UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL EN TELECOMUNICACIONES

TEMA:

"ESTUDIO PARA DETERMINAR LA PROTECCIÓN NECESARIA PARA EL LABORATORIO DE ELECTRÓNICA DE LA FACULTAD DE EDUCACIÓN TÉCNICA DE LA UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL"

Previa la obtención del Título de

INGENIERÍA EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL EN TELECOMUNICACIONES

ELABORADO POR:

STEPHANIA XIOMARA MAZZINI GOROTIZA

DIRECTOR DEL PROYECTO

Ing. María Luzmila Ruilova Aguirre

GUAYAQUIL – ECUADOR

Febrero 2014

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

INGENIERÍA EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL EN TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por la Srta. Stephania Xiomara Mazzini Gorotiza como requerimiento parcial para la obtención del título de INGENIERÍA EN TELECOMUNICACIONES CON MENCION EN GESTIÓN EMPRESARIAL EN TELECOMUNICACIONES

Guayaquil, Febrero de 2014

_____
Ing. María Luzmila Ruilova Aguirre
DIRECTORA

REVISADO POR

_____
Ing. Efraín Vélez Tacuri

_____
Ing. Luis Pinzón Barriga

_____
Ing. Miguel Heras Sánchez
RESPONSABLE ACADÉMICO

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

INGENIERÍA EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

YO, STEPHANIA XIOMARA MAZZINI GOROTIZA

DECLARO QUE:

El proyecto de grado denominado "ESTUDIO PARA DETERMINAR LA PROTECCIÓN NECESARIA PARA EL LABORATORIO DE ELECTRÓNICA DE LA FACULTAD DE EDUCACIÓN TÉCNICA DE LA UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Guayaquil, Febrero de 2014

LA AUTORA

_____

STEPHANIA XIOMARA MAZZINI GOROTIZA

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

INGENIERÍA EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, STEPHANIA XIOMARA MAZZINI GOROTIZA

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del proyecto titulado: "ESTUDIO PARA DETERMINAR LA PROTECCIÓN NECESARIA PARA EL LABORATORIO DE ELECTRÓNICA DE LA FACULTAD DE EDUCACIÓN TÉCNICA DE LA UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Guayaquil, Febrero de 2014

LA AUTORA

_____

STEPHANIA XIOMARA MAZZINI GOROTIZA

AGRADECIMIENTO

Agradezco primeramente a Dios, verdadera fuente de amor y sabiduría, por darme la oportunidad de existir, por mi vida, que la he vivido junto a él. Gracias por iluminarme darme fuerzas y caminar por tu sendero.

A mis padres y hermana, porque gracias a ellos sé que la responsabilidad se la debe vivir como un compromiso de dedicación y esfuerzo; por su incondicional apoyo, tanto al inicio como al final de mi carrera, por estar pendiente de mí en cada momento. Gracias por su ejemplo, dedicación y palabras de aliento porque nunca bajaron los brazos para que yo tampoco lo haga aun cuando todo se complicaba, los amo.

Un agradecimiento especial al Ing. Manuel Romero Paz, por su apoyo incondicional y compartir sus conocimientos a lo largo de mi carrera universitaria.

A cada uno de los catedráticos de la FETD que impartieron su conocimiento para lograr mi objetivo de convertirme en una profesional.

A mi tutora de tesis Ing. María Luzmila Ruilova Aguirre, por su apreciable gestión de tutoría para finalizar este trabajo de graduación.

LA AUTORA

_____

STEPHANIA XIOMARA MAZZINI GOROTIZA

DEDICATORIA

Dedico este proyecto de Tesis a mis padres que a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo en todo momento; depositando su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento en mi inteligencia y capacidad.

A mi hermana, que siempre me brindo un incondicional abrazo y me motivo y recordó que detrás de cada detalle existe el suficiente alivio para empezar nuevas búsquedas.

A mis familiares y amigos que de una u otra forma, con su apoyo moral me han incentivado a seguir adelante, a lo largo de toda mi formación como profesional.

LA AUTORA

_____

STEPHANIA XIOMARA MAZZINI GOROTIZA

RESUMEN

Este trabajo de investigación pretende explicar la necesidad de que la información debe mantenerse a salvo mediante procesos de seguridad y bajo este concepto se pretende presentar un estudio relativo a garantizar esa seguridad para el Laboratorio de Electrónica de la Facultad de Educación Técnica para el Desarrollo (FET) de la Universidad Católica de Santiago de Guayaquil (UCSG).

Para alcanzar el objetivo indicado se realizará un diagnóstico para determinar las fallas de seguridad presentes en el Laboratorio de Electrónica, eso permitirá determinar sus vulnerabilidades y de esta manera recomendar las seguridades que deberían implementarse para prevenirlas.

ABSTRACT

This research seeks to explain the need for the information must be kept safe by security processes and under this concept is to present a study on the security guarantee for the Electronics Laboratory, Faculty of Technical Education for Development (FET) of the Catholic University of Santiago de Guayaquil (UCSG).

To achieve the target diagnosis is performed to determine the security flaws present in the Electronics Laboratory, that will determine their vulnerabilities and thus recommend securities that should be implemented to prevent them.

ÍNDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLA

INTRODUCCIÓN

La información es considerada fundamental para las organizaciones y empresas, por esta razón es necesario establecer procesos de seguridad de la red por la que circulan esos datos. Estos procesos deben considerarse como lo más importante puesto que la información trascendental para su desarrollo, e implica adoptar las medidas necesarias para garantizar la seguridad de la información. El diseño de la seguridad de una red de información debe considerar las características indicadas con costos razonables de acuerdo a la seguridad que deba implementarse.

Al no establecerse un control del flujo de información, las redes se vuelven sensibles a la pérdida de datos que podrían ser fundamentales para la operación de la organización y que incluso se da la posibilidad de que esa información sea mal empleada. Hay que tomar en cuenta que no solo elementos externos a la institución pueden atacar la red sino también por personal interno, en el caso de esta investigación el ataque podrían realizarlo estudiantes con acceso a la red.

Como una solución para limitar esos errores en la seguridad de la red, en este caso la del Laboratorio de Electrónica, se realizará un análisis del equipamiento de dicha dependencia para elaborar un diagnóstico que permita determinar las debilidades presentes en ella, y con este resultado se podrás aconsejar las medidas de prevención que deberían establecerse en base a las normas correspondientes.

También es importante considerar que el desarrollo de los procedimientos informáticos siempre está en un continuo cambio por lo que las seguridades del sistema en estudio deben estar a cargo de una persona que reciba actualización en este campo de manera constante para evitar nuevas fallas.

ANTECEDENTES

Como ya se indicó, la Información es un bien invalorable de una institución y por lo tanto requiere de una planificación para su protección, se establece así la seguridad informática, que se encargará de proteger esa información de los ataques que puedan producirse contra ella para garantizar la operación del laboratorio y limitar los daños que puedan producirse.

La seguridad informática es la propiedad de un sistema que demuestra que el mismo no corre peligro y que está protegido contra ataques. Bajo este concepto, para sistemas operativos, *software* o redes de computadoras, es dificultoso conseguirla y según los especialistas en el tema, es imposible garantizar la infalibilidad del sistema, por esa razón se prefiere utilizar el término fiabilidad en temas de seguridad informática, es decir la posibilidad y no la seguridad de que un sistema actúe como se espera, así, ya no se dice que los sistemas son seguros sino solamente fiables.

Para que una institución pueda tener el grado de seguridad necesario debe aplicar un sistema que incluya al administrador de la red a protegerse y un conocimiento de los ataques que pueden presentarse, esta responsabilidad también corresponde a los funcionarios de la FET y en general a todo el personal de la misma.

Estándares de seguridad en redes

Para preservar la información en su propagación por las diferentes redes se aplican los estándares de seguridad BS77994 (evitar errores) y ISO/17799 (seguridad) los cuales implican los controles para garantizar la seguridad informática del sistema. En este contexto, se considera el equipamiento, políticas de la empresa, el personal y la parte legal.

Estándar BS7799

La norma BS 7799 de la *British Standard Institution* (BSI) nace en 1995 (parte 1), para brindar a las empresas medidas prácticas de gestión de seguridad de la información. En 1998 surge la parte 2 con normas mejoradas para administrar la seguridad con miras a la certificación de auditoria. (Cuevas)

En el año 2000 pasa a ser un estándar internacional como ISO/17799 y aceptado por el comité técnico como ISO/IEC JTC 1. (Mujica, 2005)

Estándar ISO/17799

Este estándar incluye controles y recomendaciones para que la empresa o institución mantenga segura su información y entre sus características se puede mencionar que es internacional, comprobado, de calidad, flexible, progresivo, con herramientas disponibles y soporte técnico.

ISO es la Organización Internacional de Estandarización, que promueve el desarrollo de normas internacionales de fabricación para comunicaciones y con la IEC que es la Comisión Internacional Electrotécnica, encargada de la normalización eléctrica y electrónica, forman un sistema especializado para la estandarización mundial. Otros organismos internacionales están en alianza con ellas y colaboran en el desarrollo de estándares internacionales, cuyos anteproyectos se elaboran de acuerdo a los reglamentos establecidos por ISO/IEC. Para aspectos tecnológicos relacionados con la información, ISO e IEC instituyen un comité técnico que revisa los anteproyectos y después se distribuyen a los organismos nacionales que votan para su aprobación. (Mujica, 2005)

De esta manera se han propuesto aspectos claves para ISO/17799 tales como las políticas de seguridad incluyendo la organizacional y física, la clasificación de bienes, el personal de seguridad, el control de acceso, la administración continúa de

operaciones y comunicaciones, el sistema de desarrollo y mantenimiento y el acatamiento a las normas y procedimientos.

DEFINICIÓN DEL PROBLEMA

La necesidad de realizar un estudio para determinar la protección adecuada contra las debilidades de la infraestructura de red del Laboratorio de Electrónica de la Facultad de Educación Técnica de la Universidad Católica de Santiago de Guayaquil.

OBJETIVO GENERAL

Realizar un estudio que para determinar la protección necesaria contra las debilidades de la infraestructura de red del Laboratorio de Electrónica de la Facultad de Educación Técnica de la Universidad Católica de Santiago de Guayaquil

OBJETIVOS ESPECIFICOS

1. Efectuar un estudio de los métodos que se utilizan para realizar ataques a la infraestructura de una red.
2. Utilizar la información obtenida en el análisis de debilidades de la red, así como los elementos de prevención y protección de errores de seguridad de la red, para corregirlos.
3. Analizar las herramientas que brinda *Backtrack* para las pruebas de la red y la forma en que se debería aplicar en la red del laboratorio de Electrónica de la FET.

JUSTIFICACIÓN

Este trabajo de investigación pretende aportar a fortalecer el sistema encargado del flujo de información que como ya se indicó, reviste singular importancia en una institución y para alcanzar este objetivo se aplicarán técnicas de seguridad para

aplicarse en redes LAN (*Local Area Network*, Redes de Área Local), aplicando *software* libre, mostrando las debilidades de la red que se quiere proteger, efectuando pruebas en un medio controlado para poder determinar claramente las fallas de seguridad para proceder a su análisis y diseñar el método de seguridad más adecuado. En este punto es importante considerar que la seguridad no es simplemente un *software* antivirus o un *firewall*, sino de la aplicación de estándares y normas correspondientes y que todos los que utilizan la red deben aplicar. En el caso de este trabajo de investigación se aplicará el estándar internacional ISO/IEC 17799.

El análisis de las debilidades de la red del laboratorio de Electrónica de la FET se realizará con los procedimientos adecuados, en este caso se utilizará *Backtrack* por los beneficios que ofrece, el cual es un conjunto de pruebas de penetración basada en *Linux* que ayuda a la seguridad para evaluar entornos donde hay penetración de la "piratería" informática. Actualmente se considera a *Backtrack-Linux.org*, la sede más alta calificada de distribución de seguridad de Linux.

Backtrack ha sido diseñada para el desarrollo de auditorías de seguridad informática y es una distribución GNU/Linux dirigida al área indicada e incluye gran cantidad de elementos para ejecutar pruebas de penetración, se presenta como *LiveCD* por lo que no es necesario instalarla y permite usar todas sus aplicaciones en pocos minutos.

HIPÓTESIS

La determinación de las debilidades de seguridad en el laboratorio de la FET, permitirá establecer un método de prevención y mejorar la seguridad de la red.

CAPITULO 1: FUNDAMENTACIÓN TEÓRICA

Para Carlos Jerez (2004) la seguridad de la información es la defensa de ésta de accesos no autorizados para su alteración o destrucción accidental o intencional, o el impedimento de procesar la información. (Jerez, 2004)

Para alcanzar este objetivo se aplican operaciones, estrategias e instrumentos para mantener la seguridad de la información de la organización. Un pirata informático (*hacker*) pretende aprovechar las debilidades de un sistema para violentar su seguridad. Estos ataques a la seguridad informática se enfocan en la confidencialidad, autenticidad, integridad y disponibilidad, cada uno de los cuales se trata a continuación:

La **confidencialidad** garantiza que la información solo esté disponible para usuarios autorizados. Es entonces la defensa de datos para evitar su transmisión no autorizada, la falta de confidencialidad representa inconvenientes legales y la pérdida del negocio o de credibilidad. La sustracción de información, contraseñas o datos durante su propagación sin encriptación por una red constituye un ataque de confidencialidad, puesto que admite a alguien diferente del receptor accesar a los datos.

La **autenticación** significa comprobar la identificación de los usuarios y el permiso de la administración durante una transmisión. Los encargados de la seguridad en redes deben mantener seguros los datos de una entidad y proteger la información. Por ejemplo, la alteración de una dirección MAC (*Media Access Control*) atenta a la autenticación al permitir que un terminal no autorizado se conecte a la red.

La **integridad** certifica que los datos no sean cambiados sin autorización, para eso se debe garantizar que la información no sufra alteraciones no autorizadas, esto podría causar fraudes, decisiones erróneas o acceso a otros ataques. Un ejemplo de este tipo de ataques son los llamados *bit-flipping* en los que los datos podrían manipularse

durante su propagación en un sistema informático y sus administradores no pueden verificar los datos del remitente.

La **disponibilidad** implica que la información está disponible para ser solicitada por alguien cuando lo requiera. De la misma manera en lo referente a la continuidad operativa de la organización, perder la disponibilidad significa la pérdida de productividad o credibilidad. Un ataque de Denegación de Servicio (DoS), significa que un hacker agrede a la disponibilidad del sistema.

Un aspecto adicional que se puede mencionar es el **no repudio,** que da protección contra la paralización de alguna de las partes enlazadas en la comunicación. Esta seguridad se estandarizó en la ISO-7498-2.

En el caso de No Repudio de origen, el usuario que envió el mensaje no puede negarlo pues el que lo recibe tiene una prueba del envío, la cual es creada por el mismo emisor y la recibe el receptor.

Si se trata de No Repudio de destino, los papeles se invierten y es ahora quien recibe el mensaje que no puede negarlo porque el que lo envió tiene pruebas de la recepción, así el emisor prueba que el destinatario un envío, realmente lo recibió y evita su negación. La prueba es creada por el receptor y la recibe el emisor.

En resumen, la **autenticidad** demuestra quién es el autor de un informe y a quien se envió, el **no repudio de origen** certifica que el emisor envió la información y el **no repudio de destino** que el receptor la recibió. De esta manera el que envía o quien recibe no pueden negar la comunicación de un informe, cada uno puede certificar la existencia del mismo.

1.1 Ataques a un sistema e inseguridades del mismo

Este análisis debe iniciarse con la determinación de los actores que componen el entorno lo cual servirá para continuar el proceso de implementación de la seguridad

informática en la entidad. La figura 1.1 presenta el entorno de seguridad de una organización.

En la figura 1.2 se muestra un esquema de seguridad informática donde se pueden apreciar el camino a seguir para determinar las metas del sistema de protección, que se inicia con la determinación de los perfiles de seguridad y de los cuales se obtiene la estructura del sistema y sus requerimientos.

Figura 1.1 Entorno de seguridad de una organización

Fuente: (UNAM)

Figura 1.2 Establecimiento de las metas del sistema de seguridad

Fuente: (UNAM)

Conocidos los objetivos del sistema se procede a diseñar la estructura de seguridad que se va a implementar, la figura 1.3 muestra los procesos asociados a esta etapa:

Figura 1.3 Procesos de la implementación del sistema de seguridad

Fuente: (UNAM)

Muchas veces una red sufre ataques mediante diversas técnicas para quebrantar la seguridad del sistema. Entre los más frecuentes se puede mencionar los siguientes:

1.1.1 Negación de acceso

Es una forma ataque para impedir el acceso del usuario a un recurso específico o de su propiedad. A modo de ejemplo se puede mencionar:

- Inundar (*floodear*) una red, para impedir la propagación de datos en ella.
- Interrupción de los enlaces entre dos equipos para impedir el acceso a un servicio.
- Impedir que un usuario acceda a un servicio.
- Impedir el acceso a un servicio específico a un usuario.

También se debe considerar que la negación de un servicio puede darse por el uso ilegítimo de recursos. Por ejemplo, un *hacker* puede ocupar una zona del FTP (*File Transfer Protocol*) anónimo para guardar archivos, ocupando espacio en el disco y produciendo tráfico en la red. Algunos ataques de este tipo pueden hacerse con

recursos pequeños contra un sistema grande y tecnificado, en un llamado ataque asimétrico. En conclusión, estos ataques podrían inhabilitar una computadora o una red, quedando la organización desconectada de Internet cierto tiempo.

Bajo estas características pueden identificarse las siguientes clases de estos ataques:

- Utilización de recursos pequeños, restringidos, o no renovables
- Eliminación o modificación de datos de configuración
- Eliminación o modificación de los elementos de la red

En el primer caso se sabe que los sistemas trabajan con recursos como el ancho de banda, capacidad de memoria, bases de datos, conexión con otras computadoras y redes, etc. Estos ataques comúnmente se realizan dirigidos a la conectividad de la red. El hacker pretende impedir la comunicación de las computadoras a la red. Un modelo de estos ataques es el *SYN flood*, en el cual el hacker realiza una conexión TCP (*Transmission Control Protocol*) a la computadora atacada, pero evitando que el enlace se complete, durante ese periodo ese terminal reserva de una cantidad limitada de las estructuras de datos requeridas una para completar el vínculo, de esta manera los enlaces reales son rechazados y la computadora atacada espera tratando de completar los vínculos falsos.

Nótese que estos ataques no dependen del ancho de banda del *hacker*, pues él utiliza las bases de datos del *kernel*, involucradas en realizar la conexión TCP. Es decir que un atacante con una conexión *dial-up* puede atacar una gran estación de trabajo en un ataque asimétrico.

En otra forma un atacante puede usar recursos del atacado contra el mismo, un ejemplo, es el caso de negación de servicio UDP (*User Datagram Protocol)*, en el cual utilizan paquetes falsificados de UDP para enlazar el servicio de producción de eco en un terminal con el servicio de *chargen* en otra computadora. De esta manera ambos servicios agotan el ancho de banda y la conectividad de los terminales de la red se ve afectada.

Bajo el mismo esquema, el atacante puede agotar el ancho de banda produciendo muchos paquetes enviados a la misma red, por lo general tales paquetes son del tipo de generación de eco de ICMP (*Internet Control Message Protocol*). Por otro lado, en este ataque no se requiere trabajar desde una sola computadora pues puede hacerse coordinando varios terminales de varias redes y llegar al mismo resultado.

También pueden agotar otros recursos de la red atacada que ésta requiera para operar. Así por ejemplo, sistemas con una cantidad limitada de bases de datos en el *kernel* puede guardar información de procesos tales como identificadores, ingresos en tablas de procesos, etc. El atacante puede hacer esto con un programa o un script que no hace nada pero que construye varias copias de sí mismo. Los sistemas operativos modernos, aunque no todos, están equipados con defensas contra esta dificultad. También hay que indicar que se consume CPU (*Central Processing Unit*) aunque las tablas de procesos no se colmen, por el número de procesos ejecutándose. Un hacker puede también acabar el espacio en disco de la computadora atacada de las siguientes maneras:

- Crear gran cantidad de mensajes electrónicos, por ejemplo *spam*, *bombing*, etc.
- Producir a propósito errores que tienen que ser "*logueados*", esto también incluye el uso ilegítimo del *syslog* en *unix*. Esto significa que se usa el proceso *syslog* del atacado para registrar eventos de otra computadora y así colmando el disco con el archivo de *syslog*.
- Poner archivos en el disco del atacado usando un FTP anónimo.

Es decir que puede emplearse cualquier medio para escribir datos en el disco del equipo atacado para realizar un ataque del tipo de negación de servicio en caso de que no se hayan establecido límites en el número de datos que se pueden ingresar. Sin embargo, hay sistemas de cierre de cuenta (*lockout*) al superar cierta cantidad de *logins* errados. Un atacante podría aplicar este método para impedir que los usuarios genuinos ingresen. Incluso cuentas protegidas como las de administrador pueden ser atacadas de esta manera. Además, un atacante podría provocar la caída del sistema o

volverlo inestable por medio del envío de datos imprevistos. La caída frecuente del sistema podría ser a causa de estos ataques. Otros elementos del sistema que pueden ser afectados por la negación de servicio y que por lo tanto deben supervisarse son las impresoras, las conexiones de red, entre otros.

1.1.2 Abertura de contraseñas (*password cracking)*

Este método de ataque se fundamenta en descubrir las contraseñas utilizadas por el usuario en las aplicaciones. Por esto se pretende encriptar los códigos de cifrado en todos los procesos informáticos. Estos métodos de cifrado actuales dificultan el descifrado de claves. Por ejemplo, con MD5 (*Message-Digest Algorithm 5*), es prácticamente imposible hallar una relación lógica entre el mensaje cifrado y el descifrado, debido a que cada clave se genera en base a una serie distinta a la que se denomina "semilla". Este es un ejemplo del desarrollo de los sistemas para descifrar claves, en los que no se pretende hallar una relación lógica, sino el cifrado de otras series que sean similares al mensaje cifrado, nótese que es un trabajo difícil que necesita buen equipamiento para descifrarlas.

1.1.3 Bombardeo de mensajes electrónicos y spams (*e-mail bombing & spamming)*

El *e-mail bombing* es el envío en repetidas ocasiones del mismo mensaje a una dirección, llenando el *mailbox* del destinatario. De manera similar el *spamming*, consiste en mandar el mensaje a gran cantidad de usuarios, por lo cual resulta El *Spamming* puede ser aún más nocivo si los destinatarios responden el mensaje, provocando que todos los usuarios reciban la respuesta.

También puede ocurrir accidentalmente al mandar un mensaje a la lista sin notar que es distribuido a muchos destinatarios, otro caso se puede presentar por la errónea configuración de un sistema de autorespuesta.

Los tipos de ataques indicados además pueden combinarse con el *e-mail spoofing* que cambia la identidad del emisor del mensaje para que sea más difícil saber quién envía en realidad el *mail*.

En conclusión, los servicios de mensajería provocan vulnerabilidad en los usuarios por los ataques de *e-mail bombing* y *spamming*, los cuales son difíciles de prevenir ya que simplemente un emisor con una dirección válida de correo puede enviar *Spam* a cualquier destinatario de *mail*.

En el caso en que un gran número de mensajes se envían a una sola dirección, puede producirse DoS debido a la pérdida de conectividad, caída del sistema o fallas en el servicio por sobrecarga de enlaces de red, uso de todos los recursos disponibles del sistema o al llenarse el disco por *postings* múltiples y de ingresos en el *syslog*.

1.2 Normas de seguridad informática

Estas reglas establecen la utilización correcta del equipamiento de la entidad, por lo tanto debe plantear objetivos precisos para cada terminal empleado para defender la red inclusive las medidas de seguridad. Son instrumentos que puntualizan los controles de seguridad que se tienen que emplear en la institución, los cuales no son prácticos sino se ejecutan, por eso los beneficiarios de la red suscriben un documento que detalla lo que pueden realizar en el sistema.

Además, esa política tiene que presentar un compendio y los objetivos. En la figura 1.4 se muestra el esquema de los procesos a seguir para implementar un sistema de seguridad informática, nótese que se inicia con el establecimiento de las políticas de seguridad.

Figura 1.4 Determinación de los objetivos de seguridad

Fuente: (UNAM)

La política para seguridad en ejecución debe tener como propósito resguardar al personal de la entidad y a ésta misma contra operaciones ilícitas que hagan daño y que son realizadas por atacantes internos o externos. Su publicación no se realiza para aplicar condiciones opuestas a la implantación de una instrucción de poder ser disponible, brindar confianza y rectitud, la seguridad representa la voluntad de todos los involucrados y ofrecen apoyo al personal que trabaja con datos confidenciales. Los usuarios tienen el compromiso de conocer las instrucciones y realizar su trabajo según lo instituido. Por eso las normas tienen que establecer la defensa del personal y de la empresa si una gestión amenaza la seguridad. Por esta razón se entrega al personal el detalle de las acciones que no se deben realizar antes de suscribir el documento de conformidad con la política, el cual también tiene que incluir los casos de excepción de las prohibiciones según la jerarquía del funcionario.

Las normas de seguridad tienen que establecer un esquema que establezca como los usuarios internos y externos deben operar con los equipos de la institución, además debe definir la implementación de la arquitectura de red y la ubicación del equipamiento. El reglamento ha de considerar las amenazas contra el rendimiento y las propiedades materiales e inmateriales de la entidad que requieren diferentes tipos de seguridad.

La protección brindada depende del acceso de las redes, si hay más acceso o trayectoria de la red se necesita más seguridad. Así, una gran empresa necesita un grado medio de protección que debe cubrir los requerimientos de control para el ingreso de los usuarios a los equipos verificándolo y ser factible de ser analizada.

Determinar el resultado de la reglamentación en el personal, identificar los problemas de seguridad, prescindir de mucha complejidad, utilizar los instrumentos más frecuentes de protección ya usados y verificados, resolver si se debe perseguir a los atacantes e instruir al personal para obtener los datos requeridos, establecer el alcance, comunicar continuamente datos de seguridad, son algunas de las acciones que tiene que considerar un reglamento de seguridad.

Las normas pueden ser simples y específicas o generales, por ejemplo reglas de mensajería electrónica, claves, asignación de cuentas de usuario, etc. En general deben evaluarse las amenazas de la entidad para determinar las debilidades y la eventualidad de que se produzcan se examina y se determina el peligro potencial. También deben considerarse los aspectos legales que se necesitan para las diferentes negociaciones de la empresa. No se pude dejar de considerar los manuales, objetivos y parámetros del manipuleo de información que realiza la institución en sus actividades.

Los peligros de seguridad deben evaluarse sistemáticamente, analizando los errores de la operación según las consecuencias de las fallas de seguridad. Estas medidas de análisis de peligros pueden realizarse en toda la entidad o únicamente en determinadas áreas, igual para los procesos informáticos específicos, un elemento particular del proceso o una prestación útil y beneficiosa.

La reglamentación de seguridad en redes define los parámetros de acceso a la red y los métodos para practicar las normas establecidas y establece el diseño del entorno de seguridad de los datos de la entidad. Este reglamento puede ser extenso y complicado, elaborado para administrar acciones como accesos, navegar en internet, claves, codificación y anexos de mensajería.

Este reglamento de protección de la red define los recursos que hay que proteger y explica cómo se debe hacerlo, con esta información se establecerá los elementos de seguridad y las acciones de moderación a aplicarse en la red.

1.2.1 Componentes del sistema

Anteriormente se indicó que una Política de Seguridad Informática debe normar las medidas de seguridad, por eso es necesaria la voluntad del personal de alcanzar los objetivos de la organización. Para lograr esto se debe considerar la importancia de las normas, disposiciones, procesos y el recurso humano al que se va a destinar, así la entidad solicita a su personal que considere a la información como uno de sus importantes valores para el impulso de los negocios. También las metas de la normativa y el establecimiento claro de los factores envueltos en su enunciación, esto incluye los compromisos de toda la entidad ante los servicios y recursos informáticos.

Además se debe considerar las obligaciones necesarias para la distribución de la seguridad de los procesos según la política establecida. Esto implica establecer los tipos de infracciones y sus derivaciones por la no observancia de las normas, es decir la responsabilidad de los actores con la información a la pueden acceder de acuerdo a su jerarquía.

Sin embargo los directivos deben explicar claramente al personal las causas que motivan la implantación de una política de seguridad, su importancia, los objetivos y resultados, incluyendo las jerarquías y el tipo de correctivos y sanciones aplicables.

La política de seguridad establecida en una organización debe ser continuamente actualizada de acuerdo a los cambios que ocurran en la entidad como el incremento de personal, modificación del sistema de computación, implementación de nuevos servicios, entre otros.

1.2.2 Indicadores del sistema

La política establecida define las normas y reglas, para lo cual se debe analizar las amenazas contra la información de la entidad, en esta fase intervienen quienes operan los recursos y servicios, quienes por su experiencia ayudarán a definir el alcance y los tipos de infracciones. Estos resultados deben informarse al recurso humano implicado en el desarrollo de las políticas, incluyendo los beneficios y riesgos correspondientes a los recursos y sus componentes de seguridad.

Es necesario verificar continuamente la aplicación de las normas y reglas en los procesos de la entidad para determinar la necesidad de cambios o actualizaciones.

1.2.3 Peligros que pueden presentarse

Anteriormente se indicó que las claves permiten determinar la autenticación, a esto puede añadirse otras medidas como por ejemplo particularidades biométricas del usuario, por ejemplo firma con reconocimiento automático, examen del fondo de ojo, huella dactilar, etc.

En el aspecto propiamente informático puede ocurrir que los procesos y la tecnología que se está utilizando no sean suficientes para los requerimientos de la institución.

Retornando al tema de la protección, pueden presentarse múltiples peligros, por eso se debe identificarlos y tomar decisiones sobre este aspecto. La implementación tiene un valor que depende de los peligros a que un sistema está expuesto, entonces debería saberse el límite de esos peligros para una entidad específica.

Entre las causas de problemas los más comunes son los errores y negligencias, tales como acceso ilícito a datos, entrega sin autorización de información grabada, siniestros por agua o fuego, alteración sin permiso de programas o su copia ilegal, aunque estos generalmente no provocan daños importantes.

Otra forma de peligro es el pirata informático o *hacker*, quien trata de ingresar al sistema muchas veces solo para demostrar su capacidad. También podría mencionarse los virus informáticos, aunque estos su peligrosidad ha disminuido actualmente, sin dejar de considerarlos como un riesgo por la aparición de nuevas versiones que obligan a la actualización e innovación de los sistemas antivirus. Los virus pueden perturbar todo el sistema especialmente por las redes, algo dificultoso por la seguridad impuesta hoy en día.

Es evidente que lo más importante que se debe proteger en una institución en caso de siniestro es el recurso humano, sin embargo debe reconocerse que de la información depende la continuación de la organización.

1.3 Introducción al hacking ético

Este método es realizado por un profesional informático que usa los mismos mecanismos y técnicas que los piratas informáticos para hallar las vulnerabilidades del sistema para protección y seguridad y se los llama *Hackers* Éticos**,** que por lo general tienen como negocio la seguridad de los datos, para lo cual realizan pruebas de penetración o de *pentest* para determinar peligros y fragilidades de los equipos y redes. De esta manera establece defensas para las amenazas identificadas y atenuar los peligros al adelantarse a las pretensiones del atacante.

Estos profesionales siempre cuentan con autorización de los responsables de la información antes de ingresar al sistema.

A continuación se conceptualizarán algunos fundamentos de la seguridad informática.

1.3.1 Vulnerabilidad de sistemas y redes

Esta característica indica la fragilidad del sistema o red y demuestra la presencia de una falla de programación, esquema lógico o una equivocación de concentración que puede causar un suceso imprevisto e indeseado.

Amenazas contra los sistemas y redes

Es la inminencia de una circunstancia que podría resultar en una posible transgresión de la seguridad, puede ser elemento exterior que trata de aprovechar una vulnerabilidad.

Agresión contra los sistemas y redes

Este hecho sucede si el sistema o red se ve afectado por una fragilidad existente, vulnerabilidad, muchas veces se efectúan mediante un *exploit* del cual se hablará más adelante.

Virus informáticos

Se denomina así a los programas informáticos que piratean automáticamente un sistema o red sin autorización para perturbar su operación corriente. Habitualmente al ingresar al sistema reemplazan ficheros ejecutables por aquellos contaminados que podrían arruinar la información guardada en un equipo.

Engaños informáticos (*spoofs*)

Estos se presentan continuamente en las redes, es una circunstancia en que un programa o atacante sustituyen al original, así consiguen falsear datos y accesar ilegítimamente a la red y sistema.

Escaneo de puertos de un equipo (*port scanning*)

Este acto permite identificar las particularidades de un sistema o red, determinando sus dispositivos activos, servicios y los procesos que tienen y su distribución.

Exploits

Representan un camino establecido para resquebrajar la seguridad de un sistema utilizando alguna fragilidad del mismo. Conceptualmente es un fragmento de un programa, instrumento o práctica que aprovecha una debilidad del sistema para conseguir libertades en un sistema, haciéndole inutilizar su rectitud o denegar servicios en el sistema atacado. Son peligrosos porque cualquier programa presenta debilidades que son conocidas por los atacantes, quienes las investigan para aprovecharlas.

Piratería informática

Anteriormente se trató acerca de los *hackers* éticos, quienes actúan legal y profesionalmente. En general los *hackers* pueden clasificarse en "sombreros" blancos (*White Hats*), negros (*Black Hats*) y grises (Gray Hats).

Sombreros blancos (*White Hats*)

Estos son los *hackers* éticos, profesionales de la seguridad que saben técnicas de piratería y sus instrumentos y utilizan esto para identificar las vulnerabilidades y establecer las defensas. Cuentan con autorización de los responsables de la información, esta es el contraste entre un *hacker* ético y uno ladino que no es de fiar.

Sombreros negros (*Black Hats*)

Estos son *hackers* ladinos o *crackers* que aprovechan sus destrezas ilegalmente o simplemente para causar daños. Invaden la seguridad del sistema con propósitos

dañinos. Ingresan sin permiso y arruinan información, impiden a los usuarios legales el servicio y causan dificultades en la entidad atacada. El público en general conceptualiza a todos los *hackers* de esta manera.

Sombreros grises (*Gray Hats*)

Son los que pueden operar atacando o defendiendo según las circunstancias, son inteligentes y al proceder ilegalmente lo hacen de buena voluntad. Pueden considerarse como híbridos entre los de sombrero blanco y negro. Por lo general no agreden por provecho propio o con malos propósitos, sin embargo están listos para realizar infracciones en sus aventuras tecnológicas para obtener más protección.

1.3.2 Pruebas de penetración *(Pentest)*

Se denomina así al método aplicado para analizar la seguridad en una auditoría, es decir que son las normas, destrezas, operaciones y maneras de ejecución aplicados en una auditoría de un sistema de seguridad informático. Así, este *test*, constituye un procedimiento práctico y probado de trabajo ejecutado con esmero para valorar el proceso de seguridad adecuadamente.

Se pueden hacer independientemente o como un segmento de un proceso para gestionar las técnicas informáticas que se pueden añadir en un ciclo de vida. En la prueba independiente se comunica y demuestra las fallas de seguridad, en cambio el técnico informático que integra un grupo consultor de seguridad, efectúa la prueba para un proceso mayor en la disposición de protección para determinar las fallas de seguridad, con estos resultados conjuntamente se define los métodos para optimizar la seguridad.

Debe notarse que la protección de un equipo no depende únicamente de los elementos del entorno informático sino también de factores determinados de seguridad para alcanzar las mejores prácticas. Esto significa emplear los requerimientos de protección apropiados, la evaluación de peligros, simulación de

amenazas, exámenes de código, la protección operativa. En definitiva esta prueba es el análisis metódico de protección ejecutado por técnicos expertos sin importar si ya conocían o no el sistema analizado. Puede emplearse para analizar los elementos de las instalaciones informáticas, incluyendo sus aplicaciones, elementos de red, sistemas operativos, formas de comunicación, protección material y el factor humano. Los resultados de las pruebas incluyen un informe de las vulnerabilidades determinadas en el sistema y las defensas recomendadas

CAPITULO 2 ANÁLISIS DE LA SEGURIDAD

Para realizar esta evaluación de la protección del sistema se utilizará una técnica empleada por los *hackers* éticos, la cual se expondrá ahora.

2.1 Método de la huella o pisada *(Footprinting)*

Es un método para compilar datos acerca de los sistemas informáticos y las organizaciones a las que corresponden aplicando técnicas de seguridad. Es conocido que la información puede encontrarse en Internet, el método de la huella emplea un navegador como Google para conseguir información, así el *hacker* establece la mejor forma de ingresar a sus objetivos. Previo a la ejecución de una agresión o el empleo de un *exploit*, el atacante prueba el sistema operativo, su versión y las aplicaciones necesarias para un ataque eficaz.

En la información obtenida en el ataque está el nombre de dominio, los dispositivos, servicios y aplicaciones de red, la construcción del sistema, los métodos de detección de intrusos, los métodos de autenticación, las direcciones IP definidas, la entrada a los equipos de control, las direcciones de contacto y números de teléfono.

De esta manera el *hacker* logra la mayor cantidad de información básica que puede acerca de la seguridad del sistema atacado. Con estos datos descarta herramientas que no son prácticas contra el sistema atacado, acelerando de esta manera el ataque y disminuye la posibilidad de ser detectado y ahorrando tiempo al emplear instrumentos apropiados.

BackTrack es un programa de GNU/Linux en *LiveCD* para auditoría de seguridad informática, utiliza herramientas del método huella como *Metagoofil* que trabaja con *Google*, consigue la información de los archivos disponibles en el dominio visitado. La información consiste en los metadatos que se incluyen en los ficheros por el *software* de creación de ellos con datos como autor, autores anteriores, empresa, modificaciones, fecha de creación, etc., son una fuente de información que el *hacker*

puede usar. Su forma de trabajo consiste en tomar ficheros sobre el dominio atacado con Google, los descarga y graba en el disco local, extrae los metadatos y almacena el resultado en un fichero HTML. Como ya se indicó, así se obtuvo el nombre del usuario, la ruta y la dirección MAC. En la figura 2.1 se muestra el escritorio de *BackTrack* versión 5.

Figura 2.1 Escritorio de *BackTrack*

Fuente: http://hacking-etico.com/2011/08/11/primeros-pasos-con-backtrack-5-parte-1/

En la sección *Applications*, se elige la opción deseada, la pantalla que se observa se muestra en la figura 2.2.

Figura 2.2 Pantalla de *BackTrack*

Fuente: http://hacking-etico.com/2011/08/11/primeros-pasos-con-backtrack-5-parte-1/

Ahora, para accesar a *Metagoofil* de *Backtrack* 5, se digitan los siguientes comandos y se obtiene la pantalla que se muestra en la figura 2.3:

cd /pentest/enumeration/google/metagoofil

./metagoofil.py

A continuación se recogen los documentos del dominio elegido, en este caso ucsg.edu.ec y se los almacena en /root/Step/Eval_segur/metagoofil.html. El comando para extraer los datos de cualquier *website* usando *Metagoofil* es:

 # ./metagoofil.py -d ucsg.edu.ec -l 20 -f all -o output.html -t temp

En esta instrucción ya se ha insertado el nombre de dominio del objetivo al cual se van a extraer los datos. La letra “f” significa que se quiere encontrar todo tipo de datos, “l” el resultado de la búsqueda, “o” el archivo de salida y “t” el fichero temporal que se borrará después del proceso. El archivo de salida brindará información importante como el nombre del usuario para el posterior ataque, la ruta del directorio para entender la estructura, la fecha de creación, entre otros.

La instrucción ./metagoofil.py options proporcionará la imagen mostrada en la figura 2.3

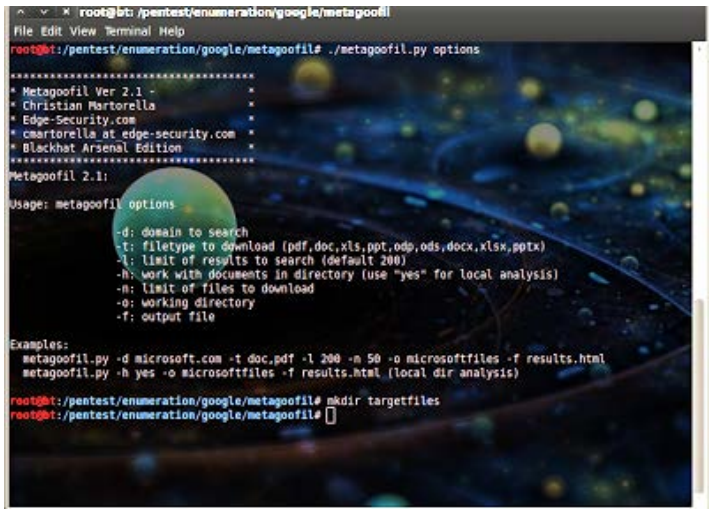


Figura 2.3 *Metagoofil* de *BackTrack*

Fuente: (GrayHathacking, 2012)

En la figura 2.4 se muestra este proceso en ejecución. En esta fase *Metagoofil* mecánicamente saca los metadatos de los ficheros que se descargaron y presenta un listado de los usuarios hallados. También se determina el programa empleado para editar los datos descargados. Las siguientes figuras 2.5 y 2.6 muestran las diferentes salidas obtenidas en teste proceso.

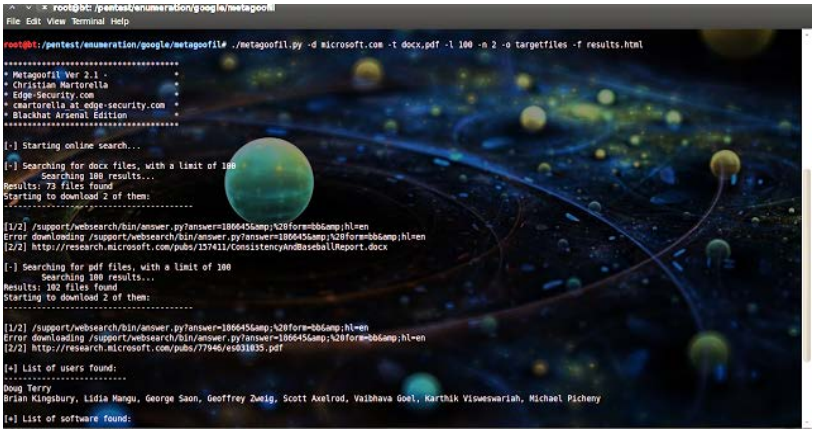


Figura 2.4 Ejecución de *Metagoofil* de *BackTrack*

Fuente: (GrayHathacking, 2012)

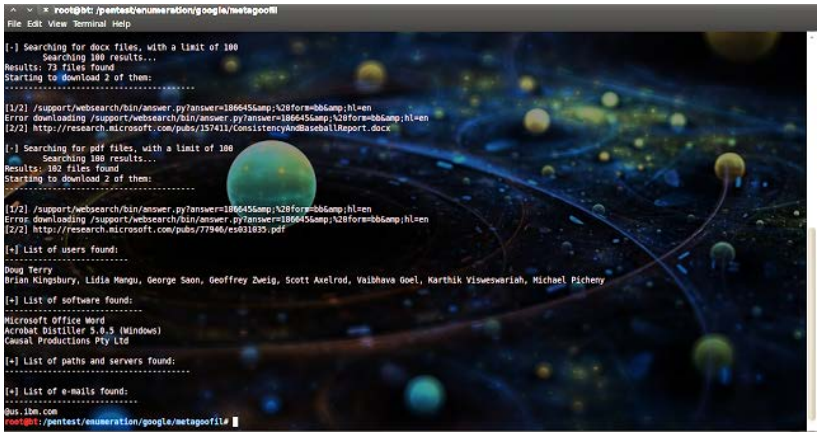


Figura 2.5 Pantalla de *Metagoofil* de *BackTrack*

Fuente: (GrayHathacking, 2012)

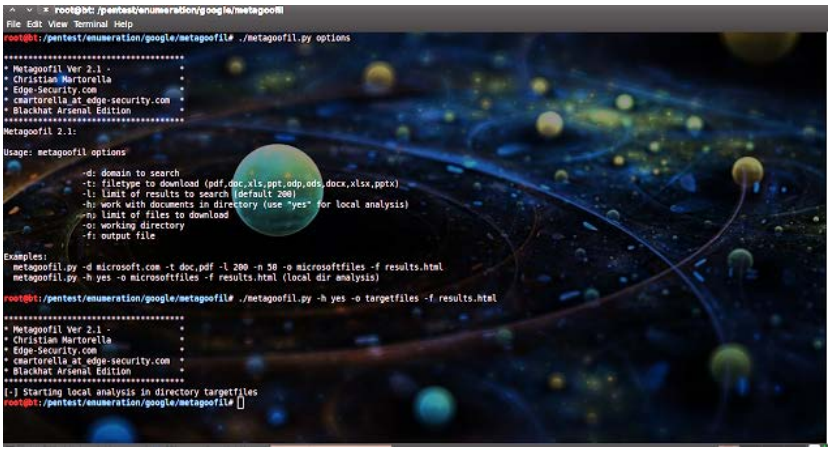


Figura 2.6 Salida de *Metagoofil* de *BackTrack*

Fuente: (GrayHathacking, 2012)

Estos mismos datos también se pude observar de manera gráfica como en la figura 2.7

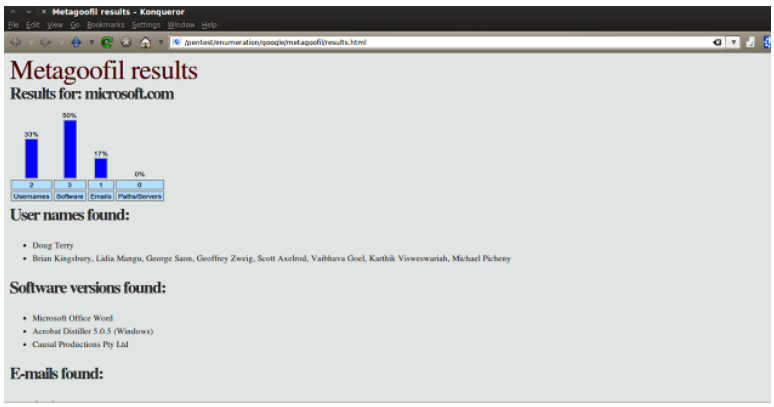


Figura 2.7 Salida gráfica de *Metagoofil*

Fuente: (GrayHathacking, 2012)

Además, *Metagoofil* puede mostrar gráficamente los resultados obtenidos porque se guardaron con la extensión .html, obteniéndose mucha información. Por ejemplo, con la denominación de los usuarios se puede elaborar diccionarios para atacar mediante claves y los datos de la ruta para predecir el sistema operativo del sistema atacado y todo se consiguió sin entrar en el dominio web del usuario atacado.

Se denomina Enumeración DNS a la ubicación de los servidores DNS (*Domain Name System*) y sus búsquedas respectivas para una entidad, la cual puede poseer los servidores DNS internos y externos con datos como denominaciones de usuarios y equipos, direcciones IP, etc. Ahora el hacker puede emplear el DNS para probar la configuración de los servidores.

NSlookup es un instrumento que hace preguntas a servidores DNS para explorar la información, es decir identificar el DNS del host remoto. *Traceroute* se usa para búsqueda paquetes y es utilizable para casi todos los sistemas operativos, enviando un ICMP a cada enrutador o entrada en todo el trayecto hasta llegar a la dirección atacada. Al enviarse los ICMP desde el enrutador el TTL (*Time To Live*) se comprime en uno en cada enrutador en el trayecto. Así el *hacker* puede saber la cantidad de saltos del enrutador al emisor. Para ingresar a *traceroute* se sigue la siguiente ruta:

BackTrack > Information Gathering > Network Analysis > Route Analysis > tcptraceroute

De acuerdo al detalle mostrado en la figura 2.8

Figura 2.8 Ingreso a *tcptraceroute*

Fuente: (HackingDNA, 2013)

Y se obtiene la pantalla mostrada en la figura 2.9.

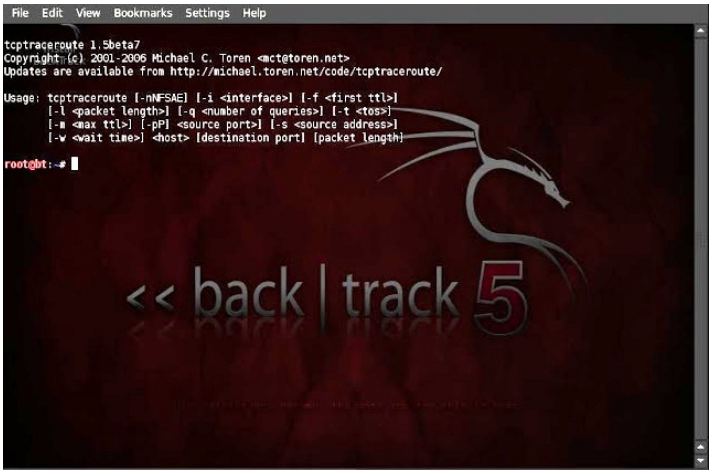


Figura 2.9 *Tcptraceroute*

Fuente: (HackingDNA, 2013)

El ajuste del TTL inicial utilizado en el primer paquete saliente se muestra en la figura 2.10

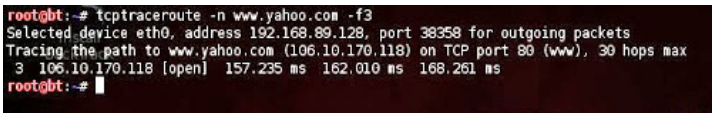


Figura 2.10 Ajuste del TTL inicial

Fuente: (HackingDNA, 2013)

Otro instrumento aprovechable es *Theharvester*, recoge cuentas de correo y denominaciones de usuarios de un dominio para emplearlos para atacar. Viene instalado en *backtrack* 5 y para abrirlo se sigue la siguiente ruta: *BackTrack > Vulnerability Assessment > Web Application Assessment > Web Open Source Assessment > theharvester*

Como se detalla en la figura 2.11. El camino corto es la ruta /pentest/enumeration/theharvester y se ingresa pudiéndose observar la siguiente pantalla (figura 2.12).

Figura 2.11 Ruta de ingreso a *Theharvester*

Fuente: (Kathayat, 2013)

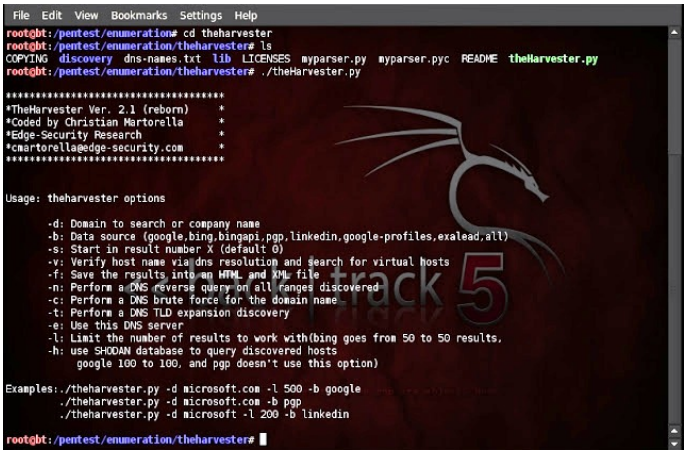


Figura 2.12 Pantalla de *Theharvester*

Fuente: (Kathayat, 2013)

Un instrumento para congregar los datos obtenidos es *Maltego*, como denominaciones de dominio y DNS, componentes de red, direcciones IP, a esta herramienta también se ingresa por *BackTrack.* La figura 2.13 muestra el logo de *Maltego* en *BackTrack* versión 5.

Figura 2.13 *Maltego*

Fuente: it.paperblog.com

Para acceder a *Maltego* en BackTrack versión 5, se sigue el siguiente trayecto:

Applications->Backtrack->Information Gathering->Network Analysis->DNSAnalysis->Maltego

La arquitectura de *maltego* se puede apreciar en la figura 2.14.

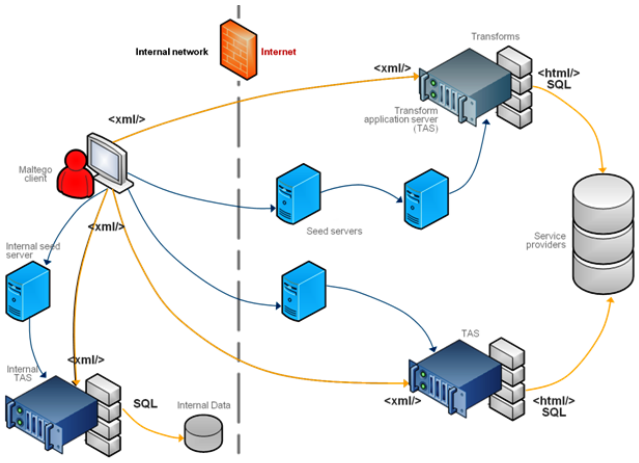


Figura 2.14 Arquitectura de *Maltego*

Fuente: (Bucker, 2012)

A continuación se abrirá la interfaz de esta aplicación pudiéndose observar las alternativas como en la figura 2.15.

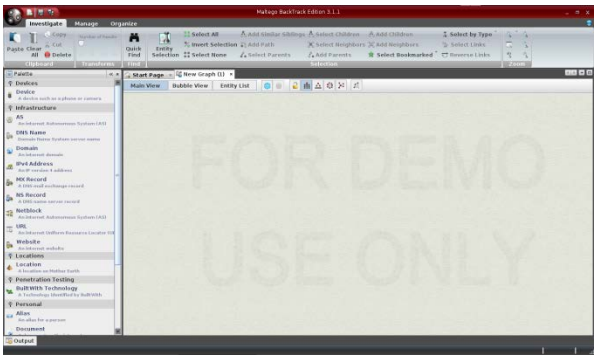


Figura 2.15 Opciones de *Maltego*

Fuente: (Bucker, 2012)

Al ingresar se encuentra la ventana de *palette* para escoger la organización a investigar, entre las opciones se tiene *Infraestructure* con comandos para localizar la entidad y *Person*, que realiza la misma función pero con personas, además *Pentesting* y *Wireless.* La pantalla correspondiente a *Infraestructure* se presenta en la figura 2.16, en ella se pueden conseguir datos de un dominio determinado, tales como DNS, IP, etc.

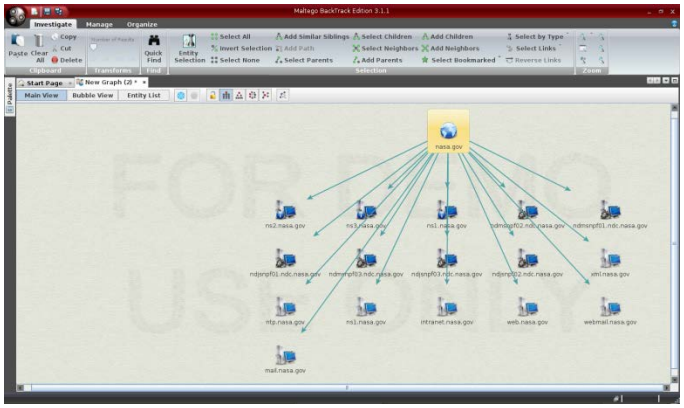


Figura 2.16 Opción *Infraestructure* de *Maltego*

Fuente: (Bucker, 2012)

Ahora se comprobará con la alternativa *Person* mostrada en la figura 2.17, esta permite conseguir datos sobre personas y sus correos electrónicos, archivos compartidos, etc., simplemente digitando el nombre de quien se va a analizar.

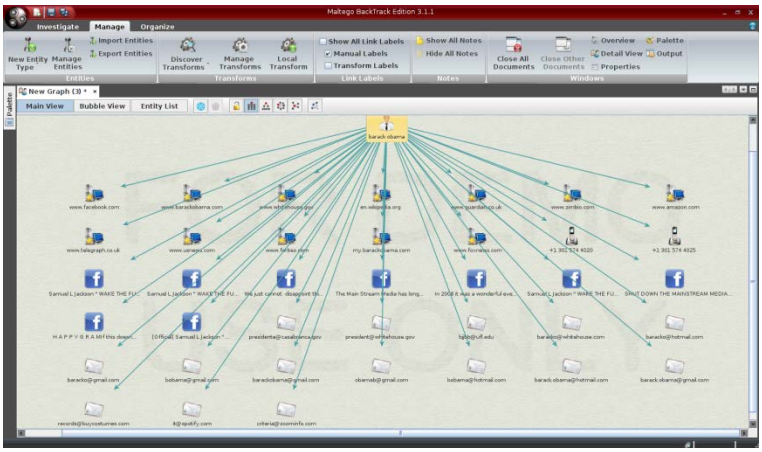


Figura 2.17 Opción *Person* de *Maltego*

Fuente: (Bucker, 2012)

Maltego además de recoger los datos identifica fragilidades y ayuda al *hacker* en su labor. En la figura 2.18 se aprecia que se ha obtenido información de teléfonos, *Facebook*, correos electrónicos, sitios web de la persona analizada.

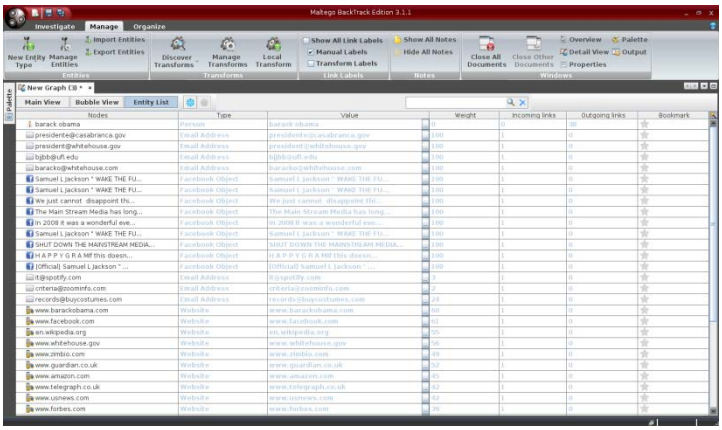


Figura 2.18 Información de la persona analizada

Fuente: (Bucker, 2012)

Ahora el *hacker* tiene una mejor información de la entidad atacada, pues estos instrumentos le brindaron datos que pueden afectarla, así como a su personal.

2.2 Proceso de Exploración (*scanning*)

Con los datos de la red obtenidos, el siguiente paso es identificar los dispositivos de la entidad para identificar el sistema operativo empleado en la computadora a atacar y determinar cuál de los equipos conectados a la red es factible de examinar, este proceso se llama exploración o escaneo y sitúa los sistemas activos conectados a la red. Así puede obtenerse las direcciones IP de los equipos, determinar si está conectado a la red y si es utilizable.

En la figura 2.19 se presentan las fases de este proceso de exploración.

Figura 2.19 Fases de la exploración

Fuente: http://img.youtube.com/vi/lJGOWX_SJws/0.jpg

En este proceso el instrumento más usado para saber si un *host* específico está activo es Ping, se manda un paquete ICMP *Echo Request* y aguarda una respuesta igual de un equipo activo, también se pueden mandar paquetes TCP/UDP si los ICMP son detenidos por un *firewall.* Ping también permite a determinar el tráfico de la red y la capacidad del equipamiento. (Malagón)

Arping es un instrumento para supervisar una red y saber si una computadora está activa, trabaja como el *Ping*, aunque éste usa paquetes ICMP que son enrutables y sus pruebas son en la capa tres de ISO y *Arping* en capa dos con pues usa el protocolo ARP (*Address Resolution Protocol*) para comprobar la actividad de las máquinas. Solo trabaja en la red LAN a la que están conectadas las máquinas, por lo

tanto si se tienen dos redes apartadas por un *router* que es un artefacto de capa tres, no sería posible que alcance a otro aparato ubicado externamente a la subred a la que corresponde, en el ejemplo mostrado en la figura 2.20 la computadora con la IP 192.168.10.10 al ejecutar un *arping* a la IP 192.168.20.10 conseguiría como producto la dirección MAC del enrutador enlazado a su subred.

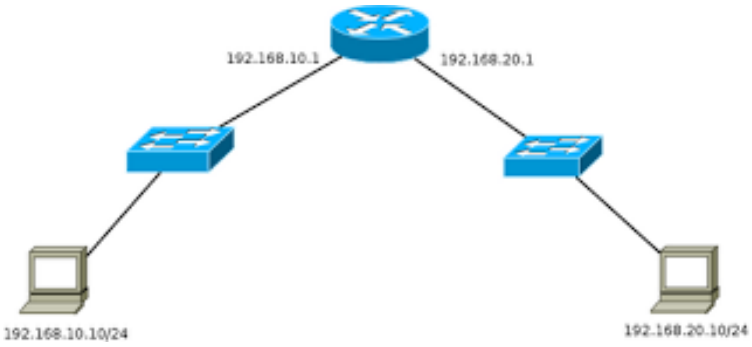


Figura 2.20 Dos subredes delimitadas por el *router*

Fuente: http://www.redesymas.org/2011/10/herramienta-de-monitoreo-de-red-arping.html

Otro instrumento usado por *BackTrack* es la plataforma para hacer herramientas de seguridad de red *Netifera*, ofrece la interfaz API (*Application Programming Interface*) para labores como enlaces asíncronos, relacionar la recepción de paquetes y la introducción de terminal directo, exploración de la red y localización en TCP y UDP, determinación del sistema operativo, etc.

Se ingresa a esta plataforma con los comandos mostrados en la figura 2.21

```
root@bt:~# cd /pentest/scanners/netifera/
```

Figura 2.21 Línea de comandos para acceder a *Netifera*

http://tutoriales-hacking.blogspot.com/2013/01/backtrack-5-r3-netifera.html

Y se observan los archivos del directorio con el comando *ls*, como se muestra en la figura 2.22.

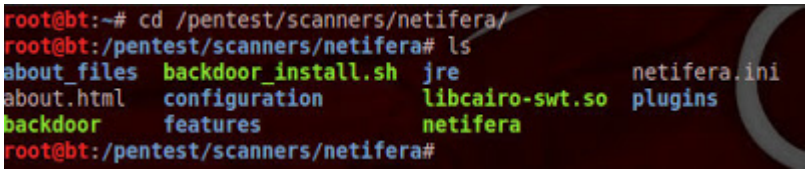


Figura 2.22 Archivos del directorio

http://tutoriales-hacking.blogspot.com/2013/01/backtrack-5-r3-netifera.html

Y se ejecuta *netifera* ./netifera (Figura 2.23)

Figura 2.23 Ingreso a *netifera* ./netifera

http://tutoriales-hacking.blogspot.com/2013/01/backtrack-5-r3-netifera.html

Abriéndose la ventana de inicio de la plataforma mostrada en la figura 2.24.

Figura 2.24 Pantalla de inicio *netifera*

http://tutoriales-hacking.blogspot.com/2013/01/backtrack-5-r3-netifera.html

Ahora se observa la interfaz gráfica GUI (*Graphical User Interface)* de *Netifera* en la figura 2.25:

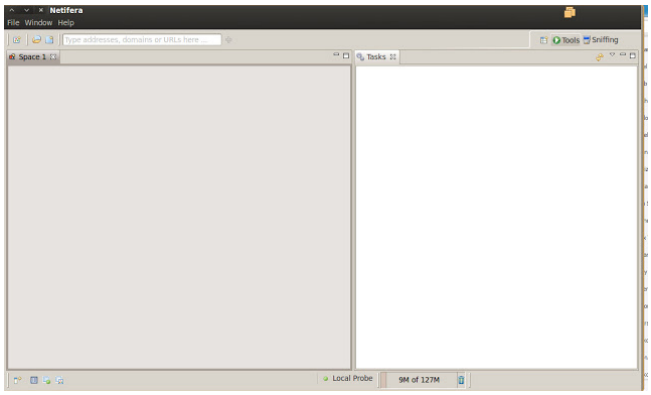


Figura 2.25 Interfaz GUI

http://tutoriales-hacking.blogspot.com/2013/01/backtrack-5-r3-netifera.html

A continuación se pone un objetivo a analizar, por ejemplo 200.29.159.11 (figura 2.26)

Figura 2.26 Objetivo

http://tutoriales-hacking.blogspot.com/2013/01/backtrack-5-r3-netifera.html

Con el ingreso del objetivo se pueden apreciar las opciones mostradas en la figura 2.27

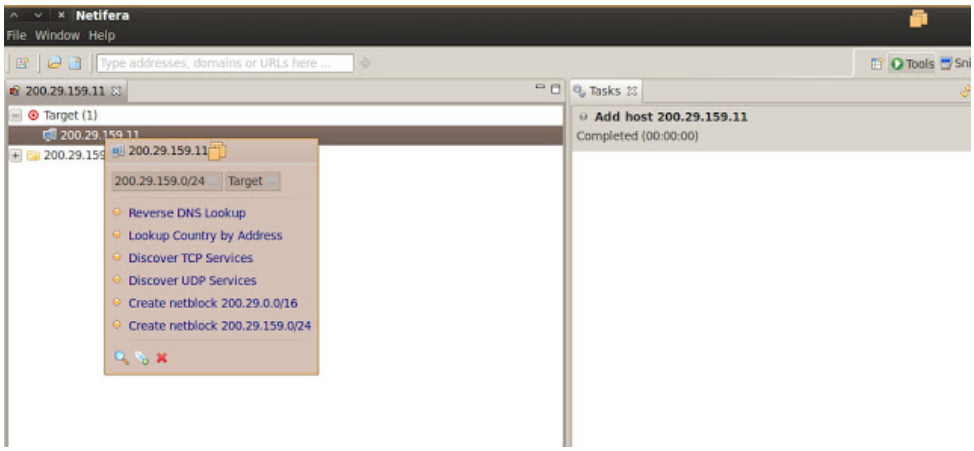


Figura 2.27 Opciones

http://tutoriales-hacking.blogspot.com/2013/01/backtrack-5-r3-netifera.html

El resultado del análisis presenta el sistema operativo de las máquinas activas, su dirección IP y los servicios operando con sus respectivos puertos.

La exploración de puertos implica la tipificación y actividad de puertos TCP/IP de un sistema, mediante estos instrumentos un atacante puede asimilar las aplicaciones o servicios activos en un sistema, estando cada uno relacionado con un puerto. Por lo general el *hacker* se dirige a los puertos más empleados.

Un instrumento que realiza con celeridad y de manera eficiente los barridos de *pings*, exploración de puertos, localización de direcciones IP, caracterización y definición del sistema operativo es *Nmap*, explorando muchos equipos en una consulta. El resultado de este examen indica si un puerto está abierto si la máquina admite el pedido de acceso en ese puerto, filtrado si hay un filtro de *firewall* en el puerto y *Nmap* determina si está abierto o cerrado.

Las pruebas fundamentadas en el protocolo TCP de tres vías, son requeridas para conectar y transmitir datos del remitente al destinatario. La figura 2.28 muestra el esquema del protocolo TCP de tres vías.

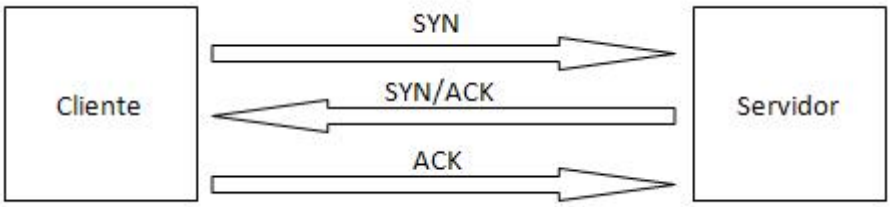


Figura 2.28 Protocolo TCP de tres vías
Fuente: danred.wordpress.com

Para realizar el enlace de tres vías y conectar dos equipos, el remitente manda un paquete TCP con el bit de sincronización (SYN), el destinatario contesta con un paquete TCP y la sincronización (SYN) y un bit ACK (*Acknowledgement*) de reconocimiento del pedido que dice a la computadora que puede aceptar datos. El emisor envía un paquete final con ACK, esto significa que el enlace está completo y la información puede transmitirse.

Como TCP es orientado a enlace, un proceso para instaurar un enlace de tres vías, el reinicio por un error de enlace y la finalización de un enlace son segmentos del protocolo, denominándose a las notificaciones *flags*. Las funciones de los parámetros TCP son:

- SYN, sincronizar para empezar el enlace entre *hosts*.
- ACK, reconocimiento para realizar el enlace entre *hosts*.
- PSH, *Push*, implica el reenvío de información de la memoria *buffer*.
- URG, urgente, asigna la prioridad de procesamiento de la información
- FIN, finalizar los envios.
- RST, *reset*, implica la restauración del enlace.

El atacante podría tratar de evitar la localización empleando *flags* en vez de consumar el enlace TCP debidamente.

La interfaz gráfica de *Nmap* se denomina *Zenmap*, y entre sus ventajas está la de ser interactiva, presenta los resultados de manera sencilla y puede hacer un seguimiento de ellos, pudiendo dibujar un diagrama de la red localizada y también puede comparar dos exploraciones. Esta interfaz además del análisis general de las IP activas admite escoger una dirección específica y explorarla más a fondo.

2.3 Proceso de Enumeración

Este factor se realiza después de que ocurren los procesos de digitalizar y resumir las denominaciones de usuario, equipos, elementos de red, operaciones y servicios. La enumeración además implica consulta o el enlace con un destinatario para conseguir esos datos.

Resumiendo puede decirse que un atacante debería cumplir los siguientes procesos para atacar un sistema: obtener las denominaciones de los usuarios con la

enumeración y datos de sus cuentas y explorar los puertos SNMP (*Simple Network Management Protocol*).
En otras palabras, la enumeración pretende caracterizar una cuenta de usuario para emplearla en el ataque. Nótese que no se necesita hallar una cuenta de administrador del sistema, porque la mayor parte de exenciones de una cuenta se puede ascender para que ella tenga mayores accesos de los que tenía antes.

Nbtscan es un instrumento empleado para explorar direcciones IP y conseguir datos de la denominación *NetBIOS* (*Network Basic Input/Output System*), presenta un resumen con la dirección IP, denominación de equipos NetBIOS, servicios activos, registros del usuario y la dirección MAC de los equipos involucrados, datos necesarios para el proceso de *PenTest*. Al emplear *Nbtscan* se produce mucho tráfico lo cual puede ser captado por los destinatarios.

Con los informes obtenidos se puede determinar el servicio NetBIOS y su correspondiente IP y dirección MAC, lo cual además es posible examinar con otros instrumentos ya mencionados, pero la superioridad de ésta es que suministra datos importantes relacionados con grupos de trabajo que corresponden al equipo por lo que el examen es más detallado.

NetBIOS, es un protocolo de *Windows* para determinación de denominaciones que es posible encapsular en TCP/IP, opera en la capa de aplicación, presentando un aspecto similar a toda red de Windows sin importar los protocolos empleados en las capas de red y transporte. Accede a compartir ficheros, dispositivos y visualizar recursos activos en la red. Máquinas que operan con *Windows* principalmente versión XP con el servicio de *NetBios* activo, pueden ser aprovechadas con *exploits* que emplean debilidades de dicho servicio.

El proceso de enumeración SNMP implica el empleo de este protocolo para enumerar cuentas de usuario en un sistema determinado. Dicho protocolo usa dos clases de elementos de programación para comunicarse, el agente SNMP, en el terminal de red y la estación de administración SNMP. La mayoría de

Casi todas las unidades de red que tengan sistema *Windows*, tienen un agente SNMP para la gestión del sistema o terminal. La estación de administración SNMP manda los pedidos a los agentes y estos las respuestas, ambas corresponden a las variables de configuración viables mediante programación del agente. Esa gestión además puede mandar pedidos para implantar el valor de determinadas variables. La base de datos de variables de disposición del terminal de red se denomina MIB (*Management Information Base*).

Para ingreso y especificación del agente de la estación de gestión, SNMP posee dos claves, la una es *read community string*, que permite visualizar la disposición del terminal o sistema y la otra es *read/write community string*, para alterar la disposición en la unidad. Una abertura en la protección ocurre cuando si las claves se dejan en la alineación por defecto, un atacante puede emplear claves por defecto para visualizar o alterar la disposición de la unidad.

Un explorador de SNMP llamado *Onesixtyone* puede emplearse para saber si está la cadena SNMP en una unidad. Este explorador se distingue de SNMP porque manda todos los pedidos del protocolo tan rápido como pueda y aguarda la réplica y los registra. Si la unidad está activa se mandan contestaciones con la cadena SNMP.

Un instrumento útil para identificar huella digital y prueba de sistemas de *IPSec VPN* (*Internet Protocol security Virtual Private Network*) se denomina *Ike-Scan*. Se basa en mandar un paquete IKE (*Internet Key Exchange*) de fase 1 a los servidores *VPN* y la observación de las réplicas que recogió. Es decir q este protocolo permite intercambiar claves y certificación par *IPsec*.

Redes punto a punto *IPSec VPN* se emplean para conectar pequeñas, medianas y grandes sucursales a la ubicación central. En la figura 2.29 se muestra la composición de un modelo de implementación *IPSec VPN* de Cisco.

Entre las características de *Ike-scan* se puede mencionar que puede mandar paquetes IKE a cualquier cantidad de destinatarios, tales paquetes se pueden hacer de manera flexible, puede decodificar y presentar las réplicas, en general los resultados incluyen el proveedor y el modelo del servidor VPN, datos útiles en la evaluación de debilidades.

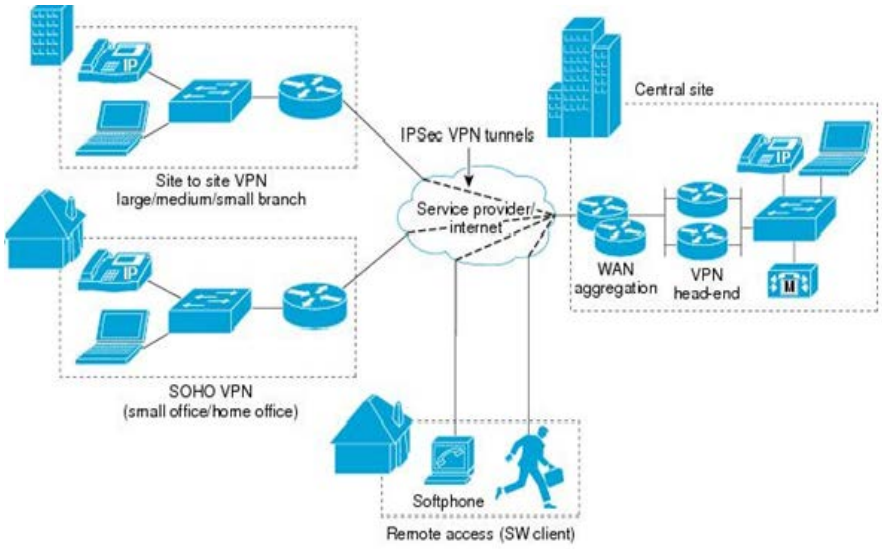


Figura 2.29 Composición de un modelo de implementación *IPSec VPN* de Cisco
Fuente: www.cisco.com

2.4 Evaluación de debilidades

Este es un proceso para determinar las debilidades de seguridad de los sistemas conectados en una red. Usualmente, una exploración de fragilidades se inicia determinando el sistema operativo y su versión, esto implica los paquetes de servicio que posiblemente estén conectados. Con esos datos el explorador determina las fragilidades del sistema operativo, las mismas que podrían ser aprovechadas en el ataque para ingresar al sistema.

Este proceso de determinar las debilidades se denomina Mapeo de Vulnerabilidades en el que se examina las principales fallas en la protección del entorno bajo estudio. Este examen es básico en un programa de gestión de debilidades en que los controles de protección de la infraestructura se examinan detalladamente. Luego de

la recopilación de datos, la identificación y la enumeración se han realizado, se debe averiguar las debilidades del objetivo que podrían poner en riesgo al sistema y posibilitar la falla de seguridad.

Las debilidades pueden ser de diseño, si se determinan por las fragilidades de las especificaciones de programación, de implementación son las fallas técnicas de protección en el código de un sistema y de funcionamiento son las que pueden aparecer por una configuración impropia.

Si un *hacker* necesita acceso local para impulsar la debilidad de un sistema accionando un código, se denomina vulnerabilidad local, aprovechando esta debilidad puede acrecentar los derechos de ingreso. En cambio, si el *hacker* no tiene ingreso previo, sino la debilidad que puede aprovecharse accionando el código malintencionado en la red es una vulnerabilidad remota, así un *hacker* puede ingresar remotamente al equipo sin enfrentar las defensas del sistema.

Un servicio de exploración de debilidades denominado *Nessus,* actúa en variados sistemas operativos, es un proceso informático del tipo *daemon, nessusd* explora el sistema objetivo y *nessus*, al cliente, este último presenta resultado de las exploraciones.

Nessus empieza explorando puertos buscando aquellos abiertos y después prueba algunos *exploits* con miras a una agresión y lo presenta en la interfaz del cliente *nessus*. Estos resultados pueden almacenarse en una base de datos como referencia para otras exploraciones. La figura 2.30 muestra la pantalla de ingreso a *Nessus*.

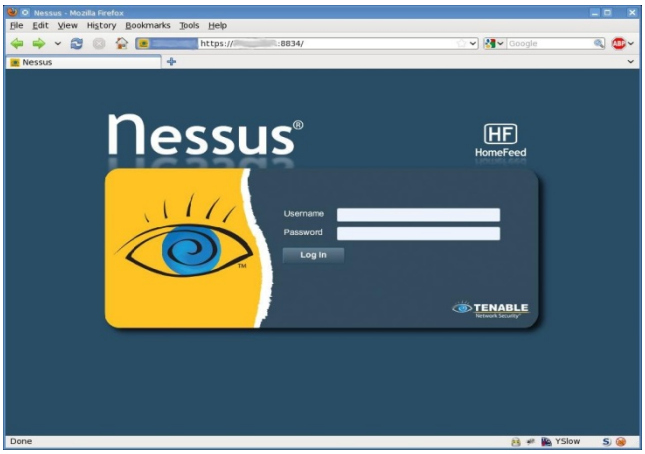


Figura 2.30 Pantalla de ingreso a *Nessus*.

Fuente: systemadmin.es

A continuación se genera una orientación individualizada en la opción *Policies* y después en *+Add*. Entonce se observa la pantalla *Add Policy*, como en la figura 2.31

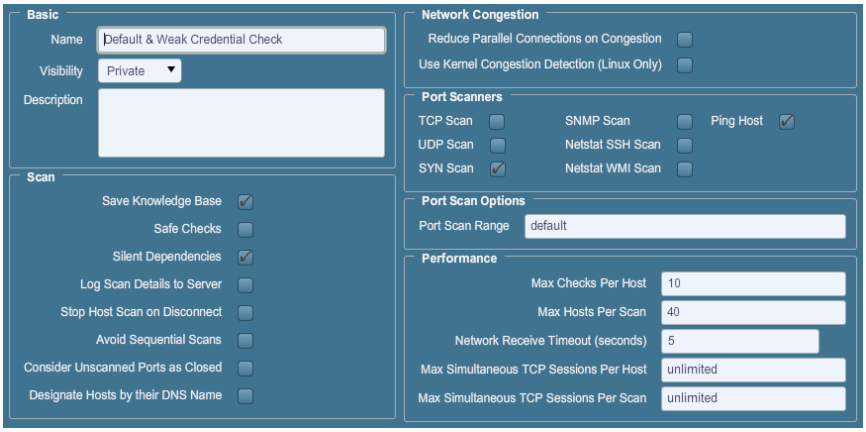


Figura 2.31 Añadiendo puna política de exploración

Fuente: www.tenable.com

Aparecen las opciones de configuración *General, Credentials, Plugins y Preferences*. Por lo general no hace falta cambiar la configuración establecida, sin embargo estas permite una supervisión más detallada de la ejecución de *Nessus*. En este caso de estudio se lo orienta a una red LAN que es la topología del entorno analizado. Ahora, se debe generar una nueva evaluación, se lo hace en la opción *Scans* y con *+Add* aparece la pantalla *AddScan* mostrada en la figura 2.32.

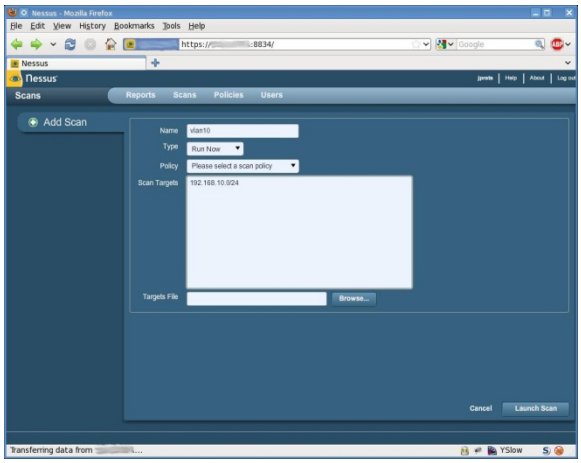


Figura 2.32 Configurando la exploración

Fuente: www.tenable.com

Se digita el nombre de identificación del análisis y se acciona *RunNow* en *Type* para la operación haciendo clic en *Submit*. A continuación en *Policy* se escoge la política que se había hecho para redes LAN, que determina las medidas de análisis de *Nessus*. Por último se indica el destino en *TargetsFile* y se realiza la evaluación. En *Reports*, se encuentra el listado de evaluaciones análisis en operación y terminadas, aquí se pueden visualizar y contrastar los resultados de las evaluaciones, observándose en el primer resumen cada host analizado con sus debilidades y puertos abiertos. Un ejemplo de este tipo de informe se presenta en la figura 2.33.

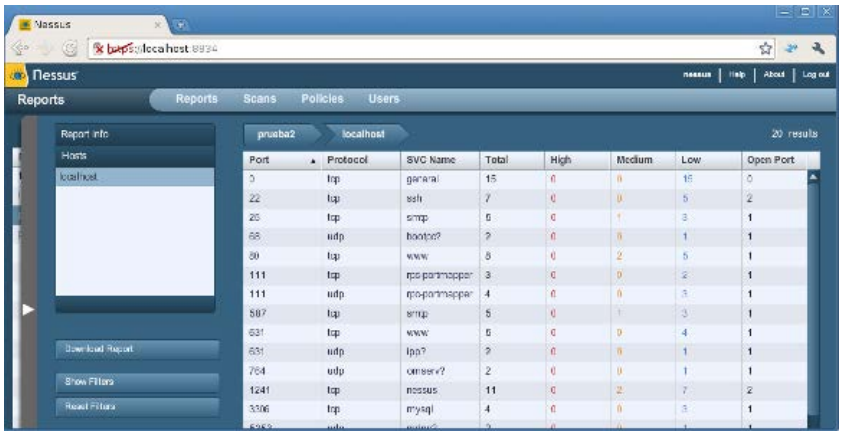


Figura 2.33 Reporte de la exploración en la pantalla de *Reports*

Fuente: www.tenable.com

El protocolo SMB (*Server Message Block*) o CIFS (*Common Internet File System*), hace posible compartir recursos en la red, así los usuarios autorizan el ingreso a sus equipos para simplificar la labor en conjunto del personal, sin embargo al mismo tiempo están permitiendo el acceso a los equipos de un *hacker*. En consecuencia, al permitir compartir ficheros en equipos con *Windows* implica fragilidades que pueden resultar en hurto de datos o ingreso de virus al sistema.

Los componentes SMB que posibilitan la compartición de ficheros archivos en *Windows* podrían ser empleados por *hackers* para conseguir datos del sistema. Con enlaces de la clase *sesión nula* mediante *NetBIOS* se puede recabar datos de denominaciones de usuarios o grupos, fechas de ingreso, claves y antecedentes de RAS (*Remote Access Services*) y emplearla en ataques al sistema.

2.1 Aplicación

Con el análisis de las debilidades encontradas a continuación hay que ingresar en el objetivo con los *exploits* aprovechables. Mediante la evaluación de fragilidades se determinó el destino y se comienza a averiguar cómo ingresar al sistema: mediante algún servicio que muestre una debilidad, un *host* cuyo *firewall* no está bien estructurado o un equipo mal configurado.

En esta sección se va a detallar escuetamente el procedimiento para aprovechar un objetivo con *Metasploit,* un programa que posee algunos mecanismos para hacer análisis de inserción para aprovechar las fragilidades de la red. La figura 2.34 muestra la arquitectura de *Metasploit.*

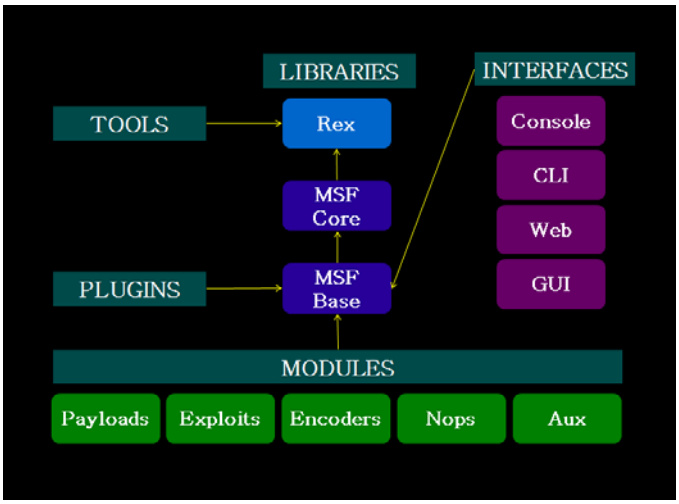


Figura 2.34 Arquitectura de *Metasploit.*

Fuente: (Aharoni, Coppola, Kearns, & otros, 2011)

En la figura 2.34 se observa el bloque *console* como integrante de las interfaces que conforman la arquitectura de *Metasploit* y se la denomina *Msfconsole,* es una interfaz *all-in-one* para la mayoría de las características de *Metasploit,* se usa para lanzar ataques, crear oyentes entre otras funciones. Viene instalado en *backtrack 5,* y se lo usa para mandar *exploits.* Una vez determinada la IP del equipo que se va a atacar, para ingresar se va a una estación de *backtrack 5* y se digita *Msfconsole,* observándose la pantalla mostrada en la figura 2.35.

Figura 2.35 Ingreso a *Msfconsole*

Fuente: (slideshare, 2012)

Después del ingreso a *Msfconsole,* se observa la pantalla mostrada en la figura 2.36

Figura 2.36 *Msfconsole*

Fuente: (slideshare, 2012)

A continuación se busca el *exploit* digitando *searchnetapi* como se muestra en la figura 2.37

Figura 2.37 Comando *searchnetapi*

Fuente: (slideshare, 2012)

Ahora se selecciona el *exploit* digitando useexplot/Windows/smb/ms08_67netapi, obteniéndose la pantalla de la figura 2.38

Figura 2.38 Comando *searchnetapi*

Fuente: (slideshare, 2012)

El siguiente paso consiste en confirmar la información para atacar el objetivo, en este caso una computadora con Windows xp, la pantalla correspondiente aparece en figura 2.39

Figura 2.39 Confirmación de información del objetivo

Fuente: (slideshare, 2012)

En la figura 2.40 se muestra la pantalla que se obtiene al estructurar el *RHOST* digitando *set rhost* y la IP del equipo, en este caso: 192.168.0.60

Figura 2.40 Estructuración del *RHOST*

Fuente: (slideshare, 2012)

Se procede ahora a buscar el *payload* en forma similar como se hizo con el *exploit*, se digita *searchpayload* y después *setpayloadwindows*/*Shell/bind_tcp* de esta manera se accede al equipo por el CMD (*command*), la pantalla correspondiente se muestra en la figura 2.41

Figura 2.41 Búsqueda del *Payload*

Fuente: (slideshare, 2012)

Las alternativas de cómo está estructurado el exploit se obtienen digitando *showoptions*, como se ve en la figura 2.42

Figura 2.42 Opciones de estructuración del *exploit*

Fuente: (slideshare, 2012)

Una vez concluida la estructuración del *exploit*, se puede atacar el objetivo digitando *exploit*, obteniendo la pantalla de la figura 2.43

Figura 2.43 Ataque con *exploit*

Fuente: (slideshare, 2012)

En este momento es posible usar una instrucción de *Windows* puesto que se tiene el control del equipo con *Msfconsole*. Nótese que se puede cambiar, borrar, escribir, etc.

CAPITULO 3: ANÁLISIS DE LA SEGURIDAD

Este estudio nace se origina por el interés de presentar las diversas debilidades de la red que se quiere analizar, en este caso la del Laboratorio de Electrónica d le FET.

Estadísticas informáticas aseguran que aproximadamente el 80% de los engaños realizados con equipos de computación son causados por el propio personal de la institución o por el mal manejo de la red local, eso demuestra que son las intranets las más sensibles a agresiones informáticas.

De esta manera, si se desea establecer los defectos de protección del sistema, hay que aplicar técnicas de *hackeo,* y de acuerdo a lo analizado hasta ahora acerca de tales métodos, se debe efectuar la prueba de penetración, de la cual ya se habló anteriormente. Ésta radica en efectuar un análisis de debilidades y luego lanzar ataques específicos a las máquinas y elementos del sistema, de esta manera se establecen los defectos de protección que permitirán recomendar las rectificaciones adecuadas para reducir el impacto en la red y las posibilidades de ser agredidos.

3.1 Objetivo del estudio

Presentar la forma de efectuar la prueba de penetración para su futura realización, lo que permitirá mejorar la protección de la red LAN del laboratorio analizado. Estas exploraciones se recomienda realizarlas con el programa *Linux Backtrack*, que como ya se ha analizado brinda las herramientas adecuadas para establecer las fragilidades de una red.

3.2 Memoria técnica

Este documento incluye las propiedades fundamentales de protección que opera la red y recomendaciones a considerar en el diseño y construcción del sistema, sus debilidades, como podría un hacker aprovecharlas, el efecto que causaría y las correcciones que deberían hacerse para defenderse de estos desafíos.

Este estudio recomienda emplear la técnica de *hacking* ético para efectuar una exploración de las debilidades de protección de la red del laboratorio.

Este análisis debe permitir encontrar la mayoría de las fragilidades y establecer el riesgo que representan y la posibilidad de que sean aprovechadas. Por esta razón, las pruebas deben incluir ataques a esas debilidades de manera controlada.

Con este examen se pretende señalar la trascendencia que significa ejecutar una prueba de penetración y la utilidad que representa.

Será necesario recoger datos y analizarlos para que contribuyan al *pentest* a ejecutarse. Para la recolección de datos se debe emplear instrumentos de *backtrack* como *footprinting, metagoofil*, *thehavester* y *maltego*, cuyas funciones ya se explicaron con anterioridad y con la que se obtienen datos de usuarios tales como denominación de dominios, subdominios y usuarios con sus IP, sistema operativo activo, unidades, servicios y aplicaciones de red, arquitectura del medio, elementos de autentificación y localización de extraños, etc., datos importantes para la determinación de debilidades de la LAN con BackTrack.

A continuación deben ejecutarse los siguientes procesos: mapeo de infraestructura, exploración de puertos y análisis de la construcción, utilizando los instrumentos *Nmap*, *netifera*, *ntbscan* y *Zenmap*, obteniéndose datos de puertos abiertos, protocolo aplicado, estado y servicio que realiza, direcciones IP y servicios activos, sistema operativo, dirección MAC, VPNs Activas, etc.

La valoración de la fragilidad significa el reconocimiento de las debilidades en el examen y la categorización de riesgo de las amenazas., obteniéndose así las clases de debilidades presentes siendo el de seriedad alta aquel de mayor fragilidad de acuerdo a la categorización *Nessus*, luego se tiene de seriedad media con una categoría moderada de peligro y la de baja seriedad o de poco riesgo lo cual implica escasa incidencia para esa fragilidad específica. Esta herramienta elabora con la información obtenida el mapa de debilidades, un resumen de las mismas con su respectiva

categoría de riesgo y sus correspondientes IP, en la forma mostrada en la figura 3.1 donde la sriedad mayor de amenaza se muestra con color rojo.

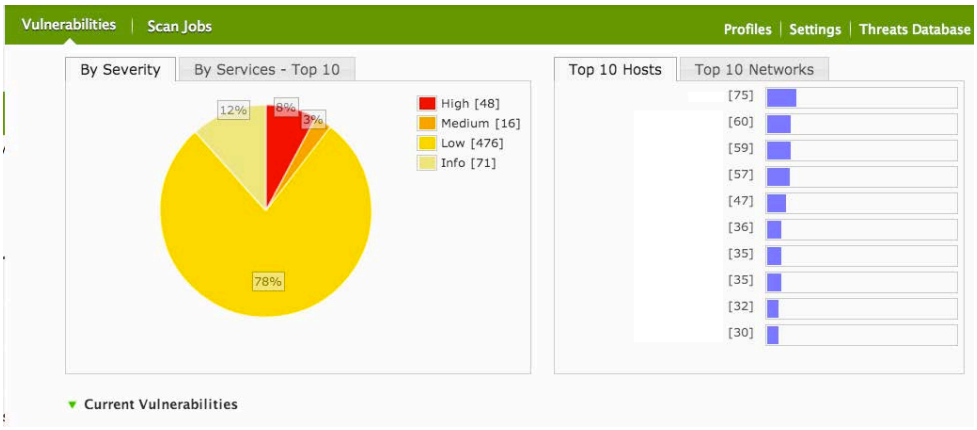


Figura 3.1 Mapa de fragilidades

Fuente: www.securitybydefault.com

3.3 Aprovechamiento de las fragilidades

El siguiente paso es el aprovechamiento de las debilidades determinadas en el punto anterior, mediante su activación con la finalidad de establecer un rango determinado de ingreso al objetivo. Para la ejecución de estos ataques pueden utilizarse diferentes instrumentos como *Nmap, Ettercap, Arp, Metaesploit, DNS*, entre otros.

Con los resultados obtenidos es posible elaborar una tabla que relaciona las debilidades determinadas con su nivel de seriedad.

3.4 Evaluación de la infraestructura del sistema

La red encargada del transporte de datos en la FET presenta una infraestructura que nace del Centro de Cómputo de la UCSG de donde parte un enlace de fibra óptica al rack principal de la facultad, ubicado en el ingreso de la misma junto a las oficinas administrativas.

De este rack se distribuye a las diferentes dependencias de la FET como se mostrará detalladamente más adelante.

A continuación se presenta la descripción de los elementos pasivos y activos de los racks de la Facultad Técnica:

RACK SALA VIRTUAL

- RACK DE PARED CERRADO
- PATCH PANEL SIEMON (24 PUERTOS) 23 PUERTOS OCUPADOS Y 1 PUERTO LIBRE (23)
- ORGANIZADOR HORIZONTAL
- SWITCH 3COM BASELINE 2824 (24 PUERTOS) (1) TODOS LOS PUERTOS OCUPADOS
- ORGANIZADOR HORIZONTAL
- SWITCH QCOM QP-108EC (8 PUERTOS) (2) 5 PUERTOS OCUPADOS Y 3 PUERTOS LIBRES (4, 5, 7)
- MULTITOMA 110V
- RACK DE PARED ABIERTO
- PATCH PANEL QCOM (48 PUERTOS) 33 PUERTOS OCUPADOS Y 15 PUERTOS LIBRES (33, 35, 36, 37….48)
- SWITCH QCOM (24 PUERTOS) (1) TOD….
- SWITCH 3COM BASELINE 2824 (24 PUERTOS) (2) TOD….

SIMBOLOGIA

(1) (2) NUMERACION DE PATCH PANEL EN ORDEN ASCEDENTE

(1) (2) NUMERACION DE SWITCH EN ORDEN ASCENDENTE

RACK SALA DE LECTURA

- RACK DE PARED ABIERTO
- 2 TRANSCEIVER
- SWITCH 3COM BASELINE 2024 (24 PUERTOS) 22 PUERTOS OCUPADOS 2 PUERTOS LIBRES (2, 16)
- ORGANIZADOR HORIZONTAL
- PATCH PANEL PANDUIT (24 PUERTOS) 21 PUERTOS OCUPADOS Y 3 PUERTOS LIBRES (22, 23, 24)

RACK DE LABORATORIO DE TELECOMUNICACIONES

- RACK DE PISO (1)
- PATCH PANEL SIGNAMAX (12 PUERTOS) /INHABILITADO
- ORGANIZADOR HORIZONTAL 3UR /INHABILITADO
- PATCH PANEL SIGNAMAX (24 PUERTOS) /INHABILITADO
- BANDEJA /INHABILITADO
- BANDEJA PARA FIBRA /INHABILITADO
- ORGANIZADOR HORIZONTAL 2UR
- SWITCH ALLIED TELESYN AT-FS716L (16 PUERTOS)
- 13 PUERTOS OCUPADOS Y 3 PUERTOS LIBRES (8, 15, 16)
- PATCH PANEL SIGNAMAX (24 PUERTOS) 13 PUERTOS OCUPADOS Y 11 PUERTOS LIBRES (14, 15…….24)
- ORGANIZADOR HORIZONTAL 2UR
- SWITCH DLINK DES-33265R (24 PUERTOS) /INHABILITADO 23 PUERTOS OCUPADOS Y 1 PUERTO LIBRE (23)
- MULTITOMA 110V /INHABILITADO
- RACK DE PISO (2)
- ESTACION DE TRABAJO)SERVIDOR)
- PATCH PANEL SIGNAMAX (12 PUERTOS) 3 PUERTOS OCUPADOS Y 9 PUERTOS LIBRES (4, 5……12)
- ORGANIZADOR HORIZONTAL 2UR

- SWITCH CNET (8 PUERTOS) 7 PUERTOS OCUPADOS Y 1 PUERTO LIBRE (8)

LABORATORIO DE ELECTRONICA

- SWITCH DLINK DES-1008D (8 PUERTOS)
- SWITCH DLINK DES-1016D (16 PUERTOS)

LABORATORIO DE CONTROL Y MOVIMIENTO

- PATCH PANEL QCOM (16 PUERTOS) (1) 14 PUERTOS OCUPADOS Y 2 PUERTOS LIBRES (15, 16)
- PATCH PANEL QCOM (16 PUERTOS) (2) 13 PUERTOS OCUPADOS Y 3 PUERTOS LIBRES (14, 15, 16)
- ORGANIZADOR HORIZONTAL 2UR
- SWITCH TP-LINK TL-SG1016 (16 PUERTOS) (1) 15 PUERTOS OCUPADOS Y 1 PUERTO LIBRE (13)
- SWITCH TP-LINK TL-SG1016 (16 PUERTOS) (2) 15 PUERTOS OCUPADOS Y 1 PUERTO LIBRE (13)

RACK PRINCIPAL (OFICINAS)

- 2 TRANSCEIVER (SALA DE LECTURA Y AULA VIRTUAL)
- SWITCH CISCO CATALYST 2950 SERIES (48 PUERTOS) (1) TODOS LOS PUERTOS OCUPADOS
- SWITCH 3COM BASELINE 2824 (24 PUERTOS) (2) 17 PUERTOS OCUPADOS 7 PUERTOS LIBRES (13, 14, 15, 18, 20, 21, 23)
- SWITCH 3COM BASELINE 3300 (24 PUERTOS) (3) 18 PUERTOS OCUPADOS 6 PUERTOS LIBRES (5, 6……23)
- ORGANIZADOR HORIZONTAL 2UR

- ORGANIZADOR HORIZONTAL 2UR
- PATCH PANEL SIEMON (24 PUERTOS) (1) 21 PUERTOS OCUPADOS Y 3 PUERTOS LIBRES (18, 19, 24)
- PATCH PANEL SIGNAMAX (24 PUERTOS) (2) 14 PUERTOS OCUPADOS Y 10 PUERTOS LIBRES (1, 7, 11, 14, 16, 18, 20, 21…23)
- SWITCH LB-LINK (16 PUERTOS)//WIFI (4)
- MULTITOMA 110V
- MULTITOMA 110V
- MULTIPAR DE TELEFONO
- ORGANIZADOR HORIZONTAL 2UR

En lo referente a las direcciones IP, considerando que este estudio se limita al Laboratorio de Electrónica, solo se indicarán las que corresponden a esta dependencia y son desde la 192.16.0.160 hasta la 192.168.191, la dirección IP 192.16.0.62 es utilizada por el encargado del laboratorio.

En la figura 3.2 se presenta un plano esquemático del diagrama unifilar del cableado estructurado correspondiente a la red de datos de la FET, puede verse el rack principal junto a las oficinas administrativas, el cual es alimentado mediante fibra óptica desde el Centro de Cómputo de la UCSG y de allí nace la distribución a todas las dependencias de la facultad, incluyendo la que alimenta al Laboratorio de Electrónica, motivo de este estudio, la distribución de la LAN de este laboratorio se muestra en la figura 3.3 y a continuación se presenta el detalle de sus instalaciones:

LABORATORIO DE ELECTRONICA

RED DE DATO	SWITCH DLINK (24 PUERTOS)	N° PUERT	OBSERVACIONE
ENLACE DE RED (SW DES-1008D)	SWITCH DLINK DES-1008D (8 PUERTOS)	1	OK
PUNTO LIBRE	SWITCH DLINK DES-1008D (8 PUERTOS)	2	OK
ENLACE DE RED (SW DES-1016D)	SWITCH DLINK DES-1016D (16 PUERTOS)	2	OK
ADMINISTRADOR 1	SWITCH DLINK DES-1016D (16 PUERTOS)	2	OK
PC 15	SWITCH DLINK DES-1008D (8 PUERTOS)	3	OK
PC 17	SWITCH DLINK DES-1008D (8 PUERTOS)	4	OK
PC 10	SWITCH DLINK DES-1016D (16 PUERTOS)	4	OK
PC 11	SWITCH DLINK DES-1016D (16 PUERTOS)	5	OBSERVACION
PUNTO LIBRE	SWITCH DLINK DES-1008D (8 PUERTOS)	5	OK
PC 6	SWITCH DLINK DES-1016D (16 PUERTOS)	6	OK
PC 5	SWITCH DLINK DES-1008D (8 PUERTOS)	6	OK
PC 13	SWITCH DLINK DES-1008D (8 PUERTOS)	7	OK
PC 3	SWITCH DLINK DES-1016D (16 PUERTOS)	7	OK
PC 14	SWITCH DLINK DES-1016D (16 PUERTOS)	8	OK
PC 16	SWITCH DLINK DES-1008D (8 PUERTOS)	8	OK
PC 4	SWITCH DLINK DES-1016D (16 PUERTOS)	9	OBSERVACION
PC 8	SWITCH DLINK DES-1016D (16 PUERTOS)	10	OK
PC 18	SWITCH DLINK DES-1016D (16 PUERTOS)	11	OK
PC 9	SWITCH DLINK DES-1016D (16 PUERTOS)	12	OK
ADMINISTRADOR 2	SWITCH DLINK DES-1016D (16 PUERTOS)	13	OK
PC 12	SWITCH DLINK DES-1016D (16 PUERTOS)	14	OK
PC 7	SWITCH DLINK DES-1016D (16 PUERTOS)	15	OK
PC 2	SWITCH DLINK DES-1016D (16 PUERTOS)	16	OK

Tabla 3.1 Datos del Laboratorio

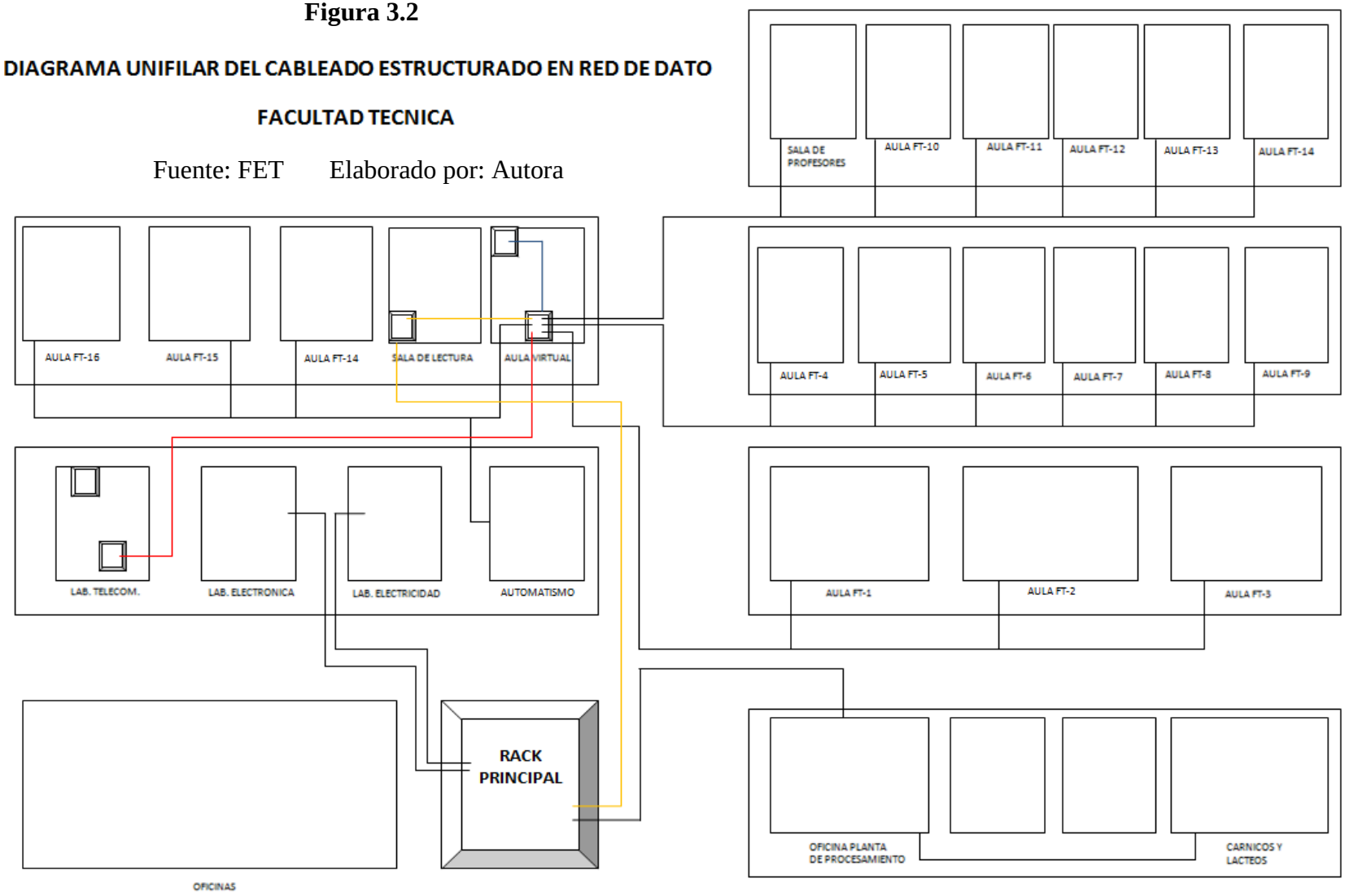
Diseño: Mazzini, 2014

Figura 3.2

DIAGRAMA UNIFILAR DEL CABLEADO ESTRUCTURADO EN RED DE DATO

FACULTAD TECNICA

Fuente: FET Elaborado por: Autora



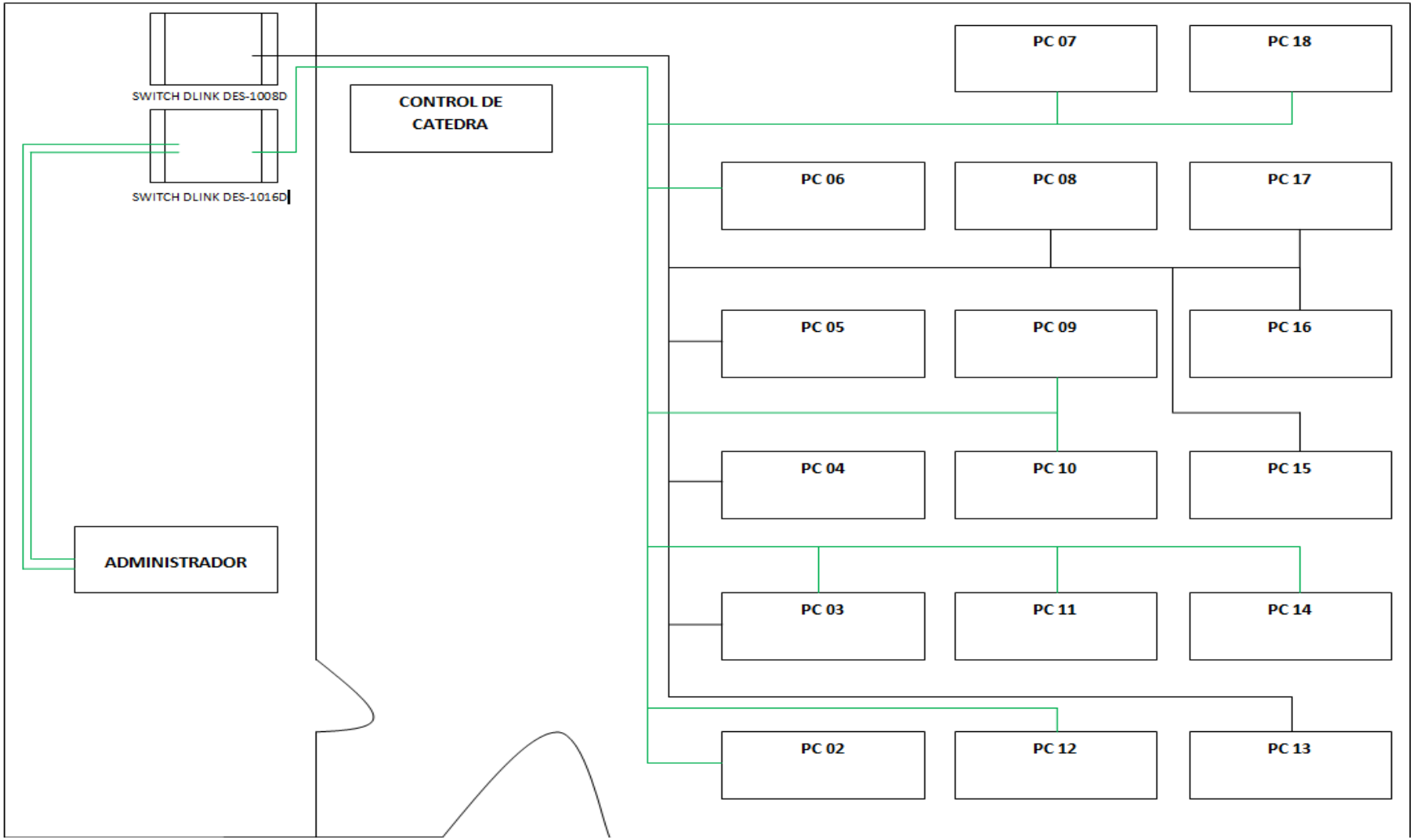


Figura 3.3 Cableado estructurado del Laboratorio de Electrónica de la FET
Fuente: FET Elaborado por: Autora

3.5 Evaluación de peligros

A fin de establecer los peligros, es necesario determinar algunas características tales como la presencia de una posibilidad de avería. Al alto porcentaje de daños causados por usuarios internos hay que añadir la poca preparación técnica de los encargados de la red, en aspectos como la gestión y protección de redes, lo cual incrementa la posibilidad de fragilidades y peligros informáticos. En este punto hay que especificar la importancia de mantener programas antivirus actualizados para proteger las computadoras.

Las averías pueden producirse por la presencia de fragilidades en el diseño de red, en su sistema operativo y en sus utilidades, por la prohibición de servicios, pérdida de datos, falsificación de identificación, a causa de la colaboración evidente de los supervisores del sistema.

El establecimiento de la valoración del peligro implica la evaluación de la posibilidad y sus resultados si el riesgo se hace realidad, pudiendo presentarse fallas como la pérdida de datos.

Al evaluar los peligros es necesario también analizar los peligros físicos y establecer si tiene la protección material y técnica adecuada, manuales de procedimientos para el personal de acuerdo a sus cargos, los controles para establecer la clase de peligro, etc.

Con los resultados obtenidos del análisis efectuado se debe realizar su estimación respecto a un peligro permisible. Es importante aceptar que excluir el peligro no es posible porque para alcanzar eso el sistema debería dejar de trabajar, por lo tanto hay que efectuara una evaluación periódica de la red, un entrenamiento continuo y actualización de conocimientos de los encargados de la gestión, uso de programas que disminuyen la posibilidad de ocurrencia de peligros. Estos análisis permitirán realizar la aplicación de las medidas adecuadas y oportunas.

El análisis de las medidas que se tomen deben examinarse continuamente, registros estadísticos para determinar la eficiencia de los métodos aplicados para disminuir el peligro y la continua evaluación a fin de ir adaptándolo a los requerimientos del sistema o de la organización que por lo general varían periódicamente.

3.6 Gestión de peligros

Para optimizar la gestión de los peligros que se puedan presentar es necesario primero reconocerlos, evaluarlos, dimensionarlos y dominarlos.

El reconocerlos significa comprender que se tienen debilidades en el procedimiento informático en la estructura de la red del Laboratorio de Electrónica de la FET, porque todos los programas presentan fallas de diseño y/o implementación las cuales significan una fragilidad de la protección de la estructura. (Katz, 2013)

Esta aseveración de uno de los *hackers* más reconocidos confirma la potencial presencia de fragilidades en las redes informáticas porque todo sistema utiliza programas para su operación. De la misma manera es posible hallar debilidades en la construcción de las redes, servicios y protocolos empleados en las organizaciones, en consecuencia la posibilidad de peligro significa una gran posibilidad de ocurrencia, en especial en establecimientos como la UCSG en que la protección de los usuarios no es preponderante, razón por la cual la presencia de virus es constante, generándose desconfianza para usar las máquinas de la universidad y causando un desprestigio a la misma.

El siguiente proceso para optimizar la gestión de los peligros que se puedan presentar es la evaluación de los mismos, asignándoles una categorización fundamentada en la magnitud del peligro según su efecto y la posibilidad de ocurrencia. Por ejemplo, el mantener programas, equipos y servicios sin actualizar significa un peligro significativo a causa de que la posibilidad de que se produzca es elevada y su efecto es perjudicial, por consiguiente debe disminuirse este peligro, para lo cual verán hacerse inversiones económicas para la

actualización de los programas y equipos con versiones más modernas que incluyen avances respecto a las anteriores.

En entornos como el de este estudio puede producirse el contagio de los equipos con virus a causa de la inobservancia del procedimiento adecuado para manejar los datos, este es un peligro inaceptable ya que la posibilidad de que se produzca es elevada y su efecto muy perjudicial para el sistema. Es por lo tanto importante adoptar las decisiones adecuadas frente a esta amenaza, por ejemplo la implementación de un manual fundamentado en la norma ISO/IEC 27001 para mejorar la gestión en lo referente a la protección de los datos, el mismo que debe implicar a todos quienes utilizan estas máquinas de acuerdo a su función y/o actividad, comprometiéndolos a su cumplimiento. (bsi)

En el dimensionamiento de los peligros, éstos se categorizan y se determina sus registros evaluando si son adecuados para especificar el rango del peligro.

Finalmente, para dominar los peligros posibles se adoptan medidas para reducirlos, evaluando la práctica de los métodos, comprobando potenciales desvíos en relación al producto deseado para la implementación de medidas de prevención, el dominio se establece con un procedimiento ante los peligros, estas medidas para aminorarlos se ejecutan mediante acciones preventivas que reducen el efecto del peligro.

3.7 Normas de protección

Un estudio para la elaboración e implementación de este tipo de reglamento, debe fundamentarse en los resultados de una evaluación realizada en la forma detallada en este trabajo de investigación, siendo necesaria la asignación de responsabilidades respecto a la gestión de la red, por ejemplo un administrador que examine continuamente la protección de las redes y sus equipos, las eventualidades que se produzcan, analizará y aprobará los planes de protección a éstas áreas, de igual manera deberá aprobar las estrategias, reglas e instrucciones relacionadas con la protección de la información, entre otras funciones vinculadas con este aspecto.

El responsable de la administración de la red se encarga de organizar la protección del sistema, asignar jerarquías a de acceso a los usuarios de manera adecuada, analizar las pruebas de ingreso y adoptar medidas de protección para el sistema bajo su responsabilidad. Esta reglamentación debe ser analizada y difundida a quienes ingresan a la red y éstos deben estar obligados a respetarla, así como cualquier norma para proteger el sistema e informar cualquier fragilidad o infracción que detecten, con la finalidad de mejorar su eficiencia.

3.7.1 Normas de ingreso al sistema

Cada usuario debe elegir una clave personal para ingresar al sistema, la cual deben recordar para no tener que anotarla en ningún sitio ni que sea posible de descubrir por alguien sin autorización. En definitiva no puede comunicar su clave a nadie y si precisa compartir información de su máquina con otro usuario debe emplear los mensajes electrónicos.

La reglamentación correspondiente debe incluir normativas para la asignación de claves a los nuevos usuarios o reasignación de las mismas en caso de olvido, éstas deben ser cambiadas por el usuario en cuanto entre al sistema.

3.7.2 Normas de inicio y fin de consulta

Al inicio de una sesión de consulta o práctica en las máquinas del laboratorio, el usuario debe ingresar su nombre y clave. Estos datos son únicos para quienes participan en este proceso. No debe permitirse el empleo de módems adicionales en los puestos de trabajo en que se ubican las máquinas conectadas a la red del laboratorio, estos dispositivos podrán utilizarse en equipos portátiles con autorización del administrador de la red y empleando un *firewall* adecuado.

En la programación del sistema debe agregarse un comunicado referente a la exclusividad de ingreso a usuarios calificados, que todo ingreso es registrado y que acepta que las

infracciones al reglamento del laboratorio ocasionarán sanciones disciplinarias y legales de ser necesario.

Durante el acceso al sistema solo hay que solicitar al usuario que se enlace y generar solo los mensajes obligatorios, sin dar datos concretos que los equipos posean de la institución, su sistema operativo y arquitectura de la red.

En caso de inactividad en una máquina por un tiempo determinado que puede ser de 5 o 10 minutos, se debe interrumpir la sesión y únicamente reiniciarse si el usuario ingresa un nombre y clave autorizada.

3.7.3 Jerarquización de acceso al sistema

La jerarquización es la asignación de concesiones en el sistema para los usuarios, implica la limitación de acceso a los programas necesarios para ejecutar el trabajo que debe realizar. Estas concesiones solo se aplicarán en casos de requerimientos autorizados.

Los usuarios no deben poder eliminar archivos y las claves de ingreso deben otorgarse solo a quienes realmente requieran ingresar al sistema.

Los programas y máquinas deben limitar el enlace a equipos con que puedan conectarse los usuarios mediante la red, esto puede realizarse con *routers*, puertos de conexión, *firewalls* y otros elementos, estos procedimientos deben impedir que un usuario pueda ir de un equipo a otro durante una sesión.

3.7.4 Rutas de ingreso al sistema

Las innovaciones a la LAN del laboratorio deben contener nueva programación, modificar las direcciones de red y reestructurar los *routers*, debiendo toda modificación ser permitida

por escrito y ejecutadas por personal autorizado. Esta reglamentación se aplica también a los proveedores de equipamiento y servicios.
No debe autorizarse a los usuarios poner en los equipos software de *blogs* o publicaciones electrónicas, redes LAN, servidores web o FTP, enlaces con modem a LANs o sistemas multiusuario para transmitir datos ni implementar nuevas formas de enlace en tiempo real entre dos o más sistemas informáticos internos sin permiso.

Aquellos equipos que se enlazan a redes locales o exteriores tienen que utilizar registros de ingreso con clave o procesos de autenticación de usuario y en el caso de puertos de sostenimiento remoto del equipamiento, estos deben invalidarse hasta que el proveedor los requiera e inhabilitarlos al terminar.

3.7.5 Programas antivirus

Es obligatorio reglamentariamente que los usuarios tengan activo en los equipos el programa antivirus instalado por la administración de la red. Este programa debe estar capacitado para investigar cualquier *software* procedente de los usuarios previo a la operación del mismo y sin prescindir de los métodos apropiados para contener la propagación del virus.

Reglamentariamente debe responsabilizarse a los usuarios por la eliminación de cualquier virus que aparezca en el equipo que estén trabajando mediante el programa adecuado implementado en las máquinas. Además debe informar al supervisor del laboratorio a fin de que no ocurran más contaminaciones y para que se solicite apoyo técnico para eliminar el virus en caso de ser necesario. La programación de las PCs del laboratorio debe duplicarse antes de la primera utilización y crear un respaldo para recobrar el sistema después de contaminaciones por virus en los equipos, trastornos del disco duro, entre otros inconvenientes que puedan ocurrir.

Los programas que se utilicen en las máquinas del laboratorio deben provenir de un origen seguro y no deben bajarse de *blogs* o publicaciones electrónicas, programas compartidos o públicos y en general ningún programa que no pase los controles establecidos.

3.7.6 Respaldo de *software* e información

El manual de procedimientos en el laboratorio debe establecer que recae en cada una de las personas que utilizan estos equipos la responsabilidad de crear el respaldo regularmente de los datos de la máquina que están operando y de la misma manera deberá procederse con cualquier dato importante del sistema. Sin embargo es el administrador quien establece el tipo de datos y los equipos que hay que respaldar, la periodicidad y el procedimiento que se aplicará para hacer el respaldo. Así por ejemplo, un sistema multiusuario como el del laboratorio debe respaldarse diariamente, en cambio en aquellos usados con procesos de trabajo con información importante deben respaldarse semanalmente. En lo referente a la información generada por el usuario en sus sesiones de prácticas de laboratorio, esta se respaldará según el criterio de quien está trabajando.

Las normas también deben estar encaminadas a elaborar procedimientos de emergencia para restituir la prestación a todos los dispositivos. Es obvio que los datos confidenciales deben codificarse para guardarse en el respaldo.

3.7.7 Codificación de la información

En el caso de datos confidenciales enviados por la red estos deben estar codificados y de no ser necesaria su transmisión se guardarán codificados también. Las técnicas de codificación aplicadas serán debidamente autorizadas.

Las contraseñas utilizadas en los procesos de codificación deben considerarse como datos confidenciales y custodiadas por el administrador y solo se compartirán con el respectivo permiso.

3.7.8 Uso de *laptops* en el laboratorio

La utilización de *laptops* en el laboratorio será responsabilidad de sus propietarios y su seguridad física e informática también.

El almacenamiento de datos confidenciales en discos compactos o externos, cinta magnética, *pendrive* o cualquier forma de grabación de datos debe ser registrado y clasificado de manera adecuada.

3.7.9 Privacidad y utilización de impresoras remotas

Al utilizar una impresora en el laboratorio debe estar bajo la observación del responsable de la impresión, además debe ser previamente autorizada su utilización. Si la impresora se ubica en un lugar seguro no será necesaria tal vigilancia. Estos procedimientos garantizan la privacidad de lo que se está imprimiendo.

Los servicios que se brindan en el laboratorio no incluyen la seguridad de los mensajes, es decir que estos no son codificados y por lo tanto no se tiene compromiso por la propagación de los datos transmitidos por la red y por consiguiente tampoco su privacidad. Si tales datos ameritan su codificación, el propietario de los mismos deberá solicitarlo.

3.7.10 Otros instrumentos de protección para el sistema

Un laboratorio que posee equipos informáticos como en este caso, requiere poseer los elementos necesarios que permitan al encargado de su supervisión constatar la protección del lugar. Estos instrumentos deben ser apropiados para el reconocimiento, localización y rectificación de inconvenientes que puedan presentarse.

Por consiguiente, de ser posible económicamente, estos instrumentos mecanizados deben implementarse en los equipos y en la red, los cuales pueden ser programas para comprobar las licencias de los equipos mediante una LAN. También deben anotarse adecuadamente

los sucesos importantes relacionados con la protección del laboratorio, tales como los cambios de identidad del usuario, tentativas de decodificar claves o acceder a funciones sin permiso, cambios en la programación del sistema, asignación de jerarquías y estructura del sistema.

Ante la posibilidad de ocurrencia de una infracción en algún equipo, los datos involucrados deben retenerse y guardarse para establecer las responsabilidades correspondientes y aplicar las medidas disciplinarias y/o legales según corresponda. Los datos mencionados corresponden a anotaciones del sistema, indicaciones para la auditoría informática que debe realizarse y más reportes de la situación presente del sistema y registros de los ficheros respectivos.

Los técnicos del Centro de Cómputo de la UCSG, se encargan del examen constante y convenientemente de los reportes correspondientes a eventos importantes para la protección de los datos y el equipamiento del laboratorio. Aquellos que utilizan las máquinas de esta dependencia tienen que saber cuáles acciones son consideradas infracciones a las normas de protección de los equipos y la red y que las mismas serán reportadas. Estos técnicos también tienen la responsabilidad de mantener actualizado el sistema operativo.

Anteriormente se indicó la importancia de los metadatos y la información que contienen, los mismos que pueden ser atacados y proporcionar datos importantes del sistema. Es importante saber los datos guardados en un archivo que se va a difundir o transmitir a otros usuarios, esto significa que para transferir un fichero debe conocerse su contenido para saber qué datos se están dando. En este proceso se aplican instrumentos apropiados para borrar los metadatos de los reportes creados. Nótese que de esta manera los reportes públicos en un portal de navegación no incluirán metadatos.

Una herramienta que ayuda en este proceso de protección es *Metashield Protector,* la cual posibilita estructurar directivas de protección de los metadatos de los documentos que se está enviando al exterior de la organización, brindando una solución completa para controlar la fuga de información. (Metashield)

3.7.11 Administración de los datos de protección del sistema

Periódicamente debe evaluarse la observancia de las normativas para proteger el sistema informático del laboratorio. Además los usuarios tienen que notificar de inmediato alguna novedad o transgresión que se produzca. De la misma manera todos los desperfectos en la programación del sistema deben comunicarse al administrador de la red.

Los datos correspondientes a las acciones de protección para los equipos del laboratorio deben ser secretos y no ser informados a quienes no tengan autorización.

3.7.12 Protección física del equipamiento del laboratorio

Todos los elementos de red deben ser protegidos contra posibles robos, utilizar controles para el ingreso físico, por ejemplo, los servidores LAN tienen que instalarse en gabinetes cerrados. El ingreso a la oficina del administrador de la red, a los armarios telefónicos de distribución, salas de cómputo y más zonas en que se manipulen datos importantes deben estar físicamente protegidas.

Únicamente el administrador de la red podrá en determinadas condiciones autorizar por escrito a ciertos usuarios utilizar sistemas que no estén acordes con estas normativas. En cambio, cualquier persona que transgreda estas reglas será sancionada disciplinariamente.

CONCLUSIONES

Durante la realización de este trabajo de investigación se realizó un estudio de los métodos que se utilizan para realizar ataques a la infraestructura de una red.

Con la información obtenida en el estudio referente a los métodos de análisis de debilidades de la red, se estableció los elementos de prevención y protección de errores de seguridad de la red, para recomendar como corregirlos.

Se realizó el análisis de las herramientas que brinda *Backtrack* para las pruebas de la red y la forma en que se debería aplicar en la red del laboratorio de Electrónica de la FET.

Con la información recabada se expusieron en cada capítulo recomendaciones para las correcciones de los errores que pueden presentarse.

En definitiva, se realizó un estudio para determinar la protección necesaria contra las debilidades de la infraestructura de red del Laboratorio de Electrónica de la Facultad de Educación Técnica de la Universidad Católica de Santiago de Guayaquil, con lo que se cumplió el objetivo general planteado.

RECOMENDACIONES

Como resultado de este trabajo, se recomienda ejecutar el análisis de fragilidades de acuerdo a la metodología detallada en el Laboratorio de Electrónica de la FET y en general en todos los laboratorios que incluyan computadoras en la UCSG para disminuir la posibilidad de que se produzcan agresiones a los sistemas de la universidad.

Designar un Administrador de la Red en la FET, el cual debe ser un profesional técnico con experiencia en protección de sistemas informáticos y que mantenga actualizados sus conocimientos para evitar el aprovechamiento de las debilidades que pueda presentar la red.

Es importante realizar la elaboración de un manual y los reglamentos y normativas necesarias, las cuales deben ser cumplidas por los usuarios del laboratorio y los directivos de la universidad deben exigir su cumplimiento, estas medidas permitirán reducir los peligros contra el sistema.

Es necesario utilizar métodos de localización de extraños al sistema para alertar acerca de los ataques que puedan producirse.

BIBLIOGRAFÍA

Agé, M., Baudru, S., Crocfer, N., Crocfer, R., Ebel, F., Hennecart, J., y otros. (2013). *Seguridad informática: conocer el ataque para una mejor defensa (Ethical hacking) Nueva edición.* ENI.

Aharoni, M., Coppola, W., Kearns, D., & otros. (2011). Tutorial de Metasploit Framework. *metasploid Unleashed Mastering the Framework*. Offensive-Securitty.

Anderson, N., & Doherty, J. (2006). *Redes locales (Manuales imprescindibles).* ANAYA MULTIMEDIA.

Anderson, N., & Doherty, J. (2009). *Introducción a las redes CISCO.* ANAYA MULTIMEDIA.

Anfinson, D. (2009). *Fundamentos de la tecnología de la información: hardware y software para PC.* PRENTICE-HALL.

Arboledas, D. (2013). *BACKTRACK 5.* RA-MA.

Barragan, A. (7 de mayo de 2012). *Topologías de red*. Recuperado el 30 de Julio de 2013, de uhu.es: http://uhu.es/antonio.barragan/content/5topologias

Black, U. (2010). *Redes (Manual imprescindible)* (2010 ed.). ANAYA MULTIMEDIA.

bsi. (s.f.). *Seguridad de la información ISO/IEC 27001*. Recuperado el 15 de Mayo de 2013, de http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001

Bucker, C. (28 de Septiembre de 2012). *Seguridad Informática.* Recuperado el 4 de Enero de 2014, de calebbucker.blogspot.com: http://calebbucker.blogspot.com/2012/09/information-gathering-mediante-el-uso.html

Bustamante, R. (s.f.). *Seguridad en redes.* Universidad Autónoma del Estado de Hidalgo.

Calles, J., & González, P. (2011). *La Biblia del Footprinting.* Recuperado el 5 de Enero de 2014, de Flu Project: la-biblia-del-footprinting.googlecode.com/.

Castaño, M. (2012). *Planificación y Administración de Redes*. Recuperado el 20 de Octubre de 2013, de Suarez de Figueroa A.S.I.R.: http://www.suarezdefigueroa.es/manuel/PAR/index.php

Castro, L. (8 de Octubre de 2012). *Topologías de las redes*. Recuperado el 30 de Julio de 2013, de Prezi: http://prezi.com/ppgfyt22yelv/copy-of-topologias-de-las-redes/

Certificación. (s.f.). Recuperado el 15 de Mayo de 20013, de http://www.iso27001certificates.com

Cuevas, R. (s.f.). *CONSULTORÍA INTEGRAL DE TIC'S*. Recuperado el 1 de Diciembre de 2013, de itescam.edu.mx: www.itescam.edu.mx/principal/sylabus/fpdb/recursos/r85351.PDF

Dhanjani, N. (2010). *La nueva generación Hacker* . ANAYA MULTIMEDIA.

EthicalHacking. (s.f.). *Metagoofil Backtrack 5 Tutorial-Metadata Analyzer Information Gathering Tool.* Recuperado el 4 de Enero de 2014, de www.ehacking.net: http://www.ehacking.net/2011/12/metagoofil-backtrack-5-tutorial.html

Gallego, A. (2009). *Routers CISCO: Edición revisada y actualizada 2010 (Guia practica).* ANAYA MULTIMEDIA.

Gómez, A. (2011). *Auditoria de seguridad informática.* STARBOOK EDITORIAL.

Gómez, A. (2011). *Gestión de incidentes de seguridad informática.* STARBOOK EDITORIAL.

Gómez, A. (2011). *Seguridad en equipos informáticos MF0486-3 Certificado de profesionalidad.* STARBOOK EDITORIAL.

Gómez, J. (2010). *Guía de campo hackers: aprende a atacar y a defenderte.* RA-MA.

Gonzalez, R. (s.f.). *Redes de area amplia - WANs.* Corrientes - Argentina: Universidad Nacional del Nordeste.

GrayHathacking. (12 de Octubre de 2012). *How To Use MetaGooFil.* Recuperado el 4 de Enero de 2014, de GrayHat Hacking Security Exploits : http://grayhathacking.blogspot.com/2012/10/how-to-use-metagoofil.html

HackingDNA. (2013). *TCPtracerroute.* Recuperado el 5 de Enero de 2014, de Hacking DNA: http://hackingdna.com/Description.aspx?ItemHeaderId=08290C53-3E45-446C-8167-C9BFD587068D#.UvvxrWJ5Orh

Harrington, J. (2006). *Manual práctico de seguridad de redes (Hardware y redes)* . ANAYA MULTIMEDIA.

ISO/IEC. (s.f.). *Comparación entre la ISO/IEC 27001 y la ISO/IEC 9001*. Recuperado el 20 de Mayo de 2013, de www.iso27000.es: http://www.iso27000.es/download/9001similaties_sp

ISO/IEC. (s.f.). *www.iso27000.es.*

Jerez, C. (6 de Mayo de 2004). *Seguridad para lograr Confiabilidad y Calidad de los Servicios Digitales en Internet*. Recuperado el 9 de Diciembre de 2013, de Colección de Tesis Digitales Universidad de Puebla: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/

Jimeno, M., Miguez, C., & Matas, A. (2010). *Hacker (Guía Práctica)* (2010 ed.). ANAYA MULTIMEDIA.

Kathayat, V. (22 de Mayo de 2013). *Harvester on Backtrack 5.* Recuperado el 4 de Enero de 2014, de Hacking DNA: http://www.hackingdna.com/Description.aspx?ItemHeaderId=13E442A1-C3D6-46FF-96A1-F6D86DFF1E69#.Uvv97oe9KK0

Katz, M. (2013). *Redes y seguridad.* Marcombo S.A.

Kernighan, B., & Pike, R. (1984). *The UNIX programming environment.* Prentice Hall.

Linux. (s.f.). *ARP Spoofing y Poisoning*. Recuperado el 6 de Enero de 2014, de www.linux-magazine.es: https://www.linux-magazine.es/issue/09/ARPSpoofing.pdf

Lockhart, A. (2007). *Seguridad de redes: los mejores trucos (O REILLY).* ANAYA MULTIMEDIA.

Malagón, C. (s.f.). *Hacking Ético.* Recuperado el 14 de Diciembre de 2013, de Universidad de Nebrija: http://www.nebrija.es/~cmalagon/seguridad_informatica/transparencias/Modulo_2.pdf

Mcmahon, R. (2003). *Introducción a las redes.* ANAYA MULTIMEDIA.

Mcmahon, R. (2003). *Introducción a las redes.* ANAYA MULTIMEDIA.

Mcnab, C. (2008). *Seguridad de redes.* ANAYA MULTIMEDIA.

Metashield. (s.f.). *Metashield*. Recuperado el 6 de Enero de 2014, de www.metashieldprotector.com/: https://www.elevenpaths.com/services/metashield.html

Meyers, M. (2003). *Redes: administración y mantenimiento.* ANAYA MULTIMEDIA.

Meyers, M. (2005). *Redes: gestión y soluciones.* ANAYA MULTIMEDIA.

Mujica, M. (15 de Junio de 2005). *Estándares Internacionales ISO/IEC 17799*. Recuperado el 8 de Diciembre de 2013, de mmujica.files.wordpress.com: http://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

Plasencia, Z. (2010). *Introducción a la informatica (Guía practica)* (2010 ed.).

Plasencia, Z. (2013). *Introducción a la informática* (2013 ed.). ANAYA MULTIMEDIA.

Rabago, J. (2010). *Guía práctica ANAYA MULTIMEDIA: Redes locales* (2010 ed.). ANAYA MULTIMEDIA.

Sánchez, A., & Hinojosa, G. (2009). *Análisis, diseño e implementación de una red LAN por medios guiados y no guiados en el Colegio Técnico Semi-presencial Intercultural Bilingüe Rumiloma.* Guaranda-Ecuador: Universidad Estatal de Bolívar.

Silberschatz, A., & Peterson, J. (1994). *Operating system concepts.* Addison-Wesley.

slideshare. (25 de mayo de 2012). *Uso de MFSconsole*. Recuperado el 4 de Enero de 2014, de slideshare: http://www.slideshare.net/dirxxxeu/msfconsole-explotar-a-windows-sp2

Stallings, W. (2003). *Fundamentos de seguridad en redes: aplicaciones y estándares.* Pearson Educación.

Stallings, W. (2007). *Network security essentials: applications and standards.* Prentice Hall.

Stallings, W. (2009). *Operating systems: internals and design principles, 6/E. .* Pearson Educación.

Tomasi, W. (2003). *Sistemas de Comunicaciones Electrónicas.* Mexico: Prentice Hall.

UNAM. (s.f.). *Seguridad Informática*. Recuperado el 4 de Enero de 2014, de Universidad Nacional Autónoma de México: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/index.php

www.iso27000.es. (s.f.). *Modos de análisis de riesgos*. Recuperado el 26 de Mayo de 2013, de http://www.iso27000.es/doc_herramientas_all.htm#riesgos