UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERO/A EN SISTEMAS INFORMÁTICOS

TEMA: ANALISIS DE VULNERABILIDADES PARA LA RED LAN DE LA EMPRESA “HIDROMAG”, BAJO LA METODOLOGIA “OSSTMM”.

AUTOR/ A: ANDRES EDUARDO NARVAEZ NARVAEZ

TUTOR/ A: Mg. CHRISTIAN VACA BENALCAZAR

QUITO- ECUADOR

AÑO: 2019

DECLARACIÓN DE AUTORÍA

El documento de tesis con título: ANALISIS DE VULNERABILIDADES PARA LA RED LAN DE LA EMPRESA “HIDROMAG”, BAJO LA METODOLOGIA “OSSTMM”, ha sido desarrollado por el señor Andrés Eduardo Narváez Narváez con C.C. No. 04012484144 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de la información de esta tesis sin previa autorización.

_____

Andrés Eduardo Narváez Narváez

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación certifico:

Que el trabajo de titulación "**ANALISIS DE VULNERABILIDADES PARA LA RED LAN DE LA EMPRESA HIDROMAG, BAJO LA METODOLOGIA OSSTMM**", presentado por Andrés Eduardo Narváez Narváez, estudiante de la Carrera Ingeniería en Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito D. M., 15 de Febrero 2019.

TUTOR

Mg. Christian Vaca Benalcázar

DEDICATORIA

Dedico este trabajo principalmente a Dios por darme la fuerza y la vida para poder alcanzar mis metas.

A mis Padres Jesús y Elsa, por su incondicional ejemplo, amor y apoyo en los momentos más decisivos de mi vida, me han permitido céntrame y lograr los objetivos propuestos.

A mis Hermanos, por brindarme todo el apoyo en este camino del estudio que me propuse, espero que le tomen como ejemplo.

Finalmente quiero agradecer a la Universidad Tecnológica Israel que me permitió continuar con mis estudios, a todos sus Ingenieros y en especial a mi tutor de tesis quien me brindo su guía para poder terminar este trabajo.

TABLA DE CONTENIDOS

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

Mediante el análisis de vulnerabilidades basado en la metodología “OSSTMM”, el presente trabajo pretende solucionar y mitigar las vulnerabilidades y brechas de seguridad que se presenten dentro de la red LAN de la Empresa “HIDROMAG. El análisis va enfocado o dirigido a una empresa mediana, la cual necesita identificar los posibles fallos de seguridad que presente la RED LAN, con la metodología propuesta “OSSTMM” (Manual de la Metodología Abierta de Testeo de Seguridad), se busca establecer un estándar de referencia para realizar el testeo de seguridad que incluya la mejores prácticas y lineamientos para realizar este tipo de análisis. Como resultado de este estudio, se desarrolló un plan de acción con estrategias de protección preventiva, correctiva y correctiva para mitigar el impacto de los riesgos. La metodología OSSTMM, adaptada al entorno empresarial, así como un conjunto de reglas de seguridad de la información para el usuario final con estándares mínimos que deben considerarse para preservar las características de seguridad de la información definida por confidencialidad, integridad y disponibilidad.

Palabras claves: vulnerabilidad, metodología OSSTMM, seguridad informática, Red LAN, brechas de seguridad, estrategias correctivas

ABSTRACT

Through the analysis of vulnerabilities based on the "OSSTMM" methodology, this work aims to solve and mitigate vulnerabilities and security gaps that arise within the LAN network of the Company "HIDROMAG. The analysis is focused or directed to a medium-sized company, which needs to identify the possible security failures presented by the LAN NETWORK, with the proposed methodology "OSSTMM" (Manual of the Open Methodology of Security Testing), it seeks to establish a standard of reference to perform safety testing that includes the best practices and guidelines for performing this type of analysis. As a result of this study, an action plan was developed with preventive, corrective and corrective protection strategies to mitigate the impact of the risks. The OSSTMM methodology, adapted to the university environment, as well as a set of information security rules for the end user with minimum standards that must be considered to preserve the security features of the information defined by confidentiality, integrity and availability.

Keywords: vulnerability, OSSTMM methodology, computer security, LAN network, security breaches, corrective strategies

INTRODUCCIÓN

En los últimos años la tecnología, las redes informáticas y en especial el internet han tenido un crecimiento importante, en especial el uso del internet para las empresas se ha convertido en un aliado para ejercer sus actividades que les permita beneficios mediante la presentación o producción de productos y servicios, precisamente por este medio es por donde se presenta el peligro para las empresas puesto que pueden realizar actividades como compras, ventas, pagos, depósitos, transferencias, consultas, etc.

Estas acciones resultan críticas para cualquier empresa ya que dichas actividades pueden ser vulneradas por personas no autorizadas, los llamados Hackers, provocando robos de información y datos importantes para las empresas, muchas veces causando daños irreparables.

Por este y muchos motivos es preciso realizar un análisis de vulnerabilidades o hacking ético que permita realizar una serie de pruebas acordadas con el cliente con el fin de encontrar brechas o fallos de seguridad que pueda afectar el desempeño y producción de la empresa. Gracias a este tipo de análisis permitirá tener un panorama del estado actual de la Red LAN a nivel de seguridades lo cual permitirá proteger la información crítica y sensible del cliente.

ANTECEDENTES DE LA SITUACION

La Empresa Hidromag, es una entidad privada dedicada a la venta y mantenimiento de equipos hidráulicos, ubicada en la ciudad de Quito, que inicio sus de actividades en el año 2009 con la firme misión de realizar trabajos de mantenimiento de equipos hidráulicos y ofreciendo repuestos de buena calidad con el mejor servicio hacia el cliente. En la actualidad el internet y las tecnologías de la información tienen un gran crecimiento, de ahí la importancia de protegerse de los ataques de hackers que ponen en peligro la estabilidad de la empresa con el robo de información, la misma que puede afectar la confiabilidad de los clientes.

La Red LAN de la Empresa Hidromag, también ha incrementado en su infraestructura física y lógica en los últimos años. Con este crecimiento de las Tecnologías de la Información, también ha aumentado las brechas y amenazas de

seguridad que afectan o ponen en riesgo la información que maneja una organización sin importar su tamaño, giro de negocio ni ubicación física.

Desde que los usuarios finales acceden al uso de la Red Interna corren el riesgo de ser vulnerados por ataques de hackers o personas que quieren obtener información, muchas veces los usuarios son víctimas de estos ataques sin darse cuenta de ello, como resultado exponen tanto la seguridad de sí mismos como la de la empresa.

Con el fin de incrementar la seguridad de información y de la infraestructura TI de la empresa Hidromag es necesario realizar un análisis de vulnerabilidades, para poder identificar las brechas de seguridad a las que se encuentra expuesta, tanto al exterior como al interior de la red de la organización.

La utilización de la metodología OSSTMM y del conjunto de herramientas libres recomendadas para cada una de las pruebas de evaluación, permite realizar una identificación completa de las vulnerabilidades y una evaluación de los riesgos a medida que se realizan las pruebas.

Con este análisis la empresa tendrá visibilidad sobre las vulnerabilidades encontradas en su infraestructura TI y en sus sistemas, lo cual es imprescindible el momento de aplicar medidas correctivas.

Planteamiento del problema

La evolución de las redes y las tecnologías de la información en la actualidad ha permitido incrementar el tamaño y el flujo de la información, permitiendo con ello agilizar flujos y procesos, pero esto trae consigo nuevas amenazas y vulnerabilidades.

Hoy en día es necesario contar con una red segura para garantizar la productividad y seguridad de la información que maneja la empresa.

Actualmente la Empresa “Hidromag” cuenta con una red LAN que necesita un rediseño, debido que presenta muchas falencias especialmente en el diseño y en la segmentación de red, lo cual puede permitir fuga y perdida de información así como también amenazas en sus sistemas. La empresa actualmente se encuentra en la búsqueda

de herramientas o mecanismos que le permita minimizar estos riesgos y vulnerabilidades como políticas de seguridad, respaldos, planes de contingencia, esquemas de seguridad perimetral, servicios de seguridad, etc.

JUSTIFICACIÓN

Hoy en día la información es un factor primordial dentro de los sistemas, las organizaciones buscan tener mayor seguridad en sus esquemas infraestructura de tecnologías de la información, con esto se ve reflejado en una buena imagen y reputación corporativa, inclusive evita tener pérdidas económicas, así como también la privacidad, integridad y confidencialidad.

El presente proyecto de investigación tiene como alcance realizar un análisis de vulnerabilidades de acuerdo a uno de los aspectos o criterios que menciona la metodología OSSTMM (Manual de Metodología Abierta de Testeo de Seguridad), con la finalidad de determinar las brechas de seguridad a la cual está expuesta la infraestructura TI y establecer recomendaciones.

OBJETIVOS

OBJETIVO GENERAL

Analizar las vulnerabilidades que pueda descubrir en la infraestructura TI de la Empresa Hidromag mediante un pentesting utilizando la metodología OSSTMM (Manual de Metodología Abierta de Testeo de Seguridad), estableciendo recomendaciones para el mejoramiento de seguridad TI de la organización.

OBJETIVOS ESPECÍFICOS

- Contextualizar la fundamentación teórica sobre el Pentesting enfocado al tipo de empresa.
- Identificar la información relevante en la red de la empresa Hidromag, implementando herramientas de software libre.

- Valorar las debilidades identificadas y clasificarlas según el CVE (Vulnerabilidades y exposiciones comunes), para su presentación en informe.
- Establecer recomendaciones sobre procedimientos de Control, Políticas y estándares que permitan a la empresa HIDROMAG la administración y protección de la información.

Descripción de los capítulos

En el capítulo 1 abarca la fundamentación teórica, en la que se realiza una descripción breve de buenas prácticas, así como se hace referencia a otras investigaciones que permitieron sustentar el desarrollo de esta investigación.

En el Capítulo 2 se realizó una descripción del tipo de investigación a utilizar así como de los métodos de recopilación de información que aplique en el análisis de vulnerabilidades.

En el Capítulo 3 se presentara la propuesta para el desarrollo del Pentesting utilizando la metodología OSSTMM en la red LAN de la Empresa Hidromag.

En el Capítulo 4 se presentan las conclusiones y recomendaciones arribadas después de la presentación de los resultados derivados de la investigación.

CAPÍTULO I. FUNDAMENTACIÓN TEÓRICA

1.1 Estado del Arte

1.1.1 Información (datos)

La información es un recurso muy importante para una institución u organización y, por lo tanto, debe estar debidamente protegida. Considerando que un recurso es valioso para una empresa, la información existe en diferentes formas: impresión, escritura en papel, archivo en formato electrónico, envío por correo, uso de medios electrónicos, proyección de película, entre otras (Hadnagy, 2017).

Por lo tanto sea cual sea la forma de la información o los medios por los cuales se almacena o transmite, siempre debe estar adecuadamente protegida.

1.1.2 Seguridad de la Información

Estas son medidas para evitar acciones no autorizadas que de alguna manera afecten a los principios de la seguridad de la información (confidencialidad, autenticidad, integridad), al tiempo que garantizan el correcto funcionamiento del equipo y su accesibilidad para los usuarios legítimos (Pacheco, 2016).

> "Siempre tenga en cuenta que la seguridad comienza y termina con las personas, por lo que requiere tiempo, dinero y esfuerzo para obtenerla. Algunas organizaciones creen que su información no es vulnerable ni interesante para los atacantes. No están buscando vulnerabilidades" (Pacheco, 2016, pág. 59).

De lo expuesto por el autor se deduce que la seguridad es inherente a las personas de ahí la importancia de su planificación y desarrollo constante de tal manera que la información confidencial sea asegurada y por ende el éxito de la empresa.

De acuerdo con la norma ISO 17799, define la seguridad de la información como el mantenimiento de la confidencialidad, integridad y disponibilidad; Además, otras

propiedades como la autenticidad, la responsabilidad, la no devolución y la confidencialidad también pueden estar involucradas (Navratilova, 2016).

a. Importancia

La seguridad de la información es la protección de la información contra una amplia gama de amenazas para garantizar la continuidad del negocio, minimizar el riesgo y maximizar el retorno de la inversión y las oportunidades de negocio.

Esto se logra mediante la introducción de un conjunto apropiado de controles; incluyendo políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles deben establecerse, implementarse, monitorearse, analizarse y mejorarse, según sea necesario, para garantizar el logro de objetivos de seguridad específicos y objetivos comerciales, esto debe hacerse en combinación con otros procesos de gestión empresarial (Ortiz & Villegas, 2014).

La seguridad de la información se puede lograr mediante el uso de un conjunto adecuado de herramientas de administración; incluyendo políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware. Es necesario instalar, implementar, monitorear, analizar y mejorar estos controles tan a menudo como sea necesario para garantizar el logro de los objetivos de seguridad.

La seguridad informática recientemente se ha vuelto muy importante, especialmente para las organizaciones públicas y privadas. Esta situación se debe al hecho de que todos los días este problema merece una atención especial. Esto debería permitir a una organización alcanzar nuevos objetivos para lograr un rendimiento óptimo basado en las condiciones adecuadas de su infraestructura de TI, lo que es vital para las instituciones en este momento (Alonso, 2016).

La interconexión entre redes públicas y privadas y el intercambio de fuentes de información complican el control de acceso. La tendencia hacia la computación distribuida también ha debilitado la eficiencia de la administración centralizada y especializada. Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que puede obtenerse por medios técnicos es limitada y debe estar respaldada

por una administración y procedimientos adecuados que determinen los controles utilizados y el tipo de planificación que se utilizará sin descuidar los detalles (Reza, 2016).

En el campo de la seguridad, se examinaron tres aspectos importantes:

- **Confidencialidad:** Es el servicio de privacidad que garantiza que los procesos no autorizados no puedan acceder ni detectar información.
- **Disponibilidad:** Un sistema seguro debe proporcionar continuamente información, equipos y software a los usuarios.
- **Integridad:** Una condición de seguridad que garantiza que la información sea creada, modificada y eliminada solo por personal autorizado.

Por lo tanto, el propósito de la seguridad es: preservar cada una de las características mencionadas inicialmente, como se menciona en la figura 1.1.

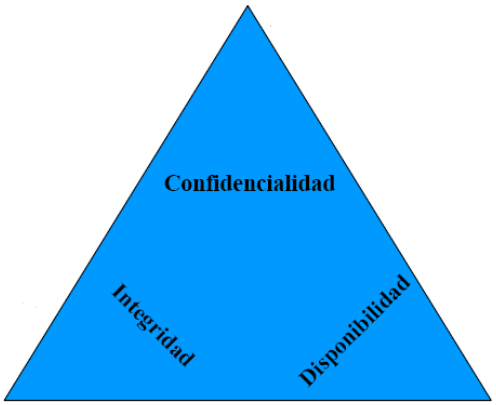

Figura 1.1 Pirámide de los servicios de seguridad
Fuente: (Chappell & Combs, 2016)

b. Tres leyes de la seguridad

Existen tres leyes de seguridad:

- No existen sistemas absolutamente seguros.
- Para reducir su vulnerabilidad a la mitad, necesita duplicar sus costos de seguridad.
- En general, los hackers ignoran la criptografía, no la violan (Navratilova, 2016).

1.1.3 Seguridad Física

Este aspecto no se tiene en cuenta en el desarrollo de un diagrama de red, pero es un punto muy importante porque permite el uso de barreras físicas y procedimientos de control, como medidas para prevenir y contrarrestar las amenazas a los recursos e información confidenciales, es decir. Introducción de mecanismos de control de acceso físico u otros componentes de conservación de los sistemas físicos de la organización (Zeltser, 2014).

Las amenazas pueden ser:

- Eventos accidentales o significativos (terremotos, inundaciones, tormentas, etc.).
- Diseñado para humanos (robo, destrucción, incendio, etc.).

1.1.4 Seguridad Lógica.

Según Kennedy (2015) indica que consiste en aplicar barreras y / o procedimientos que protegen el acceso a los datos, y solo aquellos autorizados para hacerlo tienen acceso a ellos. Se pueden ver numerosos controles de seguridad lógicos en la tesis Seguridad informática: implicaciones e implementación, pero se han tenido en cuenta los siguientes aspectos:

- **Roles:** Esto se hace verificando a través de una función o rol de usuario que requiere tal acceso.
- **Control de acceso:** Consisten en implementar controles en cualquier utilidad de red para preservar la integridad de la información y proteger los datos confidenciales del acceso no autorizado.
- **Autentificación, identificación:** La identificación es cuando el usuario se refiere al sistema y la autenticación se refiere a la verificación que el sistema realiza para esa identificación.
- **Listas de control de acceso ACL:** Su propósito es filtrar el tráfico, permitir o prohibir el tráfico de red de acuerdo con las diversas condiciones establecidas en el equipo de la red.

- **Restricciones a los servicios:** Estos controles están vinculados a restricciones que dependen de la configuración específica del uso de la aplicación o predefinida por el administrador (Kennedy, 2015).

1.2 Amenazas de la seguridad de la información

De acuerdo con Pacheco (2016) las amenazas se dividen en cuatro categorías:

Tabla 1.1 Categorías de las amenazas de seguridad de la información

Categoría	Descripción
Interrupción.	Disponibilidad de una parte o total del sistema.
Intercepción.	Confidencialidad.
Modificación.	Ataque contra la integridad.
Fabricación.	Autenticidad.

Fuente: (Pacheco, 2016)

1.2.1 Ataques informáticos

De acuerdo con Aguilera (2016) los ataques se clasifican en:

- **Ataques pasivos:** Estos ataques se basan en escuchar los datos transmitidos y no en su modificación.
- **Ataques activos:** A diferencia de los ataques pasivos, alteran o alteran la información que ha sido interceptada para causar daño (Aguilera, 2016).

La siguiente es una lista de algunos ataques informáticos que pueden ser causados por personas internas o externas.

- Actividad de reconocimiento de activos.
- Detección de vulnerabilidad en sistemas. Información de vuelo.
- Modificación del contenido y la secuencia de los mensajes transmitidos.
- Análisis de tráfico.
- Ataque de imitación Conexiones no autorizadas.
- La introducción del código malicioso.
- Denegación de servicio (Aguilera, 2016).

Según un estudio realizado por CYBSEC, parece que el 80% de los ataques son internos y el 20% externos. Como se muestra la figura 1.2 (Perramón, 2015).

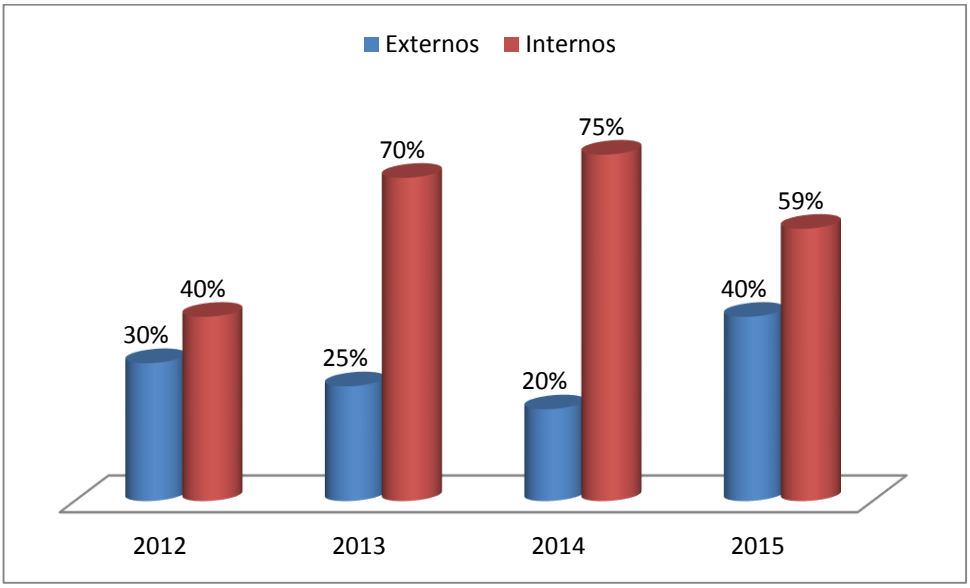

Figura 1.2 Porcentaje de los ataques internos y externos 2012 - 2015
Fuente: (CYBSEC, 2016)

Según ESET en su informe anual 2015 los principales problemas de seguridad se detallan en la figura 1.3.

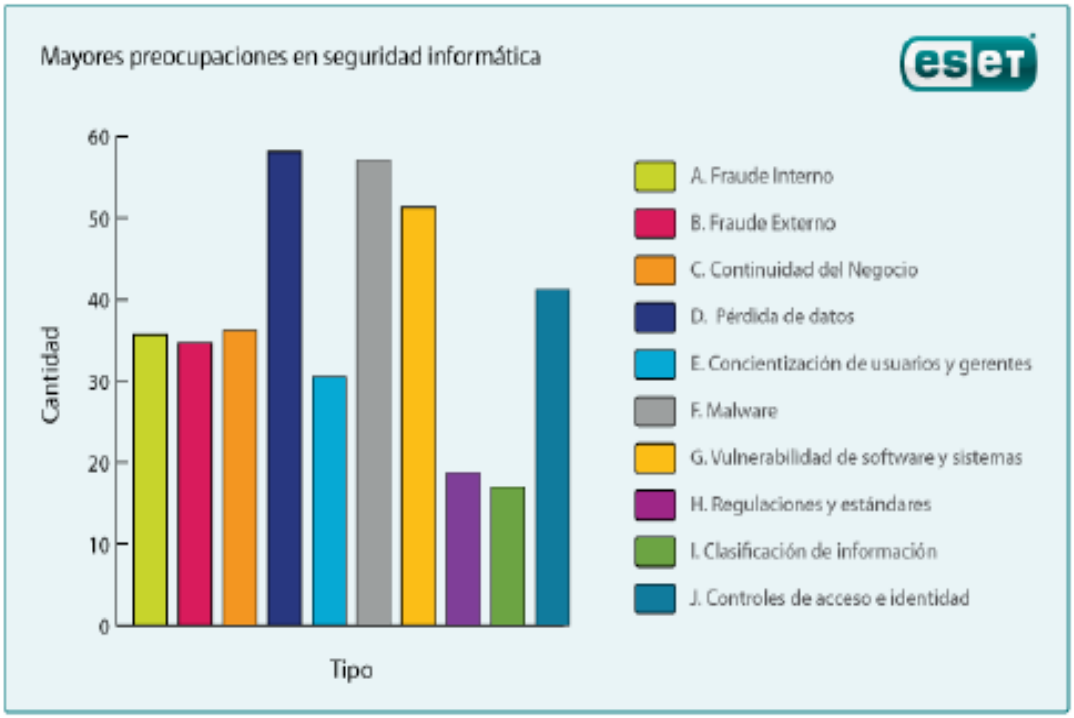

Figura 1.3 Mayores preocupaciones en Seguridad Informática.
Fuente: (ESET, 2016)

Este informe identifica los riesgos más comunes. Asimismo, los servicios internos y externos presentan riesgos comunes, tales como:

- Intercepción de mensajes.
- Suplantación de la personalidad.
- Interrupción de actividades de servicio. Información de vuelo.
- La introducción del código malicioso.
- Cambio de información

Para comprometer la seguridad de cualquier sistema, un atacante debe conocer 4 pasos para realizar una prueba de intrusión, tal como se observa en la figura 1.4.

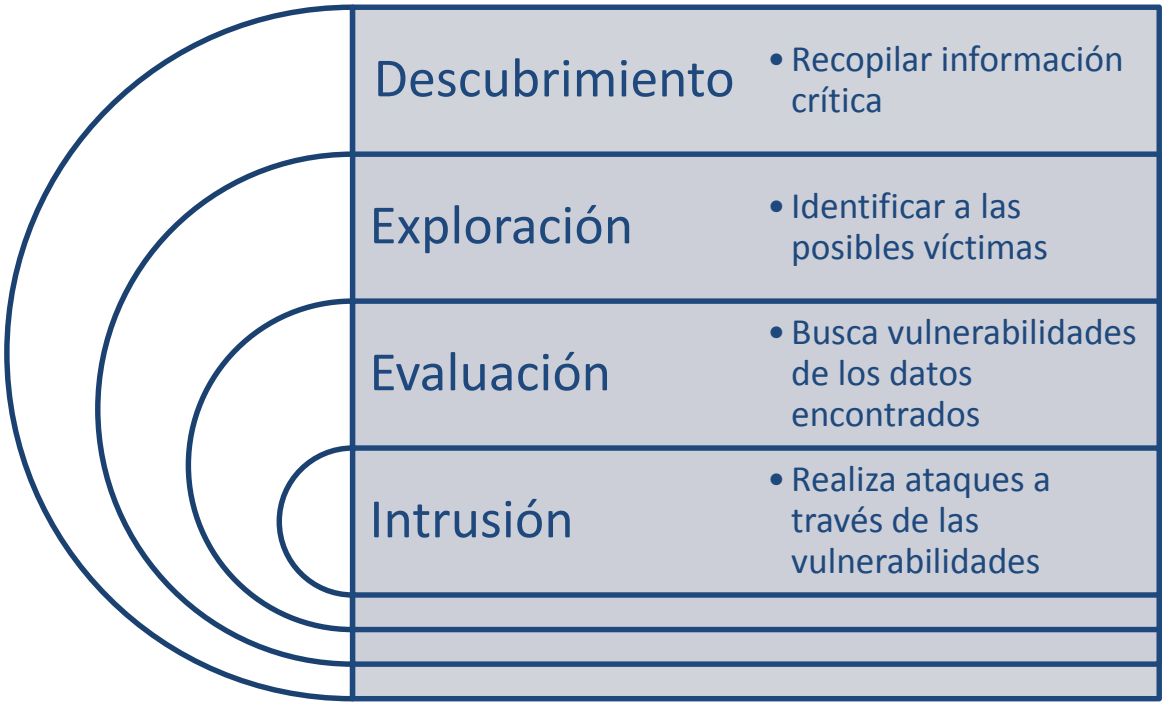

Figura 1.4 Etapas o Fases de un Test de Penetración
Fuente: (Hadnagy, 2017)

Sin embargo, conociendo los pasos, forman un triángulo de invasión, el intruso que realiza la prueba de intrusión conoce, entre otras cosas, las herramientas, los mecanismos y también las habilidades y la razón que llevaron a la realización de esta prueba de intrusión, como se indica en la figura 1.5 (Chappell & Combs, 2016).

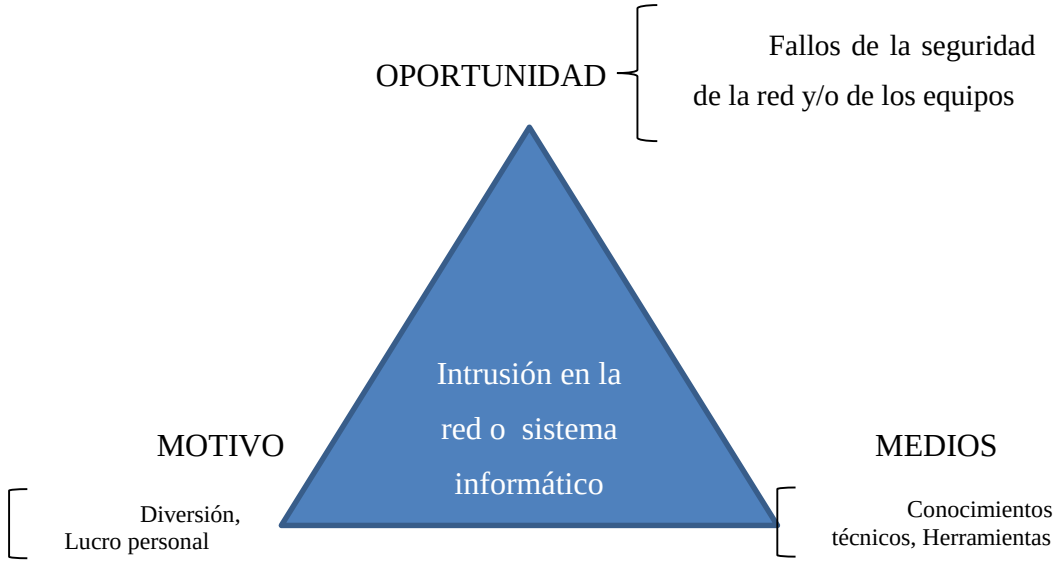

Figura 1.5 Triángulo de la intrusión
Fuente: (Chappell & Combs, 2016).

También es importante conocer los métodos de hackeo ético que se pueden aplicar de acuerdo con los requisitos de la organización.

- Ataque local.
- Ataque con material robado.
- Atacar los registros físicos de la organización.
- Ataque por ordenador sin autenticación.
- Los ataques de la ingeniería social.

En el caso de este proyecto, se ha tenido en cuenta el modo de ataque local, ya que simulará un ataque por parte del personal interno que tiene acceso a la red de la empresa, por ejemplo, por personal administrativo, contable, operativo, entre otros (Kennedy, 2015).

1.3 Seguridad en la Red LAN.

Los requisitos mínimos generales de seguridad que debe poseer una red LAN (Ortiz & Villegas, 2014) se detallan en la tabla 1.2:

Tabla 1.2 Requisitos generales para asegurar la red LAN

Necesidades	Beneficios
Conocer al detalle las aplicaciones de la red y capacidad para controlarlas.	Reducción en las inversiones en ancho de banda. Mejora del rendimiento de la red.
	Ahorre de costos.
	Disminución de problemas.
Firewall de aplicación.	Definición de políticas de control y bloqueo a nivel de aplicación, usuario, servicio, etc.
	Contar con historiales para el seguimiento de incidencias.
Sistema central de informes.	Poder escalar a los superiores el conocimiento detallado de la red para toma de decisiones.
Control de flujos no deseados	Detección y control de ataques de spam, DoS, troyanos
	Conocer que usuarios generan dichos flujos.
Mejorar el rendimiento.	Controlar el tráfico.
Sistema de alertas.	Saber lo que pasa en la red en el momento oportuno.

Fuente: (Ortiz & Villegas, 2014)
Elaborado por: Andrés Narváez

Por lo tanto, la presencia de una red local sin medidas de seguridad adecuadas es peligrosa, pero estos requisitos mínimos generales de seguridad se han mencionado para combatir la inseguridad. Una LAN inalámbrica no es una red que no sea una red cableada, sino que debe considerarse una estrategia de seguridad igual o unificada.

1.3.1 Seguridad en las capas de la pila TCP/IP

Existen cuatro niveles o capas de la pila de protocolos TCP / IP y algunas características de seguridad aplicables a cada uno (Hadnagy, 2017).

Tabla 1.3 Seguridad en las capas de la pila de protocolos TCP/IP

Capa	Protocolos
Aplicación.	HTTPS, SSH.
Transporte.	TCP, UDP sobre SSL o TLS.
Red.	IPv4, IPv6, IPSEC.
Física + Enlace.	L2TP, Ethernet, PPTP.

Fuente: (Hadnagy, 2017)

1.4 Vulnerabilidades en las redes informáticas

1.4.1 Causas de las vulnerabilidades

A continuación se enumeran las diferentes causas de vulnerabilidad descritas en el informe de ESET (Reza, 2016):

- Debilidad en el diseño de protocolos utilizados en redes.
- Errores de programación.
- Configuración inadecuada de los sistemas informáticos.
- Política de seguridad incorrecta o inexistente.
- La ignorancia de las herramientas que facilitan los ataques.
- La presencia de las puertas traseras.
- Restricción del gobierno.

Por estas razones, han aparecido los siguientes tipos de vulnerabilidades.

- Vulnerabilidades que afectan a las computadoras.
- Vulnerabilidades que afectan a software y aplicaciones (Reza, 2016).

a. El Factor humano

Según el autor Alonso (2016), de ISEC, afirma que la seguridad depende principalmente del factor humano, no del factor tecnológico. Mientras que (Reza, 2016) define como el usuario es el enlace más débil para evitar el fraude y garantizar la seguridad de la computadora en cualquier organización (Alonso, 2016).

De igual manera Ortiz & Villegas (2014), especialista en seguridad de IBM Colombia, gran parte del robo relacionado con transacciones virtuales y acciones irregulares relacionadas con la seguridad informática son el resultado de la negligencia de quienes tienen el derecho de acceso, tareas fundamentales dentro de la empresa (Ortiz & Villegas, 2014).

Para Kennedy (2015), gerente de marketing de Symantec para América Latina, el problema está claro: en el país, las aplicaciones y los métodos de seguridad de TI que evitan las transacciones fraudulentas solo se propagarán cuando el valor real (costo-beneficio) esté protegido. Esencial para las empresas (Kennedy, 2015).

Se estima que los mismos empleados producen el 82% de los datos confidenciales de la compañía. Por lo tanto, con todas estas afirmaciones, se puede decir que el usuario final es el eslabón más débil de la cadena de TI, debido a la ignorancia, la falta de cultura de seguridad o la falta de conciencia.

1.5.Herramientas para la evaluación de vulnerabilidades y riesgos.

1.5.1 Metodologías de test de penetración

De la investigación realizada se han considerado las siguientes metodologías que se podrían utilizar para el desarrollo práctico de la tesis los test de penetración son:

- OSSTMM
- ISSAF
- OTP

Tabla 1.4 Metodologías de test de penetración

Aspectos Destacados	OSSTMM	ISSAF	OTP
	Seguridad de la Información Seguridad de los Procesos Seguridad en las Tecnologías de Internet Seguridad en las Comunicaciones Seguridad Inalámbrica Seguridad Física	Una descripción del criterio de evaluación. Puntos y objetivos a cubrir. Los prerrequisitos para conducir la evaluación. El proceso mismo de evaluación. El informe de los resultados esperados. Las contramedidas y recomendaciones. Referencias y Documentación Externa.	El alcance de que testear. Principios del testeo. Explicación de las técnicas de testeo. Explicación general acerca del framework de testeo de OWASP.

Fuente: (Hadnagy, 2017).

a. OSSTMM (Manual de la metodología abierta de testeo de seguridad)

Es una metodología para realizar una prueba de penetración que evalúa la seguridad cuantificando el nivel de riesgo y también describe los pasos a seguir antes, durante y después de la prueba de penetración (Chappell & Combs, 2016).

De conformidad con la norma ISO12 17999-BS7799, este es un conjunto de reglas que indican el cómo y por qué de la prueba. Esta metodología se divide en seis secciones, cada una de las cuales incluye un conjunto de módulos.

Las secciones son:

- Seguridad física.
- Seguridad en las comunicaciones.
- Seguridad inalámbrica.
- Seguridad en tecnología de la información.

La figura 1.6, muestra el Mapa de Seguridad de la Metodología OSSTMM.

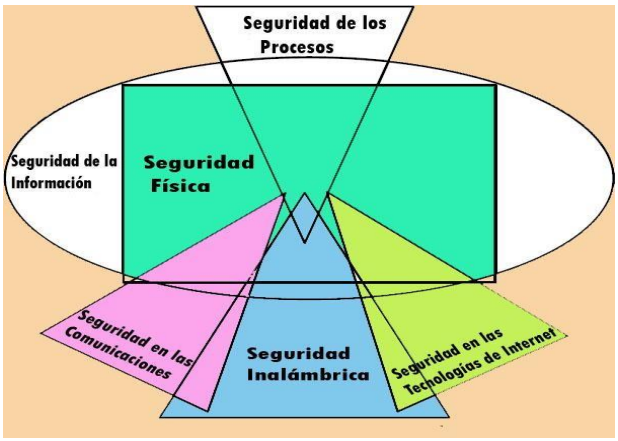

Figura 1.6 Mapa de seguridad de la Metodología OSSTMM
Fuente: (Chappell & Combs, 2016)

Sólo las secciones mencionadas anteriormente han sido pintadas. Estas cuatro secciones fueron elegidas porque corresponden a las identificadas para la investigación, tales como: prueba de red inalámbrica, voz / IP, red cableada, seguridad de contraseña y prueba de seguridad física.

En el anexo A, se describe de forma más amplia los componentes de la Metodología OSSTMM.

b. ISSAF (Information systems security assessment framework)

Según la Navratilova, (2016) proporciona una estructura detallada relacionada con las prácticas y los conceptos asociados con cada una de las actividades a realizar durante la prueba de seguridad. La información contenida en el ISSAF está organizada en torno a los criterios de evaluación (Navratilova, 2016).

Estos criterios de evaluación incluyen los siguientes elementos:

- Descripción de los criterios de evaluación.
- Puntos y objetivos a cubrir.
- Prerrequisitos para la evaluación.
- El proceso de evaluación en sí.
- Reportar los resultados esperados.
- Contramedidas y recomendaciones.

Esta metodología requiere que la estructura se actualice constantemente, por lo que sus partes no están obsoletas, pero no es una desventaja, sino un punto a tener en cuenta.

c. OTP (OWASP Testing Project)

Este es un proyecto de aplicación web dividido en dos partes. La primera parte incluye los siguientes puntos:

- Principios de prueba.
- Explicación de los métodos de ensayo.
- Explicación general de la estructura del test OWASP.

En la segunda parte, se planifican todos los métodos de prueba asociados con el ciclo de desarrollo del software, de modo que la prueba se inicie antes de que la aplicación comience la producción (Navratilova, 2016).

Artículos incluidos para la prueba:

- Personas.
- Proceso
- Tecnología.

Paso 1	**Antes del desarrollo**
	a. Visión general de las políticas y normas. b. Desarrollo de criterios de medición y métricas.
Paso 2	**Durante la definición y diseño**
	a. Revisión de los requisitos de seguridad. b. Panorámica arquitectónica del proyecto. c. Creación y revisión de modelos UML. d. Creación y revisión de modelos de amenazas.
Paso 3	**Durante el desarrollo**
	a. Código de acceso. b. Revisión del código.
Paso 4	**Durante la implementación**
	a. Prueba de penetración en la aplicación. b. Pruebas de administración y configuración.
Paso 5	**Operación y mantenimiento**
	a. Revisión operativa. b. Inspecciones periódicas. c. Control de control de moneda.

1.6 Herramienta para el análisis de riesgos

En la presente investigación se analizaron las siguientes metodologías de análisis de riesgos, figura 1.7, como:

- OCTAVE.
- MAGERIT
- CRAMM.
- COBRA.

FASES DE LA GESTIÓN DEL RIESGO	PROCESOS DE OCTAVE	PROCESOS DE MAGERIT	PROCESOS DE ISO 27005	PROCESOS DE CRAMM	PROCESOS DE NIST
1. Fase establecimiento del contexto	Proceso 1: Visión organizativa	Proceso 1: Método	Proceso 1: Establecimiento de contexto	Proceso 1: Identificación y valoración de los activos	Proceso 1: Caracterización de sistemas
	· Activos · Amenazas · Prácticas actuales · Vulnerabilidades organizativas · Requerimientos de seguridad	· Estudio de oportunidad · Determinación del alcance del proyecto · Planificación del proyecto · Lanzamiento del proyecto	· Consideraciones generales · Criterios básicos · Alcance y límites · Organización para la gestión del riesgo en la SI	· Hardware · Software · Datos · Activos de localización que componen el sistema de información	· Identificación de activos · Criticidad de datos y sistemas · Sensibilidad de datos y sistemas
2. Fase identificación de riesgos y oportunidades		Proceso 2: Análisis de riesgos	Proceso 2: Valorización del riesgo	Proceso 2: Análisis de riesgos	Proceso 2: Identificación de amenazas
					· Definición de amenazas
					Proceso 3: Identificación de vulnerabilidades
					· Lista de vulnerabilidades potenciales
3. Fase análisis de riesgos	Proceso 2: Visión tecnológica	· Caracterización de los activos · Caracterización de las amenazas · Caracterización de las salvaguardas · Estimación del estado del riesgo	· Descripción general · Análisis del riesgo · Evaluación del riesgo	· Identifica amenazas · Identifica vulnerabilidades · Probabilidad de ocurrencia	Proceso 5: Determinación de probabilidades
					· Rating de probabilidades
					Proceso 6: Análisis de impacto
	· Componentes claves · Vulnerabilidades técnicas				· Pérdida de integridad · Pérdida de disponibilidad · Pérdida de confidencialidad
					Proceso 7: Determinación del riesgo
					· Riesgos y niveles del riesgo
4. Fase evaluación de riesgos	Proceso 3: Estrategia y desarrollo del plan	Proceso 3: Gestión de riesgos			Proceso 4: Análisis de controles
5. Fase tratamiento de riesgos	· Riesgos · Estrategia de protección · Planes de mitigación	· Toma de decisiones · Plan de seguridad · Ejecución del plan	Proceso 3: Tratamiento del riesgo	Proceso 3: Medidas de seguridad	· Lista de controles actuales y planificados
			· Descripción general · Reducción del riesgo · Evitación del riesgo · Transferencia del riesgo	· Medidas organizadas en agrupaciones lógicas · Servicios de ayuda · Informes de implementación de contramedidas	Proceso 8: Recomendación de controles
			Proceso 4: Aceptación del riesgo		· Controles recomendados
			· Convivir con el riesgo		
6. Fase monitoreo y revisión			Proceso 6: Monitoreo y revisión del riesgo		
			· Factores de riesgo · Mejora de la gestión del riesgo		
7. Fase comunicación y consultas			Proceso 5: Comunicación de los riesgos		Proceso 9: Documentación de resultados
			· Entendimiento de la probabilidad y las consecuencias de estos riesgos		· Informe de valoración de riesgos

Figura 1.7 Cuadro comparativo Herramienta para el análisis de riesgos.
Fuente: (Kennedy, 2015, pág. 125)

1.6.1 OCTAVE (Amenazas Críticas Operacionales, Activos y Evaluación de Vulnerabilidades).

Administrar los recursos de su organización, como personas, equipos, software, información y sistemas, para ayudarlo a identificar y evaluar el impacto de esos riesgos en los principios de seguridad (Aguilera, 2016).

Está organizado en tres fases y cada una está dividida en diferentes procesos.

Fase I. Creación de perfiles de amenazas basados en recursos.

- Proceso 1. Identificación de la información a nivel de gestión.
- Proceso 2. Identificación de la información a nivel operacional.
- Proceso 3. Identificación de la información para el usuario final.
- Proceso 4. Consolidar información y crear perfiles de amenazas.

Fase II. Identificar las vulnerabilidades de la infraestructura.

- Proceso 5. Identificación de componentes clave.
- Proceso 6. Evaluación de los componentes seleccionados.

Fase III Desarrollo de planes y estrategias de seguridad.

- Proceso 7. Análisis de riesgos.
- Proceso 8. Desarrollo de estrategias de protección.

1.6.2 MAGERIT

La metodología para analizar y gestionar los riesgos en los sistemas de información del gobierno consiste en una serie de manuales y una herramienta auxiliar (Hadnagy, 2017).

1.6.3 CCTA Risk Analysis and Management Method (CRAMM)

Método de análisis y gestión de riesgos, herramienta de análisis de riesgos e identificación de métodos avanzados de seguridad.

1.6.3.1 Security Risk Analysis & Assessment COBRA

Herramienta de negocios, definida como un consultor externo para ayudar a tomar decisiones de seguridad.

1.7.Mejores prácticas enfocadas a la seguridad de la información.

Los mejores métodos para garantizar la seguridad de la información se describen a continuación:

- Política de seguridad
- Inventarios de activos
- Norma ISO 27001.
- Aplicar el cuestionario al administrador de la red.
- Aumentar la conciencia de la seguridad de una red local.
- Implementar niveles de seguridad informática.
- Uso de un plan de emergencia.

1.7.1. Políticas de seguridad

Las políticas de seguridad informática son un conjunto de pautas y procedimientos definidos por los administradores de la seguridad de los sistemas de información y comunicación para proteger sus sistemas e información. En términos más generales, esto indica que este es el caso y que esto no está permitido en la zona de seguridad durante la operación general de los sistemas (Perramón, 2015).

Este es un documento detallado sobre cada uno de los procedimientos para obtener un sistema seguro y confiable para prevenir ataques intencionales o causales, así como una descripción de lo que se desea proteger y por qué.

Las políticas de seguridad deben estar basadas en las siguientes características:

- Determine y elija lo que necesita ser protegido.
- Establecer los niveles de prioridad.
- Conozca las consecuencias del tiempo y los costos.
- Identificar amenazas y niveles de vulnerabilidad. Realizar un análisis de costes.
- Implementar respuestas a incidentes.

1.7.2. Inversiones de activos

Es importante hacer un inventario de todos los recursos que constituyen la red local para clasificarlos de acuerdo con su criticidad y su rendimiento y para determinar el efecto que esto tendrá en su falla (Alonso, 2016).

1.7.3. Norma ISO-27001

Es un estándar internacional para la administración de la seguridad de la información, que establece los requisitos que debe cumplir el Sistema de gestión de la seguridad de la información (SGSI).

Se basa en los riesgos del negocio para la creación, implementación, operación, monitoreo, verificación, mantenimiento y mejora de la seguridad de la información (Zeltser, 2014). El sistema de gestión incluye varios temas, pero se han evaluado los siguientes:

- Políticas de trámites y procesos.
- Aplica un enfoque de procesos a la gestión de la seguridad de la información, resaltando la importancia de los siguientes aspectos.
- Para comprender los requisitos de seguridad de la organización, es necesario establecer políticas y objetivos.
- Implementar herramientas de gestión de riesgos en un contexto empresarial. Monitorear el rendimiento del SGSI.
- Mejora continua basada en la medición del objetivo.
- Adoptar un modelo PDCA (planificar, hacer, verificar, actuar).

a. Aplicación de un cuestionario a un administrador de red

El cuestionario contiene una serie de preguntas sobre los diversos puntos de seguridad de la LAN y verifica si el administrador de la red cumple con los requisitos mínimos de seguridad (Reza, 2016).

b. Aumentar la conciencia de la seguridad de una red local.

Es muy importante publicar las políticas establecidas para la seguridad de la LAN para todos aquellos que usan los servicios, y especialmente enseñarles el verdadero significado de la seguridad mediante la realización de campañas de información para su uso correcto.

c. Implementación de niveles de seguridad informática.

Estructurar un estándar que separa diferentes niveles de seguridad al clasificar los recursos según la importancia crítica, la importancia o los riesgos de una red local. Se puede llamar un ejemplo: nivel A, nivel B, nivel C.

d. Usar un plan de emergencia.

Este documento presenta diferentes métodos para crear controles y reglas para evitar interrupciones que amenazan la disponibilidad y continuidad de los procesos y para restablecer el nivel de operación de la red local lo más rápido posible (Ortiz & Villegas, 2014).

1.8 Lógica del Negocio

MALDONADO HIDRAULICOS empresa CIA.LTDA GADZOVSKI. (HIDROMAG) se creó en 2009 en la ciudad de Quito, creado por jóvenes profesionales que deben realizar trabajos de mantenimiento relacionados con el mantenimiento de equipos hidráulicos y el suministro de piezas de calidad con el mejor servicio al cliente.

Con la creación e introducción de comercio y de acuerdo con las necesidades del mercado ecuatoriano, nuestras existencias han aumentado debido al número de bombas, motores, válvulas hidráulicas y accesorios para los sectores marítimo, petrolero e industrial. Como resultado, la empresa se ha establecido con un gran stock de equipos y piezas de repuesto para bombas totalmente originales y motores hidrostáticos OEM responsables del equipo de carreteras; Finalmente, eliminando la entrega o reparación inmediata dentro del período de registro.

En 2011 y 2012, las exposiciones HIDROMAG se presentaron en el sector petrolero y minero en Ecuador, donde demostraron que tienen productos de capacidad y potencia hidráulica disponibles de marcas reconocidas como Rexroth y Sauer Danfoss, Bolb, Terex, entre otras.

En 2013, el personal participó en todos los cursos de capacitación de HIDROMAG en el extranjero, donde analizaron los avances técnicos en el mantenimiento de equipos hidráulicos, el diagnóstico, la rehabilitación y el mantenimiento de los sistemas hidráulicos de Eaton y Danfoss funcionamiento de la bomba hidráulica de válvula proporcional Rexroth; utilizando la información adquirida y brindar servicios de alta calidad. Los empleadores están constantemente capacitados en HIDROMAG en el extranjero.

1.9 Herramientas Técnicas

Metodología OSSTMM

Las pruebas de seguridad comienzan con un registro que, en su forma más confiable, es la dirección de los sistemas controlados, la prueba finaliza con el inicio de la fase de análisis y la preparación del informe final. La metodología no influye en la forma, el tamaño, el estilo o el contenido del informe final y no determina cómo se debe analizar, esta es la tarea del probador y / o la organización (Reza, 2016).

OSSTMM se divide en secciones, que se dividen en módulos y estos en tareas específicas. Debe hacerse una distinción entre la recopilación de datos y la verificación, En otras palabras, no solo debe buscar vulnerabilidades, vulnerabilidades, etc., sino que también debe buscarlas. Por esta razón, la metodología no debe compararse con un análisis simple de vulnerabilidades o puertos. Además, para ejecutar OSSTMM, debe verificar los resultados (Reza, 2016).

Para determinar la metodología a seguir, es importante no limitar el potencial creativo del probador: en algunos casos, los estándares o formalidades podrían afectar la calidad de la prueba, El evaluador será la última palabra y podrá realizar pruebas según su experiencia y la creatividad.

Además, debe agregarse que muchas actividades no son muy específicas y abiertas, lo que no permite que las nuevas tecnologías o funciones vuelvan obsoletas estas actividades, Esto es comparable a las leyes, donde tienden a ser vagas y fáciles de interpretar, de modo que pueden cubrir más casos, porque sería totalmente imposible determinar una situación posible y futura.

Cada módulo está asociado con el anterior y el siguiente, y entre las secciones es similar, los datos y conclusiones obtenidos en el formulario se pueden utilizar para realizar la siguiente tarea, por ejemplo, puedes descubrir nuevos hosts para verificación.

1.10 Alternativas de Solución

Sección A – Seguridad de la información

- **Revisión de la inteligencia competitiva**

Este módulo es quizás el menos valioso de todas las pruebas de intrusión (legales o no), porque no es intrusivo y se puede realizar sin el conocimiento técnico previo, de hecho, se está hablando de recopilar toda la información posible de la sociedad considerada (Navratilova, 2016).

En primer lugar, se desea poder encontrar información para crear un mapa y una estructura de equipo informático. Busca en internet lo que tiene la empresa, en otras palabras, se trata de encontrar toda la información disponible que revela datos (confidenciales o no) sobre la empresa, A menudo se entiende que se puede recopilar mucha información legalmente, en sitios web, impresos, etc.

Por ejemplo, es interesante recopilar toda la información sobre los servicios que puede ofrecer una empresa (números de teléfono, correos electrónicos con personas de contacto, páginas web, servidores FTP, etc.), así como muchas otras técnicas. Aunque se pueden utilizar, por ejemplo, para la ingeniería social, algunos aspectos interesantes podrían ser:

- La sociedad de la que depende.
- Empresas dependientes de esto.

- Proveedores
- Clientes
- Productos ofrecidos

Cualquier dirección IP relacionada con algunos de ellos puede ser útil durante un ataque se considera IP si:

- Pertenece a la organización
- Utilizado por la organización.
- Están registrados a nombre de la organización
- Sirve a la organización de una manera determinada.
- Afiliado a la organización

Se debe tener en cuenta que en el momento de la auditoría, debe quedar claro para nosotros que la información recopilada en esta sección puede estar dentro y fuera del contrato. Como una oferta para el software, para ejecutar esta sección con cuidado, recientemente se habla de una aplicación de software gratuita que le permite analizar la información de la competencia de manera ordenada.

Esta aplicación se llama maltego, según el sitio web oficial (http://www.paterva.com/maltego/), Maltego es una aplicación gratuita de inteligencia y medicina forense que le permite recopilar información, así como presentar estos información Maltago, con sus bibliotecas gráficas, le permite identificar relaciones clave entre información y pre identificar sus relaciones (Alonso, 2016).

A continuación se evidencia en la Figura 1.8 la información en un test de intrusión.

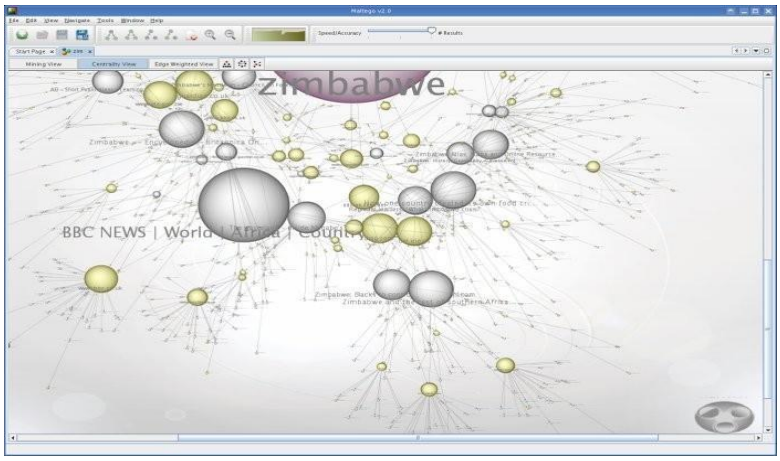

Figura 1.8 Búsqueda de información en un test de intrusión
Fuente: (Alonso, 2016)

Algo interesante para agregar a esta sección, algo que parece difundir la gloria de hoy, piratear a Google. La piratería de Google implica el uso de las funciones de búsqueda y almacenamiento de ciertos motores de búsqueda (en este caso, Google) para buscar información confidencial, que no debería estar disponible públicamente, en las bases de datos de motores de búsqueda, esto se hace usando ciertas palabras clave o frases y, como regla, ayuda mucho al oyente (Zeltser, 2014).

En su formato malicioso, se puede usar para detectar servidores web (o páginas web) vulnerables a ciertas vulnerabilidades o problemas de seguridad. Además, se utilizan para buscar información confidencial de otras personas, como tarjetas de crédito, contraseñas.

El truco de Google es utilizar operadores avanzados de filtrado de Google, por ejemplo, Intitle: admbook intitle: version filetype: php. De igual manera busca en todas las páginas web que contengan las palabras admbook y versión en el encabezado y se puede acceder al sitio web a través de PHP, esto es útil porque muchas páginas. Internet, de forma predeterminada, se proporciona con contenido de texto basado en la web que indica la versión, lo que puede ser una vulnerabilidad conocida (Chappell & Combs, 2016).

- **Descripción de la confidencialidad**

La verificación de la confidencialidad es responsable de los aspectos éticos y legales de almacenar, transferir y controlar los datos de empleados y clientes. Esto garantiza que

se respeten los derechos de las personas dentro de la empresa y que sus datos personales no sean accesibles para todo el mundo, esto también se aplica a la forma en que se distribuyen las contraseñas (Perramón, 2015).

No es lo mismo que transmitirlos en palabras, en lugar de escribir, publicar, etc. Esto puede ser muy comprometedor para la empresa y la persona interesada, por lo general, es posible encontrar muchas contraseñas escritas, por ejemplo, después de colocarlas en el borde del monitor de trabajo.

Aunque muchas leyes son locales, todas se aplican a Internet y, por lo tanto, influyen en los evaluadores de seguridad a nivel internacional, por lo tanto, es necesario tener un conocimiento básico de estas leyes y las medidas necesarias para que la empresa pueda respetarlas.

- **LOPD:**

El objetivo principal es regular el procesamiento de datos personales y archivos, independientemente del medio utilizado, los derechos de los ciudadanos sobre ellos y las obligaciones de quienes los crean o los procesan (Alonso, 2016).

- **LSSI:**
    - Obligaciones de los proveedores de servicios, incluidos aquellos que actúan como intermediarios en la transferencia de contenido a través de redes de telecomunicaciones.
    - Comunicaciones comerciales en formato electrónico.
    - Información antes y después de la celebración de contratos electrónicos.
    - Condiciones relativas a su validez y eficacia.
    - Régimen de sanciones aplicable a los prestadores de servicios de la sociedad de la información.

- **Recopilación de documentos.**

Esta sección se refiere al primer párrafo de esta sección (encuesta de competencia), aunque se enfoca más en aspectos más pequeños y específicos, como correos electrónicos,

ofertas de trabajo, etc., que se pueden recuperar información o metadatos incluyendo documentos. FOCA podría ser una herramienta interesante en este sentido (Hadnagy, 2017).

Este es un programa para descargar archivos de Office desde páginas web, extraer información oculta, metadatos y datos perdidos, también puede cruzar la información recibida e intentar obtener un mapa de la red estudiada, fue creado para los tours Up To Secure y Blackhat Europe 2009, se muestra en la Figura 1.9.

Figura 1.9 Descargando ficheros con foca (herramienta para análisis de meta datos)
Fuente: (Hadnagy, 2017)

También hay una versión en línea como se muestra en la Figura 1.10, que puede ser muy útil para crear rápidamente esta sección y desde cualquier lugar con una conexión a Internet.

Figura 1.10 FOCA Online
Fuente: (Hadnagy, 2017)

Sección B - Seguridad del proceso

- **Solicitar una prueba**

Este tipo de prueba es un sector de la llamada ingeniería social, en este caso, se intenta obtener acceso solicitando permiso al personal responsable de otorgar las autorizaciones de acceso a través de los sistemas de comunicación (correo electrónico, teléfono, etc.) a través de los cuales se pasa a otra persona (Aguilera, 2016).

Uno de los principios básicos de la ingeniería social es que los usuarios son el eslabón débil, y eso es a menudo cierto. Los problemas de seguridad de la información a menudo no provienen de una mala programación o configuración del sistema, sino de personas mal entrenadas, desprotegidas o simplemente descuidadas.

A menudo, esto se resuelve como una persona que usa Internet o un teléfono que pretende ser, por ejemplo, un empleado de un banco, una tercera empresa, un cliente, etc., que busca información para acceder al sistema.

Un ejemplo simple podría ser la falsificación de un administrador, que requiere la contraseña de un usuario para un propósito legítimo, esto se observa a menudo en la vida cotidiana de cualquier usuario de Internet cuando recibe el llamado phishing de un sujeto que requiere un número de tarjeta de crédito para realizar cualquier verificación (Ortiz & Villegas, 2014).

Este método, que parece simple como personificar a alguien, es un método curioso, que generalmente es bastante eficiente y mucho más barato que buscar fallas informáticas anormales, de hecho, se conoce que en Internet que se realizó una encuesta en Boixnet, donde el 90% de los empleados de la oficina de Waterloo abrieron sus contraseñas a cambio de una pluma económica.

No sé en qué medida será cierto porque no podría compararlo con fuentes confiables, pero al menos permite comprender cómo se adquiere en línea el concepto de ingeniería social, a menudo es difícil encontrar ejemplos concretos de ataques de ingeniería social, ya que las organizaciones involucradas no quieren admitirlo o no han sido documentadas oficialmente o pueden no haber sido conscientes de ello, sin embargo,

hay varios ejemplos del Instituto para la Seguridad Internacional (Ortiz & Villegas, 2014).

- Llaman a medianoche.
- ¿Has estado llamando a Egipto en las últimas 6 horas?
- No lo hagas
- Se graba una llamada activa en este momento, y él revisó una tarjeta telefónica a su nombre.
- También llama a Egipto. Además, tiene hasta $ 2,000 para llamadas de alguien que usa su nombre.
- Usted es responsable de esos $ 2,000, tiene que pagarlos... arriesgando el trabajo tratando de deshacerse de esos $ 2,000, pero tiene que leer su tarjeta y su PIN, y luego podrá quitarla.

Otro principio fundamental de la ingeniería social es utilizar la naturaleza humana del deseo de ayudar, las líneas de atención al cliente son particularmente vulnerables a esto porque están ahí para ayudar a los atacantes a aprovechar al máximo esta calidad. Además, las personas que ocupan estos puestos generalmente están mal informadas sobre la seguridad y reciben un salario mínimo, lo que las convierte en víctimas ideales. Por ejemplo, durante una demostración en vivo de Computer Security Institute: llamaron a la compañía telefónica a la que habían sido transferidos hasta que llegaron al centro de servicio al cliente (Navratilova, 2016).

- ¿Quién es el inspector de servicios hoy?
- Betty.
- Vete con Betty.
- [En este momento, es transferido de Betty.]
- Betty, ¿estás teniendo un mal día?
- No porque tu sistema no parece funcionar.
- No, mi sistema no funciona, parece que funciona bien.
- "Mmmm, intenta salir y entrar de nuevo". [Betty sale y entra de nuevo]
- No se nota un cambio. Sal y vuelve otra vez. [Betty sale y entra]

- Nada de eso. Tendré que iniciar sesión como usuario y averiguar qué está sucediendo con su nombre de usuario. Dame tu nombre de usuario y contraseña.

Como se puede ver, los ejemplos pueden ser bien pensados e inteligentes, y las personas que no han sido advertidas o mal capacitadas tienden a proporcionar sus datos.

2. Testeo de sugerencia guiada

Este módulo es también una rama de la ingeniería social, en muchos sentidos, coincidirá con el módulo anterior, es decir, no se excluyen mutuamente. La principal diferencia entre los dos es que, en este caso, el atacante pretende ser otra persona e invita al otro a visitar una ubicación externa (una página web o una cuenta de correo electrónico), uno de los primeros ejemplos que se puede observar es el phishing, en la que la persona puede simplemente enviar datos al atacante o la víctima (Navratilova, 2016).

Por ejemplo, al invitar a la víctima a una página web completamente idéntica al sitio web oficial (suponiendo que en el sitio web del banco, donde se le pide al usuario que ingrese su información (nombre de usuario, contraseña, código PIN de la tarjeta de crédito, etc.), y haga clic en enviar/confirmar, la página web luego envía los datos al atacante, quien puede leerlos y utilizarlos.

Una forma de evitar esto es mirar la dirección web y asegurarse de que no sea extraña y que pertenezca al sitio web oficial. Esto último lleva a hablar sobre una brecha de seguridad que apareció el verano pasado: una falla de DNS (Hadnagy, 2017).

La falla fue descubierta por Dan Kaminsky, un reconocido investigador de seguridad que trabaja para IOActive, fue muy elogiado por la forma en que enfrentó su descubrimiento, advirtió a las autoridades pertinentes y, después de unos meses, explicó el fracaso de la comunidad.

Esta falla le permitió al atacante redirigir a los clientes a otros servidores de su elección, que podría usar con fines fraudulentos. A continuación en la Figura 1.11 se describe en detalle el funcionamiento del supuesto error, suponiendo que el lector sepa cómo funciona la consulta DNS correcta, debe recordarse que los campos más importantes del paquete DNS.

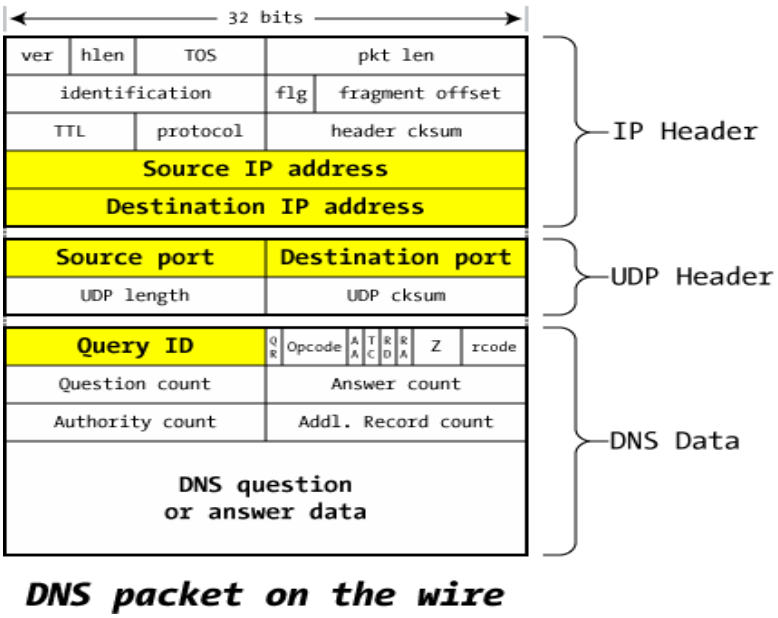

Figura 1.11 Unixwiz.net Consejos Técnicos de Steve Friedl
Fuente: (Hadnagy, 2017)

De este paquete, se está particularmente interesado en las siguientes áreas:

- Dirección IP de origen / destino: direcciones de origen y destino, respectivamente.
- Puertos de origen / destino: puertos de origen y destino, respectivamente. El puerto de destino del primer paquete siempre será 53 / UDP porque los servidores DNS normalmente escuchan en este puerto.
- ID de solicitud: solicitud de identificación. Permite a los servidores hacer coincidir las respuestas con las solicitudes recibidas porque el servidor normalmente recibe varias solicitudes al mismo tiempo.
- RD (recursión deseada): se usa para indicar si se requiere recursión (está marcada con 1) o no (está marcada con 0) para las consultas de DNS. No todos los servidores de nombres ofrecen recursión.
- Número de respuestas / autoridades / entradas adicionales: se utiliza para indicar diferentes tipos de respuestas a una solicitud realizada por un cliente.
- Q & A DNS: este campo contiene los datos de Q & A de los campos anteriores, por ejemplo, el nombre de dominio de una tupla es IP.

Una vez que se conocen estos campos, se puede explicar el error de DNS o, más correctamente, el envenenamiento de la memoria caché. El caché de DNS no es tan simple como simplemente enviar paquetes aleatorios a un servidor de nombres (a diferencia de

otros envenenamientos, como ARP), porque el servidor de nombres responde solo a solicitudes de otras fuentes (Chappell & Combs, 2016).

¿Cómo espera el servidor de nombres un paquete en particular?

- El paquete llega al mismo puerto UDP desde el que se envió.
- La sección de preguntas / respuestas (que está duplicada en la respuesta del paquete) corresponde a la pregunta / respuesta de la solicitud pendiente.
- El ID de la solicitud corresponde a la solicitud pendiente.
- Las secciones de autoridad y complementarias contienen nombres que pertenecen al mismo dominio que la aplicación. Esto se conoce como control balístico.

Si se cumplen todas estas condiciones, el servidor de nombres aceptará la respuesta como válida y almacenará en caché la nueva tupla - nombre de dominio IP en su caché.

Ahora, ¿cómo se puede obtener todas estas condiciones?

El error proviene del hecho de que es fácil adivinar el identificador de la solicitud, porque en los servidores de nombres antiguos, el identificador de la solicitud simplemente aumenta en uno con cada solicitud enviada, lo que facilita la determinación de la continuación, en la Figura 1.12 se puede ver el ID de la consulta.

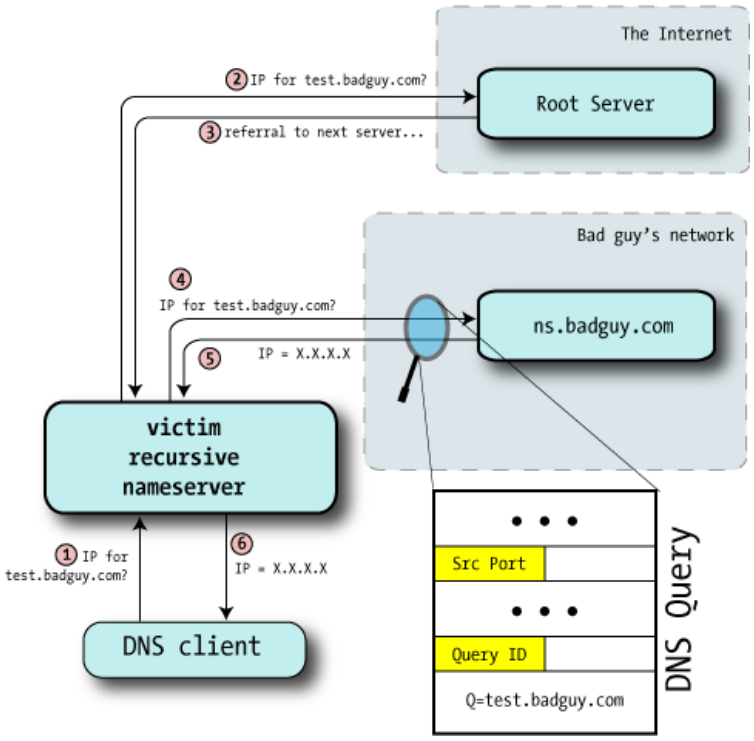

Figura 1.12 ID de consulta
Fuente: (Hadnagy, 2017)

Esto podría hacer que el servidor de nombres indique su ID de solicitud porque está configurado para:

1. Un atacante (malo en el diagrama) obliga al servidor de nombres de la zona a verificar el servidor de nombres (en el ejemplo test.badguy.com) con el servidor de nombres de la víctima. También puede preguntar directamente al servidor si permite la recursión desde la ubicación del atacante o persuade al usuario para que busque, por ejemplo, el nombre de la prueba en una página web.
2. El servidor de nombres de la víctima recibe la solicitud y funciona normalmente, intentando resolver el nombre de dominio en los servidores raíz.
3. La dirección test.badguy.com está permitida en el servidor del atacante.
4. Durante este tiempo, el atacante controla el tráfico de IP que pasa a través de la computadora y luego captura el identificador de consulta utilizado.
5. Actualmente se tiene un identificador de solicitud, aunque no se ha guardado en caché la memoria caché porque la dirección test.badguy.com era legal y pertenecía al atacante. Pero ahora se conoce cómo predecir el identificador de solicitud, así como otros datos, como el puerto UDP, los servidores de nombres requeridos, etc., a continuación en la Figura 1.13 se evidencia como usarlo para envenenar el caché.

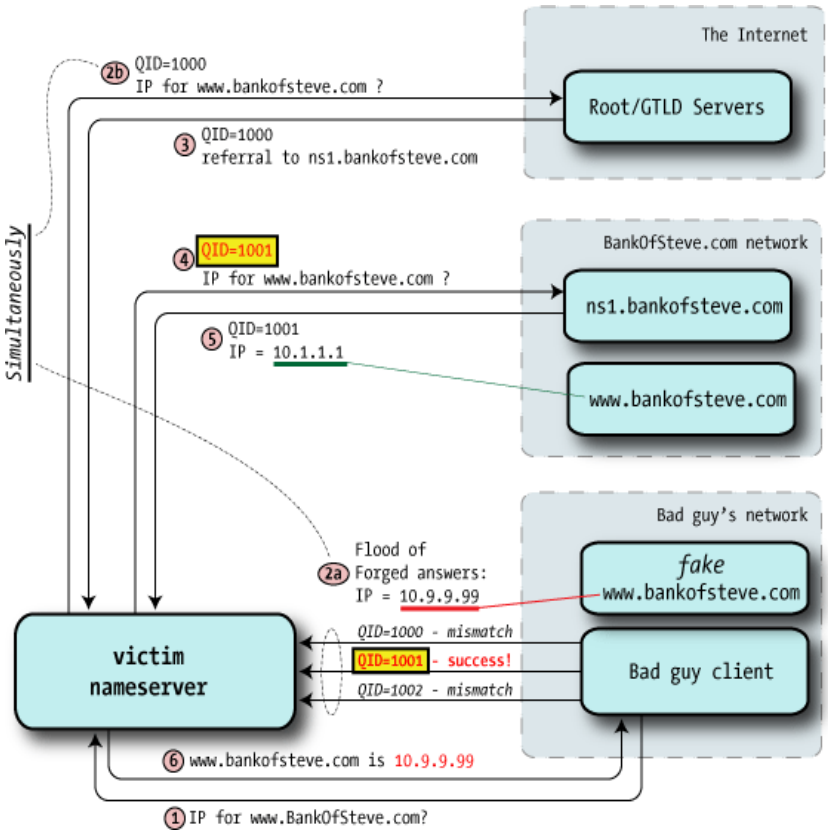

Figura 1.13 Envenenar cache en servidor
Fuente: (Hadnagy, 2017)

- **Testeo de las Personas Confiables**

Este es el tercero de los módulos sobre ingeniería social, en este último caso, difiere de otros porque requiere información privilegiada, no tiene que ser una contraseña o una licencia. En muchos casos, la mayoría de las personas no tienen problemas para revelar información confidencial que puede ser muy útil para un atacante, por ejemplo, muestra una situación ficticia que, aunque no está centrada en el negocio, bien puede mostrar el alcance de este tipo de recopilación de información (Kennedy, 2015).

Un ejemplo fue escrito por Antonio Villalón, en un blog propiedad de S2 Grupo (administrado por la empresa de seguridad de Valencia):

¿Qué sucede si solo tienes un número de móvil, sin datos adicionales?, puede colocar un anuncio en autos estacionados en diferentes partes de la ciudad, fijados por copa, a un precio atractivo y con este número de teléfono, pero eso no crea problemas puede ser un problema tratar de obtener información de esa persona; un poco de ingeniería

social nunca duele y, feliz o desafortunadamente, en este país, si se escucha la palabra GRATIS, se emite una aprobación.

Desde el prefijo móvil, el operador al que pertenece se puede determinar con un alto nivel de probabilidad, de modo que una promoción de un operador específico siempre es una buena excusa; si hay una migración, la promoción se convierte automáticamente en una oportunidad para los clientes anteriores. El resumen podría ser: Le llamaremos a XXXX para ofrecerle, después de la comparación de sus datos, una cotización por teléfono de 0 centavos, GRATIS, durante todo el mes de agosto, sin letra pequeña (Kennedy, 2015).

- Oh, dime.
- ¿Eres el señor Luis López de Salamanca?"
- No, creo que se equivoca.
- Wow, lo siento, así que no puedes acceder a la promoción... de todos modos, eres un cliente XXXX, ¿verdad?
- Sí, sí, dime ...
- ¿Tienes un correo electrónico?
- Claro
- Si nos lo proporciona, le enviaremos un correo electrónico, simplemente respondiendo al formulario, recibirá acceso exclusivo a esta promoción.
- Por supuesto, mi dirección de correo electrónico es aaaa@hotmail.com.
- Pronto recibirás un correo; tan pronto como se reciba su respuesta, nos pondremos en contacto con usted dentro de una semana para confirmar su acceso. Recibirás llamadas gratuitas durante el mes de agosto (Kennedy, 2015).
- Oh, muchas gracias, muchas gracias ...

A partir de ahí, ya no es necesario enviar un correo electrónico a esta persona desde una dirección que parezca confiable, aunque el 99% de los empleados tiene una dirección de Hotmail confiable, es mucho más difícil usar “registro@XXXXX.dyndns.org”, donde XXXX es obviamente el nombre del operador. En esta carta con los logos y trámites

oficiales que le dan credibilidad, se le pide que incluya su nombre, su código postal y el número de teléfono que desea asociar con la promoción (aunque ya lo se conoce que nunca está de más). Y así se conoce de inmediato cuál es el nombre de la persona y dónde vive (para solicitar una dirección de correo, además del hecho de que no dan nada, la gente generalmente es más renuente, pero el código postal ayuda sin problemas) (Kennedy, 2015).

Como se puede observar, al tener solo un número de teléfono, se pudo obtener una gran cantidad de información personal. Imagine la cantidad de opciones que podrían desarrollar para su uso en el mundo corporativo e imagine cómo mejorarlo si ya hubiera informado a la compañía o a la persona a la que se llama. Además, la empresa emplea a muchas más personas, por lo tanto, se puede preguntar qué se obtiene de uno de ellos para facilitar la llamada de la siguiente persona.

1.10.1. Sección C – Seguridad en las Tecnologías de Internet

- **Sondeo de la Red**

Esta forma a menudo no se considera como tal. A veces esto no se hace porque el cliente puede especificar directamente un rango de direcciones IP para verificar, además, los resultados obtenidos en este módulo a menudo se completan en los siguientes módulos (Ortiz & Villegas, 2014).

Este módulo es el primer punto de reconocimiento de la red. Se trata de descubrir todo lo que se pueda sobre él, de forma no invasiva. Haciéndolo desde el exterior, tratando de comprender todo lo que se tiene, como los rangos de direcciones IP de la empresa, los subdominios, etc.

Este módulo es muy similar al módulo en la sección A, pero solo está tratando de recopilar información más específica sobre las asignaciones de red, los bloques de IP. La búsqueda de direcciones IP individuales será la tarea de los siguientes bloques. Si encuentra una dirección IP diferente, indicaría su ubicación en lugar de la dirección IP. A menudo, esto podría ser una suposición falsa, pero por el momento está tratando de

recopilar la mayor cantidad de información posible, que filtrará más adelante (Ortiz & Villegas, 2014).

¿Qué se puede hacer para lograr este objetivo?

Hay muchas posibilidades, incluyendo:

- WHOIS
- DNS Zone Transfer

WHOIS: este es un protocolo muy utilizado para acceder a la base de datos oficial para determinar el propietario de un nombre de dominio, dirección IP, etc. Tradicionalmente, se ejecutaba desde la línea de comandos (bajo Linux usando el comando whois), aunque ahora hay sitios en ejecución, en la Figura 1.14 se detalla en el sitio whois.net.

Figura 1.14 WHOIS.NET
Fuente: (Ortiz & Villegas, 2014)

Transferencia de zona DNS, generalmente utilizada para replicar o realizar copias de seguridad de datos DNS en diferentes servidores DNS. El usuario o servidor realizará una solicitud de transferencia de zona desde un servidor de nombres específico, si el servidor se resuelve, todos los nombres DNS y las direcciones IP alojadas en el mismo servidor se transferirán al formato ASCII.

En Linux, el comando del host es el siguiente:

$ host -l rutgers.edu
> Servidor de nombres Rutgers.EDU dns1.Rutgers.EDU
> Nombre del servidor Rutgers.EDU dns2.Rutgers.EDU
> Servidor de nombres Rutgers.EDU dns3.Rutgers.EDU
> Servidor de nombres Rutgers.EDU turtle.mcc.com
> Rutgers.EDU en la dirección 165.230.4.76
> grad03.Rutgers.EDU en la dirección 128.6.20.29
> dgcacook4.Rutgers.EDU en 128.6.87.158
> grad04.Rutgers.EDU en la dirección 128.6.20.30. En Windows, se encuentra la herramienta nslookup:
> nslookup 204.228.150.3 Servidor: ns.computerhope.com Dirección: 1.1.1.1

Nombre: www.computerhope.com Dirección: 204.228.150.3 (Ortiz & Villegas, 2014).

Hay muchas otras características, como métodos de reenvío de DNS brutales, reenvío de correo SMTP o recuperación de registros de dominio, aunque son menos comunes. Puede leer más sobre el trabajo en el kit de herramientas de Open Syngress para pruebas de penetración.

- **Escaneo de Puertos**

Aquí comienza la primera parte de la prueba obsesiva. En este módulo, intenta verificar qué servicios están activos actualmente y escuchar al cliente que se conecta a él. El escaneo de puertos se solicita a los puertos del sistema en el nivel de transporte y de red y también se verifica si el firewall está configurado correctamente (Zeltser, 2014).

Cada sistema conectado a la red tiene 65,536 puertos (incluido el puerto 0). Sin embargo, no siempre se debe comprobarlos todos, la selección de los puertos a verificar es decidida por el propio equipo de auditoría. Además de revisar los puertos más importantes, si se recomienda escanear puertos inusuales de vez en cuando, esta es una forma común de detectar servicios conectados pero no deseados.

El NMAP es un escáner de puertas y hablará sobre él y su funcionamiento, en el ejemplo de la prueba de intrusión presentada en este texto.

- **Identificación de Servicios**

Este formulario verifica los resultados del escaneo del puerto. En muchos casos, los escáneres de puertos pueden obtener resultados erróneos que otro servicio escucha (por ejemplo, un troyano escucha un puerto conocido, como 53, que suele estar asociado con DNS).

Para ejecutar comprobaciones, puede conectarse a través de un programa que envía cadenas de texto y cambia los comandos con los servicios que se desea controlar. Si responden correctamente a los comandos (puede verificar qué comandos son compatibles con cada protocolo en el RFC), entonces este servicio está escuchando en el puerto encontrado, por lo que debe ser verificado. Telnet, Netstat son ejemplos de herramientas para probar y se analizarán en un ejemplo de prueba de penetración de este texto (Zeltser, 2014).

- **Identificación del sistema**

Este módulo controla el sistema operativo de las máquinas, esto se hace analizando la respuesta de las máquinas a ciertos paquetes que se les envían.

Por ejemplo, NMAP (un escáner de puertos que también identifica el sistema operativo y su versión) lo identifica basándose en un control de huellas dactilares TCP / IP. Nmap envía una serie de paquetes TCP y UDP al sistema remoto y analiza casi todos los bits de respuesta. Nmap compara los resultados de una docena de pruebas, como el análisis de TCP (número de secuencia inicial), la compatibilidad con las opciones de TCP y su orden, el análisis de IPID y la verificación del tamaño inicial de la ventana, con su base de datos nmap-os-fingerprints (Alonso, 2016).

Esta base de datos contiene más de 1,500 rastros del sistema operativo y, si existe una coincidencia, se muestra información detallada sobre el sistema operativo. Cada elemento contiene una descripción del sistema operativo en un texto libre, una

clasificación que especifica el nombre del proveedor (Sun, por ejemplo), el sistema operativo subyacente (Solaris, por ejemplo), la versión del sistema de Operación y tipo de dispositivo (propósito general, enrutador, interruptor, consola de juegos, etc.).

Aunque el programa que usa para adivinar el sistema operativo y la versión que usa, se debe tener cuidado porque a menudo cometen errores, e incluso si tienen razón, muchas personas generalmente buscan dotes para un Sistema operativo y una versión específica sin configurar para resolver un problema de seguridad documentado.

- **Búsqueda de Vulnerabilidades y Verificación**

Aquí es donde tendrá lugar el ataque: se detectarán las fallas en las máquinas de la red. En general, los programas automatizados se usan comúnmente para buscar vulnerabilidades de seguridad documentadas en términos de software y versiones de sistema operativo utilizadas por las máquinas. Debe agregarse que, según OSSTMM, se utilizan al menos dos programas automatizados diferentes para verificar la consistencia de los programas, lo que permitiría obtener más información con menos riesgo de error (Aguilera, 2016).

Por lo tanto, es necesario verificar si estos errores existen y si no son falsas alarmas. Aquí es donde aparecen los exploits, los cuales son pequeños fragmentos de código que los crackers utilizan para ingresar a las máquinas de otros. Los auditores deben hacer lo mismo, pero de manera controlada, para causar el menor daño y siempre para asegurar la presencia de estas fallas.

Se debe recordar que todos los programas existentes en el mundo contienen errores porque el hombre no es perfecto. Siempre detecta defectos en cada nueva versión del software que intenten corregir errores de la versión anterior y pueden ser de diferentes tipos, por ejemplo: desbordamiento de búfer, condición de carrera, error de control de variable, etc.

- **Testeo de aplicaciones de internet.**

En este tipo de prueba, se analizan los programas propietarios de la empresa que se analiza, su fiabilidad está controlada, buscará fallos y los explotará. A diferencia de la sección anterior, se debe implementar propios exploits aquí la forma de proceder es demasiado general para ser explicada en esta sección, aunque es interesante ver una herramienta que facilita una actividad, como el marco Metasploit (MSF) (Hadnagy, 2017).

Metasploit Framework es una herramienta para desarrollar y explotar exploits en máquinas remotas, se muestra en la Figura 1.15.

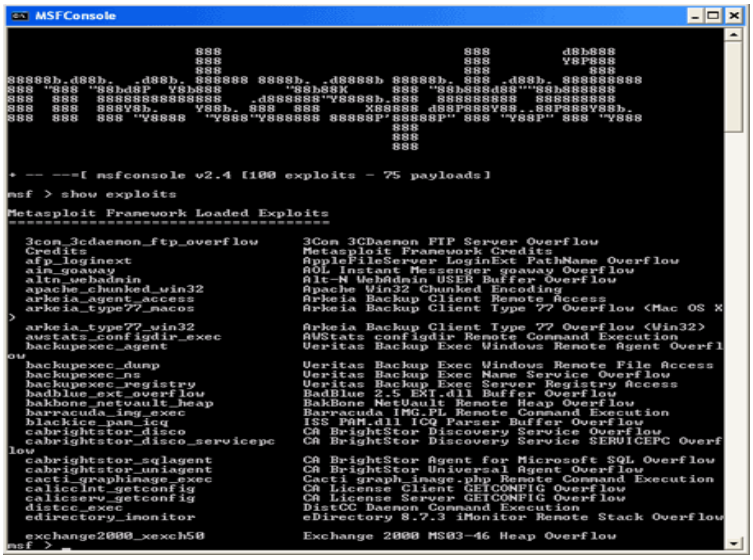

Figura 1.15 METASPLOIT FRAMEWORK
Fuente: (Hadnagy, 2017)

- **Testeo del Router**

En este módulo, se averiguará todo lo posible sobre el enrutador que separa la red de la empresa, el resto del mundo e Internet, se está tratando de determinar qué listas de control de acceso (ACL) son responsables de aceptar o rechazar paquetes (Ortiz & Villegas, 2014), una técnica interesante para lograr esto es Firewalking:

Antes de comenzar a explicar este método, se tiene que señalar las direcciones IP utilizadas son ficticias e internas (aunque este método en realidad se aplica a direcciones IP externas y direcciones IP enrutables). Firewalking es un método que se puede usar para

recopilar información de una red remota que está protegida por un firewall (Pacheco, 2016).

Para comprender esta técnica, es necesario comprender cómo funciona la herramienta Traceroute. Es una herramienta de depuración de red que se utiliza para crear un mapa de todos los hosts que se dirigen a un destino específico. Envíe paquetes UDP o un tipo de eco ICMP al host de destino y aumente gradualmente el TTL en cada turno (de manera predeterminada, una ronda consta de 3 paquetes o muestras). Si utiliza UDP, el puerto de destino se incrementará en uno para cada sonda.

Como se conoce, TTL es un campo de datagramas IP que se utiliza para limitar la cantidad de nodos a los que desea que pase el datagrama antes de que la dirección IP se restaure o regrese a su origen, porque cada vez que va a través de un nodo, se mueve a las unidades. Si incrementa este campo una vez a la vez (la vida útil inicial), devolverá un mensaje de error ICMP tan pronto como la vida útil sea cero. El host saliente sabrá en qué enrutador ha caducado el paquete (Reza, 2016).

Ahora que se conoce cómo funciona traceroute, se puede ver algunos ejemplos del comportamiento del programa en ciertas situaciones. En el primer escenario, tiene una red protegida por un firewall que bloquea todo el tráfico entrante, excepto el ping y su respuesta (ICMP tipo 8 y 0 respectivamente).

En el primer ejemplo, usa los paquetes UDP predeterminados, Figura 1.16.

```
zuul:~>traceroute 10.0.0.10
traceroute to 10.0.0.10 (10.0.0.10), 30 hops max, 40 byte
packets
 1  10.0.0.1 (10.0.0.1)  0.540 ms  0.394 ms  0.397 ms
 2  10.0.0.2 (10.0.0.2)  2.455 ms  2.479 ms  2.512 ms
 3  10.0.0.3 (10.0.0.3)  4.812 ms  4.780 ms  4.747 ms
 4  10.0.0.4 (10.0.0.4)  5.010 ms  4.903 ms  4.980 ms
 5  10.0.0.5 (10.0.0.5)  5.520 ms  5.809 ms  6.061 ms
 6  10.0.0.6 (10.0.0.6)  9.584 ms  21.754 ms  20.530 ms
 7  10.0.0.7 (10.0.0.7)  89.889 ms  79.719 ms  85.918 ms
 8  10.0.0.8 (10.0.0.8)  92.605 ms  80.361 ms  94.336 ms
 9  * * *
10  * * *
```

Figura 1.16 PAQUETES UDP
Fuente: (Reza, 2016)

Como se puede observar, en la Figura 1.16 bloquea los paquetes UDP.

En la Figura 1.17, usamos paquetes ICMP.

```
zuul:~>traceroute -I 10.0.0.10
traceroute to 10.0.0.10 (10.0.0.10), 30 hops max, 40 byte
packets
 1  10.0.0.1 (10.0.0.1)  0.540 ms  0.394 ms  0.397 ms
 2  10.0.0.2 (10.0.0.2)  2.455 ms  2.479 ms  2.512 ms
 3  10.0.0.3 (10.0.0.3)  4.812 ms  4.780 ms  4.747 ms
 4  10.0.0.4 (10.0.0.4)  5.010 ms  4.903 ms  4.980 ms
 5  10.0.0.5 (10.0.0.5)  5.520 ms  5.809 ms  6.061 ms
 6  10.0.0.6 (10.0.0.6)  9.584 ms  21.754 ms  20.530 ms
 7  10.0.0.7 (10.0.0.7)  89.889 ms  79.719 ms  85.918 ms
 8  10.0.0.8 (10.0.0.8)  92.605 ms  80.361 ms  94.336 ms
 9  10.0.0.9 (10.0.0.9)  94.127 ms  81.764 ms  96.476 ms
10 10.0.0.10 (10.0.0.10) 96.012 ms  98.224 ms  99.312 ms
```

Figura 1.17 ICMP
Fuente: (Reza, 2016)

Gracias a esto, se puede verificar que ya se puede acceder a la red y recopilar datos de ella. En el segundo escenario, se observa qué sucede si el firewall bloquea todo el tráfico entrante, excepto el puerto UDP 53, que es DNS.

```
zuul:~>traceroute 10.0.0.10
traceroute to 10.0.0.10 (10.0.0.10), 30 hops max, 40 byte
packets
 1  10.0.0.1 (10.0.0.1)  0.540 ms  0.394 ms  0.397 ms
 2  10.0.0.2 (10.0.0.2)  2.455 ms  2.479 ms  2.512 ms
 3  10.0.0.3 (10.0.0.3)  4.812 ms  4.780 ms  4.747 ms
 4  10.0.0.4 (10.0.0.4)  5.010 ms  4.903 ms  4.980 ms
 5  10.0.0.5 (10.0.0.5)  5.520 ms  5.809 ms  6.061 ms
 6  10.0.0.6 (10.0.0.6)  9.584 ms  21.754 ms  20.530 ms
 7  10.0.0.7 (10.0.0.7)  89.889 ms  79.719 ms  85.918 ms
 8  10.0.0.8 (10.0.0.8)  92.605 ms  80.361 ms  94.336 ms
 9  * * *
10  * * *
```

Figura 1.18 EXCEPCIÓN DE UDP PUERTO 53 PARA DNS
Fuente: (Reza, 2016)

Como puede ver en la Figura 1.18, la ruta de acceso se bloquea durante el octavo salto porque este paso no está permitido, excepto para consultas de DNS, sabiendo esto, se puede desarrollar un plan.

Tiene el control sobre:

- El puerto con el que empezar traceroute (recuerde que irá incrementándose).
- El número de sondas por ronda (3 por defecto).

Además, también conoce el número de saltos hacia firewall, por lo que es fácil deducir:

(puerto_objetivo – (numero_de_saltos * numero_de_sondas)) -1 Por ejemplo: (53 – (8*3)) -1 = 28 (Reza, 2016).

Por lo tanto, si especifica el puerto de salida en 28, cuando se llegue al firewall, los paquetes se enviarán al puerto 53 y permitirán transmitirlos, ejemplo Figura 1.19.

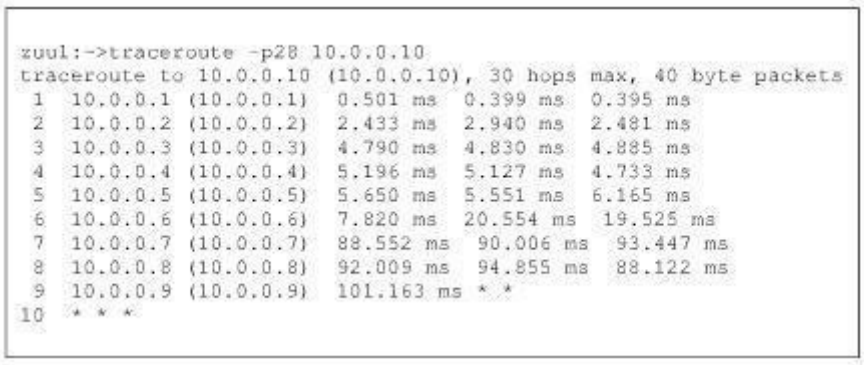

Figura 1.19 TRACEROUTE
Fuente: (Reza, 2016)

Se puede evidenciar que se logró adelantar al objetivo, pero luego quedar atascados porque no permite pasar el tráfico desde un puerto que no sea 53 y traceroute aumenta la puerta. Una solución es modificar el código traceroute para no aumentar el puerto de destino, pero esto está fuera del alcance de este documento. Por ahora, se debe asegurarse de que se conoce que el tráfico enviado al puerto 53 permite pasar y otros bloquean, además, descubrir el próximo host con un firewall.

Ahora comienza el concepto de Firewalking. Para utilizar la respuesta de acceso a la puerta como soporte, se necesita conocer dos cosas:

- Dirección IP del último puerto de acceso frente al firewall
- Dirección IP del host detrás del firewall.

El primero servirá como fuente para las mediciones (en términos de saltos), y el segundo servirá como una dirección para enviar el flujo de paquetes, se puede utilizar un método llamado escaneo de firewall, que nos permitirá saber qué puertos / protocolos permite usar el firewall para superarlos. Para hacer esto, se debe probar cada puerta y esperar respuestas, también puede intentar enviar paquetes a todos los hosts detrás del firewall para tratar de mapear la topología de la red.

A partir de ahí, traceroute limita fuertemente, por lo que presentar una nueva herramienta: Firewall. Su funcionalidad ocurrirá en dos fases, incluyendo la inteligencia y la otra, la exploración, y uno hará esto para encontrar el TTL en el que se encuentra el puerto de acceso, y otra, para realizar el firewall protocol scan (Reza, 2016), Figura 1.20.

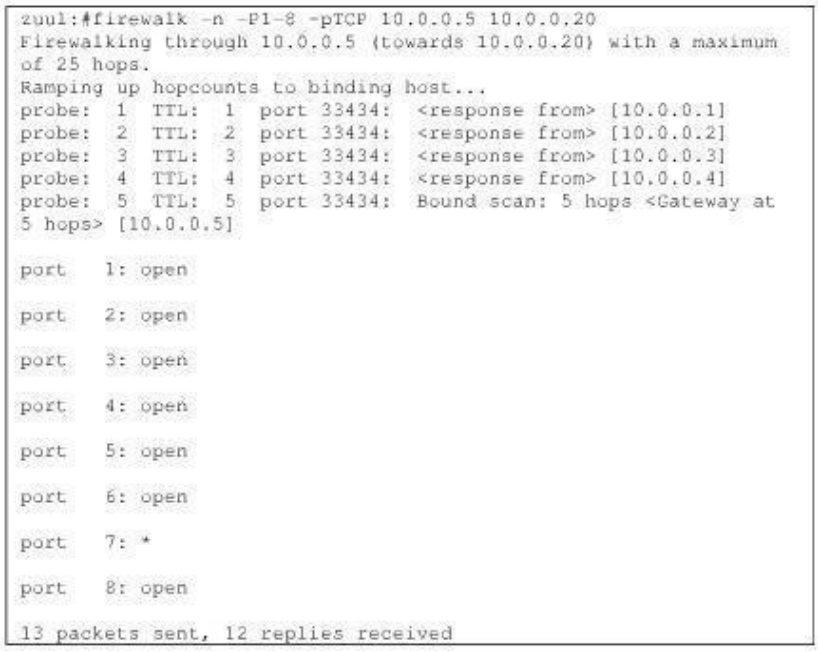

Figura 1.20 FIREWALL PROTOCOL SCAN
Fuente: (Reza, 2016)

- **Testeo de firewall**

Este módulo es muy similar a la prueba del router, los métodos aplicados en el anterior podrían ser aplicables. Este es un estudio adicional de las reglas de firewall, que conoce el 100% de todas las reglas y permite solo lo que es claramente necesario (Zeltser, 2014).

- **Testeo de Sistemas de Detección de Intrusos**

Este módulo es responsable de verificar el correcto funcionamiento de un sistema de detección de intrusos (IDS). IDS es una herramienta informática utilizada para detectar el acceso no autorizado a una red. Estos son programas que escuchan lo que está sucediendo en la red y funcionan de la misma manera que el analizador. Analizan todo lo que pasa por una cierta parte de la red, en busca de tráfico sospechoso, lo que podría conducir a un mal uso de la red. Un malentendido se entiende como un ataque de piratas

informáticos, spam, uso inapropiado de la red por parte de los usuarios, etc (Perramón, 2015).

Una de las características más comunes de IDS es la detección de modelos. IDS incluye una base de datos de patrones (conocidos como firmas) de ataques conocidos. Cuando detecta uno en la red, genera una alarma que permite a los administradores del sistema tomar las medidas adecuadas, por ejemplo, puede ser una política de la compañía que los usuarios de la red no deben visitar sitios pornográficos. Por lo tanto, IDS puede configurarse de manera que cuando detecte la palabra sexo, pornografía, etc., bloquee el acceso.

Con el descubrimiento de patrones en las URL (como en el ejemplo anterior), es interesante comentar sobre un método para evitar que las IDE se utilicen con fines fraudulentos, esto implica el uso de URL confusas.

Sobre sus principales acciones para que pueda ver cómo se puede pasar por alto el IDS, se advierte que los ejemplos que se presentan usarán más direcciones IP que han cambiado mucho, por lo que es posible que estos ejemplos no funcionen.

Una URL oculta es una URL que se ha traducido o confundido para poder engañar o engañar tanto al IDS como a la persona intentará no reconocer esta página web, por ejemplo, por uso fraudulento.

Un ejemplo de una red sin oscurecimiento: http://www.pc-help.org/obscure.htm

La misma red enredada: http: // 3468664375 @ 3468664375 / o% 62s% 63ur% 65% 2e% 68t% 6D (Perramón, 2015).

Como se puede observar, esto es difícil de reconocer y, por lo tanto, es muy probable que su contenido real pueda pasarse por alto y pasar desapercibido antes de que un IDS no esté configurado correctamente.

La parte entre http: // y @ se usa generalmente para la autenticación (como usuario: pass), pero en las direcciones donde no se requiere autenticación, sin importar lo que

coloque, el navegador y El servidor simplemente lo ignorarán. También se puede utilizar para tratar de engañar:

http: //www.upv.es@3468664375/obscure.htm

Esta dirección podría hacerle creer que el sitio es upv.es

La segunda parte (entre @ y la primera página) 3468664375 es la dirección IP que aloja la página web, con la diferencia de que se ha traducido del doble decimal. Esto hace que sea aún más difícil de reconocer. La forma de hacer esto es:

206 * 256 + 191 = * 256 + 158 = * 256 + 55 = 3468664375

Finalmente, tiene una parte entre la primera barra y el final de la URL: / o% 62s% 63ur% 65% 2e% 68t% 6D

Esta parte es equivalente a: /obscure.htm

Lo que se ha realizado aquí es la traducción de algunas letras hexadecimales (base 16) de sus códigos ASCII.

Hay muchas otras formas de hacerlo, desde la más simple hasta la más compleja. Por lo tanto, será interesante hacer esto si quiere pasar desapercibidos bajo un determinado identificador, y algo que tiene que controlar en el IDS que se controla.

- **Testeo de Medidas de Contención**

Este módulo supervisa todas las medidas de respuesta existentes en el sistema para proteger contra virus, troyanos y programas de código malicioso, por lo tanto, cómo se controlan los programas y las políticas del sistema para limpiarlos. Soluciones como aislamiento o cuarentena, copias de seguridad, antivirus (Hadnagy, 2017).

- **Password Cracking**

El descifrado de contraseñas es el proceso de verificar la dificultad de descifrar contraseñas. Se trata de obtener contraseñas, usar errores en el sistema de cifrado o en lugares débiles causados por factores humanos.

En la contraseña introducida se puede distinguir:

- Las contraseñas son demasiado cortas
- Usando la misma contraseña en múltiples sitios
- Utilizar palabras conocidas que existen en los diccionarios.
- Utilice contraseñas compartidas (dios, sol, ra, etc.), que también se pueden encontrar en los diccionarios.
- Utilizar nombre de usuario como contraseña (Nombre de usuario: Paco Pass: Paco).

El tipo de ataque más común que le permite aprovechar estos errores es el uso de ataques de fuerza bruta o un diccionario, cuyo ejemplo se proporciona en la parte técnica del documento (Kennedy, 2015).

Para mejorar la confiabilidad de las contraseñas, se recuerda que evite los errores descritos anteriormente, así como:

- Uso de mayúsculas y minúsculas
- Uso de letras y números.
- Uso de símbolos y acentos.
- Cambio de contraseña regularmente

Si se sigue estas sugerencias, el proceso se ralentizará considerablemente y el tiempo necesario para descifrar la contraseña será innecesario y también intentará acceder al sistema de otras maneras.

En cuanto a los fallos del propio algoritmo de compresión, muchos de ellos se basan en errores matemáticos o puramente criptográficos que van más allá del alcance del

documento, sin embargo, se presenta un ejemplo que se ha comentado, el fallo del MD5 que está documentado en Wikipedia:

Aunque inicialmente se consideró criptográficamente seguro, algunos estudios han revelado vulnerabilidades que hacen que el uso de MD5 sea incierto en el futuro. En agosto de 2004, Xiaoyun Wang, Dengo Feng, Xuejia Lai y Hongbo Yu anunciaron la apertura.

Colisiones de hash para MD5, su ataque fue absorbido en una hora de procesamiento con el cluster IBM P690. Aunque este ataque fue analítico, el hash (128 bits) es lo suficientemente pequeño como para ser vulnerable a ataques de fuerza bruta como el cumpleaños. El Proyecto de computación distribuida MD5CRK se lanzó en marzo de 2004 para mostrar que MD5 no estaba a salvo de dicho ataque, a pesar de que finalizó inmediatamente después de la notificación de la vulnerabilidad (Alonso, 2016).

El equipo de Wang.en conexión con el descubrimiento de métodos simples para generar colisiones hash, muchos investigadores recomiendan reemplazarlos con otros algoritmos, como SHA-1 o RIPEMD-160.

- **Testeo de Denegación de Servicio**

Una denegación de servicio (DoS) es una situación en la que el sistema deja de funcionar correctamente, se colapsa, satura y / o sobrecarga el servicio de la víctima y puede incluso provocar un fallo anormal del sistema, es decir, no obtendrá un beneficio directo de su trabajo inapropiado, sino que simplemente dejará de funcionar correctamente (Aguilera, 2016).

Esta es una situación típica, bastante común, ya que es bastante fácil de provocar, y con frecuencia se lee en la red, para los usuarios de Internet que no están de acuerdo con una decisión tomada por un grupo en particular y llamado DoS.

La denegación de servicio puede ocurrir intencionalmente o por casualidad. Por ejemplo, un servidor web puede estar involucrado en una situación en la que no puede atender a tantos clientes como sea necesario, y esta es una situación absolutamente legítima, sin intención de causar daño.

Se debe recordar que este tipo de control (prueba 2) es muy sensible al daño al sistema. Por tanto, es necesario solicitar la autorización directa de la empresa sometida a prueba. Además, OSSTMM prohíbe estrictamente algunos ataques que causan DoS, como flood o DDos (denegación de servicio dinámica), ya que pueden causar problemas no solo en la máquina que está probando, sino también en los enrutadores. Y sistemas afectados entre el probador y el controlador (Aguilera, 2016).

Un ejemplo simple de ataque DoS es la inyección ARP. Antes de explicar el ataque, debe recordarse en qué se basa el protocolo ARP:

- Solicitud de ARP: la computadora A pregunta a toda la red: "¿Quién tiene esta dirección IP?"
- Respuesta de ARP: la computadora B responde a la computadora A "Tengo esta dirección IP Mi MAC: (MAC)"
- Solicitud de ARP inversa (RARP): el mismo concepto que una solicitud de ARP, pero la computadora A pregunta: "¿Quién tiene esta dirección MAC?"
- Respuesta de RARP: la computadora B responde a la computadora A "Tengo esta dirección MAC, mi dirección IP es: (dirección IP)"

Como resultado, las computadoras pueden comunicarse traduciendo direcciones IP a MAC y viceversa. Esto sucede continuamente, siendo consciente de los cambios existentes (por ejemplo, cada vez que reinicia su computadora). Las solicitudes son aceptadas por todas las computadoras en la red, todos pueden responder, que es la base del ataque.

En el presente estudio se intentará a obligar a la máquina a creer que una dirección MAC específica es una dirección IP inexistente, por lo que no se puede contactar, en el siguiente ejemplo, desde una computadora con Windows, evitará que la computadora víctima se comunique con el enrutador, de modo que quede aislada del exterior para realizar un ataque:

Primero, se necesita saber la dirección MAC del enrutador: C: \> arp -a

Interfaz: 192.168.0.25 --- 0x2

Tipo de dirección física Dirección IP 192.168.0.1 00-09-45-e3-6f-31

Ahora, utilizando un programa llamado Nemesis, envenenará la matriz ARP de la víctima:

C: \ Nemesis \> nemesis arp -D 192.168.0.50 -S 192.168.0.1 -H 00: 01: 02: 03: 04: 05

Introducción del paquete ARP

Con este comando, ha envenenado la tabla ARP de la máquina con la dirección 192.168.0.50, que ahora considera que la dirección MAC del enrutador (con IP 192.168.0.1) tiene una dirección MAC 00: 01: 02: 03: 04: 05. Esto no es correcto, por lo que no puede comunicarse con él (porque no existe).

Esto es solo por un momento, porque, como se mencionó, los mensajes ARP se envían periódicamente. Entonces, en algún momento, el mensaje llegará con la dirección MAC correcta del enrutador. Una forma de evitar que esto suceda es incorporar paquetes hecho hasta ahora, solo en el ciclo:

C: \ Nemesis \> FOR / L% i IN (1, 1500) DO armas-arp -D 192.168.0.50

-S 192.168.0.1 -H 00: 01: 02: 03: 04: 05

Por lo tanto, la computadora de la víctima estará bajo la influencia del DoS, mientras dure el ciclo.

- **Revisión de las Políticas de Seguridad**

Las políticas de seguridad son una versión escrita y documentada de todas las medidas de seguridad de la compañía. Este módulo debe ejecutarse después de tener en

cuenta todas las secciones técnicas y las vulnerabilidades, de lo contrario, los resultados obtenidos aquí no serán comparables a las estrategias de seguridad que se implementarán (Navratilova, 2016).

Primero, es necesario garantizar que las políticas de seguridad basadas en papel se justifiquen tanto dentro de una empresa (por ejemplo, sin utilizar servicios innecesarios) como desde un punto de vista legal y ético. . Se debe prestar especial atención al respeto de las reglas de confidencialidad de los empleados y, además, a todo lo que se considere que cumple con la ley local.

Una de las funciones principales y quizás incluso la más importante es la comparación entre las medidas presentadas en el mapa y las implementadas y vigentes. Por lo tanto, es necesario garantizar que las políticas de seguridad desarrolladas se implementen y configuren correctamente.

CAPÍTULO II. MARCO METODOLÓGICO

2.1.TIPO DE INVESTIGACIÓN

La metodología elegida para la investigación se basa en estudios contrastantes e investigación ejecutiva, los estudios comparativos dan errores en las teorías para eliminar, reparar o aumentar su confiabilidad.

La investigación aplicada se basa en el hecho de que varias aplicaciones tienen teorías en una serie de trabajos que han mejorado su confiabilidad y que existen requisitos de desarrollo en el mundo que se pueden cumplir. Su propósito principal es proporcionar tecnología o planes de acción basados en el conocimiento teórico construido en secuencia, este estudio busca establecer relaciones productivas, creativas y creativas entre las posibilidades del modelo teórico y las necesidades emergentes en la práctica.

Por lo tanto, en la primera fase del proyecto de evaluación, se utilizará un estudio de contraste después de los análisis de los riesgos y vulnerabilidades identificados en la Red LAN de la empresa Hidromag, basado en la metodología OSSTMM. En la segunda parte del proyecto, se utilizará la investigación de implementación, ya que se desarrollarán un conjunto de buenas prácticas para la seguridad de la Red LAN.

Los métodos científicos utilizados en el estudio se pueden destacar:

Métodos lógicos: se utilizó el método analítico-sintético para descomponer la tarea de búsqueda en elementos específicos y definidos individualmente para resolverlos.

Métodos empíricos: el método para analizar la Red LAN de la Empresa Hidromag para identificar los riesgos de seguridad más comunes utilizando la metodología OSSTMM y los principales desafíos en la seguridad de la información.

Método Hipotético-Deductivo: El método deductivo es un procedimiento o camino que sigue el investigador para hacer de su actividad una práctica científica tiene varios pasos esenciales, la observación del fenómeno a estudiar, creación de una hipótesis, verificación o comprobación de la verdad.

Este método permitió la observación y verificación de los avances del desarrollo del sistema de información mediante procedimiento inductivos que permitió precisar los resultados y las conclusiones.

Método Analítico: Es aquel método de investigación que consiste en la desmembración de un todo, descomponiéndole en sus partes o elementos para observar las causas, la naturaleza y nos permite conocer más el objeto de estudio y establecer nuevas teorías.

2.2 TIPOS DE INVESTIGACION

Investigación de Campo: Se trata de la investigación aplicada para comprender y resolver alguna situación, necesidad o problema en un contexto determinado. El investigador trabaja en el ambiente natural en que conviven las personas y las fuentes consultadas, de las que obtendrán los datos más relevantes a ser analizados, son individuos, grupos y representaciones de las organizaciones científicas no experimentales dirigidas a descubrir relaciones e interacciones entre variables sociológicas, psicológicas y educativas en estructuras sociales reales y cotidianas

Investigación Bibliográfica: Es una amplia búsqueda de información sobre una cuestión determinada, que debe realizarse de un modo sistemático, pero no analiza los problemas que esto implica. Aplicaremos este tipo de investigación puesto que proporcionará un conocimiento general de las investigaciones ya existentes, resultados, instrumentos y técnicas usadas en lo que se refiere a construcción de un sistema de información.

2.3 TÉCNICAS DE INVESTIGACIÓN

a. **La Observación:** Es una técnica que consiste en observar atentamente el fenómeno, hecho o caso, tomar información y registrarla para su posterior análisis. Para los investigadores la observación es un elemento fundamental de todo proceso investigativo; en ella se apoya el investigador para obtener el mayor número de datos.
b. **La Encuesta:** Es una técnica destinada a obtener datos de varias personas o de una parte representativa de ella cuyas opiniones impersonales interesan al investigador. La encuesta ayudará a recopilar información mediante un cuestionario de encuesta para conocer el nivel de conocimiento de las personas encargadas de la área de sistemas o seguridad informática.

2.4 RECOPILACION DE LA INFORMACION

La técnica utilizada para la presente investigación, fue la entrevista (ver Anexo 5), considerando que para este tipo de proyectos, se realiza un kickoff para relevar el alcance, limitaciones, entregables, entre otros aspectos.

A continuación se muestra los resultados de la entrevista realizada al Jefe de Sistemas.

Preguntas y Respuestas.

1 Qué tipo de servicio presta su compañía?
La empresa presta servicios de Mantenimiento y venta de equipos hidráulicos.
2 Cómo es la estructura organizacional de su empresa?
La estructura de la compañía es jerárquica donde el área de sistemas le reporta a la Gerencia de Operaciones. El organigrama se puede observar en el anexo…
3 Cuál es su conocimiento sobre riesgos de TI?
El conocimiento del área de Sistemas es moderado es decir conocimiento básico sobre riesgos de TI.
4 A realizado auditorias de tipo seguridad informática en los últimos 3 años?
La respuesta a esta pregunta fue no, y la causa fue falta de presupuesto.

CAPÍTULO III. PROPUESTA

3.1.DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

Este capítulo se desarrolló considerando únicamente 4 de los 16 puntos de la sección C (Seguridad en Tecnologías de Internet) de la Metodología OSSTMM, debido a que muchos de los aspectos no aplican ya que la empresa no dispone de estos campos de evaluación, misma que se describe a continuación (Implementación).

La metodología OSSTMM, fue aplicada en 4 divisiones que son: seguridad de comunicaciones, seguridad de redes inalámbricas, seguridad física y finalmente seguridad de Internet. Como resultado, se realizaron una serie de procesos seleccionados, como se muestra a continuación.

a. Modelo de referencia Red LAN(Implementación)

El modelo de referencia utilizado es TCP/IP, como se puede ver en la Figura 3.1.

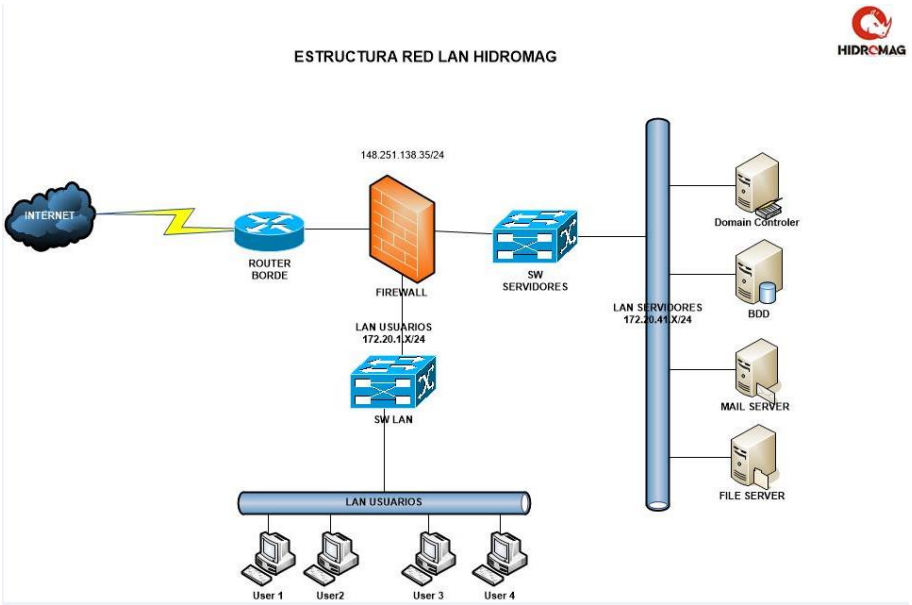

Figura 3.1 LAN HIDROMAG
Fuente: Hidromag

b. Topología.

Hay varias topologías para una LAN. HIDROMAG se caracteriza por el uso de una topología en estrella, con cada tablero de distribución conectado por fibra al nodo central y los conmutadores de acceso conectados a través de un cable UTP con distribución.

La misma topología en estrella se utiliza tanto en el diseño físico como en el diseño lógico.

c. Modelo jerárquico.

Se utiliza el modelo jerárquico tres capas de CISCO.

El Cisco: Catalyst 6500 Core Switch

Distribución: Cisco Catalyst 3550/3560 Switch Model.

Redes Interruptor: 2950/2960.

d. VLANs.

Para garantizar la seguridad de la red local, la VLAN está segmentada, lo que se ha hecho de dos maneras:

- Por la construcción.
- Para el papel del desempeño.

Además, las ACL se han establecido en el conmutador principal, definido por la política para bloquear todos los tipos de acceso predeterminados y permitir el acceso de acuerdo con los requisitos del usuario.

e. Radio

El servidor de autenticación remota del conmutador y el punto de acceso, con características AAA (Autenticación, Autorización y Registro), almacenan la información necesaria para la autenticación del conmutador y los registros de acceso de Radius se almacenan en los registros.

Para obtener información más detallada sobre las características de cada uno de los dispositivos que conforman la red local.

f. Red inalámbrica.

La red inalámbrica es ampliamente utilizada porque garantiza la movilidad de los usuarios. Ha colocado varios puntos de acceso en diferentes partes de la empresa, cada uno configurado de acuerdo con su posición. El método de seguridad implementado en múltiples puntos de acceso es WPA y el resto está abierto, tipo de cifrado TKIP.

g. Voz / IP

Dada la necesidad de implementar y utilizar la red para las comunicaciones de voz, este servicio se implementó utilizando Asterisk, para el cual se configuró un firewall con una lista de control de acceso para la administración.

h. Políticas y procedimientos de gestión de la seguridad.

Acceso.

- **Administración de acceso.**

  Su servidor Radius permite la autenticación de los usuarios de conmutadores y puntos de acceso, pero el conmutador central lo hace localmente.

- **Acceso LAN.**

  Control a través del puerto de seguridad en el nivel de acceso, teniendo en cuenta las direcciones MAC35 conocidas, varias MAC las bloquean. Aunque no todos

los switches tienen esta característica de seguridad porque se ha desactivado o configurado.

- Acceso remoto a la administración del router WAN.
- El acceso remoto a la administración del enrutador de la frontera es a través del protocolo SSH.
- Acceso VPN a servicios.

Para permitir que los usuarios del servicio VPN envíen una justificación para acceder a la cuenta de correo electrónico, cuentaseguridad@hideromag.com.ec, el acceso está permitido o denegado. En caso de autorización, el usuario recibe una contraseña que tiene permiso solo para los servicios solicitados y que está autorizada.

- Tecnología VOICE / IP para la gestión de acceso remoto
- El acceso administrativo al servidor de Asterisk es a través de SSH.
- Acceso VPN a servicios.

Para permitir que los usuarios del servicio VPN envíen una justificación para acceder a la cuenta de correo electrónico, cuentaseguridad@hidromag.com.ec, el acceso está permitido o denegado. En caso de autorización, el usuario recibe una contraseña que tiene permiso solo para los servicios solicitados y que está autorizada.

- **Tecnología VOICE / IP para la gestión de acceso remoto**

El acceso administrativo al servidor de Asterisk es a través de SSH.

Seguridad de la red local.

La política de acceso remoto para la administración del servidor se realiza a través del protocolo SSH seguro del protocolo de Escritorio remoto, en el que las ACL se configuran en el firewall ASA solo para computadoras o servidores DMZ.

Seguridad en el interruptor principal.

El núcleo tiene niveles de seguridad entre 0 y 15, pero se utilizan los siguientes:

- Nivel 14. El soporte técnico del usuario tiene el derecho de manipular ACL.
- Nivel 15. El usuario administrador tiene todos los privilegios.

Niveles de autenticación WAN.

Dos niveles de autenticación se han definido de la siguiente manera:

- Nivel 15. El administrador tiene todos los privilegios.
- Nivel 10. Usuarios como proveedores, administración de producción con derechos para ver configuraciones, pruebas de ping y enrutadores de rastreo.

Niveles de seguridad en el Firewall.

Se han instalado dos niveles de protección.

- Nivel 100: Para el interior.
- Nivel 0: Para exteriores.

Internamente, se utiliza una plantilla para solicitar permisos, que se envía a las cuentas cuentaseguridad@hidromag.com.ec.

i. Plan de emergencia.

En la WAN, extraoficialmente, se tiene un plan de emergencia, pero no se ha documentado, pero tiene conexiones de respaldo. En la red local, no se ha definido formalmente ningún plan de emergencia, pero existen interrupciones de acceso y distribución de respaldo en caso de que se produzca una falla en dicho dispositivo.

En el área de títulos del equipo de administración de seguridad, no hay un plan de contingencia y, aparte de la sala de servidores en UPSI, no hay espacio para el servidor de respaldo. Con respecto a la red inalámbrica, no hay un plan de emergencia documentado, pero si hay un problema con el dispositivo activo, hay otros dispositivos disponibles.

Durante el error del servidor Asterisk, el servidor de respaldo está habilitado, pero Voz / IP no tiene un plan de emergencia documentado.

j. Copia de seguridad.

En la red de área amplia, las copias de seguridad se crean cada 15 días en modo normal o en caso de cambios importantes, por ejemplo: agregar una nueva ruta, etc. Durante este tiempo, el interruptor principal realiza una copia de seguridad semanal del archivo de configuración.

No hay copias de seguridad en los dispositivos inalámbricos porque esto no es necesario debido a la facilidad de encontrar información desde los puntos de acceso. En Asterisk, se realiza una copia de seguridad de un archivo de configuración del servidor cada 3 meses.

k. Documentación.

Documentación para archivos de configuración y diagramas WAN. En la red local, tiene la documentación de configuración del switch. OSSIM y el firewall tienen pautas de administración, mientras que IPS tiene documentación sobre la configuración de Cisco, así como instrucciones para configurar y acceder a las VPN. La red inalámbrica y la voz / IP tienen la misma documentación administrativa.

l. Autenticación.

Cada una de estas comprobaciones de seguridad se autentica localmente en cada servidor. Durante el proceso de autenticación del firewall ASA y el servidor OSSIM, los datos se transmiten en forma cifrada, a diferencia del servidor IME, se transmiten en formato de texto. Con respecto al servicio de voz / IP, la autenticación se realiza localmente, almacenada en un archivo de texto.

m. Actualizaciones.

- Algunos conmutadores de acceso IOS se han actualizado para admitir SSH.
- Hasta hoy, todos los dispositivos en la red WAN no tenían una actualización de iOS. No fue necesario.

- En OSSIM, se escanean parches nuevos o existentes. Si cumplen con los requisitos de compatibilidad, se aplican actualizaciones para mejorar la calidad del servicio.
- IPS actualiza las firmas diariamente.
- Con respecto a la red inalámbrica, no hay una estrategia de actualización, pero cuando se introducen nuevos dispositivos, ya tienen nuevas actualizaciones.
- La voz / IP se ha aplicado al parche de seguridad del cortafuegos y la versión actual de Asterisk es 2.2.12.
- La información mencionada en las secciones anteriores se recopiló entrevistando a los administradores responsables durante la encuesta.
- Además, está la Guía de administración de seguridad de la información, que define todas las estrategias administrativas.

3.2.FACTIBILIDAD TÉCNICA

Considerando la cantidad de información que procesa a diario la Empresa Hidromag es importante se de asegurar que los ataques como la denegación de servicio, permite que el trabajo falle o finalice, o que inicien demasiado tarde, razón por la cual es necesario analizar vulnerabilidades que puede representar la Red LAN de la Empresa Hidromag.

El propósito de este análisis es identificar brechas o puntos críticos en la difusión de la seguridad de la información de la empresa; para la toma de acciones correctivas a ser implementadas que garantizarán el adecuado manejo de la seguridad de la red informática.

3.2.1. FACTIBILIDAD OPERACIONAL

Siempre se debe tener en cuenta que la vulnerabilidad crítica de una empresa ya que ninguna empresa es igual a otra, razón por la cual es necesario proteger los datos de la empresa ya que la rivalidad de las empresas es alta y la adquisición de información confidencial es muy importante para la competencia.

Entorno a lo operacional, el análisis de vulnerabilidad permitirá reducir la efectividad de posibles ataques, una de las áreas clave mencionadas es la seguridad lógica, se utilizarán barreras y se desarrollarán procedimientos de seguridad de la información, como documentos y estándares de políticas; y revisión, que proporciona solo una visión general y una evaluación de estos controles, políticas y estándares.

Cabe señalar que quienes tienen acceso a los resultados, conclusiones y recomendaciones obtenidas a través del análisis, como empleados, administradores, desarrolladores y expertos en control de calidad, tienen un conocimiento básico de los sistemas informáticos; esto se hace para crear o realizar acciones inapropiadas en relación con lo que se necesita.

3.2.2. FACTIBILIDAD ECONÓMICA

Dados los diversos factores mencionados anteriormente, solo las empresas con capital suficiente pueden introducir soluciones de seguridad que incluyen todo lo necesario en este momento y a pesar de la conciencia de la importancia de la seguridad informática; siendo para la Empresa Hidromag importante invertir en este sector.

Por lo tanto, se consideró necesario preparar este análisis para satisfacer esta necesidad, garantizar y mejorar el entorno de seguridad de bajo costo, dándole una dimensión social.

3.2.3. MODELO O ESTÁNDAR A APLICAR

OSSTMM fue creado por Peter Herzog de la organización ISECOM en diciembre de 2000, este manual es el único y más completo estándar de certificación disponible para el desarrollo de pruebas de seguridad en redes y sistemas de internet. Para garantizar que la administración siga siendo relevante, la organización se asegura de que esté al tanto de los nuevos desarrollos en el campo de la seguridad de la tecnología de la información.

OSSTMM es el trabajo del Instituto de Seguridad y Metodología Abierta (ISECOM). ISECOM se compromete a investigar, certificar, capacitar y demostrar integridad en el campo de la seguridad práctica. OSSTMM es una metodología para realizar pruebas de seguridad, dividida módulos y actividades, cada sección está dedicada

al campo que incluye el sistema de información de la organización. El OSSTMM de cada servicio asigna ciertas tareas para determinar los problemas que tienen un impacto significativo en la seguridad de la organización.

OSSTMM servirá como una guía completa de las características clave de la seguridad de la información de la compañía. Como resultado, el personal de auditoría autorizado puede revisar la información relevante relacionada con sus políticas de seguridad, lo que refleja la flexibilidad de la administración.

Para la Evaluación de Riesgos se utilizó Magerit, es una metodología de análisis y gestión de riesgos desarrollada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos asociados con el uso de las tecnologías de la información y la comunicación para implementar medidas de control. Más apropiado para reducir riesgos. Además de esto, tiene un documento completo que contiene métodos y ejemplos sobre cómo realizar el análisis de riesgos.

En particular, MAGERIT se basa en un análisis del impacto que puede tener una brecha de seguridad en una empresa para identificar las amenazas que pueden afectar a la sociedad y las vulnerabilidades que pueden ser explotadas por dichas amenazas, obteniendo así una clara Definición de las medidas preventivas y correctivas más adecuadas.

Una característica interesante de esta metodología es que proporciona una guía completa y pasó a paso sobre cómo realizar un análisis de riesgo. Esta metodología se divide en tres libros. El primero se refiere a un método que describe la estructura que debe tener un modelo de gestión de riesgos, Figura 3.2.

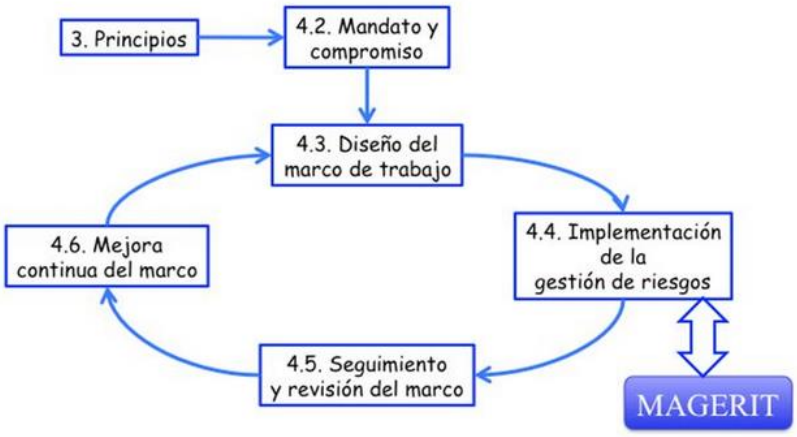

Figura 3.2 ISO 31000 marco de trabajo para la gestión de riesgos
Fuente: Libro I Magerit Versión 3

Las técnicas que recoge son:

- Análisis mediante tablas
- Análisis algorítmico
- Árboles de ataque
- Técnicas generales
- Análisis coste-beneficio
- Diagramas de flujo de datos (DFD)
- Diagramas de procesos
- Técnicas gráficas
- Planificación de proyectos
- Sesiones de trabajo: entrevistas, reuniones y presentaciones

Debe indicarse que el proceso de gestión de riesgos tiene como objetivo identificar y tratar urgentemente los riesgos potenciales, en la Figura 3.3, se puede ver el proceso.

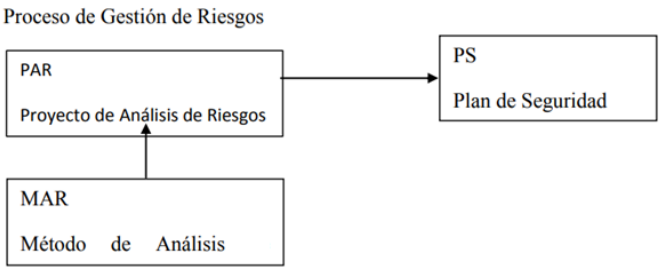

Figura 3.3 Actividades formalizadas
Fuente: Libro I Magerit Versión 3

CAPÍTULO IV. IMPLEMENTACIÓN

4.1.INFORME DE RESULTADOS

Fase I. Creación de perfiles de amenazas basados en recursos.

- Proceso 1. Identificación de la información para el usuario final.
- Proceso 2. Consolidación de información y creación de perfiles de amenazas.

Fase II. Identificar las vulnerabilidades de la infraestructura.

- Proceso 3. Identificación de componentes clave.
- Proceso 4. Evaluación de componentes seleccionados.
- Proceso 4.1 Seguridad en las comunicaciones.
- Subproceso 4.1.1 Prueba de voz / IP.

Determina los niveles de control de intercepción en las comunicaciones.

- Proceso 4.2. Seguridad inalámbrica.

- Subproceso 4.2.1 Prueba de redes inalámbricas [802.11].

    - Evaluar la capacidad de determinar el nivel de control físico del acceso a los puntos de acceso.
    - Evaluar la capacidad de interceptar o interferir con la comunicación.
    - Determina si los puntos de acceso están deshabilitados durante la hora del día cuando no están en uso.

- Proceso 4.3. Seguridad física

- Subproceso 4.3.1 Evaluación de Control de Acceso.

    - Enumera los dispositivos o elementos críticos utilizados por el usuario final. Explora dispositivos y tipos de control de acceso.
    - Determine el nivel de privacidad del dispositivo de control de acceso. Identificar las áreas físicas seguras de la empresa.
    - Explore los dispositivos de control de acceso en busca de debilidades y vulnerabilidades.
- Proceso 4.4. Seguridad en tecnologías de internet.

- Subproceso 4.4.1 Consulta de la red.

    - Definición del sistema para la encuesta. Identificar los puertos abiertos.
    - Determina las direcciones IP de las máquinas de destino. Identificar servicios activos.
    - Tipo de sistema operativo.
- Subproceso 4.4.2 Control de Privacidad.

    - Listas de métodos de recolección de datos.
    - Lista de datos recogidos.
    - Identifique información sobre empleados, organizaciones o materiales que contengan información personal.
- Subproceso 4.4.3 Recuperación de documentos.

        - Recopile las direcciones de correo electrónico personal y empresarial de personas clave.
- Subproceso 4.4.4 Exploración y verificación de vulnerabilidades.

    - Integrar escáneres, herramientas de hacking y exploits de prueba.
    - Mida su organización de destino utilizando herramientas de análisis modernas.
    - Identificar todas las vulnerabilidades relacionadas con la aplicación.
    - Identifica todas las vulnerabilidades del sistema operativo.
- Subproceso 4.4.5 Recursos compartidos.

- Analizar un host con recursos compartidos con seguridad activa e inactiva. Compruebe las contraseñas con fuerza bruta.
- Entra en el coche de la víctima.

- Subproceso 4.4.6 Reingeniería.

  - Busque combinaciones de contraseñas de fuerza bruta en las aplicaciones.
  - Recopilar información confidencial sobre ataques de tipo hombre en el medio.

- Subproceso 4.4.7 Descifrando la contraseña.

  - Consigue un nombre de usuario y contraseña.
  - Utilice las contraseñas obtenidas o sus opciones para acceder a sistemas o aplicaciones adicionales.

- Subproceso 4.4.8. Prueba de denegación de servicio

  - Análisis de la seguridad laboral.

Fase III. Desarrollo de planes y estrategias de seguridad.

- Proceso 5. Análisis de riesgos.
- Proceso 6. Desarrollo de estrategias de protección.

La Figura 4.1 ilustra cada una de las fases, así como los procesos mencionados anteriormente.

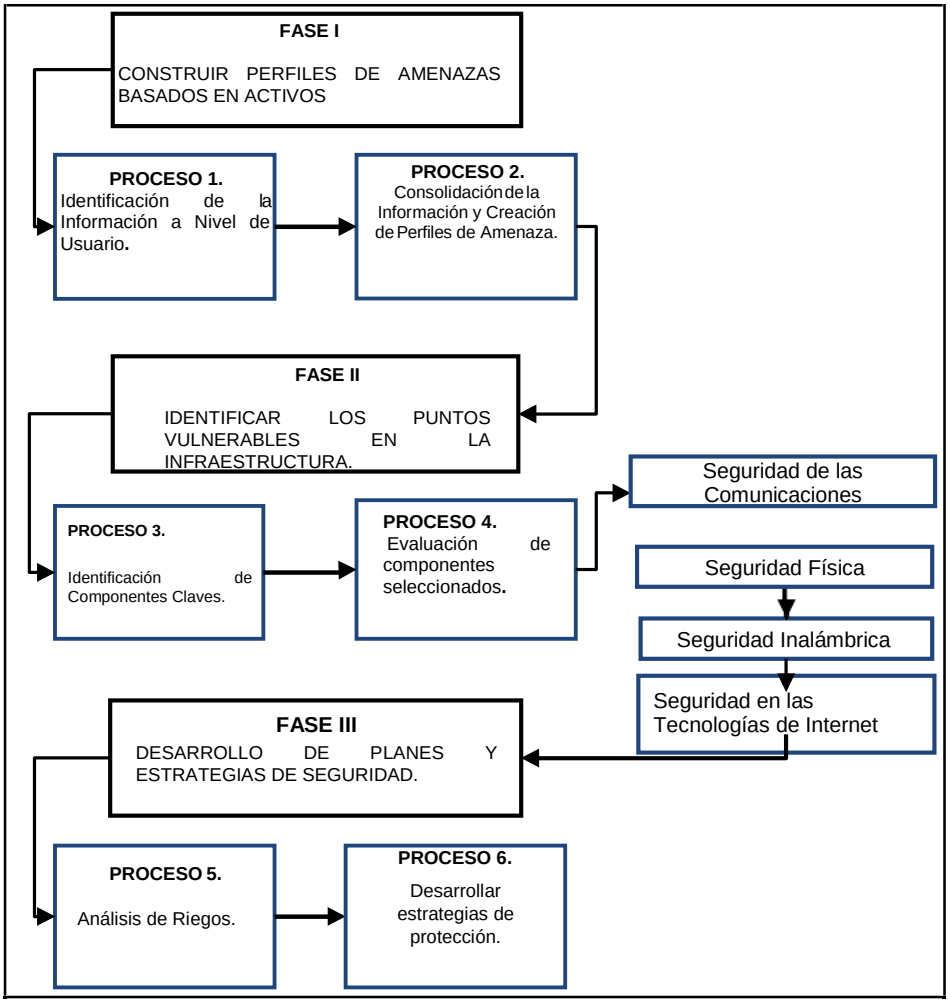

Figura 4.1 Procesos seleccionados

Así como los pasos que deben seguirse para el test de penetración, a partir de la definición de componentes clave, busque vulnerabilidades en las secciones de OSSTMM, tales como: tecnologías de comunicación, física, inalámbrica e internet.

La figura 4.2 ilustra un enfoque metodológico para encontrar vulnerabilidades, incluidas las secciones de seguridad analizadas anteriormente, con las operaciones subsiguientes y la corrección correspondiente. Si la vulnerabilidad no se resuelve, se convertirá en un riesgo potencial y deberá buscar mecanismos de seguridad; de lo contrario, desarrolle la documentación y este ciclo se convertirá en un ciclo recurrente cuando busque otras vulnerabilidades.

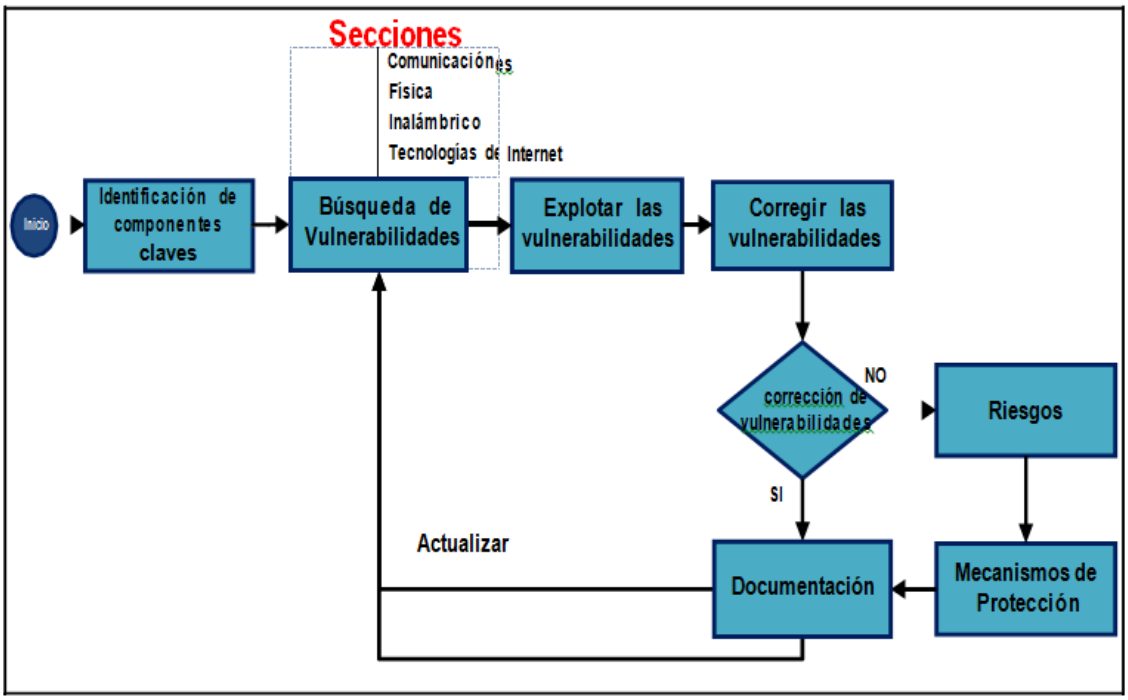

Figura 4.2 Enfoque metodológico

4.2.Aplicación de los procesos

Después de definir los procesos que se utilizarán, se desarrollarán de dos maneras: la primera para los procesos de mapeo, detección y escaneo: puertos, servicios, sistemas operativos y versiones que se ejecutarán en equipos de la empresa, luego aproveche las vulnerabilidades en un entorno de laboratorio controlado en el que todos los servicios, configuraciones generales de equipos académicos y configuraciones especiales adicionales de dispositivos de red activos están disponibles para pruebas de penetración, lo que le ahorra tiempo y esfuerzo durante la prueba, porque si estas modificaciones no se tuvieron en cuenta, la invasión tomará más tiempo, pero es posible; Las pruebas también se realizaron en la red cableada y en la red inalámbrica.

4.2.1 Aplicación de los procesos

Después de identificar los procesos a usar, se desarrollarán de dos maneras: la primera para los procesos de mapeo, detección y escaneo: puertos, servicios, sistemas operativos y versiones se implementarán en el equipo de la empresa, luego explotar las vulnerabilidades del entorno controlado, cuando todos los servicios, la configuración general del equipo y la configuración específica adicional de los dispositivos de red activos están disponibles para la prueba, esto ahorra tiempo y esfuerzo durante la prueba,

porque si estos cambios no se toman en cuenta la invasión durará más tiempo; debe indicarse que las pruebas se realizaron tanto en la red cableada como en la red inalámbrica.

a. Plantilla de los procesos seleccionados

La plantilla descrita a continuación se utiliza para realizar el test de intrusión utilizando la tecnología seleccionada, dividiéndola en fases, la misma que contiene los procesos a seguir.

Tabla 4.4 Plantilla de los procesos seleccionados

FASES	PROCESO
1. Construir perfiles de amenazas basado en activos.	P1. Identificación de la información a nivel de usuario.
	P2. Consolidación de la información y creación de perfiles de amenazas basados en activos.
2. Identificar los puntos vulnerables en la infraestructura.	P3. Identificación de componentes claves.
	P4. Evaluación de componentes seleccionados.
3. Desarrollo de planes y estrategias de seguridad.	P5. Análisis de riesgos.
	P6. Desarrollar estrategias de protección.

Elaborado por: Andrés Narváez

4.2.1.1 FASE I: Construir perfiles de amenazas basados en activos.

Proceso 1. Identificación de la información al usuario final

La empresa Hidromag tiene diferentes tipos de usuarios tales como:

- Empleados.
- Usuario especial: (autoridades, usuario financiero).
- Vendedores.
- Personas externas (Clientes)

Proceso 2: Consolidación de la información y creación de perfiles de amenaza.

Riesgos de los servicios de la red LAN.

Para llevar a cabo este análisis de los riesgos incurridos por los usuarios, los servicios se han clasificado en dos tipos:

- Servicios internos.
- Servicios externos.

La Tabla 4.5 ilustra los servicios internos y externos, incluidos el acceso al entorno, ya que también implica un riesgo.

Tabla 4.5 Arquitectura de los riesgos de la red LAN de la Empresa HIDROMAG

Arquitectura de Riesgos	Servicios	
	INTERNOS	EXTERNOS
RIESGOS	Correo electrónico	Redes sociales
	Entorno virtual de negocios	Mensajería instantánea
	Voz/IP	Programas p2p
	Recursos compartidos	Comercio electrónico
	Sistema de Gestión	Búsqueda de información
	Sistema Financiero BAAN	
	Blogs	
	Acceso al Medio Físico (Wireless, LAN)	

Elaborado por: Andrés Narváez

Los servicios internos son aquellos que la empresa proporciona a los empleados a cambio de servicios externos utilizados por el usuario pero que no son propiedad de la organización.

Estos son todos aquellos que utilizan los servicios de Internet ofrecidos por la red de la organización para llevar a cabo sus actividades diarias; Por este motivo, se consideró importante conocer los riesgos a los que están expuestos, tales como: fraude, robo de información, suplantación de identidad, entre otras cosas, verificación en un entorno de prueba.

4.3 ANÁLISIS DE VULNERABILIDADES OSSTMM

4.3.1 Análisis de vulnerabilidades con los resultados

La prueba de acceso incluyo, pero no estuvo necesariamente restringido a, un acceso mediante los siguientes métodos:

- Ataques de "intrusión" controlados y diagnóstico sobre los sistemas IT, basados en escenarios reales.
- Ataques de "intrusión" controlados y diagnóstico de los servidores y servicios publicados a Internet.
- Metodología "OWASP TOP TEN" para garantizar la cobertura y resultados de todo aquello que se pueda auditar.

Los Resultados de estos procedimientos se reflejan en el anexo 2 y 3. (Informe).

4.3.2 FASE II. Identificar los puntos vulnerables en la infraestructura

Proceso 3. Identificación de componentes claves.

Una vez que se conocen los servicios es importante evaluar los riesgos más importantes al determinar el nivel crítico de cada uno de ellos utilizando una tabla. La Tabla 4.6 examinó cómo clasificar el nivel de criticidad cualitativamente de acuerdo con el porcentaje de exposición al riesgo, por ejemplo, alto, medio y bajo.

Tabla 4.6 Clasificación del nivel de criticidad de los riesgos

NIVEL DE CRITICIDAD	PORCENTAJE DEL IMPACTO DEL RIESGO
ALTO	81% - 100%
MEDIO	61% - 80%
BAJO	50% - 60%

Para determinar el nivel de criticidad de cada riesgo, fue necesario utilizar la tabla anterior, que considera el impacto del riesgo en función de la experiencia del personal que administra estos servicios y el porcentaje de probabilidad que se produce, cabe señalar que estos resultados se centran en la continuidad del negocio y no en los servicios. Además, dependen de la organización y del enfoque propuesto Tabla 4.7.

Tabla 4.7 Evaluación de los riesgos

RIESGO	NIVEL DE CRITICIDAD
Intercepción de las comunicaciones.	MEDIO
Suplantación de identidad.	ALTO
Robo de información/ robo de usuario y contraseña.	MEDIO
Introducción de código malicioso.	MEDIO
Interrupción de las actividades de los servicios.	ALTO
Alteración de la información.	ALTO

Herramientas utilizadas

Las herramientas utilizadas en el pre test son:

Tabla 4.8 Herramientas utilizadas para el pre test

Herramienta	Descripción	Sitio Oficial
Advanced LAN Scanner	Escanea puertos y recursos compartidos.	http://www.radmin.com/products/utilities/lanscanner.php
Arp –a	Comando para ver las tablas de las direcciones físicas y lógicas.	http://www.halcom5.com/web/kb/comandos/comando_arp.html
Autoscan Network	Herramienta para escanear de los hosts de un segmento de red.	http://autoscan-network.com/
Bactrack	Distribución GNU/LINUX para el test de penetración.	http://www.backtrack-linux.org/
Caín & Abel	Herramienta de recuperación de contraseñas.	http://www.oxid.it/cain.html
Ettercap	Herramienta que funciona como sniffer para auditorias de redes LAN.	http://ettercap.sourceforge.net/
LanSpy	Analizador que permite obtener información de todos los ordenadores conectados en la red LAN.	http://lantricks.com/lanspy/index.p hp
Medusa	Permite el ataque de fuerza bruta a diferentes servicios.	http://www.rinconinformatico.net/ataque-de-fuerza-bruta-con- diccionario-usando-medusa
Nbtscan	Recopila información escaneando redes en busca de información acerca del NetBIOS.	http://inetcat.net/software/nbtscan.html

Nessus	Herramienta para el análisis de vulnerabilidades.	http://www.nessus.org/nessus/
Nmap	Herramienta para el escaneo de puertos.	http://www.nmap.org/
Netstat	Muestra las conexiones entrantes o salientes de una computadora.	http://www.alcancelibre.org/staticpages/index.php/como-netstat
Ping	Herramienta para comprobar la conexión entre dos equipos.	http://es.wikipedia.org/wiki/Ping
Smb4k	Programa libre que permite examinar y montar recursos compartidos de la red.	http://www.linux-os.com.ar/linuxos/montar-recursos-samba-en-gnulinux
Wireshark	Herramienta para el escaneo de paquetes.	http://www.wireshark.org/
Xhydra	Herramienta para revisar los recursos compartidos.	http://labs.dragonjar.org/laboratori os-hacking-tecnicas-y- contramedidas-scanning-iii

Riesgos seleccionados

Después de analizar los riesgos y establecer el nivel de criticidad se han seleccionado los siguientes riesgos con el nivel de criticidad ALTO.

- Suplantación de identidad.
- Interrupción de las actividades de los servicios.
- Alteración de la información

Proceso 4. Evaluación de componentes seleccionados

Proceso 4.1. Seguridad en las comunicaciones.

Subproceso 4.1.2 Testeo de Voz / IP.

La tecnología de voz / IP está instalada y disponible en la empresa, algunos usuarios lo utilizan como resultado del uso de los servicios ha aumentado y ha sido necesario implementar esta tecnología para verificar las amenazas.

Identificar los niveles de control de interceptaciones en las comunicaciones.

La intercepción de mensajes se realizó mediante ataques de suplantación de identidad (arp-spoofing), un ataque exitoso porque la configuración del conmutador permitió insertar dos direcciones físicas para la dirección IP y la presencia de la vulnerabilidad fue comprobado, por lo que la aplicación ha sido verificada. La voz / IP debe encapsular la comunicación a través de un protocolo seguro.

Proceso 4.2. Seguridad inalámbrica.

Subproceso 4.2.1 Verificación de redes inalámbricas [802.11].

Para probar la red inalámbrica, se utilizó un punto de control de acceso abierto para analizar las vulnerabilidades detectadas por los puntos de acceso ubicados en oficinas comerciales, financieras y de administración general sin autenticación.

Evaluar la habilidad de determinar el nivel de control de acceso físico a los puntos de acceso.

La mayoría de los puntos de acceso están ubicados en partes visibles por el usuario final, no tienen protección física, lo que los protege contra robos, daños físicos o cualquier otra circunstancia que pueda causar problemas como: pérdidas económica, denegación de servicio, etcétera.

Evaluar la capacidad de interceptar o interferir las comunicaciones.

Se pudo interceptar comunicaciones con usuarios conectados a puntos de acceso abiertos y sin ninguna protección, mientras que en puntos de acceso con protección como WPA, es difícil porque es necesario interrumpir el acceso, primero, los puntos de acceso del sistema de protección para establecer una conexión, y luego realizar la intercepción.

Determinar si los puntos de acceso son apagados durante los momentos del día en los que no son utilizados.

En este punto, fue posible determinar que los puntos de acceso no se deshabilitaron cuando no estaban en uso, por lo que permanecieron conectados al mismo punto de acceso durante el día.

Proceso 4.3. Seguridad física.

Otra parte de OSSTMM es la seguridad física, por ello se consideró necesario analizarlo. Los resultados son evaluados en los siguientes puntos:

Subproceso 4.3.1 Evaluación de controles de acceso.

Enumerar dispositivos o elementos críticos utilizados por el usuario final.

- Impresoras.
- Computadoras.
- Data Centers.
- Copiadoras.

Examinar dispositivos y tipos de control de acceso.

- Sistema de personal (Guardias).
- Sistema de circuito cerrado que incluye alarmas y cámaras.

Examinar dispositivos y tipos de control de acceso.

Las áreas internas de la empresa son seguras, de ahí que se han categorizado de dos formas áreas críticas y no tan críticas, las áreas críticas son:

- Acceso frontal
- Parqueaderos
- Bodega

Y las áreas no tan críticas son

- Departamento Financiero
- Gerencia General
- Área de ventas

Examinar los dispositivos de control de acceso en búsqueda de puntos débiles y vulnerabilidades.

En caso de robo o pérdida de material, la víctima del robo debe comunicarse con la policía para investigar. Si el elemento crítico pertenece a los activos fijos de la empresa, están asegurados para la restauración del dispositivo, de lo contrario no son responsables de daños.

Proceso 4.4. Seguridad en las tecnologías de internet.

Subproceso 4.4.1 Sondeo de red.

Identificar puertos abiertos

La tabla 4.9 indica los puertos, los servicios que corren en este y los protocolos correspondientes:

Tabla 4.9 Servicios, protocolos y puertos más conocidos

Servicio	Puerto	Protocolo
FTP	21	TCP
SSH	22	TCP
TELNET	23	TCP
SMTP	25	TCP
HTTP	80	TCP
HTTPS	443	TCP
POP3	110	TCP
MSRPC	135	TCP
NETBIOS-SSN	139	TCP
MICROSOFT -DS	445	TCP
TERMINAL SERVER	3389	TCP
VNC	5900	TCP

MY-SQL	3306	TCP
SSDP-UPnP	2869	TCP
KERBEROS	88	TCP

Identificar servicios activos

La figura 4.4 muestra el porcentaje final de todas las pruebas de host, donde se definieron los siguientes servicios activos: el servicio con el porcentaje más alto: NETBIOS, seguido de MICROSOFT-DS, el tercer servicio MSRPC, luego establecido en el servidor terminal, luego HTTPS, luego HTTP, con un porcentaje de SSH del 2% y, finalmente, con el 1% de los servicios restantes.

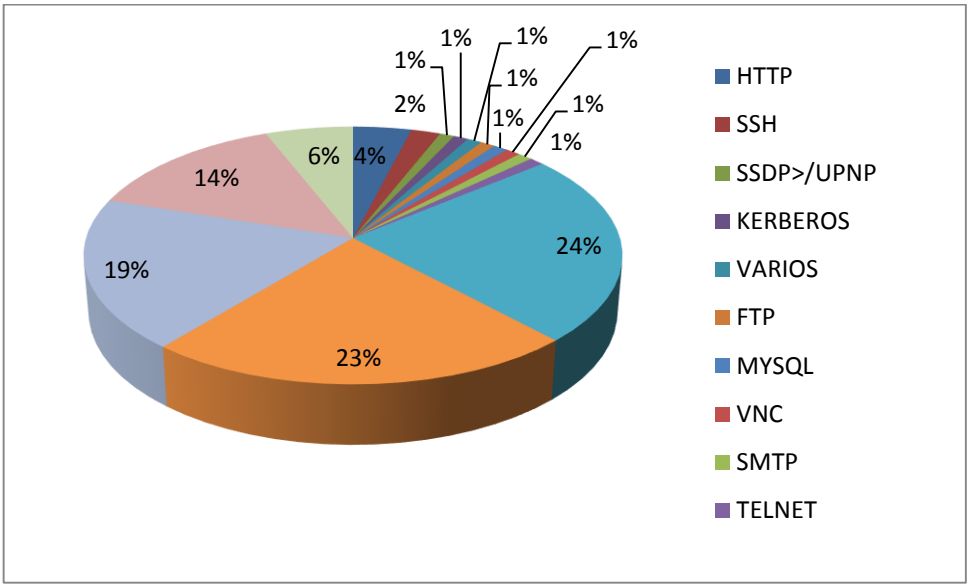

Figura 4.4 Servicios activos en las maquinas escaneadas

IPv6/IPv4.

El análisis se realizó para las direcciones IP4 e IPv6 en la red cableada y en la red inalámbrica. Por lo tanto, es posible determinar la existencia de mecanismos de seguridad eficaces y confiables para IPv4. No hay ningún mecanismo para IPv6.

Tipo de sistema operativo.

La figura 4.5 muestra que el 90% de los sistemas operativos instalaron Windows, el 7% de Linux y el 3% restante de Mac OS, después de analizar los hosts activos.

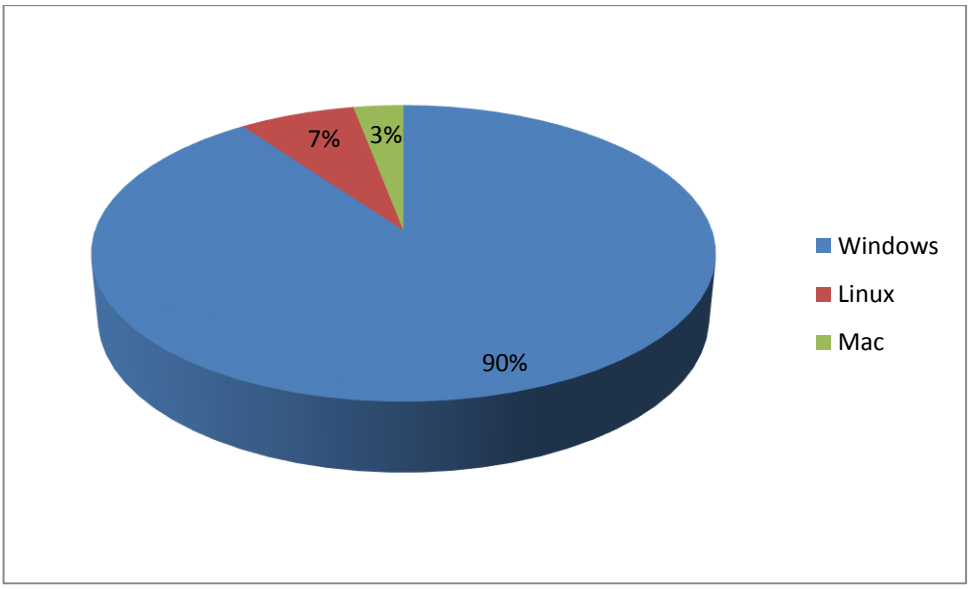

Figura 4.5 Porcentaje de los sistemas operativos

Medir la organización objetivo utilizando herramientas de escaneo habituales actualmente.

Las herramientas utilizadas en el escaneo de la red son:

- Nmap.
- Autoscan-Network.
- Ping.

Identificar todas las vulnerabilidades relativas a los sistemas operativos

Sistemas operativos utilizados: Microsoft, Linux y Mac, cada uno con vulnerabilidades. Windows se encuentra en la parte superior de la lista de los sistemas operativos más vulnerables, como Mac OS y GNU / Linux, según el informe de ESET.

La mayoría de las vulnerabilidades están relacionadas con problemas de seguridad llamados "Día 0".

- **Windows.**

Windows es un sistema operativo universal, el más utilizado por la mayoría de las personas, por lo que se ha vuelto mejor para los ataques. Microsoft ofrece una solución

similar con parches, pero la mayoría de los usuarios no actualizan su sistema operativo ni instalan los parches propuestos, lo que los hace vulnerables a los ataques.

- Susceptible a ataques de hacking
- Vulnerable a ataques de virus.
- Agujeros de seguridad en versiones de los sistemas operativos.
- Tiene en su mayoría programas vulnerables que corren en este sistema operativo.
- Se desarrolla mucho software malicioso.

Linux/Unix.

- Vulnerabilidad de seguridad en la librería libpng de Solaris. Vulnerabilidad de seguridad en Solaris XScreenSaver.
- Vulnerable a ataques de hacking.

MAC OS.

- Aplicaciones instaladas en Mac que son vulnerables a través de detección de pruebas de concepto (PoC) a través de Ransomware con el objetivo de realizar fraudes.
- Creación de troyanos con RealBasic lenguaje de programación.
- Error de Buffer overflow por diferentes aplicaciones como: Google Chrome, Mozilla, OpenBSD.
- Solucionan sus problemas de seguridad en un tiempo considerable.
- Se tuvo un problema de JRE (Java Runtime Enviromment) que podría ser blanco por los intrusos para ejecutar código con solo ingresar a una página web.

Subproceso 4.4.5 Recursos compartidos.

Escaneo host con recursos compartidos con seguridad activa e inactiva.

El escaneo para controlar los recursos compartidos se puede hacer usando la herramienta SMB4K.

Comprobar contraseñas con fuerza bruta.

Los ataques de fuerza bruta se utilizan a menudo para descifrar contraseñas de varias aplicaciones. Puede utilizar muchas herramientas, que se enumeran a continuación.

- Medusa.
- Xhydra.
- Caín & Abel.

Reunir información sensible a partir de ataques hombre-en-el-medio.

Mediante el ataque del hombre-en-el-medio, se puede obtener información confidencial.

Subproceso 4.4.7 Descifrado de contraseña.

Las aplicaciones que se pueden descifrar con contraseñas son aplicaciones que no utilizan ningún tipo de cifrado y las contraseñas asignadas por el usuario son fáciles de descifrar.

Subproceso 4.4.8 Testeo de denegación de servicios.

Análisis de la seguridad de las estaciones de trabajo.

Las estaciones de trabajo pueden tener diferentes métodos de protección, un firewall es una de las tecnologías de seguridad más involucradas que le permite bloquear, filtrar y cerrar puertos, es decir, puede desactivar Servicios que utilizan estos puertos. Otra solución es compartir recursos con seguridad habilitada y finalmente ping de bloqueo.

4.3.3 FASE III. Desarrollo de planes y estrategias de seguridad.

4.3.3.1 Análisis de riesgos.

Es muy difícil considerar la eliminación completa de los riesgos, pero el uso de contramedidas de seguridad puede mitigar y reducir los riesgos, por lo tanto, en riesgo, puede elegir tres opciones: reducirlo, moverlo o aceptar el riesgo. Las diversas pruebas realizadas deberían haber verificado el impacto de los riesgos identificados al principio.

Resultó que todos los riesgos se pueden cubrir de una manera u otra, después de todo, es posible señalar cuáles son los riesgos más probables. La figura 4.6 muestra que el riesgo de interceptar mensajes es el riesgo con mayor probabilidad de ocurrencia (30%), riesgo de robo de datos (25%), cambio de información del 20%, mientras que el riesgo de suplantación del usuario del 15%, el 7% se refiere al riesgo de interrupción de las actividades de servicio y, finalmente, con el 3% de la introducción de códigos maliciosos.

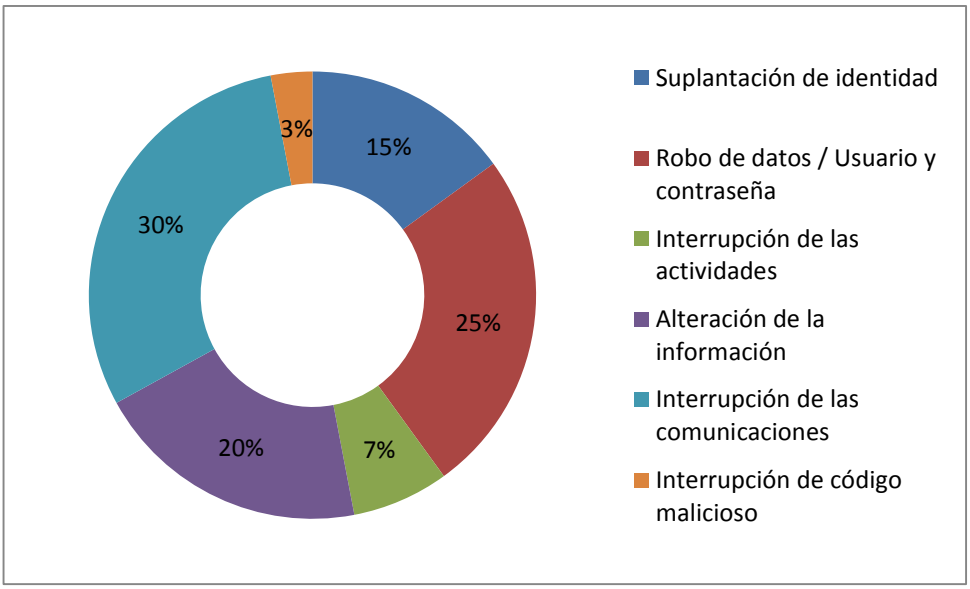

Figura 4.6 Probabilidad de ocurrencia de los riesgos

Las razones de estos riesgos son:

Protocolo ARP

El protocolo ARP no cuenta con autenticación, por lo que dicha vulnerabilidad facilita hacer ataques de hombre en el medio.

Intercepción de la las comunicaciones en la Red Inalámbrica.

Como en cualquier tecnología, existen desventajas y fallas. En una red inalámbrica, es muy difícil evitar la intercepción de mensajes, los paquetes se transmiten a través de ondas de radio; en las redes inalámbricas, este riesgo es inevitable y, lo más importante, la falta de autenticación de la administración y el control del personal.

Cuando los analizadores se utilizan en redes inalámbricas, no se pueden detectar porque los adaptadores configurados están en modo de monitoreo. Los ataques en el medio son otra amenaza, ya que una red inalámbrica sin autenticación facilita la adquisición y el reenvío de sesiones, es imposible detectar la presencia de estaciones cercanas con la misma dirección MAC o IP.

Excesiva confianza o falta de concientización de parte de los usuarios finales.

La mayoría de las personas no toman en serio el riesgo de usar una red local y no toman las medidas de seguridad necesarias para evitar ser atacados y lo más importante, no ahorran en exposición cuando se trata de provocar a algunos de ellos.

No hay presupuesto suficiente destinado a la seguridad informática y falta de apoyo por parte de la gerencia.

Otro problema es que los administradores no asignan un presupuesto suficiente para la seguridad de TI, lo que lo justifica por el hecho de que no es realmente necesario por el momento y que realmente comienzan a darse cuenta, la necesidad de causar daños graves a las funciones de seguridad, como la integridad de la confidencialidad y la disponibilidad.

Seguridad física

Con respecto a las acciones tomadas en caso de pérdida o robo de las computadoras de los estudiantes en la empresa, las medidas correctivas no se distribuyeron oficialmente.

Falta de Políticas enfocadas al usuario final.

Es importante tener en cuenta el problema de la falta de políticas de seguridad orientadas al usuario final.

No se lleva un proceso de ethical hacking de forma periódica.

Lograr el proceso ethical hacking significa actuar activamente contra los ataques, porque no hacerlo rápidamente significa no conocer las vulnerabilidades y amenazas que acechan.

Plan de contingencia inexistente.

La ausencia de un plan de emergencia oficial en todas las áreas, así como aquellos relacionados con la red local, es crucial.

Recursos compartidos sin seguridad habilitada.

En el caso de compartir recursos y la falta de protección, desafortunadamente asumimos diferentes riesgos.

Vulnerabilidades de los sistemas operativos

La administración de la computadora incluye la instalación del sistema operativo independientemente de la distribución (Windows, Linux, Mac OS), pero tiene algunas vulnerabilidades cuando no se realizan actualizaciones o no se realiza la configuración predeterminada ni configurados porque son constantemente acosados.

4.3.4 Desarrollar estrategias de protección.

Implementar varias estrategias de seguridad para la red empresarial es importante y necesario porque identifica diferentes soluciones que generan confianza, por lo tanto, estas soluciones deben evitar amenazas futuras que afecten la imagen y la reputación de la red local de la empresa. Enfatiza en que la manipulación no autorizada de información crítica puede ser invaluable, para proteger una LAN, una empresa debe implementar políticas de seguridad tales como:

- Preventivas.
- Correctivas y
- Detectivas

4.3.4.1 Estrategias de protección preventivas.

Test de intrusión internos periódicamente

Este tipo de estrategia controlará e integrará todos los sistemas de gestión de seguridad de la información implementados en la empresa y combatirá activamente los ataques a los usuarios finales. En relación con el cambio de tecnología, así como la propia organización.

Crear contraseñas robustas y cambiarlas periódicamente

Es importante que los programas o usuarios acuerden crear una contraseña de 6 caracteres como mínimo que no esté asociada con un usuario, ID u otro, para contrarrestar la probabilidad de adivinar la clave. También es importante cambiar la contraseña al menos 3 veces al año.

Ubicación física del punto de acceso.

Identifique puntos de acceso riesgosos en un lugar seguro, fuera de la vista del usuario y con la protección adecuada para protegerse contra robos, caídas, etc.

Instalar un firewall personal.

Es importante que un firewall, una configuración particularmente válida, esté instalado y activado en la computadora.

Instalar un antivirus adecuado.

Un antivirus eficaz y poderoso es necesario para evitar riesgos. Actualmente hay muchos programas antivirus en el mercado, pero debe elegir el que mejor se adapte a sus necesidades.

Defensa en profundidad

En cada nivel de la pila TCP / IP, existe una protección robusta que protege y evita la intrusión fácil de procesos o personas malintencionadas.

Implementar soluciones a nivel de host.

Una solución es implementar la protección contra intrusiones HIPS a nivel de host en las computadoras de los usuarios.

Capacitación a los miembros del equipo de seguridad.

Es muy importante que cada usuario del grupo de seguridad tenga en cuenta el rol y la responsabilidad exclusiva de la seguridad, todo a través de una capacitación adecuada y oportuna.

BCP Plan de Continuidad de Negocio

Un plan de continuidad de negocios implica garantizar que el desastre se gestione de manera efectiva y eficiente, intentando minimizar el esfuerzo, el tiempo y el dinero; Para contrarrestar la continuidad de las actividades, es necesario actualizar e implementar el PCA en la empresa.

Identificación de un plan de seguridad enfocándose al ciclo PDCA.

Este plan de seguridad tiene cuatro fases: "Planificación", "Implementación", "Prueba" y "Acciones". Cada uno de ellos tiene sus propios principios y acciones para implementar, así es como se convierte en un ciclo repetitivo y en un seguimiento continuo.

Escaneador de puertos

Esta herramienta le permite identificar puertos abiertos innecesarios, evitando futuros ataques.

Respaldo de datos

Las copias de respaldo son necesarias para su desempeño, teniendo en cuenta el tiempo y el soporte, evitando así problemas futuros relacionados con la pérdida de información u otros riesgos.

4.3.4.2 Estrategias de protección correctivas

Importancia de la implantación de una política de seguridad de la información en la organización.

La creciente necesidad de las organizaciones de obtener un certificado ISO 27001 para demostrar que las medidas de seguridad se aplican correctamente de acuerdo con la norma internacional, que representa un valor agregado.

Evitar ataques de envenenamiento de ARP

- En el sistema operativo, puede configurar un caché ARP estático o instalar una herramienta para detectar los cambios realizados en la tabla ARP de la computadora, para evitar cualquier actualización sospechosa de la actualización de la tabla ARP desde internet.
- Los 3560 conmutadores de alto rendimiento le permiten configurar la conexión entre la dirección IP-MAC y detectar estos ataques.

- Existen herramientas para monitorear los cambios de estado en la tarjeta de red, es decir, desde el estado normal hasta el modo de monitoreo.
- Para comprender que si es víctima de este tipo de ataque, debe controlar la caché ARP de la computadora, verificando la presencia de dos direcciones IP con la misma dirección MAC.
- Algunos programas antivirus incluyen un método de detección de ataques, que incluye la protección del caché ARP de su computadora.
- La configuración en los conmutadores dinámicos DAI del inspector ARP es responsable de verificar si el paquete entrante llega a través de un puerto inseguro, comparar la tabla de mapeo DHCP y verificar si la dirección IP está asociada con la dirección MAC correspondiente, si la dirección IP no está asociada, deseche y bloquee la puerta.
- Otra solución para este tipo de ataques es implementar IDS / IPS, la segmentación del usuario final y la configuración para detectar ataques de suplantación de identidad de arp.
- Para evitar ataques MIM 46 mediante el uso de la simulación de arp en la red, es conveniente configurar la seguridad del puerto en el conmutador de acceso y ARP WATCH es otra solución.

Voz/IP.

- Cifrado y autenticación del tráfico de voz en la red.
- Instalación de un sistema de detección o prevención de intrusos.

Realizar un plan de contingencia de los servicios críticos

Este plan de contingencia debe incluir todos los elementos críticos de la organización, teniendo en cuenta el impacto en caso de problemas y conocer las alternativas y estrategias.

ISO 27001, 27002 y Sistema de Gestión de la Seguridad de la Información

En la actualidad, la realidad es diferente, la introducción de estándares de seguridad se ha convertido en una necesidad y debe implementarse para proteger los recursos

críticos de la Organización, ya que los datos se convierten en uno de ellos para identificar el Riesgos y proponer soluciones adecuadas. Reducir o eliminar el impacto de los riesgos.

Certificados digitales

El uso de certificados para aplicaciones web es importante y necesario debido a la información que se procesa, ya que sin este mecanismo de seguridad, la información se mueve como texto sin formato. Es necesario informar a los usuarios finales de la importancia de conocer e identificar su origen y autenticidad, para no ser víctimas de ataques utilizando certificados digitales falsos.

Escaneo de Puertos

Es recomendable:

- Habilitar los puertos necesarios.
- Puertos seguros que no se usa con aplicaciones de autenticación.
- ID de host.

Boletines de seguridad que publican en las páginas web oficiales de los sistemas operativos.

Mantenerse al tanto de los boletines de seguridad actuales para conocer las nuevas correcciones de errores y los programas que corrigen las vulnerabilidades en su sistema operativo.

Procesos de concientización.

El proceso de informar a los usuarios finales sobre publicidad, demostraciones, demostraciones, modelado de procesos de seguridad físicos y lógicos de manera oportuna, para que estén listos para ser atacados por intrusos.

4.3.4.3 Estrategias de protección detectivas.

Políticas de seguridad.

Establezca políticas de seguridad físicas y lógicas para el usuario final utilizando la LAN de la empresa para redes cableadas e inalámbricas.

Herramientas Antisniffing

Es fácil obtener herramientas de detección, por lo que es importante usar herramientas de prevención de detección como:

- Sniffdet Linux.
- Prodetect Windows.
- Promise Detect.

Siempre estar actualizados

Tener una cultura de actualización, ya sea el sistema operativo, las correcciones a los programas o las herramientas utilizadas, reduce el riesgo de problemas de seguridad.

Recursos compartidos

Otro tipo de práctica de seguridad invisible implementada en Windows es deshabilitar los recursos administrativos comunes de la red (como C $ y Admin $). Otra forma es compartir el recurso y colocar un signo $ al final del nombre para ocultarlo. No será visible para terceros.

Criptografía

Para evitar ataques de intercepción, se debe usar IPSEC porque lo evita porque cada extremo de la conexión autentica las claves que protegen la conexión.

Realizar auditorías

La auditoría en un momento específico ayudará a mejorar los procesos de seguridad al verificar las debilidades existentes en la red local de una empresa.

Protegerse de los sniffers

Puede usar comandos locales para verificar un comportamiento anormal usando el comando ifconfig ver Figura 4.7 en Linux. El adaptador de red está en modo de monitoreo porque los analizadores utilizan este método de escucha.

Figura 4.7 Ejemplo del comando ifconfig

CONCLUSIONES Y RECOMENDACIONES

5.1.Conclusiones

- Este tipo de proyecto permite actuar de manera proactiva, anticipando los hechos que pueden ocurrir durante el análisis del impacto de los riesgos y el nivel de criticidad, también se ha demostrado que la estrategia actual no es suficiente, si no la combinación del todo. Infraestructura de seguridad con las pruebas. No puede tener un 100% de seguridad, pero el uso de ciertas estrategias de protección proporcionará una protección aceptable de acuerdo con los requisitos de seguridad necesarios.

- Los servicios internos y externos manejados por el usuario final a través de una red local aún están sujetos a una multitud de amenazas de seguridad, el nivel de gravedad determinado por cada uno de los riesgos está determinado por la continuidad de la actividad, y no por un servicio en particular, incluso en el entorno protegido. La experiencia de las personas en contacto con los usuarios finales y la probabilidad de riesgo.

- El principal problema es que la mayoría de los ataques son causados por amenazas internas, como el personal interno, lo que reduce la suposición de que las amenazas externas son la fuente. Si un atacante logra obtener la contraseña de un sistema en particular, podrá acceder a la información del sistema, imitarlos, rechazarle el servicio, en el caso de un usuario tan importante como: el administrador del servidor, los Sistemas informáticos, análisis financiero, científicos, etc. proceder a cualquier intrusión no autorizada.

- El conjunto de métodos, procesos y herramientas utilizados fue el más importante para realizar pruebas de piratería ética, recopilar información y obtener resultados. La mayoría del software es gratuito y está ampliamente disponible en Internet, lo que representa una amenaza para la seguridad.

- Los riesgos anticipados desde el inicio de esta tesis se consideraron ALTOS, pero en el curso y la final se asignaron a las mismas categorías, es urgente tomar medidas de control porque el impacto en caso de aumento, ALTO se convertirá en un problema inesperado. Sin embargo, la mayoría de estos riesgos de intercepción de mensajes, robo/ pérdida de información, robo de identidad e interrupción del servicio a veces se deben a factores humanos causados por negligencia, robo de equipos portátiles, memoria, virus informático, recursos compartidos sin protección, entre otros.

5.2.Recomendaciones

- Se recomienda realizar un análisis exhaustivo de los resultados, sabiendo en particular que el efecto de las estrategias a implementar, a corto, mediano o largo plazo, debe tener en cuenta la comodidad de la seguridad. La seguridad es un conjunto de procesos, no un producto, es recomendable estudiar el plan de acción desarrollado por los responsables de la gestión de la seguridad de la información en la empresa.

- Es importante utilizar herramientas, métodos y procedimientos para evitar, detectar o corregir las vulnerabilidades detectadas y resistir activamente los ataques cibernéticos. Por lo tanto, es recomendable implementar todos los procesos, tecnologías y servicios en la red local porque existe un proceso de exploración de vulnerabilidades para los usuarios finales por lo que se recomienda que ejecute este tipo de proyecto en un entorno de prueba para evitar cualquier interrupción del servicio de producción.

- Debido a los problemas encontrados es importante implementar IDS / IPS para todos los segmentos de red orientados al usuario, para garantizar la seguridad. Se recomienda que reciba información sobre las nuevas herramientas de seguridad disponibles para que puedan actualizar su plan de acción porque las vulnerabilidades y las amenazas aumentan y cambian rápidamente cada día. Uso de la gestión de seguridad con un plan (PLAN-DO-CHECK-ACT).

- Sin embargo, la solución de monitoreo del usuario final sería otra solución extrema para detectar el cumplimiento de políticas, se aplica al tipo de protección

con contraseña, parches de aplicación y versiones del sistema operativo, la actualización antivirus, entre otros, analiza el nivel de cumplimiento de los mismos. Es aconsejable implementar una política orientada al usuario final que se haya desarrollado, es importante utilizar métodos de difusión de políticas como la prensa o la televisión, y lo más difícil es tratar de entender que el personal respeta estas políticas, reducirá un porcentaje. Significativas amenazas ocultas durante la noche y entrenamiento apropiado en el factor humano.

- Además de la aplicación de políticas de seguridad, se recomienda un proceso de auditoría de seguridad porque es importante usarlo porque le permite verificar cómo se implementan las políticas y verificar si cumplen con los requisitos de seguridad, se recomienda la implementación de mecanismos de protección y seguridad para IPv6 y las políticas de seguridad asociadas.

- Se deben utilizar mecanismos de autenticación sólidos para administrar servicios críticos u otros servicios definidos como el rol del usuario para establecer los privilegios asignados a ese rol, pero no como un medio generalmente aceptado para asignar privilegios a un usuario con una dirección IP específica porque la dirección IP puede ser reemplazada.

REFERENCIAS BIBLIOGRÁFICAS

Aguilera, P. (2016). *Seguridad Informática.* Madrid: Editex.

Alonso, M. y. (2016). *Seguridad en las comunicaciones y en la información.* Madrid: Gran Angular.

Chappell, L., & Combs, G. (2016). *Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide.* Reno: Chappell University.

Hadnagy, C. (2017). *Ingenieria Social: El Arte del hacking Personal.* México D.F.: Anaya Multimedia.

Kennedy, D. (2015). *Metasploit The Penetration Tester's Guide.* Boston: H. Moore.

Navratilova, V. (2016). *Llegar a conocer sus servicios de red.* Chicago: Chicago Tribune.

Ortiz, A., & Villegas, R. (2014). *Seguridad de la Información. .* Guatemala: Gautemala.

Pacheco, F. (2016). *Ethical Hacking.* Buenos Aires: Planeta.

Perramón, X. (2015). *Aspectos Avanzados de Seguridad en Redes.* Barcelona: Planeta.

Reza, H. (2016). *Vulnerability Take Grant (VTG): An efficient approach.* Madrid: Elservier.

sadasd. (sdas). *asdas.* sdas: asdsad.

Zeltser, L. (2014). *Malware: Fighting Malicious Code.* New Jersy: Pearson Education.

ANEXOS

Anexo 1 Metodología OSSTMM

Dom. Cien., ISSN: 2477-8818
Vol. 3, núm. mon., agos., 2017, pp. 505-516

REVISTA CIENTIFICA DOMINIO DE LAS CIENCIAS

Metodología OSSTMM para la detección de errores de seguridad y vulnerabilidad en sistemas operativos de 64 bits a nivel de usuario final

Número Publicado el 22 de agosto de 2017

http://dx.doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.505-516
URL:http://dominiodelasciencias.com/ojs/index.php/es/index

Metodología OSSTMM para la detección de errores de seguridad y vulnerabilidad en sistemas operativos de 64 bits a nivel de usuario final

OSSTMM methodology for detecting security and vulnerability errors in 64-bit operating systems at the end user level

Metodologia OSSTMM para detectar erros de segurança e vulnerabilidade em sistemas operacionais de 64 bits no nível do usuário final

[I] Yolanda de la N. Cruz-Gavilanes
yolanda.cruz@cnt.gob.ec

[II] Carlos J. Martínez-Santander
carlos4553@hotmail.com

Recibido: 26 de enero de 2017 * **Corregido:** 13 de marzo de 2017 * **Aceptado:** 18 de julio de 2017

[I] Magíster en Seguridad Telemática, Ingeniera en Electrónica y Telecomunicaciones, Dibujante Técnica, Corporación Nacional de Telecomunicaciones.

[II] Magíster en Seguridad Telemática, Ingeniero de Sistemas, Catedrático de la Universidad Católica de Cuenca

Resumen

El objetivo de la investigación fue aplicar una metodología abierta de testeo de seguridad (OSSTMM) para la detección de errores de seguridad y vulnerabilidad en sistemas operativos de 64 Bits a nivel de usuario final, se recopiló información sobre vulnerabilidades más frecuentes que se presentan en los sistemas operativos Windows de 64 bits, además se experimentó, analizó y se aplicó el Manual de la metodología OSSTMM para solucionar estas vulnerabilidades en los equipos de cómputo, la aplicación de esta metodología se sustenta en cuatro fases de acuerdo a los requerimientos de la investigación como: 1) Levantamiento de la Información, 2) Análisis de vulnerabilidades en sistemas operativos, 3) Evaluación de riesgos, y 4) Capacitación al usuario. En los resultados se detectó un 95% de error de seguridad y de vulnerabilidades en los sistemas Windows de 64 bits que son cometidos por los usuarios finales por su desconocimiento en la configuración y actualizaciones de seguridad que se deben brindar a los sistemas informáticos de Windows de 64 bits, para evitar ser víctimas fáciles de los hackers para el robo y manipulación de equipos y datos. Por lo que se concluyó que los usuarios finales son los causantes de exponer a los equipos de cómputo a errores de seguridad por su ambiguo conocimiento en seguridad informática. Se recomienda para futuros trabajos continuar con la aplicación de la metodología OSSTMM para detectar los errores de seguridad en los sistemas informáticos y capacitar a los usuarios finales que utilizan equipos de cómputo.

Palabras clave: vulnerabilidad; Windows 64 bits; sistemas operativos; usuario final; metodología abierta de testeo de seguridad.

Abstract

The objective of this research work is to apply an Open Source Security Testing Methodology Manual (OSSTMM) for the detection of security and vulnerability errors of operative systems of 64 Bits at a final user level. The information about the most frequent vulnerabilities found in the operative system 64 Bits Windows was collected. Also, the OSSTMM was used, analyzed and applied in order to solve these vulnerabilities on computers. The application of this methodology is sustained on four phases according to the requirements of this work: 1) gathering information, 2) analysis of the vulnerabilities of the system, 3) evaluation of risks, and 4) user training. The results detected 95% of safety error and vulnerability of 64 Bit Windows. The final users, because of ignorance about configuration and safety actualizations, complete these errors. The computer 64 bit windows systems

should have update protection in order to avoid being hacked to steal or manipulate equipment and data. As a conclusion, it could be said that the final users are the ones who cause exposure of the equipment to safety errors and ambiguous knowledge on computer information safety. It is recommended to start applying OSSTMM to detect safety errors on computers and to train the final users to use the computer equipment correctly.

Keywords: vulnerability; Windows 64-bit; operating systems; end user; open security testing methodology.

Resumo

O objetivo da pesquisa foi aplicar uma metodologia de teste de segurança aberta (OSSTMM) para a detecção de erros de segurança e vulnerabilidade em sistemas operacionais de 64 bits no nível do usuário final, informações foram coletadas sobre as vulnerabilidades mais freqüentes que estão presentes em os sistemas operacionais Windows de 64 bits, o Manual de Metodologia OSSTMM também foi testado, analisado e aplicado para resolver essas vulnerabilidades em equipamentos informáticos, a aplicação desta metodologia baseia-se em quatro fases de acordo com os requisitos de pesquisa como 1) Pesquisa de informações, 2) Análise de vulnerabilidades em sistemas operacionais, 3) Avaliação de risco, y 4) Treinamento para o usuário. Os resultados detectaram um erro de 95% de segurança e vulnerabilidade nos sistemas Windows de 64 bits que são cometidos pelos usuários finais devido à falta de conhecimento nas atualizações de configuração e segurança que devem ser fornecidas aos sistemas informáticos do Windows de De 64 bits, para evitar ser fácil vítimas de hackers por roubo e manipulação de equipamentos e dados. Por conseguinte, concluiu-se que os utilizadores finais são responsáveis por expor o equipamento informático a erros de segurança devido ao seu conhecimento ambíguo na segurança informática. Recomenda-se que o trabalho futuro continue com a aplicação da metodologia OSSTMM para detectar erros de segurança em sistemas informáticos e para treinar usuários finais que usam equipamentos de informática.

Palavras chave: vulnerabilidade; Windows 64-bit; sistemas operacionais; usuário final; abra a metodologia de teste de segurança.

Introducción

En la época actual, el desarrollo de las tecnologías de la información ha tenido un salto colosal, la innovación y el crecimiento de las TIC en las organizaciones han repercutido en la mejora de los beneficios, tanto a nivel competitivo como eficiencia, por este mismo hecho se encuentran vulnerables, por cuanto se detectan situaciones de acceso no autorizado a los equipos de cómputo a través de la red, provocando la caída del sistema de forma esotérico, atacando en la confiabilidad, confidencialidad, y autenticad de los archivos que se encuentran en el equipo informático (Song, Hu, & Xu, 2009).

Por otra parte los hackers han aprovechado las configuraciones complejas que hay que realizar a un equipo informático para garantizar su seguridad, además se suma la rapidez con la que se actualiza la tecnología (Mora, 2005).

Los sistemas operativos deben ser valorados por expertos informáticos ya que representan una gran importancia para la información que va a ser almacenada; el sistema operativo es un software que ayuda en la interfaz entre usuario y ordenador (Salah, Calero, Bernabé, Perez, & Zeadally, 2013).

El sistema operativo es el elemento esencial de software de aplicaciones, sin este fundamento seguro las aplicaciones y los sistemas de seguridad no garantizarían la información almacenada (Yile, 2016).

Cuando se tiene entornos de red, la seguridad depende del sistema y de la configuración por parte del usuario que le dé a su computador, sin seguridad en los sistemas operativos no existirán valores confiables y afectará significativamente al sistema (Yile, 2016).

El propósito inicial de esta investigación es abordar las vulnerabilidades que tienen los sistemas operativos Windows de 64 bits en las versiones (XP, Vista, Seven, Eight, Server 2008) y concienciar a los usuarios finales que tienen que asegurar a su sistema informático para no ser víctima de hackeos o robos de información (Aziz & Sporea, 2014) (Liu et al., 2015).

El planteamiento surgió de la aparición de vulnerabilidades dentro de sistemas operativos, esto se debe a la inseguridad que brindan los propios usuarios en sus sistemas al no tener una metodología para detectar errores y problemas.

Tabla 7. Estadística de muestra única

Estadísticas de muestra única

	N	Media	Desviación estándar	Media de error estándar
Nu_Vulnerabilidad	40	4,13	2,323	,367

Fuente: (Cruz Yolanda, 2016)

Tabla 8. Prueba de muestra única

Prueba para una muestra

	Valor de prueba = 4					
					95% Intervalo de confianza para la diferencia	
	t	gl	Sig. (bilateral)	Diferencia de medias	Inferior	Superior
Nu_Vulnerabilidad	,340	39	,735	,125	-,62	,87

Fuente: (Cruz Yolanda, 2016)

Conclusiones

-En este trabajo se analizó las vulnerabilidades de las distintas versiones de Windows que son causadas por los usuarios finales. En particular, para su evaluación de seguridad se utilizó la metodología OSSTM y se realizó unas tablas para cada una de las versiones y se extrajeron las vulnerabilidades y las posibles soluciones que pueden utilizar los usuarios finales, ya que el principal problema de seguridad seguirá siendo el usuario.

-La comparación de las versiones de Windows dio como resultado que la seguridad está más implementada en Windows eight con menos vulnerabilidades que las anteriores.

-Los usuarios finales son el eslabón más débil de la seguridad informática.

- Lo que se detectó en el análisis, es que la institución no le da importancia a la seguridad de los sistemas operativos ya que piensan que es una pérdida de recursos.

Tabla 5. Informe de vulnerabilidades de Windows seven de 64 bits

VULNERABILIDADES DEL SISTEMA OPERATIVO WINDOWS SEVEN DE 64 BITS	
VULNERABILIDAD	**DESCRIPCIÓN**
SMB signing disabled (cifs-smb-signing-disabled)	Configurar this TechNet article
SMB signing not required (cifs-smb-signing-not-required)	Configurar this TechNet article
TCP timestamp response (generic-tcp-timestamp)	deshabilitar TCP desde panel de control
UPnP SSDP Traffic Amplification (upnp-ssdp-amplification)	Restringir el acceso a la función UPnP para activos solamente de confianza
NetBIOS NBSTAT Traffic Amplification (netbios-nbstat-amplification)	Restringiendo el acceso a los netBios solo a servicios activos de confianza

Fuente:(Cruz Yolanda, 2016)

Tabla 4 y tabla 5, muestran que suma menos vulnerabilidades que la versión anterior, pero aun así continúan la inseguridad en los sistemas operativos por el desconocimiento o falta de precaución por parte del usuario, sus propias tablas dan las posibles soluciones.

Tabla 6. Informe de vulnerabilidades de Windows Eight de 64 bits

VULNERABILIDADES DEL SISTEMA OPERATIVO WINDOWS EIGHT DE 64 BITS	
VULNERABILIDAD	**DESCRIPCIÓN**
NetBIOS NBSTAT Traffic Amplification (netbios-nbstat-amplification)	Restringiendo el acceso a los netBios solo a servicios activos de confianza

Fuente: (Cruz Yolanda, 2016)

La tabla 6, demuestra que Windows 8 funciona mejor que las versiones anteriores en lo que a seguridad se refiere, entonces la suma de riesgos de vulnerabilidades es menor, pero a pesar de existir una mínima cantidad, la no configuración por parte del usuario final sería la puerta segura para el ingreso de las atacantes, y robar o manipular la información.

Para comprobar el desconocimiento en seguridad de sistemas operativos, fue necesario la aplicación de la metodología en una importante universidad del Austro que por motivos de seguridad no es posible poner datos de la misma, además se usó un programa estadístico como es SPSS versión 22 con licencia; se aplicó a 40 sistemas operativos en donde independientemente del sistema operativo se anotó el número de vulnerabilidades, y al final se aplicó una prueba z que dio como resultado con un índice de confianza del 95% por tanto un margen de error del 5%, se presenta la comprobación de la hipótesis en el siguiente cuadro.

La tabla 2 muestra las vulnerabilidades que presenta esta versión de Windows Xp, ratificando que existe una debilidad en la seguridad del sistema operativo y en la configuración por parte del usuario final, pero a la vez presenta las soluciones que el usuario puede utilizar o configurar su equipo.

Tabla 3. Informe de vulnerabilidades de windows vista de 64 bits

SOLUCIÓN DE VULNERABILIDADES DEL SISTEMA OPERATIVO VISTA DE 64 BITS	
VULNERABILIDAD	**SOLUCIÓN**
MS09-050: Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517) (windows-hotfix-ms09-050)	Instalar parche desde http://go.microsoft.com/fwlink/?LinkId=163970
MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (windows-hotfix-ms10-054)	Instalar parche desde http://go.microsoft.com/fwlink/?LinkId=190318
MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (windows-hotfix-ms11-020)	Aplicar parche desde http://go.microsoft.com/fwlink/?LinkId=212236
SMB signing disabled (cifs-smb-signing-disabled)	Configurar a partir this TechNet article
SMB signing not required (cifs-smb-signing-not-required)	Restringiendo el acceso a los netBios solo a servicios activos de confianza
ICMP timestamp response (generic-icmp-timestamp)	Deshabilitar ICMP timestamp en el panel de control
TCP timestamp response (generic-tcp-timestamp)	Deshabilitar TCP
NetBIOS NBSTAT Traffic Amplification (netbios-nbstat-amplification)	Restringiendo el acceso a los netBios solo a servicios activos de confianza

Fuente: (Cruz Yolanda, 2016)

La tabla 3 presenta las vulnerabilidades y soluciones de la versión de Windows vista, y se observa que se tomó más en cuenta la seguridad; los usuarios deberían tomar en cuenta la configuración de algunos parámetros.

Tabla 4. Informe de vulnerabilidades de Windows server 2008 de 64 bits

SOLUCIÓN DE VULNERABILIDADES DEL SISTEMA OPERATIVO WINDOWS SERVER 2008 DE 64 BITS	
VULNERABILIDAD	**SOLUCIÓN**
SMB signing disabled (cifs-smb-signing-disabled)	Configurar this TechNet article
SMB signing not required (cifs-smb-signing-not-required)	Configurar this TechNet article
ICMP timestamp response (generic-icmp-timestamp)	Deshabilitar ICMP timestamp en el panel de control
TCP timestamp response (generic-tcp-timestamp)	Deshabilitar TCP
NetBIOS NBSTAT Traffic Amplification (netbios-nbstat-amplification)	Restringiendo el acceso a los netBios solo a servicios activos de confianza

Fuente:(Cruz Yolanda, 2016)

Tabla 2. Informe de vulnerabilidades de Windows Xp de 64 bits

SOLUCIÓN A LAS VULNERABILIDADES DEL SISTEMA OPERATIVO XP DE 64 BITS	
VULNERABILIDAD	**SOLUCIÓN**
Microsoft Server Service / CanonicalizePathName() Remote Code Execution Vulnerability (dcerpc-ms-netapinetpathcanonicalize-dos)	Instalar el parche desde http://download.microsoft.com/download/9/0/b/90b8dbba-09c1-4b27-b0c4-0cc13706823a/Windows2000-KB921883-x86-ENU.EXE
MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687) (windows-hotfix-ms09-001)	Se instala el parche desde http://go.microsoft.com/fwlink/?LinkId=132991
MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468) (windows-hotfix-ms10-012)	Instalar el parche desde http://go.microsoft.com/fwlink/?LinkId=155976
MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (windows-hotfix-ms10-054	Instalar el Parche desde http://go.microsoft.com/fwlink/?LinkId=190318
MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (windows-hotfix-ms11-020)	Instalar el parche desde http://go.microsoft.com/fwlink/?LinkId=212236
CIFS NULL Session Permitted (cifs-nt-0001)	Configurar Microsoft Knowledge Base Article Q246261
MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (windows-hotfix-ms06-035)	Instalar parche desde http://go.microsoft.com/fwlink/?LinkId=64331
SMB signing disabled (cifs-smb-signing-disabled)	Configurar this TechNet article
SMB signing not required (cifs-smb-signing-not-required	Configurar this TechNet article
ICMP timestamp response (generic-icmp-timestamp	Deshabilitar timestamp ICMP a partir del comando de control firewalls de Windows
NetBIOS NBSTAT Traffic Amplification (netbios-nbstat-amplification)	Restringiendo el acceso a los netBios solo a servicios activos de confianza

Fuente:(Cruz Yolanda, 2016)

1) Levantamiento de información de los Sistemas Operativos de 64 bits:

Datos de seguridad que los usuarios finales han dado al equipo como la configuración de firewalls, contraseñas seguras, antivirus e información sobre el tipo de usuario que está a cargo del equipo informático como se observa en la figura 2.

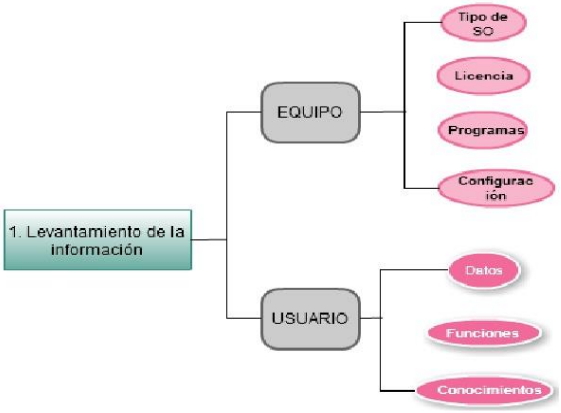

Figura 2. Levantamiento de la información
Fuente: (Cruz Yolanda, 2016)

2) Análisis de vulnerabilidades de Sistemas Operativos

Es donde se evalúan la seguridad del equipo y se recoge las vulnerabilidades que se obtienen al realizar un escaneo y realizar ataques intencionados.

Para observar el rendimiento y seguridad de cada uno de los sistemas operativos en estudio, se construyó tablas para cada versión para mostrar los problemas y soluciones de estimación de seguridad en las diferentes versiones de Windows (Xp, vista, Seven, Eight, y sever 2008).

Además, se aplicó a un cierto número de computadoras en una universidad del Austro, que por motivos de seguridad no es conveniente exponer los datos.

La investigación se centra en dos canales de la metodología OSSTMM que ayudarán a una obtención eficaz de datos, el canal de seguridad físico con la sección humano y el canal seguridad de las telecomunicaciones con la sección redes de datos que tienen sus correspondientes tareas y procedimientos, de acuerdo al canal que está siendo evaluado (López, A., 2011). Además, hace referencia al canal humano debido a que se está trabajando directamente con usuarios finales, que están en directo contacto con un equipo de cómputo, ya que son el eslabón más débil de la seguridad.

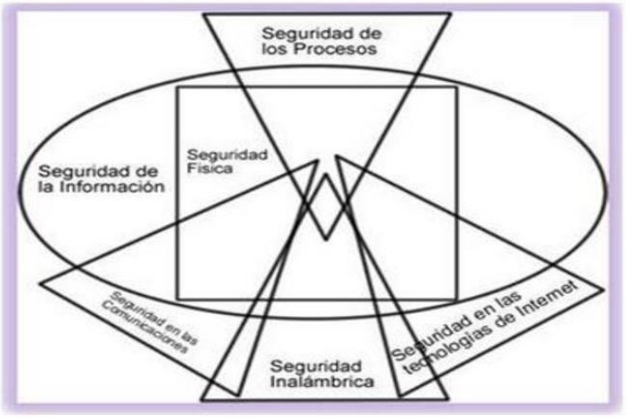

Figura 1 Esquema de la metodología OSSTMM

Fuente: (Prandini & Ramilli, 2010)

Con el fin de evaluar la seguridad de los sistemas operativos, se utiliza la metodología OSSTMM para describir las vulnerabilidades y referirse a sus precondiciones y estimaciones de ataques que puedan afectar el equipo de cómputo, ya que los hacker pueden valorar esa vulnerabilidad y realizar ataques a la información, y continuar con la siguiente vulnerabilidad que encuentre y sabotear todo el sistema.

Resultados

Para obtener los resultados de la investigación se ha evaluado cada uno de los sistemas operativos en estudio y así verificar a eficiencia y seguridad de cada uno de ellos, a través de la utilización de la metodología que se describe a continuación:

La investigación se enfocó en cómo reducir los errores de seguridad y las vulnerabilidades de sistemas operativos Windows de 64 bits a nivel de usuario final, a través de la utilización de una metodología OSSTMM (Herzog, P 2010, p 23).

El creador de la metodología OSSTMM lo definió como una guía para mejorar la seguridad en los equipos informáticos, es así que esta metodología se divide en canales, módulos, ambientes fases según sea la prueba de seguridad que se desea realizar (Herzog, P 2010, p 23). Internacionalmente, la metodología OSSTMM es estandarizada para las buenas prácticas de seguridad para implantación de un sistema de seguridad de información, (Franco, D & Guerrero, C 2013) todos estos canales.

Materiales y métodos

Esta investigación se basa en la utilización de un estudio descriptiva aplicativa fundamentada en la metodología OSSTMM.

La investigación descriptiva sirve para la recopilación de las diversas tendencias y los fundamentos del estudio de la reducción de la vulnerabilidad de seguridad en los sistemas operativos, y la investigación aplicativa permitirá generar criterios sobre la implementación de los diversos procedimientos de detección de errores, para reducir la vulnerabilidad de seguridad en los Sistemas operativos, tomando como fundamento la metodología OSSTMM.

Abarca dos de las áreas o canales que describe la tabla 1 que muestra:

Tabla 1. Canales y secciones de OSSTMM

CANAL	SECCION	DESCRIPCION
Seguridad Física	Humano	Elemento Humano
	Físico	Todo Objeto Tangible
Seguridad de las comunicaciones	Redes de Datos	Sistemas electrónicos y redes de datos
	Telecomunicaciones	Comunicaciones digitales o analógicas
Seguridad del espectro electromagnético	Comunicaciones inalámbricas	Incluyen las señales electromagnéticas

Fuente: (Valdez Alvarado, *I*)