2.6.x kernel 6...
Aplicaciones Lugares Terminal mié 22:54
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utiliz es iframe replacements to make the highlighted URL link to appear legitimate however wh en clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/T abnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection t hrough HTA files which can be used for Windows-based powershell exploitation through th e browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method
99) Return to Main Menu
set:webattack>3
Click in the virtual screen to send keystrokes
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".
Install Tools
Remind Me Later
Never Remind Me
To direct input to this VM, click inside or press Ctrl+G.
EN
8:54
27/04/2016


Other Linux 2.6.x kernel 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
pruebaKali
Other Linux 2.6.x kerne
Ossim
Ossim1
Shared VMs
Home
Other Linux 2.6.x kernel 6...
Aplicaciones Lugares Terminal mié 22:54
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
Click in the virtual screen to send keystrokes
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".
Install Tools
Remind Me Later
Never Remind Me
To direct input to this VM, click inside or press Ctrl+G.
EN
8:54
27/04/2016


Other Linux 2.6.x kernel 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
pruebaKali
Other Linux 2.6.x kerne
Ossim
Ossim1
Shared VMs
Home
Other Linux 2.6.x kernel 6...
Aplicaciones Lugares Terminal mié 23:45
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a re
port
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.10.10.1
Click in the virtual screen to send keystrokes
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".
Install Tools
Remind Me Later
Never Remind Me
To direct input to this VM, click inside or press Ctrl+G.
EN
9:45
27/04/2016


Other Linux 2.6.x kernel 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
pruebaKali
Other Linux 2.6.x kerne
Ossim
Ossim1
Shared VMs
Home
Other Linux 2.6.x kernel 6...
Aplicaciones Lugares Terminal mié 23:50
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a re
port
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.10.10.1
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.portal-wifi-temas.nauta.cu
Click in the virtual screen to send keystrokes
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".
Install Tools
Remind Me Later
Never Remind Me
To direct input to this VM, click inside or press Ctrl+G.
EN
9:50
27/04/2016

Anexo 4 Configuración de puerto espejo en los switch Huawei S3900 y S2300.

Switch Huawei S3900

Operation	Command	Description
Enter system view	system-view	—
Enter Ethernet port view of the destination port	interface *interface-type interface-number*	—
Define the current port as the destination port	monitor-port	Required LACP and TCP must be disabled on the destination port.
Exit current view	quit	—
Enter Ethernet port view of the source port	interface *interface-type interface-number*	—
Configure the source port and specify the direction of the packets to be mirrored	mirroring-port { inbound | outbound | both }	Required
Display parameter settings of the mirroring	display mirror	Required This command can be executed in any view.

Switch Huawei S2300

Comando	***Descripción***
[QuidwayS2300] observing-port 1 interface Nombre_Interfaz	Designamos la interfaz a la que queremos copiar tráfico desde otra (s) interfaz o interfaces. Creamos la instancia 1 de port-morroring.
[QuidwayS2300] interface Nombre_Interfaz [QuidwayS2300-Interfaz] port-mirroring to observe-port 1 [inbound | outbound | both]	Ingresamos a la interfaz que queremos monitorear. Indicamos que tanto tráfico entrante como saliente, o ambos, sean copiados a la instancia 1 de port-mirroring.