TRABAJO DE DIPLOMA PARA OPTAR POR EL TÍTULO DE INGENIERO EN CIENCIAS INFORMÁTICAS

Análisis forense en la red inalámbrica del Docente 1

Autor: Ernesto Melian Felpeto

Tutores: Msc. Yadira Ruiz Constanten

Ing. Bárbara Triana Morales

Universidad de las Ciencias Informáticas

Junio de 2009

Declaración de Autoría

Declaro que soy el único autor de este trabajo y autorizo a la Universidad de las Ciencias Informáticas a hacer uso del mismo en su beneficio.

Para que así conste firmo la presente a los ____ días del mes de _____ del año _____.

Ernesto Melian Felpeto: _____
Firma del Autor

MSc. Yadira Ruiz Constanten: _____
Firma del Tutor

Ing. Bárbara Triana Morales: _____
Firma del Tutor

Agradecimientos

A mis padres, por su constante preocupación, y por la enorme ayuda que me brindaron.

A mis tutoras por su ayuda en la confección de este documento.

A mi novia, Baby, mi tata, mi amiga, mi tutora, que sin su ayuda no hubiese sido posible que esto viera la luz, y por su presencia.

A Agustin Magrans de Cardenas, que me brindó una ayuda técnica invalorable.

A Orestes Rodríguez Morales, por su ayuda en la universidad y por haber abierto el camino de esta tesis.

Resumen

La necesidad de comunicarse siempre ha impulsado al ser humano a buscar formas y herramientas para interactuar con sus semejantes. Uno de los medios que más importancia tiene en la actualidad es el utilizado para comunicar computadoras, o cualquier dispositivo electrónico.

Las redes cableadas a pesar de contar con mayor velocidad, mayor seguridad, y menor costo, en muchos casos resulta inútil ante la combinación de flexibilidad, ubicuidad y distancia entre nodos de red que ofrece la tecnología inalámbrica.

La seguridad es un aspecto que cobra especial relevancia en los ambientes inalámbricos. Sin embargo, para un tercero sería relativamente fácil acceder a una red inalámbrica desplegada en una oficina, sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. En caso de que se irrumpa una red inalámbrica con cualquier fin, sería necesario realizar una investigación de lo ocurrido, que posibilite un reporte del estado de la información que transitaba por la red en ese momento. Además, identificar al atacante si se da la posibilidad; cuál fue la brecha de seguridad que utilizó y si dejó alguna puerta trasera para una futura irrupción. Este tipo de investigación es conocida como informática forense.

La Universidad de las Ciencias Informáticas tiene proyectado brindar el servicio de red inalámbrica en sus edificios docentes, la Infraestructura Productiva y en el Rectorado, lo que provoca que la información que viaje por esa red no esté segura y pueda ser atacada en cualquier momento.

En el presente trabajo se explican una serie de conceptos que son importantes para comprender la seguridad en redes inalámbricas. Además se propone una estrategia para realizar análisis forense en el Docente 1 de la Universidad de las Ciencias Informáticas, basado en las características de la infraestructura que va a montarse, la cual que tendrá especificado cada uno de los pasos concretos a seguir en el momento de investigar un ataque a la misma.

Índice

Índice de Ilustraciones

Índice de Tablas

Introducción

La necesidad de comunicarse siempre ha impulsado al ser humano a buscar formas y herramientas para interactuar con sus semejantes. La evolución que estas han tenido se caracteriza por grandes cambios y descubrimientos, contando hoy en día con soluciones muy potentes para la comunicación. Uno de los medios que más importancia tiene en la actualidad es el utilizado para comunicar computadoras, o cualquier dispositivo electrónico.

El desarrollo tecnológico ha implicado, entre muchísimos otros factores, la producción de enormes cantidades de cables que posibilitan la conexión entre dos o más puntos distantes, permitiendo establecer una comunicación entre ellos, llegándose a crear soluciones tan interesantes como lo son el cable coaxial, o la mismísima fibra óptica. Pero desde hace unos pocos años, se ha ido incrementando exponencialmente el interés de muchos en cuanto a cómo poder comunicar diferentes equipos de cómputo sin la necesidad de utilizar redes cableadas; es decir, cómo entablar comunicación entre computadoras de manera inalámbrica. Esto es debido en gran proporción por la movilidad que brinda a los usuarios, y por supuesto, a la clara solución que representa para aquellos que no tienen una red en lugares remotos o inaccesibles, para los cuales las redes cableadas son algo impensable.

Actualmente la comunicación mediante redes inalámbricas se ha hecho muy popular, siendo cada vez más frecuente la presencia de dispositivos inalámbricos, como por ejemplo, un celular, o las laptops con propiedades de conexión inalámbrica.

La necesidad de comunicación es tan amplia que las redes cableadas a pesar de contar con mayor velocidad, mayor seguridad, y menor costo, en muchos casos resulta inútil ante la combinación de flexibilidad, ubicuidad y distancia entre nodos de red que ofrece la tecnología inalámbrica.

Ahora bien, la seguridad es un aspecto que cobra especial relevancia cuando hablamos de ambientes inalámbricos. Para tener acceso a una red cableada es imprescindible una conexión física a sus cables. Sin embargo, para un tercero sería relativamente fácil acceder a una red inalámbrica desplegada en una oficina, sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Esto le posibilitaría el acceso al entorno empresarial electrónico, que devendría una ruptura en la seguridad de esa red inalámbrica. Al ocurrir esto, sería necesario realizar una investigación de lo ocurrido, que posibilite un reporte del estado de la información que transitaba por

la red en ese momento. Además, identificar al atacante si se da la posibilidad; cuál fue la brecha de seguridad que utilizó y si dejó alguna puerta trasera para una futura irrupción. Este tipo de investigación es conocida como informática forense.

La informática forense es una rama de la ciencia forense que se corresponde con las pruebas legales encontradas en las computadoras y medios de almacenamiento digital. Es también conocida como forensia digital. Y a pesar de que existen muchos conceptos para definirla, en general, se puede decir que "se usa como técnica analítica y de investigación para identificar, recopilar, examinar y preservar la evidencia o la información que se encuentra almacenada o encriptada de manera magnética." (1)

En la Universidad de las Ciencias Informáticas (UCI) está proyectado un despliegue de toda una infraestructura de tecnología inalámbrica, diseñada por la empresa cubana Tecún, utilizando el estándar IEEE[1] 802.11, también denominado Wi-Fi[2], que brindará cobertura inalámbrica a todas sus áreas docentes, lo cual brinda una solución para las personas que poseen laptops y muchas veces no encuentran un puerto de red Ethernet para trabajar, ya que estos están asignados a las computadoras de los laboratorios donde estas se encuentran.

Cabe resaltar además, que como la señal se propaga a través del aire hacia todas direcciones en este tipo de red, esta puede ser captada por personas no autorizadas y ser utilizada para la planificación de un ataque. Para esta tecnología no existe actualmente una alternativa que sea totalmente fiable para su protección y puede darse el caso de un ataque a las nuevas redes que se van a desplegar en los docentes. Esto podría provocar, por ejemplo, que en el área de la producción los datos de los proyectos fueran accedidos por personal ajeno o saboteados, o que el directorio activo de la universidad fuera bloqueado por la intrusión de algún virus, del cual dependen prácticamente todos los servicios universitarios. Para estos casos, o para cualquier otro en el que esté involucrado un ataque informático a este tipo de red, no se cuenta en la UCI con una estrategia a seguir para realizar un análisis de lo ocurrido, que pudiese identificar al atacante o verificar cuales fueron los daños ocasionados.

---

[1] Institute of Electrical and Electronics Engineers (IEEE): una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas, como publicación de literatura técnica y conferencias por todo el mundo.

[2] Nombre comercial de la Wi-Fi Alliance, que es la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11.

La Situación Problémica anterior conlleva al siguiente Problema Científico: el tráfico de información es vulnerable cuando se utilizan redes inalámbricas.

Por lo tanto, el **Objetivo General** de esta investigación es proponer una estrategia para realizar un análisis forense en la red inalámbrica del Docente 1 de la Universidad de las Ciencias Informáticas.

El **Objeto de Estudio** es el análisis forense digital en redes inalámbricas de tipo 802.11.

Siendo el **Campo de Acción** el análisis forense de la red inalámbrica del Docente 1 de Universidad de las Ciencias Informáticas.

Las **Tareas Investigativas** que guiarán la investigación son las siguientes:

- Realizar un estudio de los estándares de redes inalámbricas y sus componentes.
- Realizar un estudio de los principales ataques que pueden darse en una red inalámbrica.
- Analizar de manera significativa los protocolos de seguridad en redes inalámbricas.
- Realización del estado del arte para fundamentar la investigación y dejar definida la posición del investigador.
- Investigar las técnicas forenses en tecnologías inalámbricas.
- Identificar elementos relacionados con la detección de brechas de seguridad.

El presente documento consta de 3 capítulos:

Capítulo I: “Fundamentación Teórica”, permite encontrar los principales conceptos que se manejan a lo largo del trabajo para proporcionar suficiente información relacionada con el tema que en el mismo se expone.

Capítulo II: “Análisis forense digital”, describe las características específicas a tener en cuenta en una red inalámbrica para poder obtener la mayor cantidad de información posible a la hora de realizar el análisis forense después de un ataque.

Capítulo III: “Solución Propuesta”, se exponen las especificidades de los equipos que se instalarán para montar la red inalámbrica en la Universidad, y la estrategia a seguir para efectuar un análisis forense en caso de ataque.

Nota: A partir de este punto se pondrán en formato Cursiva aquellos elementos tratados en el Glosario de Términos.

Capítulo I Fundamentación Teórica

Introducción

En el presente capítulo se expone el proceso investigativo para la confección del Trabajo de Diploma. Se clasifican las redes inalámbricas y sus componentes. Se exponen características fundamentales como son los protocolos de seguridad, tipos de ataques más comunes que pueden ocurrir en las redes inalámbricas, entre otros temas de seguridad. Además, se expone el estado del arte de la investigación. Todo esto a manera de sentar bases, para abordar en la investigación forense digital.

Desarrollo del Tema

Actualmente se está produciendo una gran proliferación de redes inalámbricas a nivel mundial. Esto es debido, por una parte a su versatilidad y facilidad de instalación, y por otra parte a la instalación sistemática por parte de los proveedores de servicios de Internet de routers con capacidades inalámbricas cuando se contratan sus servicios.

Esta proliferación inalámbrica trae algunas consecuencias:

La más evidente es que hay una cantidad tal de redes inalámbricas en muchos países que prácticamente en cualquier zona interurbana se puede encontrar un enlace de este tipo. Del total de las redes debemos diferenciar un porcentaje pequeño de redes configuradas correctamente (en cuanto a protocolos de seguridad se refiere) y una gran mayoría de redes que no solo no tienen ningún tipo de seguridad sino que además inundan el espacio con mensajes *DHCP* invitando a todos los clientes inalámbricos en un radio relativamente amplio a utilizar sus servicios.

Poco a poco, los usuarios se van concienciando que la seguridad es un tema muy serio (normalmente después de una mala experiencia informática) y configuran en sus dispositivos inalámbricos algún protocolo de seguridad.

Antes de comenzar a abordar el tema de la seguridad y sus protocolos, es necesario conocer las características principales de las redes inalámbricas.

1.1 Redes Inalámbricas

Las redes inalámbricas permiten o facilitan la comunicación entre estaciones de trabajo que se encuentran en distintos lugares sin la necesidad de un medio físico de interconexión, es decir, no necesita cables que conecten a los distintos equipos de trabajo para entablar comunicación.

Actualmente, el desarrollo de esta tecnología ha permitido que las transmisiones inalámbricas constituyan una eficaz herramienta para la transferencia de voz y datos sin el obstáculo de tener que utilizar cables para ello. La utilización de ondas electromagnéticas para realizar este intercambio de información brinda dos ventajas muy importantes: movilidad y flexibilidad del sistema en general. Esta tecnología utiliza ondas de radiofrecuencia de baja potencia y una banda específica de uso libre para transmitir entre dispositivos.

Las redes inalámbricas se clasifican dependiendo de su alcance y del tipo de onda electromagnética utilizada. Muchas bibliografías difieren en la distancia de cobertura de cada tipo de red, y dado que el desarrollo de esta tecnología se ha incrementado mucho, es difícil mantener un límite en cuanto al alcance que cada tipo de red puede tener, ya que cada año salen nuevos productos con mejoras respecto a sus antecesores y con mayor potencia de transmisión. Es por ello que el alcance que tenía una antena hace un tiempo, prácticamente se ha duplicado en la actualidad en su versión más actual, o que los dispositivos *Bluetooth* que en sus comienzos llegaban hasta los 10 m, alcancen hoy en día los 200 m. Debido a esto, no sería apropiado en este documento establecer una clasificación de las redes inalámbricas de acuerdo a la cantidad de metros que alcanza cada tipo de red, sino clasificarlas según para lo que están diseñadas, de menor a mayor cobertura, como sigue:

1.1.2 WPAN (Wireless Personal Area Network):

La característica principal de este tipo de red es que enfoca sus sistemas de comunicaciones a un área que envuelve al dispositivo emisor ya sea que esté en movimiento o no. La idea principal es eliminar los cables en el área a la redonda de una persona, y por esta vía tener acceso de manera inalámbrica a teclados, audífonos u otros periféricos. A diferencia de las redes inalámbricas de área local (WLAN), una conexión echa a través de una WPAN involucra una baja infraestructura o conexiones directas hacia el mundo exterior. Este tipo de tecnología también procura hacer un uso eficiente de recursos, por lo que se han diseñado protocolos simples y lo más óptimos para cada necesidad de comunicación y aplicación.

Ejemplos de este tipo de red, pueden ser los audífonos y teclados inalámbricos, o la transferencia de datos entre celulares.

1.1.3 WLAN (Wireless Local Area Network):

Las redes inalámbricas de área local se diferencian de las redes de área local tradicionales en que los terminales no están interconectados físicamente mediante un cable. El soporte físico del bus ha pasado de ser un cable a ir a través de las ondas de radio de alta frecuencia, pues este tipo de red se creó para sustituir las capas FÍSICA y ENLACE A DATOS de *Ethernet*. En otras palabras, las WLAN y las LAN (redes cableadas locales) son redes iguales que se diferencian en el modo en que el ordenador o terminal accede a la red, *Ethernet* mediante cable y la WLAN mediante ondas electromagnéticas. Esta característica las hace compatibles.

Este tipo de red permite una cobertura mucho más amplia con respecto a la WPAN, de entorno a los 100 metros y velocidades entre 2 y 54 Mbps, y con el desarrollo actual, en condiciones muy favorables (sin obstáculos visibles, condiciones del tiempo normales, o interferencias electromagnéticas) puede llegar incluso a los 500 metros. La WLAN es el tipo de red que se va a montar en la UCI.

1.1.4 WMAN (Wireless Metropolitan Area Network):

Estas redes son usadas mayormente para la interconexión de dispositivos en un mismo campo, pero en el radio de una ciudad, cubriendo actualmente velocidades aproximadas de 150 Mbps. Las tecnologías WMAN permiten a los usuarios establecer conexiones inalámbricas entre varias ubicaciones dentro de un área metropolitana (por ejemplo, con una sola antena WMAN, se le podría dar cobertura a casi toda la UCI), sin el alto coste que supone la instalación de cables de fibra o cobre y el alquiler de las líneas.

1.1.5 WWAN (Wireless Wide Area Network):

Este tipo de red es más bien una colección de redes conectadas a través de una subred. Las WWAN son las de mayor alcance, así como las más utilizadas hoy día en la infraestructura de telefonía móvil. Ejemplo de este tipo de red puede ser la tecnología UMTS (Universal Mobile Telecommunications System), utilizada con los teléfonos móviles de tercera generación (3G) y sucesora de la tecnología GSM (para móviles 2G).

Esta tecnología permite a los usuarios establecer conexiones inalámbricas a través de redes remotas públicas o privadas. Estas conexiones pueden mantenerse a través de áreas geográficas extensas, como

ciudades o países, mediante el uso de antenas en varias ubicaciones o sistemas satélite que mantienen los proveedores de servicios inalámbricos.

En la industria de cómputo la proliferación de distintas formas de comunicación de datos dio pie a que se buscara un estándar para que los fabricantes hicieran compatibles sus dispositivos entre sí. De tal manera, instituciones internacionales como el IEEE y la ETSI[3] se han venido encargando de dar los lineamientos para los estándares de comunicación. Los estándares, según el tipo de red inalámbrica son los siguientes:

1.2 Estándares de Redes Inalámbricas

1.2.1 WPAN

El desarrollo de estándares para las redes inalámbricas de corta distancia se basa fundamentalmente en la norma IEEE 802.15, y la tecnología Bluetooth. Estas redes constituyen un esquema de red de bajo costo que permite conectar entre sí equipos informáticos, de comunicación portátil y móvil, como ordenadores, periféricos como impresoras, ratones, micrófonos, auriculares y lectores de código de barras, así como sensores, monitores, localizadores, teléfonos móviles, y electrónica de consumo; permitiendo a estos dispositivos comunicarse e interoperar entre ellos sin interferencias.

El esfuerzo del grupo de trabajo 802.15 se enfoca en el desarrollo de normas de consenso para redes de área personal. El objetivo es publicar estándares, prácticas recomendadas, o guías que tienen amplia aplicabilidad en el mercado y hacer frente con eficacia a las cuestiones de la coexistencia y la interoperabilidad con otras soluciones de redes de cableadas e inalámbricas. (2)

Dentro de IEEE 802.15 encontramos cinco grupos de trabajo cada uno de ellos con características e intereses específicos que generan estándares que satisfacen necesidades específicas de comunicación.

Por su lado, Bluetooth es una tecnología de comunicación inalámbrica de corto alcance destinada a sustituir a los cables de conexión portátil y/o dispositivos fijos, manteniendo altos niveles de seguridad. Las características principales de esta tecnología son la robustez, bajo consumo energético y bajo costo.

---

[3] European Telecommunications Standards Institute, ETSI: es una organización de estandarización de la industria de las telecomunicaciones (fabricantes de equipos y operadores de redes) de Europa, con proyección mundial.

La especificación Bluetooth define una estructura uniforme para una amplia gama de dispositivos que permite la conexión y la comunicación entre ellos. Puede observarse en la Ilustración 1: Logotipo de Bluetooth el logotipo utilizado en dispositivos que trabajan con esta tecnología.

Ilustración 1: Logotipo de Bluetooth

1.2.2 WLAN

La Wí-Fi Alliance es la organización más famosa que se encarga de adoptar, probar y certificar que los equipos cumplen con el estándar 802.11. Su objetivo es mantener una marca (Wi-Fi) que fomente la tecnología inalámbrica de cobertura local y que asegure la compatibilidad entre equipos. A los dispositivos certificados por la Wi-Fi Alliance se les permite usar este logotipo:

Ilustración 2: Logo Wi-Fi

El uso de esta certificación, garantiza la compatibilidad entre dispositivos que utilizan el estándar 802.11.

Entre los estándares y productos para redes de área local se destacan:

- IEEE 802.11: Evolucionando hacia los grupos de trabajo de Transmisión, y los de Extensión del mismo.

  Para la Transmisión se tienen:

  - ❖ IEEE 802.11: Especificación para 1-2 Mbps en la banda de los 2.4 GHz, usando salto de frecuencias (FHSS)[4] o secuencia directa (DSSS)[5].

[4] El espectro ensanchado por salto de frecuencia (FHSS) es una técnica de modulación en espectro ensanchado (técnica de modulación empleada en telecomunicaciones para la transmisión de datos, por lo común digitales y por

- IEEE 802.11a: El estándar de alta velocidad que soporta velocidades de hasta 54 Mbps en la banda de 5 GHz.
- IEEE 802.11b: El estándar comúnmente más usado de WLAN que soporta velocidades de hasta 11 Mbps en la banda de 2.4 GHz.
- IEEE 802.11g: Extensión de 802.11 para proporcionar 20-54 Mbps. Es compatible hacia atrás con 802.11b. Tiene mayor alcance y menor consumo de potencia que 802.11a.

Y como grupos de Extensión se encuentran:

- IEEE 802.11n: Alto rendimiento de procesamiento (High Throughput).
- IEEE 802.11k: Medida de radio del recurso de LANs inalámbricas (Radio Resource Measurement of Wireless LANs).
- IEEE 802.11i: Destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Este estándar se basa en el AES (estándar de cifrado avanzado) y puede cifrar transmisiones que se ejecutan en las tecnologías 802.11a/b/g.
- IEEE 802.11m: Igualdad del mantenimiento (Maintenance PAR).
- IEEE 802.11p: Acceso inalámbrico en el ambiente de vehículos (Wireless Access in the Vehicular Environment).
- IEEE 802.11r: El moverse rápido, y rápido Handoff[6]. Fast Roaming Fast Handoff.

---

radiofrecuencia.) en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia sincrónicamente con el transmisor.

[5] El espectro ensanchado por secuencia directa (DSSS), es uno de los métodos de modulación en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas que más se utilizan.

[6] Sistema utilizado en comunicaciones móviles celulares con el objetivo de transferir el servicio de una estación base a otra cuando la calidad del enlace es insuficiente.

- ❖ IEEE 802.11s: Acoplamiento de red malla (Mesh Networking).
- ❖ IEEE 802.11t: Predicción del funcionamiento de la red inalámbrica (Wireless Performance Prediction).
- ❖ IEEE 802.11u: Trabajo interno con las redes internas inalámbricas (Wireless Interworking With External Networks).
- ❖ IEEE 802.11v: Administración de redes inalámbricas (Wireless Network Management).
- ❖ IEEE 802.11w: Administración de marcos protegidos (Protected Management Frames).
- ❖ IEEE 802.11y: Protocolo basado en la contención (Contention Based Protocol Study Group). (3)

- HiperLAN$_2$: Estándar que compite con IEEE 802.11a al soportar velocidades de hasta 54 Mbps en la banda de 5 GHz.
- HomeRF: Estándar que compite con el IEEE 802.11b que soporta velocidades de hasta 10 Mbps en la banda de 2.4 GHz.

1.2.3 WMAN

IEEE 802.16 es la especificación para las redes inalámbricas de banda ancha de acceso metropolitano que utilizan una arquitectura punto a multipunto. El estándar define el uso del ancho de banda entre las gamas de frecuencia con licencia 10GHz y 66GHz y sub 11GHz. 802.16 admite tasas de bits muy elevadas al cargar y descargar desde una estación base a una distancia de 50 km.

Para redes de área metropolitana se encuentran tecnologías basadas en WiMax (Worldwide Interoperability for Microwave Access, es decir, Interoperabilidad Mundial para Acceso con Microondas), un estándar de comunicación inalámbrica basado en la norma IEEE 802.16, el cual usa dos bandas de frecuencia 10-66 Ghz y la 2-11 Ghz, ambas licenciadas. Estas son redes de gran ancho de banda para realizar conexiones punto-multipunto, estandarización de una tecnología llamada LMDS (Local Multipoint Distribution System). WiMax es un protocolo parecido a Wi-Fi, pero con más cobertura y ancho de banda.

El ETSI creó el estándar HiperMAN, dirigido principalmente para proveer DSL[7] inalámbrica de banda ancha, cubriendo un área geográfica grande. Se considera una alternativa europea a WiMax. La estandarización se centra en soluciones de banda ancha optimizadas para el acceso en bandas de frecuencias inferiores a los 11 Ghz (principalmente en la banda de los 3.5 Ghz). Más concretamente, éste estándar opera entre el rango de frecuencias de 2 a 11 GHz y está optimizado para redes de conmutación de paquetes, soportando aplicaciones fijas y móviles, y orientado sobre todo a usuarios residenciales y pequeños/medianos negocios.

HiperMAN se ha desarrollado con una gran cooperación del estándar 802.16 ya que posee las mismas capas FÍSICA y MAC, del tal forma que el estándar HiperMAN y el estándar 802.16 son interoperables entre sí, por lo que ambas comparten ventajas e inconvenientes.

1.2.4 WWAN

El IEEE aprobó el establecimiento del grupo de trabajo 802.20 para el desarrollo de este tipo de redes, cuya misión es desarrollar la especificación de las capas FÍSICA y ENLACE DE DATOS, del modelo OSI (Open Systems Interconnection) para proporcionar una interfaz con medio de propagación aire, basado en conmutación de paquetes y optimizado para el transporte IP que:

- Opere en las bandas de trabajo licenciadas por debajo de 3,5 GHz.
- Trabaje con velocidades de pico por encima de 1 Mbps.
- Soporte movilidad por encima de los 250 Km/h.
- Cubra tamaños de celda que permitan coberturas continuas de áreas metropolitanas.
- Obtenga eficiencias espectrales, velocidades de transmisión sostenidas y número de usuarios activos significativamente más altos que con los sistemas móviles existentes.

Se muestra a continuación una gráfica para que se entienda mejor la distribución de estos tipos de redes, y sus estándares más destacados:

---

[7] Es una familia de tecnologías que provee transmisión de datos digitales a través de los cables de una red telefónica.

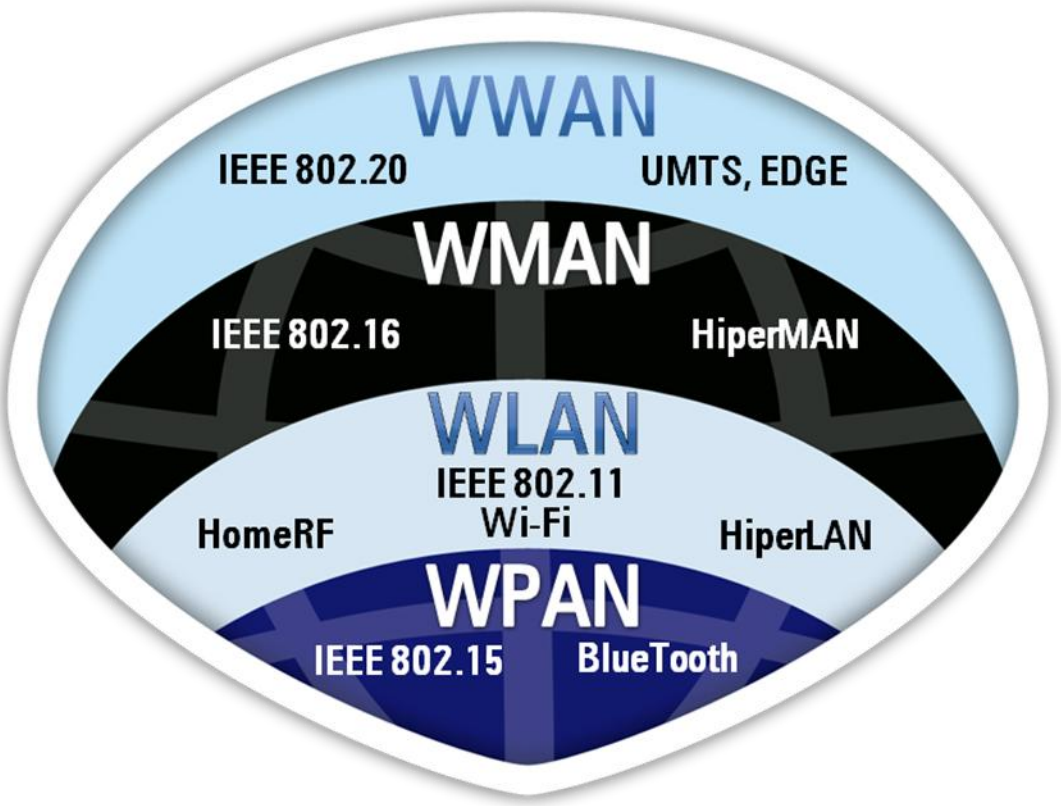

Ilustración 3: Evolución de las redes inalámbricas y sus estándares

1.3 Componentes de una red inalámbrica WLAN

Típicamente un sistema 802.11 se compone de 3 componentes fundamentales: Punto de Acceso (AP, por sus siglas en inglés: Access Point), Router y de tantas computadoras como deseemos conectar en forma inalámbrica:

- Tarjeta de red inalámbrica o conexión inalámbrica (Wi-Fi): Cada equipo que se conectará a la red inalámbrica necesitará un adaptador inalámbrico integrado o removible con el protocolo 802.11a/b/g.
- AP: Es el dispositivo que hace de puente entre la red cableada y la red inalámbrica. Este brinda la señal electromagnética que captan las tarjetas de red inalámbrica de los equipos para poder conectarse a la red.

- Ruteador (Router): Es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos. A el pueden conectarse varios AP.

Una red típica 802.11b, se denomina que está en modo BSS (Basic Service Set), y se aplica para las redes configuradas para trabajar con APs. Cada red configurada de esta manera, posee su propio nombre. Este nombre es el SSID (Service Set IDentifier) de la red, como se muestra a continuación:

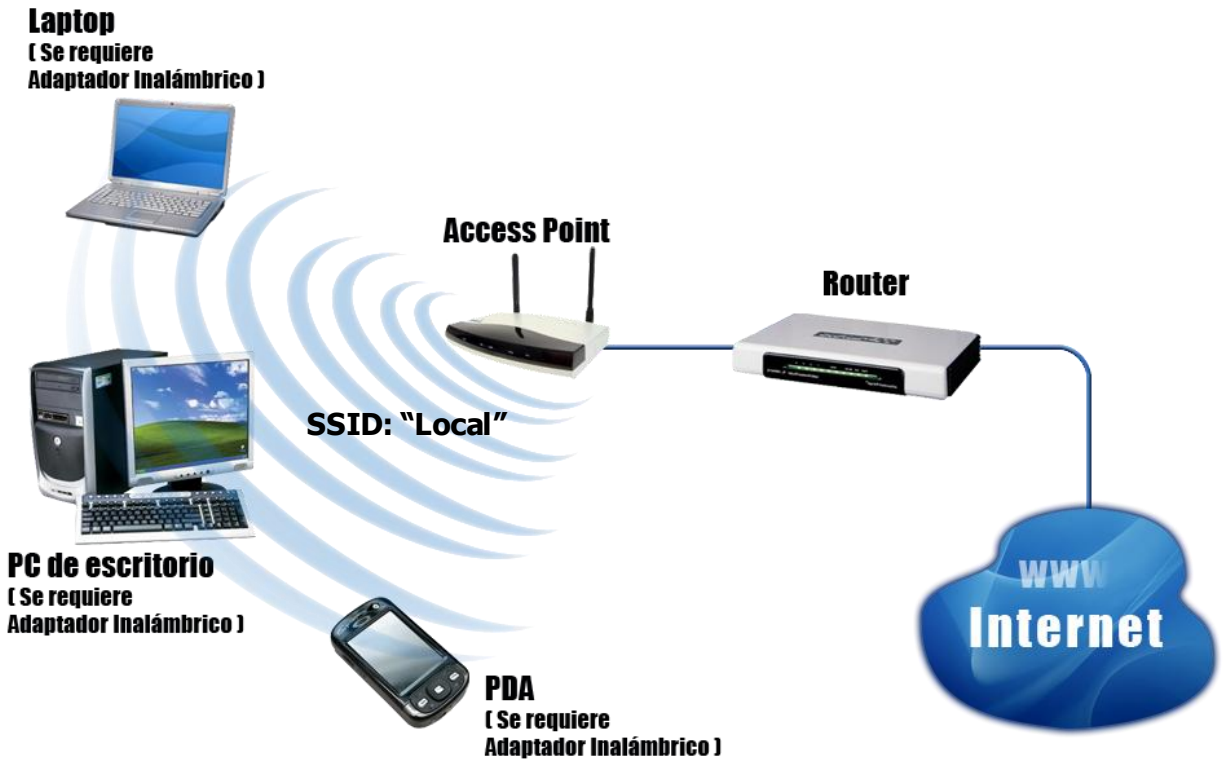

Ilustración 4: Topología típica de una red de tipo WLAN

En las aplicaciones del estándar 802.11 para interiores puede suceder que, con el fin de incrementar el área de servicio interno en un edificio, sea necesaria la instalación de más de un AP. Cada uno de estos cubrirá un área de servicio determinada y las computadoras tomarán servicio de WLAN a través del AP más cercano.

En la aplicación para exteriores puede darse el caso de que la cantidad de computadoras que van a conectarse a la red sea elevado y debido al alto tráfico que ello generaría se requiera instalar más de un AP.

En caso de que se cuente con dos o más equipos que tengan incorporado un adaptador inalámbrico (tarjeta Wi-Fi), es posible conectarlos inalámbricamente configurando una red conocida con el nombre de "ad hoc", es decir, de equipo a equipo, sin necesidad de usar un AP. También es denominado modo IBSS (Independent BSS).

En caso de que uno de los equipos de la red ad hoc esté conectado a Internet, puede compartir la conexión con los demás equipos de esa red, como en una red local tradicional, como se muestra a continuación:

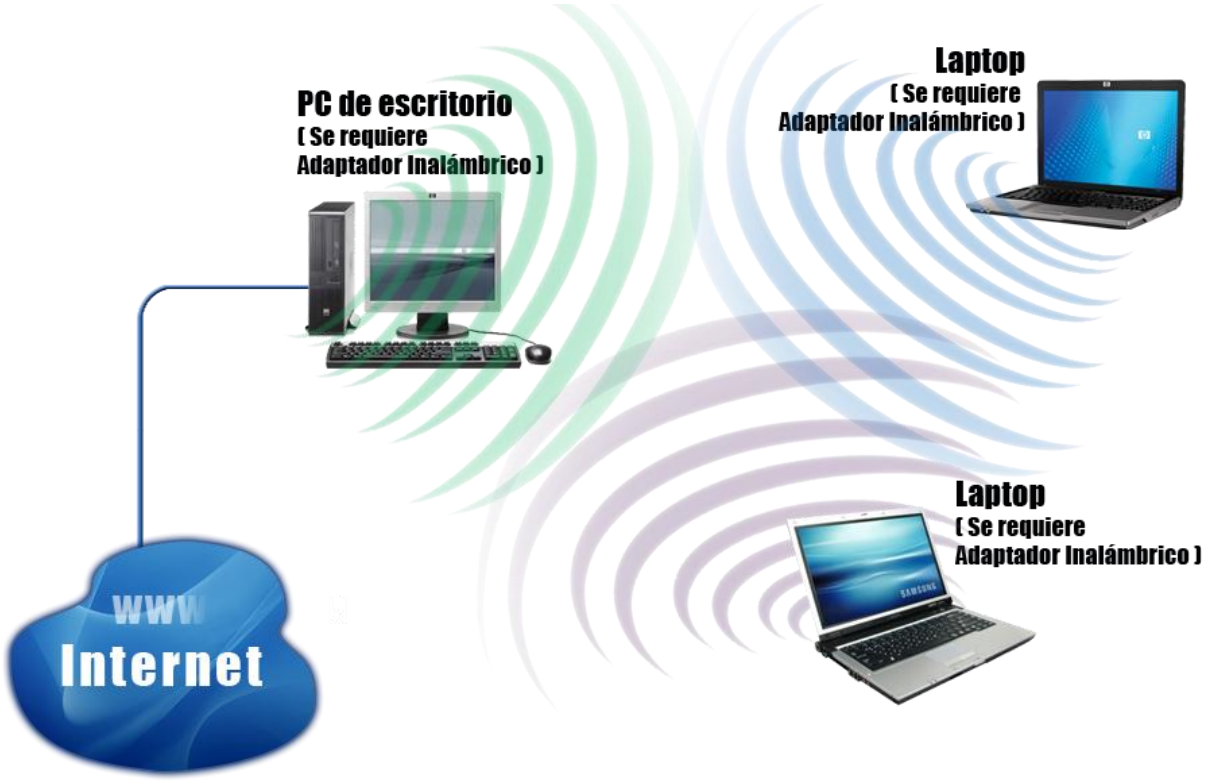

Ilustración 5: Topología Ad-Hoc en WLAN

Como se pudo apreciar, las redes inalámbricas permiten la interconexión entre dispositivos, o a Internet, sin el tedioso uso de cables. Y es precisamente esto, lo que hace que el tema de la seguridad sea tan

peculiar en estas redes. Puesto que la información viaja por el aire, esta necesita estar segura, de manera que la persona a la que se le envía sea la única capaz de leerla. Pero antes de abordar los mecanismos de protección de los datos en las redes inalámbricas, es necesario comprender la necesidad de estos, y conocer las características esenciales de los ataques que puede sufrir la información digital. De esta manera se proponen a continuación algunos conceptos relacionados con la seguridad.

1.4 Ataques Informáticos

Un "ataque" consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, programa de software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causa daño. Por lo que un incidente de seguridad informática, puede considerarse como una violación o intento de violación de la política de seguridad, de la política de uso adecuado o de las buenas prácticas de utilización de los sistemas informáticos. (4) (5)

Para bloquear estos ataques, es importante estar familiarizado con los principales tipos y tomar medidas preventivas. Los ataques pueden ejecutarse por diversos motivos:

- Obtener acceso al sistema.
- Robar información, como secretos industriales o propiedad intelectual.
- Recopilar información personal acerca de un usuario.
- Obtener información acerca de una organización (la compañía del usuario, etc.).
- Afectar el funcionamiento normal de un servicio.
- Usar los recursos del sistema del usuario, en particular cuando la red en la que está ubicado tiene un ancho de banda considerable.
- Bloquear servicios que se brindan en el *host* atacado.

Cabe ahora una categorización de dichos incidentes que aporte una base para su valoración y dé una visión de cómo afrontarlos. Aunque se han propuesto varios tipos de clasificaciones sobre taxonomías de incidentes, no existe ningún consenso al respecto y mucho menos sobre cuál de ellas es la más acertada. La que se propone a continuación tiene la finalidad de ayudar a una mejor comprensión.

1.5 Tipos de ataques

Incidentes de Denegación de Servicios (DoS):

Son un tipo de incidente cuya finalidad es obstaculizar, dañar o impedir el acceso a redes, sistemas o aplicaciones mediante el agotamiento de sus recursos.

Incidentes de código malicioso:

Cualquier tipo de código ya sea, un gusano, o un “caballo de Troya”, que pueda ejecutarse en un sistema y dañarlo.

Incidentes de acceso no autorizado:

Se produce cuando un usuario o aplicación accede, por medio de hardware o software, sin los permisos adecuados a un sistema, a una red, a una aplicación o los datos.

Incidentes por uso inapropiado:

Se dan cuando los usuarios violan la política de uso apropiado de los sistemas (por ejemplo, descargando ejecutables de Internet sin autorización).

Incidente múltiple:

Se produce cuando el incidente implica varios de los tipos anteriores.

La mayoría de los incidentes que se dan en la realidad, pueden enmarcarse en varias de las categorías expuestas, por lo que una buena forma de identificarlos es por el mecanismo de transmisión empleado. Por ejemplo, un virus que crea en el sistema atacado una puerta trasera debe ser manejado como un incidente de código malicioso y no como un acceso no autorizado, ya que el virus es el mecanismo de transmisión.

Los ataques pueden asimismo clasificarse en términos de ataques pasivos y ataques activos:

ATAQUES PASIVOS

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza (eavesdropping), para obtener información de lo que está siendo transmitido. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el uso de mecanismos como el cifrado de la información.

ATAQUES ACTIVOS

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

Suplantación de identidad:

El intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

Reactuación:

Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

Modificación de mensajes:

Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesos en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesos en la cuenta B".

Degradación fraudulenta del servicio:

Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría

interrumpir el servicio de una red inundándola con mensajes falsificados. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP[8], etc. (6)

Lo anterior visto, es una vista general de la clasificación de los ataques que pueden ocurrirle a los sistemas informáticos. Se brinda entonces a continuación los diferentes tipos de ataques que pueden manifestarse específicamente en las redes inalámbricas locales.

ACCESS POINT SPOOFING

Access Point Spoofing o "Asociación Maliciosa": en este caso el atacante se hace pasar por un Access Point (punto de acceso a la red) y el cliente piensa estar conectándose a una red verdadera. Ataque común en redes ad-hoc.

ARP POISONING

ARP Poisoning o "Envenenamiento ARP", ataque al protocolo ARP (Address Resolution Protocol) conocido como "Man in the Midle" u "hombre en medio". Una computadora invasora X envía un paquete de ARP reply para Y diciendo que la dirección IP de la computadora Z apunta hacia la dirección MAC (Media Access Control address o dirección de control de acceso al medio) de la computadora X, y de la misma forma envía un paquete de ARP reply para la computadora Z diciendo que la dirección IP de la computadora Y apunta hacia la dirección MAC de X. Como el protocolo ARP no guarda los estados, las computadoras Y y Z asumen que enviaron un paquete de ARP request solicitando esta información, y asumen los paquetes como verdaderos. A partir de este punto, todos los paquetes enviados y recibidos entre las computadoras Y y Z pasan por X (hombre en medio).

MAC SPOOFING

MAC Spoofing o "enmascarar el MAC", ocurre cuando alguien roba una dirección MAC de una red haciéndose pasar por un cliente autorizado. En general, las placas de redes permiten el cambio de lo numero MAC por otro, lo que posibilita este tipo de ataque.

---

[8] Sigla en inglés de File Transfer Protocol - Protocolo de Transferencia de Archivos): Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor.

DENIAL OF SERVICE (DoS)

> Negación de Servicio. Consiste en negar algún tipo de recurso o servicio. Puede ser utilizado para "inundar" la red con pedidos de disociación, imposibilitando así el acceso de los usuarios, pues los componentes de la red se asocian y desasocian una y otra vez. Al rechazar algún servicio, también puede dar origen a interferencias por equipamientos de Bluetooth, hornos de microondas y teléfonos inalámbricos, debido a que estos equipamientos trabajan en la misma franja de frecuencia que las redes inalámbricas. (7)

Existen varias bibliografías que consideran los siguientes elementos como ataques a las redes inalámbricas, pero en esta investigación no se consideran como tal, sino como estrategias para la preparación de un ataque a las inalámbricas:

WLAN ESCÁNERS

> WLAN Escáners o "Ataque de Vigilancia", consiste en recorrer un local que se desea invadir para descubrir redes WLAN activas en dicho local, así como equipamientos físicos, para un posterior ataque o robo.

WARDRIVING Y WARCHALKING

> Se llama de "Wardriving" a la actividad de encontrar puntos de acceso a redes inalámbricas, mientras una persona se desplaza por la ciudad en algún transporte y haciendo uso de un dispositivo con una placa de red wireless para detectar señales (puede ser una laptop). En muchos países, después de localizar un punto de acceso a una determinada red inalámbrica, se marca el área con un símbolo, e informan a otros invasores (actividad que se denomina "warchalking").

Ahora bien, haciendo un poco de historia: con el surgimiento de las redes inalámbricas y su inmersión en el mercado mundial (hacia 1991) y todas las ventajas que traían consigo, era lógico ponerse a pensar en la manera de protegerlas, pues existían muchas redes corporativas por las que transitaba información confidencial, por lo que la seguridad en las redes inalámbricas era un aspecto crítico que no se podía descuidar. Debido a que las transmisiones viajan por un medio no seguro (por el aire), se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad. Consciente de esto, en 1999 el IEEE publicó un mecanismo opcional de seguridad, denominado WEP (Wired Equivalent Privacy), como primera alternativa que brindaba solución a los problemas de seguridad

existentes en las redes inalámbricas locales. Años después fueron creados otros protocolos de seguridad, que fueron evolucionando hasta nuestros días, que serán tratados a continuación

1.6 Protocolos de Seguridad

Tras la creación del denominado protocolo de seguridad WEP, no pasó mucho tiempo para que se evidenciara que desplegado en numerosas redes WLAN, había sido roto de distintas formas, lo que lo había convertido en una protección bastante débil si el tema de seguridad debía tratarse con énfasis.

Algunas empresas en vista de que WEP era insuficiente y de que no existían alternativas estandarizadas mejores, decidieron utilizar otro tipo de tecnologías como *VPN (*Virtual Private Network*)* para asegurar los extremos de la comunicación. Pero la tecnología *VPN* es demasiado costosa en recursos para su implementación en redes WLAN, por lo que pocas empresas pueden hacer uso de esta variante.

Para solucionar las deficiencias de WEP, el IEEE crea una nueva norma de seguridad, la IEEE 802.11i, que permite dotar de mayor seguridad a las redes WLAN. Durante la implementación de este estándar, la Wi-Fi Alliance decide lanzar un mecanismo de seguridad intermedio de transición hasta que estuviese disponible 802.11i, tomando aquellos aspectos que estaban suficientemente avanzados del desarrollo de la norma. Así en 2003, es creado el protocolo WPA (Wifi Protect Access), y más tarde se comenzó a aplicar la solución definitiva: WPA2.

Un muy elevado porcentaje de redes son instaladas sin tener en consideración la seguridad convirtiendo así sus redes en redes vulnerables, sin proteger la información que por ellas circulan, es por ello que existen varias alternativas para garantizar la seguridad de las WLAN. Las más comunes son:

- Utilización de protocolos de cifrado de datos como el WEP, WPA y WPA2, que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos.
- *VPN*
- Filtrado de MAC, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados, pues cada tarjeta de red posee un único número MAC.
- Ocultación del punto de acceso: se puede ocultar el AP de manera que sea invisible a otros usuarios, o sea, que no sea detectado por los dispositivos inalámbricos.

A continuación se abordará con detalles cada uno de los protocolos de cifrado de datos anteriormente mencionados.

1.6.1 WEP

Características y funcionamiento:

WEP (traducido al español: Privacidad Equivalente al Cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN.

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. 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 aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

Este es el protocolo básico usado en la mayoría de las WLANs cuando se quiere tener un mínimo de seguridad, pues no requiere de hadware potente y es muy fácil de configurar. Es muy común ver redes Ad-hoc en la Universidad usando este protocolo de cifrado.

1.6.2 WPA

WPA (traducido al español: Acceso Protegido Wi-Fi) Esta norma soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de utilizar WPA2.

Características de WPA

Las principales características de WPA son la distribución dinámica de claves, mejora de la confidencialidad y técnicas de integridad y autentificación más fuertes que las usadas en WEP.

WPA incluye las siguientes tecnologías:

- Proporciona un control de acceso en redes basadas en *puertos*. El concepto de puerto, en un principio pensado para las ramas de un *switch*, también se puede aplicar a las distintas conexiones

de un punto de acceso con las *estaciones*. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El AP mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP (Extensible Authentication Protocol, se explica más abajo) y un servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS (Remote Authentication Dial-In User Service). Si la autorización es positiva, entonces el AP abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el AP (como priorizar ciertos tráficos o descartar otros).

- EAP, definido en la RFC 2284[9], es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (Point-to-Point Protocol), aunque WPA lo utiliza entre la estación y el servidor RADIUS (Remote Authentication Dial-In User Server). Esta forma de encapsulación de EAP está definida en el estándar IEEE 802.1x bajo el nombre de EAPOL (EAP over LAN).
- TKIP (Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama.
- MIC (Message Integrity Code) o como se conoce, Michael. Código que verifica la integridad de los datos de las tramas.

1.6.3 WPA2

Incluye el algoritmo de cifrado AES (Advanced Encryption Standard), desarrollado por el NIS (Network Information Service, Sistema de Información de Red). Requiere de un hardware potente para realizar sus algoritmos.

Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de procesamiento no pueden incorporar WPA2. 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. WPA2 hace uso de WPA2 PSK, o WPA2 Enterprise como alternativas de autenticación. Una mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS.

---

[9] http://www.ietf.org/rfc/rfc2284.txt

Hoy en día, con los nuevos avances tecnológicos, llegan nuevas vulnerabilidades que implican riesgos para las personas y las compañías ante la posibilidad de ver expuestos datos sensibles, transmitidos por éstos medios inalámbricos. Súmesele a esto que los distintos tipos de protocolos de seguridad para la tecnología 802.11 no tienen la suficiente robustez para asegurar al ciento por ciento los datos que viajan por el aire, y que pueden ser fácilmente capturados por un tercero, el cual tendría todo el tiempo que desee para desencriptar los datos y hacerse de información privada. Con todo esto, se debe estar preparado para posibles ataques a las redes inalámbricas WI-Fi, para cuando estos ocurran, seguir pasos para realizar una investigación forense sobre una red que ha sido vulnerada. Se expone a continuación las características principales de esta rama forense.

1.7 Análisis Forense Digital

La información es el activo más valioso que poseemos en la sociedad actual. Ésta es cada vez más importante para el desarrollo de las empresas y de negocios exitosos a través de la implementación de sistemas de información. Para proteger la información surge una nueva ciencia, la Informática Forense; ésta persigue objetivos preventivos así como reactivos, una vez se ha dado una infiltración en el sistema.

En la actualidad el tema del análisis forense digital está bastante desarrollado en gran parte del mundo, aunque no existen estándares internacionales aceptados aún. Existen proyectos que están en desarrollo como el “CP4DF” (Código de Prácticas para Forensia Digital), de Roger Carhuatocto, el “Open Source Computer Forensics Manual”, de Matías Bevilacqua Trabado, y las “Training Standards and Knowledge Skills and Abilities” de la International Organization on Computer Evidence.

Muchas compañías brindan servicios de recuperación de datos y auditorías de seguridad, pero en particular cada organización dentro de su grupo de especialistas informáticos posee personal con al menos un mínimo conocimiento de cómo actuar una vez ocurrido un incidente. Para bien de estos especialistas o cualquier persona u organización que desee realizar una investigación forense de su sistema, se puede encontrar en Internet una gran cantidad de herramientas con este fin, como por ejemplo:

Dupin Wi-Fi Análisis Forense

Este software ofrece los siguientes servicios:

- Detección de patrones de vulnerabilidades conocidas

- Análisis de los eventos 802.11 de la red
- Detección de anomalías en el protocolo
- Detección de ataques criptográficos 802.11i/WEP

Forensic Toolkit

Es un paquete de herramientas que analiza las especificaciones de ficheros en búsqueda de actividad no autorizada. Algunas características:

- Análisis de punta, permite descifrar y crackear password.
- Permite el uso de una base de datos para manejar su información obtenida.
- Analiza si un servidor revela información mediante NULL Sessions (login anónimo).

Existe en Internet un gran número de sitios, que al igual que personal de la rama de la seguridad informática, hacen referencia a una herramienta en particular, por lo que se puede decir que en estos momentos la herramienta por excelencia, por su profesionalidad y gran reputación en el tema, es el Encase.

Encase

Esta herramienta, con gran presencia en el mercado mundial, satisface desde las necesidades más pequeñas hasta las más complejas. Brinda a los investigadores la capacidad de crear imágenes de unidades y preservarlas usando un formato de archivo de evidencia (LEF o E01), que es un contenedor de pruebas digitales validadas y aprobadas por tribunales de todo el mundo.

Posee además una suite completa de herramientas para el análisis, la preservación y la documentación, a manera de brindar la mayor cantidad de utilidades a los examinadores forenses digitales.

Algunas características específicas:

- Soporte multiplataforma: Windows, Solaris, Macintosh, Linux, etc.
- Crea copias comprimidas de los discos fuente para poder analizarlo, buscarlo y verificarlo.
- Proporciona y documenta eficientemente fechas, horas, registros de accesos, es decir todos los rastros de intervención en un proceso.

- Permite ver archivos borrados, ocultos y los que están en el espacio Unallocated. En este mismo punto es bueno mencionar que EnCase localiza automáticamente y despliega muchos formatos de imágenes, incluyendo las que fueron eliminadas. De todas estas se escogen las imágenes más relevantes para el caso.
- Genera reporte del proceso, mostrando el caso investigado, la evidencia principal, algunos comentarios, imágenes recuperadas, tiempo en que se realizó la búsqueda, entre otros detalles.

En Cuba, no existe ninguna empresa que brinde servicios de investigación forense. Cada organización debe contar con especialistas preparados para afrontar un incidente, siempre y cuando las consecuencias no sean graves y los daños no traspasen la frontera empresarial, informando siempre del incidente a la Oficina de Seguridad para las Redes Informáticas (OSRI), adscripta al Ministerio de la Informática y las Comunicaciones, quienes son los facultados a nivel nacional para hacer este tipo de investigaciones según la RESOLUCION No. 127 /2007[10] a través de la web para el efecto: http://www.cucert.cu/.

Conclusiones del capítulo

En este capítulo se vieron los detalles principales de las redes inalámbricas, así como los protocolos de seguridad para estas redes y los distintos tipos de ataques que pueden sufrir. Se abordaron además las características generales de la forensia digital, y se hizo un estado del arte de la investigación.

[10] https://seguridad.uci.cu/documentacion/Regulaciones%20y%20Normas/R%20127-07%20Reglamento%20de%20Seguridad%20Informatica.pdf

Capítulo II Análisis forense digital

Introducción

Con el advenimiento de Internet y de las posibilidades de conexión por parte de usuarios y empresas a información que se encuentra localizada en cualquier parte del mundo, los administradores de red se han enfrentado al reto de mantener las redes de las compañías en niveles de seguridad requeridos por las mismas, en cuanto al tipo de información que poseen. Al generarse una ruptura de seguridad, se cuenta con la ayuda de los investigadores forenses, cuyo trabajo consiste no solo en conocer el tipo de información que fue comprometida, sino también los daños colaterales que se pudieron ocasionar y si es posible, la persona o personas que ocasionaron dicha ruptura.

Es por esto, que se hace necesario por parte de los investigadores forenses, un conocimiento profundo del funcionamiento de las redes inalámbricas, y de los riesgos que ellas enfrentan, para poder prestarle a las empresas, servicios de soporte preventivo y correctivo ante fallas de seguridad.

El presente capítulo no pretende ni tiene la finalidad de convertirse en manual de referencia para realizar forensia digital, simplemente relata los aspectos básicos relacionados con la Informática Forense a través de 5 fases fundamentales.

2.1 Aspectos Generales

La enorme adopción de las tecnologías inalámbricas en los últimos años, ha colocado a las redes inalámbricas de datos (las más propagadas son las de tipo Wi-Fi) como uno de los principales objetivos de ataques en las organizaciones de hoy en día. Los administradores de red y los agentes de seguridad de esta rama se han visto obligados a hacer frente a la complejidad asociada a esta tecnología cuando tienen que gestionar y dar respuesta a incidentes de seguridad.

La forensia inalámbrica es una disciplina incluida dentro de la ciencia de la informática forense y, específicamente, dentro del campo del análisis forense de redes, y es un término acuñado por Marcus Ranum[11] en 1997. Su objetivo principal es proporcionar la metodología y los instrumentos necesarios para

[11] Experto en firewalls: http://www.securityfocus.com/columnists/334

recopilar y analizar el tráfico de la red inalámbrica, a manera de poder ser presentada esta información como evidencia digital válida en un tribunal de justicia. Por evidencia se entiende a toda la información que se pueda procesar en un análisis.

Este campo de la seguridad es tremendamente heterogéneo e interesante. Analizar un entorno atacado y comprometido es un desafiante ejercicio de aplicación de ingeniería inversa, para el cual es necesario tener gran conocimiento del funcionamiento de los sistemas involucrados, las técnicas de ataque y los rastros que dejan las mismas. Tan presentes están actualmente estas técnicas de análisis en el mundo del cibercrimen, que incluso comienzan a aparecer herramientas anti-forense, es decir, herramientas y técnicas que intentan no dejar rastros, camuflarlos o borrarlos, de tal manera que complican o imposibilitan la realización de un análisis forense sobre los sistemas. La técnica anti-forense más comúnmente usada es la eliminación segura de datos almacenados en dispositivos magnéticos. Las cuales suelen realizarse por medio de aplicaciones como: PGP, Wiper, WinHex, Erase, entre muchas otras que pueden encontrarse en Internet.

La informática forense puede tomar dos vías. La primera propone una finalidad preventiva. Esta sirve a las empresas para auditar, mediante la práctica de diversas pruebas técnicas, que los mecanismos de protección instalados y las condiciones de seguridad aplicadas a los sistemas de información son suficientes. Asimismo, permite detectar las vulnerabilidades de seguridad con el fin de corregirlas. Cuestión que pasa por redactar y elaborar las oportunas políticas sobre uso de los sistemas de información facilitados a los empleados, anticipándose a un posible problema.

Por otro lado, puede tener objetivos correctivos, para brindar una solución favorable una vez que la vulneración y las infracciones ya se han producido. Cuando esto ocurre, la informática forense permite recoger rastros probatorios para averiguar, siguiendo las evidencias electrónicas, el origen del ataque (si es una vulneración externa de la seguridad) o las posibles alteraciones, manipulaciones, fugas o destrucciones de datos a nivel interno de la empresa para determinar las actividades realizadas desde uno o varios equipos concretos. En la presente investigación se sigue esta segunda vía como tema de desarrollo.

2.2 Fases del análisis forense digital

Los incidentes en una red inalámbrica pueden ocurrir de diversas formas, por lo que es poco práctico elaborar procedimientos con instrucciones paso a paso para el manejo de cada incidente. Lo mejor que puede hacer una organización es prepararse para manejar cualquier tipo de incidente y, más específicamente, para manejar los tipos más comunes según la experiencia de los administradores de red.

Dentro del análisis forense digital podemos destacar las siguientes fases, que serán desarrolladas con más detalle más adelante:

1ª. Identificación del incidente.

2ª. Recopilación de evidencias (Crear una *imagen* de los dispositivos sospechosos).

3ª. Preservación de la evidencia.

4ª. Análisis de la evidencia.

5ª. Documentación y presentación de los resultados.

Para muchas organizaciones, la parte más difícil del proceso de respuesta a incidentes es precisamente la detección y la evaluación de los mismos, y en caso de confirmarse alguno, el tipo, extensión y magnitud del problema. Lo que hace esto tan difícil es una combinación de tres factores:

- Los incidentes pueden ser detectados a través de medios diferentes, con distintos niveles de detalle y de fidelidad. La capacidad de detección automatizada incluye Sistemas de Detección de Intrusos (IDS, por sus siglas en inglés) que trabajan tanto para entornos de redes como para *host*, además de software antivirus y los analizadores de *logs*. Los incidentes también pueden ser detectados de forma no automática, como por ejemplo, los problemas reportados por los usuarios. Algunos incidentes pueden ser detectados fácilmente por signos evidentes como el bloqueo de algún servicio, mientras que otros son casi imposibles de detectar sin la automatización.
- El volumen de los posibles incidentes suele ser alto, por ejemplo, no es raro que en una organización se reciban miles o incluso millones de alertas de posibles intrusiones por día.
- Los conocimientos técnicos especializados y la amplia experiencia del personal forense son necesarios para el correcto y eficiente análisis de los datos relacionados con el incidente. En la

mayoría de las organizaciones, las pocas personas con este nivel de conocimientos son probablemente asignados a otras tareas.

Los signos de un incidente se dividen en dos categorías: indicador y precursor. Un precursor es una señal de que un incidente puede ocurrir en el futuro. Un indicador es una señal de que un incidente puede haber ocurrido o que puede estar ocurriendo. Existen innumerables tipos de indicadores, a continuación se exponen algunos ejemplos:

- El sensor de detección de intrusión en la red alerta de un intento de desbordamiento de búfer contra un servidor FTP.
- El software antivirus avisa cuando detecta que una máquina se encuentra infectada por un gusano.
- El servidor Web se bloquea.
- Los usuarios se quejan de la lentitud de acceso a Internet.
- El administrador del sistema observa un nombre de archivo con caracteres inusuales.
- El usuario contacta al servicio de asistencia para informar de un amenazante mensaje de correo electrónico.
- La PC reporta en su *log* un cambio en la configuración.
- Un grupo de usuarios pierde conectividad por el bloqueo de un AP.
- La aplicación de análisis de *logs* reporta múltiples intentos de accesos fallidos de un sistema remoto desconocido.
- El administrador de correo electrónico observa un gran número de e-mails devueltos con contenido sospechoso.
- El administrador de la red detecta una inusual desviación del flujo típico de tráfico de la red.

En algunos casos, la organización puede detectar actividades que pueden preceder a un incidente. Por ejemplo el sensor de un IDS de red puede registrar actividad de escaneo inusual de puertos dirigido a un grupo de hosts, que se produce poco antes de que un ataque DoS fuera lanzado contra uno de los host. En este caso el registro de esta actividad de escaneo sirve como precursor del posterior ataque DoS.

Otros ejemplos de precursores son los siguientes:

- Entradas de registro del servidor Web que muestran el uso de un escáner de vulnerabilidades Web.
- Un anuncio de una nueva vulnerabilidad del servidor de correo.
- Una amenaza externa que implica un ataque a la administración.

No todos los ataques pueden ser detectados a través de los precursores. Algunos ataques no tienen precursor, mientras que otros ataques generan precursores que la organización no puede detectar. Si se detectan precursores, la organización puede tener una oportunidad para evitar el incidente, modificando su postura de seguridad de manera automatizada o manual para proteger al objetivo de ataque. En los casos más graves, la organización podrá decidir actuar como si el incidente estuviese ocurriendo, de modo que el riesgo es mitigado rápidamente. Como mínimo, la organización puede monitorear determinada actividad más detalladamente (tal vez los intentos de conexión a un *host* particular o un determinado tipo de tráfico de la red).

2.2.1 Identificación del incidente

Esta primera fase de identificación del incidente viene aparejada con la fase de búsqueda y recopilación de evidencias. Antes de comenzar con la búsqueda de información, la organización debe asegurarse de que el problema no es trata de hardware ni de software de su red. Ejemplo: un servidor caído por problemas eléctricos o un fallo en el router.

Uno de los primeros lugares donde comenzar la búsqueda de indicios es en los equipos que consideremos comprometidos, hay que tener en cuenta que los atacantes han podido borrar algunos registros locales en esos equipos, pero aún así, puede haber indicios en otras máquinas próximas tales como escaneado de puertos o tráfico inusual en cortafuegos y routers de la red.

El inicio de la investigación es incierto, puede darse caso de que no se aprecie a simple vista ninguna huella o indicio del ataque, especialmente si para realizarlo han empleado e instalado en los equipos un *rootkit*. Para evitar que se eliminen huellas o se modifiquen datos en el equipo lo primero que debe hacerse es crear una imagen del equipo.

Para verificar la integridad de los ficheros del sistema, es necesario contar con utilidades como Tripwire o AIDE (Advance Intrusion Detection Enviroment) especializadas en este tipo de tareas. Es importante conocer los procesos que se están ejecutando en el equipo en busca de que alguno resulte extraño, hay que tener en cuenta aquellos que consuman recursos en exceso, con ubicaciones poco frecuentes en el sistema de archivos, que mantengan conexiones de red en puertos TCP *(*Transmission Control Protocol*)* o *UDP* (User Datagram Protocol) no habituales, etc. A partir de las conexiones mostradas hay que listar todos los puertos TCP y *UDP* abiertos además de los procesos, usuarios y aplicaciones que los utilizan, siempre con la idea de identificar actividad no usual. La aparición en el listado de procesos sin nombre pueden ser indicios de la ejecución de un troyano o puerta trasera (backdoor) en el equipo. Una buena opción sería buscar en Internet alguna referencia sobre el puerto o proceso que pueda resultar sospechoso.

En caso de que queden dudas acerca del incidente hay que consultar los archivos de registro del sistema y *logs* en busca de entradas y avisos sobre fallos de instalación, accesos no autorizados, conexiones erróneas o fallidas. Dependiendo de la plataforma que se emplee se encontrarán estos archivos en distintas ubicaciones:

Microsoft Windows: Este sistema operativo proporciona un entorno para realizar estas búsquedas; si se considera que se trata aún de una aplicación segura, se puede hacer dentro del menú Herramientas administrativas, el Visor de sucesos, el de Servicios o el de la Directiva de seguridad local. Si no se entiende bien la información que estos visores le aportan se puede consultar la base de datos de ayuda de Microsoft. Otro lugar donde se esconde gran cantidad información es el registro de Windows. La aplicación del sistema regedit.exe puede ayudar en esta tarea, pero si no se fía de ella use otras herramientas como reg (permite hacer consultas al registro sin modificarlo), o regdmp (exporta el registro en formato de texto plano: .txt), para su posterior consulta. En estos archivos tendrá que buscar “una aguja en un pajar”, debido a la cantidad de información que almacena y que se mezcla. Un punto de partida podría ser buscar en las claves del registro Run, RunOnce, RunOnceEx, RunServices, RunServicesOnce, Winlogon, pues bajo estas claves se encuentran los servicios, programas y aplicaciones que se cargarán en el inicio del sistema.

UNIX/Linux: En este tipo de sistemas se dispone de una serie de archivos de registro (*logs*), que podremos encontrar habitualmente bajo el directorio /var/log, siendo los más importantes los que se detallan a continuación:

/var/log/messages	Contiene los mensajes generales del sistema.
/var/log/secure	Guarda los sistemas de autenticación y seguridad.
/var/log/wmtp	Guarda un historial de inicio y cierres de sesión pasadas.
/var/run/utmp	Guarda una lista dinámica de quien ha iniciado la sesión.
/var/log/btmp	Guarda cualquier inicio de sesión fallido o erróneo (sólo para Linux).

Tabla 1: Archivos log en Unix/Linux

Además los programas y aplicaciones crean normalmente sus propios archivos de registro, que podrán ser encontrados bajo el directorio /var. Todos estos archivos están en modo texto, por lo que podrá utilizar cualquier editor o visor de texto para buscar indicios del ataque.

Además de estos archivos de registro, también pueden contener indicios los archivos de claves, usuarios y grupos, podrá encontrarlos en /etc/passwd, /etc/shadow, /etc/group. También se pueden encontrar indicios de actividad anómala al consultar el archivo /root/.bash_history que contiene los comandos ejecutados por el usuario root.

Para el propósito inicial de confirmación del ataque o compromiso de sus sistemas estas primeras consultas serán suficientes, aunque se tendrán que volver a utilizar de forma más exhaustiva estos datos tal y como veremos en el apartado de análisis de evidencias.

2.2.2 Recopilación de evidencias

Al concluir que el sistema informático ha sido atacado después de la fase de Identificación del Incidente se pasa a la etapa de recopilación de evidencias.

Antes de realizar cualquier acción hay que estar seguros de tener protegida la imagen del sistema. Una vez cerciorado esto los administradores deben valorar si devuelven el sistema a su estado normal cuanto

antes, lo que hará que se pierdan casi todas las evidencias que los atacantes hayan podido dejar en “la escena del crimen”, eliminando la posibilidad de realizar un análisis forense de lo sucedido que le permita contestar a las preguntas de ¿qué?, ¿cómo?, ¿quién?, ¿de dónde? y ¿cuándo? se comprometió el sistema, e impidiendo incluso llevar a cabo acciones legales posteriores si se diese el caso. Esto también puede que le lleve a volver a trabajar con un sistema vulnerable, exponiéndolo nuevamente a otro ataque.

Se recomienda a los administradores que realicen el análisis forense. Para realizarlo tendrán que seguir una serie de pasos encaminados a recopilar evidencias que le permitan determinar el método de entrada al sistema, la actividad de los intrusos, su identidad y origen, duración del compromiso y todo ello extremando las precauciones para evitar alterar las evidencias durante el proceso de recolección.

Es importante, a partir de este momento, llevar un registro de todas las operaciones que se realicen sobre los sistemas atacados: la fecha, hora de inicio y fin de cada uno de los pasos, las características como números de serie de cada equipo, de sus componentes, de su Sistema Operativo, etc. La recopilación de datos nunca es suficiente, incluso puede hacer fotografías de los equipos y del entorno. Todos estos pasos deben realizarse de manera metódica y profesional para lograr una investigación efectiva.

Existen dos formas para la recolección de evidencias: cuando el sistema está en los llamados estados “frío” y “caliente”. El primero supone el equipo apagado, cuando la información volátil ha sido limpiada. Caso contrario ocurre con el equipo en estado “caliente”, pues el sistema mantiene todos los datos. En el sistema existen pruebas ocultas con diferentes niveles de volatilidad, como los registros del procesador, estructuras de datos en la memoria RAM (Random Access Memory) o memoria de tipo caché, conexiones de red activas, usuarios y procesos actuales, sistema de archivos, etc. Será muy difícil reunir toda esta información a la vez y gran parte de esta se perderá si se decide apagar el equipo de la forma habitual, ya pues en este proceso se realizan una serie de pasos programados para cerrar el sistema de forma limpia, pero si además el atacante ha instalado las herramientas adecuadas éste podría eliminar, modificar y sustituir ficheros a su antojo durante el apagado, y se “limpiarán” también del equipo las huellas de su atacante. Además si el atacante sigue on-line, puede detectar su actividad y actuar con una acción evasiva o, peor aún, destructiva eliminando todo tipo de información.

En caso de realizar una recopilación del equipo en estado “caliente”, las evidencias deben recopilarse siguiendo el orden de mayor a menor volatilidad. Según la RFC 3227[12], se propone utilizar el siguiente orden de volatilidad y por tanto de recopilación de evidencias:

- Registros y contenidos de la caché.
- Contenidos de la memoria.
- Estado de las conexiones de red, tablas de rutas.
- Estado de los procesos en ejecución.
- Contenido del sistema de archivos y de los discos duros.
- Contenido de otros dispositivos de almacenamiento.

Los cuatro primeros puntos representan un tipo de datos volátil, que se perderán o modificarán si apaga o reinicia el sistema, es por tanto muy fácil eliminar estas evidencias de forma inadvertida.

Dentro de las evidencias volátiles será de interés recuperar los siguientes datos del sistema en tiempo real:

- Fecha y hora.
- Procesos activos.
- Conexiones de red.
- Puertos TCP/*UDP* abiertos y aplicaciones asociadas “a la escucha”.
- Usuarios conectados remota y localmente.

El proceso de recopilación de evidencias, en algunos casos, genera poca información, pero en otros puede generar tal cantidad que sea necesario el uso de medios de almacenamiento con una capacidad considerable. En estos casos es aconsejable que se utilice discos externos USB (Universal Serial Bus) para el transporte de grandes cantidades de información. Otra opción es emplear herramientas de transmisión de datos por la red, como por ejemplo Netcat, que permiten enviar toda la información

[12] http://www.faqs.org/rfcs/rfc3227.html

recopilada a un sistema seguro, como por ejemplo un equipo conectado en la misma red o un portátil conectado directamente al sistema afectado.

Tan pronto como se haya obtenido toda la información volátil del sistema se recopila la información contenida en los discos duros, teniendo en cuenta que estos dispositivos no sólo contienen las particiones, los archivos, directorios, etc. Sino que también contienen otro tipo de datos que hacen referencia a los propios archivos y a flujos de información, son los metadatos que serán de gran importancia en el análisis forense.

Cuando se realiza una copia de seguridad de un disco o soporte en general se procede a copiar los archivos tal cual el sistema operativo los "ve", perdiéndose gran cantidad de información oculta en el disco. Por el contrario si realizamos una imagen del disco, creamos una copia bit-a-bit del disco original preservando toda la información que contenga, incluyendo los bloques de los ficheros eliminados, espacio libre tras cada bloque, metadatos, etc.

2.2.3 Preservación de la evidencia

Una vez recopilada la evidencia del ataque, es importante continuar siendo metódico y sobre todo conservar intactas las "huellas del crimen" por lo que no se debe trabajar sobre la copia original de la evidencia. Por lo que se deben realizar como mínimo dos copias de estas, además de generar una suma de comprobación de la integridad de cada copia mediante el empleo de funciones hash tales como MD5[13]. Las copias deben ser etiquetadas para distinguirlas, colocando en ellas como datos principales el nombre, la fecha y hora de la creación.

La información debe ser guardada en un lugar seguro donde solamente el personal autorizado y capacitado para manipularla pueda acceder a ella.

2.2.4 Análisis de la evidencia

Con las evidencias digitales recopiladas y almacenadas de forma segura, se pasa a la fase de Análisis Forense, cuyo objetivo es reconstruir con todos los datos disponibles la línea temporal del ataque o timeline, determinando la cadena de acontecimientos que tuvieron lugar desde el instante inmediatamente

[13] http://www.fourmilab.ch/md5/

anterior al inicio del ataque, hasta el momento de su descubrimiento. Este análisis se puede dar por concluido cuando se conozcan todos o algunos de los siguientes elementos: cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc.

Para esta fase hay que tener en cuenta varios aspectos que se tratan a continuación.

2.2.4.1 Preparación para el análisis: Entorno de trabajo

Como se ha descrito antes, es importante trabajar a partir de las copias realizadas a la imagen de las evidencias. Estas imágenes tienen que ser montadas tal cual estaban en el sistema comprometido.

Lo indicado es preparar dos estaciones de trabajo, en una de ellas, que contendrá al menos dos discos duros, se instalará un sistema operativo que actué de anfitrión y que servirá para realizar el estudio de las evidencias. En ese mismo ordenador y sobre un segundo disco duro, se vuelcan las imágenes manteniendo la estructura de particiones y del sistema de archivos tal y como estaban en el equipo atacado. En el otro equipo se instalará un sistema operativo configurado exactamente igual que el del equipo atacado, además hay que mantener la misma estructura de particiones y ficheros en sus discos duros. La idea es utilizar este segundo ordenador como “conejillo de Indias” y realizar sobre él pruebas y verificaciones conforme vayan surgiendo hipótesis sobre el ataque.

2.2.4.2 Reconstrucción de la secuencia temporal del ataque

Una vez montadas las imágenes del sistema comprometido en la estación de trabajo independiente y con un sistema operativo anfitrión de confianza, el primer paso será crear una línea temporal de sucesos o timeline, para ello se recopila la siguiente información sobre los ficheros:

- *Metadatos* asociados.
- Marcas de tiempo MACD (fecha y hora de modificación, acceso, creación y borrado).
- Ruta completa.
- Tamaño en bytes y tipo de fichero.
- Usuarios y grupos a quien pertenece.
- Permisos de acceso.

- Si fue borrado o no.

Se ordenan los archivos por sus fechas, esta primera comprobación puede ser muy útil, pues la mayoría de los archivos tendrán la fecha de instalación del sistema operativo, por lo que un sistema que se instaló hace meses y que fue comprometido recientemente presentará en los ficheros nuevos, *metadatos* y fechas muy distintas a las de los ficheros más antiguos. El objetivo es buscar ficheros y directorios que han sido creados, modificados o borrados recientemente, o instalaciones de programas posteriores a la del sistema operativo y que además se encuentren en rutas poco comunes. La mayoría de los atacantes y sus herramientas crearán directorios y descargarán sus "aplicaciones" en lugares donde no se suele mirar, como por ejemplo en los directorios temporales.

Luego de buscar los archivos del sistema modificados tras la instalación del sistema operativo, debe descubrir la ubicación de los archivos ocultos para conocer dónde están y de qué tipo son, pues junto a los archivos borrados o los fragmentos de éstos, se pueden encontrar restos de *logs* y registros borrados por los atacantes.

Intentando recuperar el contenido de los archivos eliminados, anotando su fecha de borrado y comparándola con la actividad del resto de los archivos se podría dar con los primeros pasos del ataque.

Se comienza a examinar ahora con más detalle los ficheros *logs* y de registros que ya fueron vistos durante la búsqueda de indicios del ataque, con el objetivo de buscar una correlación temporal entre eventos. Los archivos *log* y de registro son generados de forma automática por el propio sistema operativo o por aplicaciones específicas, conteniendo datos sobre accesos al equipo, errores de inicialización, creación o modificación de usuarios, estado del sistema, etc. Se debe consultar también el archivo de contraseñas buscando la creación de usuarios y cuentas extrañas sobre la hora que se considere que se inició el ataque al sistema.

2.2.4.3 Determinación de cómo se realizó el ataque

Una vez que la cadena de acontecimientos que se produjeron está determinada, se debe determinar cuál fue la vía de entrada al sistema, averiguando qué vulnerabilidad o fallo de administración causó el agujero de seguridad y que herramientas utilizó el atacante para aprovecharse de tal brecha. Estos datos, deben obtenerse de forma metódica igualmente, empleando una combinación de consultas a archivos de *logs*, registro, claves, cuentas de usuarios, etc.

A partir de este punto, se deberían repasar los servicios y procesos abiertos recopilados como evidencia volátil, así como los puertos TCP/*UDP* y conexiones que estaban abiertas cuando el sistema estaba aún "caliente". Se examinan con más detalle aquellas circunstancias que resultaron sospechosas cuando se buscaron indicios sobre el ataque, y se realiza con ellos una búsqueda de vulnerabilidades a través de Internet, empleando motores de búsqueda como Google o utilizando páginas específicas donde se pueden encontrar documentadas cientos de vulnerabilidades[14].

Una vez establecida la vulnerabilidad que dejó al sistema comprometido, como elemento adicional puede hacerse una búsqueda en Internet tratando de encontrar algún *exploit* anterior a la fecha del compromiso, que utilice esa vulnerabilidad[15]. Generalmente se encuentra en forma de *rootkit*.

Es el momento de arrancar y comenzar a utilizar la máquina "conejillo de Indias". Se prueba sobre ella los *exploits* que se han encontrado, para comprobar si la ejecución de ese *exploit* sobre una máquina igual que la comprometida y en perfecto estado, genera los mismos eventos que se han encontrado entre las evidencias recolectadas.

2.2.4.5 Identificación del autor o autores del incidente

Una vez descubierto cómo entraron en el sistema, corresponde ahora saber quién o quiénes lo hicieron. Para este propósito será de utilidad consultar nuevamente algunas evidencias volátiles recopiladas en las primeras fases, revisar las conexiones que estaban abiertas, en qué puertos y qué direcciones IP las solicitaron, además de buscar entre las entradas a los *logs* de conexiones. También puede indagar entre los archivos borrados que recuperó por si el atacante eliminó alguna huella que quedaba en ellos.

La identificación de los atacantes se enfoca al hecho de llevar a cabo acciones legales posteriores o investigaciones internas en la organización. Pero si esta fase no es de importancia, puede obviarse y emplear el tiempo en otras actividades como la recuperación del sistema atacado y mejorar su seguridad.

En caso de abordar esta parte de la investigación, se deben realizar algunas *pesquisas* como parte del proceso de identificación. Para ello es necesario averiguar la dirección IP del atacante, revisando con detenimiento los registros de conexiones de red y los procesos y servicios que se encontraban a la

[14] Como por ejemplo el CERT, www.cert.org o en la base bugtraq en www.securityfocus.com

[15] Será de utilidad la siguiente dirección www.packetstormsecurity.org

escucha. También se podría encontrar esta información en fragmentos de las evidencias volátiles, la memoria virtual o archivos temporales y borrados, como restos de e-mail, conexiones fallidas, etc.

Si se obtiene un IP sospechoso, comprobar en el registro RIPE NCC[16] a quién pertenece. Pero en el caso de encontrarse en una organización, contactar con el administrador de red de la misma para saber su identidad y ubicación.

También para identificar al atacante se pueden hacer uso de técnicas de *hacker* de manera ética, por ejemplo si el atacante dejó ejecutándose en el equipo comprometido un *malware* como una puerta trasera o un troyano, está claro que en el equipo del atacante deberán estar a la escucha esos programas y en los puertos correspondientes, bien esperando noticias o buscando nuevas víctimas. Para esto se utiliza nuevamente el ordenador "conejillo de indias".

2.2.5 Documentación del incidente

Tan pronto como el incidente haya sido detectado, es muy importante comenzar a tomar notas sobre todas las actividades que se lleven a cabo. Cada paso dado debe ser documentado y fechado desde que se descubre el incidente hasta que finalice el proceso de análisis forense, esto hará más eficiente y efectivo el mismo, al tiempo que reducirá las posibilidades de error a la hora de gestionar el incidente.

Por otro lado, cuando se haya concluido el análisis y durante éste, se deben mantener informados a las personas responsables de la organización, por lo que debe ser necesario disponer de diversos métodos de comunicación. Existen muchas prácticas internacionales que se relacionan con la documentación de las evidencias digitales, durante esta investigación se realizó un compendio de algunas y se llega a la conclusión de que al menos se tienen que confeccionar dos tipos de informes, uno Técnico y otro Ejecutivo.

A continuación se explica el contenido de cada uno de estos informes.

[16] www.ripe.net

2.2.5.1 Informe Técnico

Este informe consiste en una exposición detallada del análisis efectuado. Deberá describir en profundidad la metodología, técnicas y hallazgos del equipo forense. Deberá contener, al menos, los siguientes puntos:

- Antecedentes del incidente
- Recolección de los datos
- Descripción de la evidencia
- Entorno del análisis
- Descripción de las herramientas
- Análisis de la evidencia
- Información del sistema analizado
- Características del SO
- Aplicaciones
- Servicios
- Vulnerabilidades
- Metodología
- Descripción de los hallazgos
- Huellas de la intrusión
- Herramientas usadas por el atacante
- Alcance de la intrusión
- El origen del ataque
- Cronología de la intrusión
- Conclusiones
- Recomendaciones específicas
- Referencias

2.2.5.2 Informe Ejecutivo

Este informe consiste en un resumen del análisis efectuado pero empleando una explicación no técnica, con lenguaje común, en el que se expondrán los hechos más destacables de lo ocurrido en el sistema analizado. Constará de pocas páginas, y será de especial interés para exponer lo sucedido a personal no especializado en sistemas informáticos, como pueda ser el departamento de Recursos Humanos, Administración, e incluso algunos directivos. En este informe deberá describir, al menos, lo siguiente:

- Motivos de la intrusión
- Desarrollo de la intrusión
- Resultados del análisis
- Recomendaciones

Estos informes deben ser entregados a las autoridades pertinentes, según las regulaciones de cada país y en particular de cada empresa.

Conclusiones del capítulo

En este capítulo se explicaron las particularidades de la Forensia Inalámbrica y el por qué de su necesidad. Se detalló el proceso investigativo de un Análisis Forense Digital, para el cual se siguieron 5 fases, y se explicaron las actividades generales que se deben realizar en cada una de ellas.

Capítulo III Solución Propuesta

Introducción

Como parte del proyecto de la UCI de desplegar una infraestructura de tecnología inalámbrica utilizando el estándar 802.11, la Dirección de Redes de la universidad posee una propuesta de equipamiento para las áreas docentes y algunas zonas particulares como el Rectorado y la Infraestructura Productiva, que ha sido elaborada por la empresa Tecún, distribuidora de equipamiento tecnológico nacional. En el presente capítulo se brinda una propuesta de cómo realizar un análisis forense digital en los equipos que se montarán en el Docente 1 para la red inalámbrica, sobre la base de que se conoce el equipamiento que se va a utilizar, que fue propuesto y aprobado para su despliegue en la universidad.

3.1 Forensia inalámbrica

En las redes inalámbricas actualmente existe un problema al intentar administrar la evidencia digital, debido a que es difícil definir, producir, obtener y analizar la evidencia. La imposibilidad de aplicar forensia digital por no tener disponible el dispositivo desde el cual se realizó la conexión a la red inalámbrica y analizarlo, obliga a relacionar directamente este problema con la llamada network forensics o forensia en redes, pues esta parte del tema forense especifica que la evidencia debe ser valorada como eventos de la red como tal.

Por tanto, el análisis forense en una red inalámbrica se basa en averiguar después de un ataque, que pasó y cómo pasó, y en correspondencia con los componentes básicos de una red inalámbrica la presente investigación se basa en analizar los *logs* de los APs así como de todos los dispositivos de la red como routers, switch y controladores.

El diseño y producción de los registros electrónicos (generalmente *Log*) es de vital importancia en la gestión de evidencia digital, de estos pasos depende que la evidencia digital exista de forma coherente y luego pueda ser recolectada correctamente.

La infraestructura de una red inalámbrica (APs, Access Controllers, equipos de Red complemantarios) origina una serie de registros de eventos de los cuales forma parte, como los intentos de autenticación, cambios de configuración, petición de algún servicio, etc, pero la capacidad de almacenamiento de éstos

es muy pequeña, lo cual no permite a los investigadores poderle dar seguimiento a un hecho desde sus inicios. Para solucionar este problema es muy usado mundialmente un protocolo para el envío de estos mensajes y poder guardar estos registros en servidores con grandes capacidades de almacenamiento. El protocolo mencionado es un estándar facto[17], y se detalla a continuación:

SYSLOG

Estándar para el envío de mensajes de registro en una red informática. Por syslog se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro. (8)

Un mensaje de registro suele tener información sobre la seguridad del sistema, aunque puede contener cualquier información. Junto con cada mensaje se incluye la fecha y hora del envío.

Los mensajes de syslog se suelen enviar vía *UDP*, por el puerto 514, en formato de texto plano.

Aunque syslog tiene algunos problemas de seguridad, su sencillez ha hecho que muchos dispositivos lo implementen, tanto para enviar como para recibir. Eso hace posible integrar mensajes de varios tipos de sistemas en un solo repositorio central.

Se muestra a continuación el funcionamiento básico de un servidor syslog:

Básicamente los mensajes Syslog son generados por todos los equipos de comunicaciones y son enviados a un Servidor Syslog.

Este servicio soporta 3 roles para su operación: el Dispositivo, el Repetidor[18] y el Colector.

El dispositivo y el colector actúan como fuente y sumidero, respectivamente, de las entradas de un sistema syslog. En el caso más simple, solamente se encuentran presente un dispositivo y un colector:

Ilustración 6: Caso simple de un sistema syslog

[17] Un estándar de facto es aquel patrón o norma que se caracteriza por no haber sido consensuada ni legitimada por un organismo de estandarización al efecto. Por el contrario, se trata de una norma generalmente aceptada y ampliamente utilizada por iniciativa propia de un gran número de interesados.

[18] En la bibliografía consultada aparece como *Relay.*

La relación entre dispositivos y colectores es potencialmente de muchos-a-muchos, ya que un dispositivo puede comunicarse con muchos colectores; y similarmente, un colector puede comunicarse con muchos dispositivos.

Un repetidor opera en ambos modos, aceptando entradas syslog de dispositivos u otros repetidores; o reenviando esas entradas hacia un colector u otros repetidores:

Ilustración 7: Sistema syslog con Repetidores

Como se muestra anteriormente, más de un repetidor puede estar presente entre un dispositivo y el colector.

Un repetidor puede ser necesario por razones administrativas, como por ejemplo, podría correr como una aplicación *proxy* en un firewall. Además podría haber un repetidor por cada departamento de una empresa, el cual autenticaría a todos los dispositivos del departamento, y él mismo se auto autenticaría con el colector de toda la empresa.

Un repetidor puede también servir como un filtro de mensajes. Por ejemplo, puede almacenar la información syslog de todo un servidor web, resumiendo todas las entradas para la generación de reportes. También puede ser usado para convertir los formatos de las salidas de los dispositivos hacia las entradas de los colectores. (9)

Los mensajes que se envían a través de estos elementos se componen de tres campos:

- Prioridad
- Cabecera
- Texto

Entre todos no han de sumar más de 1024 bytes, pero no hay longitud mínima.

PRIORIDAD

La prioridad es un número de 8 bits que indica tanto el recurso (tipo de aparato que ha generado el mensaje) como la severidad (importancia del mensaje), números de 5 y 3 bits respectivamente. Los

recursos y la severidad de los mensajes son numéricamente codificados con valores decimales. A algunos eventos y procesos de sistemas les han sido asignados valores de recursos. Aquellos que no han sido explícitamente asignados pueden usar cualquiera de los códigos "local use". Varios sistemas han asignado comúnmente códigos como se muestra en la siguiente tabla, junto a sus respectivos valores[19]:

CÓDIGOS DE RECURSOS

0	Mensajes del kernel
1	Mensajes del nivel de usuario
2	Sistema de correo
3	*Demonios* de sistema
4	Seguridad/Autorización
5	Mensajes generados internamente por syslogd
6	Subsistema de impresión
7	Subsistema de noticas sobre la red
8	Subsistema UUCP
9	*Demonio* de reloj
10	Seguridad/Autorización
11	*Demonio* de FTP
12	Subsistema de NTP
13	Inspección del registro
14	Alerta sobre el registro
15	*Demonio* de reloj
16	Uso local 0
17	Uso local 1
18	Uso local 2
19	Uso local 3
20	Uso local 4

[19] Según la RFC 3164 - http://www.rfc-editor.org/rfc/rfc3164.txt

21	Uso local 5
22	Uso local 6
23	Uso local 7

Tabla 2: Códigos de Recursos de syslog

CÓDIGOS DE SEVERIDAD

Los 3 bits menos significativos del campo prioridad dan 8 posibles grados.

0	Emergencia: el sistema está inutilizable
1	Alerta: se debe actuar inmediatamente
2	Crítico: condiciones críticas
3	Error: condiciones de error
4	Peligro: condiciones de peligro
5	Aviso: normal, pero condiciones notables
6	Información: mensajes informativos
7	Depuración: mensajes de bajo nivel

Tabla 3: Códigos de Severidad de syslog

CÁLCULO DE LA PRIORIDAD

Para conocer la prioridad final de un mensaje, se aplica la siguiente fórmula:

Prioridad = Recurso * 8 + Severidad

Por ejemplo, un mensaje de Seguridad/Autorización (Recurso = 4) con Severidad = 0 (emergencia), tendría Prioridad igual a 4*8+0 = 32. Uno de Alerta sobre el registro [14] de tipo información [6] tendría 14*8+6=118. Valores más bajos indican mayor prioridad.

CABECERA

El segundo campo de un mensaje syslog, la cabecera, indica tanto el tiempo como el nombre del elemento que emite el mensaje. Esto se escribe en codificación ASCII (7 bits), por tanto es texto legible.

El primer campo, tiempo, se escribe en formato Mmm dd hh:mm:ss, donde Mmm son las iniciales del nombre del mes en inglés, dd, es el día del mes, y el resto es la hora. No se indica el año.

Justo después viene el nombre de elemento (puede ser un hostname), o la dirección IP si se desconoce el nombre. No puede contener espacios, ya que este campo acaba cuando se encuentra el siguiente espacio.

TEXTO

Lo que queda de paquete syslog al llenar la prioridad y la cabecera es el propio texto del mensaje. Éste incluirá información sobre el proceso que ha generado el aviso, normalmente al principio (en los primeros 32 caracteres) y acabado por un carácter no alfanumérico (como un espacio, ":" o "]"). Después, viene el contenido real del mensaje, sin ningún carácter especial para marcar el final.

Actualmente se han desarrollado servidores Syslog Inteligentes que además de registrar los mensajes en archivos de texto, pueden almacenarlos en base de datos y mostrarlos vía Web. Y más aún, permiten crear filtros personalizados sobre los cuales a su vez, se pueden crear múltiples acciones, tales como enviar correos, redireccionar el mensaje a otro servidor Syslog, enviar mensajes a celulares, levantar aplicaciones, etc.

El Servidor Syslog debe estar corriendo en un servidor prendido durante 24 horas al día.

En la propuesta de equipos a instalar para montar la red inalámbrica, no aparece equipamiento que funcione como servidor syslog, por lo que se propone que se incluya un servidor de este tipo en la infraestructura inalámbrica a montar.

Existen en Internet muchas aplicaciones que actúan como servidores syslog, como pueden ser:

WinSyslog

Esta herramienta permite:

- Recibir mensajes de los firewalls y routers
- Soluciona problemas de red (de forma fácil y rápida)
- Cumple con las políticas de las empresas almacenando mensajes log en archivos o base de datos establecidos
- Está siempre alerta (para cuando ocurran condiciones críticas)

- Crea repositorio central de log en ambientes heterogéneos
- Capaz de correr perfectamente sin atención de personal 24 horas por 7 días

Kiwi Syslog Server

Recibe mensajes syslog de los dispositivos de la red, y los visualiza en tiempo real. Las acciones pueden ser programadas como por ejemplo el filtrado de mensajes por nombre de host, host IP, prioridad, cuerpo de mensaje, fecha u hora.

Syslog Watcher Pro

Este servidor syslog reúne todos los mensajes syslog enviados desde distintas fuentes y los concentra para análisis, auditoría y detección avanzada de problemas.

El protocolo Syslog es soportado por todos los equipos de red (conmutadores, enrutadores, corta fuegos, almacenamientos, módems, dispositivos inalámbricos, hosts Unix, etc...), por lo que Syslog Watcher es compatible con dispositivos de todos los fabricantes más importantes (Cisco, Nortel, Juniper, 3Com, HP, etc...). Brinda estas funciones:

- Colectar mensajes syslog.
- Generar reportes syslog.
- Almacenar mensajes syslog de toda una red en un solo lugar.
- Visualizar los syslog colectados en cualquier momento.
- Analizar los syslog en busca de problemas.
- Exportar syslog a CSV o XML
- Notificar de cualquier nuevo mensaje
- Extraer información adicional del contenido de los mensajes.

Syslog-ng

La aplicación syslog-ng es un sistema flexible y de gran escalabilidad para la creación de un servidor syslog. Es compatible con un gran rango de sistemas operativos y plataformas, incluyendo variantes Unix

y versiones de Windows. Puede almacenar mensajes log en archivos encriptados, con firma digital y con firma de tiempo. Provee una gran flexibilidad para la clasificación y administración de los eventos del sistema. Posee una enorme base de datos de usuarios.

Lo principal para la captura de los mensajes syslog es la configuración de cada dispositivo para que envíe sus *logs* hacia la dirección IP del sistema donde se instaló el servidor Syslog y este esté funcionando, o sea, que esté a la escucha de cualquier información que le envíen.

La mayoría de los APs permiten ver una tabla donde se muestran los clientes *DHCP* que están conectados o que estuvieron conectados a la red. A partir de esta información se podría determinar de los números de IP y *direcciones MAC* cuáles están autorizados y cuáles no pertenecen a la red. Los analistas forenses también deben revisar si ha existido algún cambio en la configuración del AP.

3.2 Cómo está estructurada la red inalámbrica en el Docente 1

Los dispositivos que se instalarán en el Docente 1 como parte del proyecto mencionado anteriormente son los siguientes:

AP:

AIR-AP1242AG-A-K9

Item	Especificaciones
Data rate support	802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
Network Standard	IEEE 802.11b and IEEE 802.11g
Frequency Band	Americas (FCC) 2.412 to 2.462 GHz; 11 channels
Antenna	2.4 GHz Radio: Two RP-TNC connectors;
Wireless Modulation	802.11g: Direct sequence spread spectrum (DSSS)

Ilustración 8: Punto de Acceso modelo AIR-AP1242AG-A-K9

Antena (se conecta al AP):

AIR-ANT4941

Item	Especificaciones
Frequency Range	2.4–2.484 GHz
Power	5 watts
Gain	2.2 dBi
Antenna Connector	RP-TNC
Mounting	To RP-TNC Connector
Polarization	Linear
Azimuth 3dB BW	Omnidirectional
Elevations 3dB BW	65 degrees
Dimensions	5.5 in

Ilustración 9: Antena modelo AIR-ANT4941

Wireless Lan Controller

AIR-WLC4402-50-K9

Item	Especificaciones
Cantidad de AP que puede manipular	50 AP Cisco
Wireless	IEEE 802.11a, 802.11b, 802.11g, 802.11d, 802.11h, 802.11n
Wired/Switching/Routing	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, IEEE 802.1Q VLAN tagging, and IEEE 802.1D
Interfaces	2-1Gb Ethernet
Expansion Slots	1
Power Supply	2

Ilustración 10: Controlador de Red Inalámbrica modelo AIR-WLC4402

Switch de pisos

WS-CE500-24PC

Item	Especificaciones
Interfaces	24-10/100 ports for connectivity (PoE) 2-10/100/1000BASE-T or SFP ports for uplink or server connectivity
Inline Power (PoE)	All 24 ports supply 15.4 W
Standards and Cisco Features Supported	IEEE 802.1d, IEEE 802.1q VLAN, IEEE 802.3af, IEEE 802.1x, IEEE 802.1p, IEEE 802.3z, IEEE 802.3ab, IEEE 802.3u, IEEE 802.3, etc
Connectors and Cabling	10/100BASE-TX, Rj45 Cat5 UTP 10/100/1000BASE-T, Rj45 Cat5 UTP 1000BASE-SX, LX, LH, 100BASE-FX, LX, BX : LC fiber connectors (SM &MM)

Ilustración 11: Switch de piso modelo WS-CE500-24PC

Distribución de AP y WLC en el edificio propuestos por Tecún:

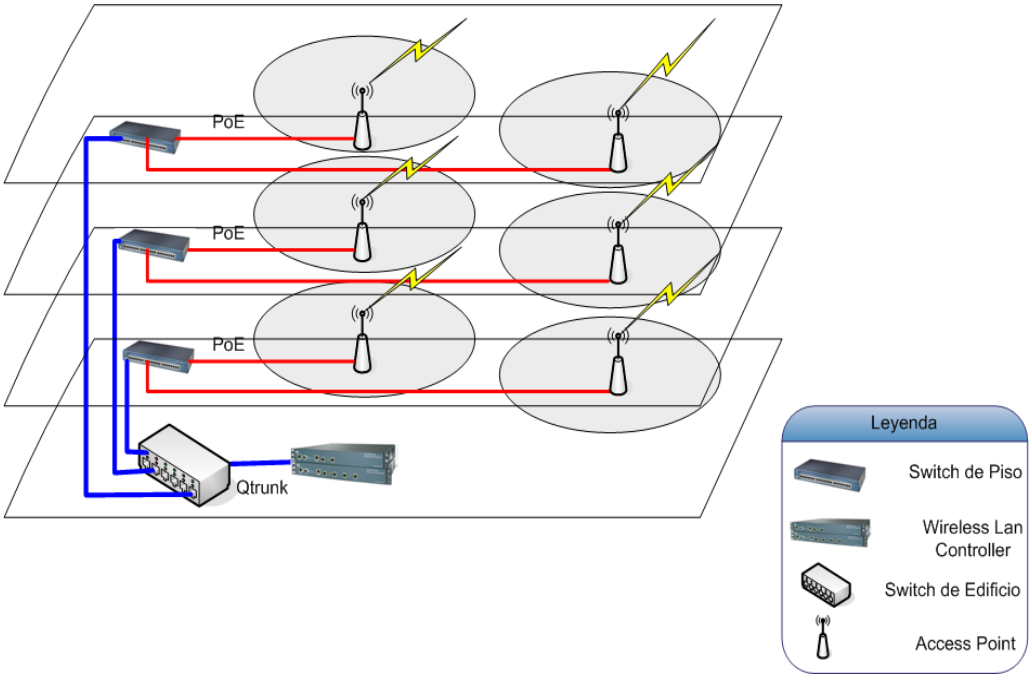

Ilustración 12: Distribución del equipamiento en el edificio

Despliegue de APs en una planta del Docente 1 propuesto por Tecún:

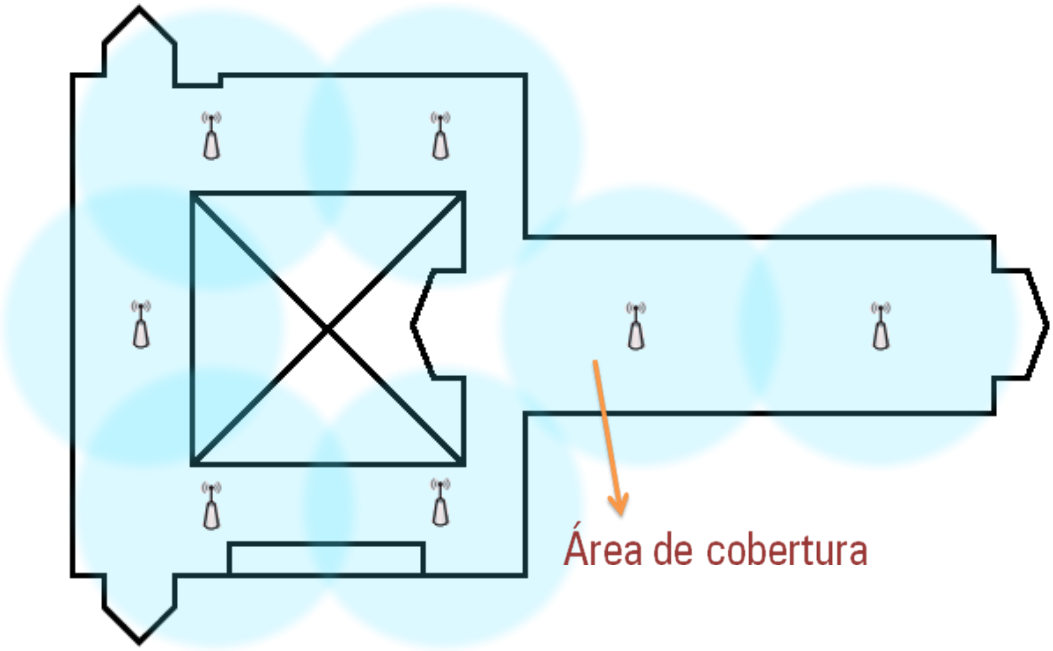

Ilustración 13: Despliegue de los APs en una planta del Docente 1

Cada equipo funciona independientemente, por lo que es necesario incluir dentro de la infraestructura un servidor NTP, de manera que todos estén sincronizados y exista una correspondencia entre los mensajes, así se garantiza que un log enviado por un equipo a una hora determinada coincida en tiempo con otro log enviado desde otro equipo. A continuación se explica en qué consiste un servidor NTP:

NTP

NTP (*Network Time Protocol*), es un protocolo diseñado para sincronizar los relojes de los sistemas informáticos a través de la red. La versión 3 de este protocolo es un *Internet Draft Standard*, formalizado en la RFC 1305. El protocolo NTP versión 4 es una importante revisión del estándar mencionado, y se encuentra en desarrollo, pero aún no ha sido formalizado en una RFC. Una versión simple de NTP (SNTP) versión 4 se describe en la RFC, que es una forma menos compleja de NTP que no requiere almacenar la información respecto a las comunicaciones previas. Este último ha ganado popularidad en dispositivos incrustados y en aplicaciones en las que no se necesita una gran precisión. (10) (11)

NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la *latencia* variable.

3.3 Investigación forense de la red inalámbrica del Docente 1

Es muy importante señalar, que la rama del análisis forense digital es muy amplia, existen muchas herramientas para su desempeño y muchos puntos de recolección de evidencia, por lo que es imposible describir detalladamente un proceso forense, pues además de lo anterior, se depende mucho del ambiente que se vaya a investigar, o sea, del tipo de hardware, de software, del tipo de información que circula, y también de los resultados que se quieran obtener.

Antes de realizar el análisis forense hay que tener una serie de bases sentadas para que la investigación sea más fácil.

Para el análisis forense de la red inalámbrica a montarse en el Docente 1, y siguiendo las fases propuestas en el capítulo anterior a continuación se muestra cómo actuar ante un incidente informático.

3.3.1 Identificación del incidente

Conociendo los tipos de ataques que pueden presentarse en una red inalámbrica, que fueron expuestos en el Capítulo I, se tiene el punto de partida a la hora de la identificación de cualquier incidente, además de que se presente algún indicador que indique claramente que existió o existe un fallo en la red. Una disminución súbita del rendimiento de las máquinas de la red, el uso de un protocolo de red raramente utilizado, o un flujo de red no habitual, pueden ser indicios de que algo extraño se ha estado llevando a cabo. Utilizando esta información se puede ir haciendo una caracterización del problema que ha tenido lugar. Los administradores de red son personas preparadas y con conocimientos suficientes para percatarse de la ocurrencia de algún suceso fuera de lo común en la red; deben chequearse todas las configuraciones de los equipos y ver si hay algún cambio en las mismas. Este personal puede también apoyarse en diferentes herramientas que aparecen en el mercado, como los IDS, ejemplos de estos pueden ser:

WLAN Guardian

Sistema de Detección de Intrusos y Sistema Experto de redes Wi-Fi. Su motor utiliza técnicas avanzadas y patrones de ataques para detectar anomalías en las redes 802.11 como fallos de rendimiento y de

seguridad. Este producto permite a personas con un conocimiento básico de redes inalámbricas poder comprender e interpretar los eventos y detectar los ataques que se están realizando a su red Wi-Fi. Su facilidad de uso le permite a personal con conocimientos básicos comprender los eventos ocurridos en su red inalámbrica, así como guardar un historial y poder seguir los consejos que esta herramienta ofrece en cada situación.

Snort para Linux / Windows

Snort es un sistema de detección de intrusos en la red, de código abierto, capaz de realizar análisis de tráfico en tiempo real y registrar paquetes en redes IP. Puede realizar análisis de protocolo, búsqueda de contenido y puede ser utilizado para detectar una variedad de ataques y sondas, tales como desbordamientos de búfer y escaneo de puertos, entre otras posibilidades.

O los poderosos IDS de la compañía Cisco, que resumen sus funciones de la misma manera que las utilidades anteriores, como:

Cisco IDS 4250 Appliance Sensor

Cisco IDS 4235 Appliance Sensor

Cisco IDS 3.1 Sensor Software[20]

Estos elementos Cisco anteriormente mencionados, a pesar de ser privativos y costosos, poseen alta rentabilidad y fiabilidad, por lo que se sería una buena inversión en caso de utilizarlos.

Cuando se compruebe que se ha producido un incidente debe informarse a la Dirección de Seguridad Informática[21] de la universidad para que el personal competente proceda a la fase 2.

A partir de este punto debe comenzar a tomarse nota de todas las acciones que se lleven a cabo y sus resultados, a manera de poder presentar un correcto informe de lo sucedido.

---

[20] http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/index.shtml

[21] https://seguridad.uci.cu/uci_cert/

3.3.2 Recopilación de evidencias

Como se mostró anteriormente la infraestructura inalámbrica a montarse en el Docente 1 constará de una serie de APs, Switch de piso y un controlador de red inalámbrica (WLC). Cada uno de estos equipos puede ser configurado para mandar los eventos que se producen en ellos a través de mensajes syslog hacia un servidor (o más de uno si se desea) que se encargue de recolectarlos. Una vez configurados todos los equipos para esto, se podrán guardar en un mismo sitio -en caso de que use un solo servidor syslog- toda la información referente a los eventos producidos en la red; y dependiendo de la utilidad que se haya utilizado como servidor, se obtendrá la base de datos de mensajes syslog, pues cada herramienta tiene sus particularidades. Por ejemplo, en caso de utilizar Syslog Watcher Pro, simplemente presionando el ícono de Reporte (Ilustración 14: Exportar Reporte en Syslog Watcher Pro) se puede obtener un reporte completo de todos los eventos en un rango de fecha especificado y/o por severidad.

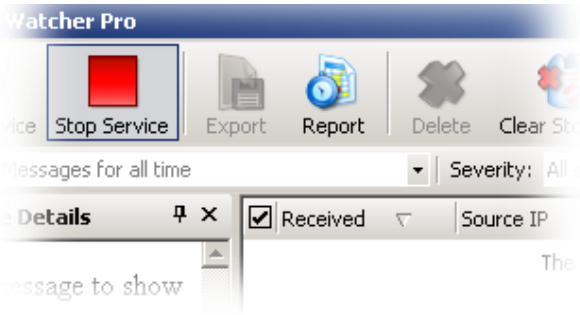

Ilustración 14: Exportar Reporte en Syslog Watcher Pro

Los archivos logs guardados son una importante fuente de información para los investigadores, pero los servidores syslog son una parte del conjunto de evidencias que se puede utilizar. Sería necio pensar que de todo el cúmulo de mensajes guardados, provenientes de varios equipos, se vaya a encontrar aquel que señale lo ocurrido, y que con esta información baste para llevar a cabo la investigación.

Es por esto que en la infraestructura de la red muchas veces los administradores de redes incluyen una herramienta de monitorización de ancho de banda, o sea, para supervisar la carga de tráfico de interfaces de red, comúnmente perteneciente a las herramientas de gestión de la red, por lo que se propone el uso de alguna de estas herramientas. Más adelante se proponen algunas.

Para recolectar la información del tráfico de los dispositivos estas aplicaciones utilizan el protocolo SNMP (Simple Network Management Protocol). Este protocolo proporciona la información en crudo de la cantidad de bytes que han pasado por ellos distinguiendo entre entrada y salida.

SNMP

El Protocolo Simple de Administración de Red es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.

Las versiones de SNMP más utilizadas son dos: SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2). Ambas versiones tienen un número de características en común, pero SNMPv2 ofrece operaciones adicionales.

SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria. (12)

Componentes básicos

Una red administrada a través de SNMP consiste de tres componentes claves:

- Dispositivos administrados
- Agentes
- Sistemas administradores de red (NMS's)

Un dispositivo administrado es un nodo de red que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras. En el caso de estudio de esta investigación, se propone que todos los equipos de la infraestructura inalámbrica cuenten con un agente SNMP para poder supervisar su comportamiento en la red.

Un agente es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de

paquetes IP recibidos, rutas), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

Un NMS ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS's proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red.

Comandos básicos

Los dispositivos administrados son supervisados y controlados usando cuatro comandos SNMP básicos: lectura, escritura, notificación y operaciones transversales.

El comando de lectura es usado por un NMS para supervisar elementos de red. El NMS examina diferentes variables que son mantenidas por los dispositivos administrados.

El comando de escritura es usado por un NMS para controlar elementos de red. El NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados.

El comando de notificación es usado por los dispositivos administrados para reportar eventos en forma asíncrona a un NMS. Cuando cierto tipo de evento ocurre, un dispositivo administrado envía una notificación al NMS.

Las operaciones transversales son usadas por el NMS para determinar qué variables soporta un dispositivo administrado y para recoger secuencialmente información en tablas de variables, como por ejemplo, una tabla de rutas.

Muchas herramientas se han desarrollado en el mercado mundial que utilizan este protocolo para la gestión de la red, como por ejemplo MRTG (Multi Router Traffic Grapher) que genera un informe en formato *HTML* (HyperText Markup Language) con gráficas que proveen una representación visual de la evolución del tráfico a lo largo del tiempo. En la Ilustración 15: Gráfica generada por MRTG del tráfico en una red se muestra un gráfico del tráfico de una red con la utilidad MRTG.

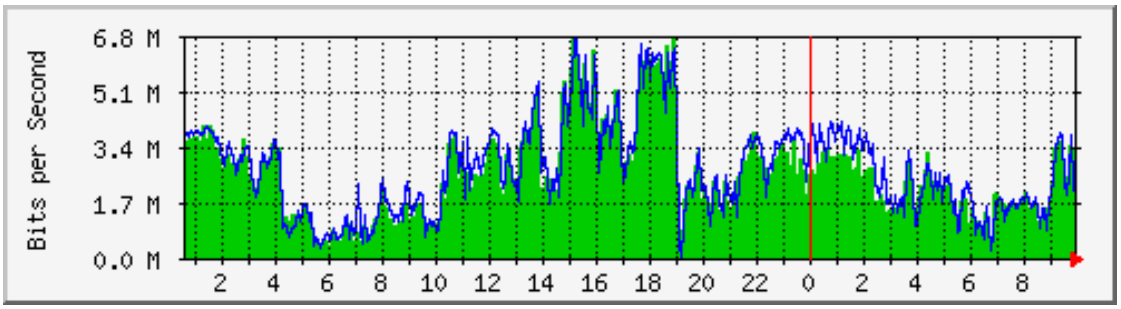

Ilustración 15: Gráfica generada por MRTG del tráfico en una red

CISCO desarrolló también un protocolo denominado NetFlow que permite ver estadísticas muy interesantes de tráfico de red. Esta tecnología ofrece eficientemente la base de medición para un conjunto de aplicaciones incluyendo la contabilidad del tráfico de la red, su planificación, así como el monitoreo de denegación de servicios y supervisión de la red. Cisco proporciona una variedad de aplicaciones NetFlow para coleccionar los datos NetFlow exportados, llevar a cabo la reducción del volumen de datos, post-procesamiento y provee a las aplicaciones de usuario final el acceso fácil de datos NetFlow.

Un ejemplo de herramienta que utiliza este último protocolo es NetFlow Analyzer, para analizar el tráfico de red y reportar el uso del ancho de banda a través de esta. Integra la funcionalidad de respuesta rápida a incidentes de la red, seguimiento más efectivo de gusanos y violaciones de seguridad. (13)

El uso de estas soluciones de gestión que integran las herramientas e información necesarias que ante un incidente permitan correlacionar eventos y llegar más rápido a las causas y su solución es otra parte muy importante de la investigación forense.

Dentro de los equipos planificados para montar la infraestructura inalámbrica, se incluyen dos servidores AAA (Authentication, Authorization and Accounting en inglés, Autenticación, Autorización y Contabilización) replicándose entre ellos para evitar la caída del servicio en caso de que falle alguno.

El modelo específico es el siguiente:

CSACSE-1113-K9

Ítem	Especificaciones
CPU / memoria RAM	3.4 GHz Intel Pentium 4, 800 MHz FSB, 2 MB cache / 1GB RAM
Disco Duro/ Media	80GB / CD / DVD combo
Dimensiones	● 429 (W) x 508 (D) x 42 (H) mm ● 16.9 (W) x 20 (D) x 1.67 (H) in.
Fuente alimentación	345 watt 115vac.
Versión ACS	4.2
Protocolos AAA	Radius / tacacs
Base de Datos	Propia / Directorio Activo de Windows.

Ilustración 16: Servidor AAA modelo CSACSE-1113-K9

Este dispositivo es el Cisco Secure ACS (Access Control Server) que es una plataforma de control de acceso que ayuda a cumplir con los requerimientos de las organizaciones. Mediante la integración con otros sistemas de control de acceso, ayuda a mejorar la productividad y contener los costos. Soporta múltiples escenarios de manera simultánea, incluyendo:

- Administración de dispositivos: Autentica administradores, autoriza comandos, y provee opciones de auditoría.
- Acceso remoto: Trabaja con VPN y otros dispositivos de acceso remoto de la red para reforzar las políticas de acceso.
- Inalámbrica: Autentica y autoriza usuarios y host de redes inalámbricas y refuerza las políticas especificas de estas redes.
- Cisco Secure ACS permite manejar de manera centralizada el acceso a los recursos de la red para una gran variedad de tipos de acceso, dispositivos, y grupos de usuarios.

El trabajo conjunto entre estos servidores, a montar en el nodo central y el Directorio Activo de la Universidad (LDAP) se convertirá en una poderosa herramienta para la seguridad de las redes, pues los

primeros ofrecen una serie de funcionales como las descritas anteriormente, que son propias de los equipos Cisco como el filtrado de MACs, y que se apoyan en el LDAP para la autenticación de los usuarios. De esta manera se obtienen *trazas* de los accesos de los usuarios, anclados junto a otros parámetros como IP del host desde el cual se conectan o AP al que se conectan.

Esto es en cuanto a los dispositivos de la red. Pero cuando es descubierto que un host ha sido atacado, lo primero que debe tenerse en cuenta es no apagar la máquina, de esta manera se conservan todos los procesos en ejecución, los consumos de memoria, las conexiones de red, los puertos abiertos, los servicios que corren en el sistema, etc. No se puede trabajar directamente sobre la PC atacada sino que hay que hacerle una imagen para preservar la evidencia. Así se preservan estos datos volátiles. De esa imagen se sacan 2 copias al menos, una para analizar y otra para entregar a la Dirección de Seguridad Informática.

Con las herramientas propuestas anteriormente se podrán recopilar las evidencias necesarias para pasar a realizar las otras fases del análisis forense.

3.3.3 Preservación de la evidencia

Una vez obtenida esta evidencia es importante asegurar su estado y establecer las políticas de seguridad para que solamente el personal autorizado sea quien la manipule. Es aconsejable según el volumen de información guardarla en algún dispositivo de almacenamiento externo de solo lectura (CD, DVD o Memoria USB con bloqueo de escritura) y crear varias copias de este, las cuales se mantendrán intactas en la Dirección de Seguridad Informática de la universidad.

Se proponen los siguientes pasos para la preservación de la evidencia:

- Asegurar el lugar de los hechos y el área a investigar.
- Mantener la integridad de los datos, buscar siempre la corroboración por testigos, documentar absolutamente todo y observar la legalidad de lo que se haga.
- Fechar las copias digitalmente y etiquetarlas físicamente.
- La preservación debe hacerse de tal forma que los datos originales no sean alterados o modificados.

3.3.4 Análisis de la evidencia

Con los pasos generales de esta fase descritos en el capítulo anterior, se propone a continuación una variante de cómo realizar la investigación forense de la evidencia, la cual no es la única vía para realizar esta actividad, ya que cada persona puede realizar los pasos conforme entienda que debe proceder y según las herramientas que utilice.

Debe tenerse una máquina preparada para volcar la imagen que se obtuvo del dispositivo sospechoso, esto es en el caso de que sea un ordenador el atacado, y se pueda hacer un estudio de los puertos abiertos, las sesiones activas y archivos con nombres extraños. Comparando estos datos con los eventos producidos, brindados por el servidor syslog, se pueden establecer coincidencias de hechos sospechosos, como por ejemplo: un *host* sufre la pérdida de su conexión a la red, y entre los procesos que tiene corriendo se encuentra uno en particular que está utilizando un puerto determinado para hacerle gran cantidad de peticiones al servidor, por lo que este último bloquea la conexión hacia el host, y en el análisis del tráfico de la red, en horario en que ocurría este incidente, aparece la conexión de otro *host* conocido, que transfiere un archivo extraño hacia un recurso compartido del *host* sin bloquear todavía, y seguidamente este informa de la apertura de uno de sus puertos, y comienza la avalancha de peticiones al servidor. De esta forma, se puede entender que debe hacerse un seguimiento del *host* desde el que originó la transferencia del archivo extraño (bien puede ser un gusano de la red) ya que tiene grandes posibilidades de ser la fuente del incidente.

Como ejemplo de recogida de archivos *log* de un sistema en particular, se puede decir que las versiones Windows tienen su principal fuente de Log en los archivos de sistema siguientes:

SysEvent.Evt. Registra los sucesos relativos al sistema

SecEvent.Evt. Registra los sucesos relativos a la seguridad

AppEvent.Evt. Registra los sucesos relativos a aplicaciones

Estos ficheros se encuentran en el directorio systemroot\system32\config. Si están auditadas las opciones de inicio de sesión, cambio de directivas y permisos, hay que centrarse con especial atención en el archivo log SecEvent.Evt. Para visualizar este fichero se puede utilizar la herramienta de Windows eventvwr.msc, comúnmente llamada Visor de Sucesos. Se abre con esta herramienta el archivo SecEvent.Evt, que es el encargado de almacenar los sucesos relativos a la seguridad, tales como

ingresos en la máquina, cambio de directivas, entre otros. Por ejemplo, se podría buscar todo acceso físico a la máquina, cambio de directivas y creación de cuentas de usuario. Eso podría dar una idea de quién "tocó" el sistema.

Otro ejemplo de suceso, sería el relativo a los eventos del sistema. Windows almacena este suceso con el identificador 6005, como se muestra en la siguiente figura:

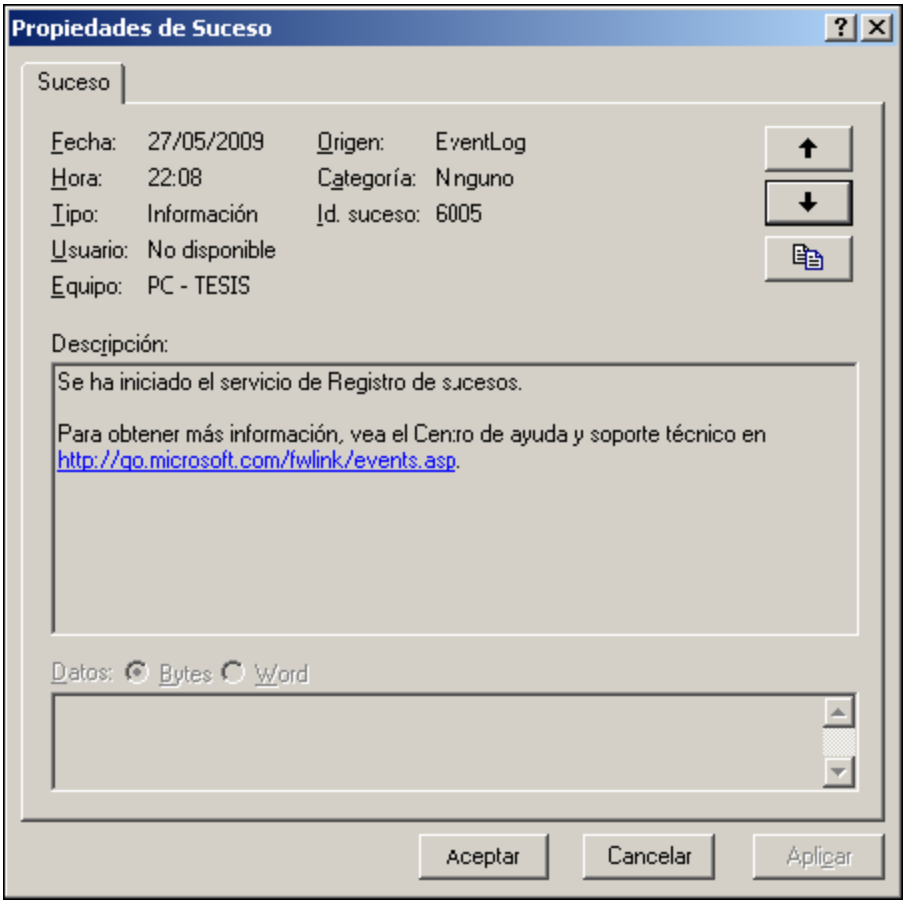

Ilustración 17: Suceso de eventos de sistema Windows

Windows almacena información sobre el usuario que ha iniciado sesión, ID de sesión, tipo de inicio de sesión y nombre de la estación de trabajo.

Windows tiene distintos archivos Log para verificar los posibles sucesos y/o errores que puedan surgir en la vida útil del sistema operativo. Algunos de ellos son:

- WindowsUpdate.log (Log de Windows Update)

- Memory.dump (Archivos de volcado de memoria)
- Archivos de registro de Windows (Software, System)

Por otra parte, el respaldo seguro de las *trazas* y estadísticas es otro elemento muy importante. Esto es utilizado en muchas instituciones, pues permite hacer un almacenamiento histórico de los incidentes ocurridos, y la solución que se les han dado. Esto brinda una especie de Solucionador de Problemas, ya que al ocurrir un evento cualquiera, si se tiene en estas bases de datos de ocurrencias y sus respectivas soluciones en el momento en que se dieron, se puede saber la solución a llevar a cabo automáticamente, sin tener que investigar todo de nuevo.

El proceso investigativo se basa en ir deduciendo los pasos que ha dejado un supuesto atacante. Tiene un origen (puede ser una alarma en el servidor de gestión de una sobrecarga en la red), y a partir de ese punto, con ayuda de las evidencias, se van tomando caminos hacia los dispositivos más específicos, como puede ser un host atacante.

La acción conjunta del servidor syslog, el Cisco Secure ACS y las trazas de las herramientas de gestión de la red, facilita descubrir la identidad de la persona involucrada en el incidente que se investiga, pues la monitorización de la red posibilita un estudio de todo lo acontecido, y de acuerdo a los eventos detectados fuera de lo común o que indiquen la ocurrencia de un incidente, se conoce el horario, la localización (tanto por host IP como por MAC), y a partir de estos datos conjugados con las sesiones de usuarios abiertas puede conocerse quien estuvo involucrado.

La herramienta de gestión de la red casi siempre es la primera en detectar un incidente puesto que está constantemente monitoreando la red en busca de irregularidades o incidentes conocidos. A partir de la información que esta brinda, como puede ser el tráfico por protocolo, el horario y la subred de incidencia, se procede a analizar los mensajes syslog captados por el servidor syslog provenientes de los hosts identificados en el monitoreo. Con este análisis y teniendo la hora como parámetro de búsqueda puede determinarse el IP del host en sospechoso, y empatando con las trazas del ACS y el LDAP puede conocerse la identidad de la persona implicada.

3.3.5 Documentación y presentación de los resultados

Hay que informar a la OSRI de todo cuanto haya ocurrido, y presentar los informes correspondientes. Siguiendo lo propuesto para esta fase en esta investigación, se deben elaborar cada uno de los informes con la información que se describe que debe contener.

Conclusiones del Capítulo

Con la propuesta de actividades a realizar en cada una de las fases que se presenta para el análisis forense se podrá hacer una investigación de los sucesos ocurridos durante el ataque a la red inalámbrica propuesta a montar en el Docente 1 de la UCI. Es preciso resaltar que lo que se propone en esta investigación no es un manual de referencia, sino que es una secuencia de pasos recopilados de la bibliografía existente y que se adaptan a las características de la infraestructura a montar en la universidad.

Conclusiones

De manera general se puede afirmar que se realizó un estudio detallado y actualizado de los estándares de las redes inalámbricas, así como de sus componentes, brindando todo un desglose de cada uno de ellos. Se realizó también una disertación acerca de las vulnerabilidades fundamentales y de los principales ataques que pueden darse en una red inalámbrica, de la misma forma que se dedicó una parte de la investigación a analizar de manera significativa los protocolos de seguridad en redes inalámbricas.

A través del estudio del arte realizado, se fundamentó de forma exhaustiva la investigación, dando elementos que avalan la situación a nivel mundial, regional y nacional del tema tratado, quedando definida la posición de investigador en función de la propuesta a realizar.

Por otra parte se identificaron los elementos relacionados con la detección de brechas de seguridad, que dan los elementos necesarios para introducir el tema del análisis forense, requisito indispensable en este documento, pues finalmente se analizó, teniendo en cuenta los requerimientos establecidos para la instalación de la red inalámbrica del Docente 1 de la Universidad de las Ciencias Informáticas, una propuesta para realizar su análisis forense en caso de que resulte agredida.

Recomendaciones

El equipamiento que se va a desplegar en el Docente 1 de la UCI, lugar exacto en que se centra esta investigación, según la propuesta elaborada por Tecún, es el mismo que se va a utilizar en el resto de los docentes de la universidad, por lo que se recomienda el estudio de esta investigación a nivel universitario y pueda ser utilizada para hacer análisis forense en los otros docentes.

También se propone la utilización de un servidor Syslog, con buen equipamiento (gran capacidad de almacenamiento y velocidad de procesamiento) que funcione para todas las infraestructuras inalámbricas que se monten.

La utilización de software propietario de Cisco para el control de la red es una variante confiable y segura, pero debido a la situación económica del país, se recomienda el estudio de variantes de código abierto libres de costo, que permitan la mayor cantidad de funcionalidades que ofrece Cisco.

Referencias Bibliográficas

1. **http://www.ieee802.org.** [En línea] [Citado el: 24 de Marzo de 2009.] http://www.ieee802.org/15/about.html
2. **Dávila, Yenlys Guerra. 2007.** *Infraestructura para redes inalámbricas de Banda Ancha.* C. Habana : s.n., 2007.
3. **http://tic-iecs.blogspot.com** [En línea] [Citado el: 24 de Marzo de 2009.] http://tic-iecs.blogspot.com/2008/06/ataques-informticos.html
4. **Pino, Dr. Santiago Acurio del. 2008.** *Introducción a la Informática Forense.* 2008.
5. **http://www.computerforensicsworld.com.** [En línea] [Citado el: 17 de Abril de 2009.] http://www.computerforensicsworld.com/modules.php?name=News&file=article&sid=1.
6. **Gonzalo Álvarez Marañón, CSIC**. Amenazas deliberadas a la seguridad de la información. [En línea] 2000. http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html.
7. **http://www.informatica-hoy.com.ar.** [En línea] [Citado el: 6 de Marzo de 2009.] http://www.informatica-hoy.com.ar/redes-inalambricas-wifi/Vulnerabilidades-de-las-redes-WIFI.php.
8. **http://www.busindre.com.** [En línea] [Citado el: 14 de Abril de 2009.] http://www.busindre.com/servidor-gnulinux-syslog-router-cisco/#more-1113
9. **http://tools.ietf.org.** [En línea] [Citado el 14 de Abril de 2009.] http://tools.ietf.org/html/rfc3195
10. **http://www.arcert.gov.ar.** [En línea] [Citado el 28 de Abril de 2009.] http://www.arcert.gov.ar/webs/tips/NTPv1.0.pdf
11. **http://insanecrew.wordpress.com.** [En línea] [Citado el 28 de Abril de 2009.] http://insanecrew.wordpress.com/2008/01/31/el-servicio-ntpd-en-mandriva-2008/
12. **http://networking-switch-cisco.blogspot.com.** [En línea] [Citado el 15 de Mayo de 2009.] http://networking-switch-cisco.blogspot.com/
13. **http://www.manageengine.com.** [En línea] [Citado el 15 de Mayo de 2009.] http://www.manageengine.com/products/netflow/network-bandwith-monitoring.html

Bibliografía

1. http://www.delitosinformaticos.com/. 31 de Marzo de 2009. http://www.delitosinformaticos.com/seguridad/clasificacion.shtml.

2. http://www.segu-info.com.ar. 6 de Marzo de 2009. http://www.segu-info.com.ar/ataques/tipos.htm.

3. http://www.ondata.es. [En línea] [Citado el: 6 de Marzo de 2009.] http://www.ondata.es/formacion/redes_wifi2.htm.

4. http://www.ondata.es. [En línea] [Citado el: 6 de Marzo de 2009.] http://www.ondata.es/recuperar/equipos-forensics.htm.

5. http://www.informatica-hoy.com.ar. [En línea] [Citado el: 6 de Marzo de 2009.] http://www.informatica-hoy.com.ar/redes-inalambricas-wifi/Vulnerabilidades-de-las-redes-WIFI.php.

6. http://es.kioskea.net. [En línea] [Citado el: 6 de Marzo de 2009.] http://es.kioskea.net/contents/attaques/attaques.php3.

7. http://www.cisco.com. [En línea] [Citado el: 25 de Mayo de 2009.] http://www.cisco.com/en/US/docs/wireless/controller/3.2/configuration/guide/c32ovrv.html.

8. http://www.syslog.org/. [En línea] [Citado el: 25 de Mayo de 2009.] http://www.syslog.org/.

9. http://www.cisco.com. [En línea] [Citado el: 25 de Mayo de 2009.] http://www.cisco.com/en/US/products/ps6366/index.html.

10. http://www.provantage.com. [En línea] [Citado el: 25 de Mayo de 2009.] http://www.provantage.com/cisco-systems-air-wlc4402-50-k9~7AIRO08P.htm.

11. http://www.sans.org. [En línea] [Citado el: 23 de Mayo de 2009.] http://www.sans.org/reading_room/whitepapers/wireless/rss/802_11_network_forensic_analysis_33023.

12. http://laconsigna.wordpress.com. [En línea] [Citado el: 23 de Mayo de 2009.] http://laconsigna.wordpress.com/2008/05/26/informatica-forense/.

13. http://www.segu-info.com.ar. [En línea] [Citado el: 4 de Mayo de 2009.] http://www.segu-info.com.ar/boletin/boletin_060603.htm.

14. http://www.revistasic.com. [En línea] [Citado el: 4 de Mayo de 2009.] http://www.revistasic.com/revista53/agorarevista_53.htm.

15. http://www.microsoft.com. [En línea] [Citado el: 3 de Mayo de 2009.] http://www.microsoft.com/spain/empresas/legal/informatica_forense.mspx.

16. http://www.microsoft.com. [En línea] [Citado el: 3 de Mayo de 2009.] http://www.microsoft.com/spain/empresas/legal/forensic.mspx.

17. http://seclists.org. [En línea] [Citado el: 3 de Mayo de 2009.] http://seclists.org/basics/2005/Sep/0110.html.

18. http://www.securityfocus.com. [En línea] [Citado el: 28 de Abril de 2009.] http://www.securityfocus.com/infocus/1885.

19. http://www.virusprot.com. [En línea] [Citado el: 20 de Abril de 2009.] http://www.virusprot.com/WIFI-tecnicas-hacking.htm.

20. http://www.computerforensicsworld.com. [En línea] [Citado el: 17 de Abril de 2009.] http://www.computerforensicsworld.com/modules.php?name=News&file=article&sid=1.

21. http://www.rzw.com.ar. [En línea] [Citado el: 16 de Abril de 2009.] http://www.rzw.com.ar/seguridad-informatica-3765.html.

22. http://www.criptored.upm.es. [En línea] [Citado el: 18 de Marzo de 2009.] http://www.criptored.upm.es/guiateoria/gt_m180b.htm.

23. http://www.criptored.upm.es. [En línea] [Citado el: 18 de Marzo de 2009.] http://www.criptored.upm.es/guiateoria/gt_m142e1.htm.

24. http://www.forensic-es.org. [En línea] [Citado el: 8 de Marzo de 2009.] http://www.forensic-es.org/node/25.

25. http://www.virusprot.com. [En línea] [Citado el: 20 de Mayo de 2009.] http://www.virusprot.com/Nt210371.htm.

26. http://www.borrmart.es. [En línea] [Citado el: 8 de Marzo de 2009.] http://www.borrmart.es/articulo_redseguridad.php?id=1088&numero=23.

27. http://www.cgmenor.com. [En línea] [Citado el: 20 de Mayo de 2009.] http://www.cgmenor.com/pdf/redesinalambricas.pdf.

28. http://www.pdaexpertos.com. [En línea] [Citado el: 22 de Mayo de 2009.] http://www.pdaexpertos.com/Tutoriales/Comunicaciones/como_montar_una_red_wifi_en_casa.shtml.

29. http://www.ieee802.org. [En línea] [Citado el: 5 de Mayo de 2009.] http://www.ieee802.org/11/Reports/802.11_Timelines.htm.

30. http://www.informatica-hoy.com.ar. [En línea] [Citado el: 2 de Abril de 2009.] http://www.informatica-hoy.com.ar/redes-inalambricas-wifi/Seguridad-en-redes-WIFI.php.

31. http://es.kioskea.net. [En línea] [Citado el: 2 de Abril de 2009.] http://es.kioskea.net/contents/wifi/wifiintro.php3.

32. http://www.busindre.com. [En línea] [Citado el: 14 de Abril de 2009.] http://www.busindre.com/servidor-gnulinux-syslog-router-cisco/#more-1113

33. http://tools.ietf.org. [En línea] [Citado el 14 de Abril de 2009.] http://tools.ietf.org/html/rfc3195

34. http://networking-switch-cisco.blogspot.com/. [En línea] [Citado el 15 de Mayo de 2009.] http://networking-switch-cisco.blogspot.com/

35. http://www.manageengine.com. [En línea] [Citado el 15 de Mayo de 2009.] http://www.manageengine.com/products/netflow/network-bandwith-monitoring.html

36. **Dávila, Yenlys Guerra. 2007.** *Infraestructura para redes inalámbricas de Banda Ancha.* C. Habana : s.n., 2007.

37. **Pino, Dr. Santiago Acurio del. 2008.** *Introducción a la Informática Forense.* 2008.

Glosario de Términos

Bluetooth: Esta es una tecnología de ondas de radio de corto alcance (2.4 giga hertzios de frecuencia) cuyo objetivo es el de simplificar las comunicaciones entre dispositivos informáticos, como ordenadores móviles, teléfonos móviles, otros dispositivos de mano y entre estos dispositivos e Internet.

Demonio: Es un tipo especial de proceso informático que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario (es un proceso no interactivo). Este tipo de programas se ejecutan de forma continua (infinita), vale decir, que aunque se intente cerrar o matar el proceso, este continuará en ejecución o se reiniciará automáticamente. Todo esto sin intervención de terceros y sin dependencia de consola alguna. Los programas demonios reciben este nombre en los sistemas UNIX. En otros sistemas existen procesos similares como los TSRs de MS-DOS o los servicios de Windows.

DHCP (Dynamic Host Configuration Protocol): Tecnología utilizada en redes que permite que los equipos que se conecten a una red (con DHCP activado) auto-configuren los datos dirección IP, máscara de subred, puerta de enlace y servidores DNS, de forma que no haya que introducir estos datos manualmente.

Dirección MAC: Es el código único de identificación que tienen todas las tarjetas de red. El accesorio Wi-Fi, al ser un dispositivo de red, también tendrá una dirección MAC única.

Estación: Es una computadora que facilita a los usuarios el acceso a los servidores y periféricos de la red. A diferencia de una computadora aislada, tiene una tarjeta de red y está físicamente conectada por medio de cables u otros medios no guiados con los servidores.

Ethernet: También conocido como estándar IEEE 802.3 aunque se diferencian en uno de los campos de la trama de datos. Es un estándar de transmisión de datos para redes de área local que se basa en el siguiente principio: todos los equipos en una red Ethernet están conectados a la misma línea de comunicación compuesta por cables cilíndricos.

Exploit: (Del inglés to exploit, explotar o aprovechar) es una pieza de software, un fragmento de datos, o una secuencia de comandos que se aprovecha de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o algo electrónico (por

lo general computarizado). Con frecuencia, esto incluye cosas tales como la violenta toma de control de un sistema de cómputo o permitir la escalada de privilegios o un ataque de denegación de servicio.

Hacker: Un hacker denominado "sombrero blanco" es un experto en una o varias ramas de la computación y telecomunicación: redes de comunicación, programación, sistemas operativos, hardware. Su función consiste en buscar defectos, puertas traseras y mejorar la seguridad del software, así como prevenir posibles errores futuros. También existen los llamados hackers "sombreros negros" que utilizan todo el conocimiento que poseen, con fines maliciosos, antimorales o incluso bélicos, como intrusión de redes, acceso ilegal a sistemas gubernamentales, robo de información y muchos más crímenes informáticos.

Host: Es una máquina conectada a una red de ordenadores y que tiene un nombre de equipo (en inglés, hostname). Es un nombre único que se le da a un dispositivo conectado a una red informática. Puede ser un ordenador, un servidor de archivos, un dispositivo de almacenamiento por red, una máquina de fax, impresora, etc. Este nombre, ayuda al administrador de la red a identificar las máquinas sin tener que memorizar una dirección IP para cada una de ellas.

HTML (Lenguaje de Marcas de Hipertexto): Lenguaje de marcado predominante para la construcción de páginas web. Es usado para describir la estructura y el contenido en forma de texto, así como para complementar el texto con objetos tales como imágenes. HTML se escribe en forma de "etiquetas", rodeadas por corchetes angulares (<,>). HTML también puede describir, hasta un cierto punto, la apariencia de un documento, y puede incluir un script (por ejemplo Javascript), el cual puede afectar el comportamiento de navegadores web y otros procesadores de HTML.

Imagen: Copia de seguridad de los datos de un dispositivo electrónico.

Latencia: En redes informáticas de datos se denomina latencia a la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes dentro de la red.

Log: Es un registro oficial de eventos durante un período de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

Malware: Del inglés *Malicious Software*, es un software que tiene como objetivo infiltrarse en el sistema, y dañar la computadora sin el conocimiento de su dueño, con finalidades muy diversas, ya que en esta categoría encontramos desde un troyano a un spyware.

Metadatos: Son datos que describen otros datos. En general, un grupo de metadatos se refiere a un grupo de datos, llamado *recurso*. El concepto de metadatos es análogo al uso de índices para localizar objetos en vez de datos. Por ejemplo, en una biblioteca se usan fichas que especifican autores, títulos, casas editoriales y lugares para buscar libros. Así, los metadatos ayudan a ubicar datos.

Pesquisa: Información o indagación que se hace de algo para averiguar la realidad de ello o sus circunstancias.

Proxy: Programa o dispositivo que realiza una acción en representación de otro. Un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor que está siendo accedido. Cuando se navega a través de un proxy, en realidad no se accede directamente al servidor donde se encuentra el website, sino que se realiza una solicitud sobre el proxy y es éste quien se conecta con el servidor que se quiere acceder y devuelve el resultado de la solicitud. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Puerto: En informática, un puerto es una forma genérica de denominar a una interfaz por la cual diferentes tipos de datos pueden ser enviados y recibidos. Dicha interfaz puede ser física, o puede ser a nivel software (por ej: puertos físicos: puertos USB, puerto de Audio; puertos de nivel de software: puerto 25 para correo electrónico, puerto 21 para FTP).

Punto de acceso (AP): Es un dispositivo que interconecta elementos de comunicación sin cables para formar una red inalámbrica. Es a donde los usuarios inalámbricos se conectan para entrar en la red.

Rootkit: El término viene de la unión de “root” y de “kit”. “Root” se refiere al usuario con máximos derechos en sistemas tipo Unix. “Kit” se refiere a un conjunto de herramientas, por lo que se entiende un rootkit como un conjunto de herramientas con categoría de administrador de un sistema. En la práctica, son programas que una vez instalados en un sistema, efectúan las modificaciones necesarias para poder llevar a cabo las tareas que tiene programadas sin que su presencia pueda ser detectada.

Fundamentalmente, tratan de encubrir a otros procesos que están llevando a cabo acciones maliciosas en el sistema.

Switch: Un conmutador o switch es un dispositivo analógico de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red. Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola.

Traza: Son las huellas digitales que quedan en los sistemas informáticos de todo cuanto ocurre en ellos.

User Datagram Protocol (UDP): Protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión. Tampoco tiene confirmación de entrega o recepción. Su uso principal es para protocolos como DHCP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

VPN: La Red Privada Virtual, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet. Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo su centro de trabajo. Todo ello utilizando la infraestructura de Internet.