UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMATICOS

Tema:

"TÉCNICA SNIFFER PARA DETECTAR VULNERABILIDADES EN EL SERVIDOR WEB, MAIL Y FTP DEL HOSPITAL REGIONAL DOCENTE AMBATO"

Proyecto de Trabajo de Graduación. Modalidad: SEMINARIO DE GRADUACIÓN presentado previo la obtención del título de Ingeniera en Sistemas Computacionales e Informáticos.

.

AUTOR: María Fernanda Conterón Tene

TUTOR: Ing. Xavier Francisco López A.

Ambato - Ecuador

Noviembre-2012

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: TÉCNICA SNIFFER PARA DETECTAR VULNERABILIDADES EN EL SERVIDOR WEB, MAIL Y FTP DEL HOSPITAL REGIONAL DOCENTE AMBATO, de la señorita María Fernanda Conterón Tene, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, 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 con el Art. 16 del Capítulo IV, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato, Noviembre del 2012

EL TUTOR

……..

Ing. Xavier Francisco López A.

AUTORÍA

El presente trabajo de investigación titulado: TÉCNICA SNIFFER PARA DETECTAR VULNERABILIDADES EN EL SERVIDOR WEB, MAIL Y FTP DEL HOSPITAL REGIONAL DOCENTE AMBATO. 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, Noviembre del 2012

EL AUTOR

……..

María Fernanda Conterón Tene

C.C: 180385604-4

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores Ing. Oswaldo Paredes Ochoa M.Sc., Presidente y los señores Miembros Ing. Pilar Urrutia e Ing. Galo López, revisó y aprobó el Informe Final del trabajo de graduación titulado "TÉCNICA SNIFFER PARA DETECTAR VULNERABILIDADES EN EL SERVIDOR WEB, MAIL Y FTP DEL HOSPITAL REGIONAL DOCENTE AMBATO", presentado por la señorita María Fernanda Conterón Tene de acuerdo al Art. 17 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ing. Oswaldo Paredes Ochoa M.Sc.
PRESIDENTE DEL TRIBUNAL

Ing. Pilar Urrutia
DOCENTE CALIFICADOR

Ing. Galo López
DOCENTE CALIFICADOR

DEDICATORIA:

Dedico este proyecto:

A mis padres, por su esfuerzo, apoyo y confianza que depositaron en mí, permitiendo la feliz culminación de este proyecto.

A mi hermana Elizabeth que ha estado a mi lado en todos los momentos de mi vida y a Luis quien ha estado apoyándome incondicionalmente en todo este proceso.

A todas las personas que de una u otra forma durante mi vida universitaria me brindaron amistad, apoyo y colaboración.

Fernanda

AGRADECIMIENTO:

A Dios por brindarme sabiduría, paciencia y fuerzas que me ayudaron en mis momentos de debilidad y permitieron la culminación de mi tesis.

Al Hospital Regional Docente Ambato por abrir sus puertas permitiendo la realización de este trabajo de investigación con la colaboración de sus funcionarios.

Al Ing. Francisco López mi tutor, por sus conocimientos y colaboración durante la elaboración de la tesis.

Fernanda

ÍNDICE GENERAL DE CONTENIDOS

CONTENIDO **PÁGS**

PRELIMINARES

CAPITULO I

EL PROBLEMA

CAPITULO II

MARCO TEORICO

CAPITULO III

MARCO METODOLOGICO

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

CAPITULO VI

PROPUESTA

INDICE DE CUADROS

CAPITULO III

CAPITULO IV

CAPITULO VI

INDICE DE FIGURAS

CAPITULO I

CAPITULO II

CAPITULO IV

CAPITULO VI

INDICE DE ANEXOS

RESUMEN EJECUTIVO

La presente investigación tiene como tema "TÉCNICA SNIFFER PARA DETECTAR VULNERABILIDADES EN EL SERVIDOR WEB, MAIL Y FTP DEL HOSPITAL REGIONAL DOCENTE AMBATO".

El contenido de la investigación comprende los aspectos más relevantes sobre la APLICACIÓN DE LA TÉCNICA SNIFFER PARA LA DETECCIÓN DE VULNERABILIDADES EN EL SERVIDOR WEB, MAIL Y FTP DEL HOSPITAL REGIONAL DOCENTE AMBATO, el mismo que está estructurado por seis capítulos.

El capítulo I contiene el Planteamiento del Problema que se enfoca a la necesidad de establecer una verdadera investigación científica sobre la aplicación de la Técnica Sniffer para la detección de las fallas existentes en los servidores WEB, MAIL y FTP. El desconocimiento y la falta de recursos han sido limitantes para la aplicación de métodos para detectar dichas fallas, dejado al descubierto la seguridad de la información que se maneja dentro de la institución.

La justificación se fundamenta al afirmar que la Técnica Sniffer, es una alternativa para lograr la detección de las vulnerabilidades de los servidores WEB, MAIL y FTP de la red del Hospital Regional Docente.

El capítulo II se refiere al Marco Teórico, el cual consta de los antecedentes investigativos en donde se puso una investigación previa similares al propuesto con sus respectivas conclusiones, de la fundamentación legal en donde se coloco los ítems de la norma ISO 27001-2005, Uso de software libre, ley de transparencia y acceso a información pública, ley de comercio electrónico, firmas electrónicas y mensajes de datos, que son necesarios para la guía del presente trabajo, logrando un tratamiento adecuado de la información obtenida y de la fundamentación teórica que con ayuda de las categorías fundamentales se pudo realizar la investigación bibliográfica.

La hipótesis planteada fue: “La aplicación de la Técnica Sniffer ayudará en la detección de las vulnerabilidades en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato.”. De aquí se desprenden las variables dependientes e independientes.

Los capítulos III y IV comprenden la metodología y el análisis de resultados; para lograr los objetivos propuestos, se realizó la investigación de campo, con el fin de recolectar la informaron a través de la entrevista realizada al Jefe del Departamento de Sistemas y las encuestas a los usuarios de la red del “Hospital Regional Docente Ambato”. Los datos obtenidos sirvieron para el análisis e interpretación de resultados y la elaboración de la propuesta.

El capítulo V contiene las conclusiones y recomendaciones más relevantes, las mismas que al ser aceptadas y llevadas a la práctica por la Institución, se convertirán en orientaciones eficientes que guiarán para la seguridad de la información sensible dando un correcto manejo.

El capítulo VI contiene la propuesta, que consiste en la aplicación de la Técnica Sniffer para poder encontrar las vulnerabilidades existentes en los servidores que están dedicados de frente al Internet en el HRDA, siendo la opción más efectiva para obtener un informe detallado de los agujeros de seguridad en los servidores involucrados.

INTRODUCCIÓN

El Hospital Regional Docente Ambato es una institución pública dedicada a brindar servicio de salud, hoy en día es una de las instituciones de gran importancia para la provincia y el Ecuador. Día tras día se ha incrementando tanto en su infraestructura física como tecnológica involucrando el manejo de gran cantidad de información de vital importancia para un correcto funcionamiento, siendo la red interna con conexión a Internet el principal medio de comunicación y medio para compartir información.

Garantizar la integridad, confiabilidad, disponibilidad y no repudio de la información es uno de los desafíos más grande del administrador. Los métodos que utilizan los hackers para alterar la seguridad de una red son infinitos, uno de ellos es la Técnica Sniffer que no es otra cosa que la captura, interpretación y almacenamiento de los paquetes de datos que viajan por redes Ethernet. Estas redes comparten un medio común para la comunicación por lo que son de fácil accesibilidad para los sniffer. En este sentido, por la existencia de un número considerable de amenazas y riesgos, es necesaria la detección de las falencias de seguridad de los servicios HTTP, SMTP y FTP, para reducir los niveles de vulnerabilidad y que permitan una eficiente administración del riesgo.

CAPITULO I

EL PROBLEMA

1.1. Tema:

Técnica Sniffer para detectar vulnerabilidades en el servidor WEB, MAIL y FTP del Hospital Regional Docente Ambato.

1.2. Planteamiento del problema

1.2.1. Contextualización

En los últimos años la evolución, y la posterior innovación de la tecnología ha generado grandes avances en todos los ámbitos a nivel mundial, es así que la intranet y el internet se ha convertido en medios imprescindibles para el intercambio de información, la mayoría de instituciones públicas o privadas utilizan estos medios para realizar actividades como por ejemplo: transacciones bancarias, compras, declaraciones de impuestos, envío de correo electrónico, intercambio de mensajes o archivos, etc. pero a la par del desarrollo tecnológico se han incrementado los métodos de espionaje informático que utilizan los hacker o crackers para realizar intrusiones e infiltraciones a una red.

En el Ecuador, La mayor parte de las instituciones, tienen enlaces que conectan diferentes redes, estos enlaces pueden ser enlaces entre redes privadas y enlaces a redes públicas (Internet) para la comunicación de una forma fácil, rápida y eficaz; los administradores son responsables de la seguridad de la red, en gran parte solo se enfocan en la funcionalidad y dejan a un lado el ámbito de la seguridad informática y más aun de la seguridad de la información. La información que circula por la red es delicada y única, convirtiéndose en un blanco ideal para ser atacados en cualquier punto intermedio, provocando daños lógicos, físicos y pérdidas económicas, por lo que es importante encontrar las fallas existentes en

los servidores WEB MAIL y FTP destinados para la transferencia de información y tomar conciencia en el tratamiento de los agujeros de seguridad.

En Tungurahua el Hospital Regional Docente Ambato (**HRDA**) es una institución pública que ha incrementado en el uso de la tecnología y el acceso a una red de computadoras, estas implementaciones conllevan a más requerimientos para compartir información entre los usuarios de la red, haciendo que cada día exista una obligatoriedad en el cumplimiento de la seguridad de la información; el problema actual en el Departamento de Sistemas del HRDA se originan fundamentalmente porque existe un desconocimiento de las vulnerabilidades de los servidores WEB, MAIL y FTP ya que los equipos informáticos se encuentran interconectados con una administración en la seguridad media en el firewall, comprometiendo la información que maneja la institución a grandes riesgos como: ataque de intersección (captura, manipulación, pérdida) suspensión de servicios y tiempo de recuperación; el flujo de información que circula a través de esta red es de alta importancia por lo que conocer algunos de los puntos débiles de los servidores WEB, MAIL y FTP con el Sniffing ayudará para que se puedan tomar decisiones correctas con respecto a esto.

1.2.1.1. ARBOL DE PROBLEMAS

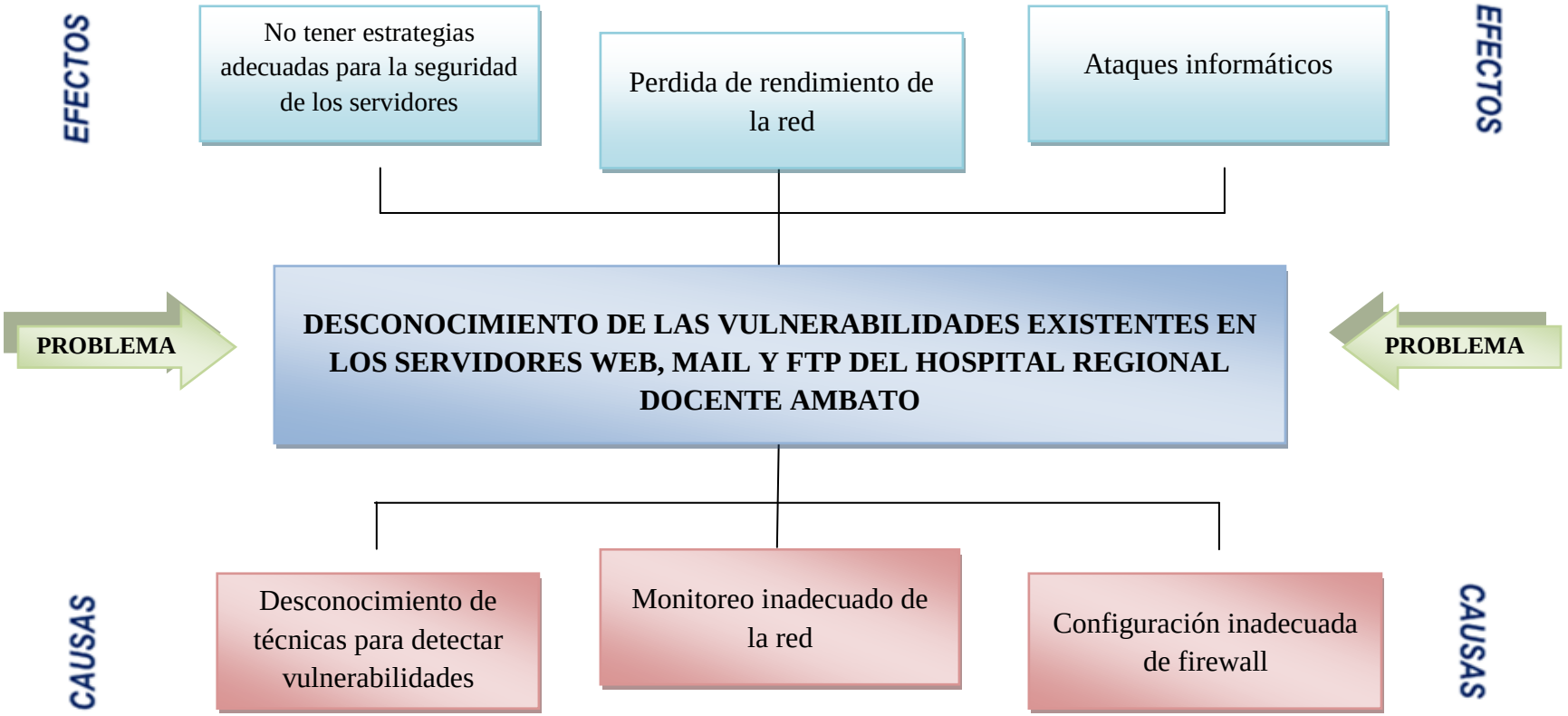

Figura Nº 1.1: Árbol de Problemas
Autor: Fernanda Conterón

1.2.2. Análisis Crítico

Hoy en día con el afán de comunicarse de una forma rápida y eficaz entre los departamentos del Hospital Regional Docente Ambato y con otras instituciones se ha olvidado un punto importante que es brindar seguridad a la información que maneja la institución, existe un desconocimiento de técnicas para detectar alguna anomalía en los servicios HTTP, Correo y FTP lo cual conlleva a no tener estrategias adecuadas para la seguridad de los servidores.

El monitoreo inadecuado de la red por parte del administrador por falta de tiempo, de recursos y por desconocimiento de las herramientas apropiadas es causa importante para que se desconozcan las vulnerabilidades existentes en los servidores WEB, MAIL y FTP, provocando pérdida en el rendimiento de la red gestionada.

La red del HRDA no tienen una adecuada configuración del firewall, dejando a la red propensa a ataques informáticos activos o pasivos, estos ataques aprovechan las vulnerabilidades de los servidores WEB MAIL y FTP para poder filtrarse en la red de forma ilegal, teniendo como objetivo adquirir información privada (claves cuentas, números de tarjetas de crédito, direcciones de e-mails), modificación o destrucción de archivos de uso exclusivo de la institución o colapsar la red, causando daños irreversibles.

1.2.3. Prognosis

De no darse la solución al problema que es el desconocimiento de las vulnerabilidades de los servidores WEB, MAIL y FTP del HRDA en base a la Técnica Sniffing, estos seguirán siendo puntos débiles en la seguridad informática y serán aprovechados por cualquier intruso, dejando susceptible la información a la captura, pérdida o daño de manera personal, grupal o institucional, también puede verse comprometiendo el desempeño de la red, perjudicando su prestigio, economía y desarrollo provocando finalmente un caos tecnológico en la institución.

Por lo tanto se hace necesario garantizar la seguridad de los datos que maneja la institución, es decir garantizar la confiabilidad, integridad y confidencialidad, para lo cual debemos detectar las vulnerabilidades en los servidores seleccionados causadas por la Técnica Sniffer, utilizándolo como herramienta de detección, permitiendo así tener una idea clara de las falencias existentes.

1.2.4. Formulación del problema

¿Cómo incide el desconocimiento de las vulnerabilidades que existen en los servidores WEB, MAIL y FTP en la seguridad de la información del Hospital Regional Docente Ambato?

1.2.5. Preguntas Directrices

¿Cómo funciona la Técnica Sniffer y su aplicación en la detección de vulnerabilidades en los servidores WEB, MAIL y FTP?

¿Cuáles son las vulnerabilidades a los que los servidores WEB, MAIL y FTP están expuestos?

¿Se podría utilizar la Técnica Sniffer como herramienta informática para detectar las vulnerabilidades de los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato?

1.2.6. Delimitación del Problema

Campo: Seguridad Informática

Área: Servidores y Red Interna

Aspecto: Ataques informáticos

Tiempo: Tiempo previsto para realizar la investigación es de 6 meses.

Lugar: Hospital Regional Docente Ambato, ubicado en la Av. Pasteur y Unidad Nacional de la ciudad de Ambato

1.3. Justificación

Ante la necesidad de utilizar la red como medio de comunicación dentro o fuera del Hospital Regional Docente Ambato se requiere que la información enviada y recibida sea confidencial, integra, no repudiable y que esté disponible para el usuario, por lo que se hace necesario la detección de las vulnerabilidades de los servidores WEB, MAIL y FTP del HRDA para poder contrarrestar cualquier riesgo representativo para la seguridad de la información.

La forma más efectiva de evitar ataques informáticos de cualquier índole en especial de ataques Sniffing es estar enterados de las vulnerabilidades antes de que lo haga un posible intruso. Existen varias técnicas y herramientas dedicadas exclusivamente a la detección de vulnerabilidades de los servidores y de una red, para el desarrollo de este proyecto se utilizó la Técnica Sniffing de manera pasiva y activa para detectar algunas fallas existentes en los servidores seleccionados, esta técnica es de gran valor ya que la mayoría de atacantes utilizan para capturar usuarios y contraseñas, es decir cualquier texto que viaja en claro por la red, aunque esta técnica es muy limitada existen herramientas que permiten realizar otros ataques que nos ayudarán para este análisis aportando así a la seguridad de la información de la institución.

El desarrollo de este proyecto fue de alto impacto para el HRDA porque se tuvo el conocimiento y un registro de las vulnerabilidades existentes en los servidores WEB, MAIL y FTP que nos permitió analizar la Técnica Sniffing, sirviendo como base al administrador de la red para la toma de decisiones y salvaguardar la integridad de la red permitiendo minimizar el riesgo de intrusiones a los datos o la información que circula por la red del Hospital Regional Docente Ambato.

El proyecto de investigación fue factible de realizarse ya que dentro del ambiente de Seguridad Informática existen varias herramientas de software libre que ayudarán al desarrollo de la solución del problema. Siendo el HRDA el primer beneficiario y sus usuarios que manejan la información permitiendo que está sea confiable, integra y oportuna.

1.4 Objetivos

1.4. 1. Objetivo General

Detectar las vulnerabilidades en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato aplicando la Técnica Sniffer como mecanismo de detección.

1.4.2. Objetivos específicos

- Analizar la Técnica Sniffing y su aplicación en los servidores WEB, MAIL y FTP.
- Determinar las vulnerabilidades a los que están expuestos los servidores WEB, MAIL y FTP.
- Plantear una propuesta que permita mediante la Técnica Sniffing detectar las vulnerabilidades en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato.

CAPITULO II

MARCO TEORICO

2.1. Antecedentes investigativos

En la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la UTA posee dentro de sus archivos una variedad de trabajos de investigación por ex alumnos de la Facultad, aunque los trabajos de seguridad informática se están realizando en estos últimos años se encontró un tema similar al propuesto el cual fue realizado por el Señor Diego Olivo Silva Lascano, que utilizo el tema, "ESQUEMAS DE SEGURIDAD EN LA RED PARA LA COMUNICACIÓN INTERNA Y HACIA EL INTERNET DE LA DIRECCIÓN PROVINCIAL DE SALUD DE TUNGURAHUA, 2011", que reposa en la biblioteca de la facultad, teniendo como conclusiones:

- La estructura lógica de la red no es la adecuada, porque permite un libre acceso entre los equipos de los usuarios.
- El acceso a internet tiene un control muy básico, razón por la cual se pueden burlar fácilmente las reglas de control de acceso.
- El firewall de Windows que se maneja en el servidor de red, lo torna altamente vulnerable a ataques e infecciones de virus.
- No cuenta con un servidor de archivos, y los usuarios realizan la compartición de los mismos de forma incorrecta ocasionando problemas con pérdida de archivos, y también difusión de virus.
- El equipo servidor, no cuenta con las características necesarias para su desempeño óptimo, se encuentra obsoleto y además se lo utiliza para tareas extras tornándolo muy sobrecargado y lento.
- Al realizar descargas o actualización de antivirus el internet se torna muy lento, porque no existe un control en el consumo de ancho de banda.

2.2. Fundamentación legal

La fundamentación legal que se obtuvo para el desarrollo de este proyecto son:

Norma ISO 27001:2005

Esta norma fue aprobada a nivel internacional en octubre de 2005 por Organización Internacional de Estandarización y por la Comisión International Electrónica.

Son normas y estándares que permite la seguridad de la información. Por tanto, podría considerarse que ISO 27001 representa la "calidad de la seguridad".

El objetivo de la seguridad de la información es preservar su:

- **Confidencialidad:** evitar que la información sea utilizada por individuos o procesos no autorizados.
- **Integridad:** proteger la precisión y completitud de cualquier cosa que posee valor para una organización.
- **Disponibilidad:** información accesible y utilizable bajo petición de las entidades autorizadas.

El objetivo fundamental es proteger la información de las empresas o instituciones para que no caiga en manos incorrectas o se pierda para siempre.

ISO 27001 establece los requisitos que debe cumplir un Sistema para la Gestión de la Seguridad de la Información (SGSI) para su certificación en términos de procesos de seguridad a nivel empresarial como lo especifica en el Anexo A (A 5 - A 15) de la norma ISO 27001 descritos en el ANEXO Nº 01 del proyecto.

USO DE SOFTWARE LIBRE

Decreto Ejecutivo 1014, Registro Oficial 119 de 10 de abril del 2008
Rafael Correa Delgado

PRESIDENTE CONSTITUCIONAL DE LA REPUBLICA

Decreta:

Considerando:

La real ventaja del Software Libre es que la adquisición del programa permite libertad al usuario. Desde la parte funcional permite que se instale en el número de máquinas que se requiera, sin la necesidad de pagar por nuevas licencias de uso.

Decreta:

El día miércoles 23 de abril del 2008 el actual Presidente de la República Rafael Correa, que todas las instituciones públicas deben utilizar software libre para el funcionamiento tecnológico. Ley detallada en el ANEXO Nº 02.

LEY DE TRANSPARENCIA Y ACCESO A INFORMACIÓN PÚBLICA

Decreto Ejecutivo 2471, Registro Oficial 507 de 19 de Enero del 2005
Lucio Gutiérrez Borbúa

PRESIDENTE CONSTITUCIONAL DE LA REPUBLICA

Considerando:

Que la Constitución Política de la República, en el artículo 81, establece que el Estado garantizará el derecho a acceder a fuentes de información y no existirá reserva respecto de informaciones que reposen en archivos públicos, excepto de los documentos para los que tal reserva sea exigida por razones de defensa nacional y por causas expresamente establecidas en la ley;

Decreto Ejecutivo 2471, Registro Oficial 507 de 19 de Enero del 2005
Lucio Gutiérrez Borbúa

PRESIDENTE CONSTITUCIONAL DE LA REPUBLICA

Decreta:

Expedir el REGLAMENTO GENERAL A LA LEY ORGANICA DE TRANSPARENCIA Y ACCESO A LA INFORMACION PUBLICA, se detalla en el ANEXO Nº 03

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS

(Decreto No. 3496)

Gustavo Noboa Bejarano

PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

Considerando:

Que, el uso de sistemas de información y de redes electrónicas, incluida la Internet ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado.

Que, es necesario impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos.

Que, se debe generalizar la utilización de servicios de redes de información e Internet, de modo que éstos se conviertan en un medio para el desarrollo del comercio, la educación y la cultura.

Que, a través del servicio de redes electrónicas, incluida la Internet se establecen relaciones económicas y de comercio, y se realizan actos y contratos de carácter civil y mercantil que es necesario normarlos, regularlos y controlarlos, mediante la expedición de una Ley especializada sobre la materia.

Que, es indispensable que el Estado Ecuatoriano cuente con herramientas jurídicas que le permitan el uso de los servicios electrónicos, incluido el comercio electrónico y acceder con mayor facilidad a la cada vez más compleja red de los negocios internacionales.

En uso de sus atribuciones, expide la siguiente:

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS, detallada ANEXO Nº 04.

2.3. Categorías Fundamentales

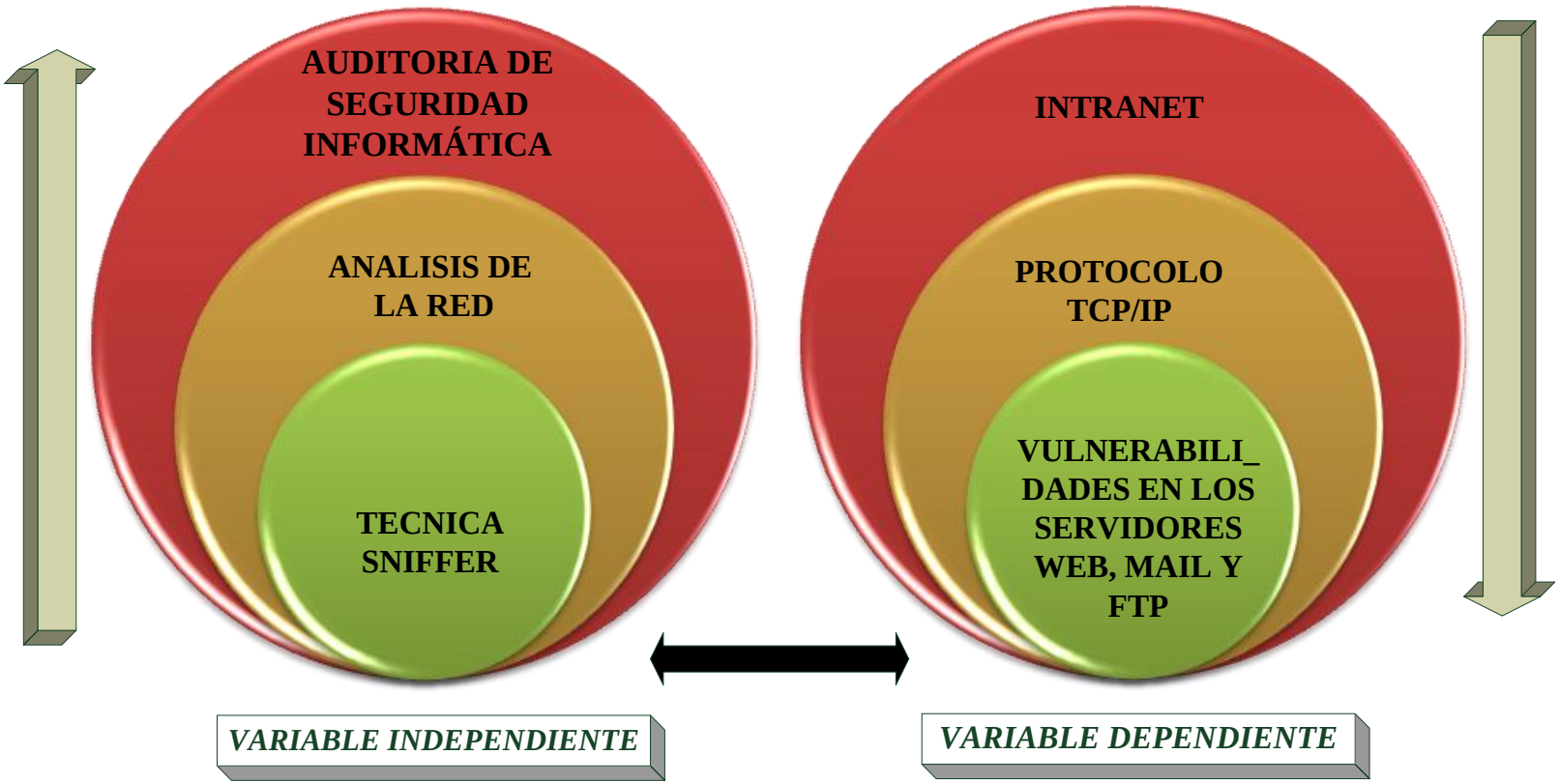

Figura Nº 2.1: Categorías Fundamentales
Autor: Fernanda Conterón

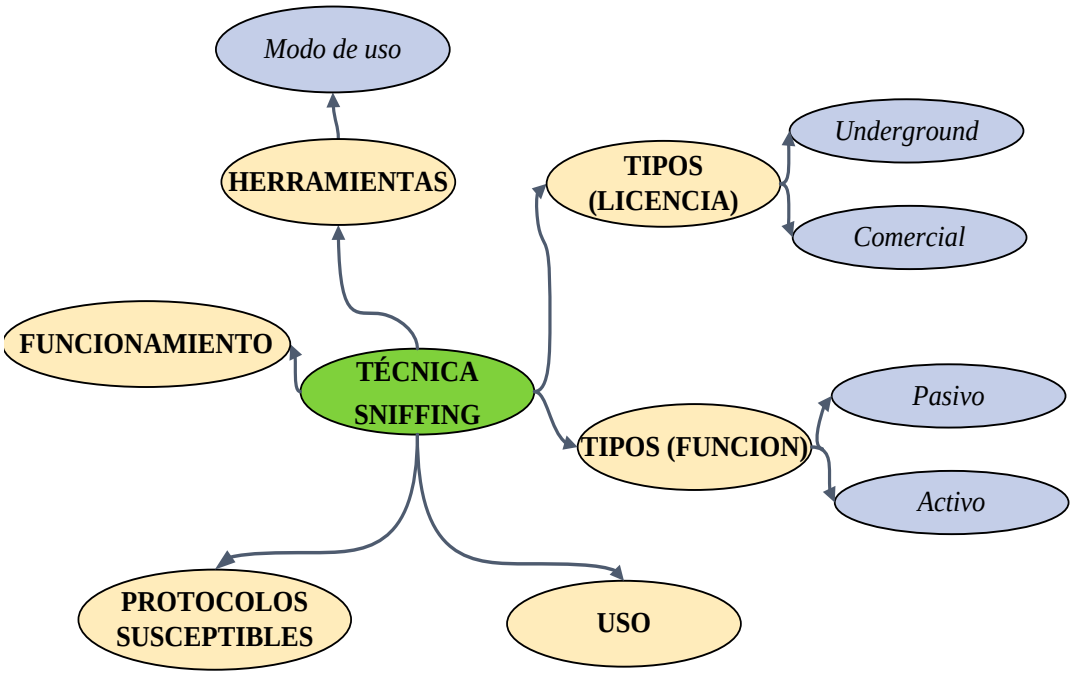

Figura Nº 2.2: Categorías Fundamentales (Subordinación-Variable Independiente)
Autor: Fernanda Conterón

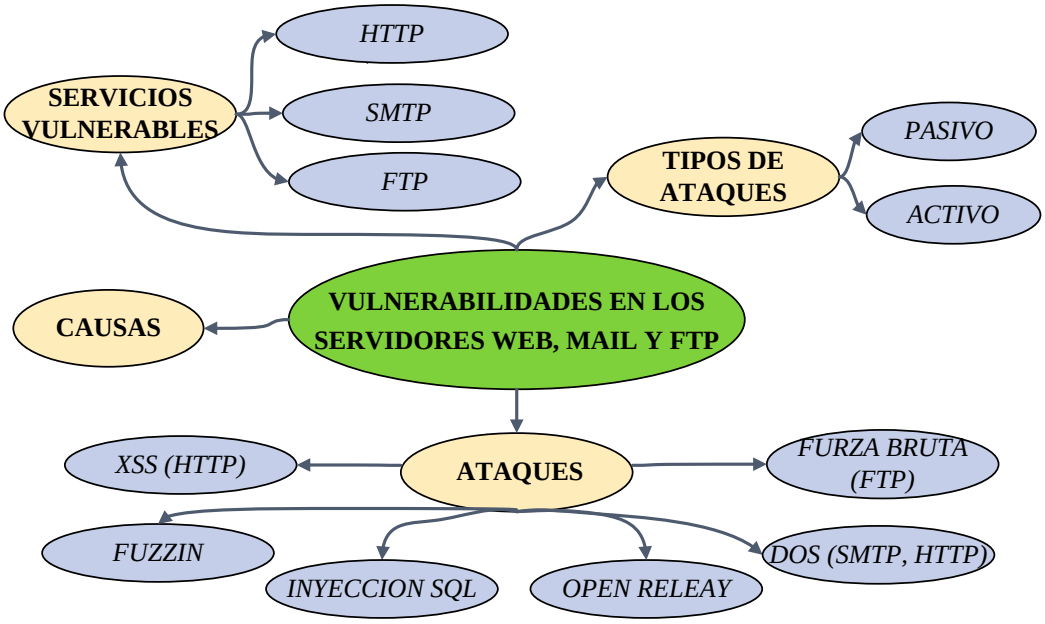

Figura Nº 2.3: Categorías Fundamentales (Subordinación-Variable Dependiente)
Autor: Fernanda Conterón

2.3.1. Auditoria de seguridad informática o auditoría de seguridad de sistemas de información (SI)

COSTAS, Jesús (2011, "29") dice que una auditoria informática o auditoria de seguridad de sistemas de información (SI) es el estudio que comprende el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servicios. Una vez obtenido los resultados, se detallan, se archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo, siguiendo siempre un proceso secuencial que permite a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Las auditorias de seguridad de SI permiten conocer en el momento de su realización cual es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

Aspectos de la seguridad

Los conceptos confidencialidad, integridad o disponibilidad son muy comunes en el ámbito de la seguridad y aparecen como fundamentales en toda arquitectura de seguridad de la información, ya sea en el ámbito de la protección de datos, normativa vigente relacionada con la protección de datos de carácter personal, como códigos de buenas prácticas o recomendaciones sobre gestión de la seguridad de la información y de prestigiosas certificaciones internacionales, estas últimas, relacionadas con la auditoría de los sistemas de información.

Junto a estos tres conceptos fundamentales se suelen estudiar conjuntamente la autenticación y el no repudio en los sistemas de información.

Confidencialidad

Se trata de la cualidad que debe poseer un documento o archivo para que este sólo se entienda de manera comprensible o sea leído por la persona o sistema que este autorizado.

De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y solo si puede ser comprendido por la persona o entendida a quien va dirigida o este autorizada. En este caso de un mensaje esto evita que exista una interpretación de éste y que pueda ser leído por una persona no autorizada.

Integridad.

La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original. Aplicando a las bases de datos seria la correspondencia entre los datos y los hechos que refleja.

Disponibilidad

Se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible por los usuarios (o procesos) autorizados cuando éstos lo requieran.

También se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mal operación accidental o situaciones fortuitas o de fuerza mayor.

Autenticación

La autenticación es la situación en la cual se puede verificar que un documento que ha sido elaborado (o pertenece) a quien el documento dice.

Aplicado a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aportar algún modo que se pueda verificar que dicha persona es quien dice ser, a partir de ese momento se considera un usuario autorizado.

La autenticación en los sistemas informáticos habitualmente se realiza mediante un usuario o login y una contraseña o password.

Otra manera de definirlo seria la capacidad de determinar si una determinada lista de personas ha establecido su reconocimiento sobre el contenido de un mensaje.

No repudio

El no repudio irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación.

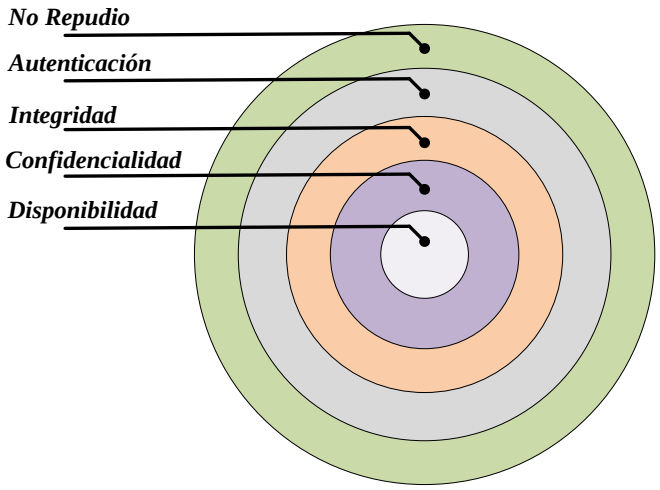

Figura Nº 2.4: Jerarquía de los aspectos de seguridad
Autor: Fernanda Conterón

Fases de una Auditoria

Los servicios de auditoría constan de las siguientes fases:

- Enumeración de redes, topologías y protocolos.
- Identificación de los sistemas operativos instalados.
- Análisis de servicios y aplicaciones.
- Detección, comprobación y evaluación de vulnerabilidades.
- Medidas especificas de corrección.
- Recomendaciones sobre implantación.

2.3.2. Análisis de la red

Seguridad en redes (http://www.monografias.com/trabajos75l-SNIFFERS.htm 14/10/2005; 01/01/2012; 09:45). Las tecnologías de transmisión de datos a través de redes de computadores son el eje central del funcionamiento de un entorno informático que presta servicios de tipo cliente/servidor. Un excelente desempeño de la red trae como consecuencia un aumento de la productividad informática.

El ingreso de nuevos equipos a la red, la existencia de protocolos no necesarios, la mala configuración de equipos activos de red o la de mantenimiento al cableado estructurado y las interfaces de red pueden causar la decadencia del desempeño de la red.

Por medio de pruebas, captura de paquetes, análisis de flujo de información y verificación de la configuración de equipos activos de red (switch, routers), podemos ofrecer una solución óptima para depurar y optimizar el funcionamiento de la red.

2.3.3. Técnica sniffing

Al implantar una red la principal característica es que ésta se segura, configuran firewalls y antivirus pero estos no son suficientes para proteger la información. Hoy en día existen una infinidad de ataques comprometiendo la seguridad de una red.

La Técnica Sniffing se encarga de la captura la información que envía una computadora a otra es decir captura todo los datos o paquetes que circulan por la red de una forma casi desapercibida, por tal razón esta técnica es un arma de doble filo ya que pueden utilizar tanto los administradores de la red como una herramienta para detectar fallos o anomalías de la red pero también puede ser utilizado como un espiador de información por usuarios no autorizados.

2.3.3.1. Sniffer

Para MACLURE, Stuart (2000, "269") los Sniffer eran originalmente herramientas que se utilizaban para depurar los problemas de funcionamiento de la red. En esencia, estas aplicaciones capturan, interpretan y almacenan los paquetes que viajan por la red para analizarlos posteriormente.

De esta forma, los ingenieros que mantienen la red disponen de una ventana para ver lo que está ocurriendo en la misma, permitiéndoles solucionar o modelizar el comportamiento de la red mediante la visión del tráfico de paquetes en su forma menos elaborada.

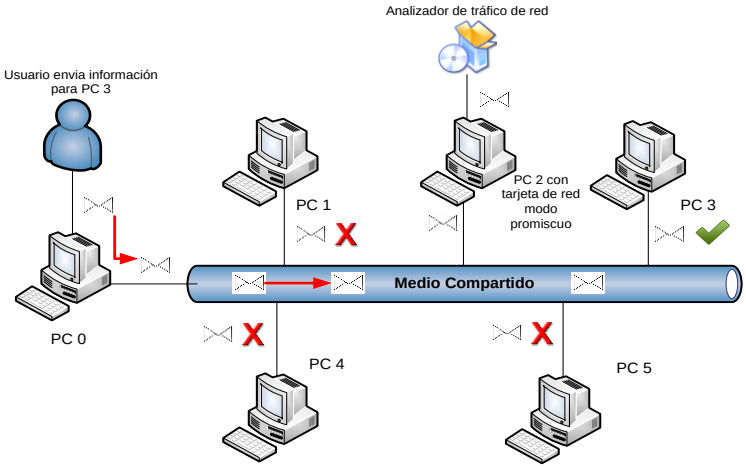

Figura Nº 2.5: Escenario sniffer
Fuente: http://www.internet-solutions.com.co/ser_analisis_trafico.php

2.3.2.2. Tipos de sniffer según licencias

Según su uso se clasifican en:

Sniffers comercial:

Los Sniffers de uso comercial son utilizados por los administradores de redes es decir para el monitoreo y mantenimiento de redes.

Sniffers Underground o de uso ilegal:

Los Sniffers Underground son usados por los crackers para asaltar los ordenadores de una red (robo de información).

2.3.2.3. Tipos sniffer según su función

Pasivo

El sniffing pasivo es el escuchar y capturar tráfico en una red. Donde mejor funciona el sniffing pasivo es en redes de computadoras conectadas al mismo hub y/o conectadas a la misma red inalámbrica (wireless). El sniffing pasivo no se puede detectar.

Activo

El Sniffing activo involucra el realizar ataques al ARP (Address Resolution Protocol) y el inundar el trafico (MAC flooding) para infiltrarse en una red conectada por Hub o por Switch.

ARP spoofing.- El trabajo del ARP es convertir direcciones IP en direcciones MAC. Los ataques al ARP también son conocidos como ARP poisoning (envenenamiento del ARP) y ARP spoofing (suplantación del ARP) ambos se refieren a lo mismo y son las técnicas usadas para atacar redes Ethernet.

El propósito del ARP spoofing es el enviar mensajes ARP falsos a un LAN Ethernet. Estos mensajes contienen direcciones MAC falsas para confundir a los dispositivos de red como los Switches.

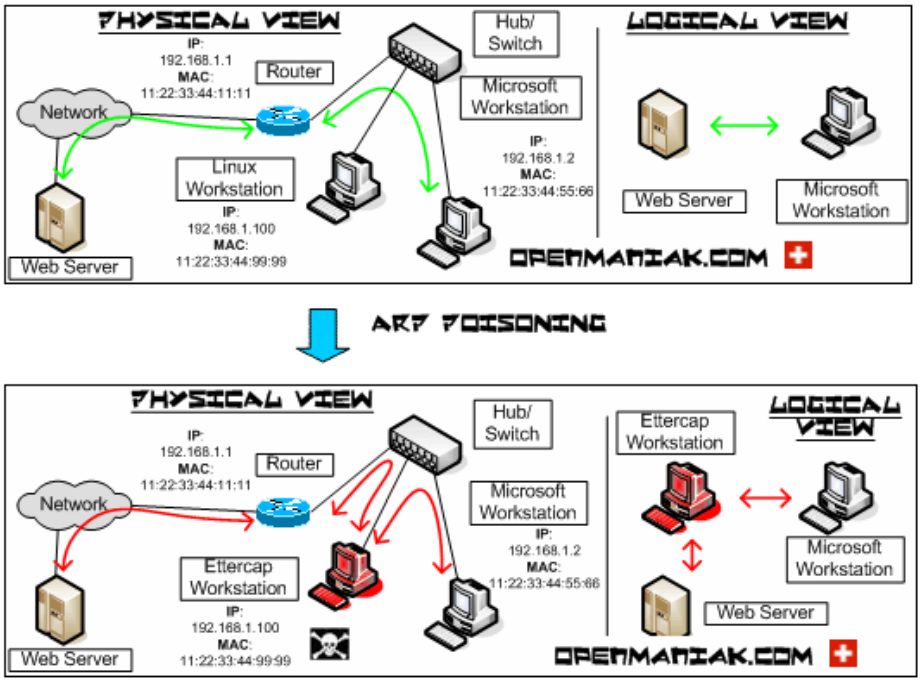

Figura Nº 2.6: Escenario ARP spoofing
Fuente: http://www.internet-solutions.com.co/ser_analisis_trafico.php

MAC flooding

El MAC flooding es el inundar el Switch con tanto trafico que este deja de funcionar como un Switch y empieza a funcionar como un HUB, enviando todo el tráfico a todos los puertos. Este ataque le permite a la computadora donde está conectado el sniffer a capturar todo el tráfico en una red.

2.3.3.4. Protocolos vulnerables al Sniffing

Cualquier protocolo que no está encriptado o cifrado es propenso o vulnerable al Sniffing:

- HTTP
- POP3
- SNMP
- FTP
- NNTP
- IMAP
- Telnet

Estos protocolos son los favoritos de los Hackers por que la data como nombres de usuario y passwords son enviados por estos protocolos en texto plano o claro.

2.3.3.5 Funcionamiento

Segun MACLURE, Stuart (2000, 269), El modo más sencillo de comprender su funcionamiento es examinando la forma en que funciona un sniffer en una red Ethernet.

Un sniffer Ethernet es un software que trabaja en conjunto con la tarjeta de interfaz de la red (NIC, Network Interface Card) para "absorber" indiscriminadamente todo el tráfico que este dentro del "umbral de audición" del sistema de escucha y no sólo del tráfico que se dirige al host que está siendo "aspirado". Normalmente una tarjeta de interface de red (NIC) de Ethernet descartará cualquier trafico que no vaya dirigido a ella o a la dirección de difusión de la red, por lo que el sniffer deberá hacer que la tarjeta entre en ese estado especial denominado *modo promiscuo*, en el que recibirá todos los paquetes que se desplazan por la red.

Una vez que el hardware de la red se encuentre en modo promiscuo, el software del sniffer puede capturar y analizar cualquier tráfico que pase por el segmento local de Ethernet. Esto limita de algún modo el alcance de un sniffer, puesto que no será capaz de captar el trafico externo al dominio local de la red (es decir, más allá de los routers, conmutadores u otros dispositivos de segmentación). Es obvio que un sniffer hábilmente situado en la columna vertebral de la red, en otro punto

de agregación de la red, podrá capturar un volumen mayor de tráfico que otro colocado en un segmento aislado de Ethernet.

2.3.3.6. Uso

Según Mundo Cisco (http://www.rankia.com/foros/consumo/temas/656938-tecnica-sniffing-red 11/12/2002; 30/11/2011:08:00) los principales usos que se le pueden dar a un Sniffer son:

- Captura de contraseñas y nombres de usuario de la red enviadas sin cifrar. Esta capacidad es utilizada en muchas ocasiones por atacantes (malamente conocidos como hackers, para atacar sistemas.
- Para administrar y gestionar la información que pasa a través de una red
- Medición del tráfico, mediante el cual es posible descubrir cuellos de botella en algún lugar de la red.
- Realizar auditoría de redes.
- Prevenir actividades de espionaje industrial.
- Monitorear las actividades de los usuarios de una red.
- Identificar paquetes de datos.
- Identificar estabilidad y vulnerabilidades de las redes LAN.
- Verificar el tráfico de una red y monitorear su desempeño.
- Filtrar los paquetes de acuerdo a la necesidad de cada usuario.
- Realizar capturas en tiempo real, control estadístico de los protocolos.

2.3.3.7. Modo de uso

Como hemos visto anteriormente existen una gama bastante amplia de Sniffers por eso los Sniffer presentan varios modos de uso, desde simples herramientas ligeras y estables diseñadas para trabajar directamente desde la línea de comandos de cualquier plataforma informática, hasta programas completamente visuales que cuentan con frontends bastante detallados con botones, menú de ayuda y representación visual del proceso de monitoreo de la red.

Como utilizarlos depende únicamente de la persona interesada en explotar estas herramientas.

2.3.4. Intranet

Según STRASSBERG, Keith (2002, "50") Las intranets se definen como redes internas sobre las que un usuario o su empresa tiene control. Como punto de referencia formal, la página web www.whatis.com define a una intranet como "una red privada contenida dentro de una empresa. Puede consistir en muchas redes de área local vinculadas entre si, y también utilizar líneas concedidas en la red de área extensa. Normalmente una intranet incluye conexiones a Internet a través de uno o más equipos de puerta de enlace.

El propósito principal de una intranet es compartir la información de una empresa y los recursos informáticos entre los empleados.

Las intranets son las LAN y las WAN que interconectan una empresa; también pueden contener puntos de entrada y salida (extranets e Internet) fuera de su control.

Para aclarar el concepto de una intranet, tenga en cuenta lo siguiente: los usuarios necesitan tener acceso a los datos de la empresa. Sin embargo, no todos los usuarios necesitarán tener acceso a toda la red. Por ejemplo: ¿Necesita el departamento de operaciones tener acceso a los datos sobre los pagos?, ¿Necesita el personal de Recursos Humanos tener acceso a la documentación sobre el servidor y la red?, ¿Necesita el departamento Jurídico tener acceso a los servidores de correo electrónico, excepto para los servicios de correo electrónicos?, ¿Necesita el departamento de ventas tener acceso a la configuración del enrutador o del conmutador? Seguramente la respuesta es *no* en la mayoría de los casos.

Para obtener el nivel más elevado de seguridad, tal vez los administradores deseen clasificar estas redes en dominios de seguridad con diferentes requisitos de seguridad e implementar firewall para controlar y filtrar el tráfico de acuerdo con esa clasificación.

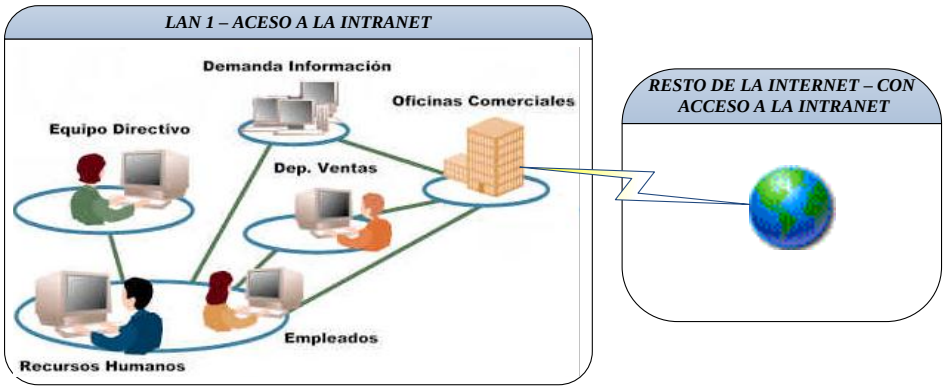

Figura Nº 2.7: Intranet
Autor: Fernanda Conterón

2.3.5. Protocolo TCP/IP

Anónimo (sf; 25/03/20; 12:18:10), El Protocolo de control de transmisión/Protocolo Internet (TCP/IP) es un conjunto de Protocolos aceptados por la industria que permiten la comunicación en un entorno heterogéneo (formado por elementos diferentes). Además, TCP/IP proporciona un protocolo de red encaminable y permite acceder a Internet y a sus recursos. Debido a su popularidad, TCP/IP se ha convertido en el estándar de hecho en lo que se conoce como interconexión de redes, la intercomunicación en una red que está formada por redes más pequeñas. TCP/IP se ha convertido en el protocolo estándar para la interoperabilidad entre distintos tipos de equipos. La interoperabilidad es la principal ventaja de TCP/IP. La mayoría de las redes permiten TCP/IP como protocolo. TCP/IP también permite el encaminamiento y se suele utilizar como un protocolo de interconexión de redes.

Según VELURTAS, Facundo Javier (2009, "20") El protocolo TCP / IP permite la comunicación entre distintos elementos sirve para enlazar computadoras con diferentes sistemas operativos (PC, minicomputadoras y computadoras centrales) sobre redes de área local y área extensa, además permite optimizar la utilización de recursos.

La tarea del protocolo TCP/IP es transmitir paquetes de datos desde la máquina origen a la máquina destino. Esas máquinas que mencionamos normalmente con computadoras y servidores. Todo paquete IP tiene un formato y estructura fija, dentro de él se encuentra la "dirección origen" desde la cual salió el paquete y la

"dirección destino". La "dirección destino" permite a los diferentes router tomar la decisión para orientar ese paquete. Dentro del paquete IP hay muchos campos, cada uno con su función específica. Cuando las máquinas pertenecen al mismo direccionamiento IP (red y marcara iguales) se comunican solo con el protocolo de "capa 2", que usa la "mac-address" "Medium Access Control address" para llevar los paquetes de una máquina a otra. Aparecen en escena los switches y los hubs, los primeros son la evolución de los hubs. Los switches usan esas mac-address para transportar los paquetes por un camino único (en condiciones normales) entre dos o máquinas, en cambio los hubs, son simplemente amplificadores que copian el tráfico entrante en todos sus puertos.

PROTOCOLO TCP/IP

CAPAS	DESCRIPCION	PROTOCOLOS
APLICACION	Define los protocolos de aplicación TCP/IP y cómo se conectan los programas de host a los servicios del nivel de transporte para utilizar la red	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows y otros protocolos de aplicación
TRANSPORTE	Permite administrar las sesiones de comunicación entre equipos host. Define el nivel de servicio y el estado de la conexión utilizada al transportar datos.	TCP, UDP, RTP
INTERNET	Empaqueta los datos en datagramas IP, que contienen información de las direcciones de origen y destino utilizada para reenviar los datagramas entre hosts y a través de redes. Realiza el enrutamiento de los datagramas IP.	IP, ICMP, ARP, RARP
ACCESO A LA RED	Especifica información detallada de cómo se envían físicamente los datos a través de la red, que incluye cómo se realiza la señalización eléctrica de los bits mediante los dispositivos de hardware que conectan directamente con un medio de red, como un cable coaxial, un cable de fibra óptica o un cable de cobre de par trenzado.	Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35

Figura Nº 2.8: Capas protocolo TCP/IP
Autor: Fernanda Conterón

2.3.6. Vulnerabilidades en los servidores WEB MAIL y FTP

2.3.6.1. Vulnerabilidad

Vulnerabilidad es definida según GOMEZ, Diego (2003, Pág. 14) como: la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

Seguridad en redes (http://www.misrespuestas.com/que-es-un-servidor-web.html 14/10/2005; 12/12/11; 08:30), vulnerabilidad es la exposición latente a un riesgo. En el área de informática, existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de troya y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

Son deficiencias de seguridad encontradas del sistema que pueden ser utilizadas para violar las políticas de seguridad.

2.3.7. Servidor

Un servidor, como la misma palabra indica, es un ordenador o máquina informática que está al "servicio" de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a estos, todo tipo de información u ofrece un servicio.

2.3.7.1. Servidor WEB

Para SIERRA, Manuel, (2011, Pág. 5) un servidor web o servidor HTTP es un programa informático que procesa una aplicación del lado del servidor realizando conexiones bidireccionales y/o unidireccionales y síncronas o asíncronas con el cliente generando o cediendo una respuesta en cualquier lenguaje o aplicación del lado del cliente. El código recibido por el cliente suele ser compilado y ejecutado por un navegador web. Para la transmisión de todos estos datos suele utilizarse algún protocolo.

Generalmente se utiliza el protocolo HTTP para estas comunicaciones, perteneciente a la capa de aplicación del modelo OSI. El término también se emplea para referirse al ordenador que ejecuta el programa.

Protocolo HTTP

El Protocolo de Transferencia de HiperTexto (Hypertext Transfer Protocol) es un sencillo protocolo cliente-servidor que articula los intercambios de información entre los clientes Web y los servidores HTTP.

2.3.7.2. Servidor MAIL

Servidor de correo (http://es.scribd.com/doc/8908926/Conceptos-Servidor-de-Correo 02/01/2012: 16:40), Servidor que me permite el intercambio de mensajes de correo electrónico, ya sea entre usuarios, servidores, cliente y servidor. Este servidor almacena y reenvía los mensajes de correo, probablemente esta es la aplicación TCP/IP más usada. Este nos permite mantenernos en contacto con personas de diferentes lugares sin necesidad de hacerlo por medio de cartas, teléfono, etc. Parar llevar a cabo el funcionamiento del servidor de correo son necesarios algunos protocolos como:

SMTP (simple mail transfer protocol/protocolo simple de transferencia de correo), se basa en una entrega punto a punto, un cliente SMTP se contacta con el servidor SMTP del host destino para entregarle directamente el correo, este nos da seguridad en la entrega al receptor ya que espera quesea guardada con éxito. El servidor SMTP administra el correo electrónico saliente y se utiliza en combinación con un servidor POP3 o IMAP de correo electrónico entrante.

POP (Protocolo de oficina de correos) le permite a los clientes obtener los mensajes que se encuentran almacenados en el servidor. El IMAP permite lo mismo pero con la diferencia que cada que voy a descargar el mensaje debo está conectado a Internet mientras que el POP después de descargar el mensaje lo guarda en el disco y puedo abrirlo cuando quiera sin necesidad de estar conectado. Otra diferencia sería que el POP me muestra todos los mensajes, mientras que IMAP me indica que escoja uno por que el otro será almacenado en el servidor.

IMAP (Internet Message Access Protocol) es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión

a Internet., permiten trabajar con los mensajes de correo electrónico sin necesidad de descargarlos antes al equipo.

Puede obtener una vista previa, eliminar y organizar los mensajes directamente en el servidor de correo electrónico, donde se guardan copias de los mismos hasta que el usuario los elimina. IMAP es más frecuente en las cuentas de correo electrónico de empresas.

2.3.7.3. Servidor FTP (File Transfer Protocol)

Es un servicio de la capa de aplicación que nos permite descargarnos archivos y subirlos a un servidor remoto. Actualmente existen infinidad de aplicaciones para todos los S.O. que nos permiten realizar el papel de cliente y conectarnos a los servidores que queramos.

En el intercambio de paquetes FTP entran en juego dos conexiones. La primera es sobre el puerto 21, la conexión de control, por donde se envían los diferentes comandos hacia el servidor y sus respectivas contestaciones. La segunda conexión es la de datos y tal y como su nombre indica, es por donde se envían y se reciben los datos pedidos.

Los servidores de correo trabajan como una agencia de correo postal, sólo que no envían paquetes, sino, datos digitales e información electrónica, la cual llega a su destino de forma casi inmediata.

2.3.8. Causas

- Debilidad en el diseño de los protocolos utilizados en las redes.
- Errores de programación.
- Configuración inadecuada de los sistemas informáticos.
- Política de seguridad deficiente o inexistente.
- Desconocimiento de las herramientas que facilitan los ataques.
- Existencia de puertas traseras.

2.3.9. Tipos de ataques

Los ataques informáticos se pueden clasificar según su comportamiento en pasivos y activos.

2.3.9.1. Ataques pasivos

Los ataques pasivos son aquellos en los que el atacante no altera la comunicación, dedicándose sólo a monitorizar la misma para obtener la información transmitida.

En este tipo de ataques no se modifican los datos por lo que suelen ser difíciles de detectar. Sin embargo, existen herramientas especialmente diseñadas para defenderse de los mismos.

2.3.9.2. Ataques activos

Los ataques activos son aquellos en los que el atacante altera la información transmitida en la comunicación pudiendo subdividirse en las siguientes categorías:

- **Suplantación de Identidad**

En este tipo de ataques el intruso se hace pasar por una identidad distinta a la auténtica.

- **Reactuación**

Mensajes auténticos son capturados y repetidos para producir efectos perjudiciales para el usuario legítimo.

- **Modificación de mensajes**

El mensaje auténtico es modificado ya sea en parte o en su totalidad para producir efectos perjudiciales.

- **Degradación fraudulenta del servicio**

Afecta al correcto funcionamiento de la gestión de recursos y de las comunicaciones informáticas.

2.3.10. Ataques a los servidores WEB, MAIL y FTP

Según el Ing. ESPERANZA, José (2007, pág. 2) loa tipos de ataques son:

2.3.10.1. Ataque Fuzzing

Se llama fuzzing a las diferentes técnicas de testeo de software capaces de generar y enviar datos secuenciales o aleatorios a una o varias áreas o puntos de una aplicación, con el objeto de detectar defectos o vulnerabilidades existentes en el software auditado. Es utilizado como complemento a las prácticas habituales de chequeo de software, ya que proporcionan cobertura a fallos de datos y regiones de código no testados, gracias a la combinación del poder de la aleatoriedad y ataques heurísticos entre otros.

2.3.10.2. Ataque Open Relay (Spam)

Consta en usar el MTA como puente para correos (usualmente spam, aunque pueden ser muchas otras cosas, como los hoax) que de otra manera no podrían llegar a destino, gracias a que los servidores bloquearon la dirección IP de origen.

De esta manera, la gente que manda spam de forma indiscriminada se ve obligada a usar otros servidores para esta tarea. Estos servidores que permiten que se envíe correos a través de ellos, se los denomina Open Relay.

2.3.10.3. Ataque DoS

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.

2.3.10.4. Inyección SQL

Este ataque se basa en manipular el código de programación SQL para ejecutar alguna secuencia en el servidor u obtener información del mismo. La gravedad del ataque puede fluctuar entre obtener información de un simple usuario hasta poder provocar una denegación de servicio

2.3.10.5. Ataque de fuerza bruta

Fuerza Bruta es un tipo de ataque en el que cada posible combinación de las letras son juzgados, números y caracteres especiales hasta que la contraseña correcta se corresponde con el nombre de usuario. La principal limitación de este ataque es el factor tiempo. El tiempo que toma para encontrar la combinación adecuada depende principalmente de la longitud y la complejidad de la password.

2.3.10.6. Ataque XSS

Desarroloweb.com (http://www.desarrolloweb.com/articulos/definicion-y-a-uien-afecta-croos-site-scripting.html 16/11/2006; 01/01/2012; 15:30), El Cross-Site-Scripting es una vulnerabilidad que aprovecha la falta de mecanismos de filtrado en los campos de entrada y permiten el ingreso y envió de datos sin validación alguna, aceptando el envió de scripts completos, pudiendo generar secuencias de comandos maliciosas que impacten directamente en el sitio o en el equipo.

2.4. Hipótesis

Con la aplicación de la Técnica Sniffer se ayudará a la detección de vulnerabilidades en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato.

2.5. Señalamiento de variables

V. Independiente

Técnica Sniffer

V. Dependiente

Vulnerabilidades en los servidores WEB, MAIL y FTP.

CAPITULO III

MARCO METODOLOGICO

3.1 Enfoque

Para el presente trabajo investigativo tomé un enfoque cuali-cuantitativo porque a través de la recolección de datos se llegó a determinar los problemas que se producen cuando existe el desconocimiento de las vulnerabilidades en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato mediante un sniffer. Todos los usuarios de la red fueron beneficiados y el departamento de sistemas fue quien aprobó la aplicación de las medidas y su administración.

3.2 Modalidades básicas de la investigación

La presente investigación tuvo las siguientes modalidades:

Modalidad bibliográfica o documentada: Se consideró esta modalidad ya que se utilizó libros, tesis de grados, internet, biblioteca lo cual nos facilito la obtención de información de distintos punto de vista teniendo un conocimiento general sobre el problema.

Modalidad experimental: Se consideró esta modalidad por la relación de la variable independiente Técnica Sniffer, y su influencia y relación en la variable dependiente detección de las vulnerabilidades de los servidores WEB, MAIL y FTP para considerar sus causas y sus efectos.

Modalidad de campo: Se consideró esta modalidad ya que el investigador fue a recoger la información primaria directamente en el lugar en que se producen los hechos tomando contacto con la realidad a través de una entrevista al Jefe del Departamento de Sistemas y una encuesta al personal al que le afecta directamente el problema.

3.3. Tipos de investigación

Se realizó una investigación exploratoria ya que permitió plantear el problema de la investigación ¿Cómo incide el desconocimiento de las vulnerabilidades que existen en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato en la seguridad de la información? como también de la misma manera permitió plantear la hipótesis.

Se consideró 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 tomó la investigación correlacional ya que permitió medir la compatibilidad de la variable independiente Técnica Sniffer con la variable dependiente vulnerabilidades de los servidores WEB, MAIL y FTP facilitando el estudio dentro de un contexto determinado.

3.4. Población y muestra

La población considerada para la siguiente investigación fueron los usuarios de la red del Hospital Regional Docente Ambato para lo cual se detalla en el siguiente cuadro:

Cuadro N° 3.1: Población

DEPARTAMENTOS	USUARIOS
FARMACIA	5
IMAGENOLOGIA	5
PEDIATRIA	3
LABORATORIO	4
NEONATOLOGIA	2
MATERNIDAD	2
ESPECIALIDADES	3
CUIDADOS INTENSIVOS	2
DIETETICO	2
ESTADISTICA	7
EMERGENCIA	3
AUDITORIO	2
TRAUMATOLOGIA	2
FINANCIERO	6
RECURSOS HUMANOS	4
ADMINISTRACION	6
SISTEMAS	1
TOTAL	**59**

Fuente: Estudio de Campo
Autor: Fernanda Conterón

Dándonos un total de 59 usuarios fundamentales para la investigación.

Cabe destacar que en esta población se encuentra incluido el Jefe de Sistemas del HRDA.

Muestra

Como la población es pequeña se determino que el mismo número de elementos que conforman la población, pasan a conformar la muestra.

3.5. Operacionalización de variables

3.5.1. Variable Independiente: Técnica Sniffer

Cuadro Nº 3.2: Operacionalización de la variable independiente (Técnica Sniffer)

Conceptualización	Categorías	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Técnica Sniffer: Es una técnica que permite monitorear el tráfico de los datos a través de la red.	Monitorear	Anomalías	¿El trafico de red de la institución es monitoreada? ¿Con que frecuencia? ¿Qué herramienta utiliza para monitorea la red?	Técnicas: *Encuesta:* Con un cuestionario dirigido a los usuarios de la red del HRDA.
	Datos	Nivel de seguridad	¿Al monitorear la red ha encontrado algún tipo de anomalías? ¿Al transferir la información por la red interna de la institución, cuales son los niveles de confiabilidad, confidencialidad e integridad en la transferencia de datos? ¿Se ha tenido pérdidas, destrucción o alteraciones en la información almacenada en los computadores a la cual solo los usuarios tienen acceso?	*Entrevista:* Con una cédula de entrevista dirigida al Jefe del Departamento de Sistemas del HRDA
	Red	Estructura	¿Cómo está estructurada la red interna?	

Autor: Fernanda Conterón

3.5. 2. Variable Dependiente: Vulnerabilidad en los servidores WEB, MAIL y FTP

Cuadro Nº 3.3: Operacionalización de la variable dependiente (Vulnerabilidad en los servidores WEB, MAIL y FTP)

Conceptualización	Categorías	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Vulnerabilidad en los servidores WEB, MAIL y FTP: Son deficiencias o agujeros de seguridad encontradas en una red que pueden ser utilizadas para violar la seguridad y cometer intrusiones.	Deficiencias o agujeros de seguridad Seguridad Intrusiones	Control de acceso Configuración Software no actualizado Políticas de seguridad Ataques Protocolos vulnerados	¿Existe un control en el acceso a la manipulación de los servidores de la red? ¿Cree que los servidores WEB, MAIL y FTP están configurados de acuerdo a la seguridad requerida para proteger la información? ¿El sistema operativo o software implementado en los servidores WEB, MAIL y FTP consta de políticas de actualización necesarias para su correcto funcionamiento? ¿El Departamento de Sistemas del Hospital Regional Docente Ambato consta de políticas de seguridad para su funcionamiento? ¿La red ha sido víctima de ataques de escaneo de tráfico? ¿Cuáles son los protocolos o puertos que han sido vulnerados con más frecuencia?	Técnica: *Encuesta:* Con un cuestionario dirigido a los usuarios de la red del HRDA. *Entrevista:* Con una cédula de entrevista dirigida al Jefe del Departamento de Sistemas del HRDA

Autor: Fernanda Conterón

3.6. Recolección y análisis de la información

Cuadro Nº 3.4: Recolección y análisis de la información

SECUNDARIA	PRIMARIA
Se recolectó los estudios realizados anteriormente, se encuentra registrado en documentos y material impreso: libros, informes técnicos, tesis de grado. Las fuentes de investigación son: bibliotecas e internet.	Se recolectó directamente del personal responsable del uso de la red del Hospital Regional Ambato.

Autor: Fernanda Conterón

Técnicas de investigación

Cuadro Nº 3.5: Técnicas de investigación

BIBLIOGRÁFICAS	DE CAMPO
Permitieron recolectar información secundaria que se encuentran registradas en: libros, informes técnicos, internet, etc. El análisis de documentos (Lectura científica).	Permitió recolectar la información primaria: • La entrevista • La encuesta

Autor: Fernanda Conterón

Recolección de la información

Cuadro Nº 3.6: Recolección de la información

PREGUNTAS	EXPLICACIÓN
1. ¿Para qué?	Recolección de información primaria para comprobar y contrastar con la hipótesis
2. ¿A qué personas o sujetos?	La población se tomara del personal responsable del uso de la red del Hospital Regional Ambato
3. ¿Sobre qué aspectos?	- Técnica Sniffer - Vulnerabilidad de los servidores WEB, MAIL y FTP
4. ¿Quién?	**Investigadora:** Fernanda Conterón
5. ¿Cuándo?	De acuerdo al cronograma establecido
6. ¿Lugar de recolección de la información?	Hospital Regional Docente Ambato
7. ¿Cuántas veces?	Una sola vez
8. ¿Qué técnicas de recolección?	- Entrevista - Encuesta
9. ¿Con que?	- Cedula de entrevista - Cuestionario
10. ¿En qué situación?	Situación normal cotidiana

Autor: Fernanda Conterón

3.7. Procesamiento y análisis de la información

Procesamiento:

- Revisión crítica de la información recogida, es decir limpieza de información defectuosa, contradictoria, incompleta, no permitente, etc.
- Repetición de la recolección, en casos para corregir fallas de contestación.
- Tabulación o cuadros según variables de cada hipótesis.
- Cuadro de cartas de control: por variables, por atributos.
- Manejo de la información estudio estadístico de datos para presentación de resultados.
- Una vez aplicados los instrumentos y analizada la validez, se procedió a la tabulación de datos cualitativos y cuantitativos los cuales se presentaron gráficamente en términos de porcentajes a fin de facilitar la interpretación.
- Acto seguido se procedió al análisis integral, enriquecido gracias a los elementos de juicio desprendidos del marco teórico, objetivos y variables de la investigación.
- A continuación se efectuó la estructuración de conclusiones y recomendaciones que organizadas en una propuesta lógica y factible, permitieron participar proactivamente en la solución o minimización de la problemática planteada.
- Finalmente, como parte medular de la investigación crítica propositiva, se estructura una propuesta pertinente al tema de investigación que nos compete.

Análisis e interpretación de resultados:

- Análisis de los resultados estadísticos, destacando tendencias relacionadas fundamentalmente de acuerdo con los objetivos e hipótesis.
- Interpretación de los resultados, con apoyo del marco teórico, en el aspecto pertinente.
- Comprobación de hipótesis, para la investigación estadística conviene seguir la asesoría de un especialista.
- Establecimiento de conclusiones y recomendaciones.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Situación actual del Hospital Regional Docente Ambato

HOSPITAL REGIONAL DOCENTE AMBATO

El Hospital Regional Docente Ambato está formado por un edificio donde funcionan varios departamentos de carácter administrativo, financiero, médicos, entre otros, ubicado en la provincia de Tungurahua en el cantón Ambato parroquia la Merced en las calles Av. Pasteur y Unidad Nacional.

Figura Nº 4.1: Hospital Regional Docente Ambato
Fuente: Diario La Hora

A continuación se detallan las diferentes oficinas que forman parte de la institución conformado por tres plantas, las cuales se distribuyen:

Planta Baja

Estadística, Emergencia, Laboratorio, Imagenología, Farmacia, Recursos Humanos, Financiero, Traumatología, Cuidados Intensivos.

Primer Piso

Departamento de Administración, Maternidad, Neonatología, Especialidades.

Segundo Piso

Departamento de sistemas, Biblioteca, Auditorio, Pediatría.

4.1.1 Análisis de la Situación Actual

El Hospital Regional Docente Ambato cuenta con el Departamento de Sistemas, encargado de la operatividad en hardware y software; manejando de forma estructurada la red que consta de servidores con plataformas de trabajo Windows Server 2003 y Linux Centos 5 y con número considerable de computadores cliente con sistema operativo Windows XP y algunos con Windows Vista.

La estructura básica de la red está basada en la implementación de redes de área local, desde el Departamento de Sistemas parten los ramales que recorre el Edificio para establecer la conexión desde el nivel más bajo hasta el último piso, luego, en cada piso, se ramifica y llega a las diferentes oficinas.

Los computadores en su mayoría están protegidos por un antivirus corporativo el mismo que es administrado de forma centralizada desde el Centro de Cómputo de la Institución.

En cuanto a la parte técnica de la Red del Hospital Regional Docente Ambato, se puede decir que en lo que corresponde a las capas físicas y de enlace de datos se usa el estándar IEEE 802.3 (o protocolo Ethernet) y en lo que corresponde a las capas de red y transporte de datos el protocolo TCP/IP

En cuanto al cableado se puede decir que el más utilizado en las instalaciones que conforman la red del Hospital Regional Docente Ambato, es el par trenzado UTP (Unshielded Twisted Pair), 100baseT.

En la configuración de par trenzado UTP la conexión conforma una topología mixta tipo árbol y estrella.

Además se da acceso a Internet a los usuarios por medio del firewall, controlándolos a través de la dirección IP Tables (IP y Mac address de cada uno de los equipos).

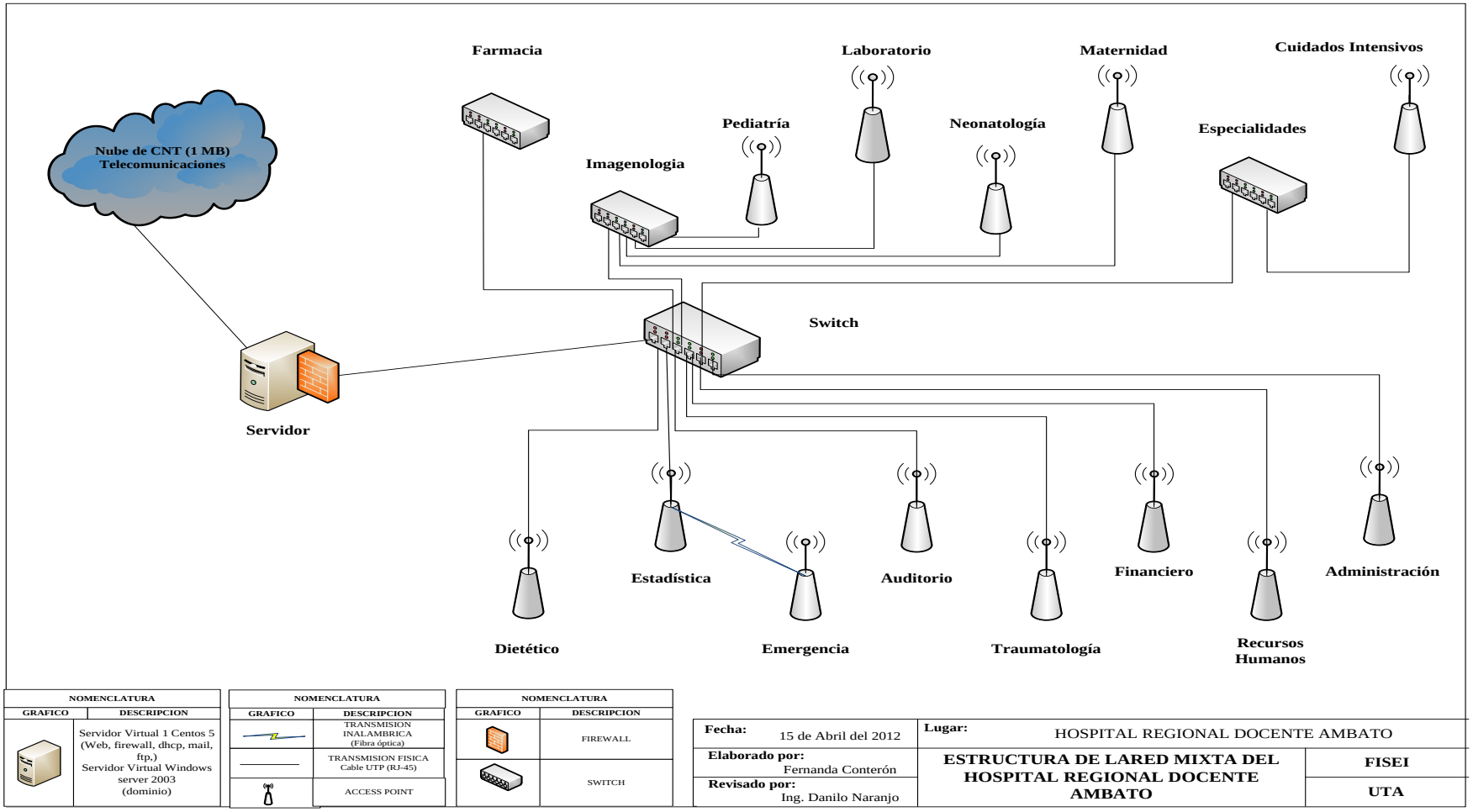

Figura Nº 4.2: Estructura de la red del Hospital Regional Docente Ambato
Autor: Fernanda Conterón

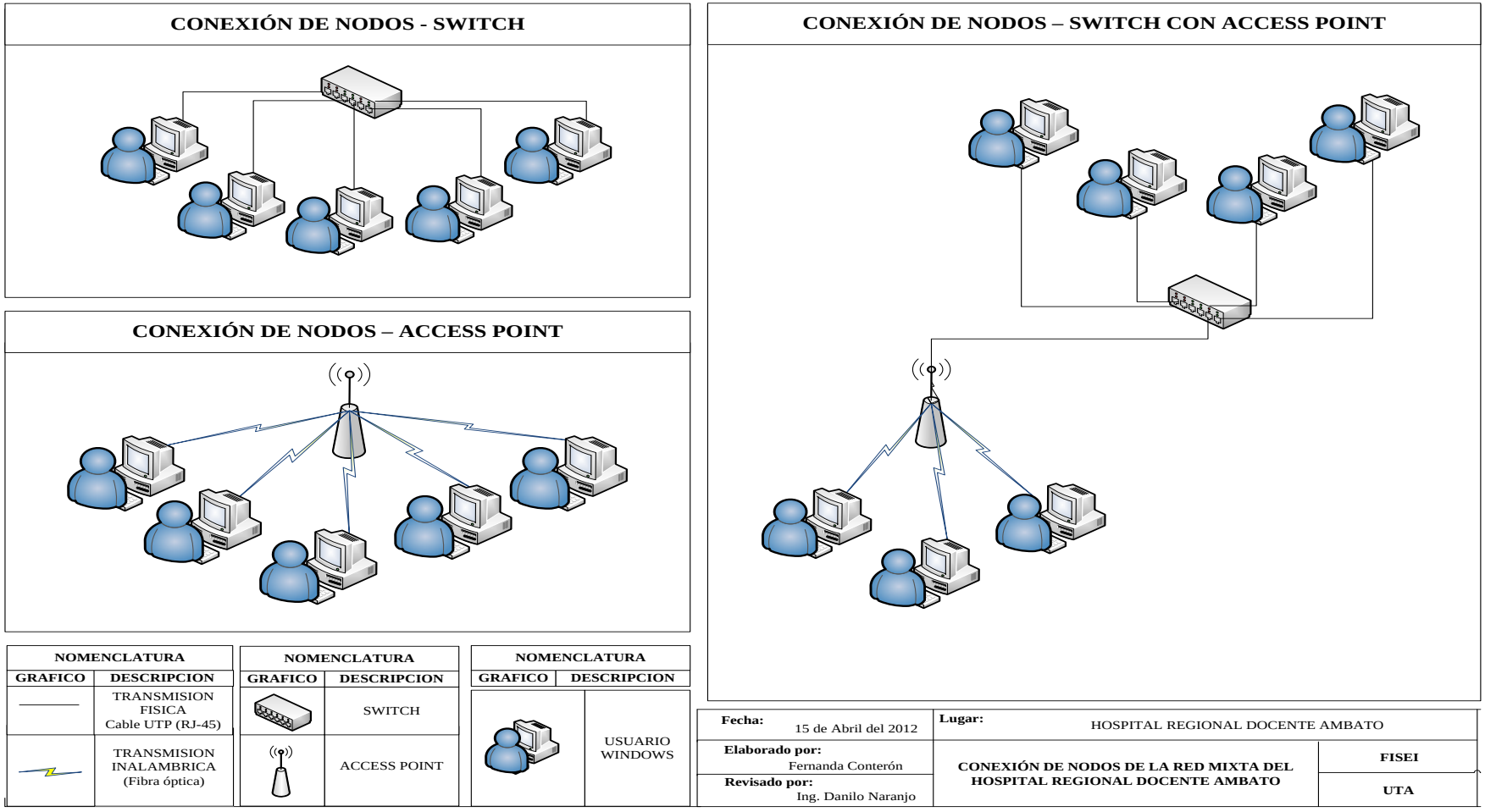

Figura Nº 4.3: Conexión de los nodos de la red del Hospital Regional Docente Ambato
Autor: Fernanda Conterón

La conexión del nodo por medio de un switch conforma el área de:

Cuadro Nº 4.1: Conexión de nodos por medio de switch

ÁREA	MÁQUINAS	CLIENTES
Farmacia	5	2 Dispensación 2 Farmacias 1 1 Bodega
Especialidades	3	1 Gastroenterología 1 Especialidades 1 Urología
Imagenlogía	5	1 Rayos X 1 Ecos 2 Trabajo Social

Autor: Fernanda Conterón

Las conexiones de los nodos por medio de **Access Point,** conforman las áreas de**:**

Cuadro Nº 4.2: Conexión de nodos por medio de Acces Point

ÁREA	MÁQUINAS	CLIENTES
Dietético	2	2 Dietético
Estadística	7	3 Ingresos 4 Estadística
Emergencia	3	1 Emergencia 2 Primera acogida
Auditorio	3	1 Biblioteca 2 Sistemas
Traumatología	2	2 Traumatología
Financiero	5	5 Financiero
Recursos Humanos	4	4 RR HH
Administración	6	3 Administración 1 Subdirección 1 Secretaria 1 Enfermería

Autor: Fernanda Conterón

Y las conexiones por medio de switch enlazados a un Access Point son:

Cuadro Nº 4.3: Conexiones por medio de Switch enlazados a un Access Point

ÁREA	MÁQUINAS	CLIENTES
Pediatría	3	2 Pediatría 1 Clínica
Laboratorio	4	2 Laboratorio 1 Soat 1 Hemoteca
Neonatología	2	1 Neonatología 1 Banco de leche
Maternidad	2	1 Maternidad
Cuidados intensivos	2	2 Unidad de cuidados intensivos

Autor: Fernanda Conterón

Las cuatro primeras áreas parten del switch de **Imagenologia** y la ultima del switch de **Especialidades**

4.2 Análisis e interpretación de resultados de la entrevista realizada al jefe del Departamento de Sistemas del Hospital Regional Docente Ambato

La entrevista que se realizo según el ANEXO Nº 05 estuvo dirigida al Jefe del Departamento de Sistemas del Hospital Regional Docente Ambato, con preguntas abiertas relacionadas con las vulnerabilidades, los ataques que ha sufrido esta red, y los servidores que han sido vulnerados para aclarar el problema y las causas que la provoquen.

Las preguntas con sus respectivas respuestas, realizadas al Jefe del Departamento de Sistemas del Hospital Regional Docente Ambato fueron las siguientes:

1. **¿Cree Ud. que la red interna del Hospital Regional Docente Ambato es vulnerable a ataques Sniffing?**

   Si, sospecho que una persona que tenga los conocimientos informáticos suficientes lo puede hacer fácilmente.

2. **¿Ha utilizado algún medio para detectar dichas vulnerabilidades?**

   No, no se ha ejecutado ningún mecanismo para detectar dichas vulnerabilidades.

3. **¿Cree Ud. necesario tomar medidas para la detección de vulnerabilidades?**

   Si, es de suma importancia detectar cuales son las vulnerabilidades en esta red, en especial las vulnerabilidades que pueden tener los servidores WEB, MAIL y FTP ante un ataque Sniffing ya que por medio de ellos se transmite información de mucha importancia para la institución, no se ha implementado ningún método para la detección por falta de tiempo y desconocimiento entorno a la aplicación de la herramienta.

4. **¿Los datos que se transmite por la red interna están encriptados?**

   No, los datos que se transmite a través de la red no están encriptados estos viajan en texto plano y cualquier intruso puede capturarlos y perjudicar en forma personal, grupal o directamente a la institución

5. **¿Alguna vez se ha comprometido la confidencialidad, integridad y disponibilidad de la información y de los servicios dentro de la institución?**

   Si, si se ha visto comprometida la red ya que a sufrido ataque de denegación de servicios y se han robado una contraseña de un usuarios del departamento financiero y frecuentemente conflictos de IP.

6. **¿Existen políticas de seguridad dentro de la institución?**

   En realidad no existe un documento que sustente las políticas de seguridad que deberían existir dentro de la institución, pero cada usuario se le ha comunicado las restricciones que posee para el uso de la red.

7. **Usted estaría interesado en que se utilice la Técnica Sniffing como mecanismo para detectar las vulnerabilidades que existen en los servicios WEB, MAIL y FTP de la red del HRDA simulando ser un atacante?**

   Si, es lo que el HRDA necesita, ya que la aplicación de dicho programa me permitirá tener una idea clara de lo que puede realizar un atacante dentro de la red y con ello nos ayudara para detectar las vulnerabilidades que existen actualmente en los servidores WEB, MAIL y FTP mediante esta técnica, y así, tener conocimiento y realizar un informe técnico con los problemas y sus posibles soluciones a cada una de las vulnerabilidades.

Interpretación

De acuerdo a la entrevista realizada al Jefe del Departamento de Sistemas manifiesta que la red del Hospital Regional Docente Ambato es vulnerable a ataques Sniffing ya que los datos transmitidos a través de la red no cuentan con un método de encriptación y estos viajan en texto plano y cualquier intruso puede capturarlos, y hacer daño a la entidad en lo económico o social, además que no se ha realizado ningún estudio de las vulnerabilidades de la red por falta de tiempo y desconocimiento del uso de las herramientas, pero el departamento de sistemas está interesado en la aplicación de la Técnica Sniffer en especial para detectar la vulnerabilidades de los servidores WEB, MAIL y FTP ya que por medio de ellos se transfiere gran cantidad de información y así tener un conocimiento de las actividades que realizaría un intruso por medio de esta técnica.

4.3 Análisis e interpretación de resultados de la encuesta realizada a los usuarios de la red del Hospital Regional Docente Ambato.

Para efectuar la encuesta se utilizo el ANEXO Nº 06 el cual estuvo dirigido a los usuarios de la red del Hospital Regional Docente Ambato con preguntas cerradas relacionadas a la seguridad y trafico de la información que manejan.

Las preguntas con sus respectivas respuestas, realizadas a los usuarios de la red del Hospital Regional Docente Ambato fueron las siguientes.

1. **¿Conoce Ud. que existen programas que pueden espiar o capturar todas las acciones que realiza en su computador y la información que se transmiten por la red?**

Cuadro N° 4.4: Datos de la pregunta 1 de la encuesta

N°	ITEMS	FRECUENCIA	%
1	Si	6	10
2	No	52	90
TOTAL		**58**	**100**

Fuente: Estudio de Campo
Autor: Fernanda Conterón

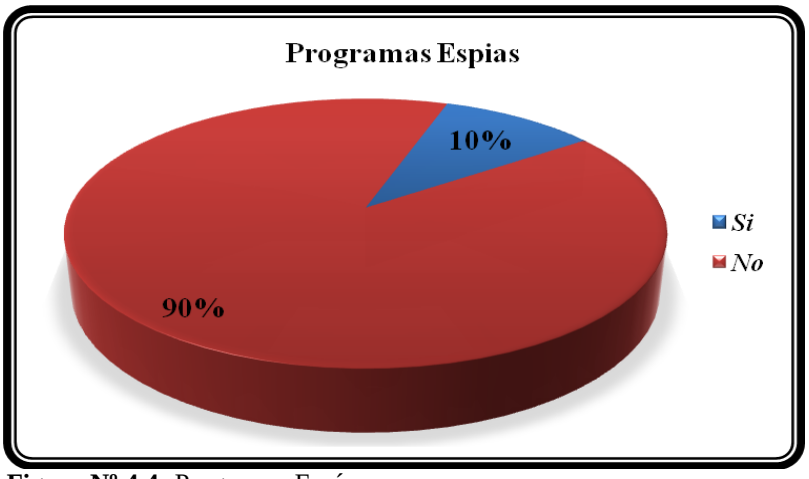

Figura Nº 4.4: Programas Espías.
Fuente: Estudio de Campo
Autor: Fernanda Conterón

De las 58 encuestas realizadas a los usuarios que utilizan la red del HRDA, el 10% que representa a 6 personas indican que si conocen que existen programas que pueden espiar todas las acciones y la información que se transmiten por la red y el 90% que representa a 52 personas manifiestan que no conocen que existen programas para la captura de información.

Interpretación:

Se observa claramente que un alto porcentaje de usuarios de la red no tienen conocimiento que existe en el mercado programas que pueden realizar espionaje a la información que manejan dentro de una red, dicha intrusión puede ser realizada por alguna persona inescrupulosa provocando daños a la red o sacando ventaja de la información obtenida.

2. ¿Ud. cree que al enviar y recibir información (datos o archivos) a través de la red interna del HRDA está seguro contra espionaje informático?

Cuadro N° 4.5: Datos de la pregunta 2 de la encuesta

N°	ITEMS	FRECUENCIA	%
1	Si	13	23
2	No	6	10
3	No sabe	39	67
TOTAL		**58**	**100**

Fuente: Estudio de Campo
Autor: Fernanda Conterón

Figura Nº 4.5: Seguridad contra espionaje
Fuente: Estudio de Campo
Autor: Fernanda Conterón

De las 58 encuestas realizadas a los usuarios que utilizan la red del HRDA, el 23% que representa a 13 personas indican que al enviar o recibir información a través de la red interna de la institución si es segura contra espionajes informáticos, el 10% que representa a 6 personas manifiestan que no es segura y el 68% que representa a 39 personas consideran no saber si al enviar y recibir archivos o datos estos están seguros contra algún espionaje.

Interpretación:

Existe el desconocimiento por parte de los usuarios de la red del HRDA, que al enviar o recibir archivos o datos estos son susceptibles a ser observados, una de estas personas es el administrador de la red o cualquier otra persona con conocimientos de espionaje informático que puede utilizar la información obtenida con fines maliciosos sin q los usuarios estén enterados.

3. **¿Cree Ud. Si sus correos electrónicos o cuentas personales están protegidos contra robo, perdida, espionaje de la información cuando usa la red del HRDA?**

Cuadro N° 4.6: Datos de la pregunta 3 de la encuesta

N°	ITEMS	FRECUENCIA	%
1	Si	10	17
2	No	15	26
3	No sabe	33	57
TOTAL		**58**	**100**

Fuente: Estudio de Campo
Autor: Fernanda Conterón

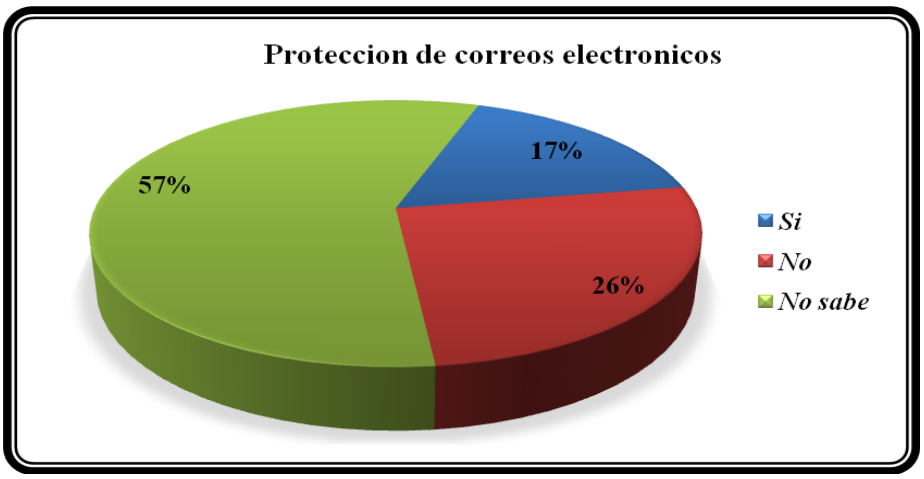

Figura Nº 4.6: Protección de correos Electrónicos
Fuente: Estudio de Campo
Autor: Fernanda Conterón

De las 58 encuestas realizadas a los usuarios que utilizan la red del HRDA, el 17% que representa a 10 personas indican que si creen que sus correos electrónicos o cuentas personales están protegidas, el 26% que representa a 15 personas manifiestan que no saben si sus cuentas al momento de usarlas están protegidas y el 57% que representa a 10 personas no saben si sus correos o cuentas personales están protegidas.

Interpretación:

Dentro de la red del HRDA, los usuarios de la red creen que no existe protección en los correos electrónicos y cuentas personales que utilizan los usuarios entendiendo que estas sean vulnerables a ser robadas, pero no saben el por qué existen o la causa de dichas vulnerabilidades.

4. **Conoce Ud. las políticas de seguridad informáticas para el manejo de la información y de la red del HRDA?**

Cuadro N° 4.7: Datos de la pregunta 4 de la encuesta

N°	ITEMS	FRECUENCIA	%
1	Si	21	36
2	No	37	64
TOTAL		**58**	**100**

Fuente: Estudio de Campo
Autor: Fernanda Conterón

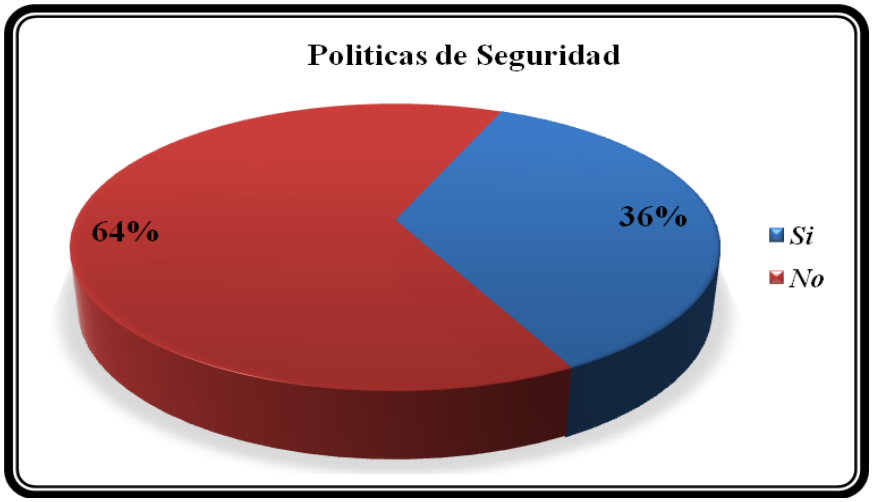

Figura Nº 4.7: Políticas de Seguridad
Fuente: Estudio de Campo
Autor: Fernanda Conterón

De las 58 encuestas realizadas a los usuarios que utilizan la red del HRDA, el 36% que representa a 21 persona indica que conocen las políticas de seguridad informática que maneja el HRDA, pero el 64% que son 37 personas manifiestan que ellos no conocen las políticas de seguridad informática.

Interpretación.

Los usuarios de la red del HRDA no conocen las políticas de seguridad informática que se han preestablecido para el uso de los sistemas y de la red del HRDA provocando que estos usuarios hagan mal uso de los recursos informáticos.

5. **¿Cómo considera Ud. el desempeño (tiempo de respuesta) de la red ante una petición de servicio o recursos (internet, correos, transferencia de archivos, etc…)?**

Cuadro N° 4.8: Datos de la pregunta 5 de la encuesta

N°	ITEMS	FRECUENCIA	%
1	Regular	14	24
2	Mala	19	33
3	Buena	20	34
4	Excelentes	5	9
TOTAL		**58**	**100**

Fuente: Estudio de Campo
Autor: Fernanda Conterón

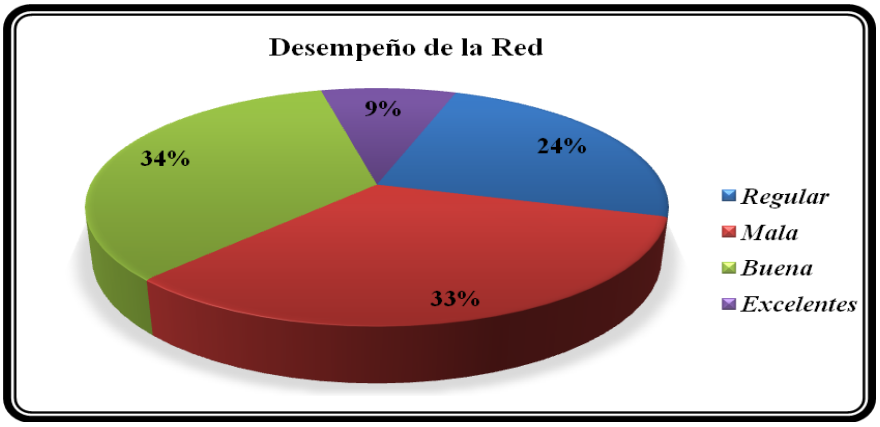

Figura Nº 4.8: Desempeño de la Red
Fuente: Estudio de Campo
Autor: Fernanda Conterón

De las 58 encuestas realizadas a los usuarios que utilizan la red del HRDA, manifiestan que el servicio de la red ante una petición de un recurso o servicio es, el 24% que representa a 14 personas indican que es regular, el 33% que representa a 19 personas indican que es mala, el 34% que representa a 20 personas indican que es buena y el 9% que representa a 5 personas indican que es excelente.

Interpretación:

Se observa claramente que el desempeño (tiempo de respuesta) de la red del HRDA ante una petición de servicio o recursos por Internet es malo y regular, estas interrupciones de servicios pueden ser por ataques de denegación de servicios.

6. ¿Ud. Sabe si la información que está bajo su responsabilidad ha sido?

Cuadro N° 4.9: Datos de la pregunta 6 de la encuesta

N°	ITEMS	FRECUENCIA	%
1	Alterada	4	7
2	Eliminada	13	22
3	Copiada	4	7
4	No ha sucedido nada	18	30
5	No sabe	19	34
TOTAL		**58**	**100**

Fuente: Estudio de Campo
Autor: Fernanda Conterón

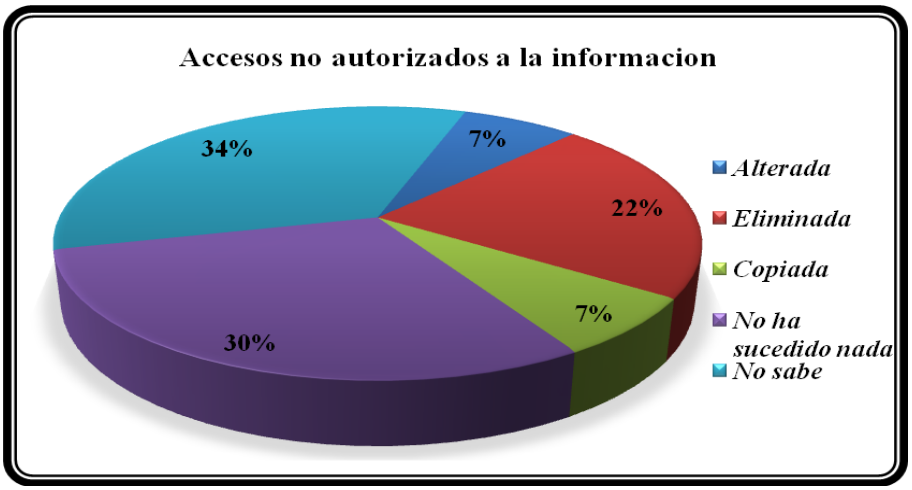

Figura Nº 4.9: Acceso no autorizados a la información
Fuente: Estudio de Campo
Autor: Fernanda Conterón

De las 58 encuestas realizadas a los usuarios que utilizan la red del HRDA, manifiestan que la información almacenada en los equipos han sido los siguientes: el 10% que representa a 6 personas indican que han sufrido alteraciones, el 16% que representa a 9 personas indican que la información ha sido eliminada, el 7% que representa a 4 personas indican que su información ha sido copiada, 33% que representa a 19 personas indican no haber sufrido ningún tipo de acceso a la información, el 34% que representa a 20 personas indican que no saben.

Interpretación:

La información que manejan los usuarios de la red del HRDA ha sufrido algún tipo de manipulación por alguna persona no autorizada.

7. **¿Conoce Ud. que existen sitios web seguros (https) que evitan que la información y claves utilizadas puedan ser plagiadas?**

Cuadro N° 4.10: Datos de la pregunta 7 de la encuesta

N°	ITEMS	FRECUENCIA	%
1	Si	23	40
2	No	35	60
TOTAL		**58**	**100**

Fuente: Estudio de Campo
Autor: Fernanda Conterón

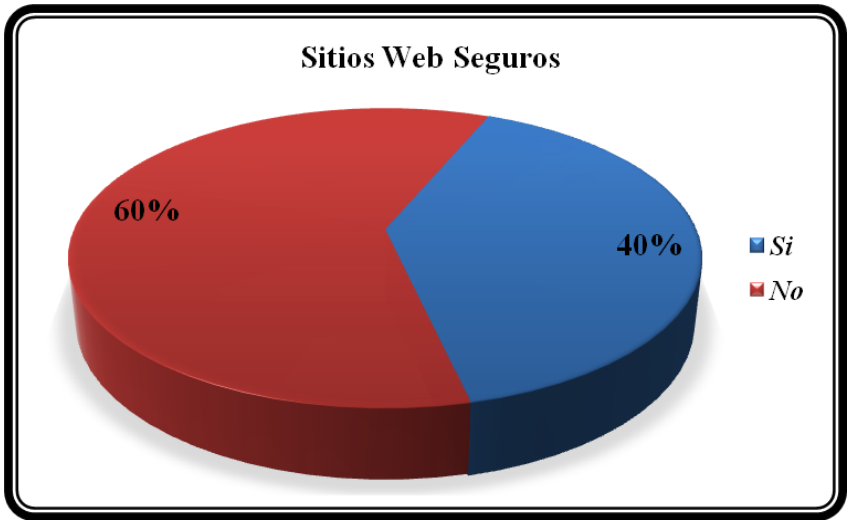

Figura Nº 4.10: Sitios Web Seguros
Fuente: Estudio de Campo
Autor: Fernanda Conterón

De las 58 encuestas realizadas a los usuarios que utilizan la red del HRDA, el 40% que representaron a 23 personas indicaron que si conocen la existencia de sitios web seguros y el 60% que representa a 35 personas indicaron no saber de que existan estos sitios.

Interpretación:

Podemos indicar que los usuarios de la red del HRDA no tienen conocimiento que al manejar Internet existen de los sitios web seguros para evitar robo de información.

8. ¿Sabe Ud. que es y el manejo de un certificado de autentificación que contiene las páginas web seguras?

Cuadro N° 4.11: Datos de la pregunta 8 de la encuesta

N°	ITEMS	FRECUENCIA	%
1	Si	14	7
2	No	44	93
TOTAL		**58**	**100**

Fuente: Estudio de Campo
Autor: Fernanda Conterón

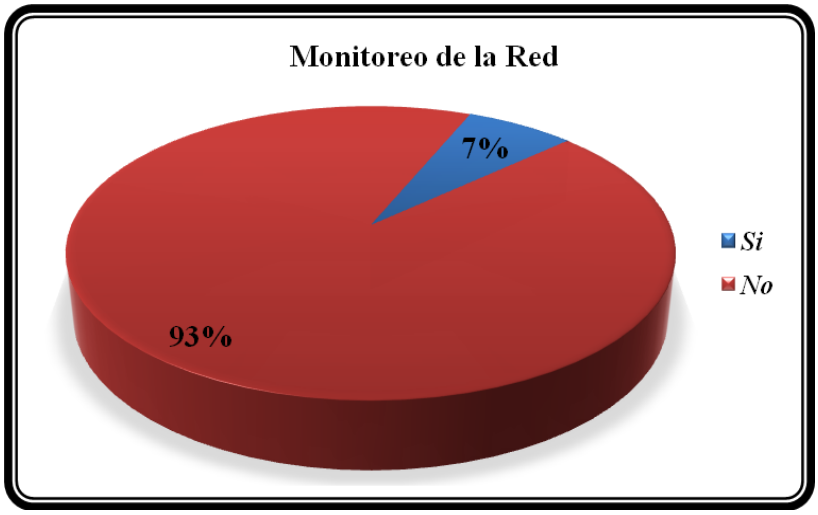

Figura Nº 4.11: Monitoreo de la red
Fuente: Estudio de Campo
Autor: Fernanda Conterón

De las 58 encuestas realizadas a los usuarios que utilizan la red del HRDA, el 7% que representa a 4 personas indican que si conocen de los certificados de autentificación y su manejo que contienen las páginas web seguras y el 93% que representa a 54 personas dicen no saber sobre el tema.

Interpretación:

Se considera que los usuarios de la red y en especial los usuarios que navegan por internet no saben sobre el uso de los certificados de autentificación que utilizan las páginas web seguras provocando que el usuario interceptor conozcan usuarios o claves.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones.

a) De la entrevista realizada al Jefe del Departamento de Sistemas se concluye que la red interna del Hospital Regional Docente Ambato tiene agujeros de seguridad en los servidores WEB, MAIL y FTP y que el departamento de sistemas no ha ejecutado técnica alguna para determinar dichos problemas por desconocimiento del uso de las herramientas que identifiquen dichas vulnerabilidades.

b) De la encuesta realizada a los usuarios de la red interna del Hospital Regional Docente Ambato, se concluye que los usuarios de la red consideran que la seguridad de la misma es muy baja, la información que manejan a través de la red puede estar bajo espionaje, sus contraseñas de cuentas personales han sido robadas y usadas por terceros demostrando que existen vulnerabilidades en los servicios WEB MAIL Y FTP de la red del Hospital.

c) De la entrevista realizada al jefe de Sistemas se concluye que la red del Hospital Regional Docente Ambato ha sufrido ataques snffing ya que los datos transmitidos a través de la red no cuentan con un método de encriptación y estos viajan en texto plano y cualquier intruso puede capturarlos, y hacer daño a la entidad en lo económico o social, además que no se ha realizado ningún estudio de las vulnerabilidades de la red por falta de tiempo.

Recomendaciones.

a) Efectuar un análisis de las herramientas para la selección de la técnica Sniffing adecuada para la detección de las vulnerabilidades existentes en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato.

b) Ejecutar la Técnica Sniffing para encontrar las vulnerabilidades que poseen los servidores WEB, MAIL y FTP de la red del Hospital Regional Docente Ambato.

c) Elaborar un informe técnico de las vulnerabilidades existentes en los servidores WEB, MAIL y FTP encontradas por medio de la Técnica Sniffing de la red del Hospital Regional Docente Ambato y brindar una posible solución a los problemas encontrados.

CAPITULO VI

PROPUESTA

6.1. Datos informativos

- **Titulo:** "Técnica Sniffing para detectar vulnerabilidades en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato"
- **Institución ejecutora:** Hospital Regional Docente Ambato
- **Director de Tesis:** Ing. Francisco López
- **Beneficiarios:** Hospital Regional Docente Ambato
- **Ubicación:** Hospital Regional Docente Ambato, ubicado en la Av. Pasteur y Unidad Nacional de la ciudad de Ambato.
- **Tiempo estimado para la ejecución:**

  Fecha de inicio: Marzo 2012
  Fecha de finalización: Julio 2012

- **Equipo técnico responsable**

  Investigador: Fernanda Conterón
  Jefe de sistemas: Ing. Danilo Naranjo

- **Costo:** $ 939.40 ANEXO Nº 07

6.2 Antecedentes de la propuesta

Los servidores WEB, MAIL y FTP son usados para transferir constantemente información entre clientes y servidores (principalmente web), y la gran mayoría de la información transmitida usando estos servicios es llevada a cabo sin ningún

método de cifrado, por esto la interceptación de dichas transmisiones origina un enorme peligro en la integridad y confidencialidad de los datos. Muchos de estos datos, son usuarios y contraseñas que pueden ser interceptados o alterados fácilmente; la interrupción de los servicios también es otro tema de interés para que no interfiera en la disponibilidad de la información.

En base a la entrevista realizada al Jefe del Departamento de Sistemas se destaca que: el Hospital Regional Docente Ambato no cuenta con ningún medio para la detección de vulnerabilidades de los servidores WEB, MAIL y FTP, en base a la Técnica Sniffing, para así poder disminuir las consecuencias causadas por este ataque y dar un tratamiento correcto en el manejo del tráfico de la información que circula por la red.

Es importante mencionar que en el Hospital Regional Docente Ambato no se han realizado trabajos similares al propuesto y el Departamento de Sistemas ha comprendido que tener un informe técnico en el que se indiquen las vulnerabilidades actuales que tienen los servidores WEB, MAIL y FTP, ayudará a la toma de soluciones y proteger la información aumentando el nivel de seguridad de la red.

6.3. Justificación

Debido a que no se ha establecido un mecanismo para detectar las vulnerabilidades en los servidores WEB, MAIL y FTP por falta de tiempo, la información no está segura, la detección de estas vulnerabilidades es una guía para un mejor tratamiento de la integridad, confidencialidad y confiabilidad de la información y el uso que se le dé a la Técnica Sniffer a es importante de señalar, ya que gracias a esto podemos ayudar a que la información que se transmite por la red tenga más seguridad. Con esto se mejorara los siguientes aspectos:

- **Seguridad de la información**

  Con la aplicación de la Técnica Sniffing ayudara para la seguridad de la información ya que cualquier persona conectado a la red interna y a Internet es una víctima potencial, sin importar a que se dedique, ya que la información

que manejan es vulnerable ante un sniffer y mediante este estudio se podrá mantener informado al administrador para que tome acciones correctivas para que la información no esté expuesta a cualquier intruso o ataque informático.

- **Vulnerabilidades**

  Mediante esta propuesta se podrá tener una lista detallada de algunas de las vulnerabilidades que existen en los servidores WEB, MAIL y FTP de la red del Hospital Regional Docente Ambato, utilizando la Técnica Sniffing como herramienta de detección, y así ayudar al Departamento de Sistemas al conocimiento, análisis y posterior solución dichas fallas.

- **Operabilidad de servicios**

  Los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato deben estar configurados correctamente y sus servicios deben ser estables y disponibles para cumplir con su propósito (la transferencia segura de información sensible y privada), es decir que no estén alterados por circunstancias o factores externos.

6.4 Objetivos

6.4.1. Objetivo general

Detectar las vulnerabilidades en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato aplicando la Técnica Sniffing como mecanismo de detección.

6.4.2. Objetivos específicos

- Seleccionar y probar las herramientas Sniffer necesarias y apropiadas para la detección de las vulnerabilidades en los servidores WEB MAIL y FTP del Hospital Regional Docente Ambato.

- Realizar los ataques que permite la herramienta Sniffer para detectar las vulnerabilidades de los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato.

- Elaborar un informe general en la que se describa las vulnerabilidades encontradas con la Técnica Sniffing en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato.

6.5. Análisis de factibilidad

- **Política**

  Una de las políticas internas del Hospital Regional Docente Ambato es mantener la información administrativa de manera confidencial, por tal razón es viable realizar el proyecto, ya que la detección de las vulnerabilidades de los servidores WEB, MAIL y FTP ayudará en la seguridad de la información la cual es importante para la institución.

- **Socio cultural**

  Es factible ya que con el funcionamiento correcto de los servicios seleccionados y un tratamiento adecuado de la información minimiza los riesgos a ataques de espías informáticos, ayudando a los usuarios de la red del Hospital Regional Docente Ambato de manera eficaz.

- **Tecnológico**

  El presente proyecto es factible de elaborar, ya que al analizar el hardware y software necesarios para el proyecto son totalmente accesibles.

- **Equidad de género**

  El conocimiento de las vulnerabilidades existentes en los servidores WEB, MAIL y FTP del HRDA ayudaran a mejorar la seguridad de la red aumentando la confiabilidad de los usuarios tanto hombres como mujeres.

- **Ambiental**

  Con la aplicación de este proyecto no se corre el riesgo de contaminación ambiental por lo cual es viable el desarrollo del mismo.

- **Económico financiero**

  El costo que genera el desarrollo del proyecto es bajo ya que las herramientas necesarias para este proyecto están disponibles. Siendo una institución pública la mayoría de software implementado es de acceso libre. En función de ello y de los beneficios que aportara este proyecto a la seguridad de la información del HRDA se lo considera económicamente factible.

- **Legal**

  El proyecto en el ámbito legal es factible porque su desarrollo cumple con todos los requerimientos establecidos a nivel del Ecuador para la seguridad de la información en las instituciones del estado.

6.6. Informe Técnico

6.6.1. Datos informativos

- **Titulo:** "Técnica Sniffing para detectar vulnerabilidades en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato"

- **Institución ejecutora:** Hospital Regional Docente Ambato

- **Director de Tesis:** Ing. Francisco López

- **Beneficiarios:** Hospital Regional Docente Ambato

- **Ubicación:** Hospital Regional Docente Ambato, ubicado en la Av. Pasteur y Unidad Nacional de la ciudad de Ambato.

- **Tiempo estimado para la ejecución:**

  Fecha de inicio: Marzo 2012
  Fecha de finalización: Julio 2012

- **Equipo técnico responsable**

  Investigador: Fernanda Conterón
  Jefe de d sistemas: Ing. Danilo Naranjo

6.6.2 Tema

"Aplicación de la Técnica Sniffing para detectar las vulnerabilidades en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato"

6.6.3 Objetivos

6.6.3.1. Objetivo general

Detectar las vulnerabilidades en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato aplicando la Técnica Sniffing como mecanismo de detección.

6.6.3.2. Objetivos específicos

- Seleccionar y probar las herramientas Sniffer necesarias y apropiadas para la detección de las vulnerabilidades en los servidores WEB, MAIL y FTP del HRDA.
- Realizar los ataques que permiten las herramientas Sniffer para detectar las vulnerabilidades de los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato.
- Elaborar un informe general en la que se describa las vulnerabilidades encontradas con la Técnica Sniffing en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato.

6.6.4 Fundamentación teórica

6.6.4.1. Escuchas de red

Según GARCÍA, Joaquín (Pág. 21) uno de los primeros ataques contra las dos primeras capas del modelo TCP/IP son las escuchas de red. Se trata de un ataque realmente efectivo, puesto que permite la obtención de una gran cantidad de información sensible.

Mediante aplicaciones que se encargan de capturar e interpretar tramas y datagramas en entornos de red basados en difusión, conocidos como escuchas de

red o *sniffers*, es posible realizar el análisis de la información contenida en los paquetes TCP/IP que interceptan para poder extraer todo tipo de información.

De esta forma, sin necesidad de acceso a ningún sistema de la red, un atacante podría obtener información sobre cuentas de usuario, claves de acceso o incluso mensajes de correo electrónico en el que se envían estas claves. Este tipo de técnica se conoce como *sniffing*.

Las técnicas de s*niffing* también se conocen como técnicas de *eavesdropping* y técnicas de *snooping*. La primera, *eavesdropping*, es una variante del *sniffing*, caracterizada por realizar la adquisición o intercepción del tráfico que circula por la red de forma pasiva, es decir, sin modificar el contenido de la información.

Por otra parte, las técnicas de *snooping* se caracterizan por el almacenamiento de la información capturada en el ordenador del atacante, mediante una conexion remota establecida durante toda la sesión de captura. En este caso, tampoco se modifica la información incluida en la transmisión.

La forma más habitual de realizar técnicas de *sniffing* en una red, probablemente porque está al alcance de todo el mundo, es la que podríamos denominar *sniffing software*.

6.6.4.2. Desactivación de filtro MAC

Una de las técnicas más utilizadas por la mayoría de los *sniffers* de redes Ethernet se basa en la posibilidad de configurar la interfaz de red para que desactive su filtro MAC (poniendo la tarjeta de red en modo promiscuo).

Las redes basadas en dispositivos Ethernet fueron concebidas en torno a una idea principal: todas las máquinas de una misma red local comparten el mismo medio, de manera que todos los equipos son capaces de ver el tráfico de la red de forma global.

Cuando se envían datos es necesario especificar claramente a quién van dirigidos, indicando la dirección MAC. De los 48 bits que componen la dirección MAC, los

24 primeros bits identifican al fabricante del *hardware*, y los 24 bits restantes corresponden al número de serie asignado por el fabricante. Esto garantiza que dos tarjetas no puedan tener la misma dirección MAC.

Para evitar que cualquier máquina se pueda apropiar de información fraudulenta, las tarjetas Ethernet incorporan un filtro que ignora todo el tráfico que no les pertenece, descartando aquellos paquetes con una dirección MAC que no coincide con la suya. La desactivación de este filtro se conoce con el nombre de *modo promiscuo*.

Con el uso adecuado de expresiones regulares y otros filtros de texto, se podrá visualizar o almacenar únicamente la información que más interese; en especial, aquella información sensible, como nombres de usuario y contraseñas.

El entorno en el que suele ser más efectivo este tipo de escuchas son las redes de área local configuradas con una topología en bus. En este tipo de redes, todos los equipos están conectados a un mismo cable. Esto implica que todo el tráfico transmitido y recibido por los equipos de la red pasa por este medio común.

Una solución para evitar esta técnica consiste en la segmentación de la red y de los equipos mediante el uso de conmutadores (*switches*). Al segmentar la red y los equipos, el único tráfico que tendrían que ver las máquinas sería el que les pertenece, puesto que el conmutador se encarga de encaminar hacia el equipo únicamente aquellos paquetes destinados a su dirección MAC. Aun así, existen técnicas para poder continuar realizando sniffing aunque se haya segmentado la red mediante *switches*. Una de estas técnicas es la suplantación de ARP.

6.6.4.3. Suplantación de ARP

El protocolo ARP es el encargado de traducir direcciones IP de 32 bits, a las correspondientes direcciones hardware, generalmente de 48 bits en dispositivos Ethernet. Cuando un ordenador necesita resolver una dirección IP en una dirección MAC, lo que hace es efectuar una petición ARP (arp-request) a la

dirección de difusión de dicho segmento de red, FF:FF:FF:FF:FF:FF solicitando que el equipo que tiene esta IP responda con su dirección MAC.

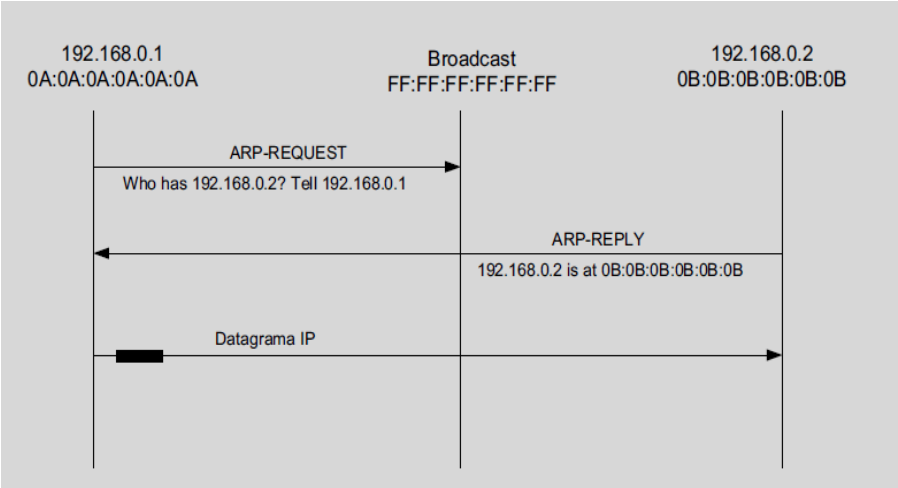

Figura Nº 6.1: Funcionamiento ARP
Fuente: Ataques contra redes TCP/IP

La figura Nº 6.1 refleja como una máquina A, con IP 192.168.0.1 y MAC 0A:0A:0A:0A:0A:0A solicita por difusión que dirección MAC está asociada a la IP 192.168.0.2. La máquina B, con IP 192.168.0.2 y MAC 0B:0B:0B:0B:0B:0B debería ser la única que respondiera a la petición.

Con el objetivo de reducir el tráfico en la red, cada respuesta de ARP (arp-reply) que llega a la tarjeta de red es almacenada en una tabla cache, aunque la máquina no haya realizado la correspondiente petición. Así pues, toda respuesta de ARP que llega a la máquina es almacenada en la tabla de ARP de esta máquina. Este factor es el que se utilizará para realizar el ataque de suplantación de ARP*.

El objetivo de un ataque de suplantación de ARP es poder capturar tráfico ajeno sin necesidad de poner en modo promiscuo la interfaz de red. Envenenando la tabla de ARP de los equipos involucrados en la comunicación que se quiere capturar se puede conseguir que el conmutador les haga llegar los paquetes. Si el engaño es posible, cuando las dos máquinas empiecen la comunicación enviarán sus paquetes hacia la máquina donde está el *sniffer*. Éste, para no descubrir el engaño, se encargará de encaminar el tráfico que ha interceptado.

En la Figura Nº 6.2 se puede ver cómo la máquina C se coloca entre dos máquinas (A y B) y les envía paquetes de tipo ARP-REPLY:

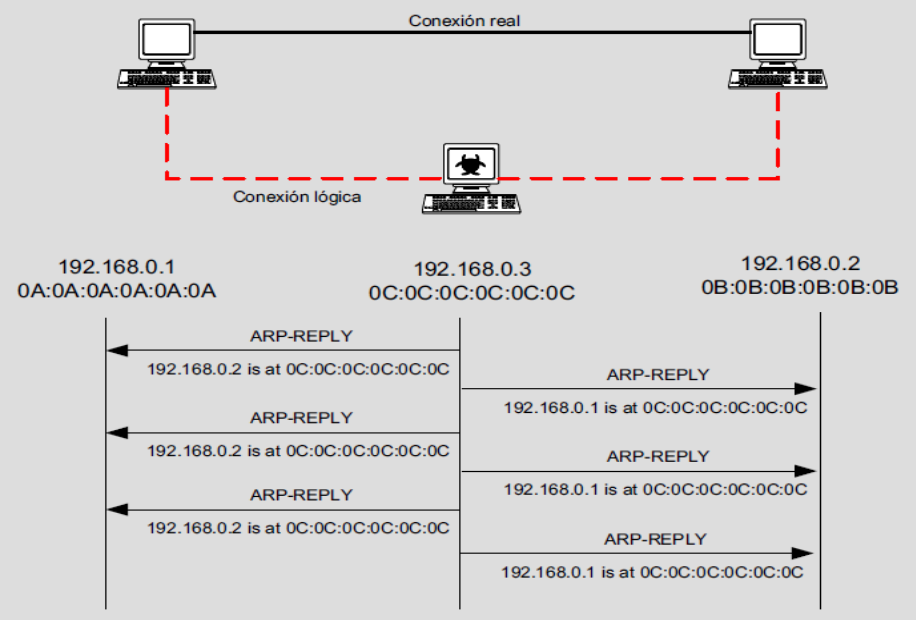

Figura Nº 6.2: Suplantación de ARP
Fuente: Ataques contra redes TCP/IP

De esta forma, toda comunicación entre las máquinas A y B pasará por la máquina C (ya que tanto A como B dirigen sus paquetes a la dirección MAC 0C:0C:0C:0C:0C:0C). El flujo de arp-reply será constante, para evitar que la tabla de ARP de las máquinas A y B se refresque con la información correcta. Este proceso corresponde al envenenamiento de ARP comentado. A partir del momento en que el envenenamiento se haga efectivo, los paquetes enviados entre A y B irán encaminados a C.

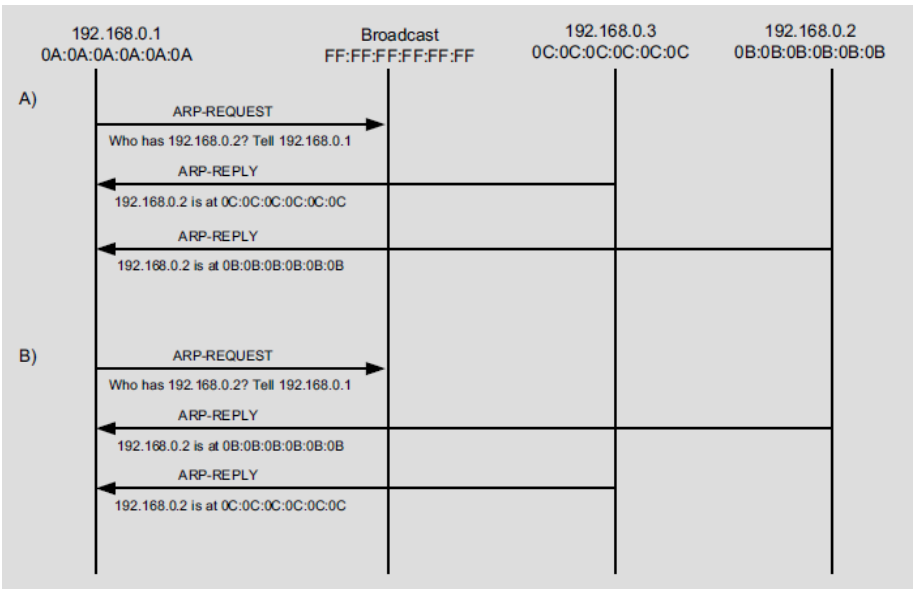

Figura Nº 6.3: Envenenamiento ARP - condición de carrera
Fuente: Ataques contra redes TCP/IP

Como vemos en la Figura Nº 6.3, al intentar realizar el envenenamiento de ARP podría producirse una condición de carrera (race condition).

Si la máquina C responde al arp-request antes que el servidor principal, su arpreplay será sobrescrito por el de la máquina verdadera (Figura Nº 6.3 A). Por otra parte, si fuera al contrario, sería el arp-reply verdadero el que sería eliminado por el de la máquina C (produciéndose en este caso el envenenamiento de ARP) (Figura Nº 6.3 B).

6.6.4.4. Sniffing

Según CRUZ, Edmanuel (Pág. 4-5) sniffing es la acción de captar tráfico de información, ya sea vía cable u inalámbrico. Para lograr esto el sniffer coloca la tarjeta de red o NIC en un estado conocido como "modo promiscuo" en el cual en la capa de enlace de datos (ver niveles OSI) no son descartadas las tramas no destinadas a la MAC address de la tarjeta; de esta forma se puede capturar (esnifar) todo el tráfico que transita por la red.

6.6.4.5. Sniffer y la topología de redes

La cantidad de tramas que puede obtener un sniffer depende de la topología de red, del nodo donde este instalado y del medio de transmisión. Por ejemplo:

- Para redes antiguas con topologías estrella, el sniffer se podría instalar en cualquier nodo, ya que lo que hace el nodo central es retransmitir todo lo que recibe a todos los nodos. Sin embargo en las redes modernas, en las que solo lo retransmite al nodo destino, el único lugar donde se podría poner el sniffer para que capture todas las tramas sería el nodo central.

- Para topologías en anillo, doble anillo y en bus, el sniffer se podría instalar en cualquier nodo, ya que todos tienen acceso al medio de transmisión .

- Para las topologías en árbol, el nodo con acceso a más tramas sería el nodo raíz, aunque con los switches más modernos, las tramas entre niveles inferiores de un nodo viajarían directamente y no se pasarían al nodo raíz.

Es importante remarcar el hecho de que los sniffer solo tienen efecto en redes que comparten el medio de transmisión como en redes sobre cable coaxial, cable par trenzado (UTP, FTP o STP), o redes WiFi.

El uso de switch en lugar de hub incrementa la seguridad de la red ya que limita el uso de Sniffers al dirigirse las tramas únicamente a sus correspondientes destinatarios.

6.6.4.6. Análisis de tráfico

El análisis de tráfico de red se basa habitualmente en la utilización de sondas con interfaz Ethernet conectadas al bus. Dichas sondas con su interfaz Ethernet funcionando en nodo promiscuo, capturan el tráfico a analizar y contribuye la plataforma en la que se ejecutaran, de forma continua aplicaciones propietarias o de dominio público, con las que se podrá determinar el tipo de información que circula por la red y el impacto que pudiera llegar a tener sobre la misma.

Así por ejemplo, podríamos determinar la existencia de texto plano o el uso excesivo de aplicaciones que comúnmente degradan las prestaciones de la red, sobre todo si hablamos de los enlaces principales que dan a Internet.

6.6.4.7. Ethernet y el modo promiscuo de la tarjeta de red

LOPEZ, Paco (2006, "9") define que Ethernet posee un medio de transmisión compartido, es decir todas las computadoras en un segmento de la red local comparten un mismo cable. Es conocido como un protocolo de **difusión (broadcast)** porque cuando un equipo intenta enviar información, envía los datos a todas las demás computadoras del mismo segmento.

Cada trama tiene un encabezado que es como el sobre que contiene la dirección de ambos, la computadora destino y origen. Aunque la información es recibida por todas la computadoras del segmento, solo la computadora que coincide con la dirección destino responderá. La tarjeta de red del resto de las computadoras desechará el mensaje automáticamente sin pasárselo al sistema operativo.

Cuando se ejecuta un sniffer, el controlador de captura activa el **modo promiscuo de la tarjeta de red** para impedir que sean desechados automáticamente los paquetes que tienen otra dirección destino. El modo promiscuo implica riesgos evidentes de seguridad, por lo que su uso en un entorno real debe limitarse al administrador de la red.

6.6.4.8. Concentrador (Hub) / Conmutador (Switch)

6.6.4.8.1. Hub o concentrador Ethernet

Son equipos repetidores (equipo de interconexión a nivel OSI) utilizados para la distribución de señal a través de par trenzado (10BaseT, 100BaseT,...). Es decir si un ordenador envía una trama a través de su cable y **el hub reenvía ese mensaje a todas las demás ordenadores que tiene conectadas.**

6.6.4.8.2. Switch o conmutador Ethernet

Tiene un aspecto externo similar a un Hub su función es diferente, ya que el switch actúa como **conmuntador,** es decir cuando un switch recibe información de una computadora no la reenvía a todas las computadoras, ya **que revisa en cada trama la dirección destino para enviarla así solo a la tarjeta de Ethernet con dicha dirección.** Por ello, la aplicación de la Técnica Sniffing es algo más complicada en redes "switcheadas"

6.6.4.9. Herramientas (Paket sniffer)

Algunos Sniffers trabajan solo con paquetes de TCP/IP, pero hay otros mas sofisticados que son capaces de trabajar con un numero más amplio de protocolos e incluso en niveles más bajos tal como el de tramas del Ethetnet.

Para conseguir los propósitos expuestos anteriormente, existen softwares diseñados con este fin. Se llaman **packet sniffers**. Existen packet sniffers para medios cableados como Ethernet/LAN y unos ejemplos de ello son Wireshark (anteriormente conocido como Ethereal), Ettercap, Cain y Abel, Tcpdump y también los hay para redes inalámbricas como Kismet.

A continuación se detallan los siguientes sniffer más populares:

6.6.4.9.1. Wireshark

Según SUAREZ, Eduardo (2009, Pág. 2,3) define a Wireshark como: Antes llamado Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos. Cuenta con todas las características estándar de un analizador de protocolos.

Usos de Wireshark

- Administradores lo usan para resolver problemas en la red.
- Ingenieros lo usan para examinar problemas de seguridad.
- Desarrolladores para depurar la implementación de los protocolos de red.
- Estudiantes los usan para aprender internamente cómo funciona una red.

Características principales de Wireshark:

- Es un capturador/analizador de paquetes de red.
- Permite ver, a un nivel bajo y detallado, qué está pasando en una red.
- Permite la captura de paquetes en vivo desde una interfaz de red.
- Este software cuenta con una interfaz gráfica lo que facilita su utilización especialmente para usuarios no muy avanzados y que no están acostumbrados a la operación mediante líneas de comandos, pero también cuenta con una versión basada en texto llamada **Tshark.**
- Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows
- Muestra los paquetes con información detallada de los mismos.
- Abre y guarda paquetes capturados.
- Filtrado de información de paquetes.

- Importar y exportar paquetes en diferentes formatos, esto permite una compatibilidad con otros software de características similares, para que así un conjunto de paquetes adquiridos mediante Wireshark pueda ser abierto y analizado por otros software de monitoreo de red.
- Resaltado de paquetes dependiendo el filtro.
- Crear estadísticas.
- Trabaja tanto en modo promiscuo como en modo no promiscuo, esto se refiere a que Wireshark funciona en máquinas conectadas a una red tanto inalámbricamente como de forma cableada.
- Puede capturar datos de la red o leer datos almacenados en un archivo (de una captura previa).
- Gran capacidad de filtrado.
- Admite el formato estándar de archivos **tcpdump**.
- Reconstrucción de sesiones **TCP**
- Es compatible con más de 480 protocolos.
- Puede leer archivos de captura de más de 20 productos.
- Packet Sniffer pasivo

6.6.4.9.2. Caín & Abel

Para PAEZ, Álvaro (http://vtroger.blogspot.com/2005/11/cain-y-abel.html 07/11/2005; 12/03/2012; 8:50) Caín & Abel es: "Una herramienta de recuperación de contraseñas para los sistemas operativos de Microsoft que se suele utilizar para hachear redes. Permite la recuperación fácil de las variadas clases de contraseñas que se difunden a través de una LAN, rompiendo contraseñas cifradas usando los ataques del diccionario, de Fuerza Bruta y de criptoanálisis, conversaciones de registración de VoIP, contraseñas web, destapando contraseñas depositadas y analizando protocolos de encaminamiento. Este programa aprovecha una cierta

inseguridad presente en los estándares de protocolo y métodos de autentificación; su propósito principal es la recuperación simplificada de contraseñas y de credenciales de varias fuentes, no obstante también tiene algunas utilidades "no estándares" para los usuarios de Microsoft Windows.

Desarrollado en principio Caín y Abel con la esperanza de que sea útil para los administradores de la red, los profesores, profesionales de seguridad, el personal forense, los vendedores de software de seguridad, el probador profesional de la penetración y para utilizarlo por razones éticas. El autor no pretende ayudar ni apoyar a ninguna actividad ilegal hecha con este programa. La última versión es más rápida y contiene nuevas características como ABRIL (encaminamiento del veneno ARP) que permite esnifar en LANs (engañando las tablas de los switch) y ataques de Hombre en el Medio. El succionador en esta versión puede también analizar protocolos cifrados tales como SSH-1 y HTTPS, y contiene los filtros para capturar las credenciales de una amplia gama de mecanismos de autentificación. La nueva versión también envía protocolos de encaminamiento que la autentificación supervisa y encamina los extractores, las cookies del diccionario y la fuerza bruta para todos los algoritmos de cálculo comunes y para varias autentificaciones específicas, las calculadoras de password/hash, los ataques del criptoanálisis, los decodificadores de la contraseña y algunas utilidades no tan comunes relacionados con la seguridad de la red y del sistema.”

6.6.4.9.3. Tcpdump

Herramienta en línea de comandos, lo cual permite analizar el tráfico que circula por la red. Permite al usuario capturar y mostrar a tiempo real los paquetes transmitidos y recibidos en la red a la cual el ordenador está conectado.

- Captura el tráfico que pasa a través de una máquina, es decir los que circulan ya sea dentro o fuera del ordenador.
- Analiza el rendimiento y las aplicaciones que generan o recibir tráfico de red.
- Analiza la infraestructura de la red por sí misma para determinar si todas las medidas necesarias de enrutamiento están correctamente

- Guarda los paquetes en un archivo, paquetes de todo o sólo los encabezados.
- Permite al usuario aislar aún más el origen de un problema.
- Interceptar y muestra las comunicaciones de otro usuario o equipo. Un usuario con los privilegios necesarios en un sistema que actúa como un enrutador o puerta de entrada a través del cual el tráfico sin cifrar, como Telnet o HTTP pasa puede usar tcpdump para ver los ID de usuario, contraseñas, la URL y el contenido de los sitios web que se está viendo, o cualquier otra información sin cifrar.
- Se puede aplicar un BPF basados en filtros para limitar el número de paquetes visto por tcpdump, lo que hace que la salida sea más fácil de usar en las redes con un alto volumen de tráfico.

6.6.4.9.4. Ettercap

Según PARRA, David (2011, pág. 3) Ettercap es "un interceptor/**sniffer** para redes LAN 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.

Sus funciones son las siguientes:

- Inyección de caracteres en una conexión establecida emulando comandos o respuestas mientras la conexión está activa.
- Compatibilidad con SSH1: puede interceptar usuarios y contraseñas incluso en conexiones "seguras" con SSH.
- Intercepta tráfico remoto mediante un túnel GRE: si la conexión se establece mediante un túnel GRE con un router CISCO, puede interceptarla y crear un ataque "Man in the Middle"
- "Man in the Middle" contra túneles PPTP (VPN).

- Compatibilidad con HTTPS: intercepta conexiones mediante HTTPS, SSL (supuestamente seguras) incluso si se establecen a través de un proxy.

Plataforma:

- Linux
- Windows

Última versión:

Ettercap NG-0.7.3

Además de las funciones de ettercap podemos añadir más mediante plugins:

- Colector de contraseñas
- Ataques DoS
- Filtrado y sustitución de paquetes.
- OS fingerprint: es decir, detección del sistema operativo remoto.
- Mata las conexiones.
- Escáner de LAN: hosts, puertos abiertos, servicios.
- Detecta otros envenenamientos ARP en la red.

Una vez que empieza a rastrear el tráfico, se obtendrá un listado de todas las conexiones activas, junto a una serie de atributos acerca de su estado (active, killed, etc.)"

6.6.4.9.5. Colasoft Capsa

Según Colasoft (http://colasoft-capsa.softonic.com/, 02/10/2010, 12/03/2012; 9:00) página oficial define como: un sniffer que monitoriza y analiza todo el tráfico que circula por una red local capturando sus paquetes TCP/IP en tiempo real.

Los usos que se le pueden dar a Colasoft Capsa son muy variados, pero entre otras cosas podremos realizar: análisis del tráfico de una red para conocer conexiones abiertas, anchos de banda consumidos, averiguar la existencia de posibles troyanos o puertas traseras, análisis de todos los correos electrónicos enviados, saber quién envía correos electrónicos, a quién se envían, el asunto del mensaje, su contenido, hora en que se produjo el envío, análisis de todas las páginas web visitadas desde todas las estaciones de trabajo de la red de una empresa u oficina, saber qué páginas web visita cada uno, si realiza descargas de programas, etc.

6.6.4.10. Ataque (Man in the Middle)

Según PARRA, David (2011, pág. 4) "El ataque clásico *Man-in-the-Middle* se basa en convencer a dos hosts de que el equipo que está en el medio es el otro host. Esto puede ser conseguido mediante *spoofing* del protocolo de resolución de direcciones (*ARP*) en la *LAN*.

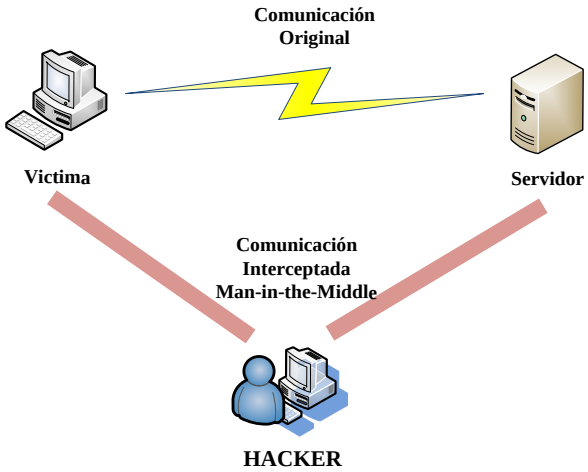

Figura Nº 6.4: Funcionamiento ataque Hombre en el Medio
Autor: Fernanda Conterón

Uno de los principales objetivos de realizar este tipo de ataque es interponerse entre una o varias máquinas con el fin de **interceptar, modificar o capturar paquetes.**

Si alguien puede elaborar y ejecutar ataques de hombre en medio entonces podrá obtener credenciales de acceso para los routers, suplantar sesiones inicializadas o desconectar usuarios válidos y otros ataques.

Estos ataques de spoofing y hombre en el medio generalmente comprometen los switchs de las organizaciones. Es importante pensar en asegurar estos dispositivos, validando que los puertos de los switchs pertenezcan a los usuarios validos del sistema, esto se logra con restricciones de MAC, tablas arp estáticas, software de monitoreo y detección de intrusos, estándares como 802.1x, etc".

6.6.4.11. Protocolo HTTPS

SANCHEZ, María (http://es.scribd.com/doc/52940650/Sniffer-con-ataque-iddle-in-man-usando-cain-y-abel 11/06/2012; 03/04/2012; 10:20) "El protocolo HTTPS se utiliza en sitios web que requieren seguridad en el acceso, de forma que se establece una sesión encriptada entre cliente y servidor para que la información crítica (contraseñas) no pueda ser leída por terceros. Esta conexión HTTPS requiere la existencia de un certificado válido de servidor verificado por una CA (Autoridad Certificadora). El equipo atacante va a situarse como Man in the Middle entre el equipo víctima y el router (puerta de enlace) de forma que todo el tráfico circule por él. Cuando el usuario víctima trate de conectarse al sitio web, utilizando protocolo HTTPS, realizará una petición de certificado válido de servidor que será servida por el equipo atacante. Al tratarse de un certificado falseado, es posible que la víctima inspeccione y rechace el certificado, y por tanto, no se produzca el inicio de sesión. Pero también es muy posible que la víctima acepte el certificado falseado, sin siquiera leerlo, y el Sniffer situado en el equipo atacante capture el usuario y contraseña de la sesión segura HTTPS".

6.6.4.12. Sistema de Detección de Intrusos (IDS)

Para HERRERA, Omar (internet 01/11/2006; 03/04/2012; 08:45:) un IDS es un software que monitorea el tráfico de una red y los sistemas de una organización en busca de señales de intrusión, actividades de usuarios no autorizados y la ocurrencia de malas prácticas, como en el caso de los usuarios autorizados que intentan sobrepasar sus límites de restricción de acceso a la información.

Algunas de las características deseables para un IDS son:

- Deben estar continuamente en ejecución con un mínimo de supervisión.

- Se deben recuperar de las posibles caídas o problemas con la red.
- Debe poderse analizar él mismo y detectar si ha sido modificado por un atacante.
- Debe estar configurado acorde con la política de seguridad seguida por la organización.
- Debe de adaptarse a los cambios de sistemas y usuarios y ser fácilmente actualizable.

6.6.4.13. Sistemas de Prevención de Intrusos (IPS)

Es una tecnología de software más hardware que ejerce el control de acceso en una red de computadores para protegerla de ataques y abusos. La tecnología de Prevención de Intrusos (IPS) es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías de firewalls; incluso los complementan, toman decisiones de control de acceso basados en los contenidos del tráfico, en lugar de hacerlo basados en direcciones o puertos IP.

La diferencia entre un Sistema de Prevención de Intrusos (IPS) frente a un Sistema de Detección de Intrusos (IDS), es que este último es reactivo pues alerta al administrador ante la detección de un posible intruso (usuario que activó algún sensor), mientras que un Sistema de Prevención de Intrusos (IPS) es proactivo, pues establece políticas de seguridad para proteger el equipo o la red de un posible ataque.

6.6.5. Informe técnico

El concepto de informe, como derivado del verbo informar, es la descripción oral o escrita, de las características y circunstancias de un suceso o asunto. Se trata en otras palabras, de la acción y efecto de informar (dictaminar).

En escritura, un informe es el documento que se caracteriza por contener información que refleja el resultado de una investigación o de un trabajo, adaptado al contexto de una situación determinada.

El informe técnico es la exposición por escrito de las circunstancias observadas en el examen de la cuestión que se considera, con explicaciones detalladas que certifiquen lo dicho. En otras palabras es un texto expositivo y argumentativo, por medio del cual se transmite una información de lo ejecutado en cierto tema y tiempo específico, o a lo que conviene hacer del mismo; generalmente están dirigidos a un destinatario que, normalmente, deberá tomar una decisión respecto al tema tratado en el texto. Ese destinatario en este caso, se refiere al Director Ejecutivo y a los Directores Corporativos (Director de Investigaciones, Director de Operaciones y Director Financiero Administrativo).

6.6.5.1. Materiales

- Red de Computadoras (victimas – atacante)
- Sniffer (Software)
- Recurso humano

6.6.5.2. Procedimientos

6.6.5.2.1. Selección de herramienta sniffer

Para la selección de las herramientas a utilizar se realiza el siguiente cuadro con las características y capacidades de las herramientas más utilizadas a nivel educativo-investigativo:

Los criterios de selección con sus respectivos pesos son:

Cuadro N° 6.1: Criterios de Selección de la herramienta Sniffer

CRITERIOS	PESO
Software libre Open Sourse	13
Interfaz Gráfica de uso	11
Monitoreo distintos S. O.	10
Eficiencia captura de tràfico	14
Envenenamiento ARP	11
Ataque DoS	12
Filtrado de Paquetes	6
Modificabilidad de paquetes	11
Escaneo de HOST	13
TOTAL	100

Autor: Fernanda Conterón

Según el Cuadro Nº 6.1 los pesos de cada uno de estos criterios están dados asumiendo la importancia de estos dentro de la investigación. Completando entre todos un total de 100%.

Para la escala de valoración de cada criterio se definió una escala numérica donde se evalúan las alternativas de acuerdo a las características individuales de cada una de las herramientas (Cuadro Nº 6.2).

Cuadro N° 6.2: Escala de valoración.

CRITERIOS (b, d, g, i)	
ESCALA	**INTERPRETACION**
1	Malo
2	Regular
3	Buena
4	Muy Buena
5	Excelente

CRITERIOS (a, c, e, f, h)	
ESCALA	**INTERPRETACION**
1	No
5	Si

Autor: Fernanda Conterón

Cuadro N° 6.3: Selección de las herramientas Sniffers

	CRITERIOS	PESO	CAIN & ABEL	ETTERCAP	WIRESHARK	TCPDUMP	CAPSA
a)	**Software libre Open Sourse**	13	5 / 65	5 / 65	5 / 65	5 / 65	1 / 13
b)	**Interfaz Gráfica de uso**	11	5 / 55	4 / 44	3 / 33	1 / 11	5 / 44
c)	**Monitorea distintos S. O.**	10	1 / 10	5 / 50	5 / 50	1 / 10	1 / 10
d)	**Eficiencia en la captura de tráfico**	14	4 / 48	5 / 70	5 / 70	5 / 70	4 / 48
e)	**Envenenamiento ARP**	11	5 / 55	5 / 55	1 / 11	1 / 11	1 / 11
f)	**Ataque DoS**	12	1 / 12	5 / 60	1 / 12	1 / 12	1 / 12
g)	**Filtrado de Paquetes**	6	1 / 6	4 / 24	5 / 30	4 / 24	4 / 24
h)	**modificabilidad de Paquetes**	11	1 / 11	5 / 55	1 / 11	1 / 11	1 / 11
i)	**Escaneo de HOST**	13	5 / 65	5 / 65	3 / 39	3 / 39	5 / 65
	TOTAL	100	327 SEGUNDA	488 PRIMERA	321 TERCERA	253 CUARTA	238 QUINTA

SELECCIÓN DE HERRAMIENTA

Autor: Fernanda Conterón

Por los valores totales obtenidos para cada una de las herramientas mencionadas en el Cuadro Nº 6.3 se concluye que las tres primeras herramientas (Ettercap NG-0.7.3, Caín & Abel v4.9.43 y Wireshark 1.6.8) son suficientes y necesarias para realizar la detección de las vulnerabilidades de los servidores seleccionados.

Para el presente trabajo se ha decidido trabajar en las plataformas Windows y Linux dependiendo la necesidad y la herramienta.

Las herramientas instaladas y operadas sobre una plataforma Windows, específicamente Windows 7 son Wireshark, y Caín & Abel y la herramienta instalada y operada sobre una plataforma Linux, específicamente Backtrack 5 es Ettercap.

6.6.5.2.2. Aplicación de la herramienta sniffer

El Hospital Regional Docente Ambato permite que los servidores WEB, MAIL y FTP sean evaluados mediante la aplicación de la Técnica Sniffing bajo las siguientes consideraciones:

- Dotación de una IP con privilegios de administrador.
- Dotación de una IP con privilegios limitados.
- No eliminar, ni modificar ninguna información.
- Manejar con total confidencialidad (no ser divulgada) la información que maneja la institución, por lo que se prohíbe la presentación de información de credenciales, dirección de IPs y MACs, y cualquier información que comprometa la confidencialidad de la misma.
- Mantener informado al administrador de la red de todas pruebas realizadas y los resultados obtenidos.

6.6.5.2.2.1. Requisitos

- La máquina atacante instalado el sniffer.
- Conocer las direcciones IP de los nodos y en especial de cuyas comunicaciones se quiere intervenir.
- Las máquinas víctimas deben estar encendida y sin problemas de conectividad.

- Los hosts víctimas y el hosts atacante deben estar dentro del mismo dominio de broadcast.

6.6.5.2.2.2. Escenario utilizado para la Técnica Sniffing

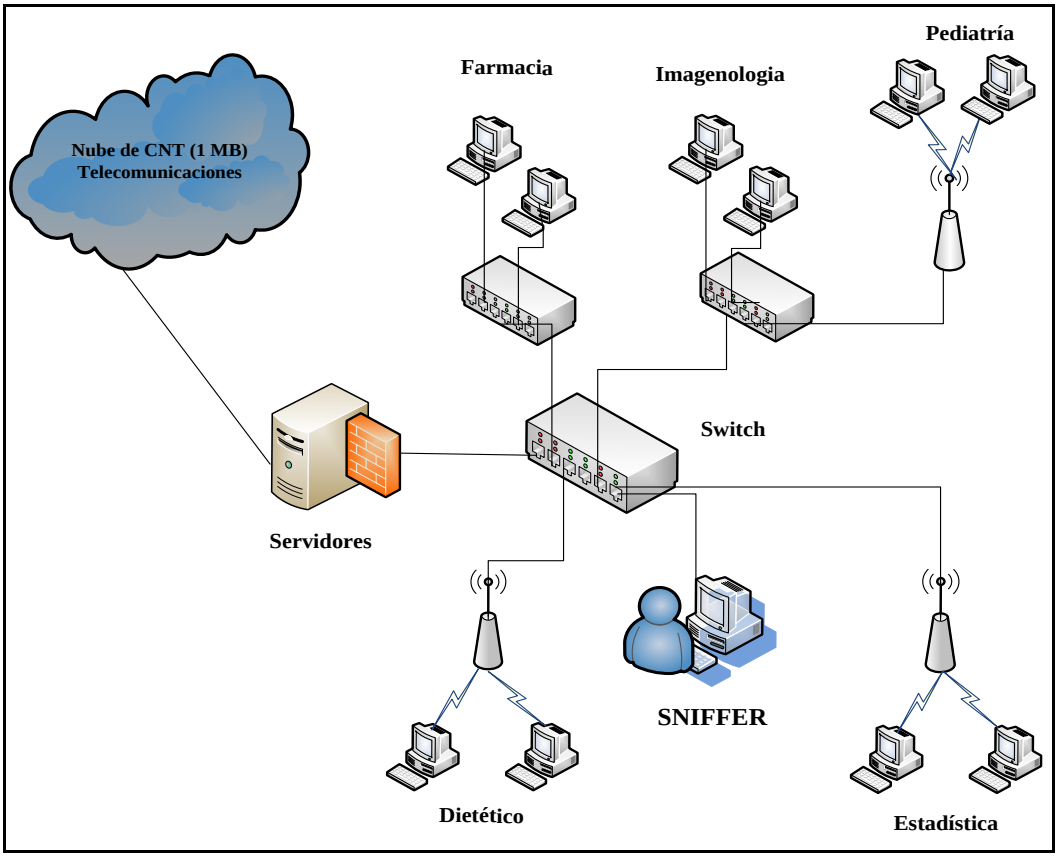

Figura Nº 6.5: Escenario utilizado para la Técnica Sniffing
Autor: Fernanda Conterón

En la figura Nº 6.5 se visualiza el escenario escogido para realizar las pruebas de sniffing, se ubica en el interior de la red específicamente en el nodo principal.

6.6.5.3. Desarrollo

6.6.5.3.1. Captura de contraseñas WEB, SMTP Y FTP

Para la captura de contraseñas se utiliza los siguientes sniffers :

- Cain y Abel v4.9.43 en Windows 7 – sniffer activo
- Ettercap NG-0.7.3 en Backtrack – sniffer activo

Estas herramientas permiten la captura del tráfico de la red en especial la captura de usuarios y contraseñas, por medio del ataque "Main in the middle" generando "certificados de autenticidad" falsos para el protocolo seguro HTTPS.

6.6.5.3.1.1. Cain y Abel v4.9.43

1. El primer paso es la instalación del sniffer, podemos descargar de la página oficial http://www.oxid.it

2. Configurar la tarjeta de red, **Configure - sniffer**, aquí se selecciona la tarjeta con la cual se captura el trafico que viaja por la red y en la pestaña **ARP(Arp Poison Routing)** se utiliza las direcciones IP y MAC real y clic en aceptar.

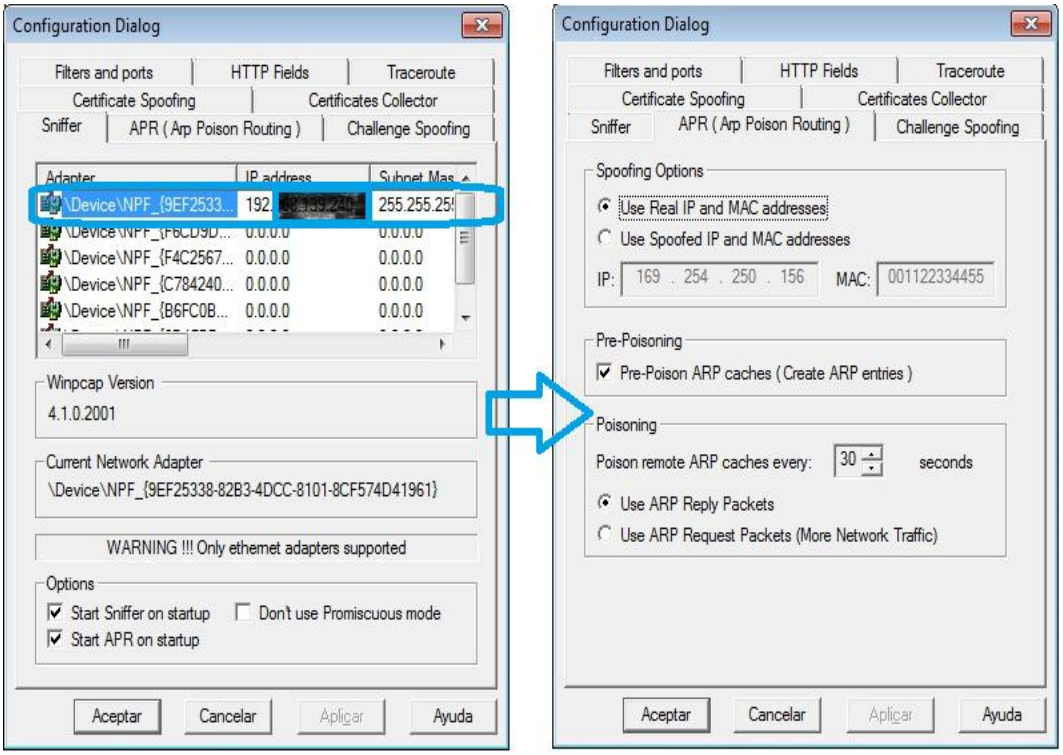

Figura Nº 6.6: Configuración de la tarjeta de red - Caín & Abel
Autor: Fernanda Conterón

3. A continuación para ver las máquinas que están conectadas y activas en la red, ir a la pestaña de **Sniffer** luego en la parte inferior del menú escoger **Host**, y presionar en el botón , empezará a escanear toda la red en busca de las direcciones IP y MAC con sus respectivos nombres.

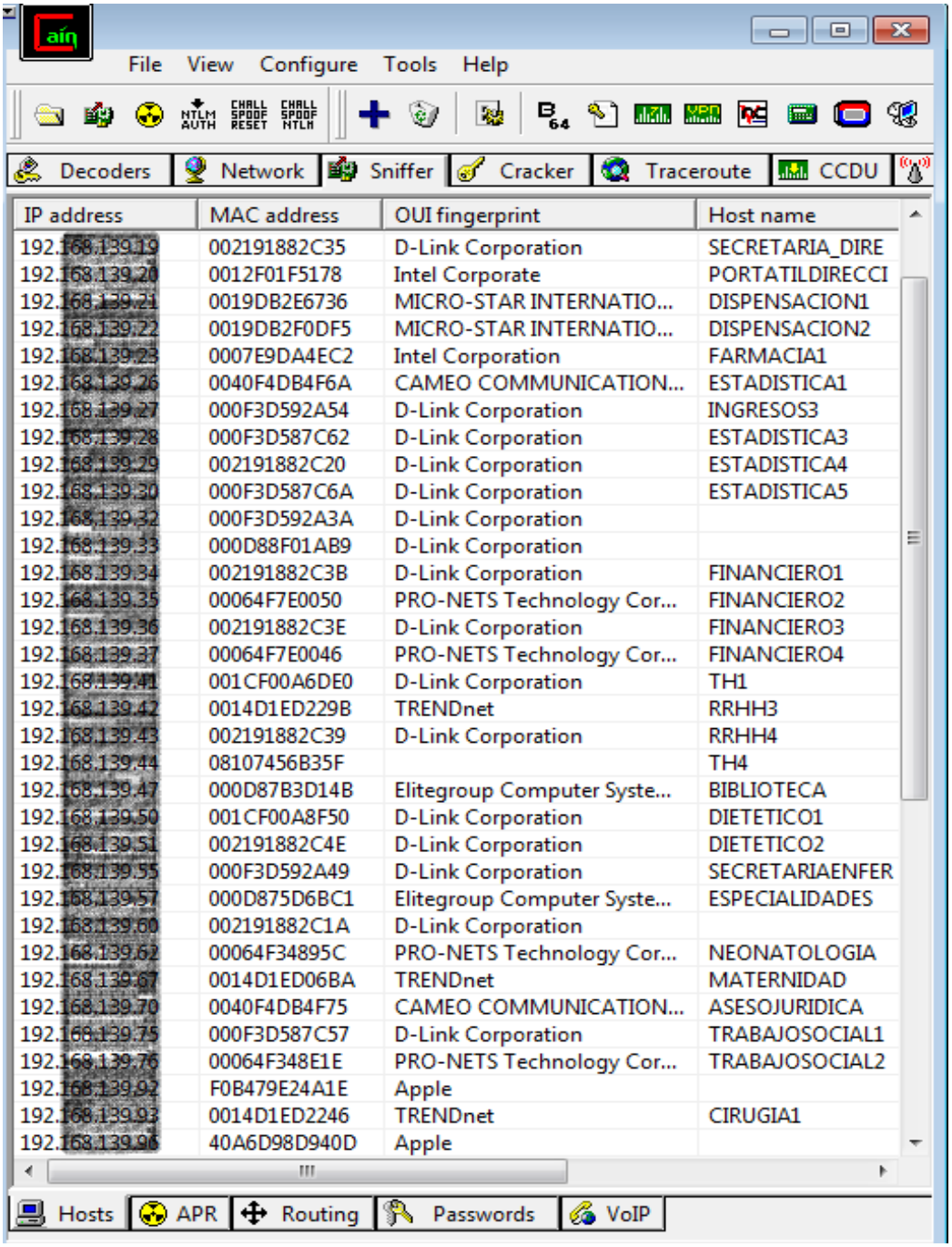

Figura Nº 6.7: Escaneo de máquinas conectadas en la red - Caín & Abel
Autor: Fernanda Conterón

En la Figura Nº 6.7 indica todos los equipos conectados a la red interna del HRDA el cual nos permite saber a qué máquina atacar.

4. Ahora se debe empezar a envenenar las tablas ARP de nuestra Red (porque se tiene un Switch, red conmutada), para eso hacer clic sobre el botón amarillo, marcado en la Imagen: 

Captura de contraseñas de clientes WEB - Caín & Abel v4.9.43

Y Caín empieza la capturar los usuarios y claves que viajen por medio de la red.

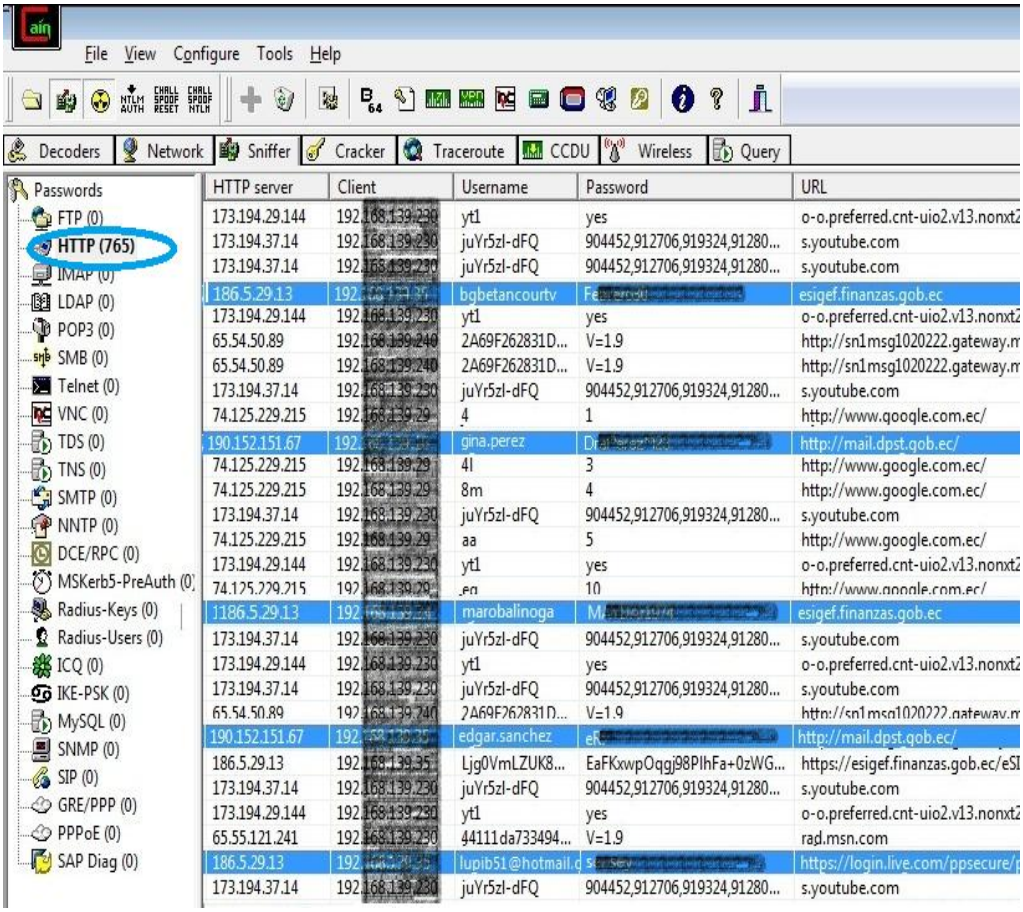

Figura Nº 6.8: Captura de usuarios y contraseñas HTTPS - Cain &Abel
Autor: Fernanda Conterón

Como se observa en la Figura Nº 6.8 el snifffer a capturado 765 usuarios y contraseñas pero no todos son validas, las credenciales útiles solo son cinco, siendo estas de protocolos seguros, es decir de sitios web como: https://esigef.gob.ec, mail.dost.gob.ec y https://hotmail.com provenientes de las áreas de Financiero, Administración y Recursos Humanos. Estas han sido capturadas por medio de certificados de autentificación falsos siendo el usuario final el principal culpable.

Captura de contraseñas de clientes FTP

Con el mismo procedimiento anterior también se puede capturar credenciales del servidor o clientes FTP y SMTP:

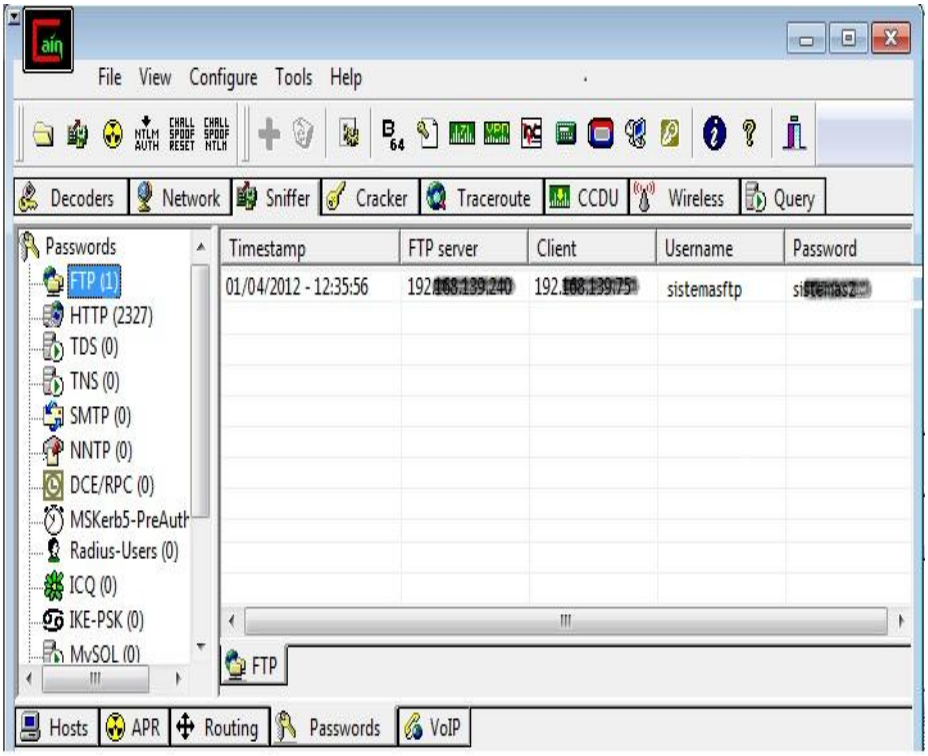

Figura Nº 6.9: captura de usuario y clave cliente FTP
Autor: Fernanda Conterón

La figura Nº 6.9 ilustra la captura de un usuario y contraseña del servicio FTP.

Captura de contraseñas de clientes SMTP

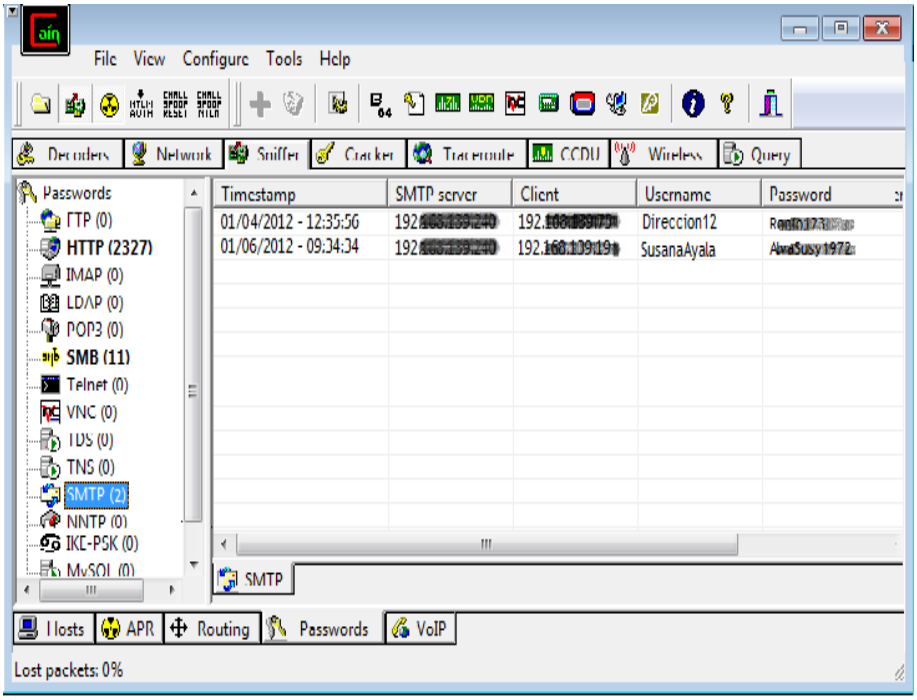

Figura Nº 6.10: captura de usuario y clave de correo
Autor: Fernanda Conterón

En la Figura Nº 6.10 se ha capturado usuario y contraseña de un usuario del servicio de correo interno del HRDA.

Las capturas de estas credenciales tanto del servicio de correo y FTP son fáciles debido que viajan en texto plano.

6.6.5.3.1.2. Ettercap NG-0.7.3

Ahora se utilizará la herramienta Ettercap para capturar de igual manera las credenciales

1. Para comenzar a capturar los paquetes que viajan por la red, hacer clic en el menú **SNIFF** y seleccionar la opción **UNIFIED SNIFFING**. A continuación solicitará indicar la interfaz de red a inspeccionar.

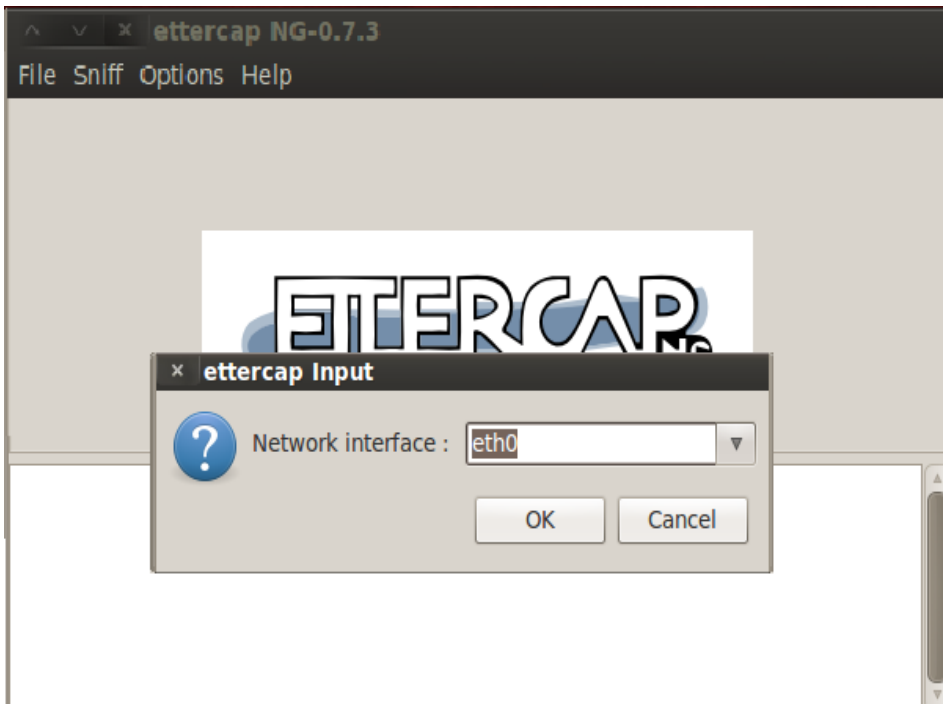

Figura Nº 6.11: Identificar interfaz de red - Ettercap
Autor: Fernanda Conterón

2. Las opciones del menú cambian. Ahora como segundo paso se debe averiguar que equipos se encuentran en la red investigada, hacer clic en el menú **HOSTS**, luego en la opción **SCAN FOR HOSTS,** finalmente escoger la opción **HOSTS LIST** para que se despliegue la lista de los equipos encontrados por el sniffer.

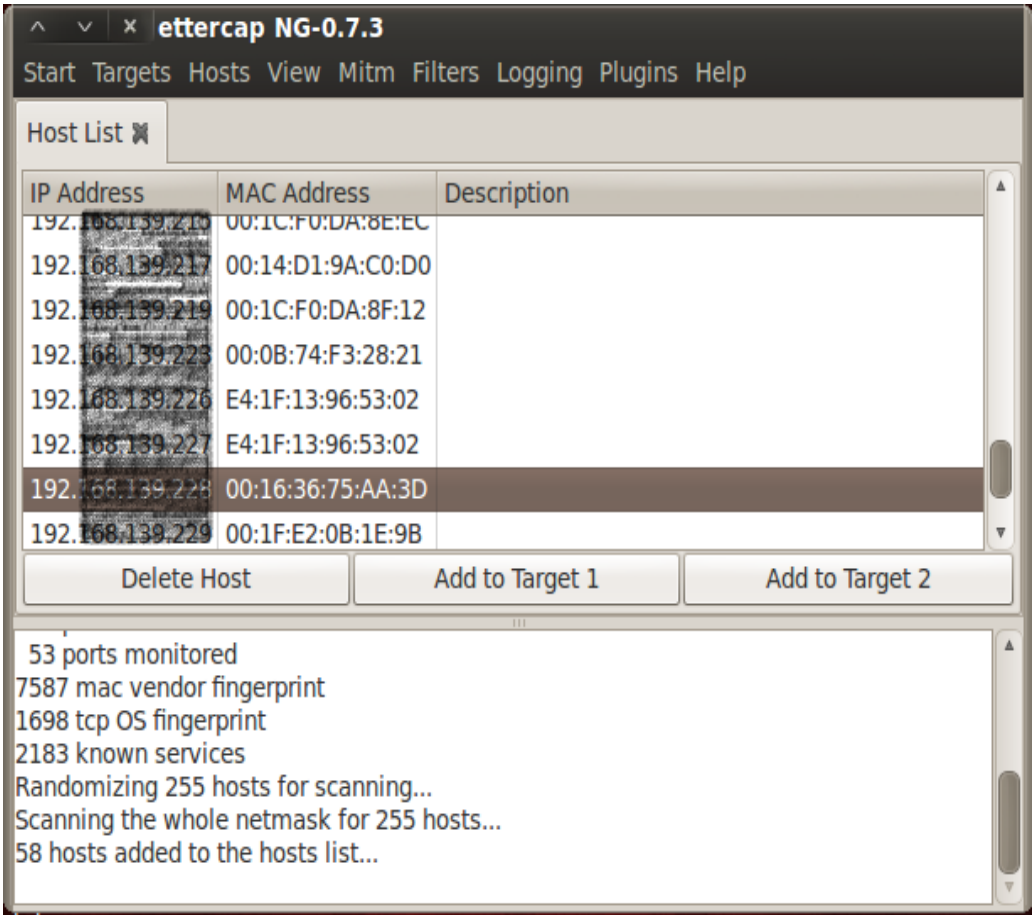

Figura Nº 6.12: Escaneo de equipos activos de la red - Ettercap
Autor: Fernanda Conterón

Al escanear los equipos de la red ETTERCAP nos indica que ha encontrado 58 equipos conectados a la red Figura Nº 6.12 de los cuales se despliega la dirección IP y MAC respectivamente.

Captura de contraseñas de clientes WEB

1. Lo primero: agregar como Destino1 la puerta de enlace, por la que sale la gente a internet 192.X.X.228, seleccionar y pulsar en "**ADD TO TARGET 1**"

   Posteriormente debemos agregar las máquinas que se espiará, en este caso sólo se tomará una en concreto, la 192.X.X.230; seleccionar la máquina en cuestión y pulsar en **"ADD TO TARGET 2",** pero si lo que realmente queremos es espiar toda la red, seleccionamos todos menos el host anterior y los agregamos como Target2 (o ninguno).

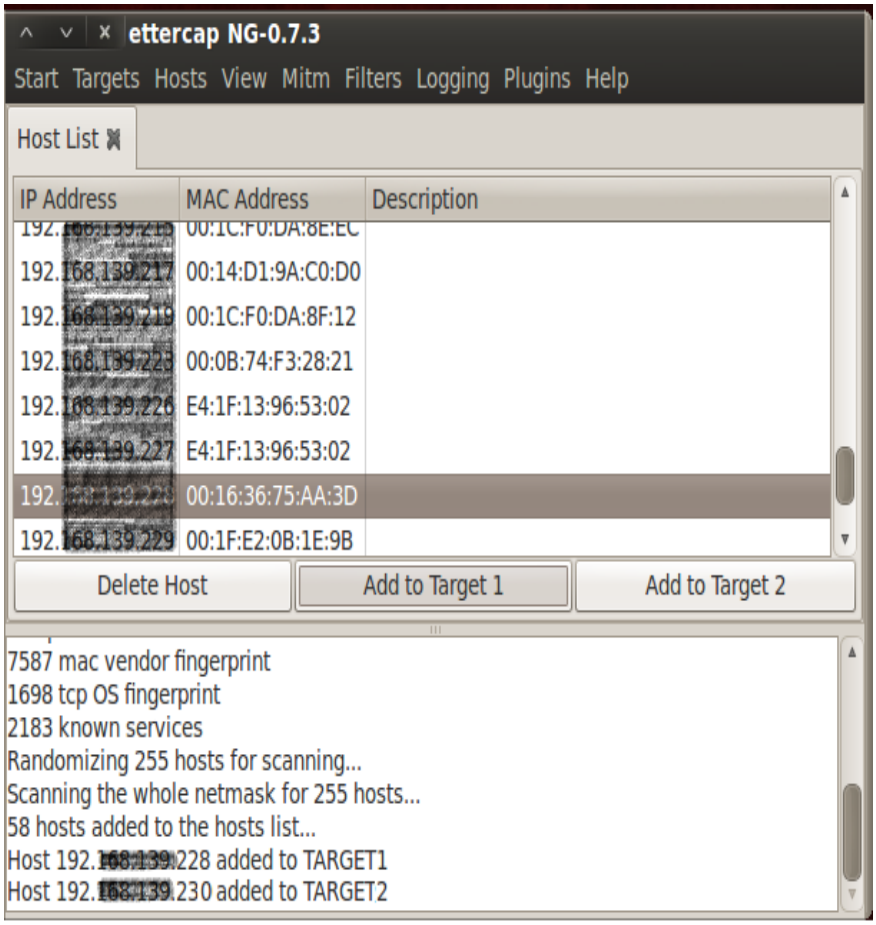

Figura Nº 6.13: Enlace de máquinas para espiar
Autor: Fernanda Conterón

2. A continuación, seleccionar en el Menú **MITM**, y luego dar clic en **ARP POISONING** y en la ventana seleccionar **"SNIFF REMOTE CONNECTIONS"** y OK.

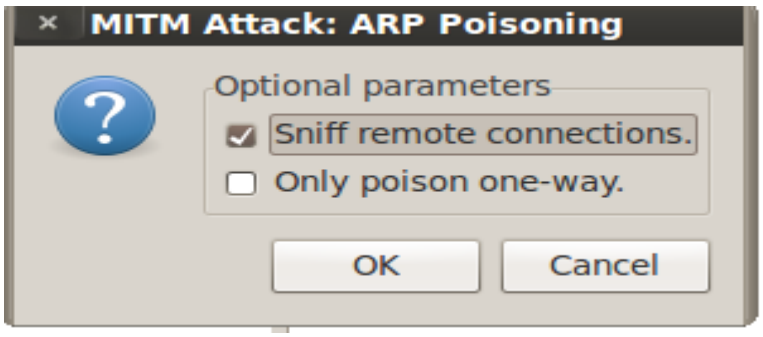

Figura Nº 6.14: Conexión remota de sniffer
Autor: Fernanda Conterón

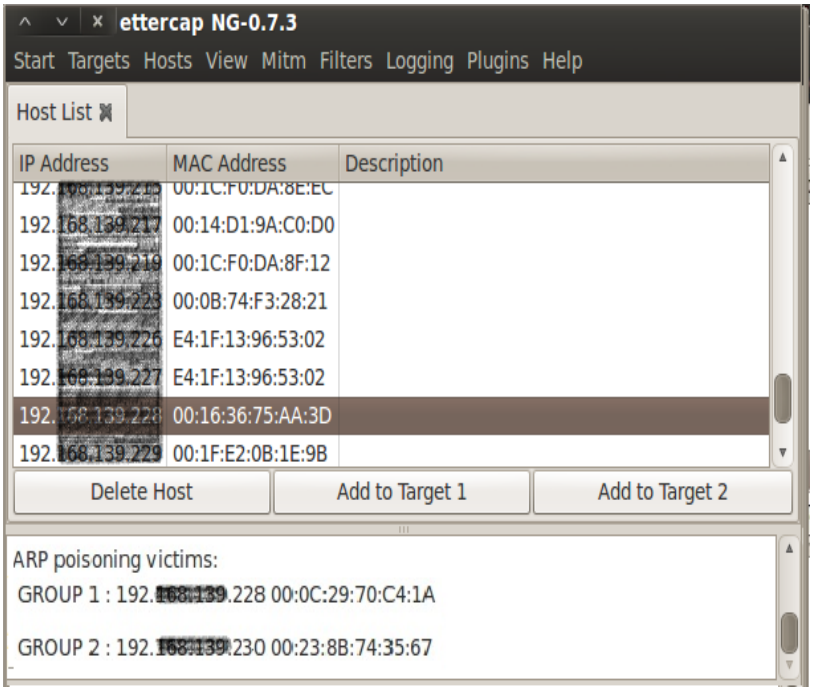

Figura Nº 6.15: Enlace de máquinas y envenenamiento ARP – Ettercap
Autor: Fernanda Conterón

3. De esta forma se está ejecutando el envenenamiento ARP de manera que todo el tráfico pasara por nuestra máquina (Bactrack), Ahora se debe activar el Sniffer para visualizar los paquetes realizando de la siguiente forma:

   Ir al Menú "**START"** y luego hacer clic en "**START SNIFFING"**

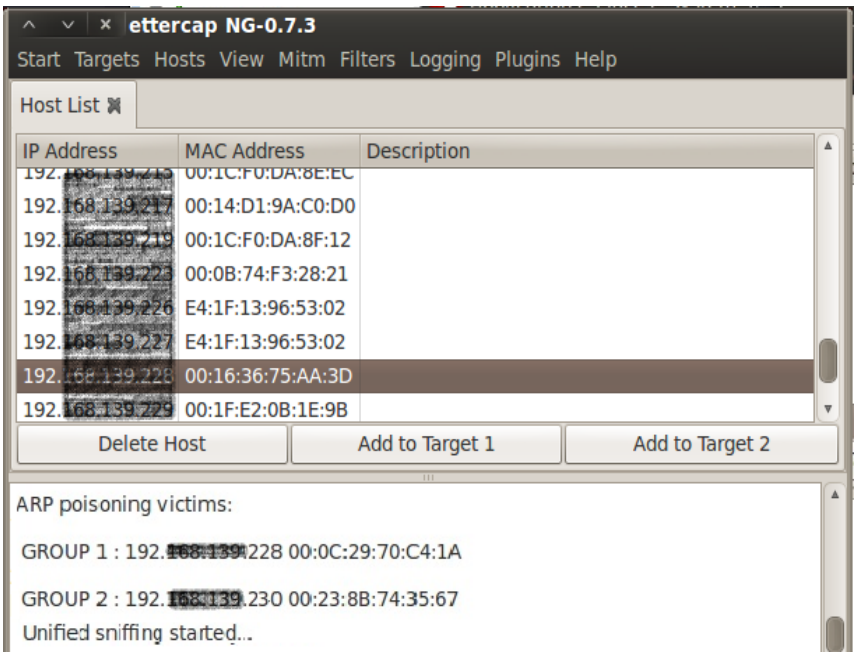

Figura Nº 6.16: Iniciando el Sniffing de la red – Ettercap
Autor: Fernanda Conterón

4. Con un poco de paciencia aparecerá en la parte inferior de la pantalla de Ettercap los usuarios y contraseñas del equipo atacado, siendo indiferente si son HTTP o HTTPS (conexiones "seguras").

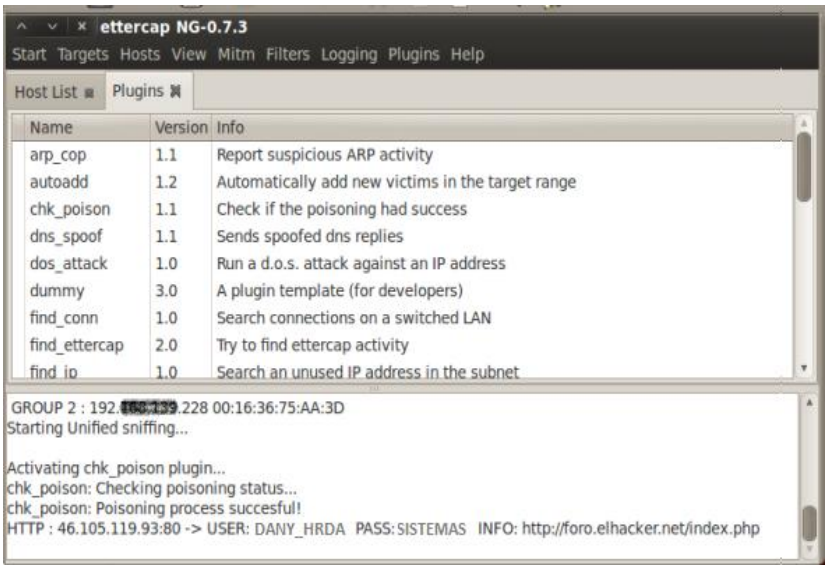

Figura Nº 6.17: Captura de contraseña – Ettercap
Autor: Fernanda Conterón

Como podemos observar en la Figura Nº 6.17 se ha capturado un usuario y una contraseña de un foro.

Como podemos darnos cuenta estas herramientas logran la captura de contraseñas sin importar la ubicación del usuario, permitiéndonos darnos cuenta que la seguridad de la información es vulnerable ante un ataque de este tipo.

6.6.5.3.1.1. Contramedida

Aplicar la encriptación de datos para la comunicación. Emplear contraseñas fuertes para que en caso de que sea capturado por ejemplo con el algoritmo de encriptación MD5, la ruptura (o el crackeo) del mismo sea algo casi imposible.

Otra medida a tomar es la aplicación de claves más fuertes rigiéndose en el estándar ISO 27001 para el cumplimiento de las normas de elección y protección para la seguridad de las claves.

Una manera de mitigar el problema de la captura de contraseñas de sitios web seguros (HTTPS), es que el usuario lea la información de los certificados de

seguridad que ofrecen estas conexiones seguras, validando que la información que estos contengan sean congruente para el sitio que se visita, por lo regular cuando se es víctima de un ataque de este tipo, los navegadores muestran un mensaje de alerta indicándonos que existe algún tipo de problema con los certificados, cuando esto suceda el usuario debe detenerse a leer la información del certificado y solo en caso de que este sea congruente y confiable continuar con la navegación.

La implementación de un Sistemas de detección de sniffers para detectar cuando se está produciendo un ataque Sniffing o escaneo de puertos.

6.6.5.3.2 Ataque Denegación de Servicios (DoS) a los servidores WEB, MAIL y FTP

Para la realización y captura de tráfico de este ataque se usa las herramientas sniffers:

- Ettercap NG-0.7.3 en Backtrack – sniffer activo
- Wireshark 1.6.8 en Windows 7 – sniffer pasivo

6.6.5.3.2.1. Ataques DoS al servidor WEB – Ettercap

La herramienta Ettercap permite realizar el ataque DoS mediante un plugin que contiene el sniffer y la captura del tráfico que genera este ataque para su análisis se realizará con la herramienta Wireshark.

Ettercap NG-0.7.3

1. Para realizar este ataque se utiliza el plugin dos_attack que contiene la herramienta Ettercap, este plugin permite dejar sin uso la IP víctima (servidor web) y asignar una IP cualquiera siempre y cuando esté disponible.

   Para esto se debe escoger en el menú "**PLUGIN"** - "**MANAGE THE PLUGIN"** y escoger la opción **"DOS_ATTACK"**.
   En el campo **"INSERT VICTIM IP:"** se ubica la IP víctima **192.X.X.228**, en este caso la IP a la que se le va hacer el ataque y en el otro campo **"INSERT**

UNUSED IP:" se ubica la IP **192.X.X.99** es decir desde donde se va a realizar el ataque como se muestra Figura 6.18.

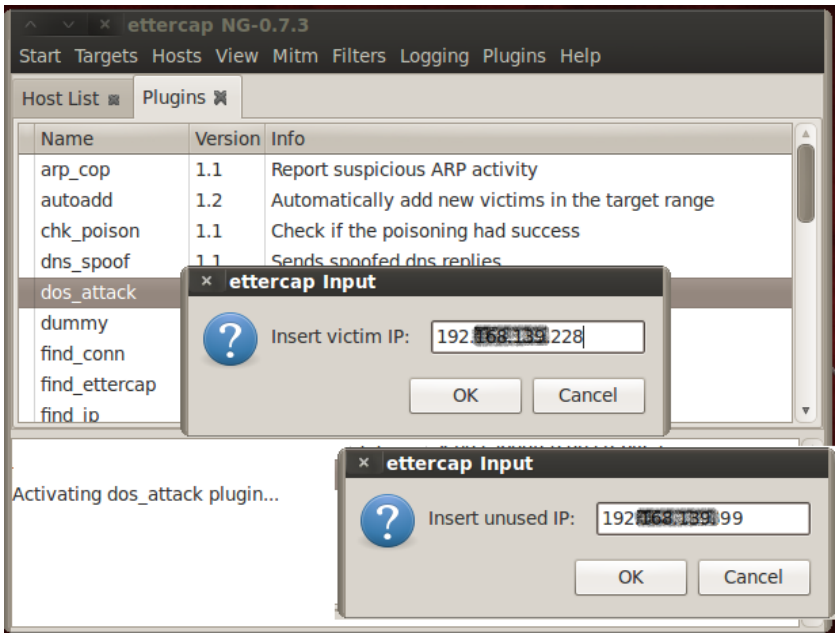

Figura Nº 6.18: Asignación de IPs – ataque DoS – Ettercap
Autor: Fernanda Conterón

NOTA: La dirección IP 192.X.X.228 es la dirección IP del servidor WEB.

La dirección IP 192.X.X.99 es una dirección IP disponible, es decir que no está siendo ocupado por ninguna máquina y está dentro del rango requerido.

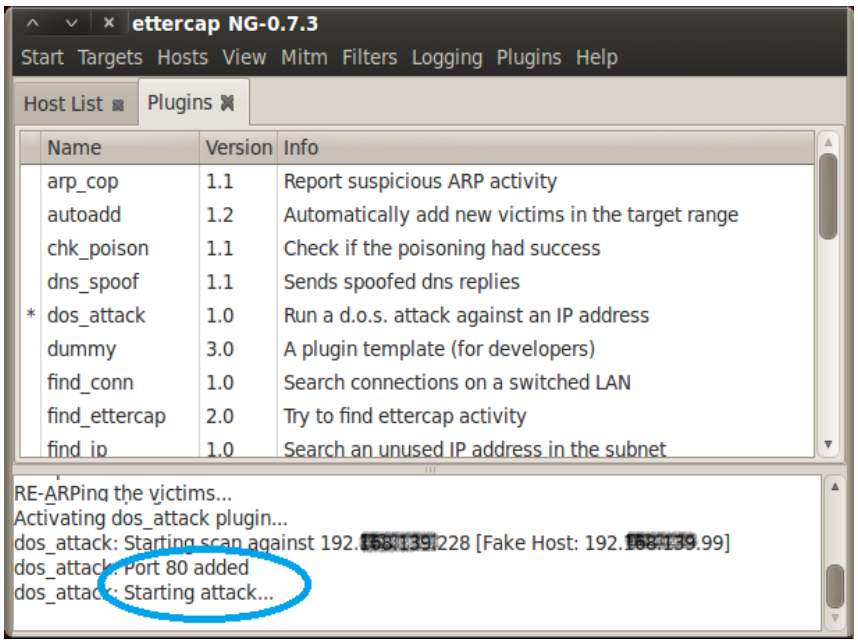

Figura Nº 6.19: Ataque DoS al servidor WEB – Ettercap
Autor: Fernanda Conterón

El plugin de DoS comienza a realizar el ataque y como se muestra en la parte inferior de la Figura Nº 6.19 que está siendo atacado por el puerto 80.

2. Cualquier usuario que intente realizar la petición a la página web no tendrá respuesta, ya que el servicio del servidor web colapso por el ataque realizado.

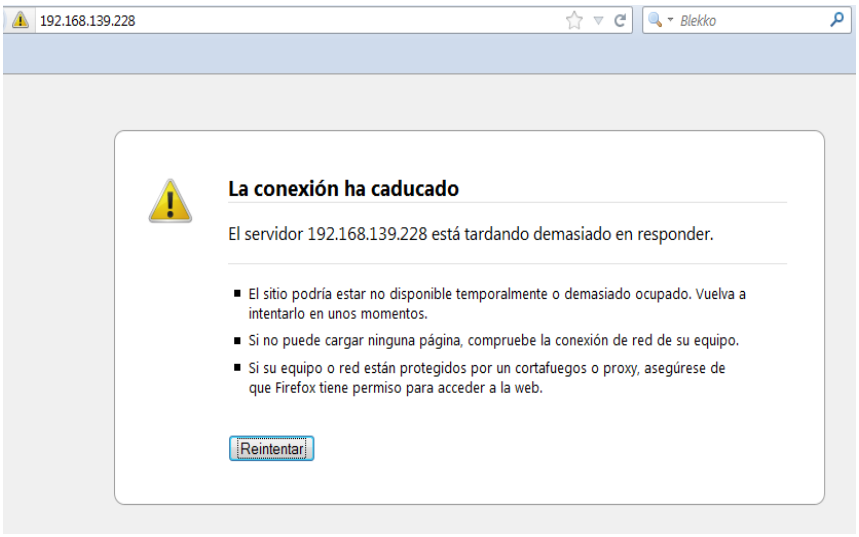

Figura Nº 6.20: Servidor WEB sin respuesta
Autor: Fernanda Conterón

6.6.5.3.2.2. Ataques DoS a los servidores de correo y FTP – Ettercap

Los pasos realizados anteriormente para el ataque DoS al servidor WEB se realiza también para este ataque.

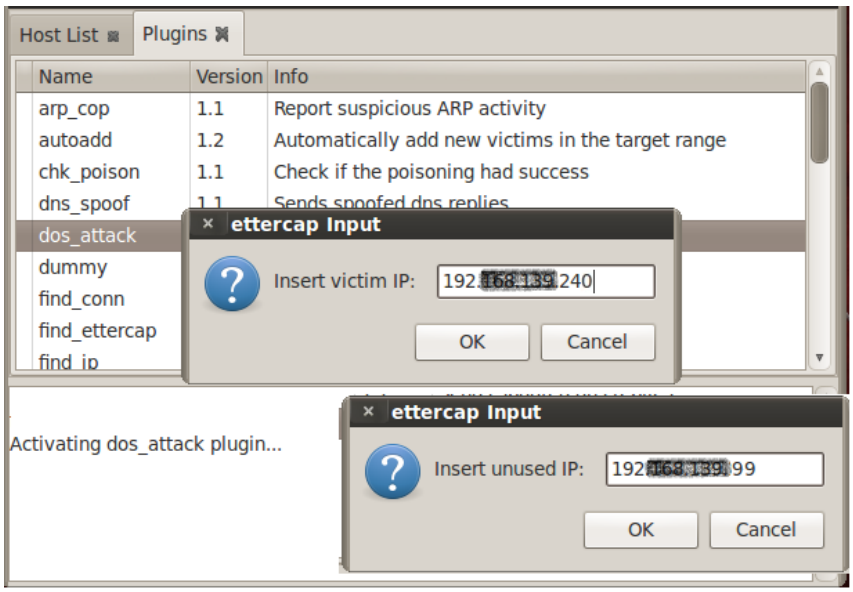

Figura Nº 6.21: Asignación de IPs – ataque DoS al servidor de correo y FTP – Ettercap
Autor: Fernanda Conterón

En el campo **“INSERT VICTIM IP:” colocamos la IP 192.X.X.240** y la otra IP será la misma utilizada anteriormente **“INSERT UNUSED IP: 192.X.X.99”** como se muestra en la Figura Nº 6.21.

NOTA: El servidor de correo y el servidor FTP contienen la mismo IP la cual es 192.X.X.240, por lo tanto con esta dirección se trabajara para dicho ataque.

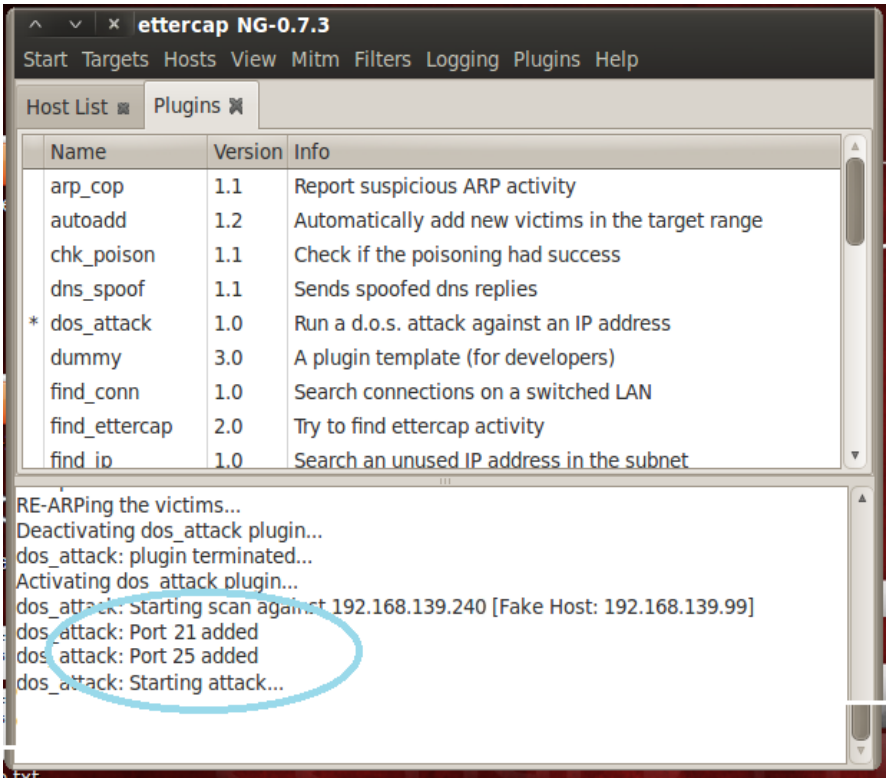

Figura Nº 6.22: Ataque DoS a los servidores MAIL y FTP– Ettercap
Autor: Fernanda Conterón

Al ejecutarse el plugin dos_attack y realizar el ataque busca los puertos abiertos y en este caso el puerto 21 y 25 son atacados dejando deshabilitados los servicios de correo y archivvos como se muestra en la parte inferior de la Figura Nº 6.22.

Captura de tráfico con Wirwshark

Para ello utilizamos la herramienta Wireshark que es una herramienta de fácil uso.

Una vez instalado para realizar la captura de tráfico de debe seleccionar en el menú **CAPTURE – OPTIONS** en el cual se elige la interfaz de red y el filtro de captura en este caso la captura se filtrara por el puerto 80.

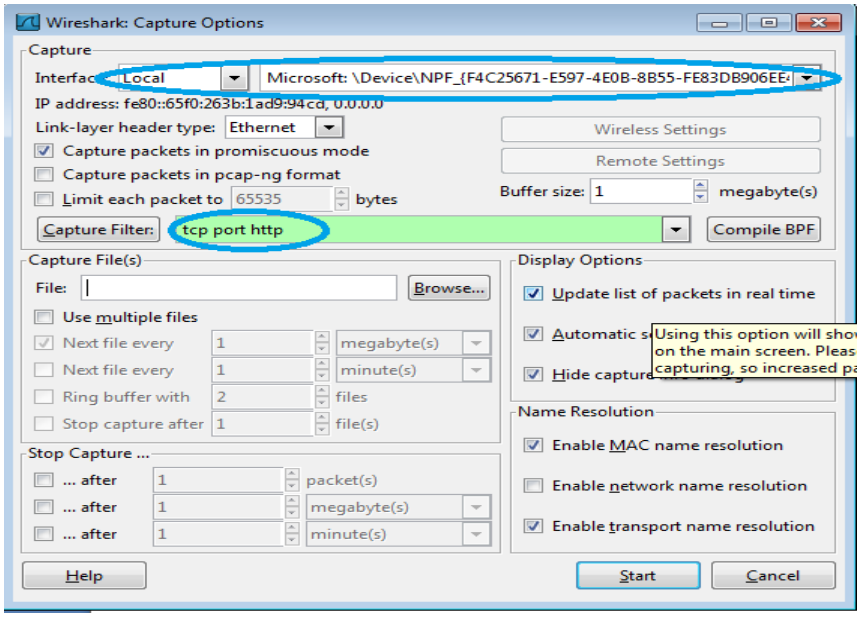

Figura Nº 6.23: Servidor WEB sin respuesta
Autor: Fernanda Conterón

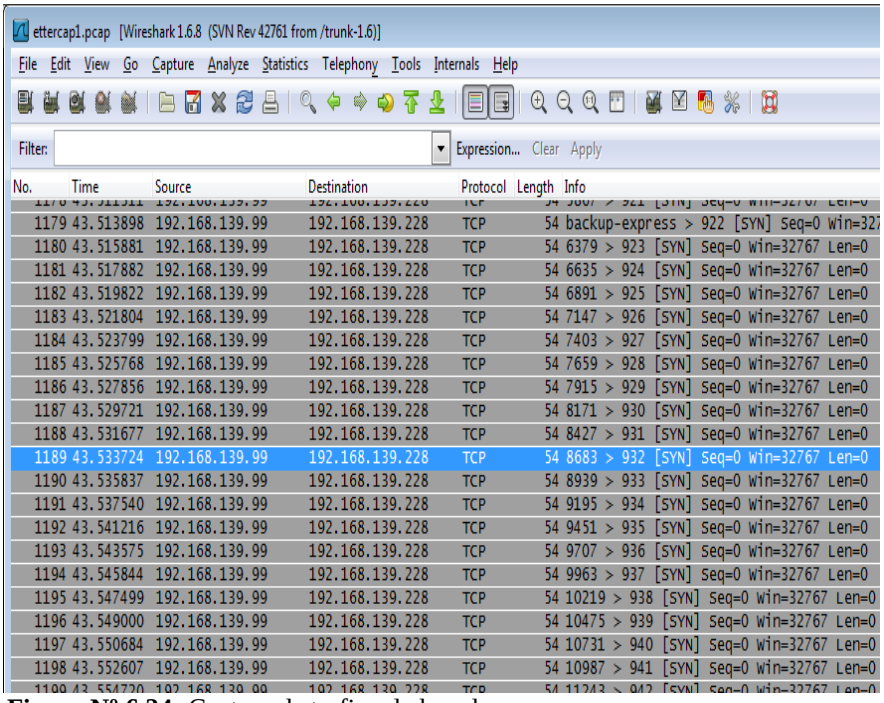

Figura Nº 6.24: Captura de trafico de la red
Fuente: Wireshark-win32-1.6.4

En la ilustración de la Figura Nº 6.24 representa la captura del tráfico de red en tiempo real con Wireshark, en la cual se observar un ataque de Denegación de Servicio (*DoS*) a pequeña escala, el cual lo realizamos con La herramienta Ettercap a modo de prueba. En el servidor WEB está instalado Apache 2.2.3 en la máquina 192.X.X.228 y se observa gran cantidad de segmentos TCP con el *flag*

SYN activados desde una misma IP, que no reciben respuesta alguna por parte del servidor WEB.

Se puede ver, de forma gráfica, la secuencia de paquetes seleccionando en el menú **STATISTICS - FLOW GRAPH**. Esta herramienta nos facilita en numerosas ocasiones seguir el comportamiento de conexiones TCP, ya que, como se ve en la Figura Nº 6.25, describe de forma muy intuitiva mediante flechas, el origen y destino de cada paquete, resaltando los *flag* activos que intervienen en cada sentido de la conexión.

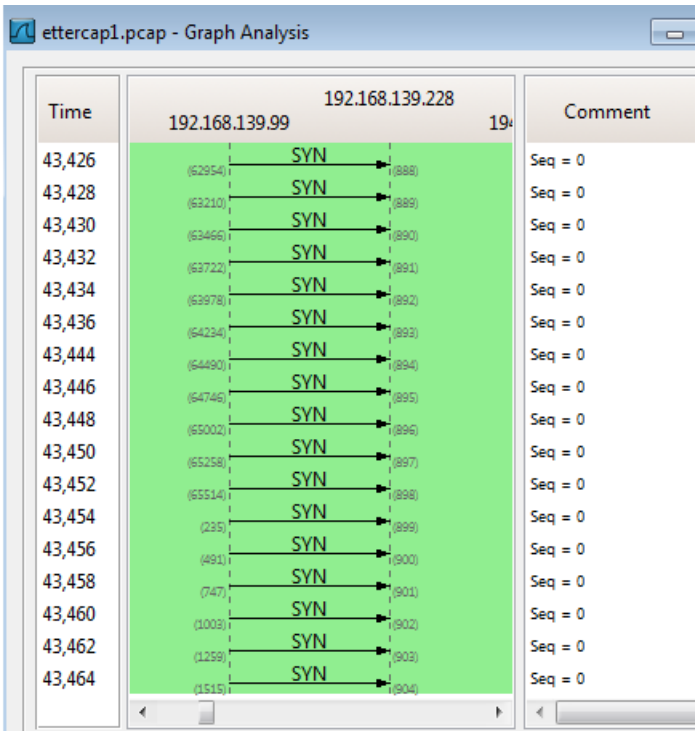

Figura Nº 6.25: Captura de trafico de la red (Forma grafica)
Fuente: Wireshark-win32-1.6.4

Con el análisis de la captura de tráfico se demuestra que se puede detectar un ataque de esta escala a los protocolos HTTP, SMTP y FTP.

6.6.5.3.2.3. Contramedida

Actualizar la versión del servicio WEB Apache 2.3

Se debe implementar un sistema de prevención de intrusos (IPS) para que bloquee a los hosts que están intentando realizar una actividad ilegal de tal forma que el

atacante se quede impedido de entrar al servicio puesto que el IPS le bloquea a nivel de red.

6.6.5.3.3. Cambiar imagen de página WEB

- Ettercap NG-0.7.3 en Backtrack

Para modificar las imágenes de la página web se utilizará la herramienta Ettercap para ello se debe crear un filtro para lo cual se debe crear un archivo .filter en este caso se crea el archivo denominado **cambiar_imagen_web.filter** con el siguiente código:

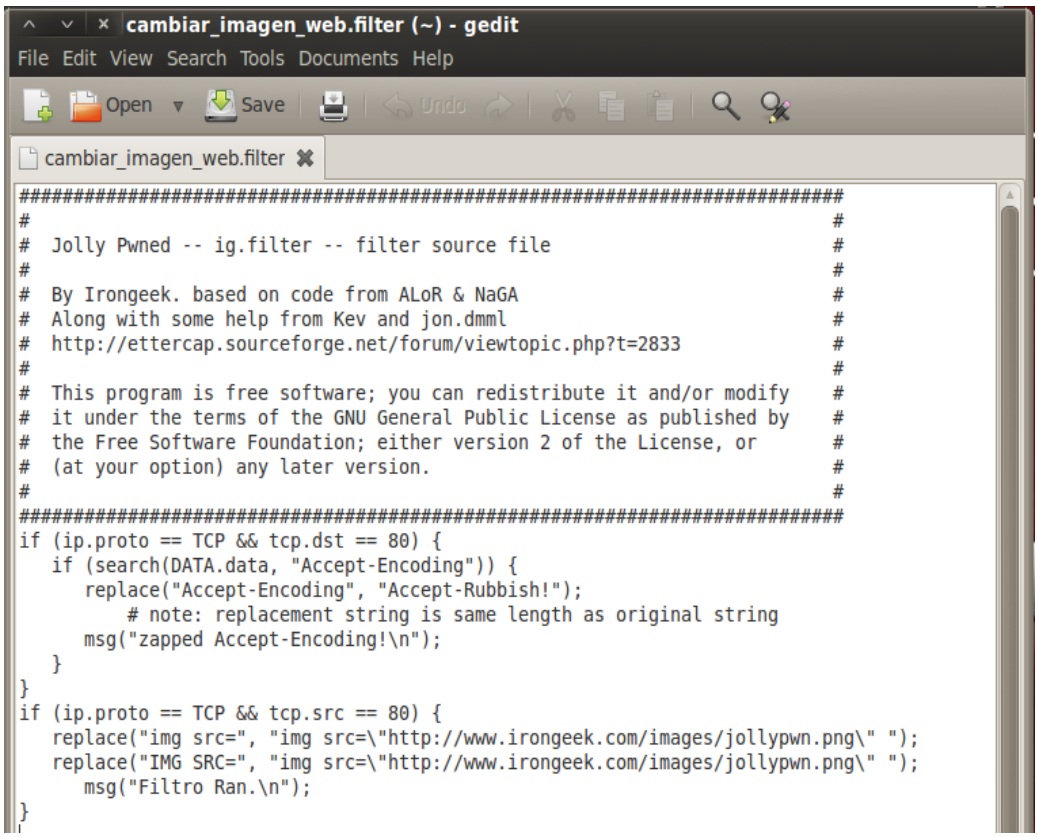

Figura Nº 6.26: Filtro para cambiar imagen de pagina web – Ettercap
Autor: Fernanda Conterón

Posteriormente se compila el archivo creado anteriormente en línea de comandos el cual se llamará cambiarimagenweb.ef:

cambiar_imagen_web.filter – o cambiarimagenweb.ef

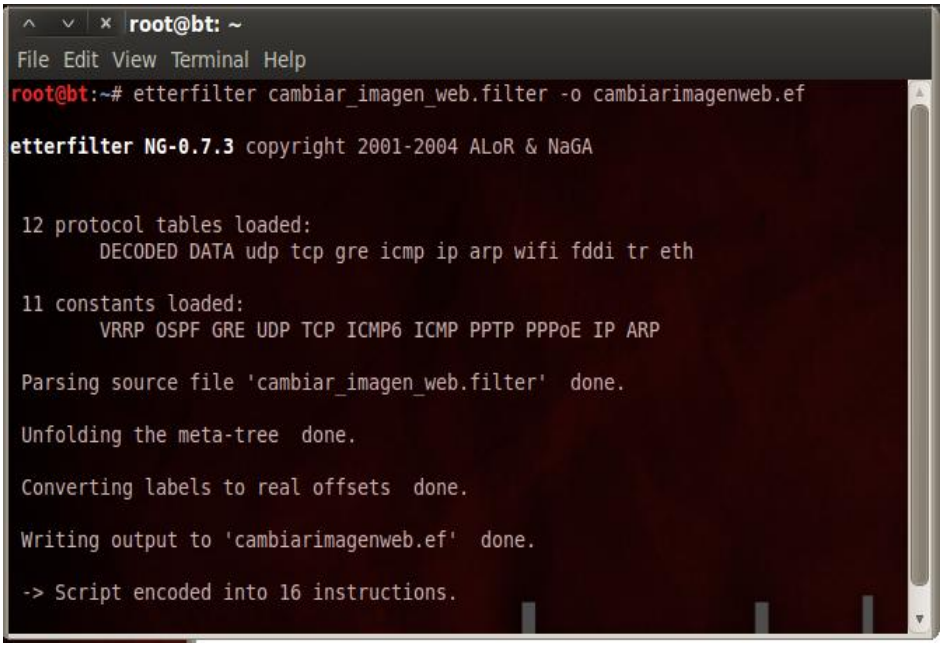

Figura Nº 6.27: Compilación de filtro – Ettercap
Autor: Fernanda Conterón

En el menú de Ettercap escoger la opción **FILTER - LOAD A FILTER - HOME - cambiarimagenweb.ef**

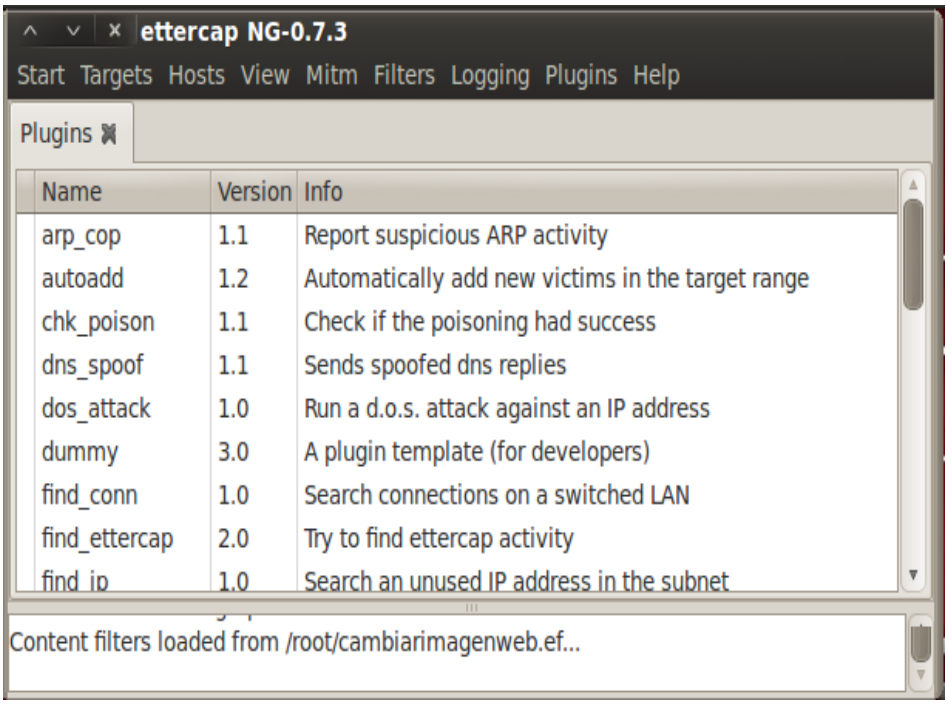

Figura Nº 6.28: Ejecución del filtro – Ettercap
Autor: Fernanda Conterón

A continuación se presenta la página web disponible para cualquier usuario:

Figura Nº 6.29 Página web original
Autor: Fernanda Conterón

Al iniciar la sesión de la página web, esta está alterada, se ha cambiado la imagen del Ministerio de Salud Publica por una imagen hacker.

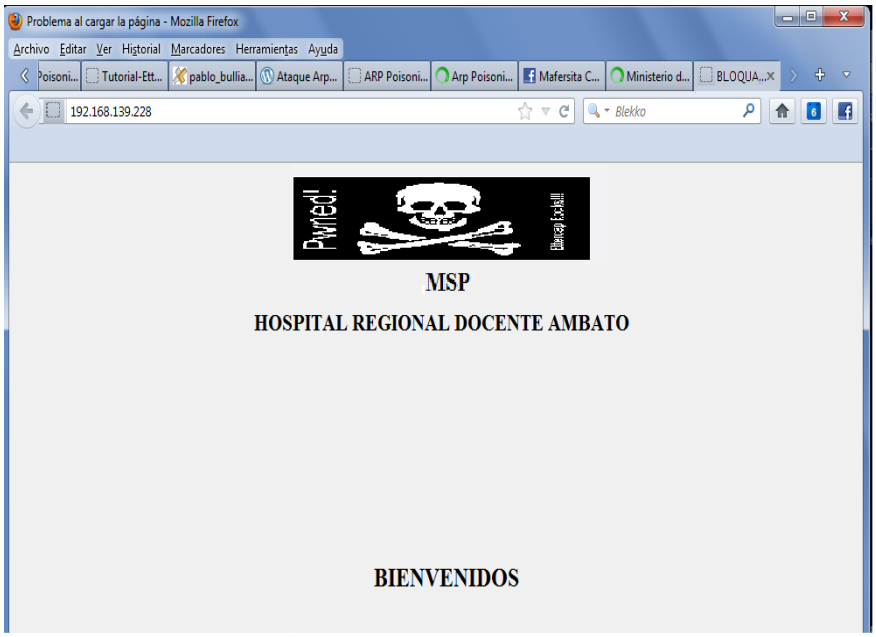

Figura Nº 6.30: Pagina web alterada (Imagen cambiada)
Autor: Fernanda Conterón

6.6.5.3.3.1. Contramedida

Implementar un sistema de prevención de intrusos (IPS) para que bloquee a los hosts que están intentando realizar una actividad ilegal de tal forma que el

atacante se quede impedido de entrar al servicio puesto que el IPS le bloquea a nivel de red.

6.6.5.4. Informe Técnico

Se desarrollo el informe técnico de las vulnerabilidades que se encontraron en los Servidores WEB, MAIL y FTP de la red del Hospital Regional Docente Ambato.

HOSPITAL REGIONAL DOCENTE AMBATO

INFORME TÉCNICO

DE VULNERABILIDADES ENCONTRADAS MEDIANTE LA TÉCNICA SNIFFER EN LOS SERVIDORES WEB, MAIL Y FTP

Departamento de sistemas

Seguridad en redes

Fernanda Conterón

2012

Índice

INTRODUCCIÓN

La Red interna del Hospital Regional Docente Ambato se ha incrementando en su infraestructura física y lógica día tras día, la comunicación dentro (correos, archivos) y fuera (Internet) de la institución es una necesidad para los usuarios finales utilizándola en un sin número de tareas, pero no todo es seguro y transparente, así como se ha incrementando la tecnología, también se ha incrementado las amenazas a las que está expuesta la red, al explotar las vulnerabilidades se convierte en un riesgos potencial para la integridad de la información.

Desde que el usuario final hace uso de la red interna ya sea solo para navegar por internet o para transmitir alguna información o archivo a los diferentes departamentos, desde ese momento está corriendo el riesgo que una persona mal intencionada realice un ataque mediante un sniffer, mediante este tipo de ataque, el delincuente informático puede obtener información valiosa o confidencial y construir ataques más elaborados, en apoyo de los datos obtenidos por esta técnica.

Los usuarios pueden ser víctimas sin ser conscientes de ello, dando como resultado el desconocimiento de las medidas a tomar o el impacto del riesgo que están expuesto, la detección de las vulnerabilidades de los servidores tanto web, mail y ftp por medio de la Técnica Sniffing son de importancia para disminuir la inseguridad alcanzada.

OBJETIVOS

2.1 Objetivo general

Determinar cuáles son las vulnerabilidades existentes en los servidores WEB, MAIL y FTP mediante la técnica Sniffer como medio de detección.

2.2 Objetivo especifico

- Analizar las vulnerabilidades encontradas.
- Priorizar las vulnerabilidades de los servidores según los niveles de riesgos.

3. DESARROLLO

3.1 Herramienta utilizada

Para la detección de las vulnerabilidades existentes en los servidores WEB, MAIL y FTP por medio de la Técnica Sniffing en el Hospital Regional Docente Ambato se determino y se utilizó las herramientas Sniffers:

- Ettercap
- Caín & Abel
- Wireshark

3.2 Presentación de los Hallazgos y Resultados

Debido a la naturaleza de las herramientas utilizadas en algunas de las pruebas a los servidores seleccionados, no se disponen de reportes formales o estructurados de los análisis realizados. En virtud de tal hecho se listará únicamente las vulnerabilidades encontradas.

Las vulnerabilidades encontradas se definen de acuerdo al nivel de riesgo que puede existir frente a un ataque.

SERVIDOR DE WEB

- **Herramientas utilizadas:**

  Caín & Abel
  Ettercap
  Wireshark

- **Pruebas realizadas:**

  Main in the Middle
  Denegación de Servicios

- **Puertos abiertos**

  Port: 80 – HTTP

Port: 443 – HTTPS

VULNERABILIDADES ENCONTRADAS

a) Nivel alto

Se encontraron las siguientes vulnerabilidades:

El servidor no ofrece ningún tipo de protocolo criptográfico por lo que es posible capturar contraseñas de páginas web seguras y no seguras en texto plano.

Factor de riesgo: alto

Es posible colapsar el servidor utilizando el ataque mediante "Denegación de Servicios".

Factor de riesgo: alto

b) Nivel medio:

Servidor apache desactualizado versión Apache 2.3.

Factor de riesgo: medio

La pagina web Apache 2.3 es vulnerable a modificaciones de las imágenes y de texto.

Factor de riesgo: medio

c) Nivel Bajo:

No se encontraron vulnerabilidades de nivel bajo.

SERVIDOR DE CORREO

- **Herramienta utilizada:**

  Caín & Abel
  Wireshark

- **Pruebas realizadas:**

  Main in the Middle
  Denegacion de Servicios

- **Puertos abiertos**

  Port: 00025 – SMTP

VULNERABILIDADES ENCONTRADAS

a) Nivel Alto:

Se encontraron las siguientes vulnerabilidades:

El servidor no ofrece ningún tipo seguridad en la transmisión de la información por lo que es posible capturar los datos que viajan por la red.

Factor de riesgo: alto

El servidor es propenso a ataque "Denegación de Servicios", dejando sin servicio de correo a los clientes.

Factor de riesgo: alto

b) Nivel medio:

No se encontraron vulnerabilidades de nivel medio.

c) Nivel Bajo:

No se encontraron vulnerabilidades de nivel medio.

SERVIDOR FTP

- **Herramienta utilizada:**

  Caín & Abel
  Wireshark

- **Pruebas realizadas:**

  Main in the Middle

Denegacion de Servicios

- **Puertos abiertos**

  Port: 21 – FTP

VULNERABILIDADES ENCONTRADAS

Se encontraron las siguientes vulnerabilidades:

a) Nivel alto:

El servidor no ofrece ningún tipo de protocolo criptográfico por lo que es posible capturar contraseñas y archivos, viajan en texto plano.

Factor de riesgo: alto

Es posible colapsar el servidor utilizando el ataque mediante "Denegación de Servicios".

Factor de riesgo: alto

b) Nivel medio:

No se encontraron vulnerabilidades de nivel medio.

c) Nivel Bajo:

No se encontraron vulnerabilidades de nivel medio.

4. Conclusiones

Después de haber realizado las pruebas necesarias en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato con las herramientas sniffers Caín & Abe, Ettercap y Wiresahrk hemos encontrado que:

a) Se tiene servicios de HTTP, correo y FTP, debido a su configuración sin seguridad (protocolos no cifrados) estos pasan las credenciales de autenticación en texto plano, las cuales pueden ser capturadas por un atacante con solo activar un Sniffer en la red (programa de captura de datos). El atacante hará uso de esta información para acceder a la información de los buzones de correo, logrando información sensible, como también lograr suplantar identidad del usuario.

b) También el personal que maneja páginas web seguras (https) no tiene una educación o instrucción sobre el tratamiento de certificados de autentificación y sus credenciales son obtenidas fácilmente con certificados falsos y cabe destacar la simplicidad en el uso de las claves, no se hace uso de procedimientos de manejo de credenciales y custodia de claves que permitan asegurarlas y tener contraseñas más robustas.

c) El servidor WEB, Apache 2.3, es vulnerable a ataques de denegación de servicios (DoS) interrumpiendo el servicio y sacando de servicio a la página web de manera definitiva y temporal, impidiendo que los usuarios regulares no puedan tener acceso.

d) La página web del HRDA no tiene la seguridad necesaria ya que permite modificaciones de imágenes y texto causando al usuario confusión o al momento de usar este sitio.

e) Cualquier usuario que se conecte a la red del HRDA puede activar un sniffer sin que el administrador se dé cuenta, no existe un control para este tipo de software.

5. Recomendaciones

a) Usar protocolos y algoritmos, que usen autenticación de doble vía o criptografía para comunicarse. Emplear contraseñas fuertes para que en caso de que sea capturado por ejemplo con el algoritmo de encriptación MD5, la ruptura (o el crackeo) del mismo sea algo casi imposible.

b) Crear medidas para la aplicación de claves más fuertes que cumplan con las normas de elección y protección establecidas en el Estándar ISO 270001.

c) Capacitar al personal que utiliza Internet sobre certificados de autenticación al ingresar a páginas web seguras.

d) Implementar un sistema de prevención de intrusos (IPS) para que bloquee a los hosts que están intentando realizar una actividad ilegal de tal forma que el atacante se quede impedido de entrar al servicio puesto que el IPS le bloquea a nivel de red.

e) Instalar un Sistema de Detección de Intrusos (IDS) para detectar cuando se está produciendo un ataque Sniffing o escaneo de puertos.

f) Verificar las vulnerabilidades a los servidores WEB, MAIL y FTP con herramientas sniffer en forma periódica.

g) Actualizar las versiones de los servicios implementados en los servidores dedicados de frente al Internet.

Cuadro N° 6.4: Plan de acción

ETAPAS	METAS	ACTIVIDADES	RECURSOS	PRESUPUESTO	RESPONSABLE	TIEMPO (SEMANA)
Sensibilización	**Inicio:** 13 de Marzo **Hasta:** 20 de Abril **Porcentaje:**10%	• Establecer un acercamiento con el Jefe de Sistemas. • Conocer el estado actual de la red del Hospital. • Conocer el software y hardware actual del hospital.	Computadora Internet Transporte Cámara	20.00 Dólares	La investigadora Tutor Jefe del departamento de Sistemas	6 semanas
Ejecución	**Inicio:** 23 de Abril **Hasta:** 13 de Julio **Porcentaje:**70%	• Determinación de la técnica Sniffer adecuada. • Instalar el software seleccionado • Ejecutar la técnica sniffer y encontrar las vulnerabilidades en los servidores WEB, MAIL y FTP. • Elaborar el informe técnico de las vulnerabilidades de los servidores WEB, MAIL y FTP. • Dar conclusiones y recomendaciones de los problemas encontrados en la red del HRDA.	Computadora Internet Transporte Impresiones Software	80.00 Dólares	La investigadora Tutor Jefe del departamento de Sistemas	12 semanas
Evaluación	**Inicio:** 16 de Junio. **Hasta:** 27 de Julio. **Porcentaje:**20%	• Revisión por el tutor. • Revisión por el Jefe del departamento de Sistemas.	Computadora Impresiones Anillado Cds Transporte	100.00 Dólares	La investigadora Tutor Jefe del departamento de Sistemas	2 semanas

Autor: Fernanda Conterón

6.7. Administración de la propuesta

Los responsables de evaluar el informe técnico de las vulnerabilidades encontradas de los servidores WEB, MAIL y FTP de la red del Hospital Regional Docente Ambato es el jefe del área de sistemas de la institución y sus funciones son:

- Analizar las vulnerabilidades que se encontraron al ejecutar el Sniffing en la red.
- Identificar las posibles soluciones que se pueden brindar a cada vulnerabilidad existente.
- Ejecutar las soluciones necesarias para cada una de las vulnerabilidades que se detallan en el informe.
- Mantener periódicamente una revisión de las configuraciones de los servidores.
- Realizar la encriptación de las contraseñas de los sistemas.
- Comunicar a todos los usuarios las políticas informáticas que se manejan en el Hospital Regional Docente Ambato.
- Monitorear permanentemente la red y administrar de una mejor manera los recursos.
- Actualizar el software de los sistemas operativos según las necesidades de la entidad.

6.8. Plan de monitoreo y evaluación de la propuesta

Para la evaluación y monitoreo de la propuesta se ha seguido como base el siguiente cuadro:

El cuadro contiene las preguntas necesarias para poder monitoria los pasos necesarios que se llevaron en la propuesta así como su evaluación.

Cuadro Nº 6.5: Monitoreo y evaluación

PREGUNTAS BÁSICAS	EXPLICACIÓN
¿Quiénes solicitan evaluar?	La Facultad de Ingeniería en Sistemas Electrónica e Industrial, y el Hospital Regional Docente Ambato
¿Por qué evaluar?	Porque se necesita establecer opiniones claras de lo desarrollado en la propuesta y de su incidencia en el problema.
¿Para qué evaluar?	Para comprobar que los objetivos planteados de la propuesta se hayan cumplido, además de comprobar que el modelo operativo este de acurdo al tema propuesto y que su desarrollo funcione para la solución del problema.
¿Qué evaluar?	Se evaluaran cada uno de los aspectos que conforman la propuesta principalmente los objetivos planteados, el contenido del modelo operativo, las conclusiones y recomendaciones que se plantean.
¿Quién evalúa?	Los encargados de evaluar son el tutor y el departamento de sistemas del HRDA.
¿Cuándo evaluar?	Cuando la propuesta esté terminada y cuando ya sea implantada las soluciones correctivas a las vulnerabilidades de los servidores WEB, MAIL y FTP.
¿Cómo evaluar?	Con una nueva ejecución de la técnica sniffer para comprobar las vulnerabilidades a las que estaban expuestos los servidores WEB, MAIL y FTP estén solucionados
¿Con qué evaluar?	Se evaluara mediante revisiones periódicas de los implicados en la evaluación de la propuesta.

Autor: Fernanda Conterón

6.9. Conclusiones

Después de haber realizado las pruebas necesarias en los servidores WEB, MAIL y FTP del Hospital Regional Docente Ambato con las herramientas sniffers Caín & Abel, Ettercap y Wireshark hemos encontrado que:

a) Se tiene servicios de HTTP, correo y FTP, debido a su configuración sin seguridad (protocolos no cifrados) estos pasan las credenciales de autenticación en texto plano, las cuales pueden ser capturadas por un atacante con solo activar un Sniffer en la red (programa de captura de datos). El atacante hará uso de esta información para acceder a la información de los buzones de correo, logrando información sensible, como también lograr suplantar identidad del usuario.

b) También el personal que maneja páginas web seguras (https) no tiene una educación o instrucción sobre el tratamiento de certificados de autentificación y sus credenciales son obtenidas fácilmente con certificados falsos y cabe destacar la simplicidad en el uso de las claves, no se hace uso de procedimientos de manejo de credenciales y custodia de claves que permitan asegurarlas y tener contraseñas más robustas.

c) El servidor WEB, Apache 2.3, es vulnerable a ataques de denegación de servicios (DoS) interrumpiendo el servicio y sacando de servicio a la página web de manera definitiva y temporal, impidiendo que los usuarios regulares no puedan tener acceso.

d) La página web del HRDA no tiene la seguridad necesaria ya que permite modificaciones de imágenes y texto causando al usuario confusión o al momento de usar este sitio.

e) Cualquier usuario que se conecte a la red del HRDA puede activar un sniffer sin que el administrador se dé cuenta, no existe un control para este tipo de software.

6.10 Recomendaciones

a) Usar protocolos y algoritmos, que usen autenticación de doble vía o criptografía para comunicarse. Emplear contraseñas fuertes para que en caso de que sea capturado por ejemplo con el algoritmo de encriptación MD5, la ruptura (o el crackeo) del mismo sea algo casi imposible.

b) Crear medidas para la aplicación de claves más fuertes que cumplan con las normas de elección y protección establecidas en el Estándar ISO 270001.

c) Capacitar al personal que utiliza Internet sobre certificados de autenticación al ingresar a páginas web seguras.

d) Implementar un sistema de prevención de intrusos (IPS) para que bloquee a los hosts que están intentando realizar una actividad ilegal de tal forma que el atacante se quede impedido de entrar al servicio puesto que el IPS le bloquea a nivel de red.

e) Instalar un Sistema de Detección de Intrusos (IDS) para detectar cuando se está produciendo un ataque Sniffing o escaneo de puertos.

f) Verificar las vulnerabilidades a los servidores WEB, MAIL y FTP con herramientas sniffer en forma periódica.

g) Actualizar las versiones de los servicios implementados en los servidores dedicados de frente al Internet.

6.11. Bibliografía

Bibliografía

ARENAS, David; (2003). “Herramienta de monitoreo de trafico”, sniffer España, Cataluña, cuarta edición, Sybex, Inc. ISBN, pág. 92, “módulos del Sniffers”

HATCH, Brian;(2001). “Hackers en Linux”, Sniffer, España, Arabaca, primera edición, Fareso S. A., pág. 244, “Uso del Sniffer”

STRASSBERG, Keith; (2002). “Firewalls”, Intranet, España, Madrid, Primera edición, Mc Graw Hill, Pág. 50, “Intranet”

MACLURE, Stuart; (2000). “HACKERS Secretos y soluciones para la seguridad de redes”, Hackers, España, Madrid, Primera edición, Mc Graw Hill, pág. 269, “Funcionamiento del sniffer”.

COSTAS, Jesús; (2011). “Seguridad Informática”, Auditorias Informáticas, Colombia, Bogotá, Primera Edición, Ra-Ma, pág. 294, “Auditoría de seguridad de sistemas de información”

SIERRA, Manuel; (2011). “Arquitectura cliente - servidor” Que es un servidor, Pág. 5, http://www.aprenderaprogramar.com/index.php?option=com_attachments&task=download&id=487

PARRA, David; (2011). “Seguridad alta disponibilidad”, Ettercap, pág. 3, 4 http://dasubipar.net23.net/Tutorial-Ettercap.pdf

VELURTªAS, Facundo Javier, (2009). “Optimización de enlaces en redes ip control de tráfico”, Características generales de TCP/IP, pág. 11,

SUAREZ, Eduardo (2009). “Redes wlan”, Wireshark, pág. 3.

GARCÍA, Joaquín (2010). “Ataques a redes TCP/IP”, Escucha de redes, pág. 20.

Linkografía

Asamblea Nacional del Ecuador, (2008), Constitución del Ecuador, Fundamentación legal, Recuperado en el 12 de Diciembre del 2011, http://www.asambleanacional.gov.ec/documentos/Constitucion-2008.pdf.

RaiSE, (2005), Arquitectura cliente/servidor, Servidor, Recuperado en el 16 de Diciembre del 2011, http://www.misrespuestas.com/que-es-un-servidor-web.html.

Wikypedia, (2011), Auditoria informática, Auditoria de sistemas informáticos, Recuperado en el 16 de Enero del 2012, http://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_de_sistemas_de_informaci%C3%B3n.

EASAsegurity, (2006), Hacking ético, "Hackers", Recuperado en el 16 de Enero del 2012 http://www.esa-security.com/web/servicios/hacking.htm,

RaiSe (2008), Hacking y Seguridad, Sniffer, Recuperado en el 20 de Enero del 2012 http://www.angelfire.com/ult/lupa/programadores/hacking.htmlweb/servidor-web-apache/servidor-http-en-linux.

Mundo Cisco, (2003), Sniffer, Usos del Sniffer, Recuperado en el 20 de Enero del 2012 http://www.rankia.com/foros/consumo/temas/656938-tecnica-sniffing-red.

Monografía.com, (2000), Intranet, Intranet, Recuperado en el 20 de Enero del 2012 http://www.monografias.com/trabajos5/queint/queint.shtml.

Anónimo, (2006), Seguridad en redes, Análisis de trafico de red, Recuperado en el 21 de Enero del 2012 http://www.internet-solutions.com.co/ser_analisis_trafico.php.

Monografías.com, (2000), Servidor web, Servidor web, Recuperado en el 22 de Enero del 2012, http://www.monografias.com/trabajos75/servidores-web/servidores-web.shtml,

Anónimo, (2009) Sniffer, Funcionamiento, Recuperado en el 21 de Enero del 2012 http://www.monografias.com/trabajos75l-SNIFFERS.htm, “”.

Scrild, (“s/f”), Servidor mail, Servidor de correo, Recuperado en el 22 de Enero del 2012, http://es.scribd.com/doc/8908926/Conceptos-Servidor-de-Correo,

Anónimo, (2011), Como funciona un servidor ftp, Servidor ftp, Recuperado en el 22 de Enero del 2012, http://www.nosolounix.com/2011/11/como-funciona-realmente-el-servicio-ftp.html.

DOMÍNGUEZ, Edgar, (2007), Computación, Escuela, GNU/Linux, Kismet, Recuperado en el 22 de Enero del 2012 http://genomorro. wordpress.com/2007/09/23/usando-kismet-y-aircrack-ng-para-descriptar-claves-wep/.

JASON, Jeff (2008), Análisis Capturas Tráfico Red. Interpretación Datagrama IP, tcpdump (Parte I), Recuperado en el 2 de Mayo del 2012, http://es.scribd.com/doc/49333184/Analisis-Capturas-Trafico-Red.

Desarroloweb.com, (2006), Definición y a quien afecta Cross-Site-Scripting, Ataque Xss, Recuperado en el 10 de Mayo del 2012, http://www.desarrolloweb.com/articulos/definicion-y-a-quien-afecta-croos-site-scripting.html.

Wikipedia, (2005), Open Relay, Ataque Openrelay, Recuperado en el 2 de Mayo del 2012 http://enciclopedia.us.es/index.php/Open_Relay.

Anonimo(s/f), Tipos de protocolos, Protocolo TCP/IP, Recuperado en el 22 de Enero del 2012, http://fmc.axarnet.es/redes/tema_06.htm.

Slideshare.net (2010), Análisis de trafico de red LAN, Trafico de red, Recuperado en el 1 de Junio del 2012, http://www.slideshare.net/chichoAnitec/sniffer-7740876.

Internet (2005), Caín & Abel, Características Caín y Abel, Recuperado en el 1 de Junio del 2012, http://vtroger.blogspot.com/2005/11/cain-y-abel.html.

Scribd (2012), Sniffer con ataque middle in man usando Caín y Abel, Protocolo HTTPS, Recuperado en el 6 de Junio del 2012 http://es.scribd.com/doc/52940650/Sniffer-con-ataque-middle-in-man-usando-cain-y-abel.

Internet (2009), Guía para la elaboración de informe técnico, Informe técnico, Recuperado en el 20 de Junio del 2012, http://www.conarroz.com/UserFiles/File/GuiaParaLaRedaccionDeInformesTecnicos.pdf.

HERRERA, Omar (2005), Seguridad Informática y Seguridad de Redes, IDS – IPS, Recuperado en el 22 de Junio del 2012 http://www.multisoft.com.co/soluciones-para-perimetro/sistema-de-prevencion-de-intrusos-de-red-ips.html.

6.12. Anexos

ANEXO Nº 01

ISO 27001:2005

ISO 27001 establece los requisitos que debe cumplir un SGSI (Sistema para la Gestión de la Seguridad de la Información) para su certificación en términos de procesos de seguridad a nivel empresarial.

Anexo A.- Objetivos de control y controles

A.5	**Política de Seguridad**		
	A.5.1	Política de Seguridad de la Información	Para proporcionar una dirección de gestión y apoyo a la seguridad de la información, de conformidad con los requerimientos del negocio y de las leyes y reglamentos pertinentes.
A.6	**Organización y Seguridad de la Información**		
	A.6.1	Organización interna	Para gestionar la seguridad de la información dentro de la organización.
	A.6.2	Partes externas	Para mantener la seguridad de la información de la organización y las instalaciones de procesamiento de información que se tiene acceso, procesados, comunicados a, o administrados por entidades externas.
A.7	**Gestión de Activos**		
	A.7.1	La responsabilidad de los activos	Para lograr y mantener la adecuada protección de los activos de la organización.
	A.7.2	Información de Clasificación	Para garantizar que la información reciba un nivel adecuado de protección.
A.8	**Recursos Humanos Seguridad**		
	A.8.1	Antes de Empleo	Para asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades, y son adecuados para las funciones que se consideran para, y para reducir el riesgo de robo, fraude o uso indebido de las instalaciones.
	A.8.2	Durante el Empleo	Para asegurarse de que todos los empleados, contratistas y usuarios de terceras partes son conscientes de las amenazas de seguridad de la información y preocupaciones, sus responsabilidades y obligaciones, y están equipados para apoyar la política de seguridad de la organización en el curso de

			su trabajo normal, y para reducir el riesgo de error humano.
	A.8.3	La terminación o cambio de empleo	Para asegurar que los empleados, contratistas y terceros usuarios salir de una organización o cambio en el empleo de una manera ordenada.
A.9	**Seguridad física y ambiental**		
	A.9.1	Zonas seguras	Para prevenir el acceso físico no autorizado, daño e interferencia a las instalaciones de la organización y la información.
	A.9.2	Equipamiento de seguridad	Para evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.
A.10	**Comunicaciones y Gestión de Operaciones**		
	A.10.1	Procedimientos operacionales y responsabilidades	Para garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.
	A.10.2	Servicio de Gestión de Entrega de terceros	Para implementar y mantener el nivel apropiado de la información de entrega y el servicio de seguridad en línea con acuerdos con terceros la prestación de servicios.
	A.10.3	Sistema de Planificación y aceptación	Para minimizar el riesgo de fallo de los sistemas.
	A.10.4	Protección contra ataques maliciosos y móviles	Para proteger la integridad del software y la información.
	A.10.5	Back-Up	Para mantener la integridad y la disponibilidad de instalaciones de procesamiento de la información y la información.
	A.10.6	Red de Gestión de la Seguridad	Para garantizar la protección de la información en las redes y la protección de la infraestructura de apoyo.
	A.10.7	Manejo del papel	Para evitar la divulgación no autorizada, modificación, eliminación o destrucción de bienes, y la interrupción de las actividades comerciales.
	A.10.8	Intercambio de Información	Para mantener la seguridad de la información y el software de intercambio dentro de una organización y con cualquier entidad externa.
	A.10.9	Servicios de Comercio Electrónico	Para garantizar la seguridad de los servicios de comercio electrónico, y su uso seguro.
	A.10.10	Monitoreo	Para detectar las actividades de procesamiento de información no autorizadas.
A.11	**Control de Acceso**		
	A.11.1	Requisito de Empresas de	Para controlar el acceso a la información

		Control de Acceso	
	A.11.2	Gestión de usuarios de acceso	Para garantizar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información.
	A.11.3	Responsabilidades del Usuario	Para prevenir acceso no autorizado, y el compromiso o robo de las instalaciones de procesamiento de la información y la información.
	A.11.4	Network Access Control	Para evitar el acceso no autorizado a servicios de red.
	A.11.5	Sistema operativo de control de acceso	Para evitar el acceso no autorizado a los sistemas operativos.
	A.11.6	Aplicación y control de acceso de información	Para evitar el acceso no autorizado a información de ayuda en los sistemas de aplicación.
	A.11.7	Informática móvil y teletrabajo	Para garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de teletrabajo.
A.12	**Sistemas de Información de Adquisiciones, Desarrollo y Mantenimiento**		
	A.12.1	Requisitos de Seguridad de los Sistemas de Información	Para garantizar que la seguridad es una parte integral de sistemas de información.
	A.12.2	Procesamiento correcto en aplicaciones	Para evitar errores, la pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.
	A.12.3	Controles criptográficos	Para proteger la confidencialidad, autenticidad o integridad de la información mediante cifrado.
	A.12.4	Seguridad de los ficheros del sistema	Para garantizar la seguridad de los archivos del sistema.
	A.12.5	Seguridad en los Procesos de Desarrollo y Soporte	Para mantener la seguridad de software de aplicación del sistema y la información.
	A.12.6	Técnico de gestión de vulnerabilidades	Para reducir los riesgos de la exploración de vulnerabilidades técnicas publicadas.
A.13	**Seguridad de la Información de Gestión de Incidentes**		
	A.13.1	De Reporte de Seguridad de la Información y Debilidades	Para garantizar la seguridad de la información los eventos y debilidades asociadas con los sistemas de información se comuniquen de una manera que permita las acciones correctivas oportunas que deban adoptarse.
	A.13.2	Gestión de Incidentes de Seguridad de la Información y Mejoras	Para garantizar un enfoque coherente y eficaz se aplica a la gestión de incidentes de seguridad de la información.

A.14	**Gestión de Continuidad**		
	A.14.1	Son los aspectos de la Gestión de la Continuidad del Negocio	Para contrarrestar las interrupciones a las actividades comerciales y proteger los procesos críticos de negocio de los efectos de los fallos principales de los sistemas de información o desastres y asegurar su pronta reanudación.
A.15	**Conformidad**		
	A.15.1	Cumplimiento de Requisitos Legales	Para evitar la violación de alguna-la, estatutarias, obligaciones reglamentarias o contractuales, así como de los requisitos de seguridad.
	A.15.2	Cumplimiento con las normas y estándares de seguridad y cumplimiento técnico	Para garantizar el cumplimiento de los sistemas con las políticas de seguridad organizativas y las normas.
	A.15.3	Sistemas de Información Consideraciones de auditoría	Para maximizar la eficacia y minimizar la interferencia desde / hacia el proceso de auditoría de sistemas de información.

ANEXO Nº 02

No. 1014

RAFAEL CORREA DELGADO

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que en el apartado g) del numeral 6 de la Carta Iberoamericana de Gobierno Electrónico, aprobada por el IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado, realizada en Chile el 1 de Junio de 2007, se recomienda el uso de estándares abiertos y software libre, como herramientas informáticas;

Que es el interés del Gobierno alcanzar soberanía y autonomía tecnológica, así como un significativo ahorro de recursos públicos y que el Software Libre es en muchas instancias un instrumento para alcanzar estos objetivos;

Que el 18 de Julio del 2007 se creó e incorporó a la estructura orgánica de la Presidencia de la República la Subsecretaría de Informática, dependiente de la Secretaría General de la Administración, mediante Acuerdo No. 119 publicado en el Registro Oficial No. 139 de 1 de Agosto del 2007;

Que el numeral 1 del artículo 6 del Acuerdo No. 119, faculta a la Subsecretaría de Informática a elaborar y ejecutar planes, programas, proyectos, estrategias, políticas, proyectos de leyes y reglamentos para el uso de Software Libre en las dependencias del gobierno central; y,

En ejercicio de la atribución que le confiere el numeral 9 del artículo 171 de la Constitución Política de la República

DECRETA:

Artículo 1.- Establecer como política pública para las entidades de la Administración Pública Central la utilización de software libre en sus sistemas y equipamientos informáticos.

Artículo 2.- Se entiende por software libre, a los programas de computación que se pueden utilizar y distribuir sin restricción alguna, que permitan su acceso a los códigos fuentes y que sus aplicaciones puedan ser mejoradas.

Estos programas de computación tienen las siguientes libertades:

a) Utilización del programa con cualquier propósito de uso común;

b) Distribución de copias sin restricción alguna;

c) Estudio y modificación del programa (Requisito: código fuente disponible); y,

d) Publicación del programa mejorado (Requisito: código fuente disponible).

Artículo 3.- Las entidades de la Administración Pública Central previa a la instalación del software libre en sus equipos, deberán verificar la existencia de capacidad técnica que brinde el soporte necesario para el uso de este tipo de software.

Artículo 4.- Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de software libre que supla las necesidades requeridas, o cuando esté en riesgo la seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno.

Para efectos de este decreto se comprende cómo seguridad nacional, las garantías para la supervivencia de la colectividad y la defensa de patrimonio nacional.

Para efectos de este decreto se entiende por un punto de no retorno, cuando el sistema o proyecto informático se encuentre en cualquiera de estas condiciones:

a) Sistema en producción satisfactoriamente y que un análisis de costo beneficio muestre que no es razonable ni conveniente una migración a software libre; y,

b) Proyecto en estado de desarrollo y que un análisis de costo - beneficio muestre que no es conveniente modificar el proyecto y utilizar software libre.

Periódicamente se evaluarán los sistemas informáticos que utilizan software propietario con la finalidad de migrarlos a software libre.

Artículo 5.- Tanto para software libre como software propietario, siempre y cuando se satisfagan los requerimientos, se debe preferir las soluciones en este orden:

a) Nacionales que permitan autonomía y soberanía tecnológica;

b) Regionales con componente nacional;

c) Regionales con proveedores nacionales;

d) Internacionales con componente nacional;

e) Internacionales con proveedores nacionales; y,

f) Internacionales.

Artículo 6.- La Subsecretaría de Informática como órgano regulador y ejecutor de las políticas y proyectos informáticos en las entidades del Gobierno Central deberá realizar el control y seguimiento de este decreto.

Para todas las evaluaciones constantes en este decreto la Subsecretaría de Informática establecerá los parámetros y metodologías obligatorias.

Artículo 7.- Encárguese de la ejecución de este decreto los señores ministros coordinadores y el señor Secretario General de la Administración Pública y Comunicación.

ANEXO Nº 03

LEY DE TRANSPARENCIA Y ACCESO A INFORMACION PÚBLICA

Decreto Ejecutivo 2471, Registro Oficial 507 de 19 de Enero del 2005

Lucio Gutiérrez Borbúa

PRESIDENTE CONSTITUCIONAL DE LA REPUBLICA

Considerando:

Que la Constitución Política de la República, en el artículo 81, establece que el Estado garantizará el derecho a acceder a fuentes de información y no existirá reserva respecto de informaciones que reposen en archivos públicos, excepto de los documentos para los que tal reserva sea exigida por razones de defensa nacional y por causas expresamente establecidas en la ley;

Decreto Ejecutivo 2471, Registro Oficial 507 de 19 de Enero del 2005

Lucio Gutiérrez Borbúa

PRESIDENTE CONSTITUCIONAL DE LA REPUBLICA

Decreta:

Expedir el REGLAMENTO GENERAL A LA LEY ORGANICA DE TRANSPARENCIA Y ACCESO A LA INFORMACION PUBLICA

CAPITULO II

DE LA DIFUSION DE LA INFORMACION

Art. 6.- Obligatoriedad.- Todas las instituciones que se encuentren sometidas al ámbito de la Ley de Transparencia y Acceso a la Información, difundirán en forma, obligatoria y permanente, a través de su página web, la información mínima actualizada prevista en el artículo 7 de dicho cuerpo legal.

Esta información será organizada por temas, en orden secuencial o cronológico, de manera que se facilite su acceso.

Art. 7.- Garantía del Acceso a la Información.- La Defensoría del Pueblo será la institución encargada de garantizar, promocionar y vigilar el correcto ejercicio del derecho al libre acceso a la información pública por parte de la ciudadanía y el cumplimiento de las instituciones públicas y privadas obligadas por la ley a proporcionar la información pública; y, de recibir los informes anuales que deben presentar las instituciones sometidas a este reglamento, con el contenido especificado en la ley.

El Defensor del Pueblo está obligado a solicitar a las instituciones que no hubieran difundido claramente la información a través de los portales web, que realicen los correctivos necesarios. Para tal efecto exigirá que se dé cumplimiento a esta obligación dentro del término de ocho días.

El Defensor del Pueblo podrá delegar ésta y las demás facultades asignadas a él por la ley, a sus representantes en las diversas provincias, en aplicación del principio de descentralización y de conformidad con la Ley Orgánica de la Defensoría del Pueblo.

Art. 8.- De la Capacitación.- Los programas de difusión y capacitación dirigidos a promocionar el derecho de acceso a la información, deberán realizarse por lo menos una vez al año en cada una de las instituciones señaladas por la ley. De la misma manera deberán realizar anualmente actividades dirigidas a capacitar a la población en general sobre su derecho de acceso a la información.

La realización de estas actividades será vigilada por la Defensoría del Pueblo, organismo al cual deberá remitirse un informe detallado de la actividad.

CAPITULO III

DE LAS EXCEPCIONES AL ACCESO A LA INFORMACION PUBLICA

Art. 9.- Excepciones.- De conformidad con la Constitución y la Ley, no procede el derecho de acceso a la información pública sobre documentos calificados motivadamente como reservados por el Consejo de Seguridad Nacional y aquella

información clasificada como tal por las leyes vigentes, tal como lo dispone la Ley Orgánica de Transparencia y Acceso a la Información Pública.

La elaboración, manejo, custodia y seguridad de la información calificada como reservada por el Consejo de Seguridad Nacional, se sujetará a las regulaciones emitidas por el Comando Conjunto de las Fuerzas Armadas sobre la materia.

Nota: Artículo sustituido por Decreto Ejecutivo No. 163, publicado en Registro Oficial 33 de 7 de Junio del 2005.

Nota: Inciso segundo agregado por Decreto Ejecutivo No. 360, publicado en Registro Oficial 80 de 11 de Agosto del 2005.

Art. 10.- Información Reservada.- Las instituciones sujetas al ámbito de este reglamento, llevarán un listado ordenado de todos los archivos e información considerada reservada, en el que constará la fecha de resolución de reserva, período de reserva y los motivos que fundamentan la clasificación de reserva. Este listado no será clasificado como reservado bajo ningún concepto y estará disponible en la página web de cada institución.

ANEXO Nº 04

LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS

(Decreto No. 3496)

Gustavo Noboa Bejarano

PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

Considerando:

Que, el uso de sistemas de información y de redes electrónicas, incluida la Internet ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado.

Que, es necesario impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos.

Que, se debe generalizar la utilización de servicios de redes de información e Internet, de modo que éstos se conviertan en un medio para el desarrollo del comercio, la educación y la cultura.

Que, a través del servicio de redes electrónicas, incluida la Internet se establecen relaciones económicas y de comercio, y se realizan actos y contratos de carácter civil y mercantil que es necesario normarlos, regularlos y controlarlos, mediante la expedición de una Ley especializada sobre la materia.

Que, es indispensable que el Estado Ecuatoriano cuente con herramientas jurídicas que le permitan el uso de los servicios electrónicos, incluido el comercio electrónico y acceder con mayor facilidad a la cada vez más compleja red de los negocios internacionales.

En uso de sus atribuciones, expide la siguiente:

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS

TITULO V

DE LAS INFRACCIONES INFORMÁTICAS

CAPÍTULO I

DE LAS INFRACCIONES INFORMATICAS

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

Reformas al Código Penal

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

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

1. Inutilización de sistemas de alarma o guarda;

2. Descubrimiento o descifrado de claves secretas o encriptadas;

3. Utilización de tarjetas magnéticas o perforadas;

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

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

Artículo 63.- Añádase como segundo inciso del artículo 563 del Código Penal el siguiente: "Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando los medios electrónicos o telemáticos".

Artículo 64.- A continuación del numeral 19 del Art. 606 añádase el siguiente:
"..... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.".

ANEXO Nº 05

ENTREVISTA

EMPRESA: Hospital Regional Docente Ambato.

ENTREVISTADO: Sr. Danilo Naranjo (Jefe de Sistemas)

ENTREVISTADOR: María Fernanda Conterón Tene

LUGAR: Áreas de Sistemas

FECHA: 10 de Diciembre del 2011

OBJETIVO DE ESTUDIO: Medidas de protección en servidores para prevenir ataques SNIFFER en la red del Hospital Regional Docente Ambato.

1. **¿Cree Ud. que la red interna del Hospital Regional Docente Ambato es vulnerable a ataques Sniffing?**

   ……
   ……
   ……
   ……

2. **¿Ha utilizado algún medio para detectar dichas vulnerabilidades?**

   ……
   ……
   ……
   ……

3. **¿Cree Ud. necesario tomar medidas para la detección de vulnerabilidades?**

   ……
   ……
   ……
   ……

4. **¿Los datos que se transmite por la red interna están encriptados?**

   ……
   ……
   ……
   ……

5. **¿Alguna vez se ha comprometido la confidencialidad, integridad y disponibilidad de la información y de los servicios dentro de la institución?**

   ……
   ……
   ……
   ……
   ……
   ……

6. **¿Existen políticas de seguridad dentro de la institución?**

   ……
   ……
   ……
   ……
   ……
   ……

7. **Usted estaría interesado en que se utilice al sniffer como herramienta para detectar las vulnerabilidades que existen en los servicios WEB, MAIL y FTP de la red del HRDA simulando ser un atacante?**

   ……
   ……
   ……
   ……
   ……

ANEXO Nº 06

ENCUESTA
FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS

Encuesta dirigida al personal del Hospital Regional Docente Ambato., con el propósito de recopilar información necesaria para elaborar el proyecto de Estudio enfocado a las Medidas de protección sobre ataques SNIFFING en la red del Hospital Regional Docente Ambato

OBJETIVO: Determinar los parámetros de la red utilizada en el Hospital Regional Docente Ambato.

1. **¿Conoce Ud. que existen programas que pueden espiar o capturar todas las acciones que realiza en su computador y la información que se transmiten por la red?**

   a) Si ☐
   b) No ☐

2. **¿Ud. cree que al enviar y recibir información (datos o archivos) a través de la red interna del HRDA está seguro contra espionaje informático?**

   a) Si ☐
   b) No ☐
   c) No sabe ☐

3. **¿Cree Ud. Si sus correos electrónicos o cuentas personales están protegidos contra robo, perdida, espionaje de la información cuando usa la red del HRDA?**

   a) Si ☐
   b) No ☐
   c) No sabe ☐

4. **Conoce Ud. las políticas de seguridad informáticas para el manejo de la información y de la red del HRDA?**

   a) Si ☐
   b) No ☐

5. **¿Cómo considera Ud. el desempeño (tiempo de respuesta) de la red ante una petición de servicio o recursos (internet, correos, transferencia de archivos, etc…)?**

   a) Regular ☐
   b) Mala ☐
   c) Buena ☐
   d) Excelente ☐

6. **¿Ud. Sabe si la información que está bajo su responsabilidad ha sido?**

   a) Alterada ☐
   b) Eliminada ☐
   c) Copiada ☐
   d) No ha sucedido nada ☐

7. **¿Conoce Ud. que existen sitios web seguros (https) que evitan que la información y claves utilizadas puedan ser plagiadas?**

   a) Si ☐
   b) No ☐

8. **¿Sabe Ud. que es y el manejo de un certificado de autentificación que contiene las páginas web seguras?**

   a) Si ☐
   b) No ☐

GRACIAS POR SU COLABORACIÓN