UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

SEMINARIO DE GRADUACIÓN "SEGURIDAD INFORMÁTICA"

Tema:

"Análisis De Las Amenazas Informáticas Para La Implementación De Políticas De Seguridad En La Comunicación Inalámbrica De La Empresa Automekano De La Ciudad De Ambato"**.**

Trabajo de Graduación. Modalidad: SEMINARIO, presentado previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

AUTOR: Carlos Ismael Carrillo Miranda

TUTOR: Ing. Xavier Francisco López Andrade

Ambato – Ecuador

Abril 2013

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: **"ANÁLISIS DE LAS AMENAZAS INFORMÁTICAS PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD EN LA COMUNICACIÓN INALÁMBRICA DE LA EMPRESA AUTOMEKANO DE LA CIUDAD DE AMBATO"**, del señor Carlos Ismael Carrillo Miranda, estudiante de la carrera de Ingeniería en Sistemas Informáticos y Computacionales, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato, 26 de Abril del 2013

Ing. Xavier Francisco López Andrade.

AUTORÍA

El presente trabajo de investigación titulado **"ANÁLISIS DE LAS AMENAZAS INFORMÁTICAS PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD EN LA COMUNICACIÓN INALÁMBRICA DE LA EMPRESA AUTOMEKANO DE LA CIUDAD DE AMBATO."**, es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son exclusiva responsabilidad del autor.

Ambato, 26 de Abril del 2013

_____

Carlos Ismael Carrillo Miranda

C.C.: 180327249-9

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. David Guevara, Ing. Luis Solís, revisó y aprobó el Informe Final del trabajo de graduación titulado **"ANÁLISIS DE LAS AMENAZAS INFORMÁTICAS PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD EN LA COMUNICACIÓN INALÁMBRICA DE LA EMPRESA AUTOMEKANO DE LA CIUDAD DE AMBATO."**, presentado por el señor Carlos Ismael Carrillo Miranda de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

_____

Ing. Edison Álvarez Mayorga
PRESIDENTE DEL TRIBUNAL

_____ _____

Ing. David Guevara
DOCENTE CALIFICADOR

Ing. Luis Solís
DOCENTE CALIFICADOR

DEDICATORIA:

El presente trabajo está dedicado a mis amados padres, hermano, abuelitos, enamorada y a todas esas personas que incondicionalmente están junto a mí dándome ese apoyo infinito y palabras de aliento necesarias para seguir adelante y enfrentar los obstáculos de la vida diaria. Pero todo esto no se hubiese logrado sin las bendiciones de Dios, que siempre está conmigo y además guiándome por el camino del bien.

Carlos Ismael Carrillo Miranda.

AGRADECIMIENTO:

Primeramente a Dios que siempre ha sido mi guía, y por haberme bendecido con una familia única, que a pesar de todo obstáculo siempre estamos unidos y apoyándonos entre todos.

En especial al Ing. Xavier Francisco López quien con su experiencia me ha sabido guiar y ayudar en todo lo necesario. También un eterno e infinito agradecimiento a las Compañías Automekano Cía. Ltda. y Ambacar Cía. Ltda. por haber confiado en mí al abrirme sus puertas y a las excelentes e inolvidables personas: Ing. Jorge Parra, Ing. Edit Correa e Ing. Marco Altamirano, gracias por todo su apoyo.

Carlos Ismael Carrillo Miranda.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

El tema del presente trabajo trata sobre el análisis de las amenazas informáticas en la comunicación inalámbrica de la empresa AUTOMEKANO de la ciudad de Ambato y la implementación de políticas de seguridad en dicha empresa.

Para cumplir el objetivo principal de esta investigación, el presente trabajo está estructurado por seis capítulos: en el primer capítulo se plantea de una forma transparente el problema, por qué se decidió realizar el presente proyecto, además se señalan los objetivos que llevaron a la realización de la investigación, así como también la respectiva justificación con argumentos claros con los que se sustenta el porqué de este trabajo.

En el segundo capítulo se encuentran los antecedentes investigativos, la fundamentación legal, las categorías fundamentales que nos servirán para encontrar una posible solución al problema planteado; así como la importante definición de las variables dependiente e independiente.

En el capítulo tercero se describe la modalidad y el nivel de la investigación, la población y muestra, recolección y procesamiento de la información son indispensables y por ende abarcados.

El capítulo cuarto y quinto narran el análisis e interpretación de los resultados de las encuestas realizadas a los usuarios de la Institución, la verificación de la hipótesis y las conclusiones a las que se ha llegado con sus respectivas recomendaciones.

Finalmente el capítulo sexto describe detalladamente la propuesta planteada al problema de investigación y las acciones que se tomaron como consecuencia de dicha propuesta.

INTRODUCCIÓN

Las amenazas informáticas se pueden definir como los problemas o peligros que se aprovechan de las vulnerabilidades existentes en la red o los sistemas informáticos, y tienen como objetivo causar daño. Estas amenazas no solo se refieren a ataques realizados por software, sino también se involucra el factor humano interno/externo de la empresa.

Por otra parte las políticas de seguridad en la comunicación inalámbrica se refieren a la elaboración de un documento donde constan un conjunto de reglas, guías elaboradas y estructuradas con el fin de mantener cierto nivel de seguridad dentro de una empresa o institución.

En la actualidad según varias estadísticas, más del 60% de redes inalámbricas en todo el mundo, se encuentran muy mal protegidas y por ende existe el acceso a las mismas (vulnerabilidades), es notoria la baja aplicación y/o las escasas políticas de seguridad a nivel mundial.

CAPÍTULO I

1.- EL PROBLEMA

1.1 Tema: Análisis de las Amenazas Informáticas para la implementación de políticas de seguridad en la comunicación inalámbrica de la empresa AUTOMEKANO de la ciudad de Ambato**.**

1.2 Planteamiento Del Problema

1.2.1 Contextualización

A lo largo de la historia, de los años, hasta la actualidad, el avance de la informática y de la información se ha venido ampliando satisfactoriamente día a día, al igual que las amenazas informáticas, atentados, vulnerabilidades en dicho avance.

No se toman las debidas precauciones frente a esta situación, por lo que se torna peligroso utilizar cualquier aparato que contenga tecnología inalámbrica, ya sean los mismos computadores, celulares, PDA, etc., además no existe la colaboración que debería prevalecer por parte de los usuarios con un buen trato de la información, una navegación consciente y educada, es por eso que las diferentes amenazas informáticas y ataques están presentes y cada día se fortifican más.

En la actualidad según varias estadísticas, más del 60% de redes inalámbricas en todo el mundo, se encuentran muy mal protegidas y por ende existe el acceso a las mismas

(vulnerabilidades), es notoria también la escasez de políticas de seguridad a nivel mundial.

Las amenazas informáticas están presentes a toda hora, en todo momento y en cualquier lugar, para contrarrestar esto, el camino que se está siguiendo es demasiado lento e impreciso.

Las principales amenazas informáticas que se dan en el mundo actual globalizado son los infaltables virus que han sido uno de los enemigos históricos de los dispositivos electrónicos; también se tiene el escaneo de puertos, wardialers, exploits, control remoto de equipos, eavesdropping, IP spoofing, repetición de transacciones, backdoors, DHCP starvation, trashing, denegación de servicio, denegación de servicio distribuida, software ilegal, pérdida de copias de respaldos, etc.

En la actualidad, los usuarios de computadoras están expuestos a los peligros mencionados al conectarse al Internet o a cualquier otra red.

En el Ecuador la alternativa de usar las nuevas tendencias para la comunicación inalámbrica de acuerdo con el constante crecimiento y la evolución tecnológica, es muy rentable y más aún para los lugares o zonas donde se carece de infraestructura: pero de igual manera las amenazas informáticas para con las comunicaciones inalámbricas siguen en pie, así como también el considerable aumento en los riesgos, ya que en nuestro país según las publicaciones en Internet y GMS: empresa líder en soluciones integradas de telecomunicaciones y seguridades, no se toman los correctivos necesarios para enfrentar, encarar y tratar de reducir este mal que cada vez ataca con más fuerza y es más difícil de detectar, esto se está dando también porque existe poco conocimiento sobre políticas de seguridad informáticas.

De acuerdo al taller “El cibercrimen en Ecuador” realizado por GMS, la mayoría de las empresas públicas o privadas no tienen bien definido este aspecto y se confían

solamente de los servicios que prestan los dispositivos inalámbricos para el control de la seguridad.

AUTOMEKANO desde su creación en la ciudad de Ambato, como en toda empresa de infraestructura grande, se maneja abundante información, la misma que se difunde interna o externamente para sus fines pertinentes. Debido a su crecimiento también se optó por utilizar tecnología inalámbrica para sus comunicaciones, pero no se cuenta con políticas de seguridad para el buen tratamiento de los datos e información en todo ámbito, los usuarios navegan en Internet y están diariamente expuestos a las amenazas informáticas que se encuentran por toda la red, también de cierta manera, consciente o inconscientemente los mismos usuarios internos se convierten en una amenaza informática para la empresa, por lo que no existe un control pertinente sobre aquello.

Las políticas de seguridad en la comunicación inalámbrica no se tienen establecidas frente a posibles ataques y/o amenazas informáticas, son escasas ya que solamente se cuenta con el uso de los antivirus y la confianza en los protocolos de seguridad de sus propios equipos inalámbricos y servidores que se utilizan en la red. Lo cual actualmente no es suficiente porque no se puede controlar el acceso de usuarios no autorizados a la red, captura de los datos que viajan en el aire, intentos de ataque a los servidores principales, lo que la presencia de las amenazas informáticas es evidente.

1.2.2 Árbol del Problema

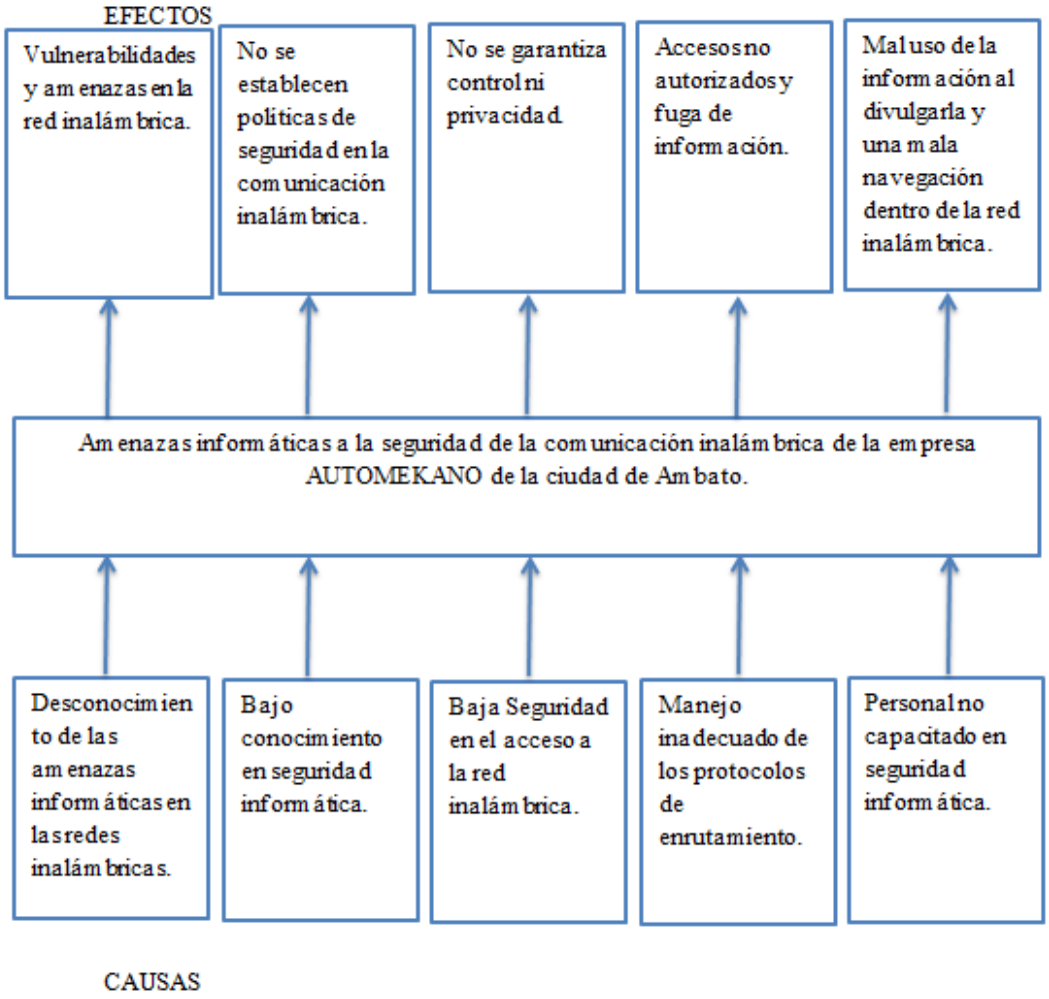


Figura 1. 1 Árbol del Problema. Figura realizada por el investigador.

1.2.3 Análisis Crítico

En la empresa Automekano no se ha tomado muy en cuenta el análisis de las diferentes amenazas informáticas que pueden existir, no solamente en la comunicación inalámbrica, sino también en las redes físicas, esto se da debido al desconocimiento de dichas amenazas informáticas en redes inalámbricas por parte del

personal de Automekano, como consecuencia tenemos la presencia de vulnerabilidades y amenazas en las redes.

El mínimo interés que se pone sobre este mal es notorio, las amenazas informáticas crecen cada día, por eso también se destaca como punto clave, el bajo conocimiento en seguridad informática, y como resultado de ello, no se establecen políticas de seguridad en la comunicación inalámbrica de Automekano.

Otra de las causas importantes es la mala aplicación en sí del término seguridad informática, ya que se tiene una baja seguridad en el acceso a la red inalámbrica, provocando que no se garantice control ni privacidad en el tratamiento de la información dentro y fuera de la empresa.

El manejo inadecuado de los protocolos de enrutamiento es otro de los puntos a tomar en cuenta dentro de Automekano, ya que no se tiene un control sobre estos mecanismos que permiten la comunicación entre los computadores, y las consecuencias son los evidentes accesos no autorizados y la fuga de información.

No tener al personal capacitado en seguridad informática, amenazas informáticas y el daño grave que causan a la información de la empresa es otro de los factores importantes que intervienen en la institución, desencadenando en: el mal uso de la información, al divulgarla y una mala navegación dentro de la red inalámbrica por parte de los usuarios de Automekano.

1.2.4 Prognosis

Si en el caso de que la empresa AUTOMEKANO siga con este escaso control y análisis de las amenazas informáticas a la seguridad de la comunicación inalámbrica, en un corto plazo el mal manejo y la pérdida vital de los datos e información podrían generar descontento, desconfianza en el personal, pérdidas económicas y la posible

mala reputación de la empresa será inevitable por la exposición de los datos perdidos de los usuarios, clientes, etc., de la empresa.

1.2.5 Formulación del Problema

¿Cómo influye el análisis de las amenazas informáticas en la implementación de políticas de seguridad en la comunicación inalámbrica de la empresa AUTOMEKANO de la ciudad de Ambato?

1.2.6 Preguntas Directrices

- ¿Con qué herramientas de hardware y software se contará para el análisis de las amenazas informáticas?

- ¿Con qué método se debe analizar las amenazas informáticas para una correcta implementación de políticas de seguridad en la comunicación inalámbrica?

- ¿Cuáles son los pasos apropiados para el análisis de las amenazas informáticas e implementación de políticas de seguridad en la comunicación inalámbrica?

- ¿De qué manera se debe aplicar los pasos para el análisis de las amenazas informáticas e implementación de políticas de seguridad en la comunicación inalámbrica?

1.2.7 Delimitación del Problema

Campo: Seguridad Informática y de la Información.

Área: Seguridad inalámbrica.

Aspecto: Protección de la información y la red.

Delimitación Espacial: Agencia Principal de “AUTOMEKANO Cía. Ltda.”; ubicada en la ciudad de Ambato, perteneciente a la Provincia de Tungurahua en la Av. Indoamérica km. 1.

Delimitación temporal: 6 meses a partir de la aprobación del proyecto.

1.2.8 Justificación

Se procederá con este proyecto de investigación ya que las amenazas informáticas y la falta de una implementación de políticas de seguridad en la comunicación inalámbrica de la empresa, es un problema a considerar, porque no se está tomando en serio este gran problema de las amenazas informáticas, con su respectivo análisis, el cual constituirá un factor importante a la hora de elaborar una correcta implementación de políticas de seguridad.

Con esto se establecerá mucha certeza y seguridad necesaria para el tratamiento de los datos e información con su correcta manipulación, sin temor a que nuestra información sea robada o caiga en manos de personas equivocadas.

Asimismo se anhela brindar una mayor confiabilidad y reducir notablemente el grado de desconfianza y temor por parte de empleados, gerente, usuarios, etc., al tratar con su información.

El presente trabajo es factible porque se posee los conocimientos necesarios para realizar el proyecto, también se cuenta con el asesoramiento de personal especializado, y las facilidades que proporciona la empresa en cuanto al acceso de la información se refiere. Los beneficiarios del presente trabajo serán los directivos de la

empresa, los empleados quienes manipulan la información, y los usuarios quienes usan Internet para realizar consultas o pedidos.

1.2.9 Objetivo General

Analizar las amenazas informáticas para la implementación de políticas de seguridad en la comunicación inalámbrica de la empresa AUTOMEKANO de la ciudad de Ambato.

1.2.10 Objetivos Específicos

- Establecer los tipos de amenazas informáticas mediante herramientas software en la empresa AUTOMEKANO de la ciudad de Ambato.

- Determinar las vulnerabilidades en base al análisis de las amenazas informáticas en la empresa AUTOMEKANO de la ciudad de Ambato.

- Proponer una solución que permita implementar políticas de seguridad en la comunicación inalámbrica de la empresa AUTOMEKANO para reducir las amenazas informáticas.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes Investigativos

Claudio Armando Cabrera Proaño, Análisis a la Seguridad de Redes Inalámbricas, UTN – FICA – EISIC.
Reposa en Cobuec
http://repositorio.utn.edu.ec/bitstream/123456789/593/1/CAPITULO%20I.pdf

Johanna Morayma Solano Jiménez; Mercedes Beatriz Oña Garcés, Estudio de portales cautivos de gestión de acceso inalámbrico a Internet de la Espoch, 2009.
Reposa en Cobuec
http://dspace.espoch.edu.ec/bitstream/123456789/103/1/18T00381.pdf

Conclusión: Para el investigador, tomar como antecedentes investigativos estos trabajos, ayudará a elaborar y tener un estudio bibliográfico que servirá como referencias para plantear una posible solución a las amenazas informáticas a la comunicación inalámbrica de la empresa AUTOMEKANO.

2.2 Fundamentación Legal

CONSTITUCIÓN POLÍTICA VIGENTE DEL ECUADOR

Sección tercera

Comunicación e Información

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:
1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.

2. El acceso universal a las tecnologías de información y comunicación.

3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas.

4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad.

5. Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación.

Sección novena

Personas usuarias y consumidoras

Art. 52.- Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características.

La ley establecerá los mecanismos de control de calidad y los procedimientos de defensa de las consumidoras y consumidores; y las sanciones por vulneración de estos derechos, la reparación e indemnización por deficiencias, daños o mala calidad de bienes y servicios, y por la interrupción de los servicios públicos que no fuera ocasionada por caso fortuito o fuerza mayor.

Sección octava

Ciencia, tecnología, innovación y saberes ancestrales

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.

2. Recuperar, fortalecer y potenciar los saberes ancestrales.

3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS

TITULO II

DE LAS FIRMAS ELECTRÓNICAS, CERTIFICADOS DE FIRMA ELECTRONICA, ENTIDADES DE CERTIFICACION DE INFORMACIÓN, ORGANISMOS DE PROMOCIÓN DE LOS SERVICIOS ELECTRÓNICOS, Y DE REGULACIÓN Y CONTROL DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS.

CAPÍTULO I

DE LAS FIRMAS ELECTRÓNICAS

Artículo 13.- Firma electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Artículo 14.- Efectos de la firma electrónica. La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio.

Artículo 15.- Requisitos de la firma electrónica.- Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

a) Ser individual y estar vinculada exclusivamente a su titular**;**

b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta Ley y sus reglamentos;

c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado.

d) Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario; y,

e) Que la firma sea controlada por la persona a quien pertenece.

Artículo 16.- La firma electrónica en un mensaje de datos.- Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste. Se presumirá legalmente que el mensaje de datos firmado electrónicamente conlleva la voluntad del emisor, quien se someterá al cumplimiento de las obligaciones contenidas en dicho mensaje de datos, de acuerdo a lo determinado en la Ley.

Artículo 17.- Obligaciones del titular de la firma electrónica.- El titular de la firma electrónica deberá:

a) Cumplir con las obligaciones derivadas del uso de la firma electrónica;

b) Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;

c) Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente;

d) Verificar la exactitud de sus declaraciones.

e) Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia.

f) Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y,

g) Las demás señaladas en la Ley y sus reglamentos.

Artículo 18.- Duración de la firma electrónica.- Las firmas electrónicas tendrán duración indefinida. Podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el Reglamento a esta ley señale.

Artículo 19.- Extinción de la firma electrónica.- La firma electrónica se extinguirá por:

a) Voluntad de su titular;

b) Fallecimiento o incapacidad de su titular**;**

c) Disolución o liquidación de la persona jurídica, titular de la firma;

d) Por causa judicialmente declarada.

La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

TITULO V

DE LAS INFRACCIONES INFORMÁTICAS

CAPÍTULO I

DE LAS INFRACCIONES INFORMATICAS

Artículo 57.- Infracciones Informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente Ley.

Reformas al Código Penal

Artículo 58.- A continuación del Art. 202, inclúyanse los siguientes artículos innumerados:

"Artículo ....- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realizan por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Artículo ...- Obtención y utilización no autorizada de Información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.".

Artículo 59.- Sustitúyase el Art. 262 por el siguiente:

"Art. 262.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo".

Artículo 60.- A continuación del Art. 353, agréguese el siguiente artículo innumerado:

“Art….- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;

2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.”

Artículo 61.- A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

“Art.....- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

Art. .....- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica.".

Artículo 62.- A continuación del Art. 549, introdúzcase el siguiente artículo innumerado:

"Art.... Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

"Art. ….- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;

2. Descubrimiento o descifrado de claves secretas o encriptadas;

3. Utilización de tarjetas magnéticas o perforadas;

4. Utilización de controles o instrumentos de apertura a distancia; y,

5. Violación de seguridades electrónicas, informáticas u otras semejantes.".

Artículo 63.- Añádase como segundo inciso del artículo 563 del Código Penal el siguiente:

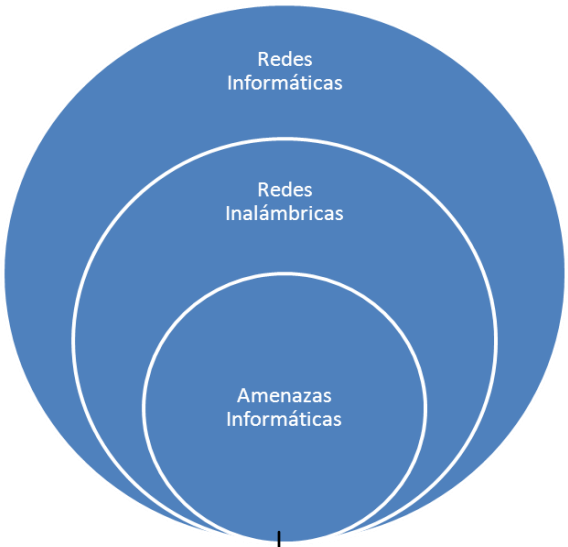
"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando los medios electrónicos o telemáticos".

Artículo 64.- A continuación del numeral 19 del Art. 606 añádase el siguiente:

"..... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.".

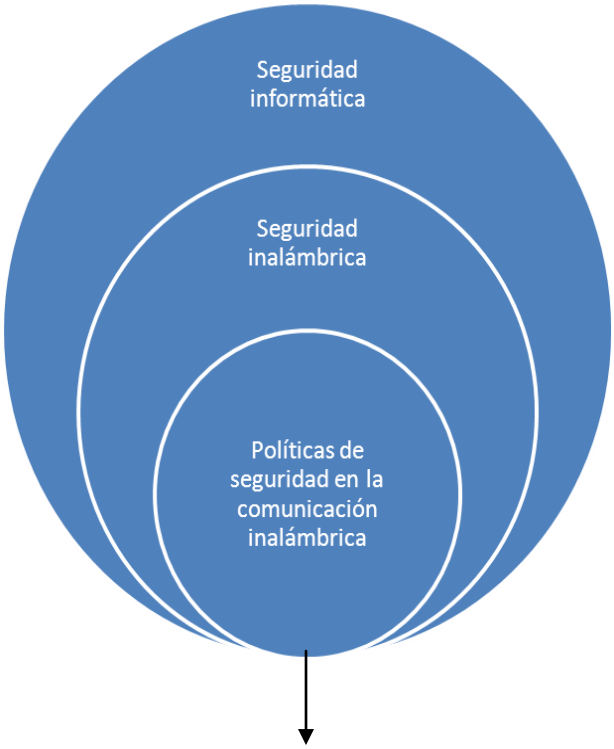
2.3 Categorías Fundamentales

Variable Independiente: Amenazas Informáticas



- Exploits.
- Escaneo de puertos.
- Virus Informático.
- Control remoto de equipos.
- Eavesdropping.
- Denegación de servicios.

Variable Dependiente: Políticas de Seguridad en la Comunicación Inalámbrica



- Tecnología WI-FI: 802.11b, 802.11g, 802.11n, 802.1x.
- Encriptación WEP, WPA, WPA2.
- Filtrado de direcciones MAC.
- Enrutamiento de protocolos.

2.3.1 Redes Informáticas

Una red informática es un conjunto de computadores o dispositivos que se encuentran conectados entre sí con la finalidad de compartir recursos, ya sea mediante enlaces no físicos y/o físicos. La conexión mediante medios físicos se lo realiza con cables, y si no se utilizan conexiones físicas se está hablando de redes inalámbricas.

Como lo manifiesta DORDOIGNE José (2006, pág.10) "Una red es un medio que permite a personas o grupos compartir información y servicios. La tecnología de las redes informáticas constituye el conjunto de las herramientas que permiten a los ordenadores compartir información y recursos.

Una red está constituida por equipos llamados nodos. Las redes se categorizan en función de su amplitud y de su ámbito de aplicación.

Para comunicarse entre ellos los nodos utilizan protocolos, o lenguajes, comprensibles para todos ellos".

Una red de ordenadores es un sistema en el que los ordenadores están conectados para compartir información y recursos. La conexión se puede hacer de uno a uno o cliente / servidor.

Ventajas de las Redes Informáticas

- Una de las ventajas en cuanto se refiere al manejo de los datos e información, es notoria dicha ventaja, ya que la manipulación y distribución de los datos es mucho mejor, los cuales se encuentran concentrados (centralizados) en un servidor.

- El mejoramiento de la red y velocidad depende del tipo de cable que se utilice para la conformación de la misma.

- Otra ventaja es la utilización de sistemas distribuidos para las empresas o instituciones.

Desventajas de las Redes Informáticas

- Aumento de riesgos en cuanto tiene que ver con la seguridad (interna y/o externa).

- Dependiendo del tipo de red a implementar, el costo es un factor importante, si se habla a nivel empresarial.

2.3.2 Redes Inalámbricas

Una red inalámbrica no es más que interconectar varios y distintos dispositivos entre sí, para que tengan la capacidad de compartir información, pero sin la utilización de medios físicos de transmisión (sin cables). Estos dispositivos no necesariamente tienen que ser computadores, pueden ser de varias formas y tecnologías.

Como se menciona en la publicación (Internet, 2010, 21-10-2011 19:30:00) "Una red WLAN (Wireless Local Area Network) o Red de Área Local inalámbrica, es un sistema de comunicaciones de datos flexible que se incorpora como una extensión o una alternativa a la red LAN cableada.

Utiliza ondas de radio de alta frecuencia en lugar de cables para la transmisión y recepción de datos, minimizando la necesidad de conexiones con cable, de esta forma las redes WLAN combinan la conectividad de datos con la movilidad del usuario (José M. Caballero, 1998)".

Ventajas de las Redes Inalámbricas

- **Flexibilidad**

  La flexibilidad se refiere a la extensión o expansión hasta donde llega la señal emitida en una red inalámbrica, lo que facilita el uso de los dispositivos conectados a la red (sin utilización del cable), haciéndolo más cómodo.

- **Reducción de la Planificación**

  A diferencia de como se lo hace con las redes cableadas, lo único que se debe tener en cuenta es que el área donde se va a poner en funcionamiento la red, esté dentro de la cobertura de red.

- **Robustez**

  Dependiendo de los desastres que se pueden dar en una red cableada, como por ejemplo desconectar los cables involuntariamente o el mal funcionamiento de los mismos; ya sea también por desastres naturales, estas redes podrían quedar no disponibles, en cambio una red inalámbrica soportaría mucho mejor este tipo de circunstancias e inconvenientes.

Desventajas de las Redes Inalámbricas

- **Calidad de Servicio**

El servicio es muy bajo respecto a las redes cableadas, por ejemplo en la velocidad, las redes cableadas son mucho mejor, las comunicaciones en las redes inalámbricas son bien lentas.

- **Soluciones Propietarias**

  Se maneja un poco lo que es el monopolio, ya que algunas empresas han elaborado y desarrollado soluciones a ciertas falencias o necesidades, entonces empresas que se encuentren atadas a las soluciones propietarias de cierta manera, si se necesita algún tipo de mantenimiento o soporte en el sistema se deberá recurrir siempre a la empresa propietaria que brinda dichos servicios, sin poder romper el círculo del monopolio.

- **Restricciones**

  Por ejemplo tenemos la limitación en el ancho de banda para la transmisión de los datos. También depende de ciertas políticas y reglas de cada país, empresa, institución.

- **Seguridad**

  De acuerdo a la tecnología o políticas de seguridad que se utilicen a la hora de planificar una red inalámbrica, a futuro se evaluará si no existen posibles atentados, robos de información. Existen varias amenazas informáticas en cuanto se refiere a las redes inalámbricas.

2.3.3 Amenazas Informáticas

Las amenazas son intentos de hacer daño, si existen vulnerabilidades o puertas abiertas en las redes inalámbricas o en los sistemas de las empresas o instituciones,

estos huecos o puertas son aprovechadas por las amenazas, generándose los distintos ataques que puede existir.

Según la publicación (Internet, 03-12-2006, 19-10-2011 15:28:00) "México, DF.- El robo y suplantación de identidad en Internet se ha convertido en un problema de seguridad de alcance nacional que afecta tanto al patrimonio como a la integridad física y psicológica de los miles de usuarios de la llamada supercarretera de la información.

Arropados por el anonimato, ya sea en grupo o en solitario, expertos en informática conocidos como ¿hackers?, obtienen ilegalmente contraseñas, números de cuentas, claves de tarjetas de crédito, así como información personal almacenada en correos electrónicos que puede convertirse en materia útil para secuestros y extorsiones.

¿Quién no ha guardado en sus correos electrónicos fotografías, datos personales, cartas y otros documentos de los que se podrían inferir parentescos y relaciones afectivas que podrían resultar potencialmente peligrosas de caer en manos equivocadas?".

Aspectos Fundamentales y Principales Amenazas Informáticas

Como se menciona en la publicación (Internet, 01-06-2004, 10-10-2011 09:46:00) "Se debe tomar en cuenta los desafíos para poder desarrollar nuevos métodos de protección contra los ataques.

Establecimiento de claves, autenticación, privacidad, robustez frente a ataques de negación de servicio, enrutamiento seguro, captura de nodos".

Algunos de los ataques más comunes son:

- ✓ SSID (network name) sniffing.
- ✓ WEP (ataques contra llaves).
- ✓ ARP envenenamiento.
- ✓ MAC spoofing
- ✓ Access Point, claves (ataques).
- ✓ Negación de Servicio.
- ✓ Suplantación de direcciones MAC.

- **Sniffing**

  Como los datos viajan por el aire, es más fácil que pueden ser interceptados, capturados por los atacantes, peor aún si no llevan una encriptación. El tráfico en redes inalámbricas es mucho más vulnerable que en una LAN, sólo se necesita una laptop con tarjeta de red inalámbrica.

- **Análisis de Tráfico**

  Al ser examinado por el atacante el tráfico de una red, ya obtendrá información, por ejemplo cuando existe tráfico, en que momento, lugar, etc.

- **Suplantación**

  Hay varias maneras, por ejemplo instalando y configurando un Punto de Acceso falso, para llamar la atención de la víctima y así se conecte a él. También se lo puede hacer mediante un sniffer para hacerse con las direcciones MAC válidas.

- **DOS**

  DOS significa denegación de servicios, el atacante puede interceptar y puede modificar los datos que envía un usuario hacia otro o hacia un determinado servidor.

2.3.4 Seguridad Informática

Según la publicación (Internet, s.f., 09-10-2011 17:05:00) ¨La seguridad informática se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.”.

Como se dice en la publicación de IEEE (Internet, 01-01-2003, 19-10-2011 18:41:00) “Seguridad informática y de red, o la seguridad cibernética, son problemas críticos. Pero la mera protección de los sistemas que contienen datos sobre los ciudadanos, empresas y agencias del gobierno no es suficiente. La infraestructura de redes, routers, servidores de nombres de dominio, y los interruptores que pegar estos sistemas juntos, no debe fallar, o las computadoras ya no serán capaces de comunicarse de forma precisa o fiable.”.

La seguridad informatica es una disciplina que se ocupa de diseñar las normas, procedimientos, funciones, metodos y tecnicas para conseguir que un sistema o una red cuente con todos los pilares básicos de la seguridad.

2.3.5 Seguridad Inalámbrica

Si los recursos, información, componentes, etc. son utilizados por personas o usuarios autorizados (de confianza), se puede decir que la red es segura y confiable. Pero hay que tomar en cuenta que los ataques no solo pueden ser externos, también los hay internos, personas de la misma organización o empresa.

La seguridad física también puede ser afectada ya que con o sin intención los usuarios pueden tener contacto con los dispositivos; y desconectarse de la red. No solo los usuarios pueden tener contacto, también existen amenazas de tipo natural, etc. para ello se recomienda proteger los dispositivos de la humedad, agua, organizar bien el cableado.

Pese que el estándar IEEE 802.11 tiene mecanismos de seguridad (claves encriptadas, autenticación, etc.) hace falta mucho más hoy en día, luego se ha implementado WPA y sus variantes. Pero cada día debe haber más investigación para poder implementar métodos efectivos que permitan reducir los riesgos, porque cortarlos de raíz es casi imposible.

La información que se transmite en las redes inalámbricas se lo hace por medio de ondas de radiofrecuencia (RF), esto quiere decir que los datos viajan por el aire y están expuestos a que alguien capture dicha información durante el viaje.

Es vital primero analizar, identificar, detectar las posibles y amenazas potenciales, para poder diseñar y establecer políticas de seguridad, ya sea en base a mecanismos de seguridad, o por cualquier otro método factible.

Como lo comenta ROLDAN David (2005, pág.162) “Cualquier red inalámbrica se caracteriza porque emplea como medio de transmisión el aire. Esto quiere decir que, al menos en principio, cualquier persona equipada con los dispositivos adecuados

puede acceder a la información que transita por la red. Por esta razón, es necesario tomar medidas que eviten, por un lado, que usuarios no autorizados se conecten a la red (o, ciertos servicios que se implementan sobre ella) y, por otro, la confidencialidad de las comunicaciones entre dos usuarios".

Estándares y Tecnologías Inalámbricas

- **WIFI**

  También llamada 802.11; es la tecnología de redes de área local inalámbrica más explotada. El diseño y creación de esta tecnología empezó en 1997, a partir de ahí se aplicaron varios estándares como son 802.11a, 802.11b, 802.11g, 802.11x, 802.11i, 802.11n. 802.11 permite vincular equipos que se encuentren a distancias de aproximadamente 90 metros (300 pies) con una velocidad compartida que ondea entre una docena de Megabits por segundo (Mbps) a varias docenas de Mbps.

2.3.6 Políticas De Seguridad en la Comunicación Inalámbrica

Las políticas de seguridad informática son consideradas como herramientas organizacionales, que tienen como objetivo, concientizar a todos y cada uno de los empleados de la o las organizaciones, instituciones, empresas, sobre la importancia y lo tan vulnerable que es la información.

Algunas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos, directrices y recomendaciones que orientan en el uso correcto de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

Una Política de Seguridad es un conjunto de requisitos donde se establece en términos generales que se permite y que no en el área de seguridad durante la operación general del sistema.

La RFC 1244 define Política de Seguridad como: una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán.

Como se menciona en la publicación (Internet, 16-10-2008 , 10-10-2011 22:26:00) "Uno de los primeros pasos que debe dar una compañía es definir una política de seguridad que pueda implementar en función a las siguientes cuatro etapas:

- Identificar las necesidades de seguridad y los riesgos informáticos que enfrenta la compañía así como sus posibles consecuencias
- Proporcionar una perspectiva general de las reglas y los procedimientos que deben implementarse para afrontar los riesgos identificados en los diferentes departamentos de la organización
- Controlar y detectar las vulnerabilidades del sistema de información, y mantenerse informado acerca de las falencias en las aplicaciones y en los materiales que se usan
- Definir las acciones a realizar y las personas a contactar en caso de detectar una amenaza

La política de seguridad comprende todas las reglas de seguridad que sigue una organización (en el sentido general de la palabra). Por lo tanto, la administración de la organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.".

2.4 Hipótesis

El análisis de las amenazas informáticas influirá en la implementación de políticas de seguridad en la comunicación inalámbrica de la empresa AUTOMEKANO de la ciudad de Ambato en el I semestre del 2011.

Unidades de observación: empleados y usuarios de AUTOMEKANO en la ciudad de Ambato.

2.5 Señalamiento de Variables

Variable independiente = Amenazas informáticas.

Variable dependiente = Políticas de seguridad en la comunicación inalámbrica.

CAPÍTULO III

3.1 Enfoque

El presente trabajo investigativo tomará un enfoque cuali-cuantitativo con las siguientes consideraciones:

Participativa, ya que se tomará muy en cuenta los criterios, opiniones de cada una de las personas involucradas en el problema.

Humanista, porque se llevará a cabo conjuntamente el desarrollo humano y tecnológico, para el crecimiento ético, moral, profesional de cada persona.

Interna, obviamente para un análisis a fondo del problema en la parte interna de la empresa.

Nomotética, porque el proyecto tiende a un solo sentido o dirección.

Externa, analizar a fondo las amenazas externas, las que afectarían a los involucrados.

3.2 Modalidades básicas de la investigación

La presente investigación tiene las siguientes modalidades:

Modalidad bibliográfica o documentada: Se ha considerado esta modalidad ya que Se utilizarán libros, manuales, páginas de Internet, bibliotecas virtuales y monografías que brindarán un aporte vital al análisis de las amenazas informáticas en una forma adecuada.

Modalidad experimental: Se ha considerado la relación de la variable independiente: Amenazas informáticas y su influencia y relación en la variable dependiente: Políticas de seguridad en la comunicación inalámbrica para considerar sus causas y efectos.

La modalidad de campo: Se ha considerado esta modalidad ya que el investigador irá a recoger la información primaria directamente de los involucrados a través de una encuesta; y de esta manera podemos conocer mejor los inconvenientes que se producen en la Empresa al no contar con un análisis de las amenazas informáticas.

3.3 Tipos de Investigación

Se ha realizado la investigación exploratoria, ya que permitió plantear el problema de investigación: Amenazas informáticas a la seguridad en la comunicación inalámbrica de la empresa AUTOMEKANO de la ciudad de Ambato.

Como de la misma manera ayudó a plantear la hipótesis: El análisis de las amenazas informáticas influirá en la implementación de políticas de seguridad en la comunicación inalámbrica de la empresa AUTOMEKANO de la ciudad de Ambato en el I semestre del 2011.

Se ha considerado la investigación descriptiva porque permitió analizar el problema en sus partes como delimitar en tiempo y en espacio construyendo el análisis crítico, la contextualización y los antecedentes investigativos.

Por otro lado se ha tomado la investigación correlacional ya que ha permitido medir la compatibilidad de la variable independiente: las amenazas informáticas con la variable dependiente: implementación de políticas de seguridad en la comunicación inalámbrica.

3.4 Población y muestra

La población considerada para la presente investigación son los empleados de la empresa AUTOMEKANO, en total son 27 empleados, de los cuales la muestra a tomar son 8 personas, los mismos que desempeñan labores de jefes del departamento de sistemas y empleados de talleres, ventas externas.

Departamento	Funcionarios
Sistemas	3
Talleres, Ventas	5
TOTAL	8

Tabla 3. 1 Número de funcionarios por Departamento de Automekano

3.5 Operacionalización de Variables

Variable Independiente: Amenazas Informáticas

Conceptualizaciones	**Categorías**	**Indicadores**	**Ítems**	**Técnicas e Instrumentos**
Amenazas informáticas.- Son intentos de hacer daños, principalmente a las redes inalámbricas y/o a los sistemas de las empresas. Existen varios tipos de amenazas informáticas.	Daños.	En los sistemas. Debilidades en la red. En los Puertos. Software. Conexión.	¿Alguna vez notó algún comportamiento extraño o fuera de lo común dentro de la red inalámbrica, como por ejemplo direcciones IP duplicadas, fallos en la conexión, etc.? ¿Ha notado algún comportamiento extraño mientras está	Encuestas, cuestionarios.

Conceptualizaciones	Categorías	Indicadores	Ítems	Técnicas e Instrumentos
			conectado a la red inalámbrica?	
	Redes inalámbricas.	Interconexión de dispositivos. Intercambio de información. Seguridad.	¿Se maneja algún servidor configurado que sirva para garantizar la comunicación inalámbrica? ¿Qué tipo de información es considerada vital dentro de la empresa AUTOMEKANO? ¿Ha tenido más de una vez problemas para	Encuestas, cuestionarios.

Conceptualizaciones	Categorías	Indicadores	Ítems	Técnicas e Instrumentos
			conectarse a la red inalámbrica? ¿Verifica de alguna forma si la información que recibe dentro de la red es del remitente correcto? ¿Cree usted que la navegación dentro de la red inalámbrica es segura? ¿Para conectarse a la red inalámbrica utiliza una	

Conceptualizaciones	Categorías	Indicadores	Ítems	Técnicas e Instrumentos
			contraseña? ¿Qué le parece el servicio de la red inalámbrica? ¿Cuántos dispositivos para la comunicación inalámbrica se utilizan y que mecanismos de seguridad se aplican en cada uno de ellos?	
	Tipos de Amenazas informáticas.	Virus. Gusanos. Troyanos.	¿Conoce sobre los diferentes tipos de amenazas informáticas	Encuestas, cuestionarios.

Conceptualizaciones	Categorías	Indicadores	Ítems	Técnicas e Instrumentos
		Negación de servicios. Exploits.	que existen en las redes inalámbricas?	

Tabla 3. 2 Operacionalización de la variable independiente

Variable dependiente: Políticas de Seguridad en la comunicación inalámbrica.

Conceptualizaciones	Categorías	Indicadores	Ítems	Técnicas e Instrumentos
Políticas de Seguridad en la comunicación Inalámbrica.- Establecer normas mediante una serie de procedimientos para reducir los riesgos que existan dentro de la red inalámbrica.	Riesgos Informáticos.	Intercepción de datos. Crackeo. Pérdida de información.	En calidad de administrador de la red inalámbrica, ¿usted controla o sabe si un usuario instaló algún tipo de software en su computador de trabajo?	Encuestas, cuestionarios.
	Normas.	Requerimientos mínimos de las políticas.	¿Cuáles son los requerimientos	Encuestas, cuestionarios.

Conceptualizaciones	Categorías	Indicadores	Ítems	Técnicas e Instrumentos
		Confianza al transmitir información.	mínimos de las políticas de seguridad en la comunicación inalámbrica de Automekano? ¿Considera usted pertinente implementar políticas de seguridad con la finalidad de garantizar la seguridad en la comunicación inalámbrica? ¿Cree usted que la implementación de políticas de seguridad mejorará la confianza y se usará de mejor	

Conceptualizaciones	Categorías	Indicadores	Ítems	Técnicas e Instrumentos
			manera la información a transmitir dentro y fuera de la red?	
	Procedimientos	Pasos para cumplir con las normas.	¿Cuáles son los pasos necesarios para cumplir con las normas dentro de las políticas de seguridad en la comunicación inalámbrica de Automekano?	Encuestas, cuestionarios.

Tabla 3. 3 Operacionalización de la variable dependiente

3.6 Recolección y análisis de la información

Secundaria	Primaria
Se recolectó de estudios realizados anteriormente, como lo son tesis de grados que reposan en Cobuec. Las fuentes de información utilizadas son: biblioteca, archivos, Internet.	Se recolectó a través del contacto directo entre el sujeto investigador y el objeto de estudio, es decir con la realidad.

Técnicas de investigación

Bibliográficas	De campo
Libros, revistas científicas, informes técnicos, memorias, Internet, etc. El análisis de documentos (lectura científica). El fichaje.	La encuesta

Recolección de la información

Preguntas	Explicación
¿Para qué?	Recolectar información primaria para comprobar y contrastar con la hipótesis.
¿A qué personas o sujetos?	La población se tomará en cuenta a los empleados de la empresa AUTOMEKANO de Ambato.
¿Sobre qué aspectos?	V.I.: Amenazas informáticas V.D.: Políticas de seguridad en la comunicación inalámbrica.
¿Quién?	Investigador: Carlos Carrillo.
¿Cuándo?	De acuerdo al cronograma establecido.
¿Lugar de recolección de la información?	AUTOMEKANO.
¿Cuántas veces?	Una sola vez
¿Qué técnica de recolección?	Encuesta

Preguntas	Explicación
¿Con qué?	Cuestionario
¿En qué situación?	Situación normal y cotidiana.

3.7 Procesamiento y análisis de la información

El plan para el procesamiento y análisis de la información es el siguiente:

- Elaboración de la encuesta.
- Definir los sujetos que van a ser encuestados.
- Aplicar la encuesta.
- Recopilar la información.
- Revisión y codificación de la información.
- Categorización y tabulación de la información
  - Tabulación manual.
  - Tabulación computarizada
- Análisis de los datos.
  - La presentación de los datos se lo hará a través de gráficos
- Interpretación de los resultados.
  - Estudiar cada uno de los resultados por separado.
  - Redactar una síntesis general de los resultados.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis de Resultados

1. ¿Conoce sobre los diferentes tipos de amenazas informáticas que existen en la red?

Número	Indicador	Frecuencia	Porcentaje
1	SI	3	100%
2	NO	0	0%
	TOTAL	3	100%

Tabla 4. 1 Tabulación de la encuesta – Pregunta 1

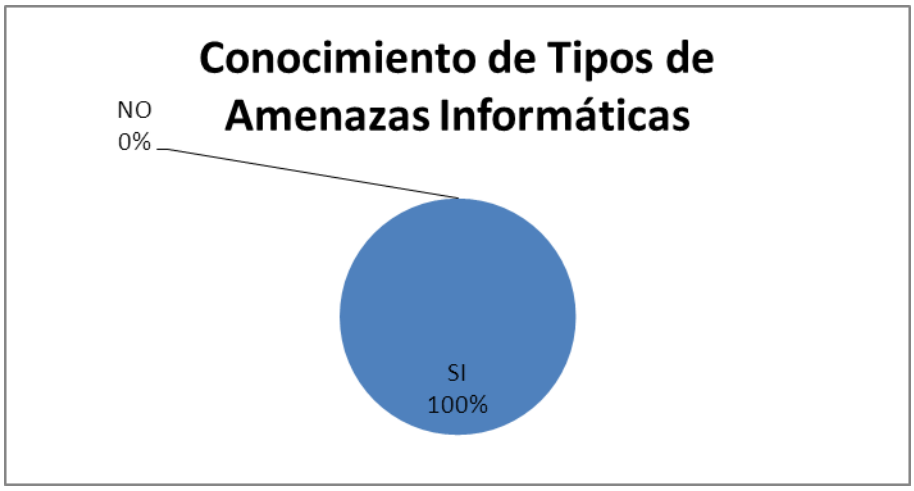


Figura 4. 1 Tabulación de la encuesta – Pregunta 1

De 3 personas encuestadas, las tres respondieron que SI a la pregunta planteada, equivaliendo al 100% del total; por lo tanto como se menciona en la publicación (Internet, 01-06-2004, 10-10-2011 09:46:00) "Se debe tomar en cuenta los desafíos para poder desarrollar nuevos métodos de protección contra los ataques.

Establecimiento de claves, autenticación, privacidad, robustez frente a ataques de negación de servicio, enrutamiento seguro, captura de nodos".

2. **¿Alguna vez notó algún comportamiento extraño o fuera de lo común dentro de la red inalámbrica, como por ejemplo direcciones IP duplicadas, fallos en la conexión, etc.?**

Número	Indicador	Frecuencia	Porcentaje
1	SI	3	100%
2	NO	0	0%
	TOTAL	3	100%

Tabla 4. 2 Tabulación de la encuesta – Pregunta 2

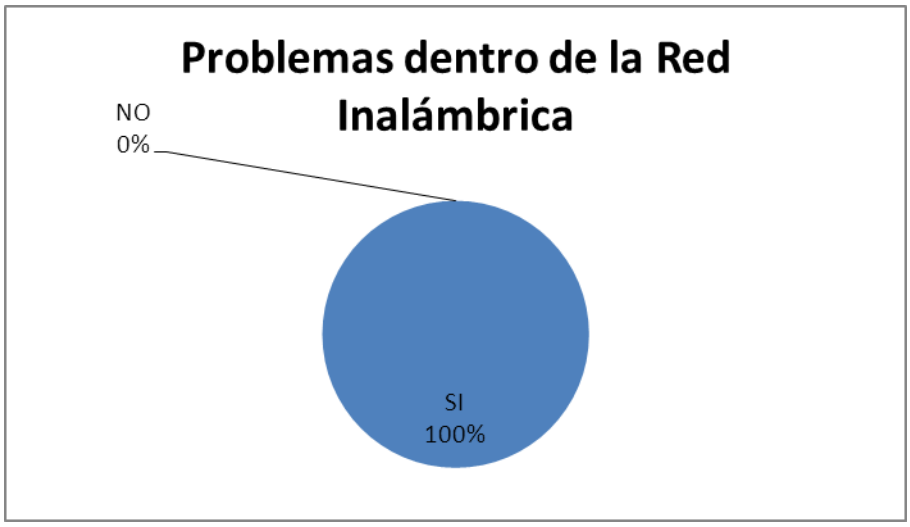


Figura 4. 2 Tabulación de la encuesta – Pregunta 2

De 3 personas encuestadas, el 100% respondió que SI a la pregunta planteada; por lo tanto se debe analizar las amenazas informáticas dentro de la red inalámbrica, ya que como se menciona en la publicación (Internet, 2010, 21-10-2011 19:30:00) "Una red WLAN (Wireless Local Area Network) o Red de Área Local inalámbrica, es un sistema de comunicaciones de datos flexible que se incorpora como una extensión o una alternativa a la red LAN cableada.".

3. ¿Verifica de alguna forma si la información que recibe dentro de la red es del remitente correcto?

Número	Indicador	Frecuencia	Porcentaje
1	SI	0	0%
2	NO	3	100%
	TOTAL	3	100%

Tabla 4. 3 Tabulación de la encuesta – Pregunta 3

Figura 4. 3 Tabulación de la encuesta – Pregunta 3

De 3 personas encuestadas, el 100% respondió que NO a la pregunta planteada; por ende se debería realizar el análisis respectivo en la comunicación inalámbrica para despejar las dudas al momento de transmitir los datos e información.

4. ¿Cree usted que la navegación dentro de la red inalámbrica es segura?

Número	Indicador	Frecuencia	Porcentaje
1	SI	0	0%
2	NO	3	100%
	TOTAL	3	100%

Tabla 4. 4 Tabulación de la encuesta – Pregunta 4

Figura 4. 4 Tabulación de la encuesta – Pregunta 4

De 3 personas encuestadas, el 100% respondió que NO a la pregunta planteada; por lo cual se debe realizar un análisis de las amenazas informáticas e implementar políticas de seguridad en la comunicación inalámbrica y así garantizar la seguridad.

5. **En calidad de administrador de la red inalámbrica, ¿usted controla o sabe si un usuario instaló algún tipo de software en su computador de trabajo?**

Número	Indicador	Frecuencia	Porcentaje
1	SI	1	33%
2	NO	2	67%
	TOTAL	3	100%

Tabla 4. 5 Tabulación de la encuesta – Pregunta 5

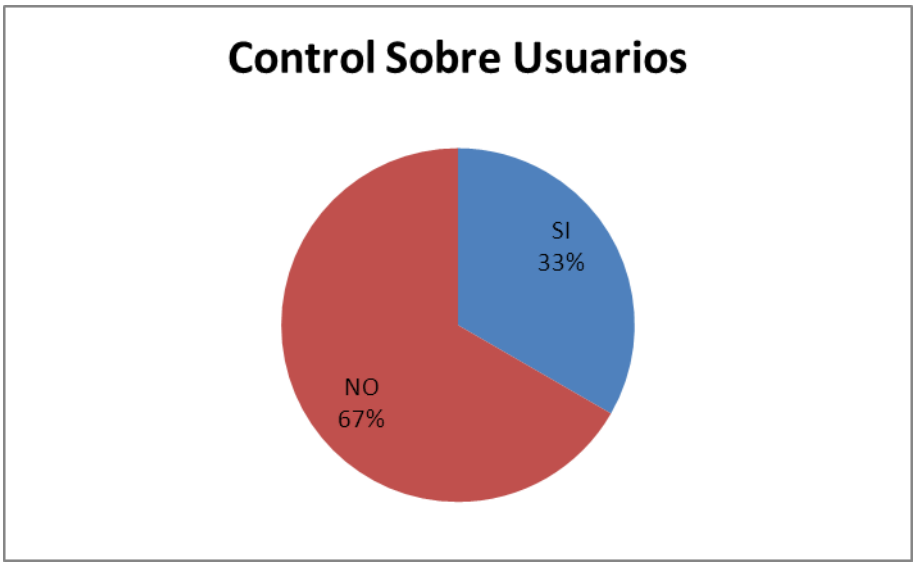


Figura 4. 5 Tabulación de la encuesta – Pregunta 5

El 33% de las personas encuestadas respondieron que SI a la pregunta planteada, equivalente a una persona, mientras las dos personas restantes dijeron que NO, equivalente al 67% del total; por lo tanto se deberían implementar políticas de seguridad, ya que los usuarios realizan cualquier acción dentro de la red inalámbrica sin control alguno.

6. ¿Considera usted pertinente implementar políticas de seguridad con la finalidad de garantizar la seguridad en la comunicación inalámbrica?

Número	Indicador	Frecuencia	Porcentaje
1	SI	3	100%
2	NO	0	0%
	TOTAL	3	100%

Tabla 4. 6 Tabulación de la encuesta – Pregunta 6

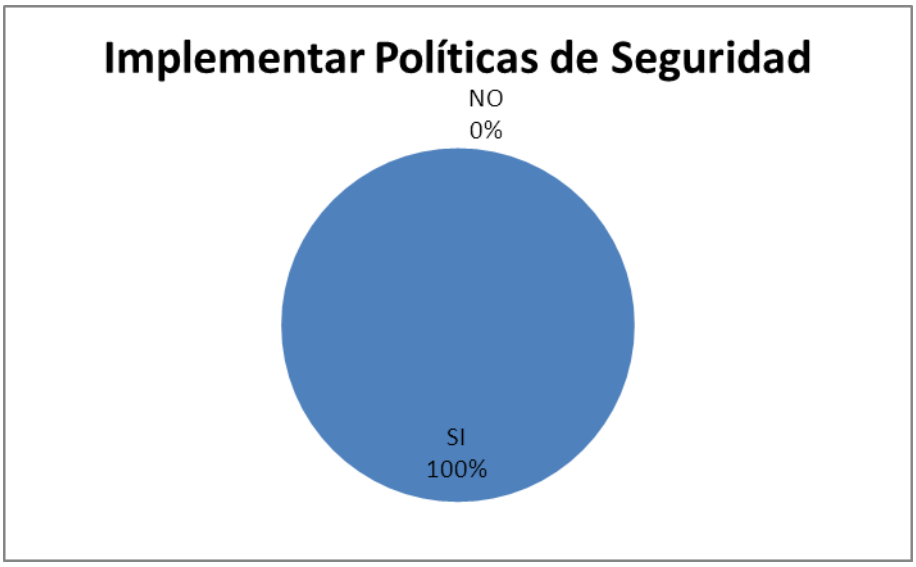


Figura 4. 6 Tabulación de la encuesta – Pregunta 6

De 3 personas encuestadas, las tres respondieron que SI a la pregunta planteada, equivaliendo al 100% del total; por lo tanto como se menciona en la publicación (Internet, 16-10-2008, 10-10-2011 22:26:00) "Uno de los primeros pasos que debe dar una compañía es definir una política de seguridad que pueda implementar en función a las siguientes cuatro etapas.".

7. **¿Cree usted que la implementación de políticas de seguridad mejorará la confianza y se usará de mejor manera la información a transmitir dentro y fuera de la red?**

Número	Indicador	Frecuencia	Porcentaje
1	SI	3	100%
2	NO	0	0%
	TOTAL	3	100%

Tabla 4. 7 Tabulación de la encuesta – Pregunta 7

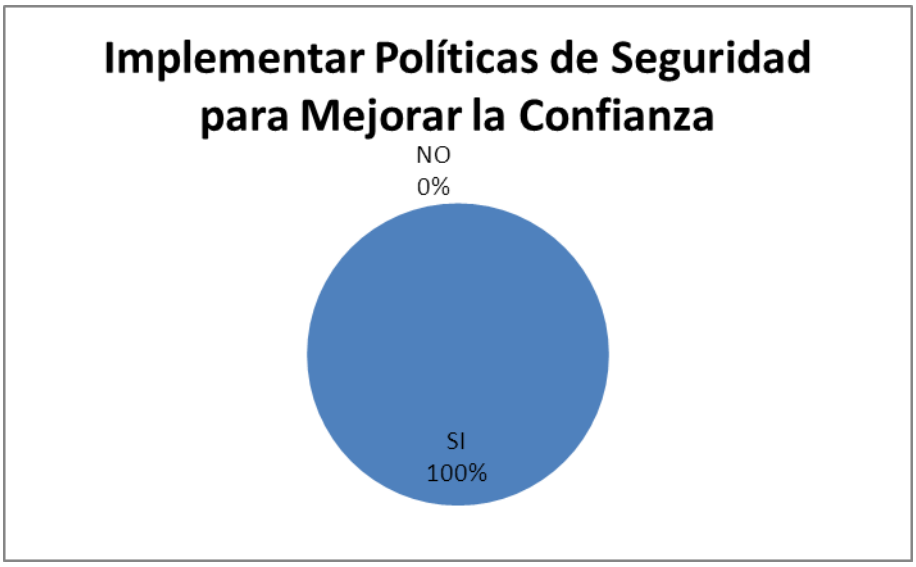


Figura 4. 7 Tabulación de la encuesta – Pregunta 7

De 3 personas encuestadas, las tres respondieron que SI a la pregunta planteada, equivaliendo al 100% del total; por lo tanto es necesario implementar políticas de seguridad y así garantizar confianza.

8. ¿Conoce sobre los diferentes tipos de amenazas informáticas que existen en las redes inalámbricas?

Número	Indicador	Frecuencia	Porcentaje
1	SI	0	0%
2	NO	5	100%
	TOTAL	5	100%

Tabla 4. 8 Tabulación de la encuesta – Pregunta 8

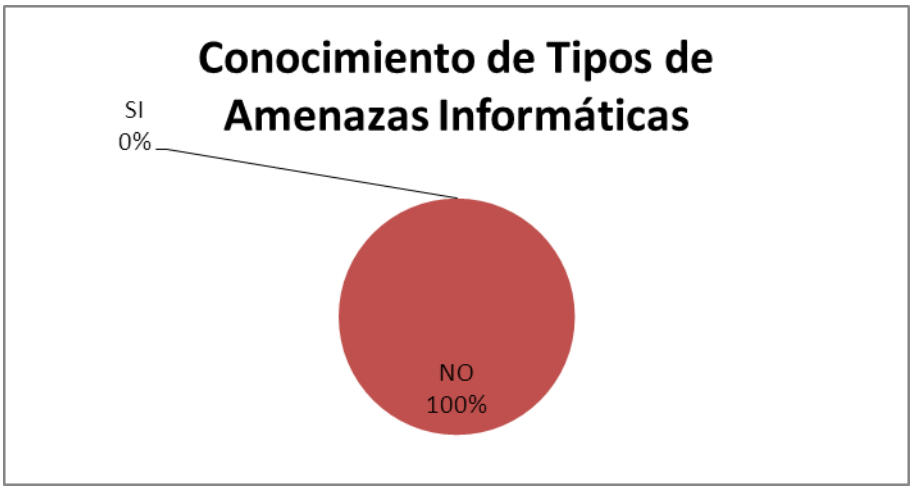


Figura 4. 8 Tabulación de la encuesta – Pregunta 8

De 5 personas encuestadas, las cinco respondieron que NO a la pregunta planteada, equivaliendo al 100% del total; por lo tanto como se menciona en la publicación (Internet, 01-06-2004, 10-10-2011 09:46:00) "Se debe tomar en cuenta los desafíos para poder desarrollar nuevos métodos de protección contra los ataques.

Establecimiento de claves, autenticación, privacidad, robustez frente a ataques de negación de servicio, enrutamiento seguro, captura de nodos".

9. ¿Para conectarse a la red inalámbrica utiliza una contraseña?

Número	Indicador	Frecuencia	Porcentaje
1	SI	5	100%
2	NO	0	0%
	TOTAL	5	100%

Tabla 4. 9 Tabulación de la encuesta – Pregunta 9

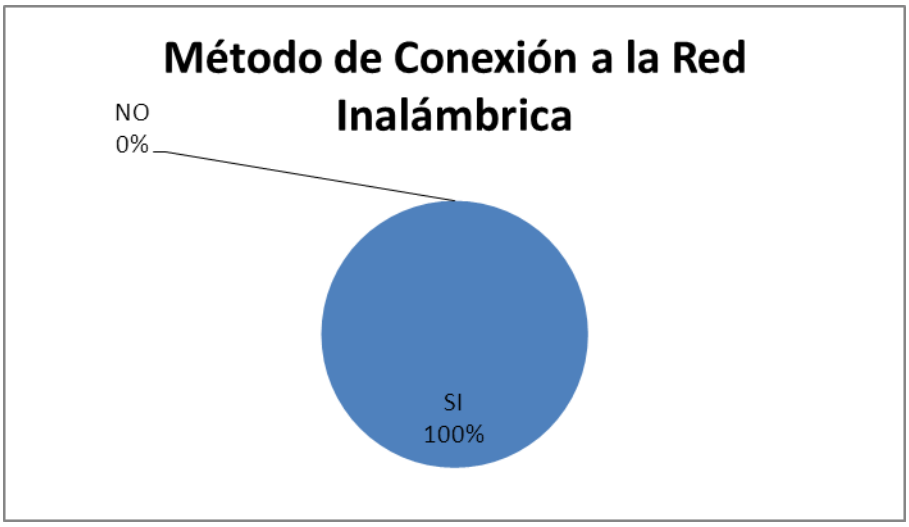


Figura 4. 9 Tabulación de la encuesta – Pregunta 9

De 5 personas encuestadas, las cinco respondieron que SI a la pregunta planteada, equivaliendo al 100% del total; por lo tanto es necesario implementar políticas de seguridad que se relacionen con las contraseñas.

10. ¿Ha tenido más de una vez problemas para conectarse a la red inalámbrica?

Número	Indicador	Frecuencia	Porcentaje
1	SI	4	80%
2	NO	1	20%
	TOTAL	5	100%

Tabla 4. 10 Tabulación de la encuesta – Pregunta 10

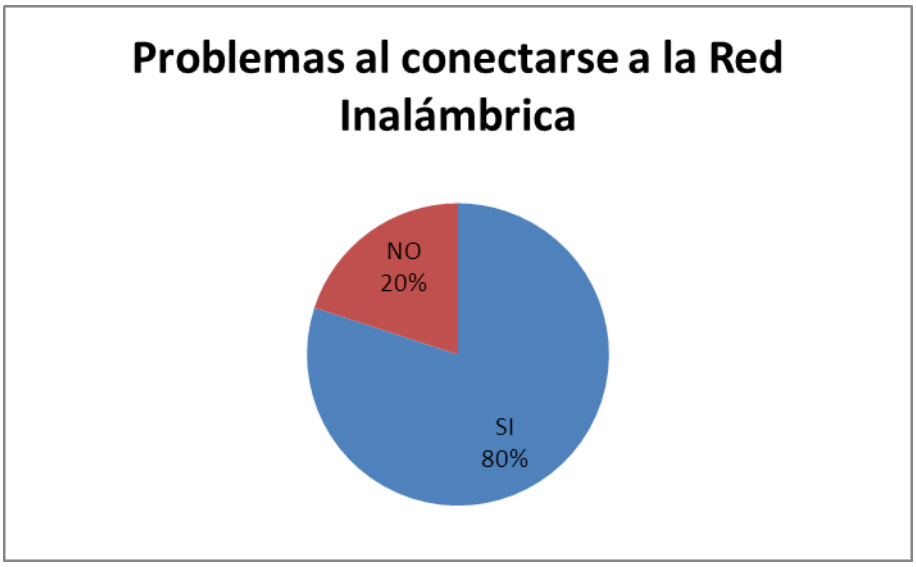


Figura 4. 10 Tabulación de la encuesta – Pregunta 10

El 80% de las personas encuestadas respondieron que SI a la pregunta planteada, equivalente a cuatro personas, mientras la una persona restante dijo que NO, equivalente al 20% del total; por lo tanto se deberían realizar constantes análisis a los dispositivos de la red inalámbrica.

11. ¿Ha notado algún comportamiento extraño mientras está conectado a la red inalámbrica?

Número	Indicador	Frecuencia	Porcentaje
1	SI	4	80%
2	NO	1	20%
	TOTAL	5	100%

Tabla 4. 11 Tabulación de la encuesta – Pregunta 11

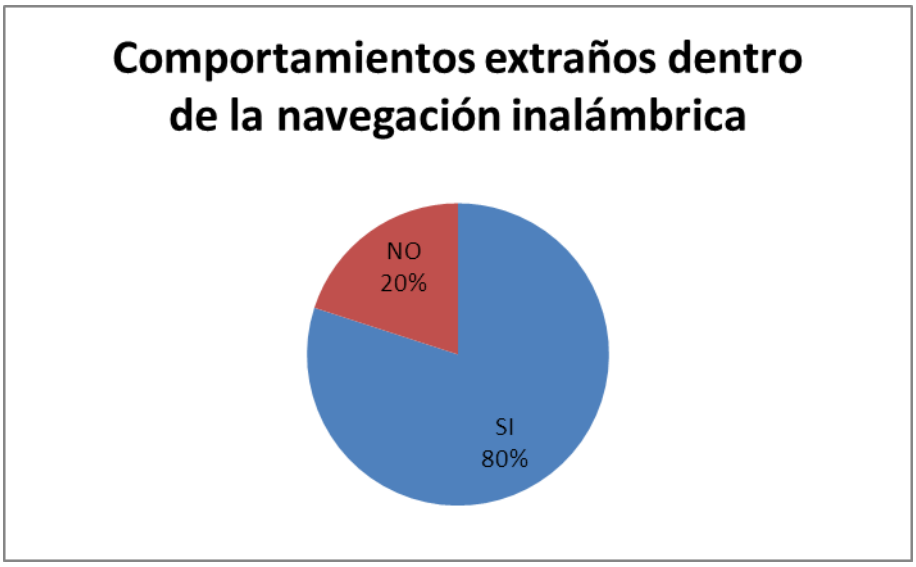


Figura 4. 11 Tabulación de la encuesta – Pregunta 11

De 5 personas encuestadas, el 80% respondió que SI a la pregunta planteada, mientras el 20% restante dijo que NO; por lo tanto se debe analizar las amenazas informáticas dentro de la red inalámbrica, ya que como se menciona en la publicación (Internet, 2010, 21-10-2011 19:30:00) "Una red WLAN (Wireless Local Area Network) o Red de Área Local inalámbrica, es un sistema de comunicaciones de datos flexible que se incorpora como una extensión o una alternativa a la red LAN cableada.".

12. ¿Considera usted que la red inalámbrica es un medio seguro para transmitir datos e información de una manera íntegra?

Número	Indicador	Frecuencia	Porcentaje
1	SI	1	20%
2	NO	4	80%
	TOTAL	5	100%

Tabla 4. 12 Tabulación de la encuesta – Pregunta 12

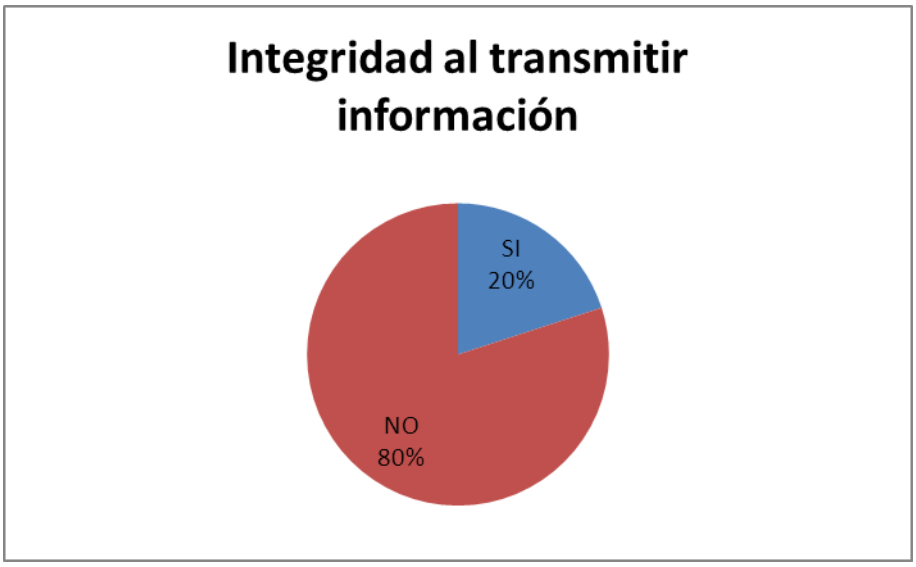


Figura 4. 12 Tabulación de la encuesta – Pregunta 12

De 5 personas encuestadas el 80% dijo que NO, equivaliendo a cuatro personas, mientras que la persona restante dijo que SI, equivaliendo al 20% del total; y por ende se debería implementar políticas de seguridad para garantizar la integridad de la información.

13. ¿Qué le parece el servicio de la red inalámbrica?

Número	Indicador	Frecuencia	Porcentaje
1	EXCELENTE	0	0%
2	BUENA	2	40%
3	REGULAR	3	60%
4	MALA	0	0%
5	DEFICIENTE	0	0%
	TOTAL	5	100%

Tabla 4. 13 Tabulación de la encuesta – Pregunta 13

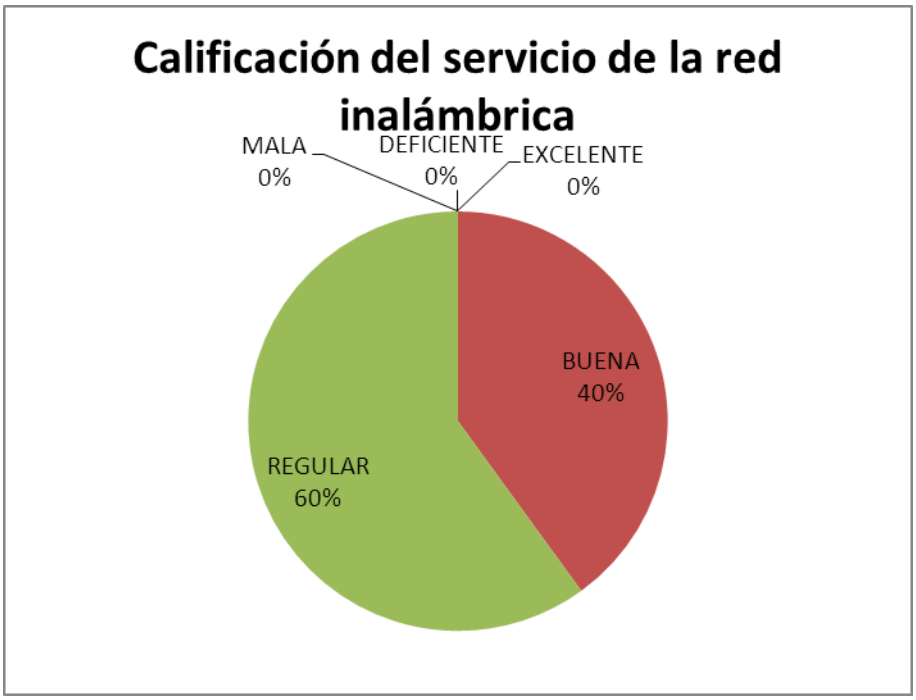


Figura 4. 13 Tabulación de la encuesta – Pregunta 13

De 5 personas encuestadas tres dijeron que el servicio de la red inalámbrica es regular, lo que equivale al 60%, mientras que el 40% restante dijo que el servicio es bueno, cuyo equivalente son dos personas; por lo tanto se debería implementar políticas de seguridad para mejorar los servicios y la seguridad dentro de la red inalámbrica.

14. ¿Cuántas veces a la semana usa la red inalámbrica?

Número	Indicador	Frecuencia	Porcentaje
1	MENOS DE 2 VECES	0	0%
2	2 A 3 VECES	5	100%
3	4 A 6 VECES	0	0%
	TOTAL	5	100%

Tabla 4. 14 Tabulación de la encuesta – Pregunta 14

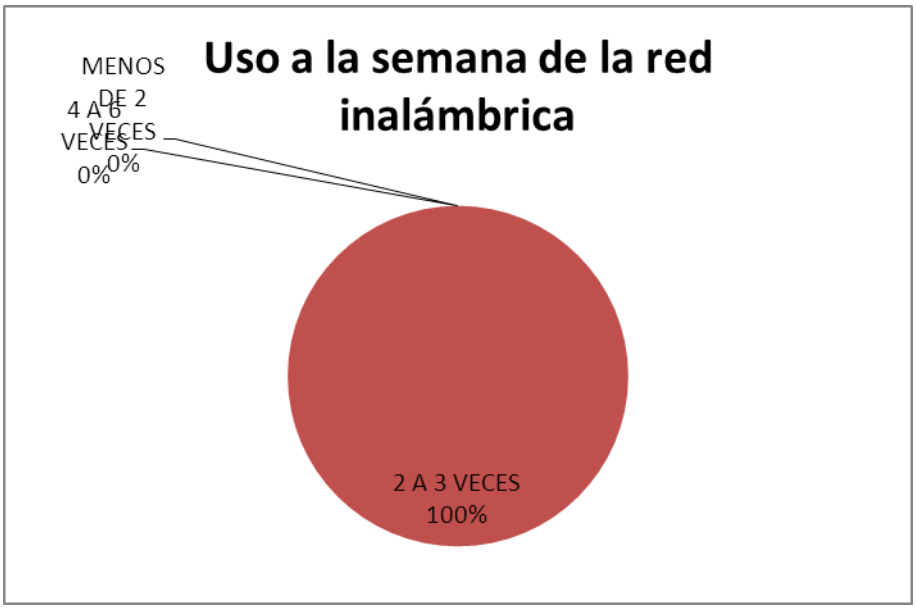


Figura 4. 14 Tabulación de la encuesta – Pregunta 14

De 5 personas encuestadas el 100% respondió que usan la red inalámbrica de dos a tres veces a la semana, por lo que se debería tener más control sobre los usuarios y así no tener problemas respecto a ningún tipo de amenaza informática que se pudiera presentar.

15. ¿Cuál es el tiempo de uso aproximado de la red inalámbrica al día?

Número	Indicador	Frecuencia	Porcentaje
1	MENOS DE 2 HORAS	0	0%
2	DE 2 A 4 HORAS	5	100%
3	DE 4 A 6 HORAS	0	0%
	TOTAL	5	100%

Tabla 4. 15 Tabulación de la encuesta – Pregunta 15

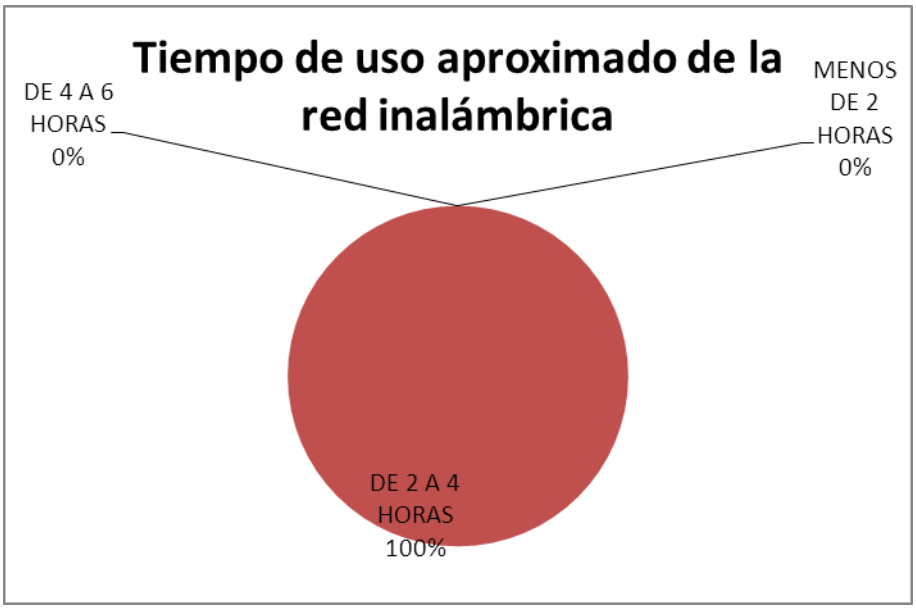


Figura 4. 15 Tabulación de la encuesta – Pregunta 15

De 5 personas encuestadas, el 100% respondió que usa la red inalámbrica de dos a cuatro horas al día, por lo que se debería implementar políticas de seguridad para que exista la confianza de los usuarios hacia la red inalámbrica.

16. ¿Considera usted pertinente implementar políticas de seguridad con la finalidad de garantizar la seguridad en la comunicación inalámbrica?

Número	Indicador	Frecuencia	Porcentaje
1	SI	5	100%
2	NO	0	0%
	TOTAL	5	100%

Tabla 4. 16 Tabulación de la encuesta – Pregunta 16

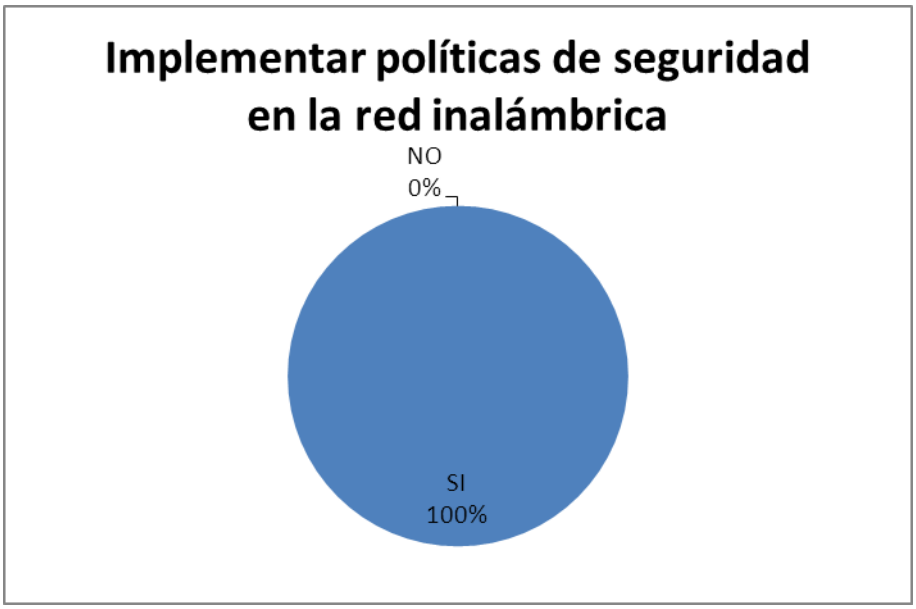


Figura 4. 16 Tabulación de la encuesta – Pregunta 16

De 5 personas encuestadas, las cinco respondieron que SI a la pregunta planteada, equivaliendo al 100% del total; por lo tanto es necesario implementar políticas de seguridad y así garantizar confianza.

4.2 Interpretación de Resultados

Se ha tomado en cuenta las dos preguntas discriminantes, la pregunta número 4 y la número 6 de la encuesta aplicada, ya que los resultados arrojados dicen que la red inalámbrica no es segura. Por lo cual se deberá garantizar la seguridad mediante un análisis de las amenazas informáticas para la implementación de políticas de seguridad en la comunicación inalámbrica de la empresa AUTOMEKANO de la ciudad de Ambato.

4.3 Verificación de la Hipótesis

Paso 1. Planteamiento de la Hipótesis

Modelo Lógico:

"El análisis de las amenazas informáticas influirá en la implementación de políticas de seguridad en la comunicación inalámbrica de la empresa Automekano de la ciudad de Ambato en el I semestre del 2011".

Hipótesis Nula:

"El análisis de las amenazas informáticas NO influirá en la implementación de políticas de seguridad en la comunicación inalámbrica de la empresa Automekano de la ciudad de Ambato en el I semestre del 2011".

Hipótesis Alterna:

"El análisis de las amenazas informáticas SI influirá en la implementación de políticas de seguridad en la comunicación inalámbrica de la empresa Automekano de la ciudad de Ambato en el I semestre del 2011".

Paso 2. Decisión

Para constatar lo que se manifiesta en la encuesta, se realizó una observación por parte del investigador en donde se interactuó directamente con la red inalámbrica; se verificó vulnerabilidades y tipos de amenazas informáticas existentes. Entonces se

rechaza la hipótesis nula y se toma la hipótesis alterna, ya que para una correcta implementación de políticas de seguridad en la comunicación inalámbrica de la empresa Automekano se requiere de un análisis de las amenazas informáticas.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Todas las personas que usan la red inalámbrica en la empresa AUTOMEKANO afirmaron que la utilizan de dos a tres veces por semana.

- Los involucrados en la encuesta están conscientes y conocen sobre los diferentes tipos de amenazas informáticas existentes y los daños que pueden causar dentro de la comunicación inalámbrica.

- No se verifica que los datos y la información enviada a los distintos empleados, usuarios receptores es la correcta, ni por parte del emisor, peor aún por parte del receptor; según los encuestados.

- No todos los administradores de la red inalámbrica hacen un control sobre la instalación de software adicional por parte de los empleados, usuarios de la empresa AUTOMEKANO.

- Mediante la percepción de las encuestas realizadas a los empleados y usuarios de la empresa, se concluye que la navegación dentro de la red inalámbrica no es segura, por lo tanto la desconfianza por parte de los empleados y usuarios es evidente.

5.2 Recomendaciones

- Se recomienda determinar las posibles vulnerabilidades existentes en la empresa AUTOMEKANO de la ciudad de Ambato.

- En la actualidad las amenazas informáticas se hacen más fuertes, ya que conforme avanza la tecnología, también lo hacen las amenazas y se recomienda estar al día e investigar sobre las amenazas informáticas.

- Garantizar la integridad de los datos e información mediante la ejecución y seguimiento correcto de políticas de seguridad en la comunicación inalámbrica de la empresa.

- Establecer funciones a nivel de administradores de carácter estricto y con el uso de herramientas software poder realizar el debido control de la instalación de software adicional por parte de los empleados, usuarios de la empresa AUTOMEKANO.

- Se recomienda un análisis de las amenazas informáticas para implementar políticas de seguridad en la comunicación inalámbrica de la empresa AUTOMEKANO de la ciudad de Ambato.

CAPÍTULO VI

PROPUESTA FINAL

6.1 Datos Informativos

6.1.1 Título

"Análisis de las amenazas informáticas para la implementación de políticas de seguridad en la comunicación inalámbrica de la empresa AUTOMEKANO de la ciudad de Ambato".

6.1.2 Institución Ejecutora

Empresa AUTOMEKANO de la ciudad de Ambato.

6.1.3 Director de Tesis

Ing. Xavier Francisco López.

6.1.4 Beneficiarios

Empleados de la empresa AUTOMEKANO de la ciudad de Ambato.

6.1.5 Ubicación

Av. Indoamérica Km. 1 – Entrada a las Viñas.

6.1.6 Tiempo estimado para la ejecución

Fecha de Inicio:	Febrero del 2012
Fecha de Finalización:	Enero del 2013

6.1.7 Equipo Técnico Responsable

Investigador:	Carlos Carrillo Miranda
Administrador de Sistemas AUTOMEKANO:	Ing. Edit Correa
Tutor de Investigación:	Ing. Xavier Francisco López.

6.2 Antecedentes de la Propuesta

Para la presente investigación, y con la ayuda de las personas involucradas, se ha podido determinar información importante que servirá para el desarrollo del proyecto, ya que en la actualidad en el campo de la informática no existe una seguridad al cien por ciento; lo que se pretende es minimizar los riesgos, amenazas informáticas, vulnerabilidades, y todo tipo de mal que pretenda afectar a los datos e información dentro de la comunicación inalámbrica. En la empresa por parte del personal a cargo del área de sistemas, conocen sobre los diferentes tipos de amenazas informáticas

existentes en la actualidad, lo que no se verifica es que exista integridad en la información que es enviada y recibida en la red; dicha integridad es uno de los pilares fundamentales para la seguridad. Otro de los puntos a tomar en cuenta es el control sobre la instalación de software adicional por parte de los empleados, ya que los mismos podrían instalar programas que afecten en cierto sentido al/los computador/es, a los sistemas, ocasionando graves problemas de seguridad en toda la red. Finalmente se tiene que la navegación dentro de la red inalámbrica no es segura, por lo tanto la desconfianza por parte de los empleados y usuarios es notoria.

Por lo planteado anteriormente y tomando en cuenta el avance tecnológico, se recomienda estar al día en conocimiento en cuanto se refiere a las amenazas informáticas, también garantizar los pilares básicos de seguridad, como son la integridad de los datos e información, la confidencialidad, la disponibilidad, y la autenticidad. El uso de herramientas software para el control interno de usuarios y computadores es muy recomendable, y lo más importante realizar un análisis de las amenazas informáticas e implementar políticas de seguridad en la comunicación inalámbrica de la empresa, ya que dicha implementación justamente es uno de los primeros pasos para comenzar a garantizar seguridad informática dentro de una empresa o institución.

6.3 Justificación

En la actualidad, para proteger un computador, los datos e información, una red, etc. de una empresa, no es suficiente hacerlo con un simple firewall, o con un antivirus, antispyware, ya que con ello no se garantiza seguridad en el mundo actual, las amenazas informáticas pueden nacer dentro de la misma empresa, con el mal uso de la tecnología por parte de los usuarios de AUTOMEKANO.

Para garantizar la seguridad dentro de la empresa no es solamente comprar los equipos más caros ni de mejor tecnología, hardware y software, si no se sabe cómo explotarlos y usarlos de la mejor manera.

Por lo que primero se debe concientizar a los usuarios sobre la importancia y sensibilidad de los datos e información que se transmiten dentro de la comunicación inalámbrica, por lo cual es factible implementar políticas de seguridad en la empresa AUTOMEKANO, para tener un mejor control sobre los usuarios, los mismos que deberán llevar a cabo de manera responsable y profesional el cumplimiento de todas las normas, procedimientos que estén implementados dentro de las políticas de seguridad; para así reducir los riesgos, vulnerabilidades y las amenazas informáticas existentes en la actualidad.

Se utilizarán herramientas software de carácter gratuito para el previo y respectivo análisis de las amenazas informáticas.

6.4 Objetivos de la Propuesta

6.4.1 Objetivo General

Analizar las amenazas informáticas para la implementación de políticas de seguridad en la comunicación inalámbrica de la empresa AUTOMEKANO de la ciudad de Ambato.

6.4.2 Objetivos Específicos

- Interpretar las amenazas informáticas previamente analizadas en la comunicación inalámbrica de la empresa AUTOMEKANO de la ciudad de Ambato mediante el uso de herramientas software.

- Establecer políticas de seguridad en la comunicación inalámbrica de toda la empresa AUTOMEKANO en la ciudad de Ambato.

- Realizar las pruebas necesarias para garantizar la reducción de las amenazas informáticas en la comunicación inalámbrica de la empresa AUTOMEKANO de la ciudad de Ambato.

6.5 Análisis de Factibilidad

6.5.1 Factibilidad Política

Garantizar la seguridad de los datos e información que fluyen dentro de la comunicación inalámbrica de la empresa AUTOMEKANO.

6.5.2 Factibilidad Socio Cultural

La implementación de políticas de seguridad en la comunicación inalámbrica garantizará la integridad de los datos e información de todos los usuarios de la empresa.

6.5.3 Factibilidad Tecnológica

AUTOMEKANO, cuenta con equipos informáticos de última generación, que satisfacen todos los requerimientos de hardware y de software para el desarrollo e implementación de políticas de seguridad.

6.5.4 Factibilidad Equidad de Género

La implementación de políticas de seguridad en la comunicación inalámbrica se deberá aplicar para todas las personas, sin discriminar el género.

6.5.5 Factibilidad Ambiental

El desarrollo del proyecto no afectará al medio ambiente en ningún sentido.

6.5.6 Factibilidad Económica Financiera

El proyecto de investigación en el ámbito económico es factible de realizarlo; al emplear herramientas software libre. La inversión por parte de la institución no es necesaria, porque no se debe pagar por el uso de las herramientas a utilizar.

6.5.7 Factibilidad Operativa

Durante el análisis de las amenazas informáticas, se identificaron todas las amenazas informáticas existentes en la empresa, lo que generó en la implementación de políticas de seguridad en la comunicación inalámbrica que satisfacen las necesidades de la institución, lo cual resulta operativo en todas las áreas.

6.5.8 Factibilidad Legal

El desarrollo del proyecto no infringe ninguna ley o norma establecida a nivel local, ni estatal.

6.6 Fundamentación Teórica

6.6.1 Amenazas Informáticas

Las amenazas son intentos de hacer daño, si existen vulnerabilidades o "puertas abiertas", en las redes inalámbricas o en los sistemas de las empresas o instituciones, estos "huecos" o "puertas" son aprovechados por las amenazas, generándose los distintos ataques que puede existir.

Según la publicación (Internet, 03-12-2006, 19-10-2011 15:28:00) "México, DF.- El robo y suplantación de identidad en Internet se ha convertido en un problema de seguridad de alcance nacional que afecta tanto al patrimonio como a la integridad física y psicológica de los miles de usuarios de la llamada supercarretera de la información.

Arropados por el anonimato, ya sea en grupo o en solitario, expertos en informática conocidos como ¿hackers?, obtienen ilegalmente contraseñas, números de cuentas, claves de tarjetas de crédito, así como información personal almacenada en correos electrónicos que puede convertirse en materia útil para secuestros y extorsiones.

¿Quién no ha guardado en sus correos electrónicos fotografías, datos personales, cartas y otros documentos de los que se podrían inferir parentescos y relaciones afectivas que podrían resultar potencialmente peligrosas de caer en manos equivocadas?".

6.6.1.1 Tipos de Amenazas informáticas

Algunos de los ataques más comunes son:

- ✓ SSID (network name) sniffing.
- ✓ WEP (ataques contra llaves).
- ✓ ARP envenenamiento.
- ✓ MAC spoofing
- ✓ Access Point, claves (ataques).
- ✓ Negación de Servicio (DOS).
- ✓ Suplantación de direcciones MAC.

- **Sniffing**

  Como los datos viajan por el aire, es más fácil que pueden ser interceptados, capturados por los atacantes, peor aún si no llevan una encriptación. El tráfico en redes inalámbricas es mucho más vulnerable que en una LAN, sólo se necesita una laptop con tarjeta de red inalámbrica.

- **Análisis de Tráfico**

  Al ser examinado por el atacante el tráfico de una red, ya obtendrá información, por ejemplo cuando existe tráfico, en que momento, lugar, etc.

- **Suplantación**

  Hay varias maneras, por ejemplo instalando y configurando un Punto de Acceso falso, para llamar la atención de la víctima y así se conecte a él. También se lo puede hacer mediante un sniffer para hacerse con las direcciones MAC válidas.

- **DOS**

  DOS significa denegación de servicios, el atacante puede interceptar y puede modificar los datos que envía un usuario hacia otro o hacia un determinado servidor.

6.6.1.2 Análisis de las Amenazas Informáticas

Para realizar un análisis se puede utilizar una variedad de herramientas informáticas, por ejemplo Snort, Nessus, Cain & Abel, Wireshark, MAC MakeUP y las que se incluyen en la distribución Linux Backtrack 5, como son aircrack-ng, kismet, ettercap, nmap, airodump-ng.

6.6.1.3 Herramientas para el análisis de amenazas informáticas

- **Snort**

Según la publicación (Internet, 16-05-2011, 03-02-2012 3:00pm) "**Snort** es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión). Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es

MySQL. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida".

Como se menciona en el video publicado en la web (Internet, 12-03-2012, 15-05-2012 12:00pm) "Primero iniciamos el servicio snort, en la opción: Backtrack/Services/Snort Service/Snort Start.

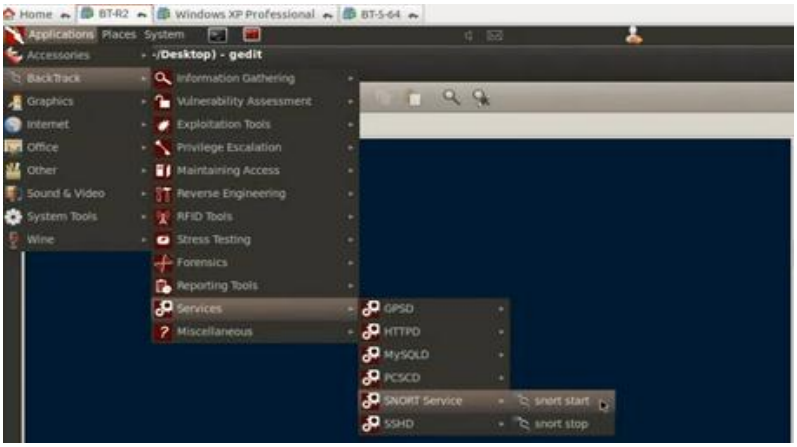


Figura 6. 1 Iniciar el servicio Snort

Luego se procede a editar el archivo snort.conf, y modificar la variable: var HOME_NET any a var HOME_NET ip. Con el siguiente comando: vim /etc/snort/snort.conf

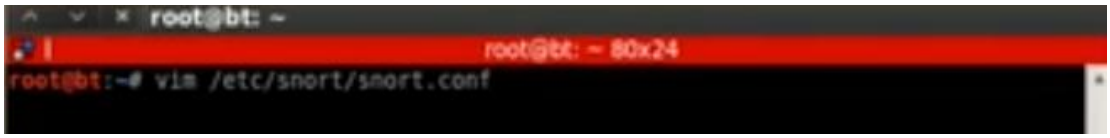


Figura 6. 2 Editar el archivo snort.conf con el editor vim

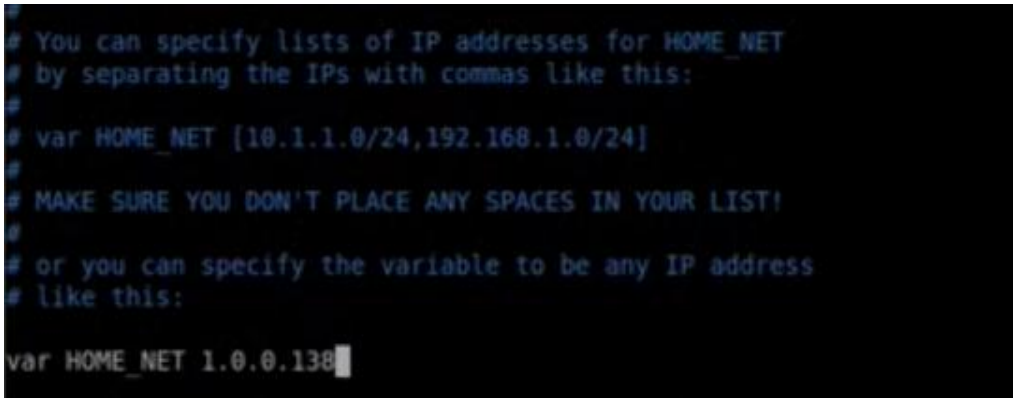


Figura 6. 3 Cambiar el valor de la variable var HOME_NET del archivo snort.conf

Despues de haber guardado el archivo modificado y reiniciado el servicio snort, abrir una terminal y poner el siguiente comando: snort –q –A console –i eth0 –c /etc/snort/snort.conf. Donde:

–q modo tranquilo.
-A console, es para poner el modo de alerta en la consola.
-i es la opción para indicar la tarjeta de red.
eth0 es la interfaz de red a usar.
-c /etc/snort/snort/snort.conf son las reglas a usar, que están en el archivo de configuración.

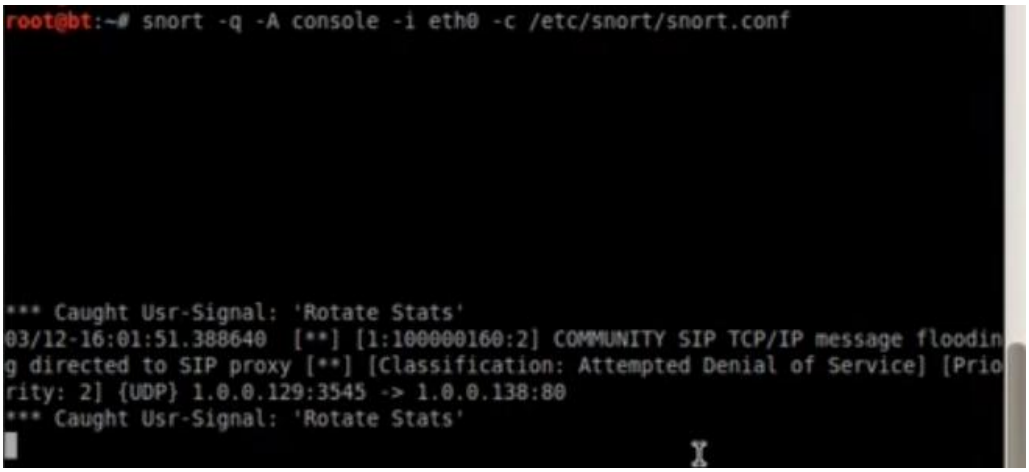


Figura 6. 4 Ejecutar snort: snort –q –A console –I eth0 –c /etc/snort/snort.conf

Después de unos segundos se detectó los tipos de amenazas informáticas: ataque de denegación de servicios (DOS), escaneo de puertos (nmap).”

- **Nessus**

Según la publicación (Internet, 24-03-2011, 06-02-2012 09:30 pm) “El escaner de vulnerabilidades Nessus es un software que permite detectar vulnerabilidades de forma remota que cambió de licencia en 2005 (a partir de **Nessus 3**), generándose como **fork** de **Nessus 2** el escaner de vulnerabilidades open source OpenVAS. Para uso personal tenemos una licencia que nos permite su uso”.

Para usar la herramienta, después de haberla instalado se debe ingresar a la consola web, colocando el nombre de usuario y la respectiva contraseña (previamente creados durante la instalación).

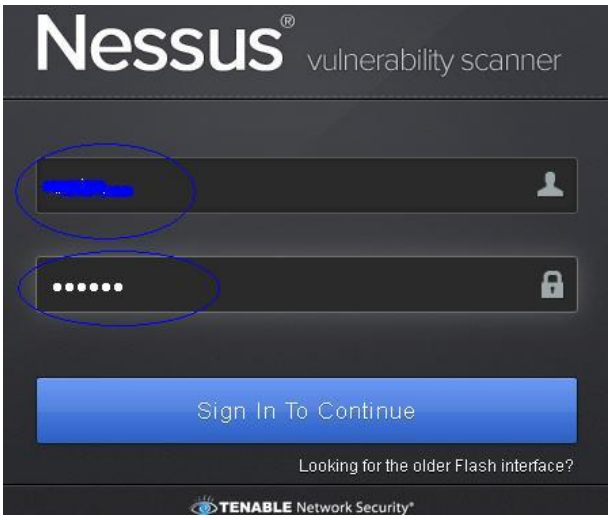


Figura 6. 5 Ingreso a la consola web de Nessus

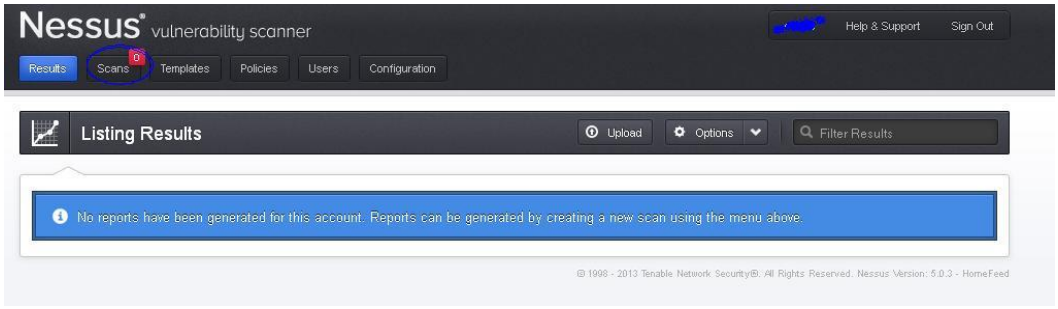


Figura 6. 6 Consola Web de Nessus

Después para realizar un nuevo escaneo a un computador se debe dar clic en la opción **Scans** y en la opción **New Scan**

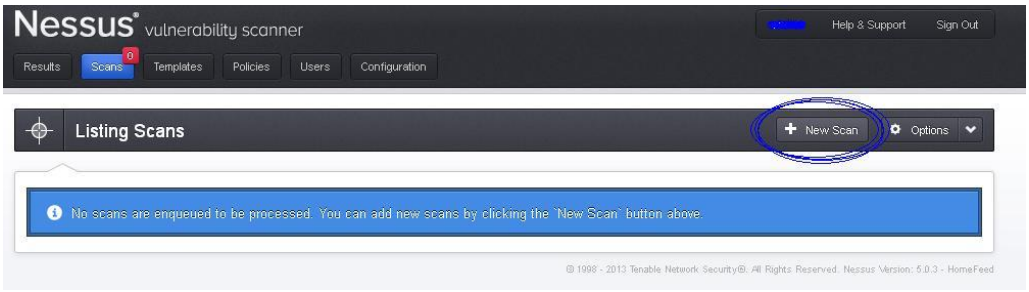


Figura 6. 7 Nuevo escaneo.

En la siguiente ventana se escogen opciones, como son un título, un tipo, una política, y la dirección IP para el escaneo nuevo.

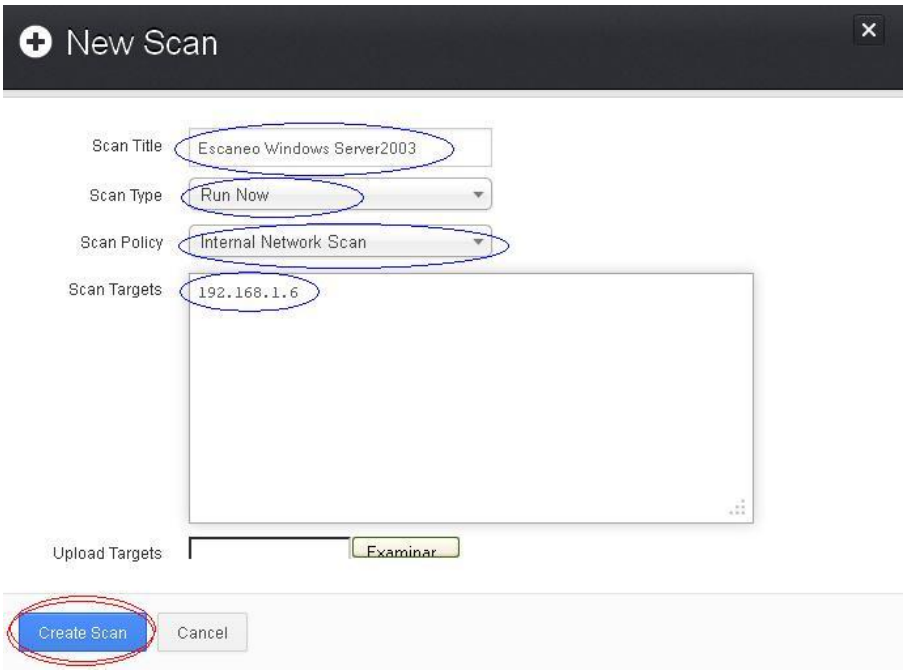


Figura 6. 8 Opciones para crear el nuevo escaneo

Una vez creado el escaneo, comenzará el proceso del mismo y una vez finalizado se obtendrán los siguientes resultados: información general, número de vulnerabilidades y su respectiva clasificación (crítica, mediana, alta, baja, etc.).

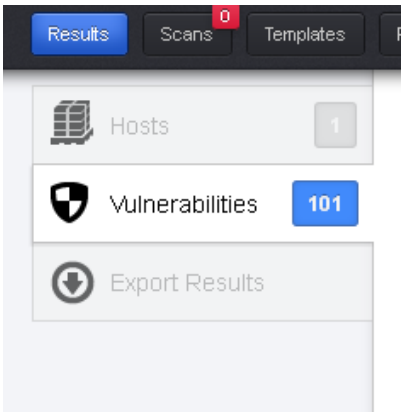


Figura 6. 9 Resultado del análisis de vulnerabilidades

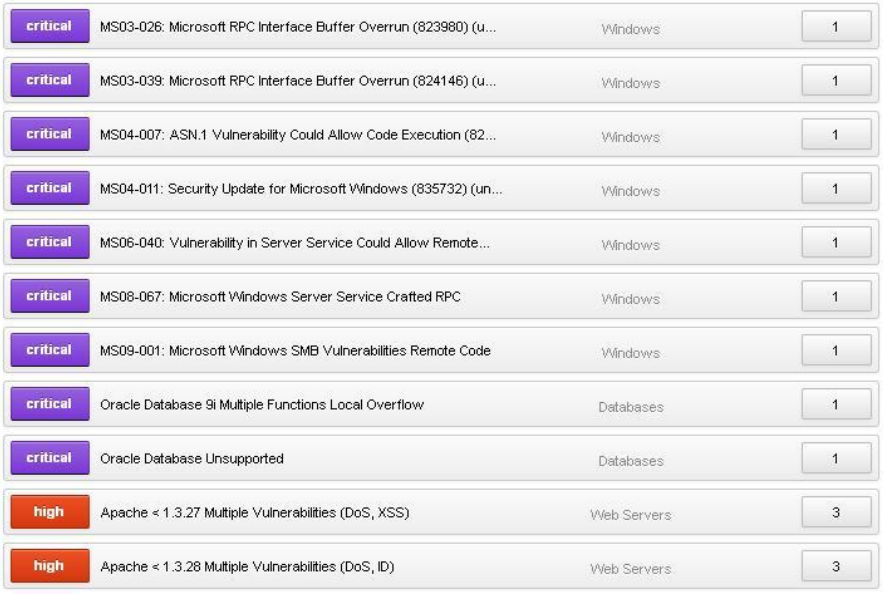


Figura 6. 10 Resultado del análisis de vulnerabilidades con su grado de clasificación.

- **Distribución Linux Backtrack 5**

Como se menciona en la publicación (Internet, 09-09-2011, 04-02-2012 10:08:00 am) "BackTrack, es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad (desencriptar claves wifi) y relacionada con la

seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática".

Las herramientas incluidas en Backtrack 5 son:

- **Aircrack-ng**

  Es una suite de software de seguridad inalámbrica. Consiste en un analizador de paquetes de redes, un crackeador de redes WEP y WPA/WPA2-PSK y otro conjunto de herramientas de auditoría inalámbrica.

  Entre las herramientas que se incluyen en la suite Aircrack-ng se encuentran las siguientes:

  - airbase-ng
  - aircrack-ng
  - airdecap-ng
  - airdecloak-ng
  - airdriver-ng
  - aireplay-ng
  - airmon-ng
  - airodump-ng
  - airolib-ng
  - airserv-ng
  - airtun-ng
  - easside-ng
  - packetforge-ng
  - tkiptun-ng
  - wesside-ng
  - airdecloak-ng

Las herramientas más utilizadas para la auditoría inalámbrica son:

- Aircrack-ng (descifra la clave de los vectores de inicio)
- Airodump-ng (escanea las redes y captura vectores de inicio)
- Aireplay-ng (inyecta tráfico para elevar la captura de vectores de inicio)
- Airmon-ng (establece la tarjeta inalámbrica en modo monitor, para poder capturar e inyectar vectores).

- **Kismet**

Es un sniffer, un husmeador de paquetes, y un sistema de detección de intrusiones para redes inalámbricas 802.11. Kismet se diferencia de la mayoría de los otros sniffers inalámbricos en su funcionamiento pasivo. Es decir que lo hace sin enviar ningún paquete detectable, permitiendo detectar la presencia de varios puntos de acceso y clientes inalámbricos, asociando unos con otros.

- **Ettercap**

Es un interceptor/sniffer/registrador para LANs con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle (Spoofing).

- **Nmap**

Es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias *Fyodor Vaskovich*). Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

- **Desautenticación de un usuario utilizando herramientas de Backtrack.**

Como se menciona en el video publicado (Internet, 17-05-2010, 06-02-2012 03:25:00 pm) Para este DOS (Negación de Servicio) se puede utilizar la distribución Linux Backtrack 5, en donde primero se debe tener conectado la tarjeta de red inalámbrica, y para ello se puede verificar digitando el comando **ifconfig** en la consola de comandos.

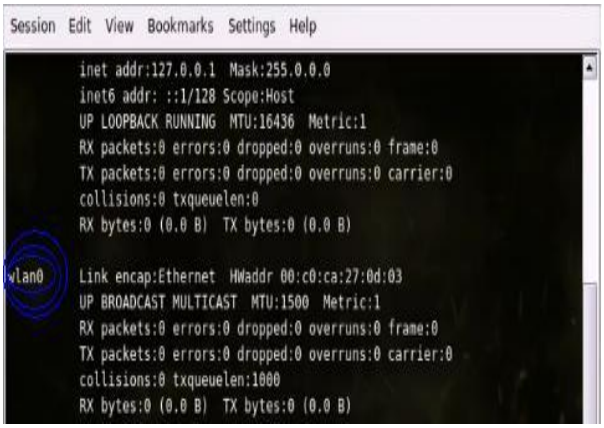


Figura 6. 11 Verificar la interfaz inalámbrica: wlan0.

Luego se procede a colocar la interfaz / tarjeta de red inalámbrica (wlan0) en modo monitor (mon0) para poder "escuchar" todo el tráfico en la red, con el comando **airmon-ng start wlan0**.

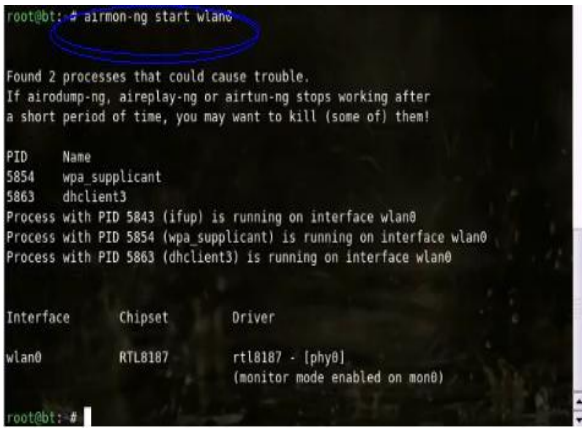


Figura 6. 12 Interfaz inalámbrica a modo monitor (mon0).

Después se utiliza el comando **Airodump-ng wlan0**, para capturar el tráfico de la red (paquetes), por ejemplo obtener el BSSID (dirección MAC del punto de acceso), ESSID (nombre de la red inalámbrica), CH (canal por donde transmite el punto de acceso), etc. de las posibles redes que se puede tener al alcance.

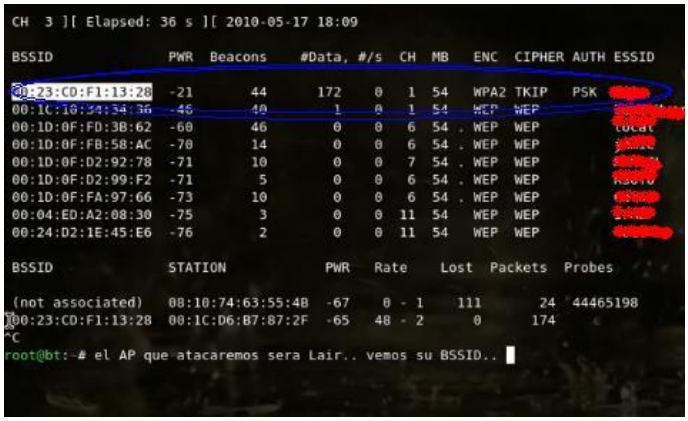


Figura 6. 13 Captura del tráfico de la red inalámbrica.

Luego se usa la herramienta aireplay para la desautenticación de usuarios, de la siguiente forma: **aireplay-ng -0 666 –a 00:23:CD:F1:XX:XX –c 00:1C:D6:B7:XX:XX mon0** Donde:

-0 significa ataque de desautenticación en una red.

666 es el número de paquetes a inyectar para la desautenticación.

-a es la opción para indicar la dirección MAC del punto de acceso.

-c es la opción para indicar la dirección MAC del cliente.

mon0 es el modo monitor de la tarjeta inalámbrica.

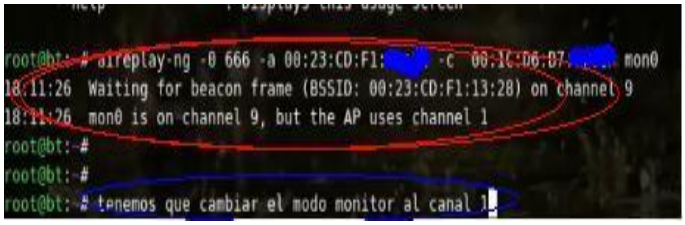


Figura 6. 14 Utilización de comando aireplay-ng para desautenticar.

El modo monitor se debe cambiar al canal 1, ya que el punto de acceso usa ese número de canal (el número de canal puede ser cualquier número), se lo puede realizar con el comando **Airmon-ng start wlan0 1** Donde:

wlan0 es la interfaz inalámbrica.

1 es el número de canal por donde "escuchará" la tarjeta de red inalámbrica el tráfico de red.

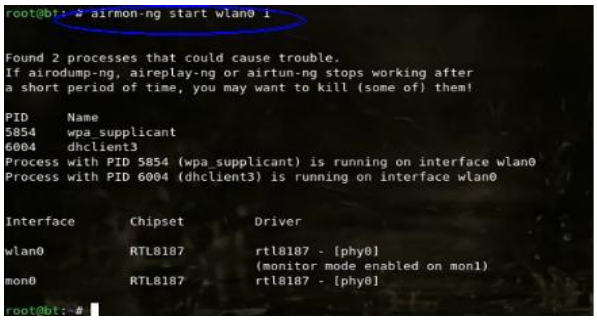


Figura 6. 15 Cambio de canal del modo monitor a mon1.

Y ahora si aplicar nuevamente el comando **aireplay-ng -0 666 –a 00:23:CD:F1:XX:XX –c 00:1C:D6:B7:XX:XX mon1** para desautenticar al usuario de la red inalámbrica seleccionada.

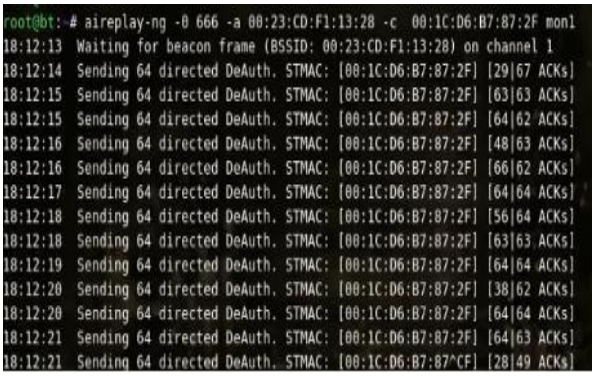


Figura 6. 16 Utilización del comando aireplay-ng con interfaz en mon1 para desautenticar.

- **Obtener Claves WPA, WPA2 de puntos de acceso inalámbricos mediante el uso de Backtrack 5**

Como se menciona en la publicación (Internet, 09-11-2009, 08-01-2012 10:35:00 pm) “Primero que nada debemos poner la tarjeta en modo monitor:

airmon-ng start wlan0

Ahora que ya la tenemos en Modo Monitor, al igual que en WEP escaneamos las redes que podemos tener al alcance. Para eso usamos: # airodump-ng eth0 o airodump-ng mon0 en caso de Backtrack 4.

Por ejemplo, la red llamada Alfa-Omega es una víctima perfecta... Tiene una muy buena señal y un cifrado WPA2, así que nos vamos por esa y al igual que en WEP lo hacemos así.

 # airodump-ng -c 6 --bssid 00:80:5A:5A:79:9F -w captura eth0

Bien, ahora tendríamos que esperar a que se conecte algún cliente para obtener el handshake que es lo que nos interesa, esto puede tomar harto tiempo...

Si ya hay algún cliente conectado, lo que podemos hacer es desautentificarlo de la red para que se vuelva a identificar y asi obtener el handshake.. Para eso, cuando hacemos airodump-ng en la parte inferior de la captura nos aparece si hay algún cliente conectado a dicha red

Ahora tomamos los datos del cliente conectado para desautenticarlo de la red. Para eso usamos aireplay-ng.

 # aireplay-ng -0 1 -a 00:80:5A:5A79:9F -c 00:11:22:33:44:55 eth0

Flags:

0 = Es para desautentificar de la red
1 = Repeticiones de la desautentificacion.
-a= Dirección MAC del AP.
-c= Dirección MAC del cliente que deseamos desautentificar.

Ahora solo tenemos que crackear al igual que con WEP usaremos aircrack-ng.
En la terminal tecleamos:

 # aircrack-ng -w pass *.cap

Flags:

(IMPORTANTE) Necesitamos un diccionario para poder hallar la clave, ya que se encuentra por fuerza bruta.
-w Es la ruta del diccionario que se usará, en este caso el diccionario está en la misma carpeta así que no es necesario poner la ruta.

*.cap Es (son) el (los) archivo(s) donde se encuentran los paquetes capturados (handshake) y examina todos los archivos con extensión .cap

Si airodump-ng no capturo el handshake mostrara un mensaje diciendo que no se ha capturado ningun handshake. Si sale ese mensaje, tendras que volver a desautentificar a algun usuario de la red.

Ahora, crackeamos. Esto puede tomar mucho tiempo, dependiendo del diccionario que usemos.".

- **Herramienta Wireshark para capturar paquetes en la red**

Según la publicación (Internet, 07-02-2012, 09-02-2012 04:15:00 pm) "Wireshark es un código abierto y libre- analizador de paquetes. Se utiliza para la resolución de problemas en la red, análisis, software, el protocolo de comunicaciones, desarrollo y educación.

Wireshark es multiplataforma , usando la GTK + Widget Toolkit para implementar su interfaz de usuario, y el uso de pcap para capturar los paquetes, sino que se ejecuta en varios Unix-como sistemas operativos, incluyendo Linux , Mac OS X , BSD y Solaris , y en Microsoft Windows . También hay un terminal basado en (sin GUI) versión llamada tshark. Wireshark, y los demás programas distribuidos con él, como tshark, son software libre, publicado bajo los términos de la GNU General Public License.".

- **Captura de Paquetes con Wireshark**

Como se menciona en la publicación (Internet, s.f., 01-02-2012 09:12:00 pm) "Una de las principales funciones de WireShark es capturar paquetes con la finalidad de que los administradores y/o ingenieros de redes puedan hacer uso de estos realizar el análisis necesario para tener una red segura y estable. Como requisito para el proceso de capturar datos es ser administrador y/o contar con estos privilegios y es necesario identificar exactamente la interfaz que se quiere analizar.

WireShark cuenta con cuatro maneras para iniciar la captura de los paquetes:

1. Haciendo doble clic en  se despliega una ventana donde se listan las interfaces locales disponibles para iniciar la captura de paquetes.

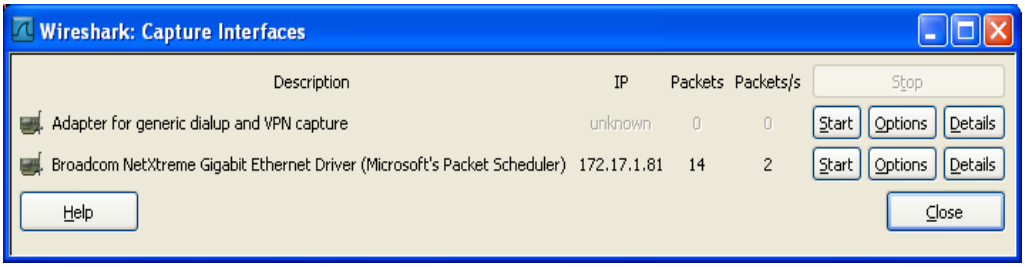


Figura 6. 17 Pantalla Captura de interfaces (Adaptadores de red).

Tres botones se visualizan por cada interfaz

- Start, para iniciar
- Options, para configurar
- Details, proporciona información adicional de la interfaz como su descripción, estadísticas, etc.

2. Otra opción es seleccionar con el Mouse el icono  en la barra de herramientas, se despliega la siguiente ventana donde se muestra opciones de configuración para la interfaz.

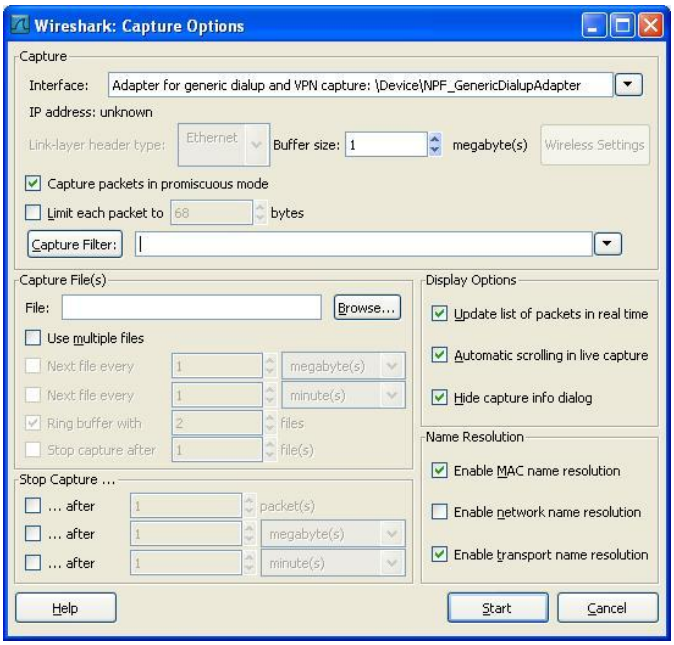


Figura 6. 18 Opciones de configuración de interfaz.

3. Si es el caso donde se ha predefinido las opciones de la interfaz, haciendo clic en  se inicia la captura de paquetes inmediatamente.

4. Otra manera de iniciar la captura de paquetes es desde la línea de comandos ejecutando lo siguiente:

```
wireshark –i eth0 -k
```

Donde –i es la opción que hace referencia a la interfaz de red y eth0 corresponde a la interfaz por la cual se desea iniciar la captura de paquetes.

- **Detener/Reiniciar la captura de paquetes con Wireshark**

Para detener la captura de paquetes podemos aplicar una de las siguientes opciones:

- Haciendo uso del icono  desde el menú Capture o desde la barra de herramientas.
- Haciendo uso de ctrl+E.
- La captura de paquetes puede ser detenida automáticamente, si una de las condiciones de parada definidas en las opciones de la interfaz se cumple, por ejemplo: si se excede cierta cantidad de paquetes.

Para reiniciar el proceso de captura de paquetes se debe seleccionar el icono  en la barra de herramientas o en desde el menú Capture.

- **Filtrado de paquetes con Wireshark**

Wireshark hace uso de libpcap para la definición de filtros. Su sintaxis consta de una serie de expresiones conectadas por conjugaciones (and/or) con la opción de ser negada por el operador not.

```
[not] Expresión [ and|or [not] expresión…]
```

La siguiente expresión define un filtro para la captura de paquetes desde/hacia los host con dirección IP x.y.z.w y a.b.c.d

```
ip.addr==172.17.250.1 and ip.addr==172.17.1.81
```

- **Manipulando las paquetes capturados (análisis) con Wireshark**

Una vez que se tienen capturados los paquetes estos son listados en el panel de paquetes capturados, al seleccionar uno de estos se despliega el contenido del paquete en el resto de los paneles que son panel de detalles de paquetes y panel en bytes.

Expandiendo cualquiera parte del árbol presentado en el panel de detalle del paquete, se puede seleccionar un campo en particular cuyo contenido se muestra resaltado en negritas en el panel de bytes. En la siguiente imagen se identifica en campo TTL del la cabecera del IP.

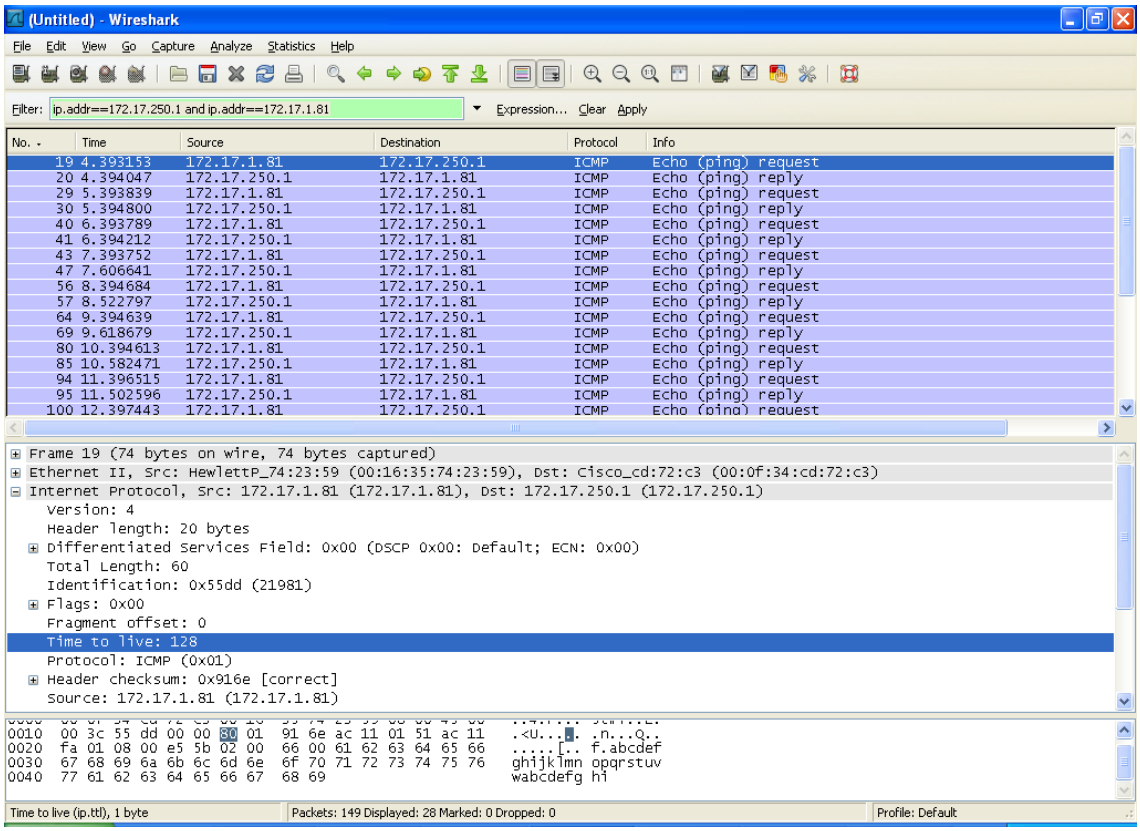


Figura 6. 19 Paquetes capturados con Wireshark.

Existe una manera de visualizar los paquetes mientras esta activo el proceso de captura esto se logra, seleccionando la opción Update list packets in real time desde menú Edit->Preferentes->Capture. Adicionalmente, Wireshark permite visualizar el contenido de un paquete seleccionado en el panel de paquetes capturados en una ventana individualmente seleccionando la opción Show Packet in new Windows en menú principal View. Esto permite comparar con más facilidad dos o más paquetes.".

- **Cain & Abel para realizar ataque de envenenamiento ARP**

Según el sitio oficial (Internet, s.f., 04-02-2012 10:00:00 pm) "Cain & Abel es una herramienta de recuperación de contraseña para los sistemas operativos de Microsoft. Permite una fácil recuperación de diversos tipos de contraseñas por inhalación de la red, craqueo de contraseñas encriptadas usando ataques de diccionario, fuerza bruta y Criptoanálisis, grabación de conversaciones VoIP, decodificación revueltos contraseñas, recuperación de claves de red inalámbrica, revelando cuadros de contraseña, el descubrimiento de contraseñas en caché y el análisis de enrutamiento protocolos. El programa no explota ninguna vulnerabilidad de software o errores que no podían ser corregidos con poco esfuerzo.

La última versión es más rápida y contiene una gran cantidad de nuevas características como APR (Arp Poison Routing), que permite mirar el tráfico en las LAN conmutadas y los ataques Man-in-the-Middle. El succionador en esta versión también se puede analizar protocolos cifrados, como SSH-1 y HTTPS, y contiene filtros para capturar las credenciales de un amplio rango de mecanismos de autenticación. La nueva versión también viene monitores de enrutamiento de protocolos de autenticación y extractores de rutas, de diccionario y de fuerza bruta, cookies para todos los algoritmos hash comunes y para varias autenticaciones específicas, calculadoras contraseña / hash, ataques de criptoanálisis, decodificadores

de contraseñas y algunas utilidades no tan comunes relacionados con la red y sistema de seguridad.”.

- **Sniffing con Cain y Abel**

Como se menciona en la publicación (Internet, s.f., 12-03-2012 08:00pm) “Caín, Necesita ser configurado, para eso abrimos el programa, y nos dirigimos al Menú "**Configure**", ahí seleccionamos nuestro adaptador de red, y en la pestaña "**APR (Arp Poison Routing)**" tenemos opciones de utilizar nuestras direcciones IP y MAC reales, o spoofearlas:

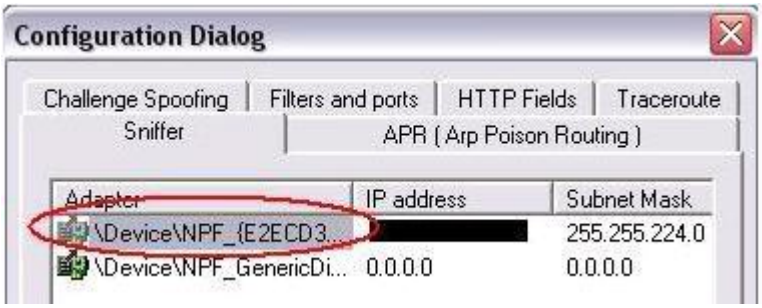


Figura 6. 20 Selección de la tarjeta de red con Cain.

Bien, una vez hecho ésto, clickeamos en <Aceptar> y tendremos frente a nosotros a Caín. Hoy sniffaremos de todo lo que salga, Contraseñas Encriptadas, Texto Plano, Ftp, Http, Myspace, Hi5, etc. Venga, nos vamos a la Pestaña Superior "**Sniffer**" y luego a la Pestaña inferior "**Hosts**", Una vez ahí, Arrancamos el Sniffer, ¿Cómo?, pues en el Segundo botón que aparece arriba, al lado de una carpeta:

Figura 6. 21 Opción para iniciar o detener el sniffer.

Listo, ahora Hacemos click secundario sobre Caín y seleccionamos "**Scan Mac Addresses**" como en la Imagen:

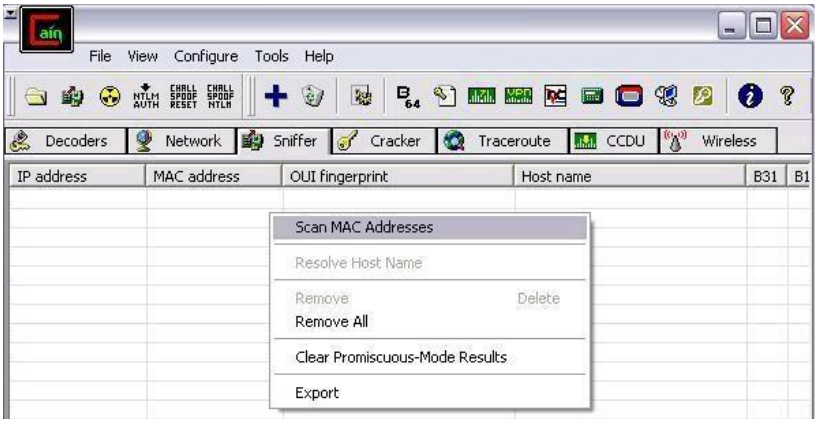


Figura 6. 22 Opción para escanear las direcciones MACs, IPs de la red.

Esto buscará direcciones MAC de ordenadores en nuestra Red, así que esperamos...

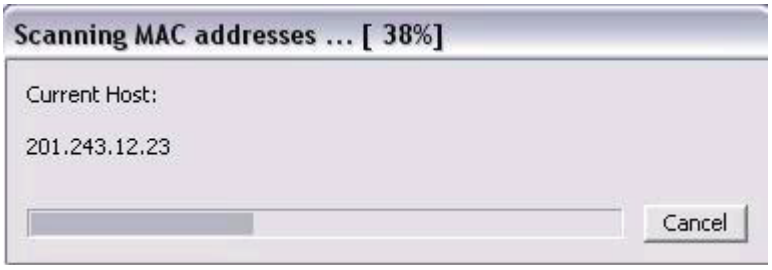


Figura 6. 23 Escaneo de las direcciones MACs conectadas y activas en la red.

Pasado un tiempo, Caín ya habrá escaneado toda la Red, así que seleccionamos las direcciones IP de los "Targets" u objetivos que queremos sniffar, para eso nos vamos a la pestaña inferior "APR" y clickeamos sobre el botón "Add to list":

Figura 6. 24 Seleccionar y añadir direcciones IP a sniffar a la lista.

Acto seguido aparecerá una ventana doble, En la izquierda seleccionamos el objetivo "A" de la lista de IPs, esto llenará el lado derecho con otras direcciones IP, en ese lado debemos seleccionar la IP del objetivo "B" (El Gateway), Justo como un 'Man In The Middle':

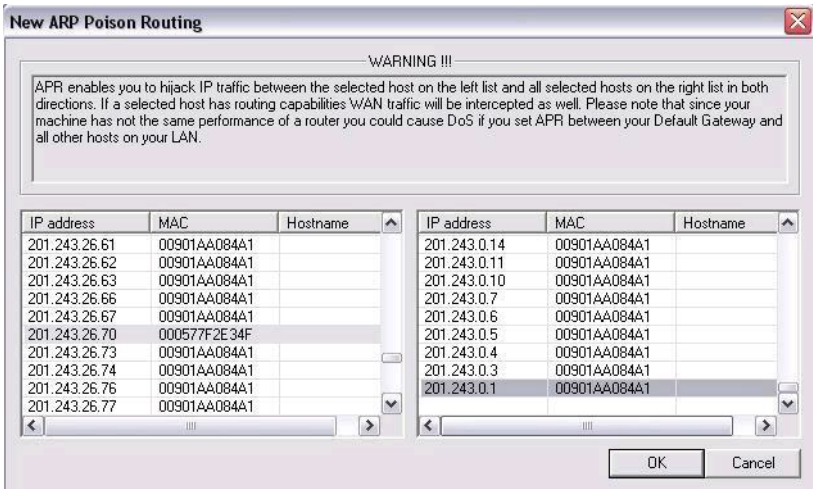


Figura 6. 25 Seleccionar IP objetivo “A” (víctima) e IP objetivo “B” (gateway).

Esa es la tabla en la que le indicaremos a Caín cómo deberá envenenar las tablas ARP (Address Resolution Protocol) de las víctimas.

Nota: Si estás en una red concentrada (Conectada por Hubs), no es necesario envenenar las tablas ARP de nadie, ya que los paquetes llegan solos, en cambio, si estás en una red conmutada (Switch), sí es necesario envenenar las tablas ARP de la red.

Hecho esto, debemos empezar a envenenar las tablas ARP de nuestra Red (porque estoy bajo un Switch, mi red es conmutada), para eso hacemos click sobre el botón amarillo de "APR", marcado en la Imagen, también he marcado en azul la indicación de Caín de que está "Poisoning" es decir, envenenando:

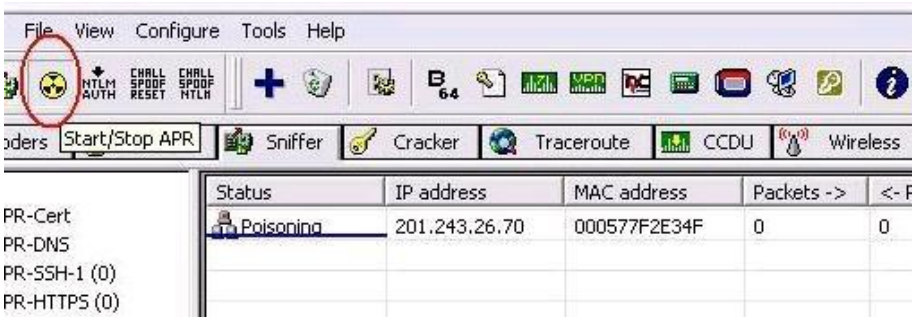


Figura 6. 26 Opción para empezar a envenenar tablas ARP.

Ya ha empezado el ataque, ya sólo nos queda tomarnos un café, y esperar a que nuestra víctima introduzca todas sus contraseñas como lo haría todos los días, ya que no se dará cuenta del envenenamiento...

Sólo 2 minutos después, revisemos el resultado de Caín, para eso nos dirigimos a la pestaña superior Sniffer y a la pestaña inferior Passwords. Veamos:

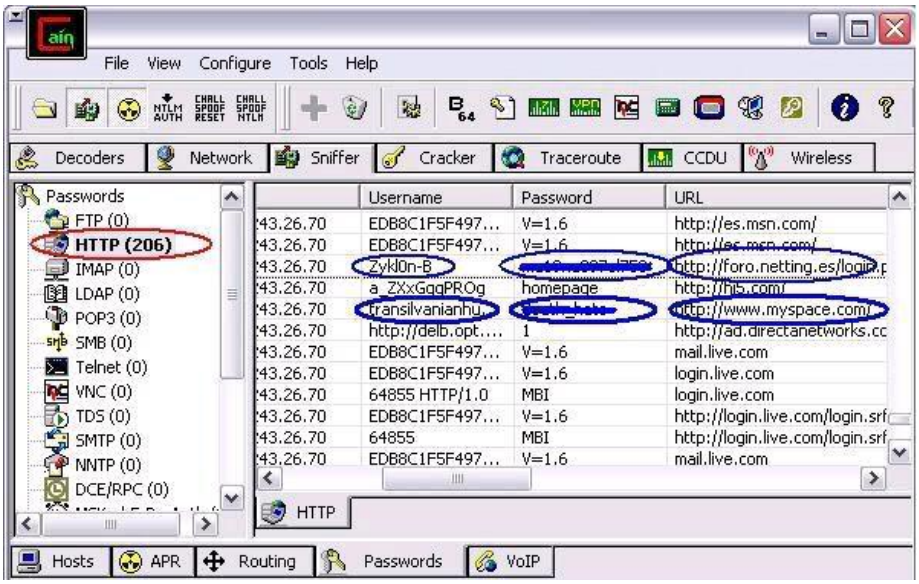


Figura 6. 27 Resultado del ataque con envenenamiento ARP.

¡Vaya, 206 passwords! , Pero no se emocionen, sólo son paquetes, pero he resaltado en azul los passwords que sí son verdaderos, y para colmo, viajan en texto plano. Un ejemplo:

Figura 6. 28 Usuarios y Contraseñas obtenidas por el ataque de envenenamiento ARP.

Ahí podemos ver las contraseñas de Myspace, Google y Hi5, todas en texto plano. Vaya seguridad, ¿eh?

Así sucede con los passwords en FTP, SMTP, HTTP, POP3, VNC, MYSQL, ICQ, Hi5, Photobucket, Yahoo, Hotmail, Gmail, etc.,. Y además, Caín contiene "Certificados de Autenticidad" falsos. Para hacerle creer a la víctima que todo anda bien y legal, como verán, "Hackear contraseñas" no es nada del otro mundo cuando disponemos de Caín.

Ahora, ¿qué sucede cuando el Caín detecta passwords encriptados? ¿Los desecha? Pues no, Caín, automáticamente los lleva a la pestaña superior "Cracker" ¿Qué es eso? ¡Hombre! es lógico lo que es, un crackeador múltiple de contraseñas. Ahí tenemos una lluvia de opciones, podemos desencriptar contraseñas a través de diversos modos, Bruteforce, Criptoanálisis, Ataque por Diccionario, etc.
Caín, también funciona Sniffando paquetes Wireless, y hasta tiene herramientas de Wep Cracking y demás, y puede ser combinado con otras herramientas tales como Airpcap, Airdump, etc.

Nota: Les recomiendo que cuando se encuentren sniffando no abran en sus ordenadores páginas ni ningún tipo de conexiones, ya que esto les dificultará más el trabajo, recuerden que estamos "Husmeando" los paquetes que llegan a nuestra tarjeta de Red, y si nosotros metemos más paquetes ni les cuento...
¡Ah! que se me olvida, para poder cerrar Caín deben parar el envenenamiento APR y detener el Sniffer.”.

- **Herramienta MAC MakeUP para ataque de suplantación de identidad**

Es un programa Windows que permite cambiar la dirección física (MAC) de un computador. Tiene la opción para digitar la dirección MAC a cambiar o también se puede generar una dirección física de una manera aleatoria.

Al ejecutar el programa primero se debe seleccionar la tarjeta de red a usar, como se muestra en la siguiente figura:

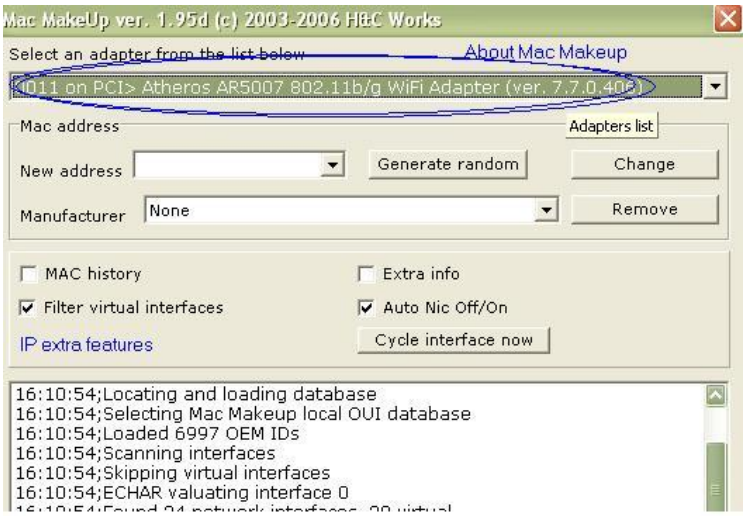


Figura 6. 29 Seleccionar la tarjeta de red a usar.

Una vez seleccionada la tarjeta de red, se tiene que escribir la nueva dirección física (MAC) o presionar el botón que dice Generate random (para generar aleatoriamente una dirección MAC) y finalmente presionamos el botón Change (cambiar).

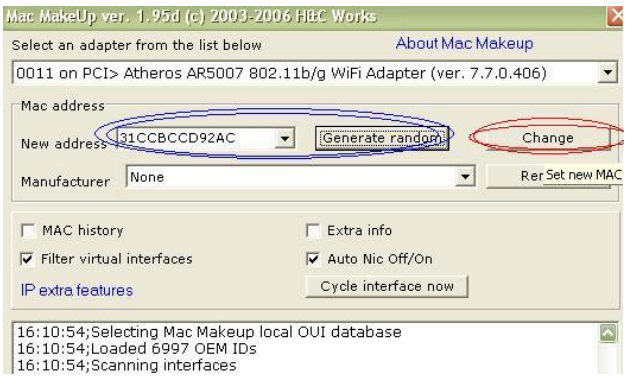


Figura 6. 30 Escribir o seleccionar la nueva dirección MAC.

6.6.2 Políticas de Seguridad

Según la publicación (Internet, s.f., 05-02-2012 06:02:00 pm) “Declaración general de principios que presenta la posición de la administración para un área de control

definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías. Las políticas deben ser pocas (es decir, un número pequeño), deben ser apoyadas y aprobadas por las directivas de la universidad, y deben ofrecer direccionamientos a toda la organización o a un conjunto importante de dependencias. Por definición, las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción.".

Como se menciona en la publicación (Internet, 16-10-2008, 10-10-2011 22:26:00) "Uno de los primeros pasos que debe dar una compañía es definir una política de seguridad que pueda implementar en función a las siguientes cuatro etapas:

- Identificar las necesidades de seguridad y los riesgos informáticos que enfrenta la compañía así como sus posibles consecuencias.

- Proporcionar una perspectiva general de las reglas y los procedimientos que deben implementarse para afrontar los riesgos identificados en los diferentes departamentos de la organización.

- Controlar y detectar las vulnerabilidades del sistema de información, y mantenerse informado acerca de las falencias en las aplicaciones y en los materiales que se usan.

- Definir las acciones a realizar y las personas a contactar en caso de detectar una amenaza.

La política de seguridad comprende todas las reglas de seguridad que sigue una organización (en el sentido general de la palabra). Por lo tanto, la administración de la

organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.”.

- **Etapas en el desarrollo de una Política**

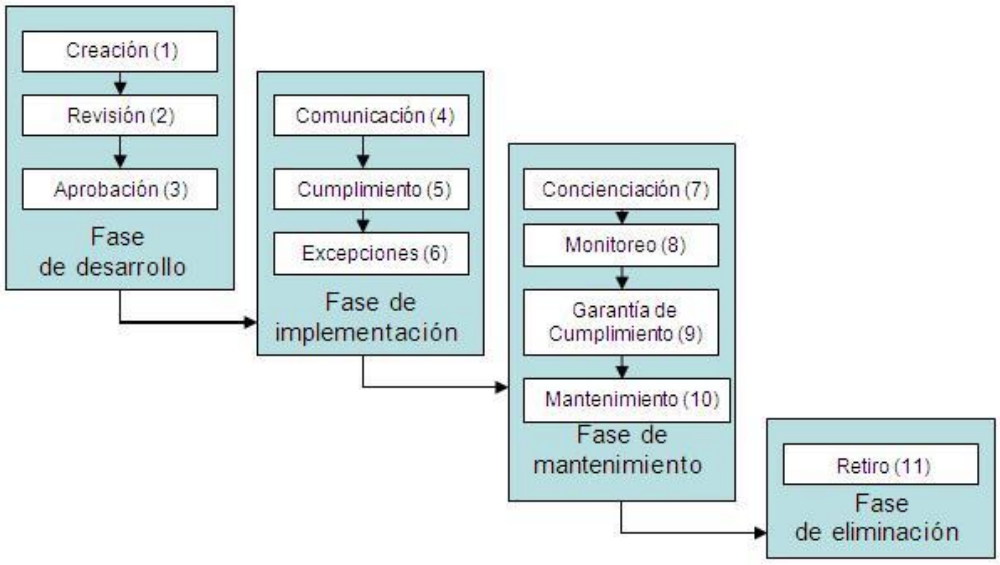


Figura 6. 31 Etapas en el desarrollo de políticas.

Como se menciona en la publicación (Internet, s.f., 06-02-2012 03:15:00 pm) “Hay 11 etapas que deben realizarse a través de “la vida” de una política. Estas 11 etapas pueden ser agrupadas en 4 fases.

1. Fase de desarrollo: durante esta fase la política es creada, revisada y aprobada.
2. Fase de implementación: en esta fase la política es comunicada y acatada (o no cumplida por alguna excepción).
3. Fase de mantenimiento: los usuarios deben ser conscientes de la importancia de la política, su cumplimiento debe ser monitoreado, se debe garantizar su cumplimiento y se le debe dar mantenimiento (actualizarla).
4. Fase de eliminación: La política se retira cuando no se requiera más.

- **Creación:** Planificación, investigación, documentación, y coordinación de la política

El primer paso en la fase de desarrollo de una política es la planificación, la investigación y la redacción de la política o, tomado todo junto, la creación. La creación de una política implica identificar por qué se necesita la política (por ejemplo, requerimientos legales, regulaciones técnicas, contractuales u operacionales); determinar el alcance y la aplicabilidad de la política, los roles y las responsabilidades inherentes a la aplicación de la política y garantizar la factibilidad de su implementación. La creación de una política también incluye la investigación para determinar los requerimientos organizacionales para desarrollar las políticas (es decir, que autoridades deben aprobarla, con quién se debe coordinar el desarrollo y estándares del formato de redacción), y la investigación de las mejores prácticas en la industria para su aplicabilidad a las necesidades organizacionales actuales. De esta etapa se tendrá como resultado la documentación de la política de acuerdo con los procedimientos y estándares de la universidad, al igual que la coordinación con entidades internas y externas que la política afectará, para obtener información y su aceptación. En general, la creación de una política es la función más fácil de entender en el ciclo de vida de desarrollo de una política.

- **Revisión:** Evaluación independiente de la política

La revisión de la política es la segunda etapa en la fase de desarrollo del ciclo de vida. Una vez la documentación de la política ha sido creada y la coordinación inicial ha sido iniciada, esta debe ser remitida a un grupo (o un individuo) independiente para su evaluación antes de su aprobación final. Hay varios beneficios de la revisión independiente: una política más viable a través del escrutinio de individuos que tienen

una perspectiva diferente o más vasta que la persona que redactó la política; apoyo más amplio para la política a través de un incremento en el número de involucrados; aumento de credibilidad en la política gracias a la información recibida de diferentes especialistas del grupo de revisión. Propio de esta etapa es la presentación de la política a los revisores, ya sea de manera formal o informal, exponiendo cualquier punto que puede ser importante para la revisión, explicando su objetivo, el contexto y los beneficios potenciales de la política y justificando por qué es necesaria. Como parte de esta función, se espera que el creador de la política recopile los comentarios y las recomendaciones para realizar cambios en la política y efectuar todos los ajustes y las revisiones necesarias para obtener una versión final de la política lista para la aprobación por las directivas.

- **Aprobación:** Obtener la aprobación de la política por parte de las directivas

El paso final en la fase de desarrollo de la política es la aprobación. El objetivo de esta etapa es obtener el apoyo de la administración de la universidad, a través de la firma de una persona ubicada en una posición de autoridad.

La aprobación permite iniciar la implementación de la política. Requiere que el proponente de la política haga una selección adecuada de la autoridad de aprobación, que coordine con dicho funcionario, presente las recomendaciones emitidas durante la etapa de revisión y haga el esfuerzo para que sea aceptada por la administración. Puede ocurrir que por incertidumbre de la autoridad de aprobación sea necesaria una aprobación temporal.

- **Comunicación:** Difundir la política

Una vez la política ha sido aprobada formalmente, se pasa a la fase de implementación. La comunicación de la política es la primera etapa que se realiza en

esta fase. La política debe ser inicialmente difundida a los miembros de la comunidad universitaria o a quienes sean afectados directamente por la política (contratistas, proveedores, usuarios de cierto servicio, etc.). Esta etapa implica determinar el alcance y el método inicial de distribución de la política (es posible que deban tenerse en cuenta factores como la ubicación geográfica, el idioma, la cultura y línea de mando que será utilizada para comunicar la política). Debe planificarse esta etapa con el fin de determinar los recursos necesarios y el enfoque que debe ser seguido para mejorar la visibilidad de la política.

- **Cumplimiento:** Implementar la política.

La etapa de cumplimiento incluye actividades relacionadas con la ejecución de la política. Implica trabajar con otras personas de la universidad, vicerrectores, decanos, directores de departamento y los jefes de dependencias (de división o de sección) para interpretar cuál es la mejor manera de implementar la política en diversas situaciones y oficinas; asegurando que la política es entendida por aquellos que requieren implementarla, monitorearla, hacerle seguimiento, reportar regularmente su cumplimiento y medir el impacto inmediato de la política en las actividades operativas. Dentro de estas actividades está la elaboración de informes a la administración del estado de la implementación de la política.

- **Excepciones:** Gestionar las situaciones donde la implementación no es posible.

Debido a problemas de coordinación, falta de personal y otros requerimientos operacionales, no todas las políticas pueden ser cumplidas de la manera que se pensó al comienzo. Por esto, cuando los casos lo ameriten, es probable que se requieran excepciones a la política para permitir a ciertas oficinas o personas el no cumplimiento de la política. Debe establecerse un proceso para garantizar que las solicitudes de excepciones son registradas, seguidas,

evaluadas, enviadas para aprobación o desaprobación, documentadas y vigiladas a través del periodo de tiempo establecido para la excepción. El proceso también debe permitir excepciones permanentes a la política al igual que la no aplicación temporal por circunstancias de corta duración.

- **Concienciación:** Garantiza la concienciación continuada de la política.

La etapa de concienciación de la fase de mantenimiento comprende los esfuerzos continuos realizados para garantizar que las personas están conscientes de la política y buscan facilitar su cumplimiento. Esto es hecho al definir las necesidades de concienciación de los diversos grupos de audiencia dentro de la organización (directivos, jefes de dependencias, usuarios, etc.); en relación con la adherencia a la política, determinar los métodos de concienciación más efectivos para cada grupo de audiencia (es decir, reuniones informativas, cursos de entrenamiento, mensajes de correo, etcétera); y desarrollo y difusión de material de concienciación (presentaciones, afiches, circulares, etc.). La etapa de concienciación también incluye esfuerzos para integrar el cumplimiento de la política y retroalimentación sobre el control realizado para su cumplimiento. La tarea final es medir la concienciación de los miembros de la comunidad universitaria con la política y ajustar los esfuerzos de acuerdo con los resultados de las actividades medidas.

- **Monitoreo:** Seguimiento y reporte del cumplimiento de la política.

Durante la fase de mantenimiento, la etapa de monitoreo es realizada para seguir y reportar la efectividad de los esfuerzos en el cumplimiento de la política. Esta información se obtiene de la observación de los docentes, estudiantes, empleados y los cargos de supervisión, mediante auditorias formales, evaluaciones, inspecciones, revisiones y análisis de los reportes de contravenciones y de las

actividades realizadas en respuesta a los incidentes. Esta etapa incluye actividades continuas para monitorear el cumplimiento o no de la política a través de métodos formales e informales y el reporte de las deficiencias encontradas a las autoridades apropiadas.

- **Garantía de cumplimiento:** Afrontar las contravenciones de la política.

La etapa de garantía de cumplimiento de las políticas incluye las respuestas de la administración a actos u omisiones que tengan como resultado contravenciones de la política con el fin de prevenir que sigan ocurriendo. Esto significa que una vez una contravención sea identificada, la acción correctiva debe ser determinada y aplicada a los procesos (revisión del proceso y mejoramiento), a la tecnología (actualización) y a las personas (acción disciplinaria) involucrados en la contravención con el fin de reducir la probabilidad de que vuelva a ocurrir. Se recomienda incluir información sobre las acciones correctivas adelantadas para garantizar el cumplimiento en la etapa de concienciación.

- **Mantenimiento:** Asegurar que la política esté actualizada.

La etapa de mantenimiento está relacionada con el proceso de garantizar la vigencia y la integridad de la política. Esto incluye hacer seguimiento a las tendencias de cambios (cambios en la tecnología, en los procesos, en las personas, en la organización, en el enfoque del negocio, etcétera) que puede afectar la política; recomendando y coordinando modificaciones resultado de estos cambios, documentándolos en la política y registrando las actividades de cambio. Esta etapa también garantiza la disponibilidad continuada de la política para todas las partes afectadas por ella, al igual que el mantenimiento de la integridad de la política a través de un control de versiones efectivo. Cuando se

requieran cambios a la política, las etapas realizadas antes deben ser re-visitadas, en particular las etapas de revisión, aprobación, comunicación y garantía de cumplimiento.

- **Retiro:** Prescindir de la política cuando no se necesite más.

Después que la política ha cumplido con su finalidad y no es necesaria (por ejemplo, la empresa cambió la tecnología a la cual aplicaba o se creó una nueva política que la reemplazó) entonces debe ser retirada. La etapa de retiro corresponde a la fase de eliminación del ciclo de vida de la política, y es la etapa final del ciclo. Esta función implica retirar una política superflua del inventario de políticas activas para evitar confusión, archivarla para futuras referencias y documentar la información sobre la decisión de retirar la política (es decir, la justificación, quién autorizó, la fecha, etcétera). Estas cuatro fases del ciclo de vida reúnen 11 etapas diferentes que deben seguirse durante el ciclo de vida de una política específica. No importa cómo se agrupen, tampoco importa si estas etapas son abreviadas por necesidades de inmediatez, pero cada etapa debe ser realizada. Si en la fase de desarrollo la universidad intenta crear una política sin una revisión independiente, se tendrán políticas que no estarán bien concebidas ni serán bien recibidas por la comunidad universitaria. En otras circunstancias, y por falta de visión, puede desearse omitir la etapa de excepciones de la fase de implementación, pensando equivocadamente que no existirán circunstancias para su no cumplimiento. También se podría descuidar la etapa de mantenimiento, olvidando la importancia de mantener la integridad y la vigencia de las políticas. Muchas veces se encuentran políticas inoficiosas en los documentos de importantes organizaciones, indicando que la etapa de retiro no está siendo realizada.

No sólo se requiere que las once etapas sean realizadas, algunas de ellas deben ser ejecutadas de manera cíclica, en particular mantenimiento, concienciación,

monitoreo, y garantía de cumplimiento. ”.

- **Acompañamiento de la política de seguridad.**

Una política de seguridad para que sea efectiva, necesita contar con elementos indispensables que apoyen este proceso: La cultura organizacional, las herramientas y el monitoreo. Esto involucra la participación directa y comprometida de las personas, el diseño de planes de capacitación constante a los usuarios. La disponibilidad de recursos financieros, técnicos y tecnológicos es fundamental y sobre todo actividades de control y retroalimentación que diagnostiquen e identifiquen puntos débiles para fortalecerlos siguiendo las mejores prácticas.
Las organizaciones pueden definir unos ámbitos básicos o esenciales en donde empezar a implementar políticas de seguridad; entre los más comunes encontramos:

- Seguridad física: acceso físico, estructura del edificio, centro de datos5.
- Seguridad de la red corporativa: configuración de los sistemas operativos, acceso lógico y remoto, autenticación, Internet, disciplina operativa, gestión de cambios, desarrollo de aplicaciones.
- Seguridad de usuarios: composición de claves, seguridad en estaciones de trabajo, formación y creación de conciencia.
- Seguridad de datos: criptografía, clasificación, privilegios, copias de seguridad y recuperación, antivirus, plan de contingencia.
- Auditoria de seguridad: análisis de riesgo, revisiones periódicas, visitas técnicas, monitoreo y auditoria.
- Aspectos legales: prácticas personales, contratos y acuerdos comerciales, leyes y reglamentación gubernamental.”.

6.7 Metodología.

Las herramientas que se utilizarán para el presente proyecto son: distribución Linux Backtrack 5 y sus componentes de análisis (airmon-ng, airodump-ng, aireplay-ng), Mac MakeUp (herramienta Windows), Wireshark (herramienta Windows), Cain (herramienta Windows).

Para la creación de las políticas de seguridad para la comunicación inalámbrica de la empresa se utilizará el siguiente esquema (publicación web), donde se realizará las dos primeras fases (Fase de Desarrollo, Fase de implementación):

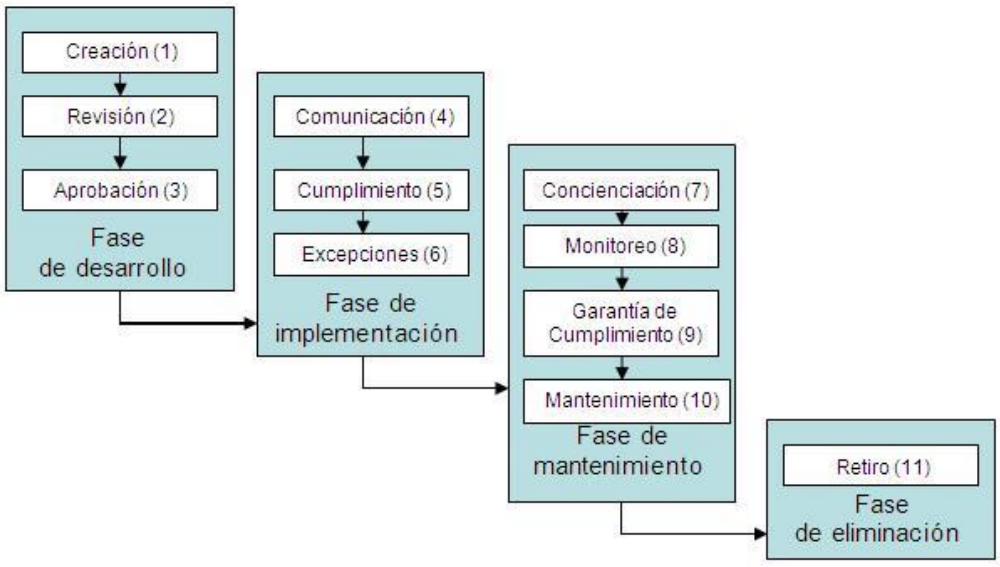


Figura 6. 32 Según publicación web, esquema de las etapas de elaboración de políticas.

6.8 Modelo Operativo.

Se utilizó la herramienta Snort para establecer los tipos de amenazas informáticas en la empresa Automekano; para determinar las vulnerabilidades se realizó un escaneo

de un computador servidor (Windows Server 2003) con la herramienta informática Nessus. El respectivo análisis de las amenazas informáticas se lo efectuó mediante los siguientes ataques por parte del investigador: Negación de servicios (DOS), Romper la clave WPA del punto de acceso, suplantación de dirección MAC, captura de paquetes FTP, para lo cual se utilizaron: Dos computadoras portátiles, una fue el cliente y la otra el atacante; También el respectivo punto de acceso inalámbrico (empresa AUTOMEKANO); Además se usó un servidor (Windows Server 2003) con servicio FTP (cliente/servidor) que ya viene funcionando en la empresa.

6.8.1 Tipos de Amenazas Informáticas en la comunicación inalámbrica mediante el uso de la herramienta Snort.

Se utilizó la distribución Linux Backtrack5, al iniciarla se procedió a conectar la tarjeta inalámbrica de la computadora a la red. El punto de acceso asignó al computador la dirección IP 192.168.1.4.

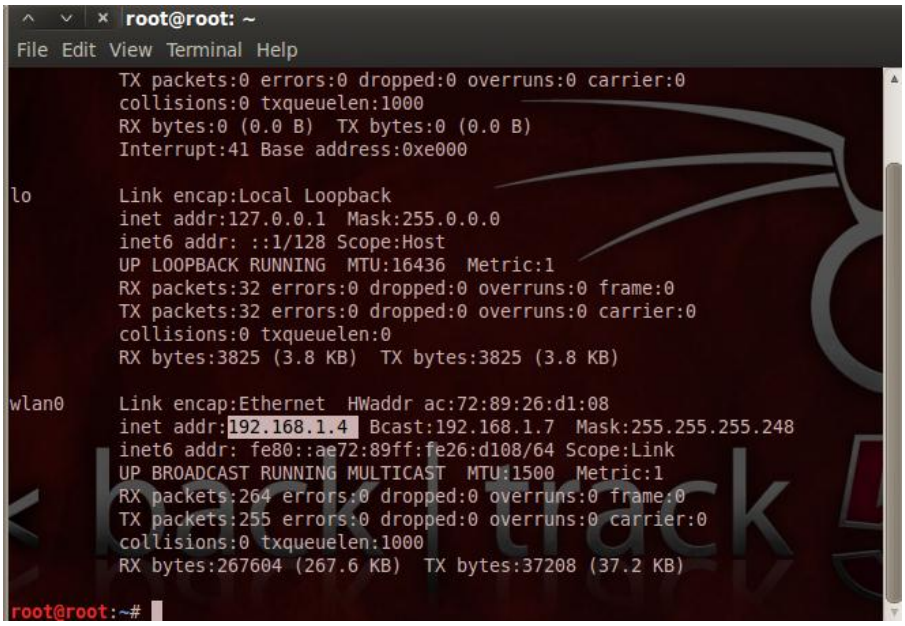


Figura 6. 33 Dirección Ip de la computadora conectada a la red.

Seguidamente se dio inicio al servicio snort: **/etc/init.d/snort start** y se abrió el archivo snort.conf del software snort con un editor de texto (vim), con el siguiente comando: **vim /etc/snort/snort.conf**

Figura 6. 34 Comando para abrir el archivo snort.conf

Una vez abierto el archivo, se debió cambiar la variable: var **HOME_NET any** por var HOME_NET 192.168.1.4 (dirección Ip que asignó el punto de acceso inalámbrico al computador) y var **EXTERNAL_NET any** queda igual.

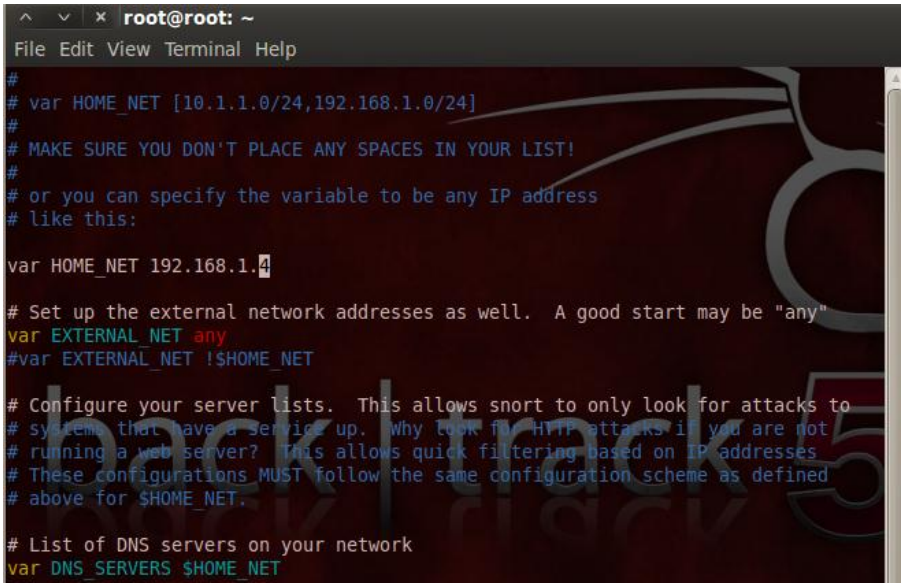


Figura 6. 35 Modificando las variables necesarias, var HOME_NET any.

Después se reinició el servicio snort, con lo siguiente: **/etc/init.d/snort restart**

Figura 6. 36 Reinicio del servicio snort

Para empezar a revisar las amenazas informáticas en la red, se realizó el siguiente comando: **snort –q –A console –i wlan0 –c /etc/snort/snort.conf**

Figura 6. 37 Empezar con el uso de snort y verificar amenazas informáticas.

Se encontró amenazas informáticas, escaneo de puertos, negación de servicios:

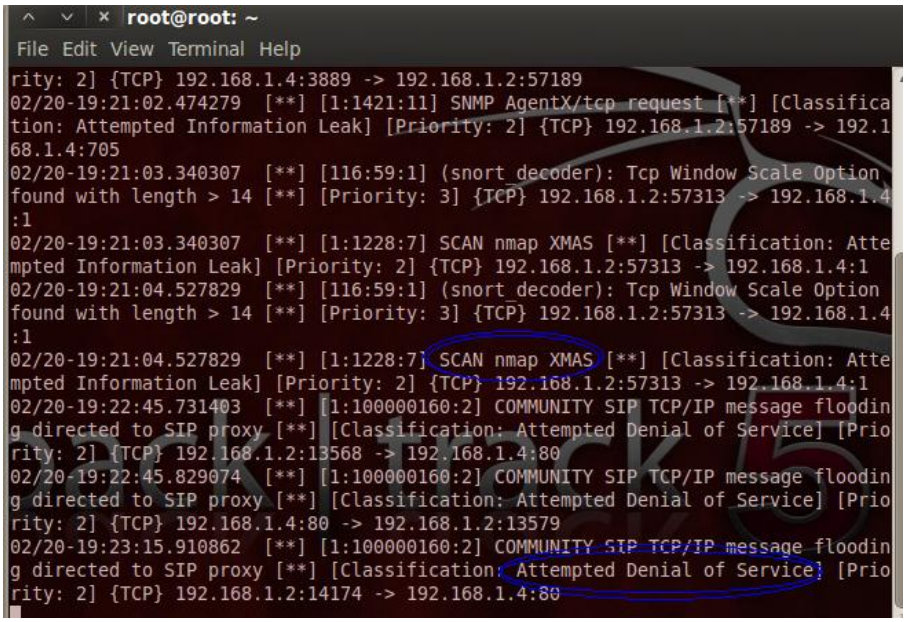


Figura 6. 38 Amenazas informáticas encontradas.

6.8.2 Vulnerabilidades En la comunicación inalámbrica mediante el uso de la herramienta Nessus

Para ello se usó la herramienta Nessus. Lo primero que se hizo es ingresar a la consola web de la herramienta, colocando el nombre de usuario y la respectiva contraseña.

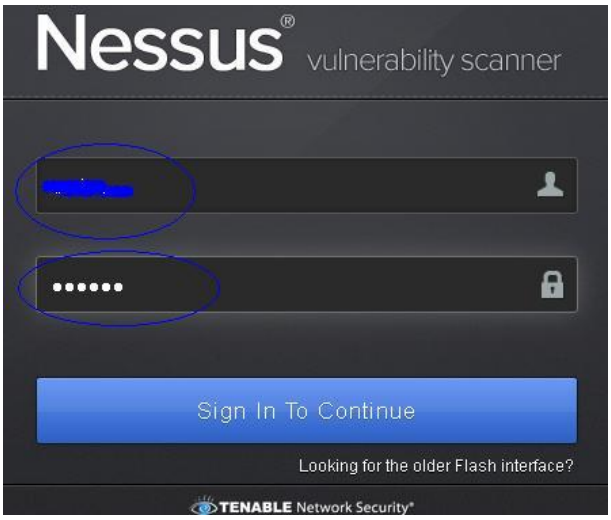


Figura 6. 39 Ingreso a la consola web de Nessus

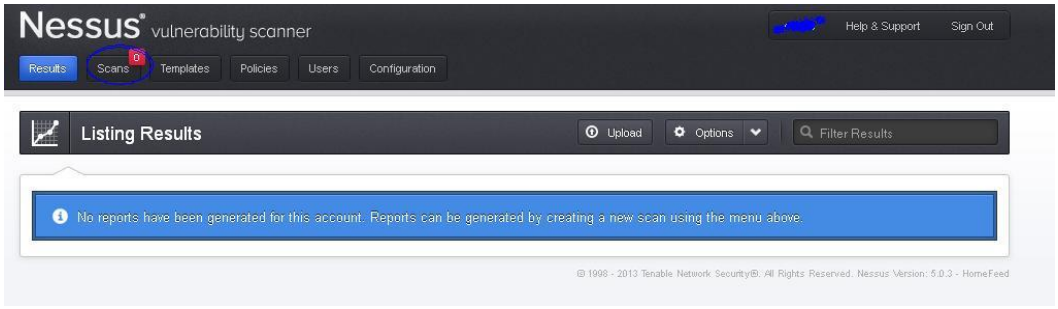


Figura 6. 40 Consola Web de Nessus

Después se hizo un nuevo escaneo, a un computador de la empresa (Windows Server 2003 con servicio FTP); para lo cual se dio clic en la opción **Scans** y en la opción **New Scan**

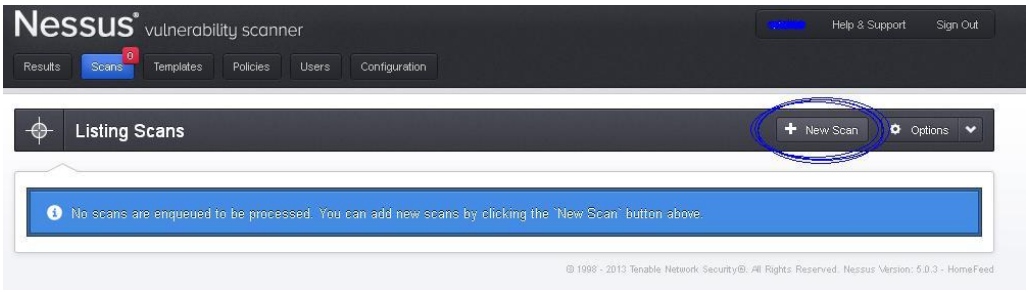


Figura 6. 41 Nuevo escaneo.

En la siguiente ventana se escogieron opciones, como fueron un título, un tipo, una política, y la dirección IP para el escaneo nuevo.

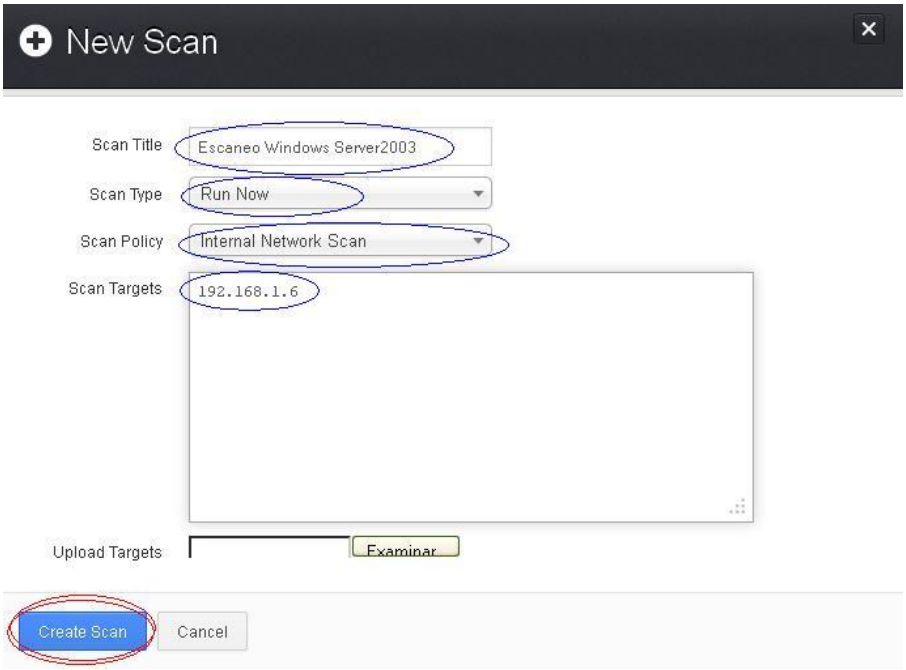


Figura 6. 42 Opciones para crear el nuevo escaneo

Una vez creado el escaneo, comenzó el proceso del mismo y una vez finalizado se obtuvo los siguientes resultados: Se encontraron 101 vulnerabilidades, 9 son de carácter crítico, 30 de nivel alto, 54 son consideradas medias y 8 de nivel bajo.

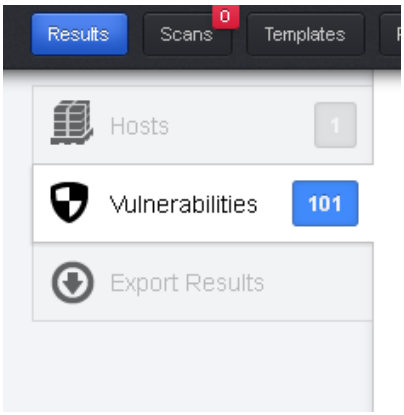


Figura 6. 43 Resultado del análisis de vulnerabilidades

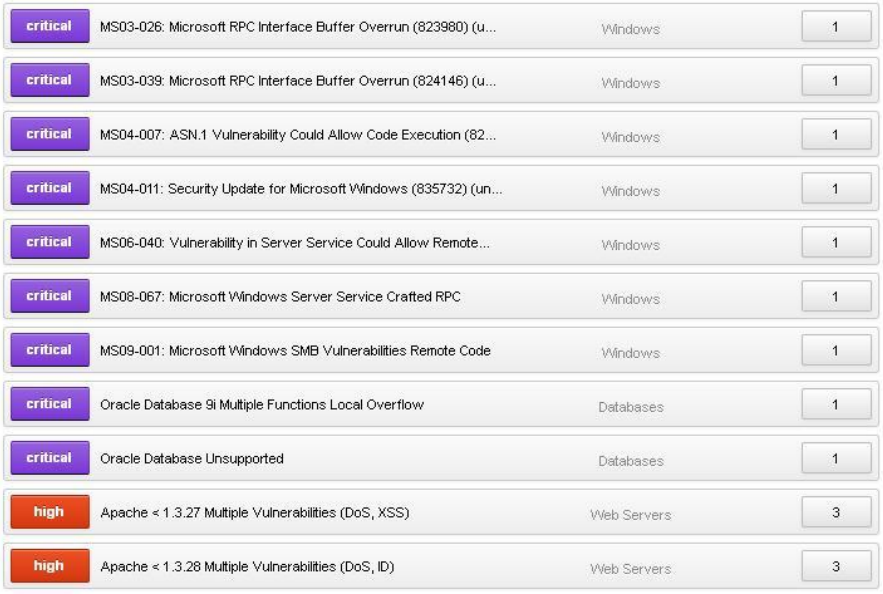
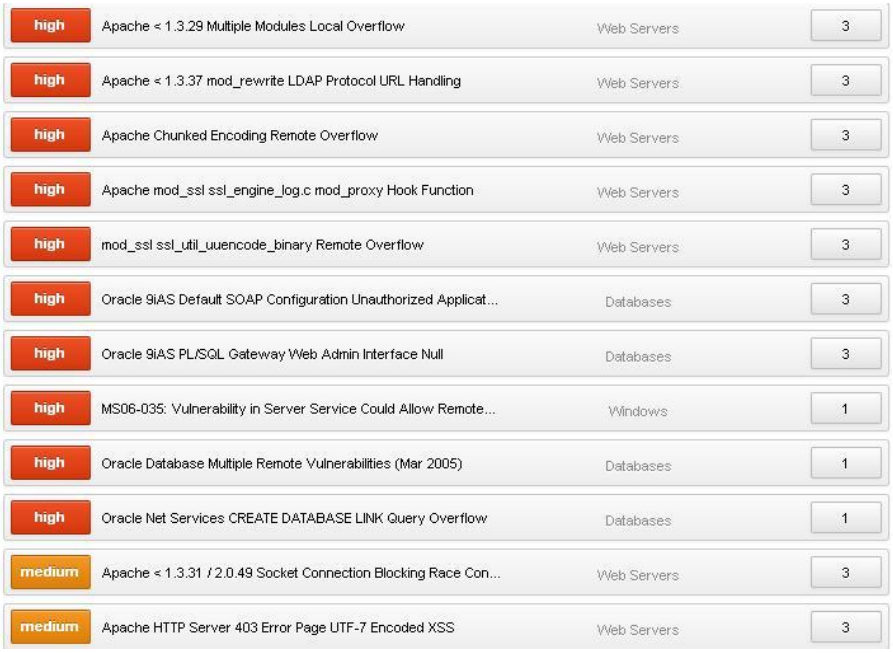
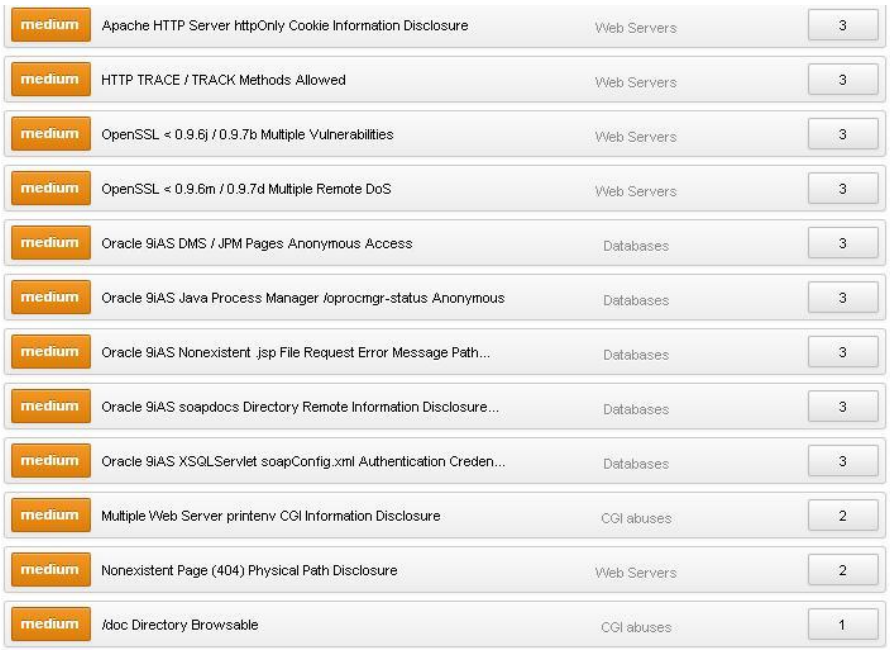


Figura 6. 44 Resultado del análisis de vulnerabilidades a)



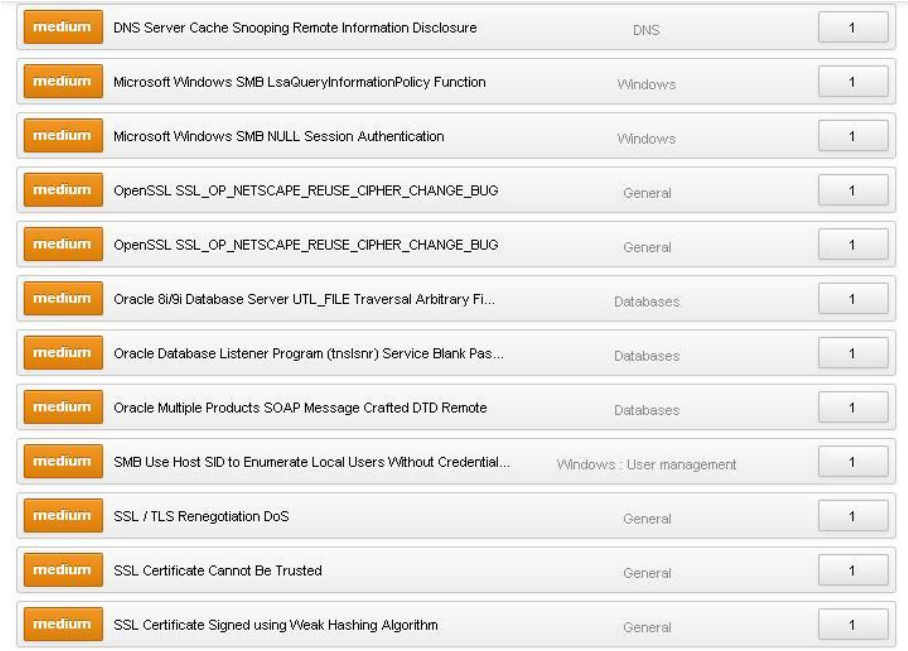
high	Apache < 1.3.29 Multiple Modules Local Overflow	Web Servers	3
high	Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling	Web Servers	3
high	Apache Chunked Encoding Remote Overflow	Web Servers	3
high	Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function	Web Servers	3
high	mod_ssl ssl_util_uuencode_binary Remote Overflow	Web Servers	3
high	Oracle 9iAS Default SOAP Configuration Unauthorized Applicat...	Databases	3
high	Oracle 9iAS PL/SQL Gateway Web Admin Interface Null	Databases	3
high	MS06-035: Vulnerability in Server Service Could Allow Remote...	Windows	1
high	Oracle Database Multiple Remote Vulnerabilities (Mar 2005)	Databases	1
high	Oracle Net Services CREATE DATABASE LINK Query Overflow	Databases	1
medium	Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Con...	Web Servers	3
medium	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS	Web Servers	3

Figura 6. 45 Resultado del análisis de vulnerabilidades b)



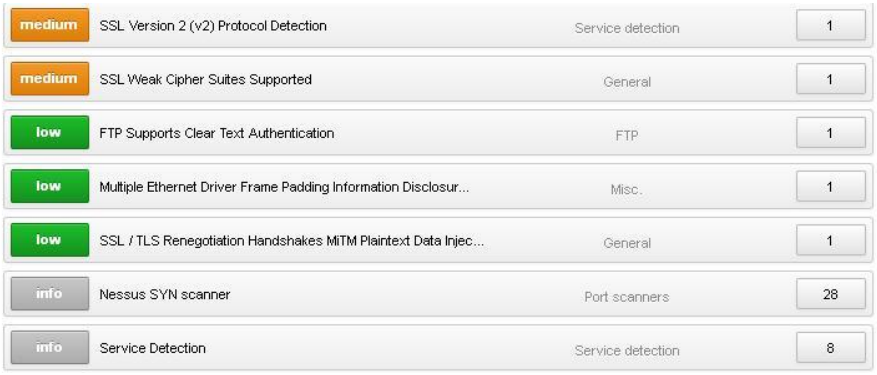
medium	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers	3
medium	HTTP TRACE / TRACK Methods Allowed	Web Servers	3
medium	OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities	Web Servers	3
medium	OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS	Web Servers	3
medium	Oracle 9iAS DMS / JPM Pages Anonymous Access	Databases	3
medium	Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous	Databases	3
medium	Oracle 9iAS Nonexistent .jsp File Request Error Message Path...	Databases	3
medium	Oracle 9iAS soapdocs Directory Remote Information Disclosure...	Databases	3
medium	Oracle 9iAS XSQLServlet soapConfig.xml Authentication Creden...	Databases	3
medium	Multiple Web Server printenv CGI Information Disclosure	CGI abuses	2
medium	Nonexistent Page (404) Physical Path Disclosure	Web Servers	2
medium	/doc Directory Browsable	CGI abuses	1

Figura 6. 46 Resultado del análisis de vulnerabilidades c)



medium	DNS Server Cache Snooping Remote Information Disclosure	DNS	1
medium	Microsoft Windows SMB LsaQueryInformationPolicy Function	Windows	1
medium	Microsoft Windows SMB NULL Session Authentication	Windows	1
medium	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG	General	1
medium	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG	General	1
medium	Oracle 8i/9i Database Server UTL_FILE Traversal Arbitrary Fi...	Databases	1
medium	Oracle Database Listener Program (tnslsnr) Service Blank Pas...	Databases	1
medium	Oracle Multiple Products SOAP Message Crafted DTD Remote	Databases	1
medium	SMB Use Host SID to Enumerate Local Users Without Credential...	Windows : User management	1
medium	SSL / TLS Renegotiation DoS	General	1
medium	SSL Certificate Cannot Be Trusted	General	1
medium	SSL Certificate Signed using Weak Hashing Algorithm	General	1

Figura 6. 47 Resultado del análisis de vulnerabilidades d)



medium	SSL Version 2 (v2) Protocol Detection	Service detection	1
medium	SSL Weak Cipher Suites Supported	General	1
low	FTP Supports Clear Text Authentication	FTP	1
low	Multiple Ethernet Driver Frame Padding Information Disclosur...	Misc.	1
low	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injec...	General	1
info	Nessus SYN scanner	Port scanners	28
info	Service Detection	Service detection	8

Figura 6. 48 Resultado del análisis de vulnerabilidades e)

6.8.3 Ataque De Negación De Servicio

Para efectuar este ataque, lo primero que se realizó fue arrancar la distribución Linux Backtrack 5 con un live CD.

Una vez dentro de Backtrack 5, el siguiente paso fue verificar si está conectada la tarjeta inalámbrica y que nombre la identificaba, para lo cual se abrió una ventana de comandos y se procedió a escribir: **iwconfig**.

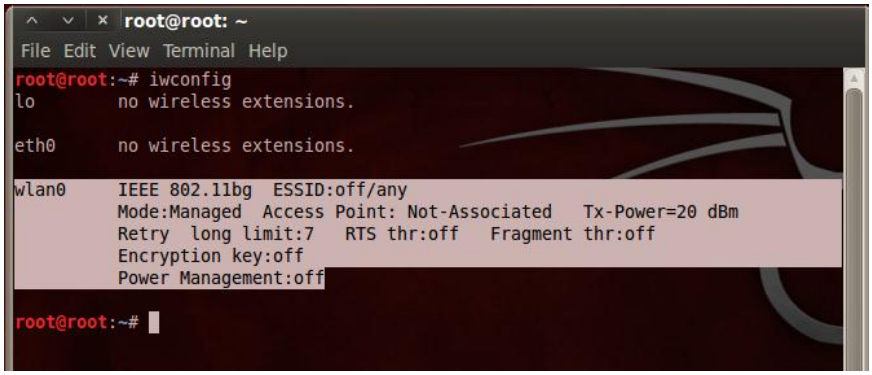


Figura 6. 49 Verificación de tarjetas inalámbricas.

Cuando ya fue identificada la tarjeta inalámbrica se procedió a cambiarla a modo monitor (para escuchar el tráfico de la red), con el comando: **airmon-ng start wlan0**.

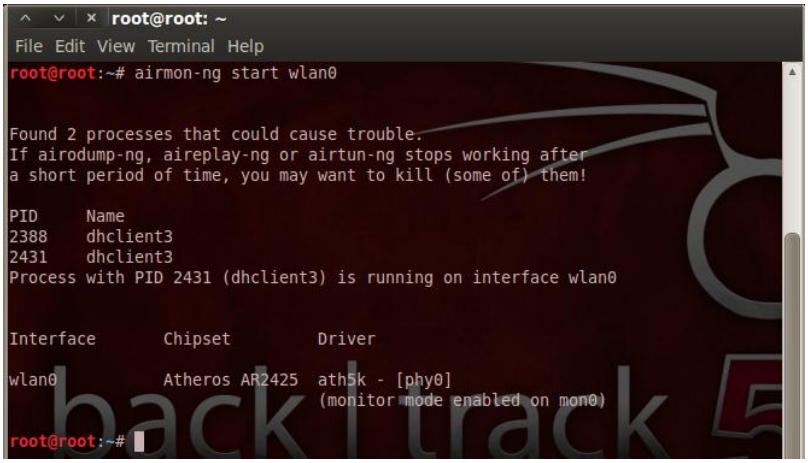


Figura 6. 50 Cambio de la tarjeta inalámbrica a modo monitor.

El identificador que fue asignado a la tarjeta inalámbrica para modo monitor fue: **mon0**, luego para observar todo el tráfico de la red se usó el siguiente comando: **airodump-ng mon0**. Y por consiguiente se pudo obtener información vital como son

las direcciones MAC de los puntos de acceso (AP) a redes inalámbricas y de los clientes inalámbricos; el tipo de encriptación del dispositivo; el ESSID; el canal por el cual transmite el dispositivo inalámbrico; entre otros.

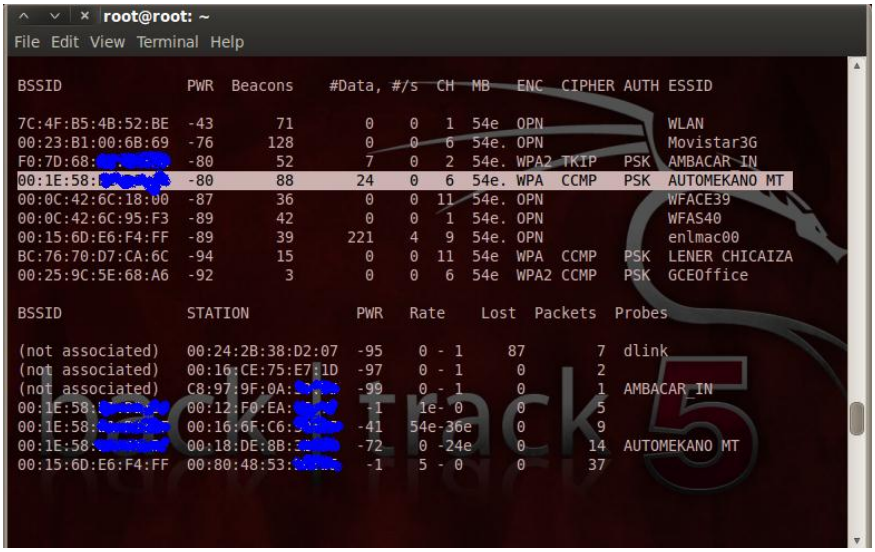


Figura 6. 51 Observación del tráfico de red.

Para concretar con el ataque se necesitó las direcciones MAC del punto de acceso cuyo ESSID es AUTOMEKANO MT y de un cliente conectado al mismo. Se usó el siguiente comando: **aireplay-ng -0 20 –a 00:1E:58:XX:XX:XX –c 00:16:6F:C6:XX:XX mon0**.

Figura 6. 52 Ejecutando el ataque de desautenticación de un usuario.

Después de ejecutar el comando anterior, se empezó a mandar paquetes para la respectiva desautenticación a dicho usuario.

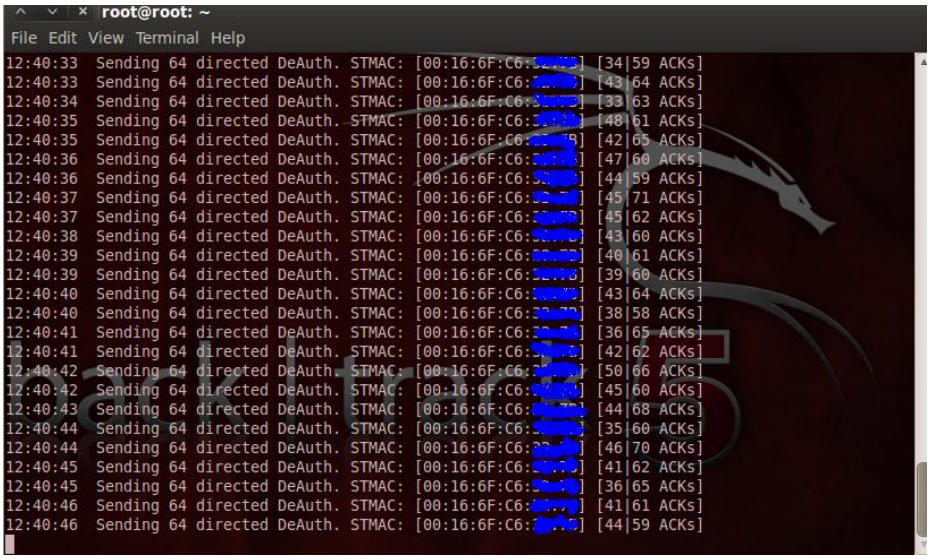


Figura 6. 53 Envío de paquetes para la respectiva desautenticación.

El usuario afectado no podrá volver a conectarse al punto de acceso inalámbrico hasta que se terminen de enviar el número de paquetes que se definió en: aireplay-ng (fue 20).

6.8.4 Ataque Para Romper Claves WPA de un Punto de Acceso Inalámbrico

Este ataque también se lo realizó con la ayuda de Backtrack 5, igual que en el ataque anterior se verificó que la interfaz de red inalámbrica esté conectada, con el comando: **iwconfig**.

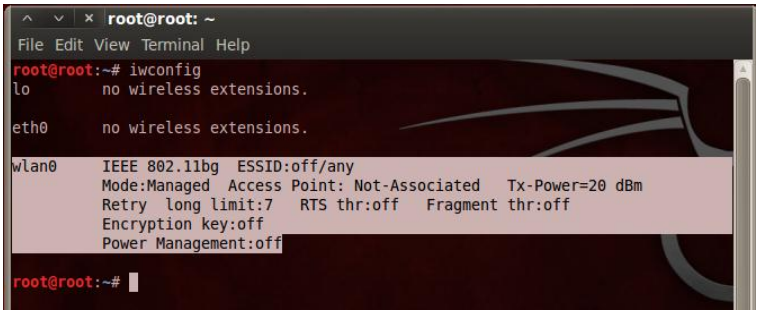


Figura 6. 54 Verificación de tarjetas inalámbricas.

También para poder ver el tráfico de red inalámbrico, se procedió a cambiar a modo monitor la tarjeta inalámbrica con el comando: **airmon-ng start wlan0 6**

El número 6 equivale al canal donde está transmitiendo el punto de acceso inalámbrico de la empresa. El identificador para la tarjeta fue **mon0**.

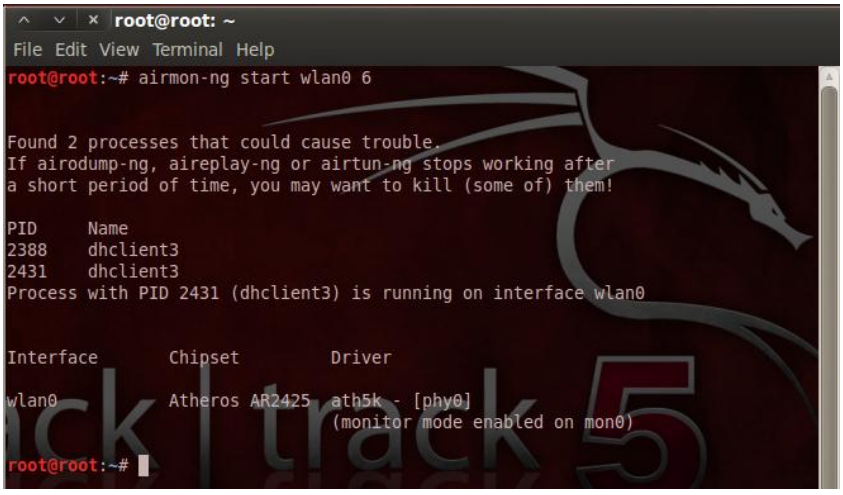


Figura 6. 55 Cambio de la tarjeta inalámbrica a modo monitor.

Seguidamente se pudo observar el tráfico por el canal 6 (el que interesaba) y se tuvo que crear un archivo llamado **handshakefile** en el cual se guardaría el contenido de la clave de autenticación (pero cifrada) que se necesita para acceder a la red mediante el punto de acceso. Se usó el siguiente comando: **airodump-ng --BSSID 00:1E:58:B1:XX:XX –w handshakefile –c 6 mon0**.

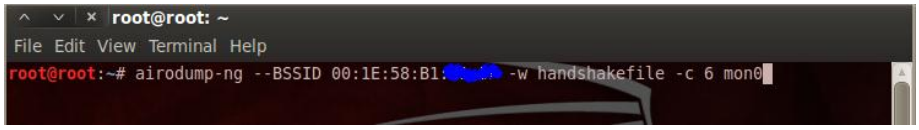


Figura 6. 56 Creación del archivo necesario para almacenar la llave de autenticación a capturar.

La siguiente pantalla muestra el tráfico solo por el canal 6, el cual es donde está transmitiendo el punto de acceso con ESSID AUTOMEKANO MT, y cuando un cliente se conectó, se capturó el archivo cifrado y lo guardó en el archivo creado anteriormente (handshakefile).

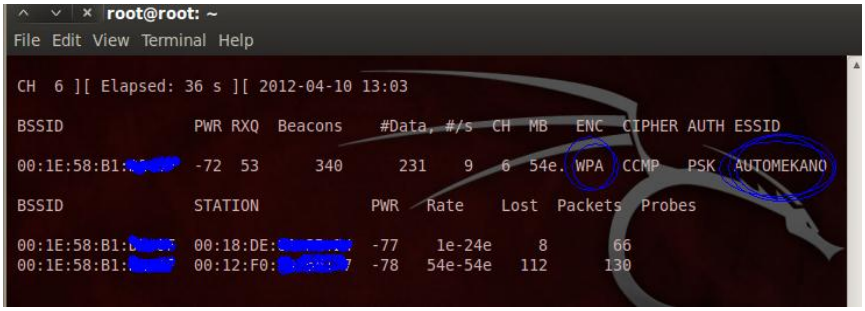


Figura 6. 57 Observación del tráfico por el canal 6.

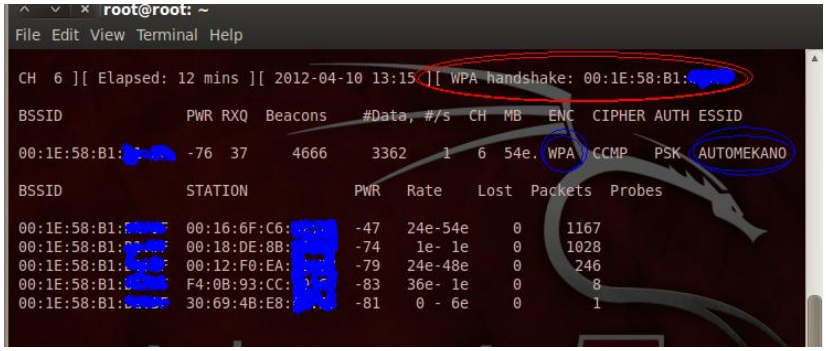


Figura 6. 58 Captura y almacenamiento de la respectiva llave de autenticación.

Finalmente se ejecutó el siguiente comando para descifrar la clave contenida en el archivo cifrado, para lo cual se usó un diccionario. El comando fue: **Aircrack-ng –w password.lst handshakefile*.cap**.

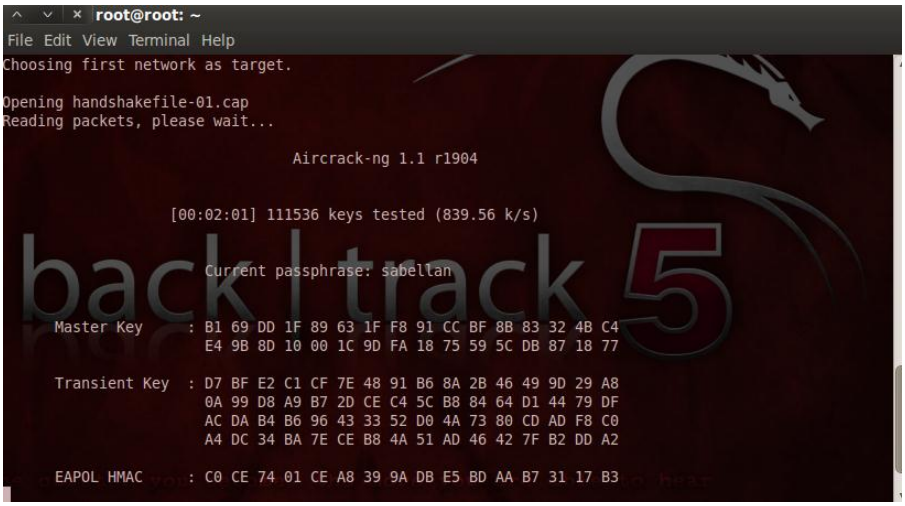


Figura 6. 59 Descifrando la contraseña almacenada en el respectivo archivo creado anteriormente.

6.8.5 Ataque de Suplantación De Identidad Remplazando La Dirección MAC de un cliente

Para poder obtener una dirección MAC de un cliente conectado a un dispositivo inalámbrico, se utilizó nuevamente la distribución Linux Backtrack 5, y lo primero que se realizó fue verificar que esté conectada la interfaz inalámbrica e iniciar el modo monitor para poder ver el tráfico inalámbrico. **Airmon-ng start wlan0**

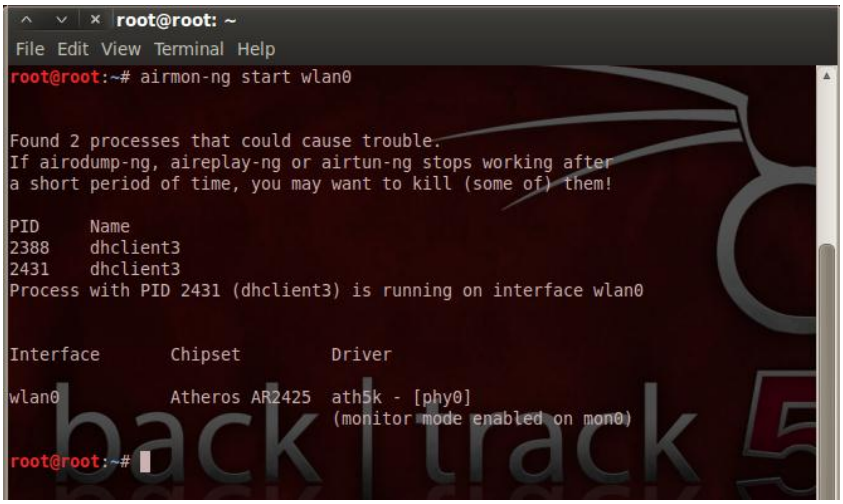


Figura 6. 60 Cambio de la tarjeta inalámbrica a modo monitor.

Luego se observó el tráfico relacionado con el dispositivo inalámbrico y se obtuvo una dirección MAC del cliente (victima). El comando utilizado: **airodump-ng mon0.**

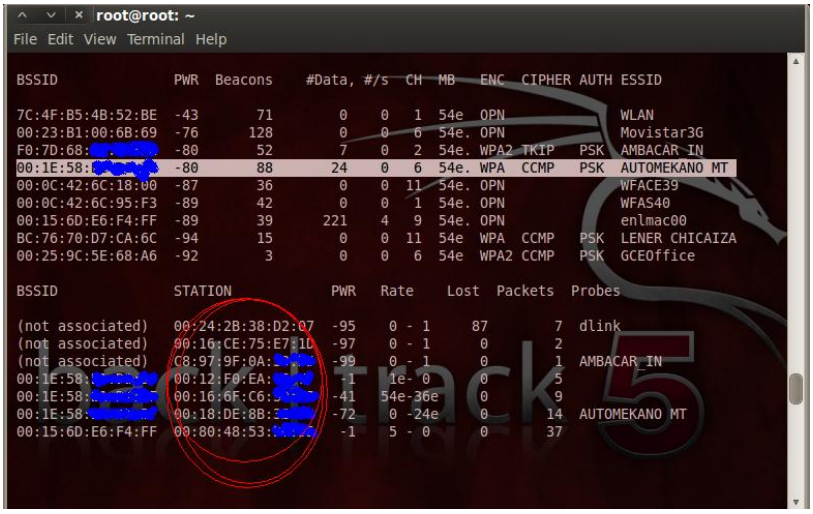


Figura 6. 61 Observación del tráfico de red para elección de una dirección MAC.

Como en un ataque anterior ya se obtuvo la contraseña para acceder a la red y ahora se obtuvo la dirección MAC de un cliente, se procedió a cambiar la dirección MAC del atacante por la dirección MAC de la víctima y así poder conectarse a la red inalámbrica (el atacante se conectó como si fuese el cliente que tiene autorización). El

cambió de la dirección MAC se lo realizó desde Windows, y el cliente con autorización se quedó sin acceso a la red inalámbrica.

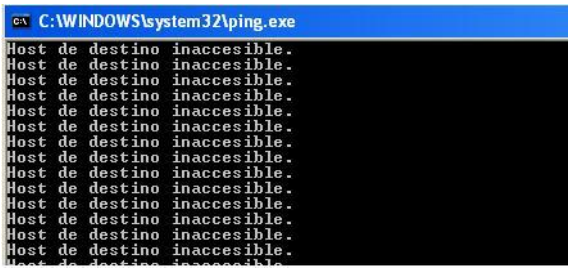


Figura 6. 62 Cliente con autorización al ser suplantada su dirección MAC se quedó sin respuesta en la red.

Las direcciones MAC del cliente con autorización y la del atacante que se utilizaron son las siguientes:

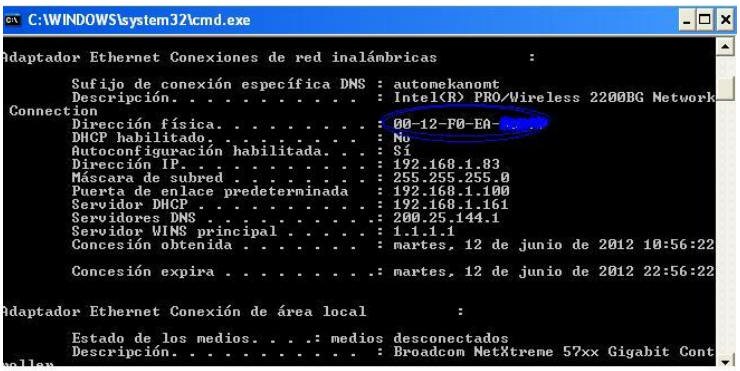


Figura 6. 63 Dirección MAC del cliente autorizado.

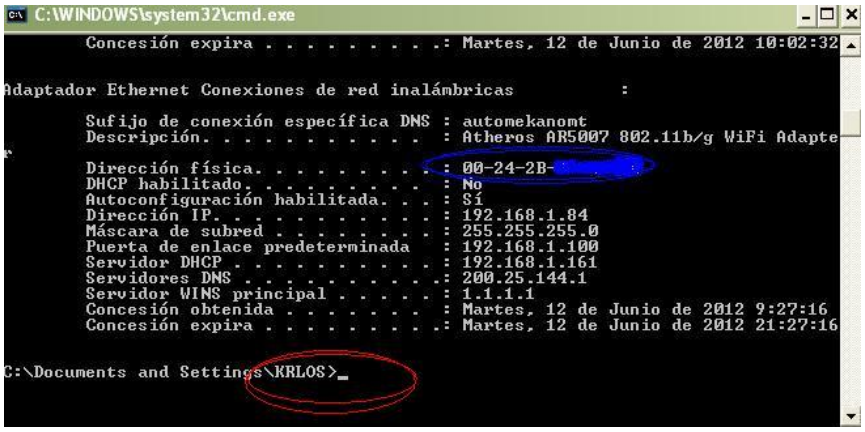


Figura 6. 64 Dirección MAC del atacante.

El programa que se usó en Windows XP para el cambio de una dirección MAC fue el Mac MakeUp, en donde primero se seleccionó el adaptador de conexión a la red inalámbrica (Atheros Wifi Adapter) y en la opción **New Address** se colocó la dirección MAC de la víctima.

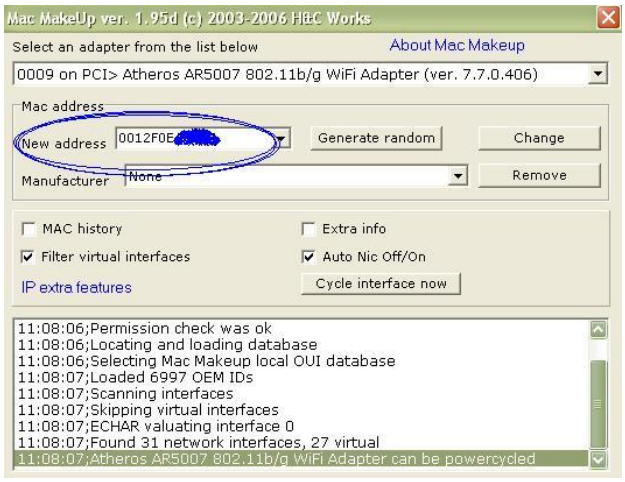


Figura 6. 65 Selección del adaptador de red y de la nueva dirección MAC.

Después se presionó el botón **change** y el programa cambió la dirección MAC (apagando y levantando la interfaz inalámbrica con la nueva dirección MAC).

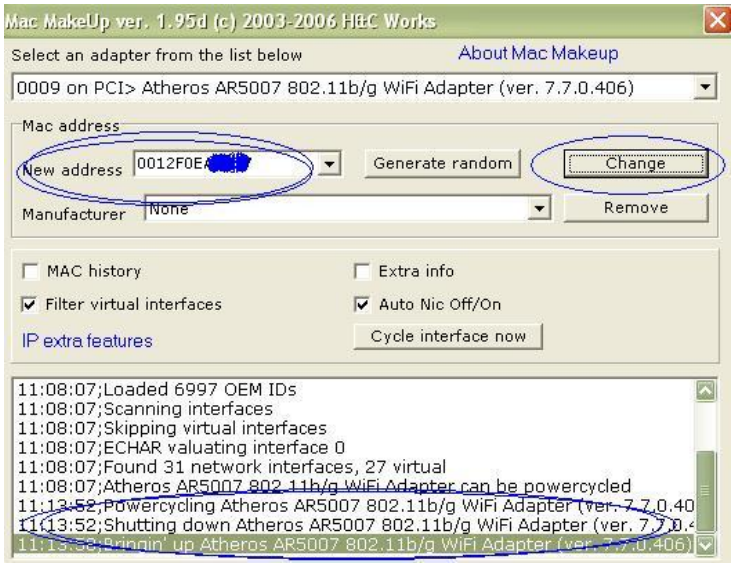


Figura 6. 66 Verificación del cambio de la dirección MAC.

Finalmente con la dirección MAC cambiada y con el conocimiento de la contraseña para acceder a la red, se procedió a conectarse a la red inalámbrica. En la línea de comandos de Windows XP se verificó la conexión. **Inicio/Ejecutar/cmd** y en la ventana se escribió: **ipconfig /all**.

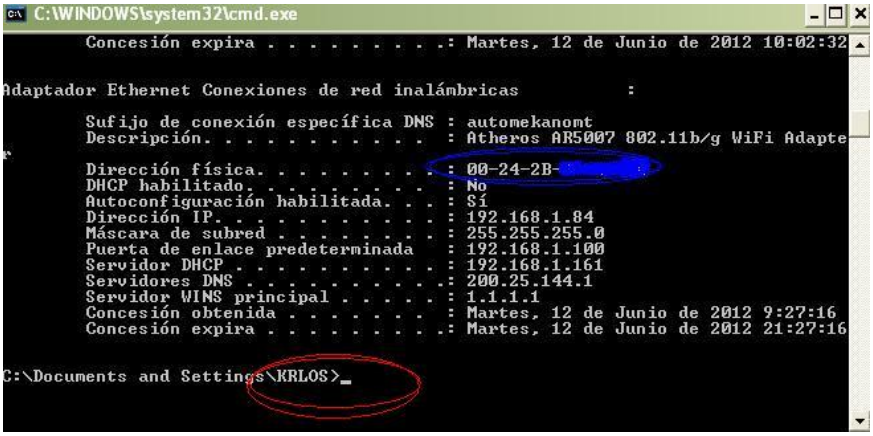


Figura 6. 67 Dirección MAC original del atacante.

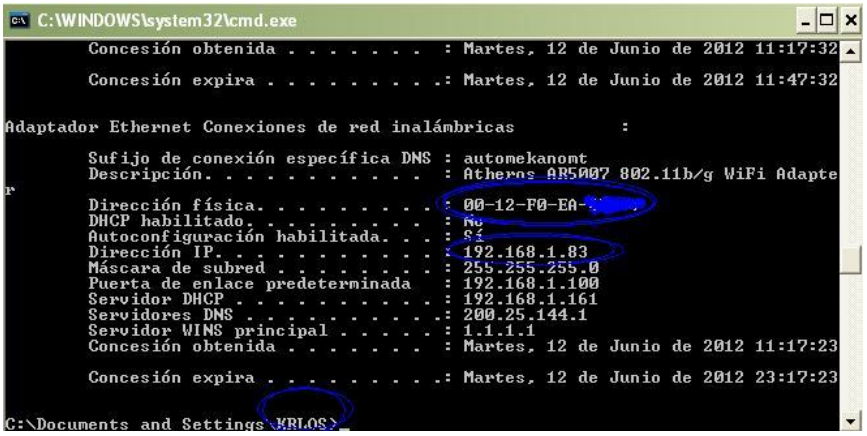


Figura 6. 68 Dirección MAC cambiada del atacante.

Si se desea volver a colocar la dirección MAC original a la computadora del atacante, en el programa **Mac MakeUp** hay que presionar un clic sobre el botón **Remove**.

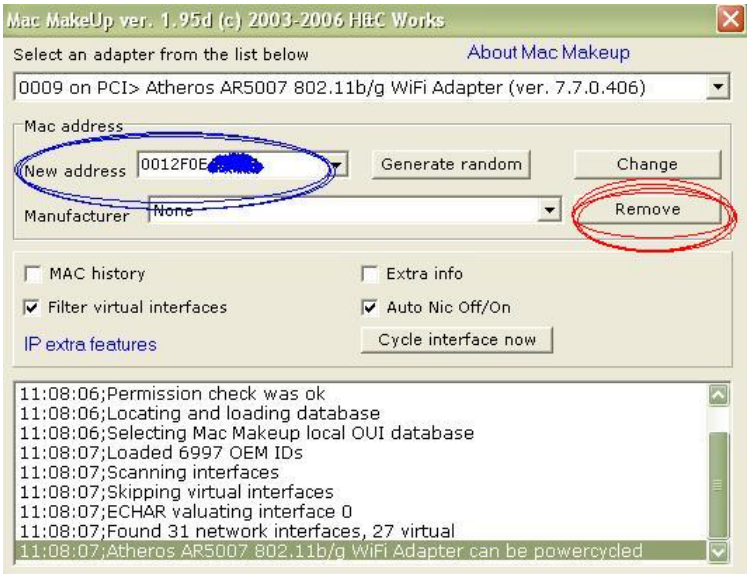


Figura 6. 69 Cambio a la dirección MAC a la original.

6.8.6 Capturar Tráfico FTP Con Wireshark y Cain

Para capturar el tráfico de la red inalámbrica, el ftp en este caso se utilizó las herramientas Wireshark y Cain (instalados en Windows XP).

Primero se debió configurar la herramienta Caín, luego de abrir la aplicación, se seleccionó la opción Configure de la barra de herramientas de Caín.

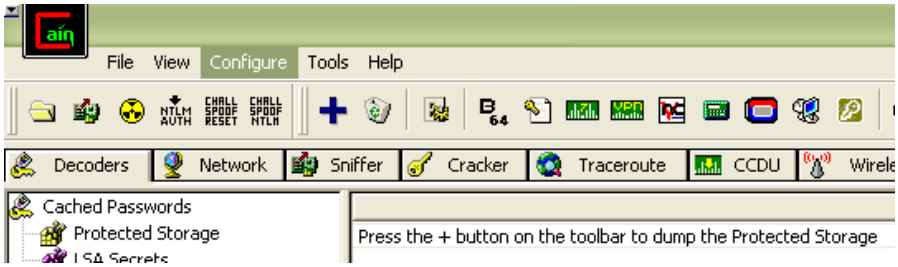


Figura 6. 70 Configuración de la herramienta Caín.

En la ventana siguiente, se escogió la opción Sniffer y se procedió a dar clic en el adaptador de red inalámbrico utilizado cuya dirección IP fue 192.168.1.117.

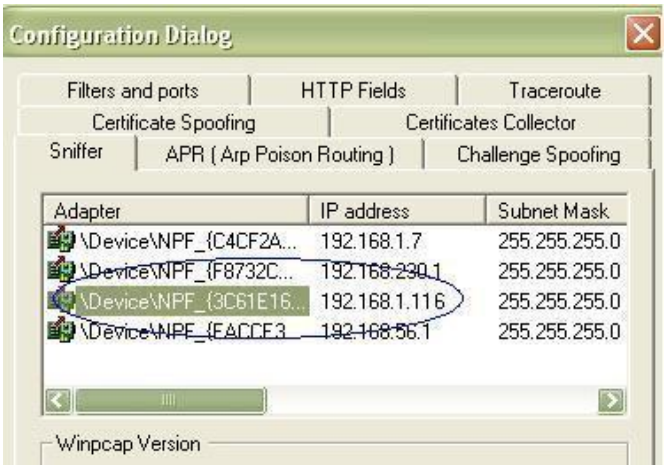


Figura 6. 71 Selección del adaptador de red a utilizar.

Posteriormente se dio inicio al Sniffer Cain como se indica en la figura.

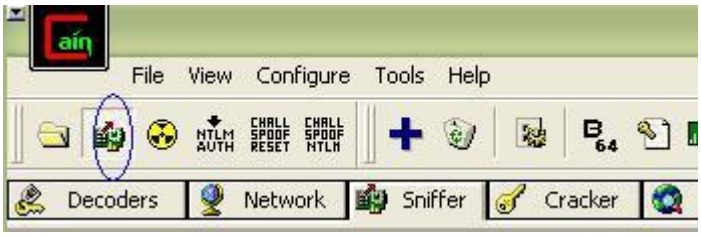


Figura 6. 72 Iniciar el sniffer Caín.

Después se obtuvo información sobre qué usuarios se encontraban conectados en ese momento. Seleccionando la opción Sniffer/Hosts/ y presionando clic derecho sobre la lista vacía de los hosts o direcciones ips y seleccionando la opción Scan MAC Addresses.

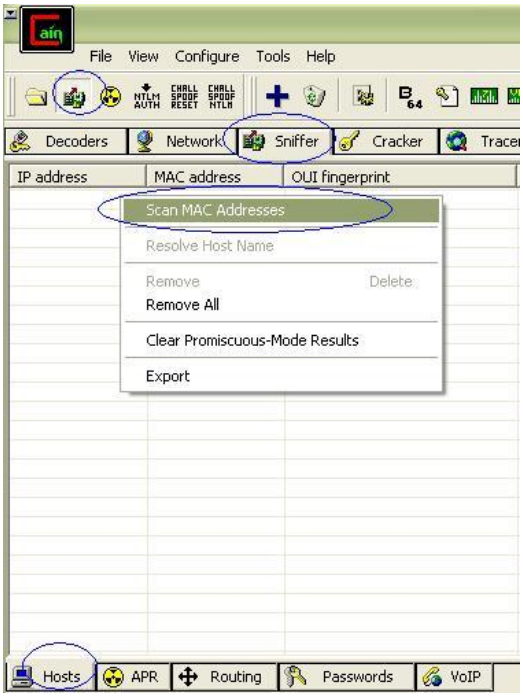


Figura 6. 73 Escaneo de las direcciones MAC conectadas y activas en la red.

Para el escaneo de los clientes conectados por medio de la herramienta Caín, existen dos formas: Rango de direcciones IP, o escanear toda la red. En este caso se realizó por medio de la segunda opción, como se muestra en la figura.

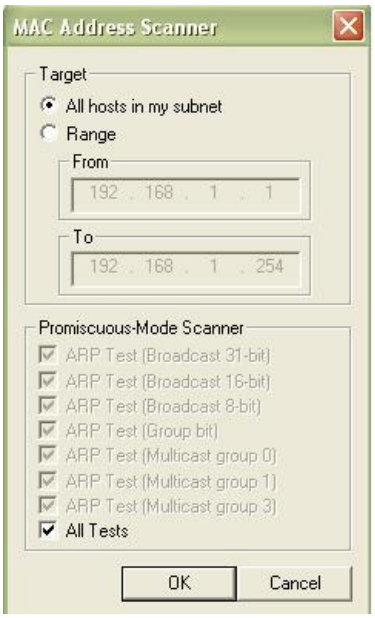


Figura 6. 74 Selección de la forma de escaneo para obtener clientes conectados a la red.

Para continuar con el ataque ARP, se procedió a la selección de las direcciones IP: víctima y servidor FTP. Con la opción Sniffer/ARP y presionando un clic sobre el símbolo + de color azul.

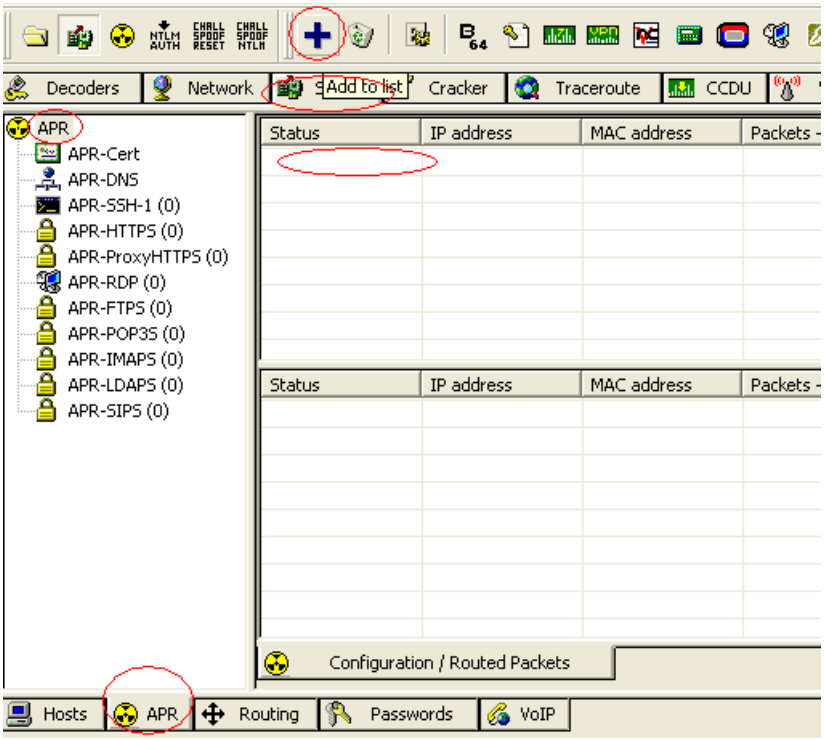


Figura 6. 75 Opción para añadir direcciones IP a la lista para ataque ARP.

En la siguiente ventana, en la parte izquierda se seleccionó la dirección IP de la víctima (192.168.1.117) y en la parte derecha la dirección IP del servidor FTP (192.168.1.105).

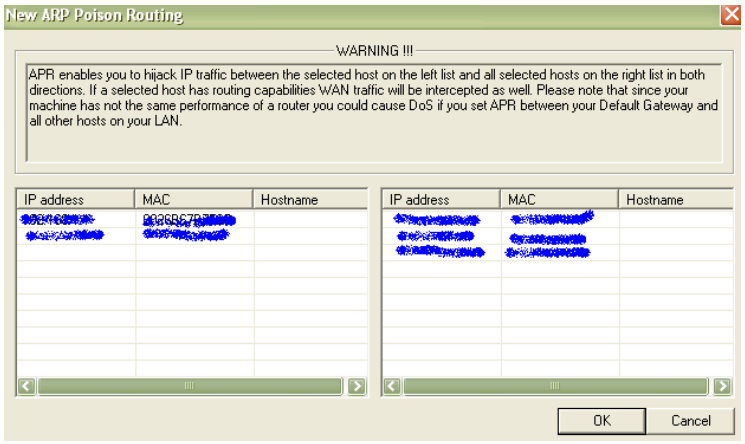


Figura 6. 76 Selección de direcciones IP víctima y del servidor FTP.

Al presionar Ok apareció la configuración anterior con las direcciones IP seleccionadas. Y se procedió a iniciar con el ataque ARP, presionando sobre la opción Start/Stop ARP.

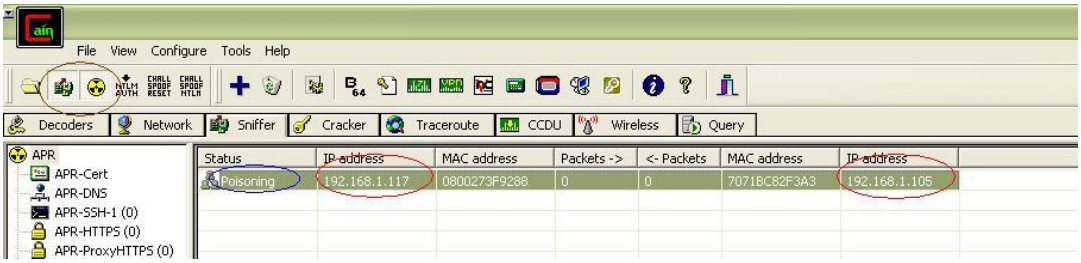


Figura 6. 77 Inicio del ataque ARP con la opción Start.

Para poder observar el tráfico, se seleccionó la opción Sniffer/Password y en este caso FTP. Y se pudo obtener el usuario y contraseña del servicio FTP.

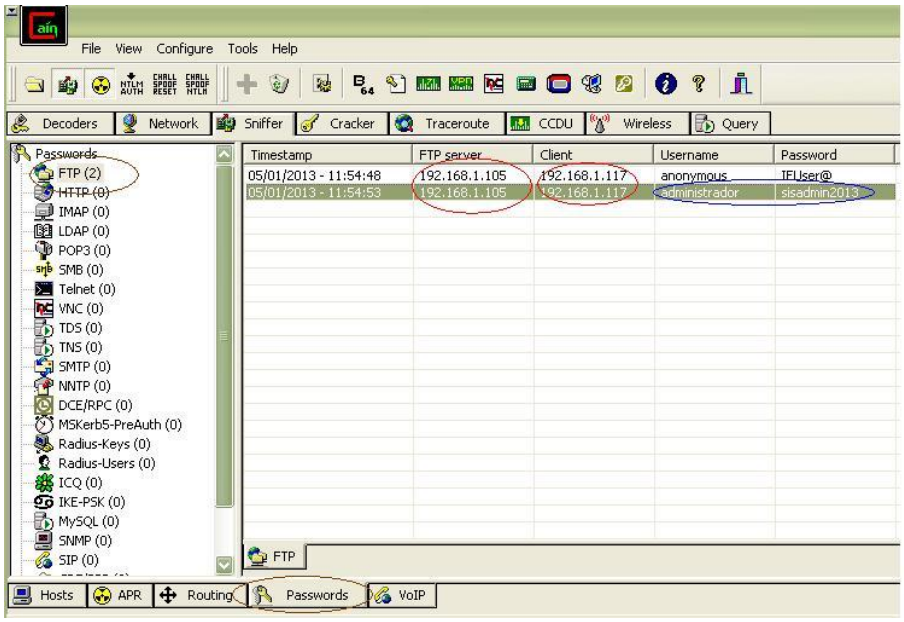


Figura 6. 78 Observación del tráfico FTP con Caín.

Para capturar de igual manera el tráfico FTP, se utilizó la herramienta Wireshark, la cual se usó conjuntamente con la aplicación Cain, para que funcione sin problemas.

Al abrir la herramienta Wireshark lo primero que se hizo fue seleccionar la opción **Capture** de la barra de herramientas y escoger: **options**.

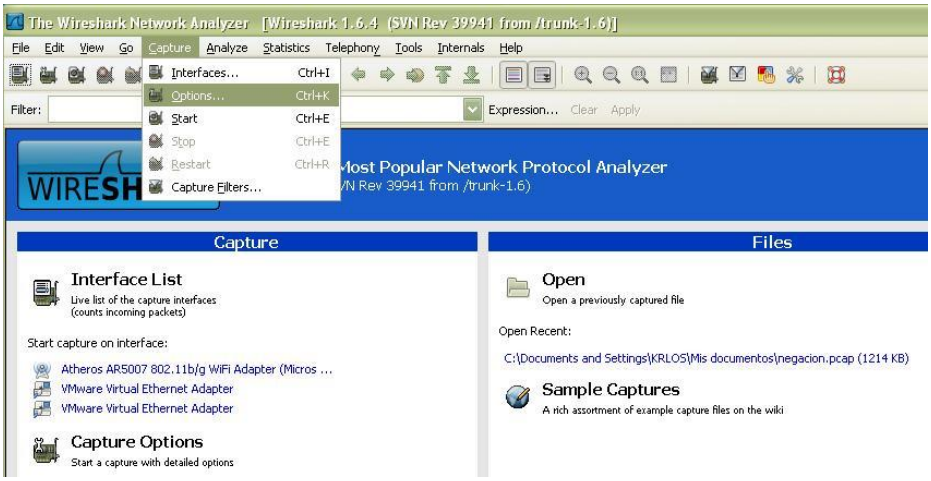


Figura 6. 79 Opciones de Captura de paquetes con Wireshark.

En la siguiente pantalla se tuvo que escoger la tarjeta de red inalámbrica a utilizar (Atheros WIFI Adapter) y quitar el visto de la opción **Capture packets in promiscuous mode** (acción a realizar porque se escogió la tarjeta inalámbrica). Posteriormente se dio un clic en el botón **start** para empezar la captura de paquetes en toda la red.

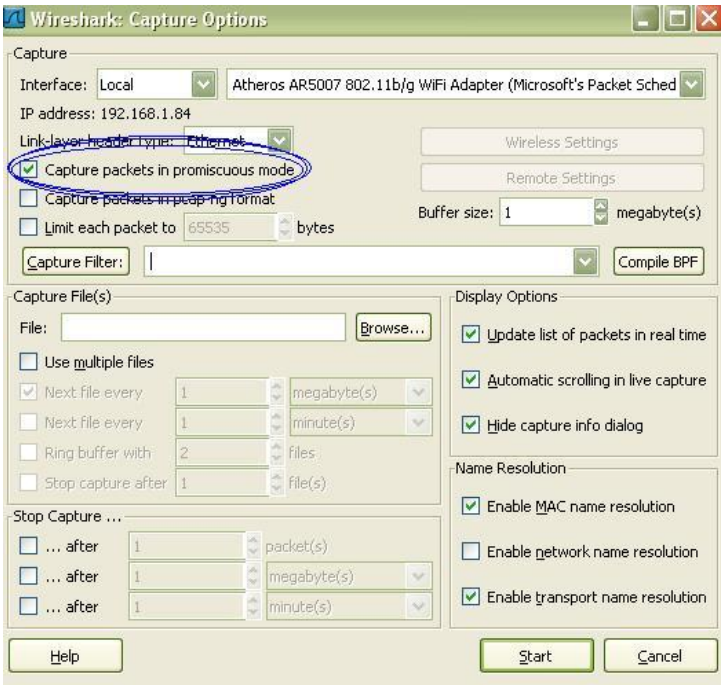


Figura 6. 80 Selección de la tarjeta inalámbrica a utilizar.

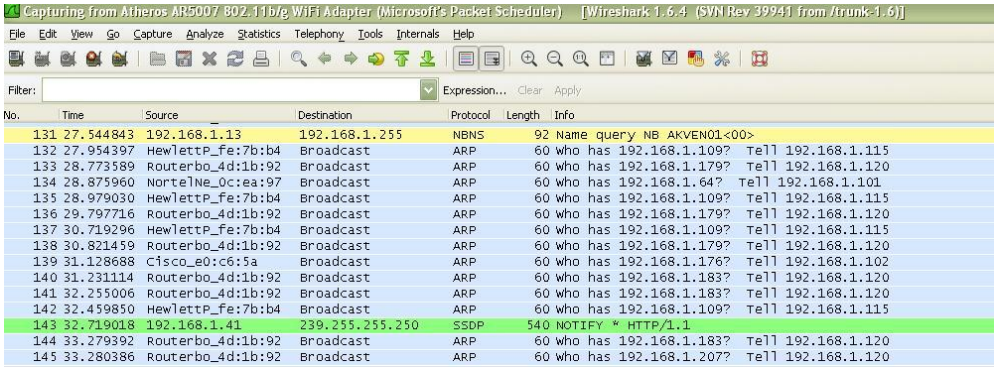


Figura 6. 81 Observación del tráfico de paquetes con Wireshark.

Por otra parte, en el lado de un cliente se procedió a la conexión ftp para abrir archivos. Se Abrió mi PC y en la barra de dirección se colocó **ftp://192.168.1.105**

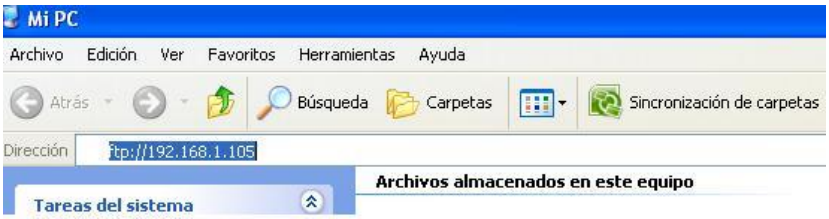


Figura 6. 82 Iniciar conexión FTP por parte del cliente.

Al presionar enter, apareció una ventana de inicio de sesión para poder acceder al servidor ftp y ver los archivos contenidos en él.

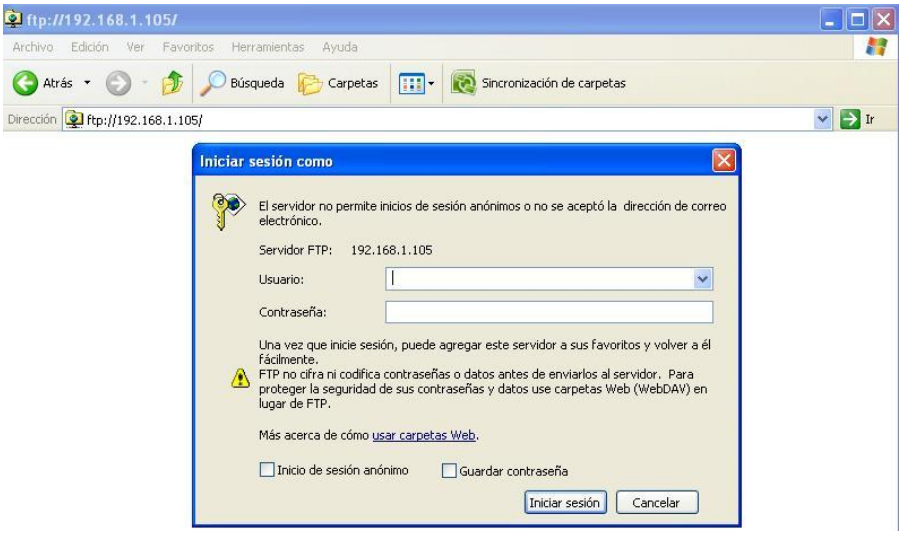


Figura 6. 83 Inicio de sesión del cliente FTP.

Se escribió el respectivo nombre de **usuario** y la **contraseña**.

Figura 6. 84 Escribir el respectivo nombre de usuario y contraseña para acceder al servicio FTP.

Al iniciar sesión se abrió la pantalla con todos los archivos contenidos por el servidor ftp. Mientras tanto en la herramienta Wireshark, en la captura que se estaba ejecutando, se procedió a buscar las capturas que se relacionen con el protocolo **ftp** y se pudo observar satisfactoriamente el usuario y contraseña del cliente ftp.

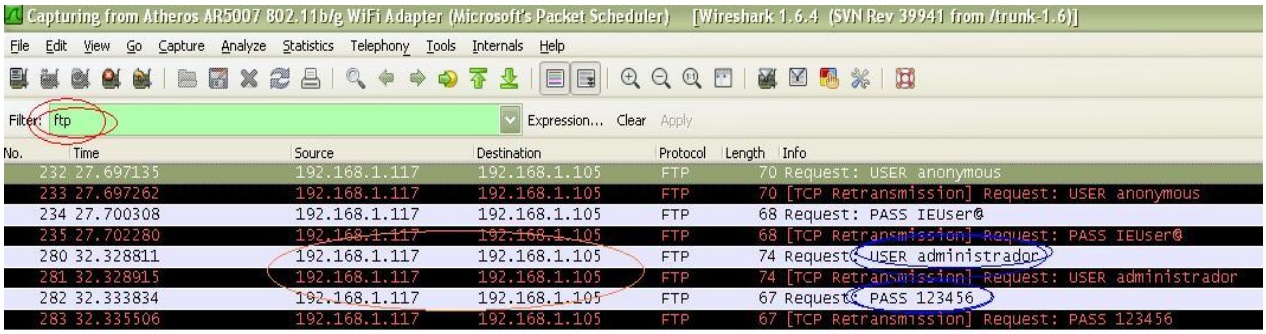


Figura 6. 85 Utilización del filtro FTP y observar el tráfico correspondiente (usuario y contraseña).

6.8.7 Tabla y Gráfica de los ataques realizados

ATAQUES REALIZADOS	Efectividad (%)
Desautenticación usuarios	100
Romper Claves WPA/WPA2 del AP	100
Suplantación de dirección MAC	100
Capturar tráfico FTP	100

Tabla 6. 1 Porcentaje de efectividad de los ataques informáticos realizados.

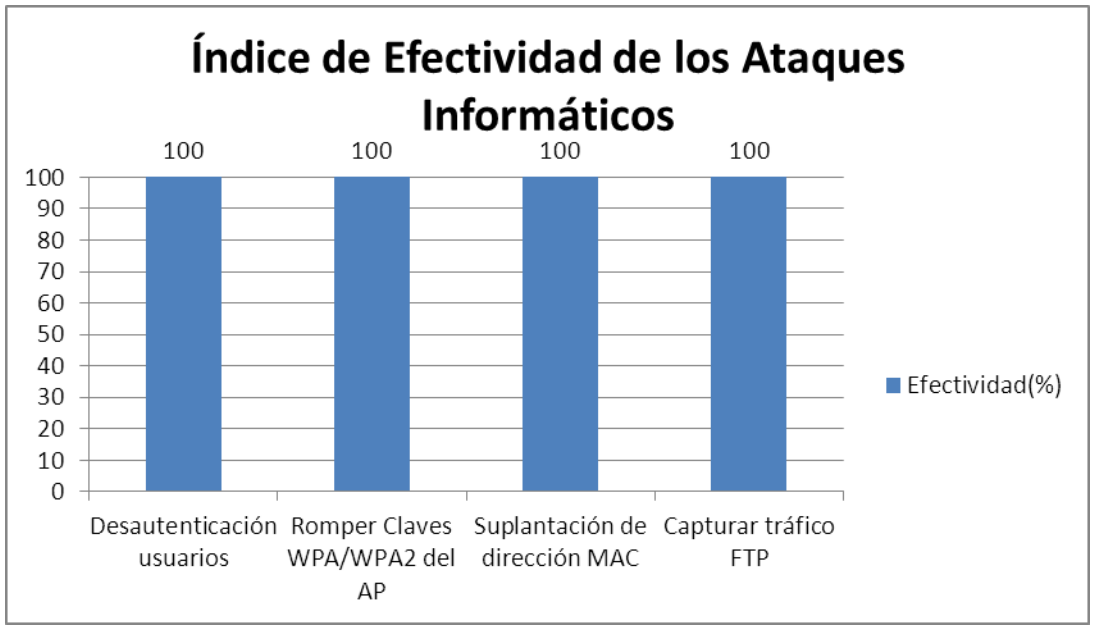


Figura 6. 86 Porcentaje de efectividad de los ataques informáticos realizados antes de la implementación de políticas de seguridad.

6.8.8 Políticas de Seguridad en la Comunicación inalámbrica de la empresa AUTOMEKANO de la Ciudad de Ambato

6.8.8.1 Alcance de las Políticas de Seguridad.

Las políticas de seguridad se aplicarán a todos los departamentos y usuarios involucrados de la empresa AUTOMEKANO Ambato.

6.8.8.2 Elaboración de las Políticas de Seguridad

1. Los servicios que presta la red inalámbrica de la empresa AUTOMEKANO son exclusivamente para uso laboral, gestiones administrativas y demás actividades que se vinculen netamente con las funciones de la empresa.

2. Los administradores de la red inalámbrica son los encargados de dar a conocer específicamente los servicios autorizados para los usuarios de la empresa AUTOMEKANO.

3. El departamento de sistemas debe realizar respaldos constantes de la información de la empresa AUTOMEKANO de los usuarios definidos como críticos.

4. Ejecutar revisiones periódicas del estado de la red inalámbrica, en el caso que existan irregularidades, se aplicarán multas y sanciones establecidas a los usuarios infractores.

5. El departamento de sistemas de la empresa debe elaborar planes de contingencia (seguridad informática) y capacitar a los usuarios sobre seguridad informática.

6. El departamento de sistemas es el encargado de la revisión, monitoreo, auditorías y análisis de vulnerabilidades de todos los equipos informáticos (Routers, Access Points, laptops, Pcs de escritorio) que acceden a la red inalámbrica.

7. Los usuarios de la red inalámbrica no deben utilizar los sistemas administrativos de la empresa donde se transmiten o reciben datos confidenciales. Sólo tienen acceso a Internet.

8. Los datos y la información manejada, procesada o almacenada por los empleados de la institución, son propiedad única y exclusiva de la empresa AUTOMEKANO.

9. Los usuarios de la empresa AUTOMEKANO son los responsables por los daños que puedan causar desde la red interna/externa a la información, o activos de cualquier naturaleza (equipos informáticos).

10. El departamento de sistemas debe revisar que los servidores de antivirus estén actualizados y sincronizados con todos los equipos hosts (computadores conectados a la red).

11. Los usuarios de la empresa AUTOMEKANO tienen la obligación de verificar que la información manejada (interna/externa) esté libre de virus, código malicioso o cualquier amenaza que afecte el funcionamiento de los equipos informáticos. En caso de que existan amenazas, notificarlo al departamento de sistemas.

12. Está prohibido el acceso a la red inalámbrica con dispositivos informáticos / electrónicos como: Smartphone, Ipad, Tablet, etc., que no sean propiedad de la empresa.

13. Los usuarios de la empresa AUTOMEKANO tendrán acceso únicamente a los datos e información que les sea útil para desarrollar sus funciones.

14. Los usuarios de la empresa AUTOMEKANO al crear o cambiar sus contraseñas de acceso a los diferentes servicios autorizados de la red, deben utilizar una longitud mínima de contraseñas que será igual a 8 caracteres (Las contraseñas estarán constituidas por la combinación de caracteres alfabéticos, especiales y números. Ejemplos: cl@v3s3gur@123, Karl@s#1890M).

15. El departamento de sistemas debe monitorear los archivos logs (registro de eventos) de enrutadores, puntos de acceso, conmutadores, entre otros.

16. Los usuarios de la empresa AUTOMEKANO tienen la obligación de cambiar todas sus contraseñas de acceso a los diferentes servicios autorizados de la red de la empresa cada 30 días.

17. Si el usuario no desea cambiar totalmente sus contraseñas, podrá optar por reemplazar las letras con cualquier caracter especial. Ejemplo: a por @, e por el número 3, i por ¡ ó por !, etc. Ejemplo: reemplazar clave123 por cl@v3123.

18. Los usuarios de la empresa AUTOMEKANO no deben revelar bajo ningún concepto su contraseña a otra persona, ni mantenerla escrita a la vista o alcance de terceros.

19. El departamento de sistemas debe cumplir y hacer cumplir las políticas de seguridad de la red inalámbrica establecidas.

20. Los usuarios de la empresa AUTOMEKANO bajo ningún motivo deben usar los nombres de usuario y contraseñas de otros usuarios.

21. Los usuarios de la empresa AUTOMEKANO no pueden instalar software que no esté autorizado por la empresa.

22. El departamento de sistemas debe desarrollar aplicaciones de usuario aplicando las respectivas seguridades informáticas.

23. Los administradores de la red inalámbrica tienen que configurar el ESSID (nombre que identifica a la red inalámbrica) de los equipos inalámbricos de tal manera que no contengan información relacionada o que identifique a la empresa AUTOMEKANO.

24. Los administradores de la red inalámbrica tienen la obligación de actualizar los firmwares (aplicación que controla los circuitos electrónicos) de hardware y así cubrir todas las posibles brechas de seguridad.

25. Los administradores de la red inalámbrica deben desactivar los paquetes (beacons) que emiten los equipos inalámbricos, y así no dar a notar su presencia a posibles intrusos.

26. Los administradores de la red inalámbrica tienen que registrar las direcciones MAC de los computadores de los usuarios seleccionados y activar el servicio DHCP de los puntos de acceso (AP) con el necesario rango de direcciones IP.

27. En caso de que no se requiera el uso de la red inalámbrica, el departamento de sistemas debe apagar los equipos inalámbricos.

28. Los usuarios de la red inalámbrica deben ser creados por el departamento de sistemas a través de un sistema centralizado. Ejemplo: un sistema de manejo de usuarios y contraseñas.

29. El departamento de sistemas debe crear contraseñas más complejas para los enrutadores (Routers), switch, puntos de acceso (AP), entre otros, y cambiarlas cada 60 días.

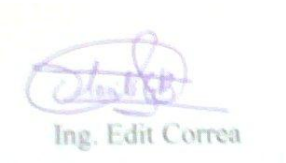
6.8.8.3 Aprobación de las Políticas de Seguridad

Ambato, 12 de octubre del 2012

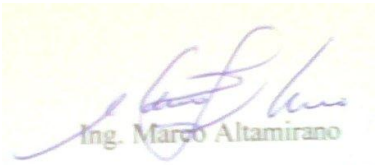
APROBACIÓN DE DOCUMENTOS

De acuerdo al documento elaborado por el señor Carlos Ismael Carrillo Miranda, titulado: "POLÍTICAS DE SEGURIDAD EN LA COMUNICACIÓN INALÁMBRICA DE LA EMPRESA AUTOMEKANO DE LA CIUDAD DE AMBATO" y a la respectiva revisión del mismo, se procede a informar que la aprobación de dicho documento es totalmente concedida para los fines respectivos.

FIRMAS DE AUTORIZACIÓN



Ing. Edit Correa
Dpto. de Sistemas AUTOMEKANO



Ing. Marco Altamirano
Dpto. de Sistemas AUTOMEKANO

6.8.8.4 Implementación de las Políticas de Seguridad

Se emitió un comunicado mediante correo electrónico a todos los usuarios involucrados (usuarios inalámbricos) de la empresa AUTOMEKANO manifestándoles sobre la creación, aprobación de políticas de seguridad para la comunicación inalámbrica de la empresa; indicando además la fecha desde cuándo éstas políticas se hacen efectivas.

6.8.8.5 Excepciones de las Políticas de Seguridad Implementadas

- Todas las políticas implementadas serán cumplidas por todos los empleados, usuarios y directivos de la empresa AUTOMEKANO.

- Se reconoce que en circunstancias poco usuales, algunos empleados y usuarios de la empresa necesitarán emplear sistemas o aplicaciones que no estén conformes con estas políticas. Todos esos casos deben ser autorizados por escrito y con previa solicitud dirigida a la Gerencia General de la empresa AUTOMEKANO indicando la razón y el tiempo que se aplicará a la excepción.

6.8.9 Pruebas realizadas después de la Implementación de las Políticas de Seguridad.

Después de concluir con la implementación de las políticas de seguridad, se realizaron las siguientes pruebas, con el fin de constatar la reducción de amenazas informáticas en la comunicación inalámbrica de la empresa AUTOMEKANO.

6.8.7.1 Ataque De Negación De Servicio

Para efectuar este ataque, lo primero que se realizó fue arrancar la distribución Linux Backtrack 5 con un live CD.

Una vez dentro de Backtrack 5, el siguiente paso fue verificar si está conectada la tarjeta inalámbrica y que nombre la identificaba, para lo cual se abrió una ventana de comandos y se procedió a escribir: **iwconfig**.

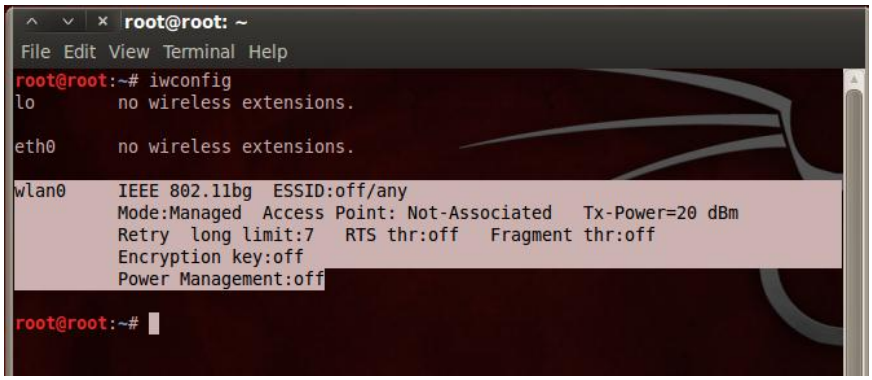


Figura 6. 87 Verificación de tarjetas inalámbricas.

Cuando ya fue identificada la tarjeta inalámbrica se procedió a cambiarla a modo monitor (para escuchar el tráfico de la red), con el comando: **airmon-ng start wlan0**.

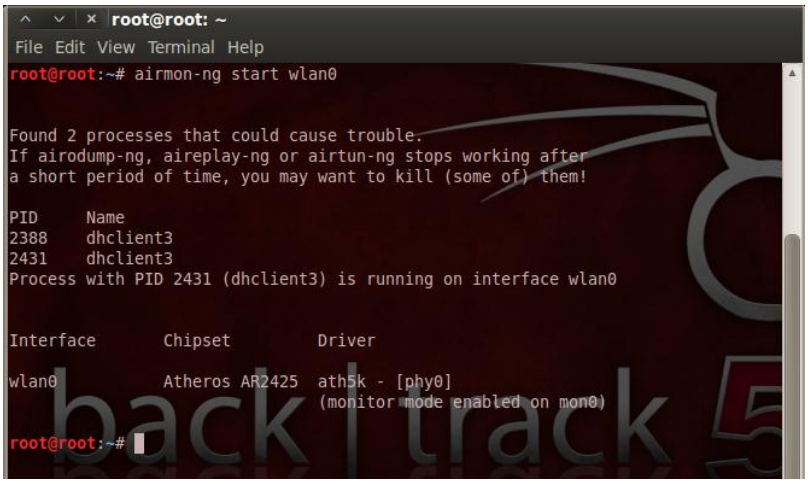


Figura 6. 88 Cambio de la tarjeta inalámbrica a modo monitor.

El identificador que fue asignado a la tarjeta inalámbrica para modo monitor fue: **mon0**, luego para observar todo el tráfico de la red se usó el siguiente comando: **airodump-ng mon0**. Y por consiguiente se pudo obtener información vital como son las direcciones MAC de los puntos de acceso (AP) a redes inalámbricas y de los clientes inalámbricos; el tipo de encriptación del dispositivo; el ESSID; el canal por el cual transmite el dispositivo inalámbrico; entre otros.

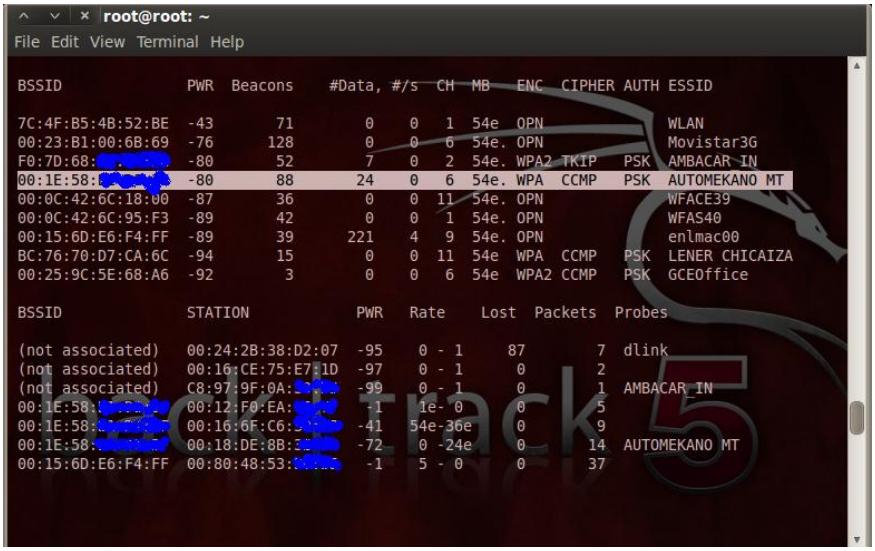


Figura 6. 89 Observación del tráfico de red.

Para concretar con el ataque se necesitó las direcciones MAC del punto de acceso cuyo ESSID es AUTOMEKANO MT y de un cliente conectado al mismo. Se usó el siguiente comando: **aireplay-ng -0 20 –a 00:1E:58:XX:XX:XX –c 00:16:6F:C6:XX:XX mon0**.

Figura 6. 90 Ejecutando el ataque de desautenticación de un usuario.

Después de ejecutar el comando anterior, se empezó a mandar paquetes para la respectiva desautenticación a dicho usuario.

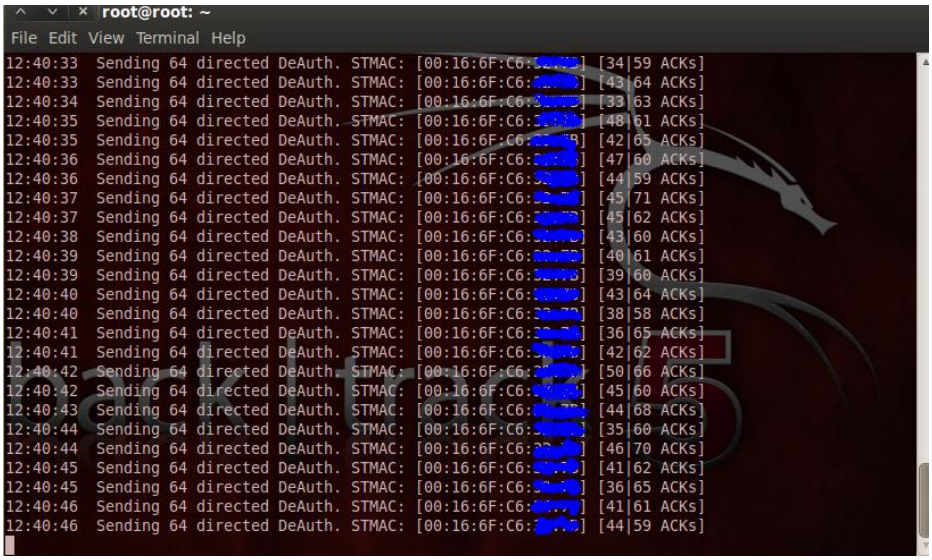


Figura 6. 91 Envío de paquetes para la respectiva desautenticación.

El usuario afectado no podrá volver a conectarse al punto de acceso inalámbrico hasta que se terminen de enviar el número de paquetes que se definió en: aireplay-ng (fue 20).

6.8.7.2 Ataque Para Romper Claves WPA de un Punto de Acceso Inalámbrico

Este ataque también se lo realizó con la ayuda de Backtrack 5, igual que en el ataque anterior se verificó que la interfaz de red inalámbrica esté conectada, con el comando: **iwconfig**.

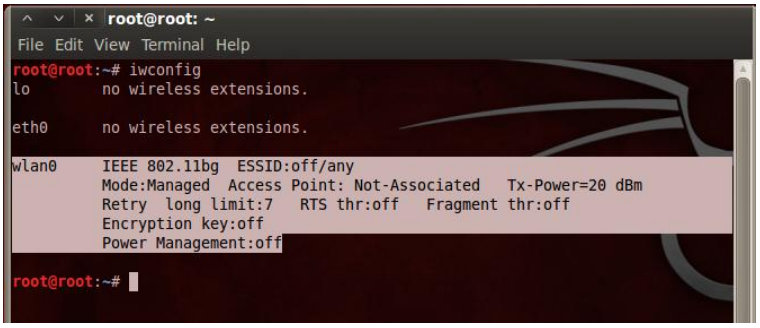


Figura 6. 92 Verificación de tarjetas inalámbricas.

También para poder ver el tráfico de red inalámbrico, se procedió a cambiar a modo monitor la tarjeta inalámbrica con el comando: **airmon-ng start wlan0 6**
El número 6 equivale al canal donde está transmitiendo el punto de acceso inalámbrico de la empresa. El identificador para la tarjeta fue **mon0**.

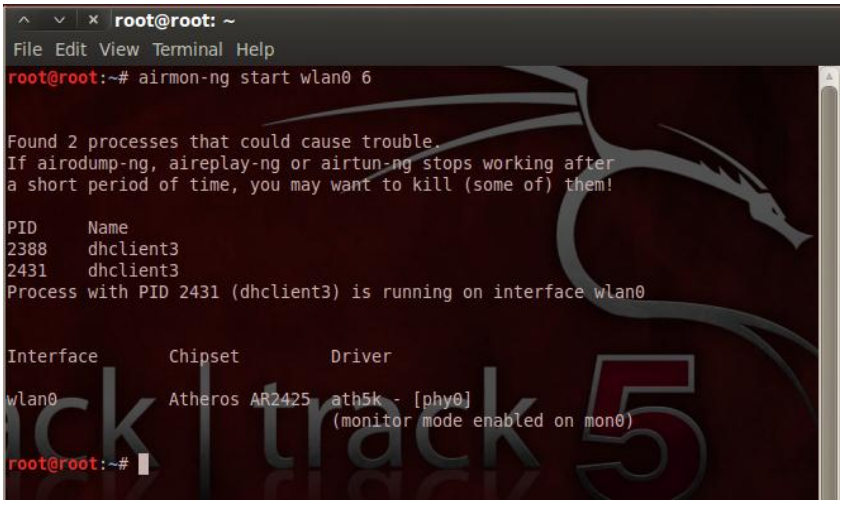


Figura 6. 93 Cambio de la tarjeta inalámbrica a modo monitor.

Seguidamente se pudo observar el tráfico por el canal 6 (el que interesaba) y se tuvo que crear un archivo llamado **handshakefile** en el cual se guardaría el contenido de la clave de autenticación (pero cifrada) que se necesita para acceder a la red mediante el punto de acceso. Se usó el siguiente comando: **airodump-ng --BSSID 00:1E:58:B1:XX:XX –w handshakefile –c 6 mon0**.

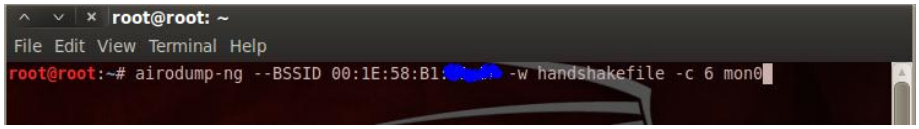


Figura 6. 94 Creación del archivo necesario para almacenar la llave de autenticación a capturar.

La siguiente pantalla muestra el tráfico solo por el canal 6, el cual es donde está transmitiendo el punto de acceso con ESSID AUTOMEKANO MT, y cuando un cliente se conectó, se capturó el archivo cifrado y lo guardó en el archivo creado anteriormente (handshakefile).

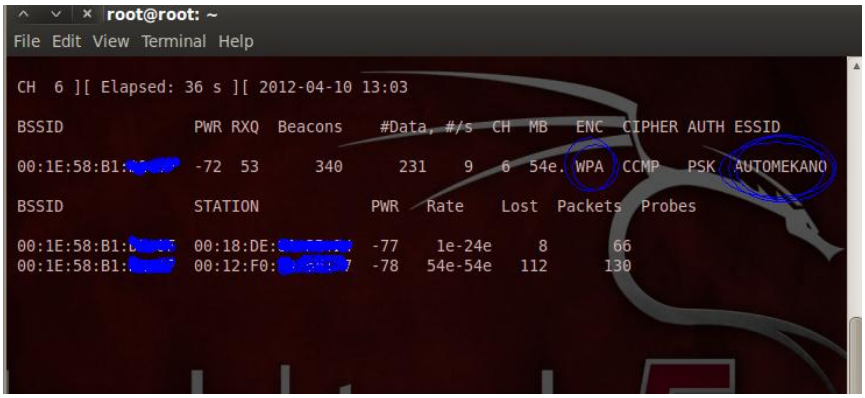


Figura 6. 95 Observación del tráfico por el canal 6.

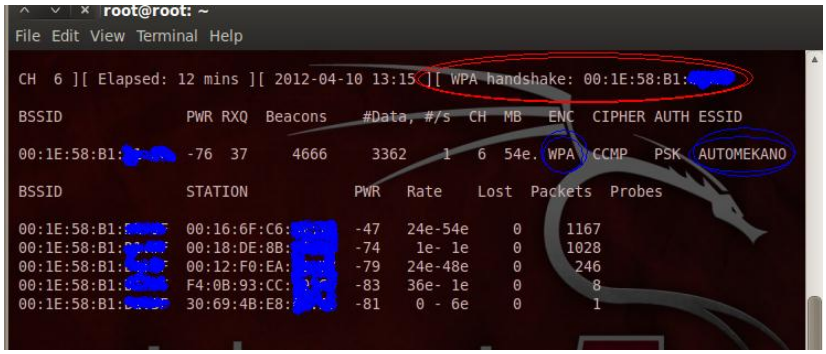


Figura 6. 96 Captura y almacenamiento de la respectiva llave de autenticación.

Debido a que se cambió y se reforzó la contraseña del punto de acceso, no se la pudo descifrar, ya que pasó demasiado tiempo en el análisis.

6.8.7.3 Suplantación De Identidad Remplazando La Dirección MAC de un cliente

Para poder obtener una dirección MAC de un cliente conectado a un dispositivo inalámbrico, se utilizó nuevamente la herramienta Backtrack 5, y lo primero que se realizó fue verificar que esté conectada la interfaz inalámbrica e iniciar el modo monitor para poder ver el tráfico inalámbrico. **Airmon-ng start wlan0**

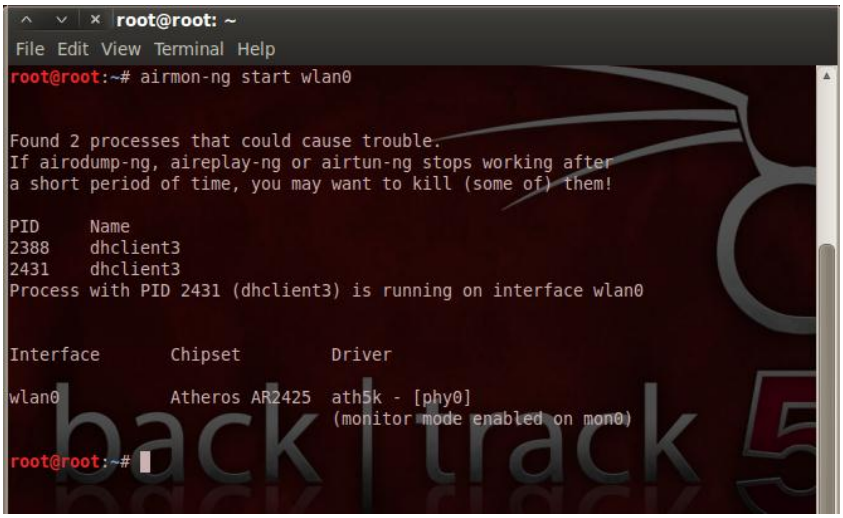


Figura 6. 97 Cambio de la tarjeta inalámbrica a modo monitor.

Luego se observó el tráfico relacionado con el dispositivo inalámbrico y se obtuvo una dirección MAC del cliente (victima). El comando utilizado: **airodump-ng mon0.**

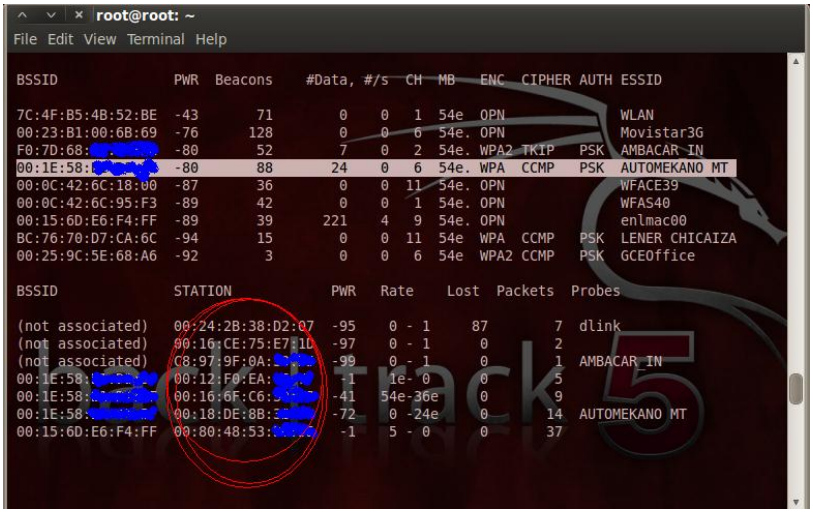


Figura 6. 98 Observación del tráfico de red para elección de una dirección MAC.

Como en el ataque anterior no se pudo obtener la contraseña para acceder a la red, éste ataque se lo efectuó de forma interna (ya conectado a la red). Se procedió a cambiar la dirección MAC del atacante por la dirección MAC de la víctima. El cambió de la dirección MAC se lo realizó desde Windows, y el cliente con autorización se quedó sin acceso a la red inalámbrica.

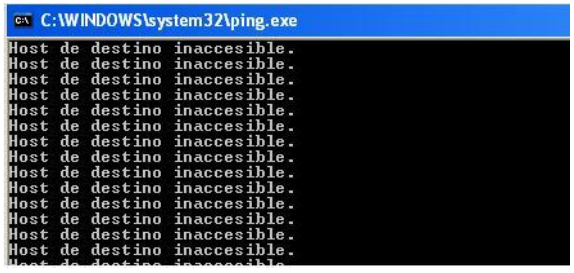


Figura 6. 99 Cliente con autorización al ser suplantada su dirección MAC se quedó sin respuesta en la red.

Las direcciones MAC del cliente con autorización y la del atacante que se utilizaron son las siguientes:

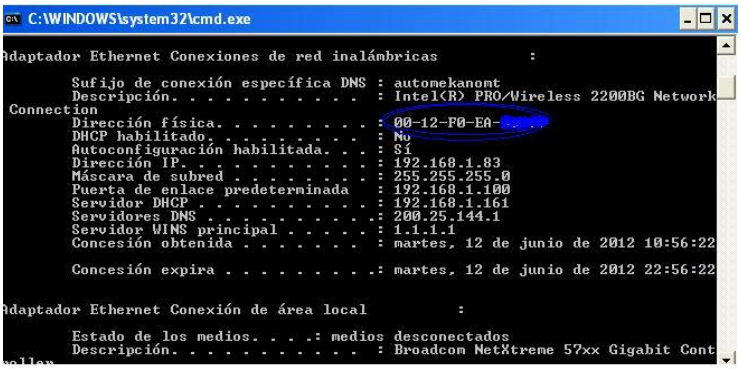


Figura 6. 100 Dirección MAC del cliente autorizado.

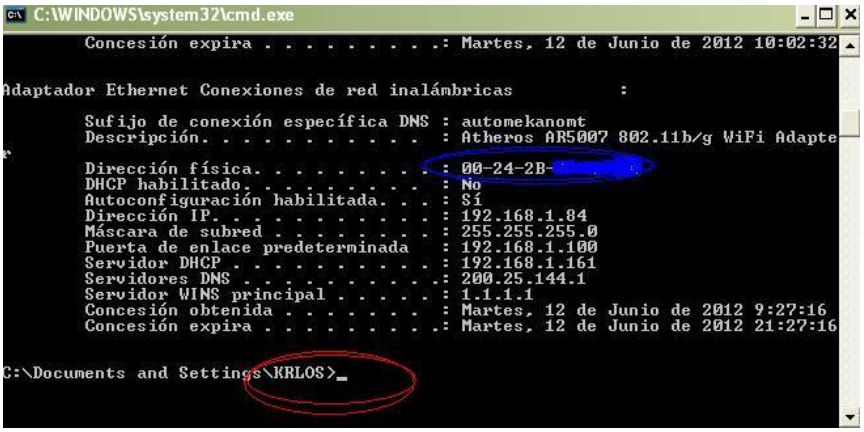


Figura 6. 101 Dirección MAC del atacante.

El programa que se usó en Windows XP para el cambio de una dirección MAC fue el Mac MakeUp, en donde primero se seleccionó el adapatador de conexión a la red inalámbrica (Atheros Wifi Adapter) y en la opción **New Address** se colocó la dirección MAC de la víctima.

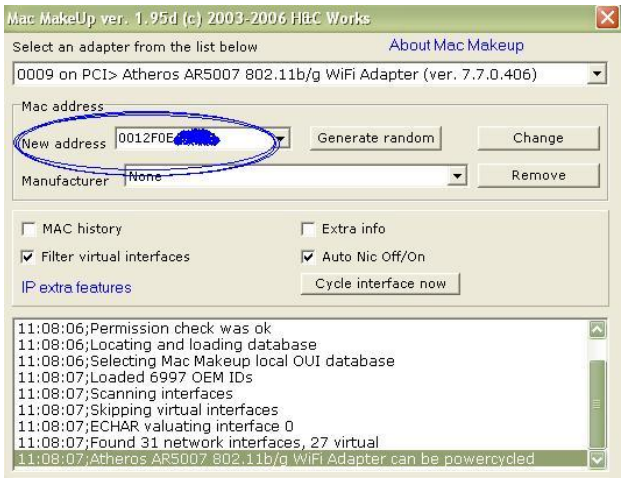


Figura 6. 102 Selección del adaptador de red y de la nueva dirección MAC.

Después se presionó el botón **change** y el programa cambió la dirección MAC (apagando y levantando la interfaz inalámbrica con la nueva dirección MAC).

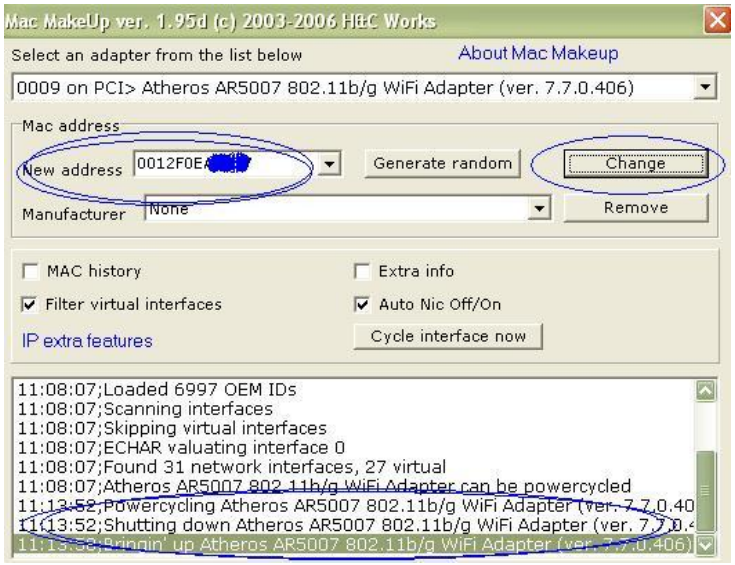


Figura 6. 103 Verificación del cambio de la dirección MAC.

Finalmente con la dirección MAC cambiada y con el conocimiento de la contraseña para acceder a la red, se procedió a conectarse a la red inalámbrica. En la línea de comandos de Windows XP se verificó la conexión. **Inicio/Ejecutar/cmd** y en la ventana se escribió: **ipconfig /all**.

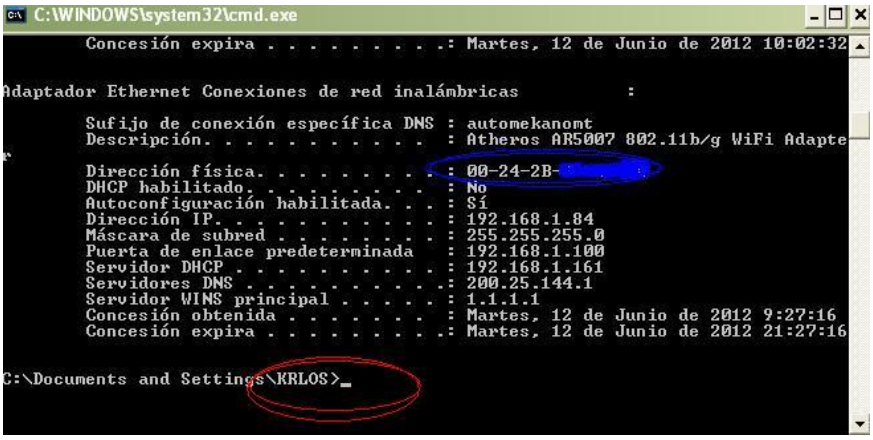


Figura 6. 104 Dirección MAC original del atacante.

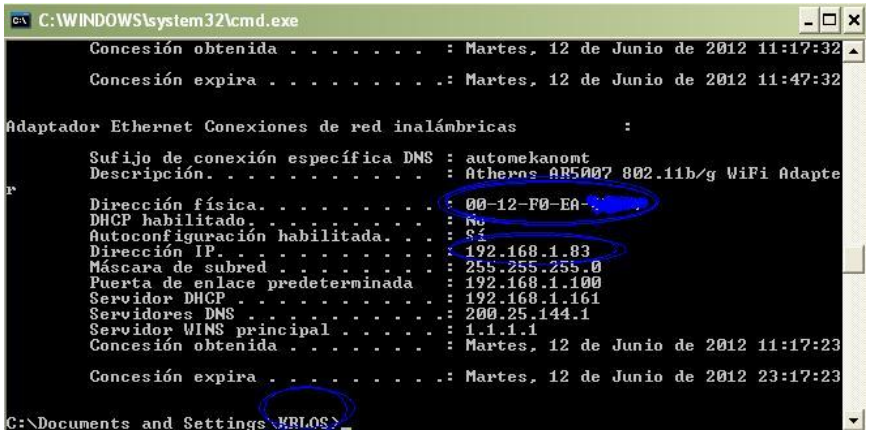


Figura 6. 105 Dirección MAC cambiada del atacante.

Si se desea volver a colocar la dirección MAC original a la computadora del atacante, en el programa **Mac MakeUp** hay que presionar un clic sobre el botón **Remove**.

Figura 6. 106 Cambio a la dirección MAC a la original.

6.8.7.4 Capturar Tráfico FTP Con Wireshark y Cain

Para capturar el tráfico de la red inalámbrica, el ftp en este caso se utilizó las herramientas Wireshark y Cain (instalados en Windows XP).

Primero se debió configurar la herramienta Cain, luego de abrir la aplicación, se seleccionó la opción Configure de la barra de herramientas de Cain.

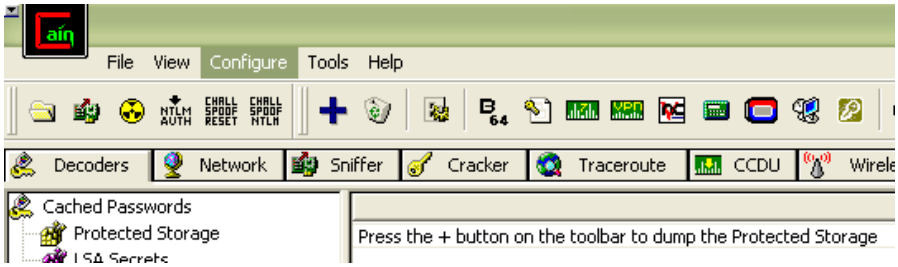


Figura 6. 107 Configuración de la herramienta Caín.

En la ventana siguiente, se escogió la opción Sniffer y se procedió a dar clic en el adaptador de red inalámbrico utilizado cuya dirección IP fue 192.168.1.117.

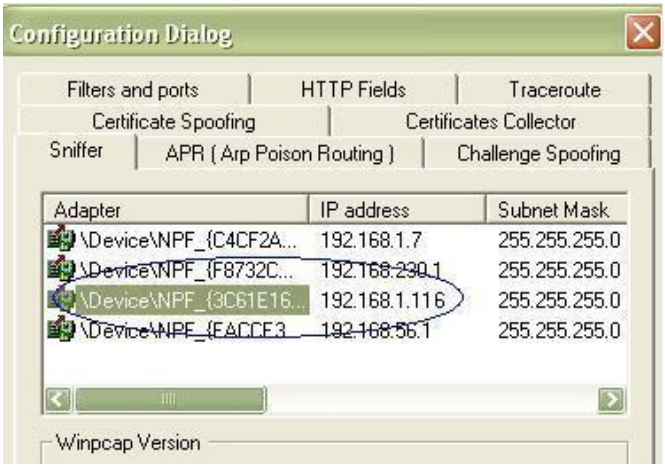


Figura 6. 108 Selección del adaptador de red a utilizar.

Posteriormente se dio inicio al Sniffer Cain como se indica en la figura.

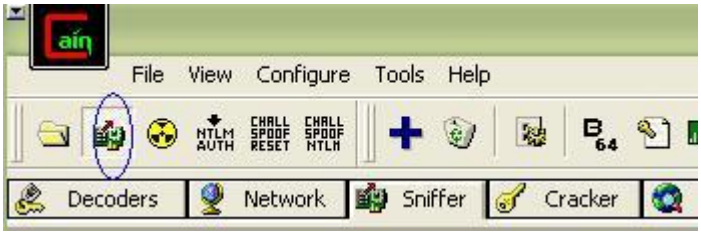


Figura 6. 109 Iniciar el sniffer Caín.

Después se obtuvo información sobre qué usuarios se encontraban conectados en ese momento. Seleccionando la opción Sniffer/Hosts/ y presionando clic derecho sobre la lista vacía de los hosts o direcciones IP y seleccionando la opción Scan MAC Addresses.

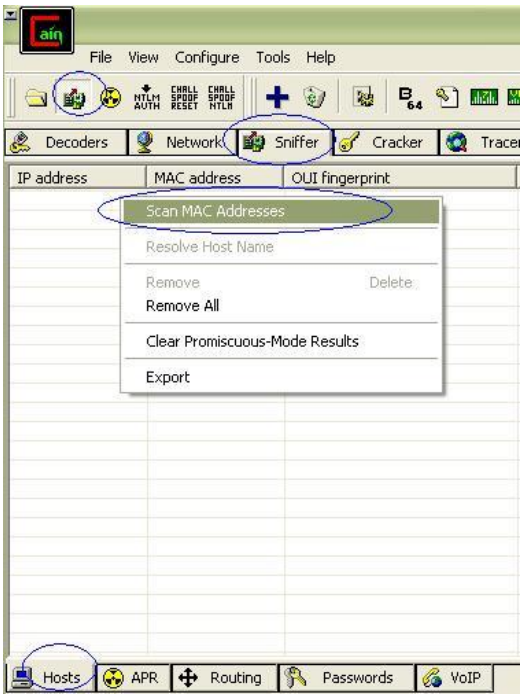


Figura 6. 110 Escaneo de las direcciones MAC conectadas y activas en la red.

Para el escaneo de los clientes conectados por medio de la herramienta Cain, existen dos formas: Rango de direcciones Ip, o escanear toda la red. En este caso se realizó por medio de la segunda opción, como se muestra en la figura.

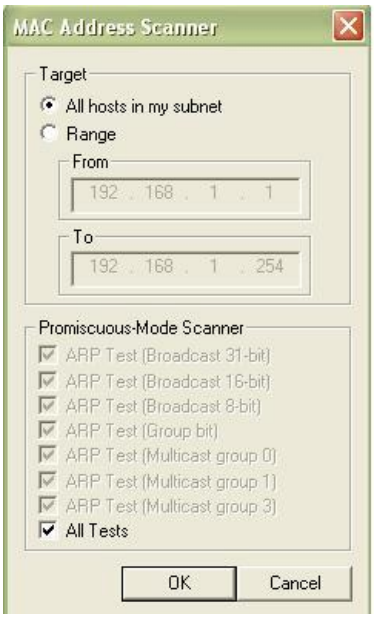


Figura 6. 111 Selección de la forma de escaneo para obtener clientes conectados a la red.

Para continuar con el ataque ARP, se procedió a la selección de las direcciones IP: víctima y servidor FTP. Con la opción Sniffer/ARP y presionando un clic sobre el símbolo + de color azul.

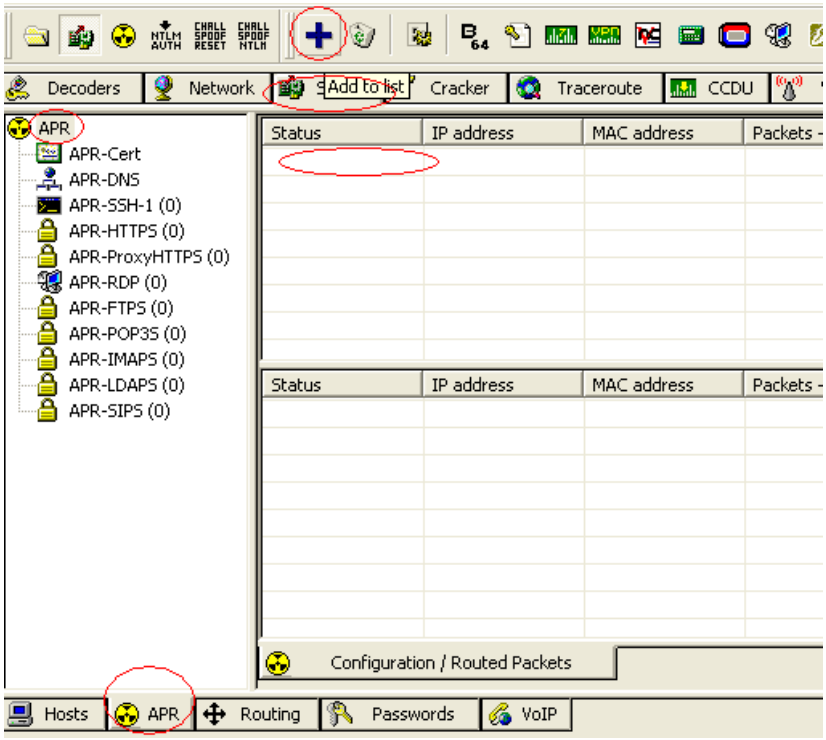


Figura 6. 112 Opción para añadir direcciones IP a la lista para ataque ARP.

En la siguiente ventana, en la parte izquierda se seleccionó la dirección IP de la víctima (192.168.1.117) y en la parte derecha la dirección IP del servidor FTP (192.168.1.105).

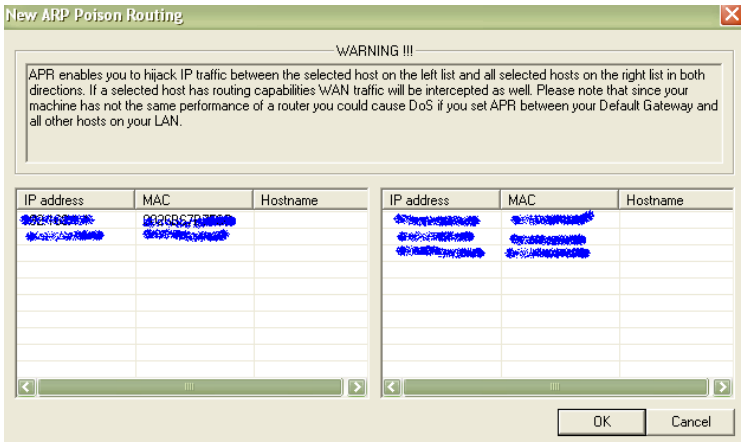


Figura 6. 113 Selección de direcciones IP víctima y del servidor FTP.

Al presionar Ok apareció la configuración anterior con las direcciones IP seleccionadas. Y se procedió a iniciar con el ataque ARP, presionando sobre la opción Start/Stop ARP.

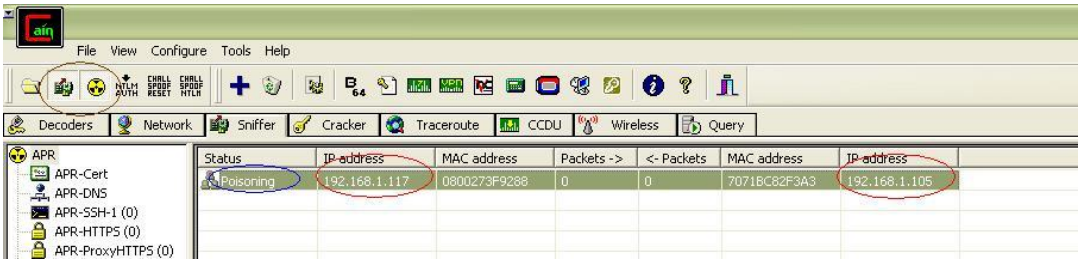


Figura 6. 114 Inicio del ataque ARP con la opción Start.

Para poder observar el tráfico, se seleccionó la opción Sniffer/Password y en este caso FTP. Y se pudo obtener el usuario y contraseña del servicio FTP.

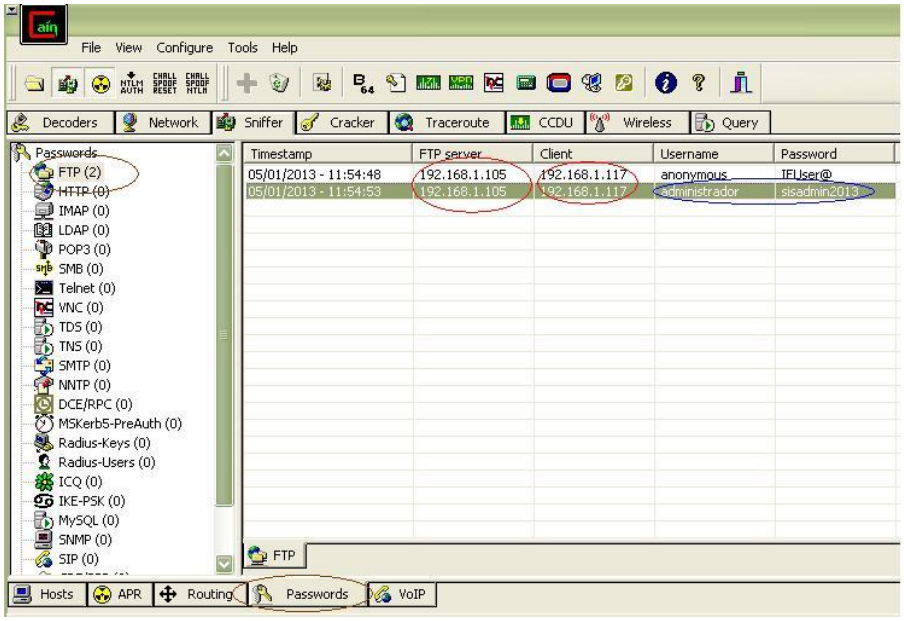


Figura 6. 115 Observación del tráfico FTP con Caín.

Para capturar de igual manera el tráfico FTP, se utilizó la herramienta Wireshark, la cual se usó conjuntamente con la aplicación Cain, para que funcione sin problemas.

Al abrir la herramienta Wireshark lo primero que se hizo fue seleccionar la opción **Capture** de la barra de herramientas y escoger: **options**.

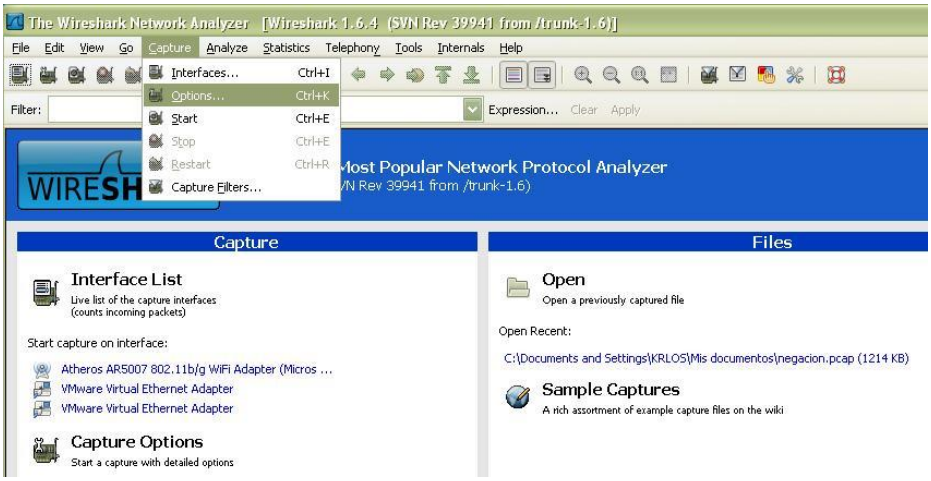


Figura 6. 116 Opciones de Captura de paquetes con Wireshark.

En la siguiente pantalla se tuvo que escoger la tarjeta de red inalámbrica a utilizar (Atheros WIFI Adapter) y quitar el visto de la opción **Capture packets in promiscuous mode** (acción a realizar porque se escogió la tarjeta inalámbrica). Posteriormente se dio un clic en el botón **start** para empezar la captura de paquetes en toda la red.

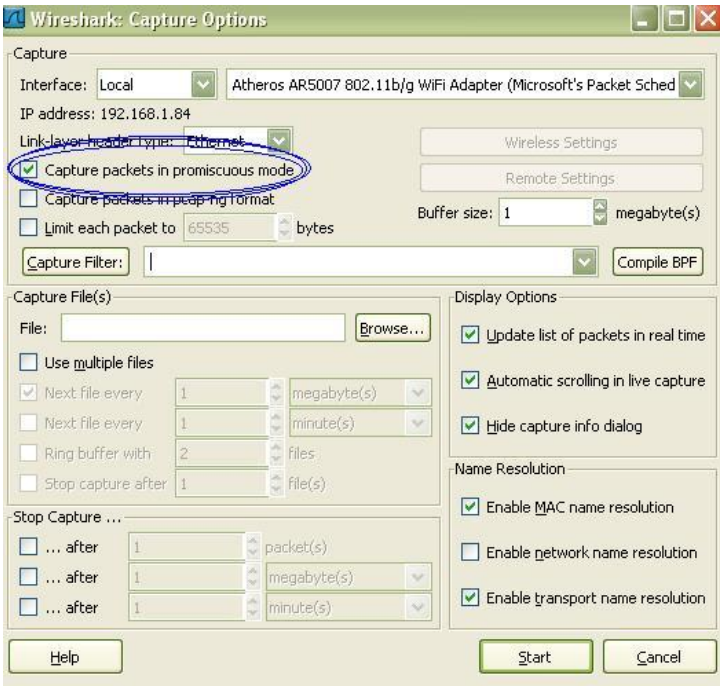


Figura 6. 117 Selección de la tarjeta inalámbrica a utilizar.

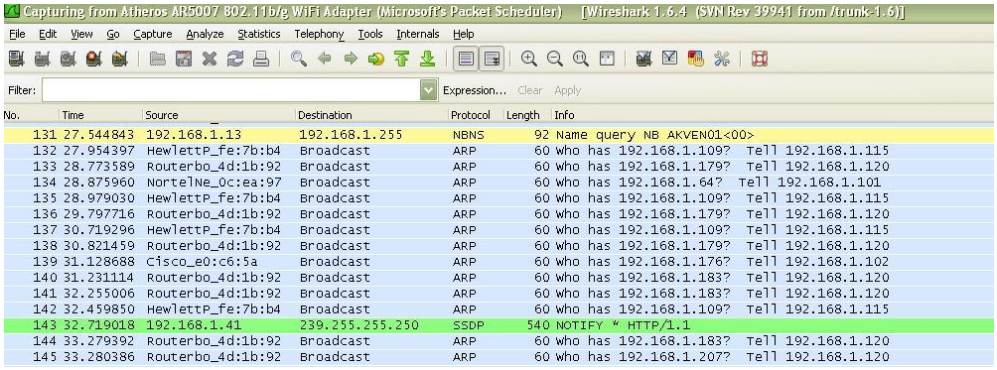


Figura 6. 118 Observación del tráfico de paquetes con Wireshark.

Por otra parte, en el lado de un cliente se procedió a la conexión ftp para abrir archivos. Se Abrió mi PC y en la barra de dirección se colocó **ftp://192.168.1.105**

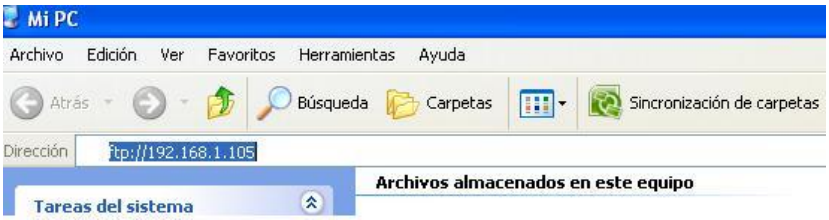


Figura 6. 119 Iniciar conexión FTP por parte del cliente.

Al presionar enter, apareció una ventana de inicio de sesión para poder acceder al servidor ftp y ver los archivos contenidos en él.

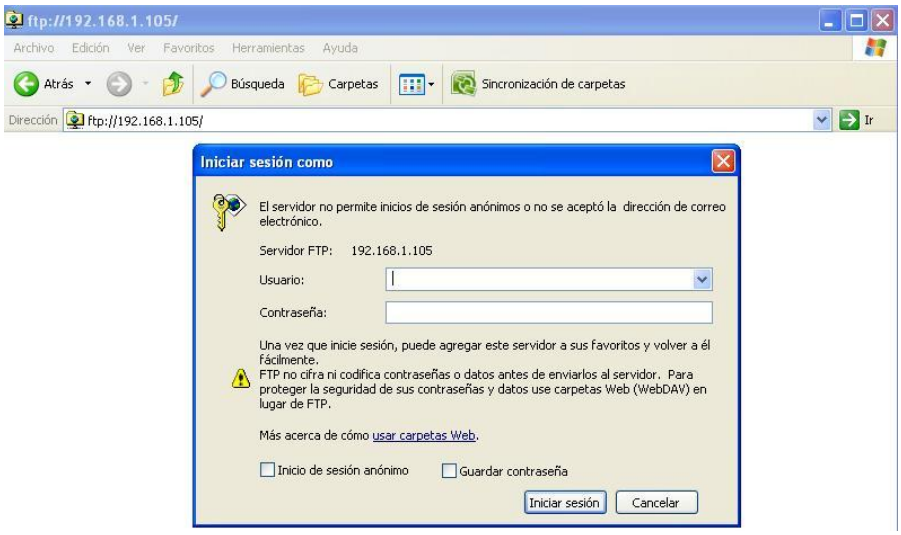


Figura 6. 120 Inicio de sesión del cliente FTP.

Se escribió el respectivo nombre de **usuario** y la **contraseña**.

Figura 6. 121 Escribir el respectivo nombre de usuario y contraseña para acceder al servicio FTP.

Al iniciar sesión se abrió la pantalla con todos los archivos contenidos por el servidor ftp. Mientras tanto en la herramienta Wireshark, en la captura que se estaba ejecutando, se procedió a buscar las capturas que se relacionen con el protocolo **ftp** y se pudo observar satisfactoriamente el usuario y contraseña del cliente ftp.

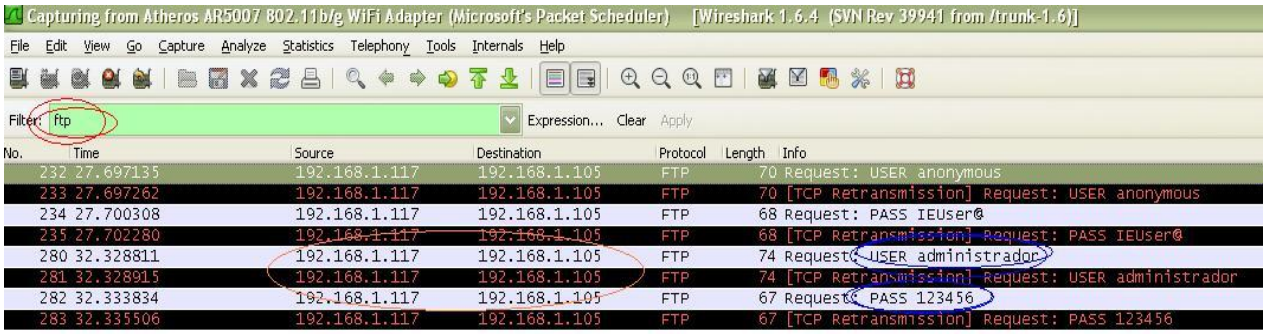


Figura 6. 122 Utilización del filtro FTP y observar el tráfico correspondiente (usuario y contraseña).

6.8.8 Tabla y Gráfica de los ataques realizados

ATAQUES REALIZADOS	Efectividad (%)
Desautenticación usuarios	100
Romper Claves WPA/WPA2 del AP	50
Suplantación de dirección MAC	100
Capturar tráfico FTP	100

Tabla 6. 2 Porcentaje de efectividad de los ataques informáticos realizados.

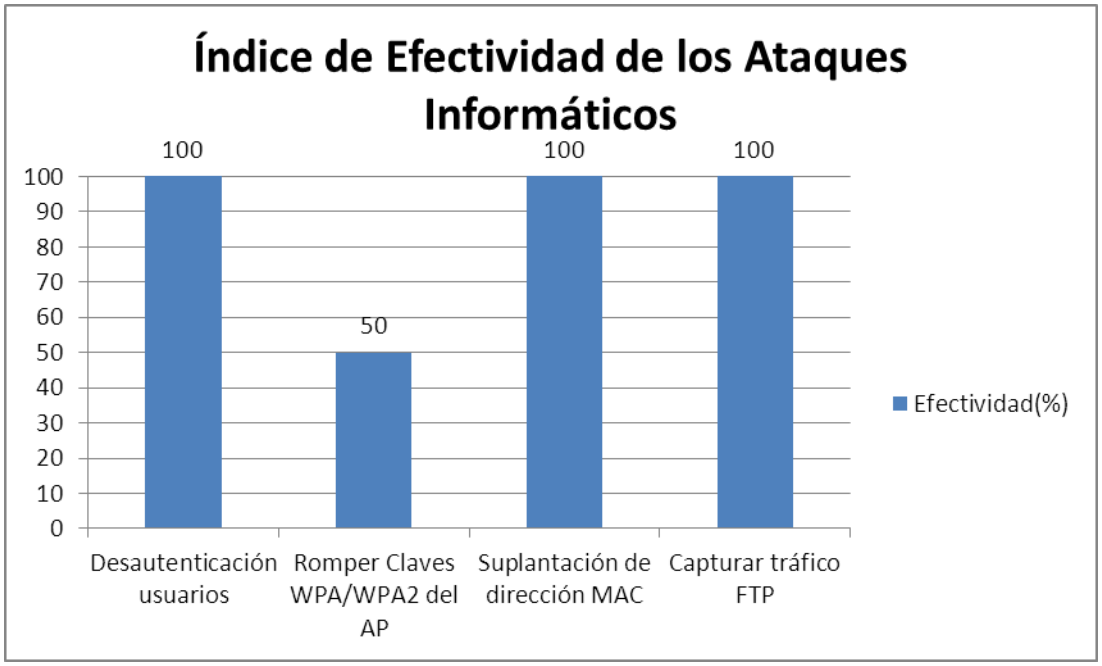


Figura 6. 123 Porcentaje de efectividad de los ataques informáticos realizados después de la implementación de políticas de seguridad.

6.9 Conclusiones Y Recomendaciones de la Propuesta

6.9.1 Conclusiones

- Se interpretaron las amenazas informáticas (según figura 6.86), por lo tanto los usuarios de la empresa AUTOMEKANO están conscientes del constante peligro que éstas representan y el daño que pueden causar a la empresa.

- La empresa AUTOMEKANO ahora ya cuenta con la implementación de políticas de seguridad en la comunicación inalámbrica.

- Con la implementación de las políticas de seguridad, y luego de haber aplicado las pruebas necesarias, se concluye que las amenazas informáticas se redujeron en un 12.5% (según figura 6.123), considerando que se aplicó un 17.24% de las políticas de seguridad recomendadas.

- Al seguir correctamente las políticas de seguridad establecidas, se ha tomado el camino correcto hacia un buen uso de la red inalámbrica y por ende reducir los riesgos informáticos.

- El tiempo de vida establecido para las políticas de seguridad no debe intervenir en su eficiencia y eficacia.

- Las políticas de seguridad implementadas en la comunicación inalámbrica se adecúan perfectamente a las necesidades y recursos de la empresa AUTOMEKANO.

6.9.2 Recomendaciones

- Seguir con las capacitaciones sobre seguridad informática y de la información, por parte del departamento de sistemas hacia los usuarios de la empresa AUTOMEKANO.

- El departamento de sistemas de la empresa AUTOMEKANO debe continuar con el mantenimiento de las políticas de seguridad en la comunicación inalámbrica y garantizar la seguridad en la empresa.

- El departamento de sistemas debe tener claro su responsabilidad en cuanto a la seguridad informática se refiere; y deberá realizar los respectivos monitoreos dentro y fuera de la comunicación inalámbrica.

- Es imposible reducir al 100% las diferentes amenazas informáticas que existen hoy en día, lo que se puede hacer es prevenirlas y reducirlas en cierto porcentaje, todo depende del uso consciente que se le dé a la tecnología.

- Se recomienda limitar el rango de la distribución de la señal del punto de acceso inalámbrico, así los usuarios podrán conectarse solo hasta cierta distancia y dentro del rango físico de la empresa.

- Si los puntos de acceso inalámbricos no se encuentran en uso, se recomienda apagarlos.

- Usar una herramienta de cifrado, para mantener la seguridad, integridad en los datos, correos electrónicos, archivos, entre otros, que se manejan en toda la empresa. Por ejemplo la herramienta GPG.

- **Bibliografía**

- **Libros**

  - ATELIN Philippe, DORDOIGNE José. (Noviembre 2006). Redes Informáticas. Eni. Barcelona-España. ISBN 10:2-7460-3482-4, 13:978-27460-3482-2.

  - CAZAR Héctor. (2001). Compendio de Computación Siglo XXI. Reivaj. Primera Edición. Quito-Ecuador. ISBN 9978-41-858-X.

  - ROLDAN David. (Mayo 2005). Comunicaciones Inalámbricas. Alfaomega Ra-Ma. Primera edición. México. ISBN 970-15-1078-X.

- **Páginas de Internet**

  - Computer Networking. Recuperado el 14-10-2011 y disponible en http://www.functionx.com/networking/index.htm
    Sitio Web donde existen lecciones básicas sobre redes.

  - Redes Informáticas. Recuperado el 15-10-2011 y disponible en http://es.scribd.com/doc/16298096/Redes-Informaticas
    Sitio Web donde se encuentran cargados archivos sobre diferentes temas de interés.

  - Introduction to Network Types. Recuperado el 16-10-2011 y disponible en http://compnetworking.about.com/od/basicnetworkingconcepts/a/network_types.htm
    Sitio Web donde se encuentran artículos sobre varios temas.

- Redes Inalámbricas. Recuperado el 17-10-2011 y disponible en http://blyx.com/public/wireless/redesInalambricas.pdf
  Descarga de archivos relacionados con varios temas.

- Redes Inalámbricas. Recuperado el 18-10-2011 y disponible en http://wifi.cablesyredes.com.ar/html/topologias.html
  Sitio Web de CablesyRedes Wi-Fi, para conocer soluciones óptimas al momento de instalar redes inalámbricas.

- Principales Amenazas. Recuperado el 22-10-2011 y disponible en http://www.arcert.gov.ar/politica/versionimpresa.htSS
  Sitio web donde se describe las Amenazas Informáticas.

- Ataques Externos. Recuperado el 22-10-2011 y disponible en http://www.ivlabs.org/home/?p=296
  Sitio Web.

- Cryptography and Network Security. Recuperado el 23-10-2011 y disponible en http://www2.cs.ucy.ac.cy/courses/EPL475/slides/ch17.pdf
  Descarga de archivos relacionados con varios temas.

- Redes en redes inalámbricas WIFI. Recuperado el 20-10-2011 y disponible en http://www.iec.csic.es/gonzalo/descargas/SeguridadWiFi.pdf
  Descarga de archivos relacionados con varios temas.

- Redes inalámbricas en países de desarrollo. Recuperado el 25-10-2011 y disponible en http://wndw.net/pdf/wndw-es/about-es.pdf
  Archivo publicado bajo la licencia: Creative Commons Attribution-ShareAlike 2.5.

- Qué es Seguridad en WIFI. Recuperado el 23-10-2011 y disponible en http://www.coit.es/publicaciones/bit/bit152/95-99.pdf
  Descarga de archivos relacionados con varios temas.

- Seguridad en Redes WiFi - Puntos Débiles. Recuperado el 21-10-2011 y disponible en http://www.virusprot.com/cursos/Redes-Inal%C3%A1mbricas-Curso-gratis7.htm
  Sitio Web.

- PWireless Network Security 802.11, Bluetooth and Handheld Devices. Recuperado el 18-10-2011 y disponible en http://www.itsec.gov.cn/docs/20090507161834185644.pdf
  Descarga de archivos relacionados con varios temas.

- Protocolos de seguridad en redes inalámbricas. Recuperado el 22-10-2011 y disponible en http://www.saulo.net/des/SegWiFi-art.pdf
  Descarga de archivos relacionados con varios temas.

- Políticas de Seguridad de la Información. Recuperado el 25-10-2011 y disponible en http://www.segu-info.com.ar/politicas/polseginf.htm
  Sitio web de seguridad de la información.

- Guía para elaborar políticas v1.0-Universidad Nacional de Colombia. Recuperado el 05-02-2012 y disponible en http://www.slideshare.net/SuperFonso/guia-para-elaborar-politicas-v1-0
  Slideshare

- Walc 2004 Track 6 Seguridad Informática- Políticas de Seguridad. Recuperado el 27-10-2011 y disponible en http://www.eslared.org.ve/walc2004/apc-aa/archivos-aa/1e60354f4717edb9fb793dbc5219499d/politica2004.pdf
  Descarga de archivos relacionados con varios temas.

- Seguridad en Redes Inalámbricas Usando Herramientas de Software Libre. Recuperado el 21-10-2011 y disponible en http://cdigital.uv.mx/bitstream/123456789/28546/1/sanchez%20perez.pdf
  Sitio Web de un Repositorio Institucional para descargar archivos pdf de Tesis o trabajos similares.

- Amenaza en la Red. Recuperado el 19-10-2011 y disponible en http://www.elsiglodetorreon.com.mx/noticia/249143.amenaza-en-la-red.html
  Sitio Web con noticias.

- Introducción a la seguridad informática. Recuperado el 10-10-2011 y disponible en http://es.kioskea.net/contents/secu/secuintro.php3
  Sitio web, libre.

- Cain & Abel. Recuperado el 04-02-2012 y disponible en http://www.oxid.it/cain.html

- Sniffing con Cain y Abel. Recuperado el 12-03-2012 y disponible en http://houdinihck.netai.net/Lecciones/Sniffing%20con%20Cain%20y%20Abel.pdf

- How to Use Snort on Backtrack .ogv. Recuperado el 15-05-2012 y disponible en http://www.youtube.com/watch?feature=player_embedded&v=sPPDksiQmg Youtube

- Nessus – Escaner de vulnerabilidades. Recuperado el 06-02-2012 y disponible en http://systemadmin.es/2011/03/nessus-escaner-de-vulnerabilidades Tu referencia para la administración de sistemas.

Glosario de Términos

802.11.- Es un grupo de trabajo del IEEE que desarrolla distintos estándares para el uso de la tecnología de radiofrecuencia en las redes de área local (LAN).

Ad-hoc.- Configuración del equipo cliente que ofrece conectividad independiente entre dispositivos dentro de una red LAN inalámbrica. Como alternativa, los ordenadores se pueden comunicar entre sí a través de un punto de acceso.

Amenazas Informáticas.- Las amenazas Informáticas son los problemas más vulnerables que ingresan a nuestra computadora con el hecho de afectarlo.

AP.- Del inglés Access Point, o punto de acceso. El punto de acceso corresponde a un transmisor-receptor de redes inalámbricas, o "estación base", que puede conectar una red LAN cableada a uno o varios dispositivos inalámbricos.

Beacons.- Son tramas que emiten los puntos de acceso (AP) para que otros puntos sepan que existe un punto de acceso activo.

BSSID.- (**B**asic **S**ervice **S**et **ID**entifier – Identificador de Servicio Básico) Dirección MAC del punto de acceso, la emplean las tarjetas inalámbricas para identificar y asociarse a redes Wireless.

Canales.- Las redes inalámbricas emplean canales. Cada canal inalámbrico tiene una frecuencia diferente. Existen hasta 14 canales diferentes que se pueden utilizar en una red inalámbrica.

Clave de codificación.- Una serie de letras y números que permite codificar datos y después decodificarlos de forma que se puedan compartir de manera segura entre los

miembros de una red. Los usuarios de WEP utilizan una clave de codificación que codifica automáticamente los datos salientes. Esta misma clave le permite al ordenador receptor decodificar automáticamente la información para que se la pueda leer.

Cliente.- Una aplicación instalada en un ordenador o dispositivo conectado a una red que solicita servicios (archivos, impresión) de otro miembro de la red.

DHCP.- Del inglés Dynamic Host Configuration Protocol, o Protocolo de configuración dinámica de host. El DHCP es una utilidad que le permite a un servidor asignar de manera dinámica direcciones IP desde una lista predefinida y limitar el tiempo de uso de manera que se puedan volver a asignar.

Dirección IP.- Un número que identifica cada emisor o receptor de información enviada en una red.

Dirección MAC.- (siglas en inglés de media access control; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo.

DNS.- Del inglés Domain Name System (Service o Server), también llamado Sistema (servicio o servidor) de nombres de dominio. El DNS es un programa que traduce los URL en direcciones IP ingresando a una base de datos ubicada en una serie de servidores Internet. Este programa funciona en segundo plano para que el usuario pueda navegar por Internet utilizando direcciones alfabéticas en vez de una serie de números.

DOS.- (Denial of Service – Denegación de Servicio) Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Eavesdropping.- Significa escuchar secretamente en una red, se ha utilizado tradicionalmente en ámbitos relacionados con la seguridad. Se refiere a ataques de escuchas, tanto sobre medios con información cifrada, como no cifrada.

Enrutador.- Punto de acceso o dispositivo que envía datos desde una red de área local (LAN) o red de área amplia (WAN) a otra. El enrutador monitorea y controla el flujo de datos, y envía información a través de la ruta más eficiente en función del tráfico, el costo, la velocidad, las conexiones, etc.

ESSID.- (**E**xtended **S**ervice **S**et **ID**entifier – Identificador de Servicio Extendido) Se utiliza cuando en las redes de infraestructura (cliente/servidor) incorporan un punto de acceso. El ESSID consta de como máximo 32 caracteres. Es necesario conocer el ESSID del punto de acceso para poder formar parte de la red inalámbrica.

Exploit.- fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

Handshake.- El handshake se genera cuando un cliente se asocia a la red inalámbrica, es como un saludo (apretón de manos) entre el punto de acceso y el cliente.

Host.- El término es usado para referirse a las computadoras conectadas a una red, que proveen y utilizan servicios de ella.

Http.- Hypertext Transfer Protocol o **HTTP** (protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la World Wide Web. HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado.

Https.- Hypertext Transfer Protocol Secure (Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas **HTTPS**, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

IP.- Del inglés Internet Protocol, o Protocolo de Internet. Tecnología que permite la transmisión de voz, datos y vídeo a través de Internet, redes WAN y LAN con conexión IP.

Live CD.- Es un sistema operativo almacenado en un medio extraíble, tradicionalmente un CD o un DVD (de ahí sus nombres), que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro de una computadora.

Políticas de Seguridad.- Instrumento gerencial, consta de normas, procedimientos, cuyo objetivo es garantizar la seguridad.

Redes Inalámbricas.- Es la interconexión de distintos dispositivos con la capacidad de compartir información entre ellos, pero sin un medio físico de transmisión.

Redes Informáticas.- Una red es un sistema donde los elementos que lo componen (por lo general ordenadores) son autónomos y están conectados entre sí por medios físicos y/o lógicos y que pueden comunicarse para compartir recursos.

RFC.- (Request For Comments – Solicitud de comentarios) Consiste en un documento que puede ser escrito por cualquier persona y que contiene una propuesta para una nueva tecnología, información acerca del uso de tecnologías y/o recursos existentes, propuestas para mejoras de tecnologías, proyectos experimentales y demás.

Seguridad Informática.- Es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

Sistema Operativo.- Un Sistema Operativo (SO) es el software básico de una computadora que provee una interfaz entre el resto de programas del ordenador, los dispositivos hardware y el usuario.

Sniffer.- Programa de captura de paquetes de red; puede ser empleado con fines didácticos, maliciosos o constructivos. El funcionamiento de un sniffer depende del estado en que se coloca la tarjeta de red: modo promiscuo o normal. En modo promiscuo el sniffer captura todo el tráfico de red, a diferencia del modo normal de funcionamiento que solamente intercepta el tráfico saliente o entrante que corresponda a la tarjeta de red.

SSH.- (**S**ecure **SH**ell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.

SSL.- (Secure Sockets Layer, capa de conexión no segura) y su sucesor **Transport Layer Security** (**TLS**; seguridad de la capa de transporte) son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet. SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.

TCP/IP.- Tecnología tras Internet y las comunicaciones entre ordenadores en una red.

Virus Informático.- Es un malware (tipo de software) que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

WEP.- Del inglés Wired Equivalent Privacy, o Privacidad equivalente al cableado. Seguridad básica para sistemas inalámbricos proporcionada por Wi-Fi. En algunos casos, WEP se encuentra disponible en modos de codificación de 40 bits (también conocido como codificación de 64 bits), o 108 bits (o codificación de 128 bits).

WI-FI.- Del inglés Wireless Fidelity, o Fidelidad inalámbrica. Término creado por Wi-Fi Alliance que se utiliza para describir redes inalámbricas estándar tipo 802.11. Los productos que Wi-Fi Alliance haya probado y certificado como "Wi-Fi" pueden operar entre sí incluso si son de marca diferente.

WPA.- Del inglés Wi-Fi Protected Access, o Acceso Wi-Fi protegido. Se trata de un estándar de seguridad para redes Wi-Fi que trabaja con productos Wi-Fi existentes compatibles con WEP (Wired Equivalent Privacy, Privacidad equivalente al cableado). Codifica los datos a través del protocolo TKIP (Temporal Key Integrity Protocol, Protocolo de integridad de clave temporal). TKIP mezcla las claves y garantiza que no se hayan alterado. La autenticación del usuario se realiza mediante el protocolo EAP (Extensible Authentication Protocol, Protocolo de autenticación ampliada) para garantizar que sólo usuarios autorizados puedan ingresar a la red.

WPA2.- (Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades

detectadas en WPA. WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.

ANEXOS

ANEXO 1: Estructura de la Encuesta A

UNIVERSIDAD TECNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRONICA E INDUSTRIAL
Agencia Matriz de la Empresa AUTOMEKANO

Encuesta dirigida a los Jefes del Departamento de Sistemas.

OBJETIVO: La presente encuesta tiene como fin evaluar el conocimiento que existe en la empresa sobre las amenazas informáticas, políticas de seguridad y obtener sugerencias u observaciones previas a la ejecución del proyecto.

Señores, su veracidad en las respuestas permitirá al investigador desarrollar un trabajo real y efectivo.

Agradecemos su colaboración y garantizamos absoluta reserva de su información

CUESTIONARIO

1. ¿Conoce sobre los diferentes tipos de amenazas informáticas que existen en la red?

   SI ( ) NO ( )

2. ¿Alguna vez notó algún comportamiento extraño o fuera de lo común dentro de la red inalámbrica, como por ejemplo direcciones IP duplicadas, fallos en la conexión, etc.?

   SI ( ) NO ( )

3. ¿Verifica de alguna forma si la información que recibe dentro de la red es del remitente correcto?

SI ( ) NO ( )

4. ¿Cree usted que la navegación dentro de la red inalámbrica es segura?

SI ( ) NO ( )

5. En calidad de administrador de la red inalámbrica, ¿usted controla o sabe si un usuario instaló algún tipo de software en su computador de trabajo?

SI ( ) NO ( )

6. ¿Considera usted pertinente implementar políticas de seguridad con la finalidad de garantizar la seguridad en la comunicación inalámbrica?

SI ( ) NO ( )

7. ¿Cree usted que la implementación de políticas de seguridad mejorará la confianza y se usará de mejor manera la información a transmitir dentro y fuera de la red?

SI ( ) NO ( )

8. ¿Qué tipo de información es considerada vital dentro de la empresa AUTOMEKANO?

_____

_____

9. ¿Cuántos dispositivos para la comunicación inalámbrica se utilizan y que mecanismos de seguridad se aplican en cada uno de ellos?

_____
_____
_____

10. ¿Se maneja algún servidor configurado que sirva para garantizar la comunicación inalámbrica, si es así detallar la fecha de inicio de uso, plataforma, características básicas de configuración?

_____
_____
_____

11. ¿Diariamente cuál es la cantidad máxima y mínima de conexiones en la red inalámbrica de la empresa?

_____
_____
_____

12. ¿Desearía adjuntar sugerencias u observaciones a considerarse para el desarrollo e implementación de políticas de seguridad en la comunicación inalámbrica?

_____
_____
_____

GRACIAS POR SU COLABORACIÓN

Fecha de aplicación: ……

ANEXO 2: Estructura de la Encuesta B

UNIVERSIDAD TECNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRONICA E INDUSTRIAL
Agencia Matriz de la Empresa AUTOMEKANO

Encuesta dirigida al personal de la empresa que utiliza la red inalámbrica.

OBJETIVO: La presente encuesta tiene como fin evaluar el conocimiento que existe en la empresa sobre el uso consciente de la red inalámbrica y obtener información que servirá a la ejecución del proyecto.

Señores, su veracidad en las respuestas permitirá al investigador desarrollar un trabajo real y efectivo.

Agradecemos su colaboración y garantizamos absoluta reserva de su información

CUESTIONARIO

1. ¿Conoce sobre los diferentes tipos de amenazas informáticas que existen en las redes inalámbricas?

   SI ( ) NO ( )

2. ¿Para conectarse a la red inalámbrica utiliza una contraseña?

   SI ( ) NO ( )

3. ¿Ha tenido más de una vez problemas para conectarse a la red inalámbrica?

SI ( ) NO ( )

4. ¿Ha notado algún comportamiento extraño mientras está conectado a la red inalámbrica?

SI ( ) NO ( )

5. ¿Considera usted que la red inalámbrica es un medio seguro para transmitir datos e información de una manera íntegra?

SI ( ) NO ( )

6. ¿Qué le parece el servicio de la red inalámbrica?

Excelente ( )
Buena ( )
Regular ( )
Mala ( )
Deficiente ( )

7. ¿Cuántas veces a la semana usa la red inalámbrica?

Menos de 2 veces ( )
De 2 a 3 veces ( )
De 4 a 6 veces ( )

8. ¿Cuál es el tiempo de uso aproximado de la red inalámbrica al día?

Menos de 2 horas ( )
De 2 a 4 horas ( )

De 4 a 6 horas ( )

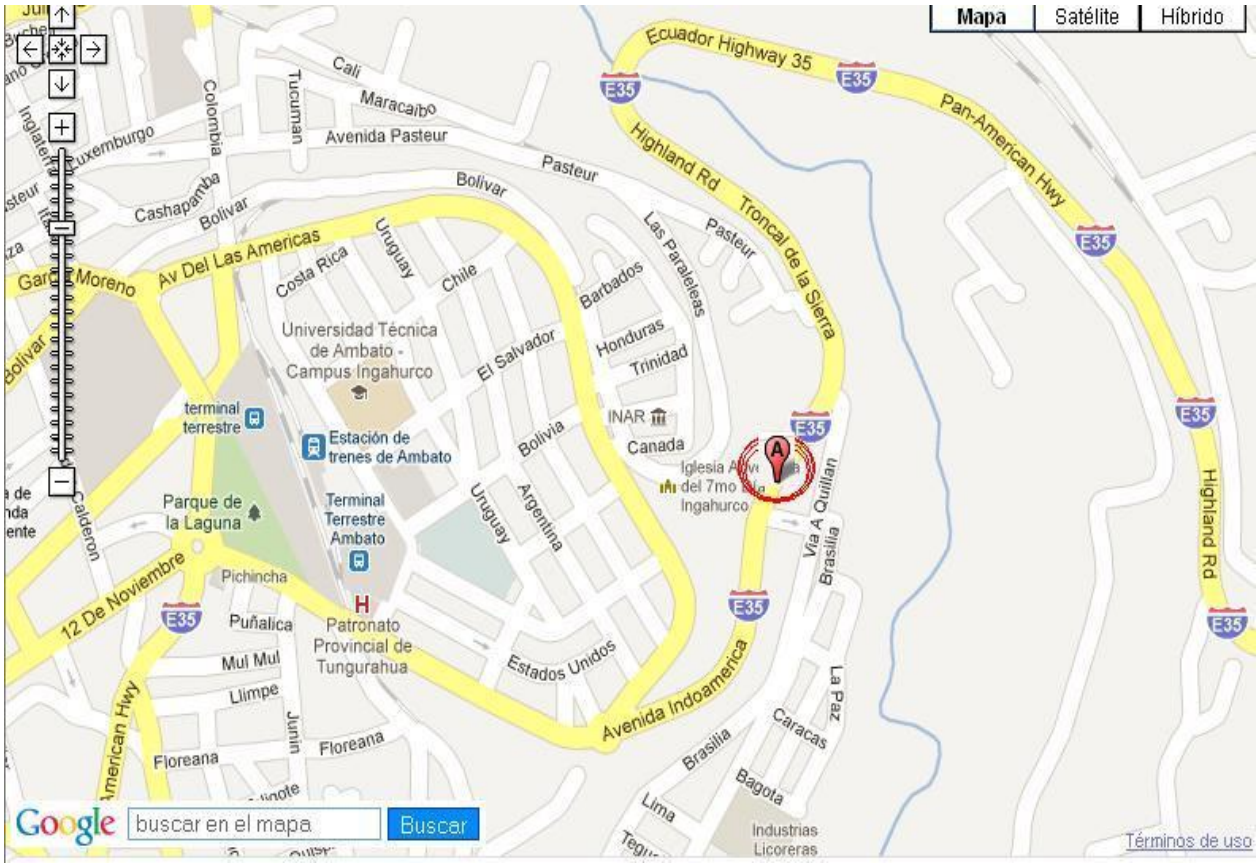
9. ¿Considera usted pertinente implementar políticas de seguridad con la finalidad de garantizar la seguridad en la comunicación inalámbrica?

SI ( ) NO ( )

GRACIAS POR SU COLABORACIÓN

Fecha de aplicación: ……

ANEXO 3: Croquis del Problema (Empresa AUTOMEKANO Ambato)



Av. Indoamérica Km. 1 – Entrada a las Viñas.

ANEXO 4: Estándares WIFI

El estándar 802.11 vio la luz en junio de 1997 y se caracteriza por ofrecer velocidades de 1 y 2 Mbps, un sistema de cifrado sencillo llamado WEP (Wired Equivalent Privacy) y operar en la banda de frecuencia de 2.4 Ghz; en dos años, septiembre de 1999, aparecen las variantes 802.11ª y 802.11b que ofrecen velocidades de 54 y 11 Mbps respectivamente. Pronto se pondrían de manifiesto las carencias a nivel de seguridad de estos estándares.

La familia 802.11 está compuesta, a día de hoy, por los siguientes estándares:

802.11a: (5.1-5.2 Ghz, 5.2-5.3 Ghz, 5.7-5.8 Ghz), 54 Mbps. OFDM: Multiplexación por division de frecuencias orthogonal.

802.11b: (2.4-2.485 Ghz), 11 Mbps.

802.11c: Define características de AP como Bridges.

802.11d: Múltiples dominios reguladores (restricciones de países al uso de determinadas frecuencias).

802.11e: Calidad de Servicio (QoS).

802.11f: Protocolo de conexión entre puntos de acceso (AP), protocolo IAPP: Inter Access Point Protocol.

802.11g: (2.4-2.485 Ghz), 36 o 54 Mbps. OFDM: Multiplexación por division de frecuencias orthogonal. Aprobado en 2003 para dar mayor velocidad con cierto grado de compatibilidad a equipamiento 802.11b.

802.11h: DFS: Dynamic Frequency Selection, habilita una cierta coexistencia con HiperLAN y regula también la potencia de difusión.

802.11i: Seguridad (Aprobada en junio de 2004).

802.11j: Permitiría armonización entre IEEE (802.11), ETSI (HiperLAN2) y ARIB (HISWANa).

802.11m: Mantenimiento redes wireless.