`

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

INSTITUTO DE POSGRADO Y EDUCACIÓN CONTINUA

METODOLOGÍA OSSTMM PARA LA DETECCIÓN DE ERRORES DE SEGURIDAD Y VULNERABILIDAD EN SISTEMAS OPERATIVOS DE 64 BITS A NIVEL DE USUARIO FINAL

Proyecto de Investigación, presentado ante el Instituto de Postgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de

MAGÍSTER EN SEGURIDAD TELEMÁTICA

AUTORA: Yolanda de la Nube Cruz Gavilánez

Riobamba-Ecuador

Marzo-2016

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

INSTITUTO DE POSGRADO Y EDUCACIÓN CONTINUA

MAESTRIA EN SEGURIDAD TELEMATICA

El tribunal de trabajo de titulación certifica **Metodología OSSTMM para la detección de errores de seguridad y vulnerabilidad en sistemas operativos de 64 bits a nivel de usuario final,** de responsabilidad de Yolanda de la Nube Cruz Gavilánez, ha sido minuciosamente revisado por los Miembros del Tribunal de Tesis, quedando autorizada su presentación.

Dr. Patricio Noboa .PhD. **PRESIDENTE**	FIRMA
Ing. Hugo Moreno Avilés .PhD. **DIRECTOR**	FIRMA
Ing. Verónica Mora Chunllo .Mgs. **MIEMBRO**	FIRMA
Ing. Wilson Baldeón López .Mgs **MIEMBRO**	FIRMA
DOCUMENTALISTA **SISBIB ESPOCH**	FIRMA

Riobamba – Ecuador

2016

DERECHO DE AUTOR

Yo **Yolanda de la Nube Cruz Gavilánez soy** responsable de las ideas, doctrinas y resultados expuestos en la presente Investigación, y que el patrimonio intelectual generado por la misma pertenece a la **Escuela Superior Politécnica de Chimborazo.**

_____

FIRMA
0301588513

DEDICATORIA

El trabajo de investigación va dedicada con todo el cariño a mi familia de manera especial a mis padres **Alberto y Magdalena** a mis hijos **Dana, Adrei y Francisco** que me supieron apoyar en todos los momentos, brindándome toda su comprensión en el trayecto para el término de la meta añorada.

Nube

AGRADECIMIENTO

Agradezco a mi dios por llevarme siempre de su mano en este camino que represento arduo, a mis queridos maestros y amigos **Dr. Hugo Moreno, Mgs. Verónica Mora y Mgs Wilson Baldeon** que con sus conocimientos supieron guiarme para el ansiado termino de este trabajo investigativo y a todas las personas que se involucraron en la obtención de la meta ansiada Gracias a todos ellos.

Nube

INDICE

INDICE DE TABLAS

INDICE DE FIGURAS

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 recopilo información sobre vulnerabilidades más frecuentes que se encuentran presentes 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 4) Capacitación al usuario. En los resultados se detecto 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 CLAVES: <VULNERABLIDAD > <WINDOWS 64 BITS > <SISTEMAS OPERATVOS> <USUARO FINAL> < METODOLOGÍA ABIERTA DE TESTEO DE SEGURIDAD [OSSTMM] >

SUMMARY

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. These errors are completed by the final users because of ignorance about configuration and safety actualizations. 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.

KEY WORDS: <VULNERABILITY> <64 BIT WINDOWS> <OPERATIVE SYSTEMS> <FINAL USERS> <OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL [OSSTMM]>

CAPITULO I

1. INTRODUCCIÓN

Al referirnos a seguridad informática es necesario resaltar que ello abarca un tema extenso en todos los sistemas informáticos, es por ello que está investigación, se ha enfocado a los errores de seguridad en los sistemas operativos por parte de los usuarios finales, debido a que la mayoría de errores de seguridad son cometidos por los prenombrados usuarios. En los sistemas informáticos, los errores de seguridad son las debilidades, falta de conocimientos y falta de cultura que tienen los usuarios finales.

Los sistemas operativos desde su origen nacieron con una percepción de inseguridad propia de su diseño aunque en cada sistema operativo que hoy en día sale al mercado sus fabricantes están mitigando las vulnerabilidades que tienen los sistemas operativos. La exposición permanente de los equipos informáticos a posibles autómatas que aplican métodos o técnicas para localizar y aprovechas brechas en los sistemas informáticos, obliga a las instituciones gubernamentales y no gubernamentales, y a todos los usuarios que cuentan con una computadora asumir una adecuada gestión de seguridad, pero el usuario normal quiere seguir siendo usuario y no dedicar tiempo a las fallas de seguridad que se puede presentar en un S.O.

La escalabilidad que han tenido en los últimos años los S.O ha contribuido para ir mejorando los huecos de inseguridad que presentan los sistemas informáticos y que son aprovechados por los Hackers para cometer delitos informáticos, estos delitos en años pasados fueron cometidos por personas que sentían la curiosidad y ego de entrar y manipular ciertas informaciones de algunas organizaciones pero hoy en día son cometidos para ejecutar robos y extorciones es decir buscan sacar provecho de estas vulnerabilidades, es crucial buscar en los sistemas operativos donde situar la seguridad, implantar cada medida como(configurar, dar mantenimiento, concienciar a los usuarios finales) .

El propósito inicial de esta investigación es mitigar las vulnerabilidades que tienen los si temas 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.

El planteamiento surgió por la aparición de vulnerabilidades dentro de un sistemas operativos esto se debe a la inseguridad que brindan los propios usuarios en sus sistemas al no tener una metodología para detectar errores. Es necesario aplicar metodologías como OSSTMM que ayuda a detectar los errores de seguridad, aplicar políticas, que ayudaran a mitigar riesgos, que son identificados de manera positiva, en los SO se amplía como medida de seguridad la utilización de software, antivirus, firewalls en ciertas áreas de la red pero no son cubiertos todos los espacios y dejan abiertos ciertas zonas donde los hackers pueden ingresar y robar información

1.1 Problema de investigación

1.1.1 Planteamiento del problema

Muchas empresas y entes privados, públicos como los ministerios estatales, a nivel internacional invierten una gran cantidad de recursos en lo que respecta o refiere a infraestructura, pues ello les permite mantener protegidos sus equipos informáticos, pero además se esfuerzan en contratar personal de tecnologías de la información especializados en seguridad informática para administrar dicha infraestructura. Sin embargo durante el proceso y la inversión realizada, existe un eslabón que se convierte en la división más débil de la cadena de la seguridad informática que es el usuario final.

Las organizaciones e instituciones tanto privadas como públicas han obviado los problemas serios que sufren los usuarios que poseen un conocimiento escaso de la seguridad informática mientras sus equipos se encuentran enlazadas a Internet. El problema principal de seguridad, radica en que la mayoría de los usuarios es la falta de cultura en tema de seguridad informática, lo cual los hace vulnerables ante la gran diversidad de riesgos y amenazas existentes, aunque el usuario no llega a ser afectado físicamente, si puede verse perjudicado en el aspecto laboral, económico y de su vida privada (GADAE NETWEB, 2015, p.1)

En el tema de seguridad informática el investigador considera que al hablar de vulnerabilidad se refiere a la debilidad que tienen los sistemas informáticos permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad y control de acceso de los Sistemas Operativos, como lo es el software básico de la computadora, provee de una interfaz entre los programas dispositivos hardware y usuario final o la persona que va a manipular de manera directa el software. De esta manera se hace fácil el uso de los dispositivos electrónicos. Las vulnerabilidades de los sistemas operativos se deben a la inseguridad que brindan los propios usuarios en sus sistemas al no tener una metodología para detectar errores y problemas. Es necesario aplicar métodos y políticas de seguridad, los que mitigan los riesgos, que son identificados de manera empírica, como la amplia distribución y utilización de software antivirus, la utilización de firewalls en ciertas áreas de la red pero no son cubiertos todos los espacios y dejan abiertos ciertas zonas donde los hackers pueden ingresar y robar información

Dentro de las tecnologías de la información y Comunicación existen vulnerabilidades que afectan los S.O las mismas que son causadas por el usuario final, el objetivo de la investigación es aplicar la metodología OSSTMM para evitar que el usuario cometa errores de seguridad y los sistemas operativos se encuentren vulnerables (POLICIA CIBERNETICO DE GERRERO, 2014,p.1)

1.2 Formulación del problema

Como Reducir los errores de seguridad y la vulnerabilidades de sistemas operativos Windows de 64 bits a nivel de usuario final a través de la utilización de una metodología OSSTMM.

1.3 Sistematización del problema

¿Cuál es la posibilidad de error del usuario y amenaza de los atacantes sobre las vulnerabilidades de los sistemas operativos Windows de 64 bits?

- ¿Qué sección de la metodología OSSTMM ayudara a la mejora de las vulnerabilidades en los sistemas operativos y disminuir los errores a nivel de usuario final?

- ¿Qué procedimientos de metodología OSSTMM de seguridad se debe tomar en cuenta para evadir vulnerabilidades y disminuir los errores en los S.O a nivel de usuario final?

- ¿Cuáles son los tipos de seguridad que se debe tomar como base para evitar vulnerabilidades en los sistemas operativos a nivel de usuario final?

1.4 Justificación

1.4.1 Teórica

Debido a los errores que pueden causar problemas potenciales en un procesador segmentado aparecen los modelos de seguridad a nivel físico, estos ayudaran a disminuir los errores y detectar sus vulnerabilidades para lo cual se analizara las ventajas de los modelos de seguridad informática existentes y mejorarlo para tener mejor seguridad y evitar riesgos en los sistemas operativos Windows de 64 bits.

La reducción de errores, podría permitir que exista la probabilidad de que un error sea una amenaza, utilizando diferentes políticas, normas, actividades que incluyan la evaluación de errores, estrategias para poder manejarlo y mitigarlo utilizando los recursos disponibles.

El investigador procederá en el presente trabajo investigativo utilizara la metodología OSSTMM (metodología de testeo de seguridad), el objetivo de esta metodología es un test de seguridad minucioso y cabal, los diferentes test son evaluados y ejecutados donde sean aplicables, hasta arribar a los resultados.

El OSSTMM tiene una lista de módulos en un mapa de seguridad los mismos que tienen elementos primarios en cada sección de la metodología, en cada módulo debe incluir todas las dimensiones de seguridad que están integradas con tareas a ser desarrolladas. Para entender mejor una sección es son el modelo total de seguridad dividido en porciones manejables y analizables. El módulo requiere una entrada para ejecutar las tareas del módulo y de otros módulos en otras secciones. Las tareas son los test de seguridad a ejecutarse dependiendo de la entrada del módulo. Los resultados de las tareas pueden ser inmediatamente analizados para actuar como un resultado procesado o se pueden dejar sin analizar esperados, (LÓPEZ LÓPEZ, AGUSTÍN, 2011, p.82)

Para desarrollar el análisis de seguridad OSSTMM de una sección en particular todos los módulos de la sección deben ser desarrollados y para aquellos que no existen infraestructura y no pueden ser verificados debe definirse como NO APLICABLE en la hoja de datos, en base a cada uno de los elementos emitidos anteriormente Se espera obtener resultados de la detección de las vulnerabilidades, (PETE HERZOG, 2003,p.9).

1.4.2 Metodológica

La principal ventaja en la detección de errores es trabajar de manera oportuna para evitar que las vulnerabilidades en los sistemas operativos Windows se concreten.

Entre las metodologías de seguridad para la detección de errores y vulnerabilidades de los sistemas Operativos Windows por parte del usuario final es OSSTMM

La metodología OSSTMM se divide en cinco secciones o ambientes, las que permitirán identificar y enfocar los errores que tienen los sistemas operativos y tomar medidas para evitar posibles inconvenientes. Esta metodología abierta de testeo de seguridad OSSTMM se relaciona directamente con la identificación de errores y vulnerabilidades. Esta investigación se basa exclusivamente en esta metodología OSSTMM 3 en el canal de seguridad, , (PETE HERZOG, 2003,p.23).

Figura 1-1 Esquema de la metodología OSSTMM
Fuente: (PETE HERZOG, 2003, p.23).

1.4.3 Practica

El investigador utilizará un laboratorio en el que se realizaran pruebas de seguridad con sistemas operativos de la familia de Windows utilizando Nessus, Kali Linux, Nexpose Data Sheety otro software especializado en sacar las vulnerabilidades de estos sistemas operativos. Luego de tener las vulnerabilidades se procederá a listar las que son causadas por parte del usuario que en el mayor de los casos es por desconocimiento. Para realizar todas estas pruebas se utilizará la metodología OSSTMM.

1.5 Objetivos

1.5.1 General

Aplicar una Metodología Osstmm para la detección de errores de seguridad y vulnerabilidad en Sistemas Operativos de 64 Bits a Nivel de Usuario Final

1.5.2 Específicos

- Determinar la probabilidad de error y amenaza de nuestro ambiente informático ya que los atacantes conocen las vulnerabilidades de los sistemas operativos Windows como Xp, vista, seven, eight y los server -2008

- Analizar la sección de la metodología OSSTMM ¿que ayudara a la mejora de las vulnerabilidades en los sistemas operativos y reducir los errores de usuario final?
- ¿Proponer criterios en los procedimientos de seguridad para evadir vulnerabilidades en los S.O y disminuir los errores de usuario final?
- ¿Encontrar medidas de seguridad y basarse en ellas para evitar vulnerabilidades en los sistemas operativos a nivel de usuario final?

1.6 Hipótesis

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

CAPITULO II

2. MARCO DE REFERENCIA

Durante la investigación se puede apreciar que muchos entes y empresas privadas y ministerios públicos a nivel internacional, invierten una gran cantidad de recursos en una infraestructura que les permita mantenerse protegidos sus equipos informáticos, así como también se esfuerzan en contratar personal de tecnologías de la información especializados en seguridad informática para administrar dicha infraestructura, Pero se ha dejado de pensar en el eslabón más débil de la cadena de la seguridad informática que es el usuario final, ya que las organizaciones tanto privadas como públicas han ignorado los problemas serios que sufren los usuarios que poseen un conocimiento escaso de la seguridad informática mientras sus equipos se encuentran conectados a Internet.

2.1 Seguridad informática

2.1.1 Antecedentes

La Seguridad Informática suele ser la forma más habitual con la que se refiere a todo aquello que tiene que ver con la seguridad de los computadores y sus sistemas. Hace hincapié en la seguridad de los sistemas, tomando en consideración las amenazas de carácter fundamentalmente tecnológico

La Seguridad Informática es una definición que se dio en tiempos donde no surgía muchos conceptos de celulares, ancho de banda redes móviles, sociales y tiendas virtuales. También hace énfasis en la protección de todo equipo electrónico y su arquitectura dentro de una empresa, pero suele perder su orientación para una organización, en la Figura 1-2 muestra el esquema de seguridad informática (ING. RODRIGO FERRER, 2001,p.1)

.

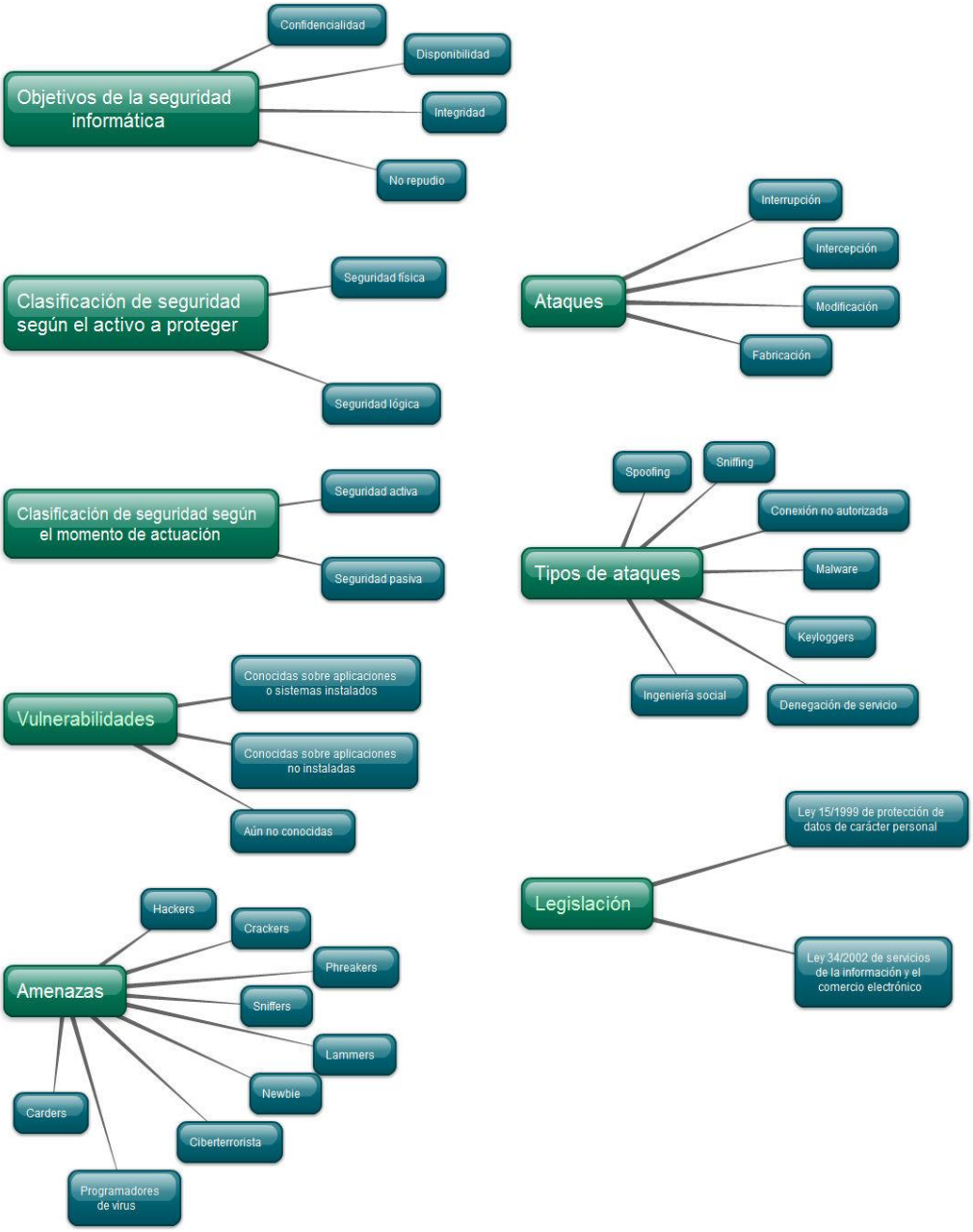

Figura 1-2 Esquema de seguridad informática
Fuente: (VICTOR MAZZACOTE, 2014)

2.1.2 Principios fundamentales de seguridad

La seguridad de los sistemas de información son métodos que evolucionan diariamente, y se centrar en que todas las empresas cumplan con su enfoque de servicio contando con

los cuidados en gestión de riesgos de los sistemas involucrados (JAVIER AREITIO BERTOLÍN, 2008,p.2).

Existen tres (3) principios fundamentales que ineludiblemente integran la seguridad de la información como son Confidencialidad, Integridad y Disponibilidad.

.

Figura 2-2 Fundamentos de seguridad informática
Fuente: (MAZZACOTE, VÍCTOR, 2014)

2.1.2.1 Confidencialidad:

El principio de Confidencialidad, es mantener segura la información privada de personas no autorizadas.

A los datos que son guardados durante su proceso, y transmisión son protegidos confidencialmente para que no sea alterado el mensaje que sale desde el emisor hasta el receptor y llegue el mensaje original lo más recomendable seria que los datos al ser enviados sean encriptados para asegurarse que los datos son confiables (JAVIER AREITIO BERTOLÍN, 2008,p.3).

2.1.2.2 Integridad:

El principio de la integridad se basa en avalar que la información no ha sido modificada por personal no autorizado y así no tener pérdidas en los mensajes.

Cuenta con dos etapas la de integridad de datos y del sistema.

Integridad de datos es el que garantizan que no hayan sido manipulados en el proceso, almacenamiento y envió.

Integridad del sistema garantiza que cuando un sistema realiza su función no está deteriorada ni manipulada sin autorización (AREITIO BERTOLÍN JAVIER, 2008,p.3).

2.1.2.3 Disponibilidad:

Tiene la capacidad de avalar que trabaje puntualmente con rapidez y sin dificultad es decir que el sistema les dé acceso a las personas con autorización. Este principio protege al sistema contra cualquier sabotaje intencional o accidental por parte del personal no autorizado.
Así mismo existen otros principios más generales en seguridad como los siguientes:

2.1.2.4 Privacidad:

Trata de información que puede ser expuesta al público con permiso de las empresas.

2.1.2.5 Seguridad

Son seguridades que se brinda a la información para mantenerla restringida.

2.1.2.6 Datos

Es información procesada

2.1.2.7 Base de datos

Son conjuntos de información de cualquier temática que tienen entre si un vínculo y su meta es ordenarlos en conjunto.

Brinda seguridad en los datos; proporciona consulta de lenguajes, implanta y cambia datos y tiene independencia en los datos.

2.1.2.8 Acceso

Según (PATIÑO SANCHEZ & LAMILLA RUBIO, 2009,p.88), un acceso es la obtención de información guardada en un computador.

2.1.2.9 Ataque

Ataque se define como asalto o la irrupción de información es decir tratar de tomar el control del sistema por parte de intrusos, existen dos tipos de ataque activo y pasivo. Ataque activo es cuando se modifican los datos y pasivo es la divulgación de la información (GAINZA SANCHEZ SABINO ISAO, 2009,p.27).

2.1.2.10 Amenaza:

Es el peligro que podría causar perjuicio a la información estos ya sean naturales humanas o ambientales.

2.1.2.11 Incidente:

Se los llama como sucesos que ocurren en el momento que se da un ataque.

2.1.2.12 Golpe (breach):

Se denomina como la ruptura a las medidas de seguridad (PATIÑO SÁNCHEZ & LAMILLA RUBIO, 2009,p.16)

2.1.3 Niveles de seguridad

Los niveles de seguridad se observaran en la tabla 1-2

Tabla 1-2 Niveles de Seguridad

Nivel	Especificación
Aplicación	-Es lo que ve el usuario -Es el nivel más complejo y menos fiable -La mayor parte de los fraudes ocurren aquí
Middware	-Implica los sistemas de gestión de BD y manipulación de software
Sistema Operativo	-Trata de gestión de archivos y comunicaciones
Hardaware	-es el nivel menos complejo y más fiables -Características de seguridad en el Cpu y en el hardware

Fuente (JAVIER AREITIO BERTOLÍN, 2008, p.5)

2.2 Tipos de seguridad según el activo a proteger

Al hablar de seguridad en informática se conoce diferentes tipos de seguridad como de herramientas de las que están diseñadas o de los ataques que pueden ser expuestos. Existen dos (2) tipos seguridad activa - pasiva y física – lógica.

2.2.1 Seguridad activa y pasiva:

Va a depender de los elementos que se manipulen en seguridad y de cómo operen para utilizar la seguridad activa o pasiva.

2.2.1.1 Seguridad activa

Es toda medida que se toma para detectar amenazas y si se encuentran buscar mecanismos para controlar los problemas, la seguridad activa se puede encontrar en las contraseñas o códigos de acceso, antivirus, firewall (GARCÍA ALFONSO, HURTADO CERVIGÓN, & ALEGRE RAMOS MARÍA DEL PILAR, 2011,p.3)

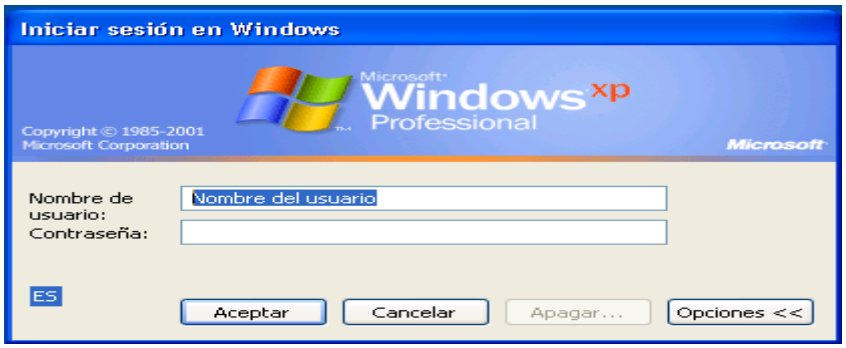

Figura 3-2 Seguridad activa
Realizado Por: (CRUZ, NUBE, 2015)

2.2.1.2 Seguridad pasiva

Son las medidas utilizadas cuando se produce el ataque o el error en la seguridad ayuda que el impacto sea menor y activar mecanismos de recuperación, este tipo de seguridad se encuentra en las copias de seguridad de datos firewall (ALFONSO GARCÍA, CERVIGÓN HURTADO, & MARÍA DEL PILAR ALEGRE RAMOS, 2011,p.6)

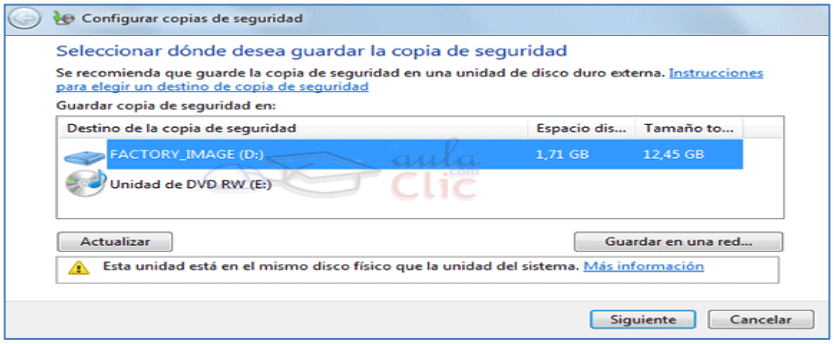

Figura 4-2 Seguridad Pasiva
Realizado Por: (CRUZ, NUBE, 2015)

2.2.2 Seguridad física y lógica

Al hablar de seguridad física y lógica traducimos seguridad material y del software del sistema a continuación se definen los dos términos.

2.2.2.1 Seguridad física

Son muros físicas y mecanismos de control para mantener a salvo los sistemas informáticos, las amenazas físicas pueden ser afectadas por el hombre de manera

accidental, provocada y por causas naturales firewall (ALFONSO GARCÍA, CERVIGÓN HURTADO, & MARÍA DEL PILAR ALEGRE RAMOS, 2011,p.6)

Cuando son provocadas por el hombre existen dos (2) tipos de amenazas:

-**Accidentales** olvido de claves, eliminar archivos de forma accidental.

-**Provocadas** robo de información, hackeo de contraseñas.

Por causas naturales se puede mencionar incendios e inundaciones.

La seguridad física se puede encontrar en la utilización de reguladores de voltaje, personal seguridad, cámaras, alarmas, extintores, climatizadores, disipador de calor, etc.

Figura 5-2 Seguridad Física
Realizado Por : CRUZ, NUBE, 2015)

2.2.2.2 Seguridad lógica

Toma la responsabilidad de mantener seguro todo el software (programas, archivos) del sistema es decir todo lo no físico, se encarga de controlar el acceso no autorizado utilizando redes externas a través de Vpn, ssh, telnet, PPP, PPSP, HTTP, HTTPS, FTP.

Los sistemas operativos están encargados del control de acceso de los usuarios y procesos de los sistemas es así que controlan la seguridad del equipo ya se por error de mal uso del sistema operativo o del usuario por un acceso no controlado como virus espías troyanos phising, el peligro más eminente que le puede venir al sistema es por internet, intercambio de archivos por medio de discos extraíbles (ALFONSO GARCÍA, CERVIGÓN HURTADO, & MARÍA DEL PILAR ALEGRE RAMOS, 2011,p.6)

Para contrarrestar estas amenazas en el sistema operativo informático es usar contraseñas, encriptación de la información, antivirus, cortafuegos.

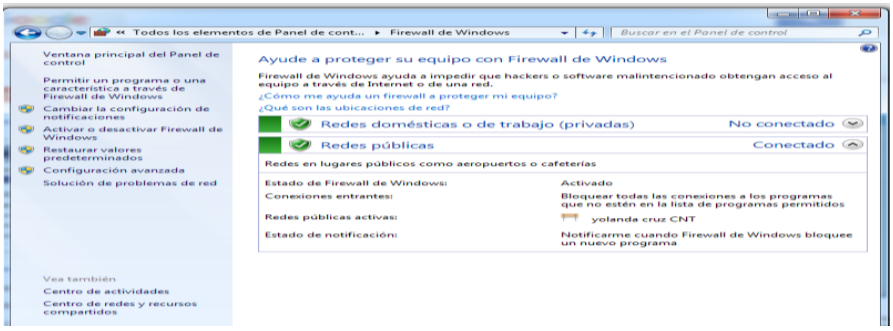

Figura 6-2 Seguridad Lógica
Realizado Por: (CRUZ, NUBE, 2015)

2.3 Seguridad y vulnerabilidades en sistemas operativos

2.3.1 Seguridad en sistemas operativos

Los sistemas operativos se enfocan en tres seguridades iniciando en cómo evitar la pérdida de datos, controlar la confidencialidad de los datos, controlar el acceso a los datos y recursos (YANNETH GUTIÉRREZ, 2013,p.1).

Figura 7-2 Seguridad de los Sistemas Operativos
Fuente: (GUTIÉRRE JANNETH Z, 2013)

La pérdida de datos surge por causa natural o artificial que destruyen los datos (Incendios), a errores del hardware o del software de la computadora (quema del disco duro) o a errores humanos (borrado accidental de archivos) (GUTIÉRREZ YANNETH, 2013,p.1).

Controlar la confidencialidad de los datos se lo solucionar internamente, la base para este control es la distribución de datos, transacciones por medio del internet debido a que se envían los números claves sin encriptarlos por parte de los usuarios finales (GUTIÉRREZ YANNETH, 2013,p.1).

El control del acceso a datos y recursos es la función que pertenece a los sistema operativo, para su control los usuarios no deben acceden a archivos para los que no tienen permisos de acceso, a cuentas de otros usuarios o a páginas de memoria o bloques de disco que contienen información de otros usuarios, para su solución deben ejecutarse test de seguridad; el control de acceso incluye dos problemas: autenticación de usuarios y protección frente a accesos indebidos (GUTIÉRREZ YANNETH, 2013,p.1).

En el ámbito informático, la seguridad equivale principalmente a garantizar al usuario:
•Consistencia: mantener su comportamiento sin cambios inesperados;
•Servicio: debe ofrece de manera confiable, constante y consistente
•Protección: Si un programa tiene errores y sufre una caída, no debe afectar a la ejecución de otros procesos
•Control de Acceso: Los datos generados por un usuario no deben ser accesibles a otro usuario sin autorización.
•Autenticación: El sistema debe poseer los mecanismos necesarios para asegurarse que un usuario es quien dice ser y tiene suficientes privilegios para llevar a cabo todas las operaciones que desee realizar, debe ser capaz de notificar al administrador acerca de cualquier anomalía (GUTIÉRREZ YANNETH, 2013,p.1).

2.3.2 Tipos de seguridad en sistemas

La seguridad de los sistemas operativos se divide:
- seguridad externa
- seguridad operacional que se encuentra dentro de la seguridad externa.

En la Figura 8-2 se evidencia su clasificación

Figura 8-2 Clasificación de seguridad en Sistemas Operativos
Fuente: (Chaparro Henrry, 2015)

2.3.2.1 Seguridad externa

La seguridad externa es la llamada seguridad de SO y consiste en:
-Seguridad física.
-Seguridad operacional.
La seguridad física incluye protección contra desastres y protección contra intrusos, aquí son significativos ciertas detecciones como: detectores de humo y de movimiento, sensores de calor.
Seguridad física evita el ingreso a personas no autorizadas a nivel físico como tarjetas de identificación, sistemas de huellas digitales e identificación por medio de la voz (MAGISTER LA RED MARTINEZ DAVID LUIS, 2001,p.469).

2.3.2.2 Seguridad operacional

Trata de políticas y procedimientos efectuados por la administración de la instalación Computacional, en esta parte se selecciona quien tiene acceso y a qué, además los datos y usuarios son divididos en clases que hace referencia a derechos de acceso, asignación de personal.

Cuando se selecciona al personal se debe dividir y otorgar responsabilidades y no es necesario conocer en su totalidad el sistema si no la responsabilidad, para cumplir con esta meta es el compromiso del personal que ayude a reducir la probabilidad de violar la seguridad, y detectar brechas de seguridad .

El personal debe estar al tanto de que el sistema dispone de controles, pero no cuales a si se reduce la posibilidad de violentarlo; para evitar las violaciones a la seguridad de SO se debe conocer y numerar las amenazas potenciales y estar claro que medidas de seguridad se desea (MAGISTER LA RED MARTINEZ DAVID LUIS, 2001,p.470)

2.3.3 Errores de seguridad en sistemas operativos por parte del usuario

Todos los Sistemas Operativos desarrollados hasta el momento tienen algún error de seguridad y los cuales son cometidos generalmente por los usuarios finales entre ellos tenemos los siguientes.

Uso indebido o malicioso de programas

Son causados por los usuarios por el uso indebido, o malicioso, de programas, estos fallos dan a lugar dos técnicas caballo de Troya y la puerta de atrás.

-*El caballo de Troya* crea programas para que haga cosas no autorizadas en el sistema cuando actúa en el entorno adecuado.

-*La puerta de atrás* consiste en crear un agujero de seguridad al sistema a través de un programa privilegiado que lo permite.

Las puertas de atrás pueden tener varias causas dejarlas a propósito para probar el sistema, para mantener el sistema, se deja encubierto para extraer información sí que el dueño lo sepa (GUTIÉRREZ YANNETH, 2013,p.1).

Usuarios inexpertos o descuidados

Son los más peligrosos ya que pueden borrar archivos no deseados, dejar abiertos los accesos al sistema durante largo tiempo o escribir la palabra clave en un papel junto a la computadora son más frecuentes de lo que parece, este problema se debe tener atención especial por el administrador del sistema.

Usuarios no autorizados

Ciertos SO tienen cuentas para usuarios autorizados, las cuentas tienen contraseñas palabras claves que pueden tener el dueño a estos se le llama súper-usuario porque puede tener acceso a las mismas, y los usuarios pueden dejar esta posibilidad abierta si no tienen la mínima precaución.

El reconocimiento del usuario que se llama autenticación sirve para evitar que usuarios no autorizados accedan al sistema, estas personas piratea, se saltan o rompen procesos con usuarios legítimos y puede hacer todo lo que su identificación falsa le conceda como borrar datos y crearse cuentas verdaderas con identidad falsa o cambiar contraseñas (GUTIÉRREZ YANNETH, 2013p.1).

-*Virus*

Otro error de seguridad que cometen los usuarios finales en los sistemas es la no instalación de antivirus y se inundan de virus que son programas autorreplicables con fines destructivos o de violación de seguridad. Estos necesitan de un programa que los lleve y los traiga para infectar a otros, una infección por un virus puede adoptar dos formas: Comprobación manual de todos los dispositivos de almacenamiento para limpiarlos del virus y la creación de un antídoto que también se propague y limpie el virus (Janneth Gutiérrez, 2013,p.1).

-*Gusanos*

Es un programa pequeño que tiene dos partes el uno es un cargador que, una vez compilado y ejecutado en el sistema destino, carga el gusano principal, y el error más común de los usuarios es abrir cualquier tipo de programa desconocido en donde vienen anclados los gusanos. El gusano lee las tablas de encaminamiento del sistema infectado y enviaba el cargador a todos los sistemas remotos que podía, usando para ello tres mecanismos de penetración:

- Intérprete de mandatos remoto (rsh).
- Demonio del finger.
- sendmail.

Con estos mecanismos, el gusano provocó la caída de miles de computadoras en la red, antes de ser detectado y eliminado, e problema de los gusanos no es que sean destructivos, que la mayoría no lo son, sino que colapsan las redes de comunicaciones (GUTIÉRREZ YANNETH, 2013, p.1).

-*Rompedores de sistemas de protección*

Estos programas llevan a cabo distintas pruebas sobre sistemas, generalmente remotos, para tratar de romper la seguridad de los mismos y poder ejecutar accesos ilegales. Para ello prueban con los mecanismos que dieron fallos de seguridad anteriormente en virus y gusanos: intérpretes de mandatos remotos, ftp anónimo, finger, etc.

Un error común de usuarios finales es tener sus claves con nombres comunes y conocidos (GUTIÉRREZ YANNETH, 2013,p.1).

-*Bombardeo*

Un ataque de seguridad con mucho éxito en Internet es el que consiste en llevar a cabo bombardeos masivos con peticiones de servicio o de establecimiento de conexión a un servidor determinado. Estos ataques masivos provocan que el servidor deniegue sus servicios a los clientes legales y pueden llegar a bloquear al servidor.

Para lograr que estos ataques tengan éxito, los atacantes se enmascaran con las direcciones e identidades de otros usuarios (spoofing) y llevan a cabo los ataques desde múltiples clientes.

Un usuario descuidado, o malicioso, que cree procesos de forma recursiva y sin límite colapsará el sistema continuamente. Para evitarlo, los usuarios finales deben poner límites, siempre que sea posible, a los recursos que cada usuario puede tener simultáneamente (número de procesos, impresoras, etc.) (GUTIÉRREZ YANNETH, 2013, p.1).

*Firewalls***.** Un firewall ayuda a prevenir que la información entre o salga de su computadora sin su permiso. Lo ayuda a que usted sea invisible en Internet y bloquea las comunicaciones de fuentes no autorizadas.

Algunos sistemas operativos ya vienen con firewalls de software como es el caso de windows. Los usuarios finales deberían dejar el firewall de Windows activado a menos de que lo reemplace con otro firewall de software, pero son errores comunes ya que deben configurar apropiadamente (GUTIÉRREZ YANNETH, 2013,p.1).

2.3.4 Antecedentes de vulnerabilidades de sistemas operativos

Hace cinco (5) años especialistas en seguridad informática encontraron problemas de seguridad en SO (SANS) así como las vulnerabilidades que son aprovechadas por los gusanos y virus que afectan exclusivamente a los ordenadores que utilicen el sistema operativo Windows. La segunda lista, por su parte, incluye los 10 problemas específicos de sistemas Unix y Linux.

En Enero del 2015 el laboratorio Eset observo vulnerabilidades en los sistemas operativos durante varios meses los especialista de google fueron publicando vulnerabilidades en diferentes sistemas Operativos, tuvieron una extensa polémica debido a que se encontraron riesgos peligrosos.

2.3.5 Concepto de vulnerabilidad

Es una debilidad o falla de un sistema de información, diseño, procedimientos de seguridad, controles internos, o ejecución que puede ser explotada o desencadenada por una fuente de amenaza, causando una violación de seguridad o un incumplimiento de las políticas de seguridad del sistema (MIERES JORGE, 2009,p.5-15)

2.3.6 Vulnerabilidades en los sistemas operativos por parte del usuario

Windows publico varias vulnerabilidades que presentaba alguna de las cuales fueron solucionadas gracias a las actualizaciones periódicas que ofrece Microsoft cada mes,

estas actualizaciones trajeron importantes cambios en el boletín de seguridad de este sistema operativo numeramos sus vulnerabilidades: Existencia de servidores web y sus servicios asociados, Servicio Workstation, Servicios de acceso remoto de Windows, Microsoft SQL Server, Autenticación de Windows, Navegadores web, Aplicaciones de compartición de archivos, Subsistema LSAS, Programa de correo (ALBORS JOSEP, 2015,p.1)

En MacOS google dio a conocer tres vulnerabilidades para el sistema Apple, estas vulnerabilidades permitirían ejecutar código pero de acceso físico, lo cual se les concedió un tiempo prudente para mitigar y corregir estas vulnerabilidades (ALBORS JOSEP, 2015,p.1).

- *1 vulnerabilidad***:** que está relacionada con XPC de netwokd, el demonio utilizado por OS X para el manejo de redes.
- *2 vulnerabilidades***:** tiene que ver con la ejecución IO/Kit, que está en el kernel, por una referencia a un puntero nulo en el Intel Accelerator.
- *3 vulnerabilidades***:** tiene relación con una corrupción de memoria por la conexión con Bluetooh.

Linux no se ha quedado fuera de presentar vulnerabilidades, la conocida GHOST que permitiría a un atacante tomar remotamente el control de un sistema sin conocer las credenciales de acceso, este tipo de vulnerabilidad afecto a varias distribuciones de Linux, a las pocas horas que fue publicado presentaron el parche pero ya poniendo en peligro millones de dispositivos conectados en internet (ALBORS JOSEP, 2015,p.1)

Sus vulnerabilidades son: Software BIND, Servidor Web, Autenticación, Sistemas de control de versiones, Servicio de transporte de correo y Mala configuración de los servicios de red (ALBORS JOSEP, 2015,p.1)

2.4 Usuarios finales

2.4.1 Concepto de usuario final

Un usuario final es un individuo o grupo de individuos que van a manipular de forma directa una computadora, sistema operativo, servicio o cualquier sistema, además se utiliza para clasificar a diferentes privilegios, permisos a los que tiene acceso un usuario o grupo de usuario, para interactuar o ejecutar con el ordenador o con los programas instalados en este.

2.4.2 Tipos de usuarios finales

Los usuarios finales se dividen en cuatro categorías

*Usuario Final Directo***:** Opera El Sistema, tiene interacción directa a través del equipo de Sistemas. Responsable de alimentar el sistema con datos (BONIVENTO GERMAN, 2014,p.7).

*Usuario Final Indirecto***:** Emplea los reportes y otros tipos de información generada por el sistema, pero no opera el equipo de sistemas. La responsabilidad es por las aplicaciones que existen en el área encargada (BONIVENTO GERMAN, 2014,p.7).

Administradores: Supervisan la intervención en el desarrollo o uso del sistema. Tienen la responsabilidad ante la organización de controlar las actividades del sistema (BONIVENTO GERMAN, 2014,p.7).

*Directivos***:** Incorporan los usos estratégicos y competitivos de los sistemas de información en los planes y estrategias de la organización. Evalúan los riesgos originados por fallas en los sistemas de información (BONIVENTO GERMAN, 2014,p.7).

Figura 9-2 Tipos de usuarios finales
Fuente: (LÓPEZ FLORES ARTURO, 2009)

2.4.3 Tipos de errores que cometen los usuarios finales

Microsoft evalúa frecuentemente las explotabilidad de vulnerabilidades asociadas a una actualización de Microsoft pero en ocasiones los ataques que se reciben no son problemas de la plataforma sino errores humanos ya que son ellos los que olvidan o no tienen conocimientos de seguridad que se debe tener en cuenta que pueden ser flanco fácil de un atacante externo por no realizar actualizaciones sobre su sistema operativo, configurar correctamente el firewalls, abrir documentos sospechoso, no tener instalado un antivirus o actualizado y no utilizar herramientas en las computadoras que me ayuden a proteger de los atacantes que están a la expectativa de cualquier agujero que exista o que los usuarios no lo hayan prevenido entre ellos existen errores que dan paso a u vulnerabilidades y que se dividen en tres tipos (MICROSOFT, 2009,p.1)

Tabla 2-2. Evaluación de errores que dan origen a la explotabilidad

Evaluación de errores que dan origen a la explotabilidad	Breve definición
1	Probabilidad de código de error de seguridad coherente
2	Probabilidad de código de error de seguridad incoherente
3	Improbabilidad de código operativo de error de seguridad

Fuente:(MICROSOFT, 2009)

Probabilidad de código de error de seguridad coherente.- Esta clasificación significa que nuestro análisis demostró que se puede crear un código de error de seguridad de manera que un atacante puede explotar esa vulnerabilidad de manera coherente. Por ejemplo, una error de seguridad podría provocar la ejecución remota del código de ese atacante varias veces y de manera que un atacante podría esperar los mismos resultados de forma coherente. Esto la convertiría en un objetivo atractivo para los atacantes y, por lo tanto, habría más probabilidades de crear un código de vulnerabilidad de seguridad. De ser así, los clientes que revisaron el boletín de seguridad y determinaron su capacidad de aplicación dentro de su entorno podrían tratar el asunto con alta prioridad (MICROSOFT, 2009, p.1)

Probabilidad de código de error de seguridad incoherente.- Esta clasificación significa que nuestro análisis demostró que se pudo crear un código de error de seguridad, pero que probablemente un atacante experimentaría resultados incoherentes, incluso si fijara como objetivo el producto afectado. Por ejemplo, un error de seguridad podría provocar la ejecución remota de código, pero sólo puede funcionar 1 de 10 veces, o 1 de 100 veces, según el estado del sistema que se fija como objetivo y la calidad del código de error de seguridad. Aunque un atacante puede aumentar la coherencia de sus resultados a través de una mejor comprensión y control del entorno objetivo, la naturaleza poco confiable de este ataque la vuelve un objetivo menos atractivo para los atacantes. Por lo tanto, es probable que se cree un código de error de seguridad, pero es improbable que los ataques sean tan eficaces como otras vulnerabilidades que se pueden explotar de forma más coherente. De tal modo, los clientes que revisaron el boletín de seguridad y determinaron su capacidad de aplicación dentro de su entorno deben considerarlo una actualización de material, pero si se clasifica por orden de prioridad frente a otros errores altamente explotables, podría otorgarle una clasificación más baja en su prioridad de implementación (MICROSOFT, 2009, p.1)

Improbabilidad de código operativo de error de seguridad.- Esta clasificación significa que nuestro análisis demostró que es improbable que se lance un código de error de seguridad que opere correctamente. Esto significa que podría ser posible que se lanzara un código de error de seguridad que podría activar la vulnerabilidad y provocar un

comportamiento anormal, pero es improbable que un atacante pueda explotar la vulnerabilidad con un impacto total. Dado que los errores de este tipo necesitarían una inversión importante por parte de los atacantes para que fueran satisfactorias, el riesgo de que se cree y use un código de error de seguridad es mucho menor. Por lo tanto, los clientes que revisaron el boletín de seguridad para determinar su capacidad de aplicación dentro de su entorno podrían clasificar por orden de prioridad esta actualización por debajo de otros errores dentro de un lanzamiento (MICROSOFT, 2009,p.1) Tenemos códigos de errores que son detectados por Windows cuando estos están vulnerables a los ataques:

Error de no actualizar el sistemas Operativo.- Es posible que el equipo quede expuesto a riesgos o que experimente problemas innecesarios con Windows o los programas. Continuamente surge nuevo software malintencionado que trata de aprovecharse de las vulnerabilidades de Windows u otros programas para dañar los datos o el equipo, o para obtener acceso a ellos. Las actualizaciones de Windows y demás actualizaciones de software corrigen estas vulnerabilidades al poco tiempo de ser descubiertas. Si retrasa o no aplica las actualizaciones, el equipo puede volverse vulnerable a estas amenazas (MICROSOFT, 2009,p.1). Para la actualización del sistema operativo se recomienda a los usuarios utilizar Windows update

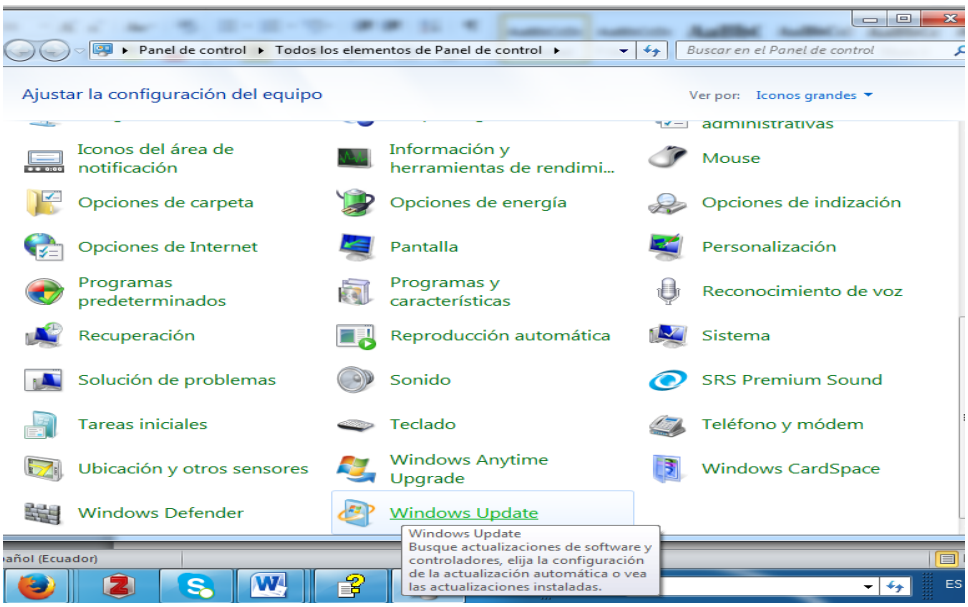

Figura 2-2 Configuración de Windows update
Fuente: (Microsoft, 2009)

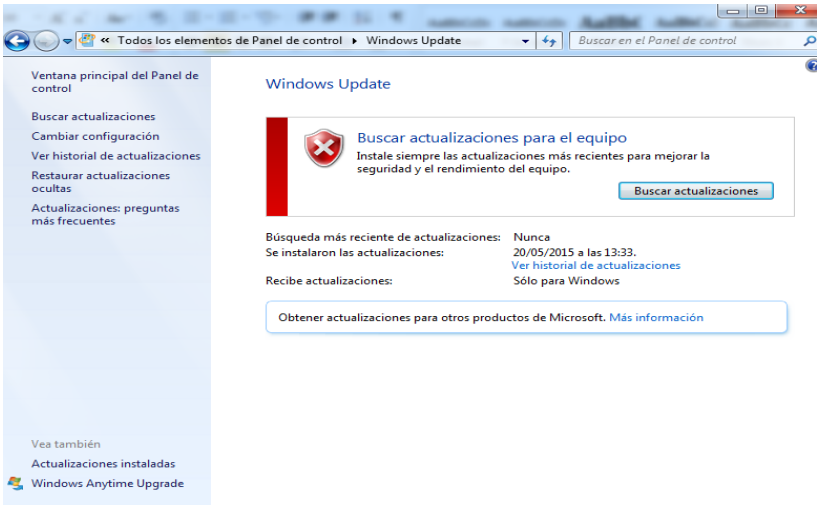

Figura 3-2 Actualización de un Sistema Operativo
Fuente: MICROSOFT, 2009)

Error de no configurar el firewalls.- Un firewall es software o hardware que ayuda a evitar que los hackers y algunos tipos de malware lleguen a los equipos a través de una red o de Internet. Realiza esta tarea comprobando la información que viene de Internet o de la red y bloqueándola o permitiendo que pase a su equipo.

Un firewall no es lo mismo que una aplicación antivirus o antimalware. Los firewalls ayudan a proteger contra gusanos y hackers, mientras que las aplicaciones antivirus protegen contra virus y las aplicaciones antimalware ayudan a proteger contra malware. Las tres aplicaciones son necesarias. Puedes usar Windows Defender, el software antivirus y antimalware que está incluido en Windows 8, o puedes usar otra aplicación antivirus y antimalware (MICROSOFT WINDOWS, 2015).

Firewall de Windows viene con Windows y está activado de manera predeterminada. Ver **Figura 12-2** que muestra cómo funciona el firewall:

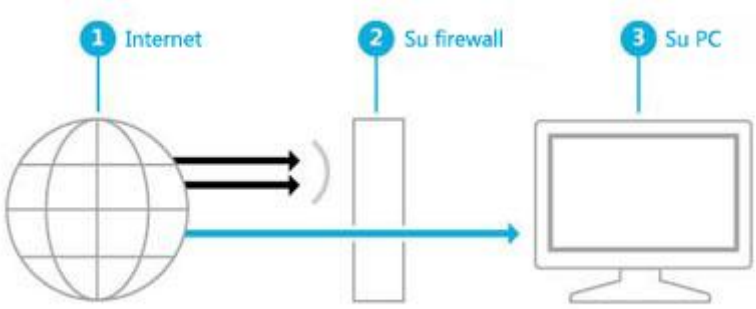

Figura 4-2 Firewall crea una barrera entre internet y el equipo
Fuente: (MICROSOFT WINDOWS, 2015)

Error de no utilizar antivirus.-

Existen las amenazas de los virus y lo que los usuarios cometen continuamente es no utilizar en sus computadoras un antivirus, no los actualiza. Los mecanismos conocidos hasta el momento para la propagación de virus son los archivos ejecutables, es decir aquellos con extensión .exe, .com o .bat, y los componentes de Microsoft Office que aceptan macros para Aplicaciones, principalmente Word y Excel con macros. Los troyanos se propagan también a través de archivos ejecutables (MICROSOFT WINDOWS, 2015).

Las formas de infección son las siguientes:

• Ejecutando un programa infectado, ya sea directamente desde un memory, bajado desde Internet o abierto desde un "attach" recibido por correo electrónico.

•Abriendo un documento de MS-Office 2010 (o superior) teniendo deshabilitada o haciendo caso omiso a la alerta contra macro virus habilitada por defecto en Office.

Error de no utilizar una cuenta de usuario con pocos privilegios (no administrador) en su equipo, solo utilizar esta cuenta de administrador cuándo se quiera cambiar una configuración o instalar un software de confianza. Siempre, se debe ser cauteloso con todo lo que se ejecuta (MICROSOFT WINDOWS, 2015)..

Error que transfiera un archivo desde la Internet a su PC se debe tener la precaución de revisarlo por si tiene virus ó malwares, pero también es muy importante saber cuál es su origen y si el mismo es de una fuente confiable (MICROSOFT WINDOWS, 2015)..

Error de no Comprobar los archivos comprimidos **(**ZIP, RAR, ARJ,GZIP, GZ, ACE, CAB, 7z…etc) (MICROSOFT WINDOWS, 2015)..

Error de no realizar copias de respaldo (backups) de programas y documentos importantes, los mismos pueden ser guardados en un Memoria **USB**, **CD**, **DVD** ó **Disco Duro** externo entre otros medios (MICROSOFT WINDOWS, 2015)..

Error de instalar programas de un origen dudoso

Error de navegar por sitios potencialmente dañinos buscando cosas como **"pornografía"**, **" mp3 gratis"**, claves, licencias ó cracks para programas comerciales (MICROSOFT WINDOWS, 2015)..

Error de descargar programas, archivos comprimidos ó ejecutables, desde redes peer-to-peer (P2P) ya que en realidad no se sabe el real contenido de la DESCARGA (MICROSOFT WINDOWS, 2015).

Error de no crear una contraseña de alta seguridad en su PC, tanto en la cuenta de administrador como en las demás cuentas (MICROSOFT WINDOWS, 2015)..

Error de usar la misma contraseña tanto en su PC como en los distintos sitios webs como **Hotmail**, **Yahoo**, **AOL**, **Gmail** y redes sociales como: **Facebook**, **Google +**, **Twitter**, **MySpace, Linkedin, Hi5**, etc (MICROSOFT WINDOWS, 2015).

Error de No realizar escaneos periódicos (diarios, semanales) con el antivirus instalado en su PC asi como con el antispyware residente, en caso de tener más de un antispyware instalado debe tener solo uno como residente, pudiendo con los demás realizar escaneos periódicos en su ordenador (MICROSOFT WINDOWS, 2015)..

Error de desactivar la interpretación de VBScript y permitir JavaScript, ActiveX y cookies sólo en páginas web de confianza (MICROSOFT WINDOWS, 2015).

2.5 Metodología OSSTMM

2.5.1 Introducción

Refiere a un manual que describe una metodología aplicable a las Pruebas de la seguridad, si tiene fines prácticos se señala lo más importante para un mejor entendimiento. El OSSTMM se rige a reglas y leyes Internacionales, nacionales, Locales, Industriales y Políticas establecidas en la organización (RAMÍREZ LÓPEZ JORGE, 2009,p.58).

Este manual también contempla el cumplimiento de normas y mejores prácticas como las establecidas en el NIST, ISO 27001-27002 e ITIL entre otras. Lo que hace de este manual uno de los más completos en cuanto a la aplicación de pruebas a la seguridad de la información en las instituciones (RAMÍREZ LÓPEZ JORGE, 2009,p.59)

2.5.2 Propósito

Garantizar la inspección de seguridad de una organización, surtir guias para el auditor y por ultimo conocer y manejar los módulos se lo aplica a cualquier tipo test de seguridad (PINZÓN LILIANA CAROLINA MIHDIBADI TALERO Y JOHN A. BOHADA, 2014,p.32).

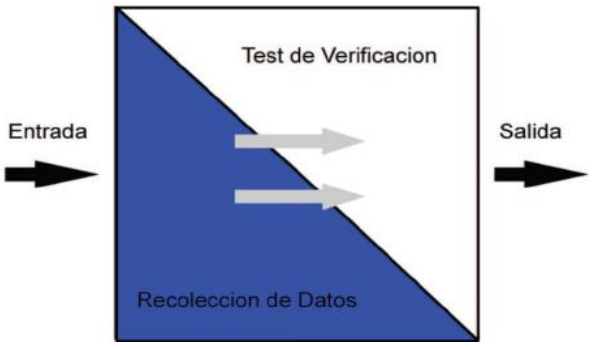

Figura 5-2 Propósito de OSSTMM
Fuente:(Oswaldo Andrés Acosta Naranjo, 2013)

En la **figura15-2** se observa cada uno de los procedimientos que deben ser adoptados por el personal que realice el control de vulnerabilidades de cualquier ambiente informático

que presente las empresas públicas y privadas utilizando esta metodología OSSTMM, están divididas en bloques para su mejor entendimiento.

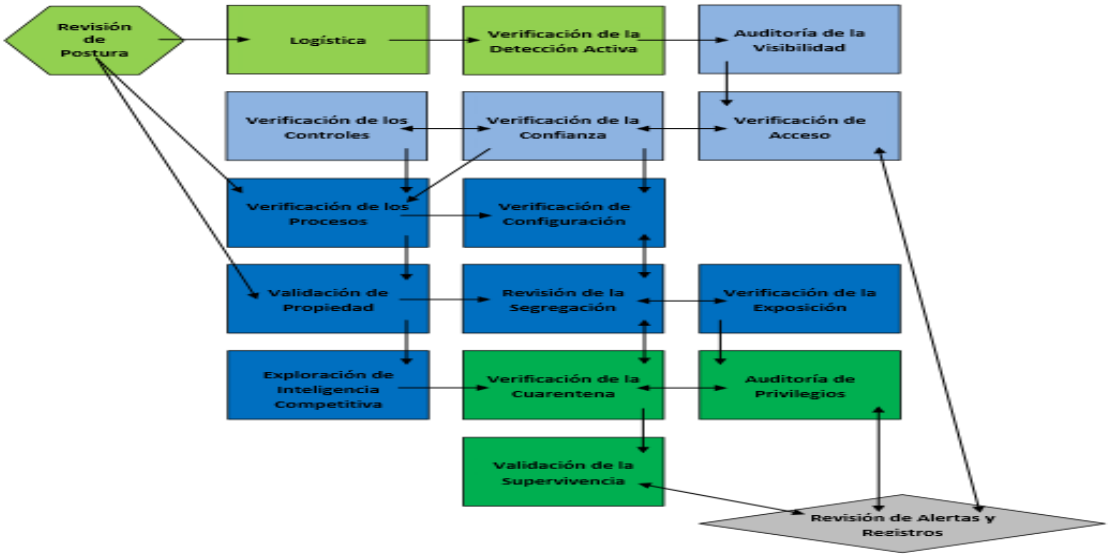

Figura 6-2 Diagrama de bloques de la metodología OSSTMM
Fuente: (HERZOG, PETO 2010)

2.5.3 Ámbito y limitaciones de OSSTMM

En el documento de metodología de testeo de seguridad se define como un conjunto de reglas y lineamientos para CUANDO, QUE y CUALES eventos son testeados. Esta metodología cubre únicamente el testeo de seguridad externo, es decir, testear la seguridad desde un entorno no privilegiado hacia un entorno privilegiado, para evadir los componentes de seguridad, procesos y alarmas y ganar acceso privilegiado (HERZOG PETO, 2010,p.13).

La limitación al alcance del testeo de seguridad externo está dada por las diferencias considerables entre testeo externo a interno y testeo interno a interno. Estas diferencias radican fundamentalmente en los privilegios de acceso, los objetivos, y los resultados asociados con el testeo interno a interno (HERZOG PETO, 2010,p.13).

2.5.4 Tipos de test

*Caja Blanca***.-**El testeador posee conocimiento previo integral de los elementos o del entorno a ser testeados (RAMÍREZ LÓPEZ JORGE, 2009).

Caja Gris.- El testeador tiene un conocimiento previo de los elementos o del entorno a testear (RAMÍREZ LÓPEZ JORGE, 2009,p.60)..

Caja Negra.-El testeador no tiene conocimiento previo de los elementos o del entorno a testear (RAMÍREZ LÓPEZ JORGE, 2009,p.60).

Sombrero Negro.-Un hacker que es caótico, anarquista e infringe la ley (RAMÍREZ LÓPEZ JORGE, 2009).

Tándem o Secuencial (Tándem): El auditor y el objetivo están preparados para la auditoría y ambos conocen los avances y detalles de la auditoría. Se establece una serie de pruebas de protección (Tándem test) y controles del objetivo. Es una prueba minuciosa de acuerdo a la visión del auditor del total del análisis.

Este es un proceso transparente por lo que se le llama de Caja de Cristal en el cual tanto el auditor como el objetivo trabajan en las pruebas (RAMÍREZ LÓPEZ JORGE, 2009,p.60).

Inverso: El auditor participa con el objetivo de manera completa en el proceso de la seguridad operacional. Pero el objetivo no conoce el ¿Qué?, ¿Cómo? Y ¿Cuándo? el auditor realizará las pruebas.

La meta es desconocida en este tipo de pruebas. La amplitud y profundidad depende de la calidad de la información provista al auditor. Esto permite por lo regular lo que se llama un Ejercicio de Equipo Rojo (Read Team Exercise), (RAMÍREZ LÓPEZ JORGE, 2009,p.60).

Figura 7-2. Etapas de un test de penetración
Fuente: (PINZÓN LILIANA CAROLINA MIHDIBADI TALERO Y JHON A. BOHADA, 2014, p.29)

2.5.5 Fases de la metodología OSSTMM

La metodología OSSTMM cuenta con cuatro fases que se deben seguir para una eficaz prueba de seguridad en los sistemas informáticos así se tiene:

A. Fase Inducción

B. Fase de Interacción

C. Fase indagatoria

D. Fase de Intervención

A. Fase Inducción

Cada viaje comienza con una dirección. En la fase de inducción, el analista comienza la auditoría con una comprensión de los requisitos de auditoría, el alcance y las limitaciones a la auditoría. A menudo, el tipo de prueba se determina mejor después de esta fase **(HERZOG PETO, 2010, p.99).**

Tabla 3-2 Fase de inducción

Modulo		**Descripción**	**Explicación**
A.1	Revisión de postura	La revisión de la cultura, las reglas, normas, reglamentos, legislación y políticas aplicables a la meta.	Conocer el alcance y lo que tienen que hacer exámenes. Requerido si la fase C se lleve a cabo correctamente.
A.2	Logística	La medición de las limitaciones de interacción tales como la distancia, la velocidad, y falibilidad para determinar los márgenes de precisión en los resultados.	Conocer las limitaciones del ser que la auditoría. Esto minimizará el error y mejorar eficiencia
A.3	Verificación	Detección activa La verificación de la práctica y la amplitud de la detección de la interacción, la respuesta, y la previsibilidad de respuesta.	Conozca las restricciones impuestas a las pruebas interactivas. Esto es necesario para realizar correctamente las fases B y D.

Fuente:(HERZOG PETO, 2010,p.99)

B. *Fase de Interacción*

El núcleo de la prueba de seguridad básica requiere conocer el alcance en relación a las interacciones con los objetivos transmitidos a las interacciones con los activos. En esta fase se definirá el alcance (**HERZOG, PETO 2010, p.100)**

Tabla 4-2. Fase de interacción

Modulo		**Descripción**	**Explicación**
B.4	Auditoría Visibilidad	La determinación de los objetivos a ensayar dentro del alcance. La visibilidad es considerada como "presencia" y no se limita a la vista humana.	Conozca cuáles existen objetivos y cómo interactúan con el alcance, en todo caso. Un objetivo muerto o desaparecido es también un objetivo de responder. Sin embargo, un objetivo que no responde no es necesariamente un objetivo faltante
B.5	Verificación de Acceso	La medición de la amplitud y profundidad de los puntos de acceso interactivos dentro de la meta y autenticación requerida.	El punto de acceso es el punto principal de cualquier interacción de activos. Verificación de un punto de acceso que existe es una parte de la determinación de su propósito. Verificación completa requiere conocer todo lo que hay que saber sobre el punto de acceso.
B.6	Verificación de confianza	La determinación de las relaciones de confianza y de entre los objetivos. Un fideicomiso existe relación donde el objetivo acepta la interacción entre los objetivos en el ámbito de aplicación.	Fideicomisos para nuevos procesos son a menudo muy limitado donde los procesos de mayor edad tienen una evolución aparentemente caótica para el forastero. Conocer las relaciones de confianza entre los objetivos mostrará la edad o el valor de la interacción

Fuente: (HERZOG PETO, 2010, p.100)

C. Fase indagatoria

Gran parte de la auditoría de seguridad se trata de la información que el analista descubre. En esta fase, los distintos tipos de valor o en detrimento de la información fuera de lugar y mal administrada como un activo salen a la luz : **(HERZOG PETO, 2010,p.101)**

Tabla 5-2. Fase indagación

Modulo		**Descripción**	**Explicación**
C.8	Verificación de Procesos	La determinación de la existencia y eficacia del registro y mantenimiento de los niveles reales de seguridades existentes o diligencia definidos por la revisión de la postura y los controles de indemnización.	Conozca los controladores y sus rutinas para los controles. La mayoría de procesos tendrán un conjunto definido de reglas, sin embargo las operaciones reales reflejan ninguna eficacia, la pereza, o la paranoia que puede redefinir las reglas. Así que no es sólo que el proceso está ahí, pero también cómo funciona
C.9	Validación de la Propiedad .	La medición de la amplitud y profundidad en el uso de ilegal o sin licencia propiedad intelectual o aplicaciones dentro de la meta	Conozca la situación de los derechos de propiedad de propiedad.
C.10	Revisión Segregación	La determinación de los niveles de información de identificación personal definido por la revisión de la postura.	Conozca los que se aplican los derechos de privacidad y en qué medida la información de identificación personal al descubierto pueden clasificarse en base a estos requisitos.
C.11	Verificación de exposición	La búsqueda de información de libre acceso que describe indirecta visibilidad de los objetivos o los activos dentro del canal elegido del alcance.	La palabra en la calle tiene valor. Destape información sobre objetivos y activos de fuentes públicas incluida la de los propios objetivos.
C.12	Inteligencia Competitiva	Scouting La búsqueda de información de libre acceso, directa o indirectamente, lo que podría dañar o afectar negativamente el dueño de destino a través de medios externos y competitivas.	Puede haber más valor en la información de los procesos y objetivos que los activos que están protegiendo. Destape información que por sí mismo o en conjunto pueden influir en las decisiones de negocios competitivos.

Fuente: (HERZOG PETO, 2010, p.101)

C. Fase de Intervención

Estas pruebas se centran en los recursos de los objetivos, requieren en el ámbito de aplicación. Esos recursos se pueden cambiar por estar, sobrecargados o murieron por causar la penetración o interrupción. Esto es a menudo la fase final de una prueba de seguridad para asegurar las interrupciones no afecta a las respuestas de las pruebas menos invasivas y porque la información para la toma de estas pruebas no puede ser conocida hasta otras fases se han llevado a cabo. El último módulo, de Alerta y Revisión de Listado, está obligado a verificar las pruebas anteriores que proporcionaron ninguna interactividad backto el analista. La mayoría de las pruebas de seguridad que no incluyen esta fase todavía pueden tener que ejecutar un examen de final de la perspectiva de los objetivos y de los activos para aclarar cualquier anomalía **(HERZOG PETO, 2010, p.102)**

Tabla 6-2 Fase de intervención

Modulo		**Descripción**	**Explicación**
D.13	Cuarentena Verificación	La determinación y medición del uso efectivo de cuarentena para todos los accesos hacia y dentro de la meta.	Determinar la efectividad de los controles de autenticación y subyugación en términos de lista cuarentenas en blanco y negro.
D.14	Privilegios de Auditoría	La cartografía y la medición del impacto de la mala utilización de los controles subyugación, credenciales y privilegios o la escalada no autorizada de privilegio.	Determinar la efectividad de la autorización en la autenticación, indemnización, y los controles de subyugación en términos de profundidad y roles.
D.15	La supervivencia de validación / Continuidad del Servicio	La determinación y la medición de la resistencia del objetivo a los cambios excesivos o adversos donde controles de continuidad y resistencia se verían afectados.	Determinar la efectividad de los controles de continuidad y resistencia a través de la verificación de denegación de servicio y la negación de la interactividad.
D.16	Alerta y registro de revisión / Encuesta Fin	Una revisión de las actividades de auditoría realiza con la verdadera profundidad de las actividades según lo registrado por el blanco o de un tercero como en el control de la alarma	. Conozca cuáles partes de la auditoría dejaron un rastro utilizable y confiable.

Fuente: **(HERZOG PETO, 2010, p.102)**

2.5.6 Secciones de prueba

En el modelo OSSTMM 3 se dividen en cinco secciones como muestra la tabla7-2

Tabla 7-2 Secciones de OSSTMM

MODULO	SECCIÓN OSSTMM	DESCRIPCIÓN
Seguridad Física	Humano	Todo el elemento humano comprometido en la organización
	Físico	Todo lo referente a hardware de la organización
Seguridad de las comunicaciones	Redes de datos	Son los sistemas electrónicos y redes de datos de la organización
	Telecomunicaciones	Comunicaciones analógicas y digitales de la comunicación
Seguridad del espectro electromagnética	Inalámbricas	Señales electromagnéticas en las comunicaciones o cualquier emanación de espectro

Fuente: (RAMÍREZ LÓPEZ JORGE, 2009, p.61)

Para el caso de esta investigación se estudiaran dos secciones que intervienen para determinar las vulnerabilidades que tienen los sistemas operativos:

a. Pruebas de Seguridad Humana

Es una prueba de identificación, la relación con la gente, los más importantes los que operan los ámbitos de cumplimiento de seguridad se puntualizan la seguridad personal.

Los analistas competentes requerirán ambas habilidades de las personas diligentes y habilidades de pensamiento crítico para asegurar la recolección de datos de hecho crea resultados de hecho a través de la correlación y análisis (HERZOG PETO, 2010,p.105)

Se debe tomar en cuenta las siguientes consideraciones para asegurar una prueba de alta calidad:

-Revisión de postura

Logística

Preparación del entorno de prueba de canal necesario para prevenir falsos positivos y falsos negativos que conducen a resultados inexactos (HERZOG PETO, 2010,p.107)

Equipo de comunicaciones

Comunicaciones.

Tiempo

-Verificación detección activa

Determinación de controles activos y pasivos para detectar la intrusión de filtrar o rechazar los intentos de la prueba se debe hacer antes de la prueba para mitigar el riesgo de crear falsos positivos y negativos en los datos obtenidos de los ensayos, así como cambiar el estado de alarma de monitoreo personal o agentes (HERZOG PETO, 2010,p.108).

Monitoreochannel

Canal Moderación

Supervisión

Asistencia Operador

-Auditoría visibilidad

Acceso de identificación

Personal Enumeración

-Verificación de acceso

Las pruebas para la enumeración de los puntos de acceso para el personal dentro del alcance.

Si bien el acceso al personal fuera del ámbito de aplicación es un escenario real y uno

de uso frecuente para el robo de propiedad de la información, esto puede limitarse a alcance de sólo la interacción de proteger los derechos de privacidad independientes del personal en su privado vida (HERZOG PETO, 2010,p.109)

Proceso Acceso

Mapa y explorar el uso de canales en el alcance para llegar a los activos. Documentar todos los métodos utilizados y los resultados de esos métodos (HERZOG PETO, 2010,p.109).

Autoridad

Use el personal en posiciones de autoridad con el control de acceso o que ocupan puestos de gatekeeper a los activos dentro del alcance. Métodos de documentos utilizados en el descubrimiento de personal clave (HERZOG PETO, 2010,p.109)

Autenticación

Enumerar y prueba de las deficiencias de personal de puerta de enlace y qué privilegios son necesarios para interactuar con ellos para asegurar que sólo identificable autorizada, partes destinadas tengan acceso (HERZOG PETO, 2010,p.109),

-Verificación de confianza.

Declaraciones falsas
Fraude

-La desinformación

Phishing

Son pruebas donde se identifica la suplantación de identidad (HERZOG PETO, 2010) *Abuso de Recursos*

Prueba donde se identifica al personan no autorizado obtener información del ámbito informático sin el debido (HERZOG PETO, 2010,p.110)

En terrorem

-Controles de verificación.

No repudio
Confidencialidad
Privacidad.
Integridad
-Verificación de procesos
Mantenimiento
La desinformación
Due Diligence
Indemnización.

-Verificación de entrenamiento

Educación
Política de Interrupción Mapeo Conciencia
Mapa de las limitaciones descubiertas en la formación de la conciencia de seguridad para el personal a través de análisis de las deficiencias de los procedimientos reales, incluyendo pero no limitado a: la provisión de activos a través de cualquier canal, la capacidad de reconocer la identificación inadecuada y forjado o métodos necesarios, el método de identificación adecuada entre el personal, el uso de medidas de seguridad personales de uno mismo y de los activos, el manejo de los activos confidenciales y sensibles, y la conformidad con la política de seguridad de la organización (HERZOG PETO, 2010,p.115)
Conciencia Secuestro
Revisión segregación
Privacidad Mapeo de Contención
Información Evidente
Divulgación
Limitaciones
-Verificación de exposición

Asignación de exposición

Profiling

Competitiva Scouting Inteligencia

Negocios Molienda

Ambiente de Negocios

Verificación

Niveles de contención

Privilegios

Identificación.

Autorización

Escalation

Discriminación.

Subyugación.

Continuidad del Servicio.

La resiliencia

Continuidad

Seguridad

Mapa y documentar el proceso de porteros de desconexión canales debido a las preocupaciones de evacuación o de seguridad como un análisis de las deficiencias con la regulación y la política de seguridad (HERZOG PETO, 2010,p.116)

Encuesta Fin

Alarma

Verificar y enumerar el uso de un sistema de alerta localizada o en todo el ámbito de aplicación, registro, o un mensaje para cada pasarela de acceso sobre cada canal donde una situación sospechosa se observa por parte de personal ante la sospecha de intentos de elusión, la ingeniería social, o la actividad fraudulenta (HERZOG PETO, 2010,p.116-117)

Almacenamiento y Recuperación

Documento y verifique el acceso privilegiado y eficiente para la alarma, registro, y los lugares de almacenamiento de notificación y la propiedad (HERZOG PETO, 2010,p.116-117)

Se ha detallado la seguridad humana como canal de prueba de seguridad para la investigación que se está realizandando puesto que existen algunos ítems que cumplen con la metodología.

e. Pruebas de redes de datos de seguridad

Las pruebas para el canal de datos Redes de Seguridad (COMSEC) requieren interacciones con las garantías de funcionamiento de la red de comunicación de datos existentes que se utilizan para controlar el acceso a la propiedad (HERZOG PETO, 2010,p.167)

Este canal cubre la implicación de los sistemas informáticos, principalmente las redes de explotación dentro del ámbito objetivo o marco. Mientras que algunas organizaciones consideran que esto simplemente como "pruebas de penetración", el objetivo del cumplimiento cierto de las pruebas de seguridad en este canal es la interacción del sistema y la calidad de funcionamiento pruebas con mediciones brecha a la norma de seguridad requerido se indica en la política de la empresa, regulaciones de la industria, o la legislación regional (HERZOG PETO, 2010,p.167)

Durante las pruebas, los operadores de terminales y la inteligencia artificial pueden reconocer en curso ataques tanto por proceso y firma. Por esta razón, será necesario el Analista de tener una variedad suficiente de los métodos para evitar divulgación de las pruebas o trabajos con los operadores para asegurar que donde la seguridad falla y cuando tiene éxito es traído a la luz , (RAMÍREZ LÓPEZ JORGE, 2009,p.16)

Las pruebas que se centran sólo en el descubrimiento de nuevos problemas sólo dejan espacio para correcciones y no diseños para futuras mejoras. Los analistas competentes requerirán un conocimiento adecuado de redes, habilidades de pruebas de seguridad diligentes y habilidades de pensamiento crítico para asegurar la recolección de datos de hecho crea resultados fácticos a través de correlación y análisis, (RAMÍREZ LÓPEZ JORGE, 2009,p.168)

Los test de prueba de seguridad que utiliza la metodología OSSTMM ver en el Anexo1

CAPITULO III

3. METODOLOGÍA OSSTMM APLICADO A DETECCION DE VULNERABILIDADES EN SISTEMAS OPERATIVOS WINDOWS DE 64 BITS

3.1 Introducción

Hoy en día se cuenta con la metodología abierta de testeo de seguridad OSSTMM que es un manual de análisis y testeo de la seguridad de la información basándose en estándares internacionales como lo son la ISO 2701 y la 27002, esta metodología trabaja de forma esquemática a través de canales, módulos, fases y secciones de acuerdo al tipo de vulnerabilidad que están expuestos los sistemas operativos y obtener resultados exactos, fiables y correctos.

Las acciones que se tome sugiere pronosticar y no violentar políticas, decretos para el análisis y pruebas de seguridad de la información sean sistematizadas con los que requieran la utilización de esta metodología

.

Los sistemas operativos son conocidos por todos los usuarios que tienen a cargo un equipo de cómputo pero estos mismos usuarios desconocen las seguridades que tienen que brindar a su computador no llegar a ser víctimas de atacantes internos y externos que puedan llegar a robar información, suplantar identidades, invadir de programas maliciosos, tener el control del equipo a través de las redes de datos y llegar a tener un daño considerable.

Por las explicaciones dadas en los párrafos anteriores es menester conocer las vulnerabilidades que tienen los sistemas operativos Windows y dar a conocer al usuario final para que este precavido y active todos los sistemas de seguridad y alertas que pueden presentar en cierto instante esta interfaz.

3.2 Metodología

Esta investigación se basa en la utilización de la investigación descriptiva aplicativa
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.

Esta investigación está fundamentada en la versión 3 de OSSTMM
La metodología OSSTMM para la práctica toma los módulos y secciones más importantes y presenta el análisis y pruebas de seguridad, se toman dos de los módulos seguridad Física y seguridad de las comunicaciones que se subdividen en secciones tomadas para el estudio del módulo físico se toma la sección humana puesto que hace referencia a los errores que comenten los usuarios finales y del módulo de comunicaciones se toma la sección de redes de datos.

Se toman los módulos y secciones puesto que abarcan los análisis y las pruebas que se necesitan para identificar las vulnerabilidades de los sistemas operativos
La sección humana se divide en ámbitos

1. *Revisión de postura*
2. *Revisión logística*

3. Equipo de comunicaciones
Comunicaciones.
Tiempo.
4. Verificación detección activa
Monitoreochannel
Canal Moderación
Supervisión
Asistencia Operador
5. Auditoría visibilidad

Acceso de identificación

Personal Enumeración

6. Verificación de acceso

Proceso Acceso

Autoridad

Autenticación

7. Verificación de confianza.

Declaraciones falsas

Fraude

8. La desinformación

Phishing

Abuso de Recursos

En terrorem

9. Controles de verificación.

No repudio

Confidencialidad

Privacidad.

Integridad

10. Verificación de procesos

Mantenimiento

La desinformación

Due Diligence

Indemnización.

11. Verificación de entrenamiento

Educación

Política de Interrupción Mapeo Conciencia

Conciencia Secuestro

12. Revisión segregación

Privacidad Mapeo de Contención

Información Evidente

Divulgación

Limitaciones

13. Verificación de exposición

Asignación de exposición

Profiling

14. Competitiva Scouting Inteligencia

Negocios Molienda

Ambiente de Negocios

Verificación

15. Niveles de contención

Privilegios

Identificación.

Autorización

Escalation

16. Discriminación.

Subyugación.

Continuidad del Servicio.

La resiliencia

Continuidad

Seguridad

alarma

Almacenamiento y recuperación.

Y la sección de redes de datos en 16 ámbitos

1. Logística y Controles
2. Sondeo de Red
3. Identificación de los Servicios de Sistemas
4. Búsqueda de Información Competitiva
5. Revisión de Privacidad
6. Obtención de Documentos
7. Búsqueda y Verificación de Vulnerabilidades
8. Testeo de Aplicaciones de Internet
9. Enrutamiento
10. Testeo de Sistemas Confiados
11. Testeo de Control de Acceso
12. Testeo de Sistema de Detección de Intrusos
13. Testeo de Medidas de Contingencia

14. Descifrado de Contraseña
15. Testeo de Denegación de Servicios
16. Evaluación de Políticas de Seguridad

3.3 Aplicación de la metodología OSSTMM para detectar errores de seguridad y vulnerabilidades en S.O de 64 bits a nivel de usuario final

Uno de los principales problemas de seguridad está dado por el usuario de los sistemas operativos ya que como su nombre lo indica, ellos simplemente hacen uso de las herramientas y en si del sistema operativo sin preocuparse de la seguridad de los mismos que a la vez conlleva a la seguridad de sus datos y de su propia integridad con lo que se refiere a datos e información.

Tomados de la metodología OSSTMM y en lo expuesto anteriormente se sigue el siguiente esquema para la detección de vulnerabilidades en SO Windows de 64 bits ver Figura 17-3:

1) Levantamiento de información de los Sistemas Operativos de 64 bits:
2) Análisis de vulnerabilidades de Sistemas operativos
3) Evaluación de riesgos
4) Capacitación
5) Informe final

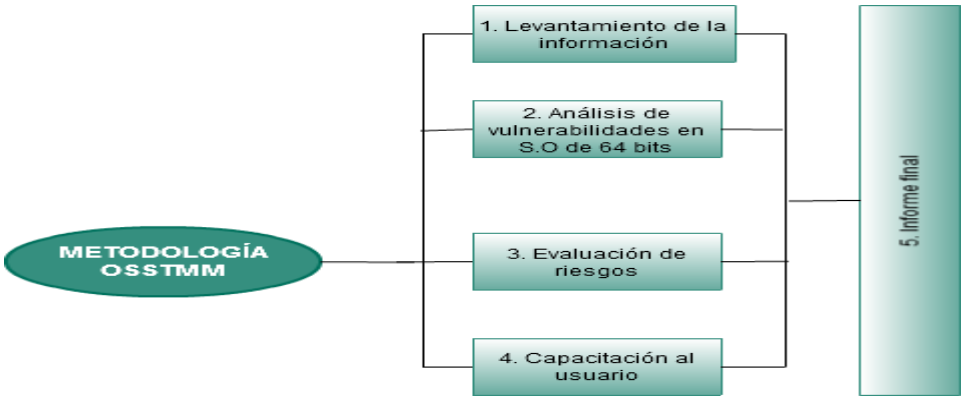

Figura 1-3 Metodología OSSTMM para la detección de vulnerabilidades en SO
REALIZADO POR: (CRUZ NUBE, 2015)

En la primera (1) fase) de la metodología OSSTMM se habla de un levantamiento de información que se enfoca a la obtención de datos del equipo , como el tipo de sistema operativo que se encuentra instalado, si cuenta con licencia, programas que están instalados y configuraciones que se han realizado en el equipo y en cuanto a la información sobre el usuario se puede conocer los datos personales del usuario final, funciones que desempeña en la empresa organización u entidad pública y lo más importante es indagar sobre los conocimientos que tiene sobre la seguridad que se debe brindar a los sistemas operativos para no ser víctimas de robo , hackeo o intrusión de información de los quipos informáticos.

El ámbito que abarca es toda la seguridad operativa y se compromete en utilizar áreas o canales de OSSTMM, para la detección de vulnerabilidades en los SO se tomaran dos canales seguridad Física con la sección humano debido a que trata el elemento humano en los procesos y de las comunicaciones con la sección redes de datos puesto que incluye todos los sistemas de redes de datos.

En la Figura 1-3 se observa como en cada fase de la metodología se subdivide de acuerdo a lo que se necesita conocer y todos los puntos tomados de la metodología.

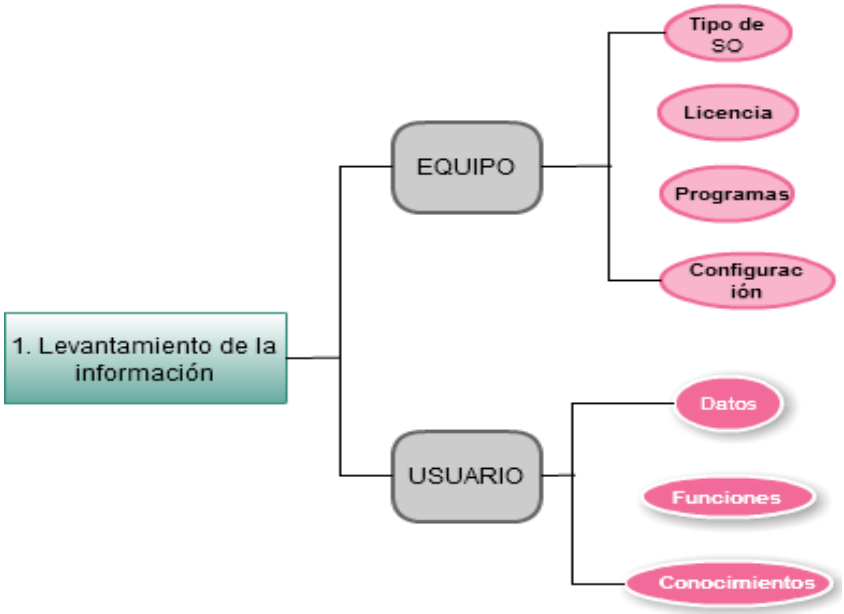

Figura 2-3 Primera fase de la metodología OSSTMM para detectar errores de seguridad en SO

Realizado por: (CRUZ, NUBE, 2015)

En la segunda (2) fase) es donde se observa, numera, comprueba y verifica la función operativa es decir analiza las vulnerabilidades que presentan los sistemas operativos de 64 bits de la metodología OSSTMM tomando el módulo de verificación de accesos donde se numera todos los puntos de acceso a la red de datos que cuenta con 3 puntos importantes como son procesos de acceso, servicio y autenticación además, otro modulo donde se puede analizar las vulnerabilidades es la verificación de confianza y controles, verificación de confianza y verificación de procesos ver figura 19-3.

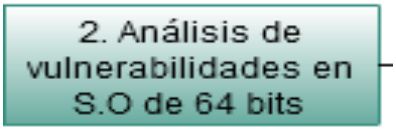

Figura 3-3 Fase 2 Análisis de vulnerabilidades SO
REALIZADO POR: (CRUZ NUBE, 2015)

Fase tres (3) se analiza la evaluaciones de riesgos se valoraran tres aspectos importantes como son los riesgos de robo de información, riesgos técnicos y riesgos económicos

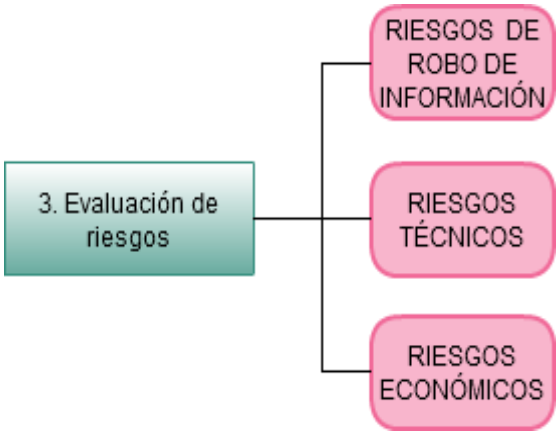

Figura 4-3 Fase 3 Evaluación de riesgos
Realizado Por: (CRUZ, NUBE, 2015)

En la fase Cuatro (4) se centra a la capacitación de los usuarios que desconocen acerca de la seguridad en Sistemas operativos de sus equipos de cómputo, la capacitación va orientada a que el usuario debe conocer:

Los tipos de programas que tienen instalados o va a instalar en su computador saber si son maliciosos dando lugar a técnicas como caballos de Troya o la puerta de atrás, si cuentan con antivirus.

Formar a los usuarios con los temas de seguridad para que no sean inexpertos o descuidados como en la configuración (firewall) de su equipo crear contraseñas y dejar a la vista de personal ajeno al proceso, borrar archivos y no contar con respaldos, etc.

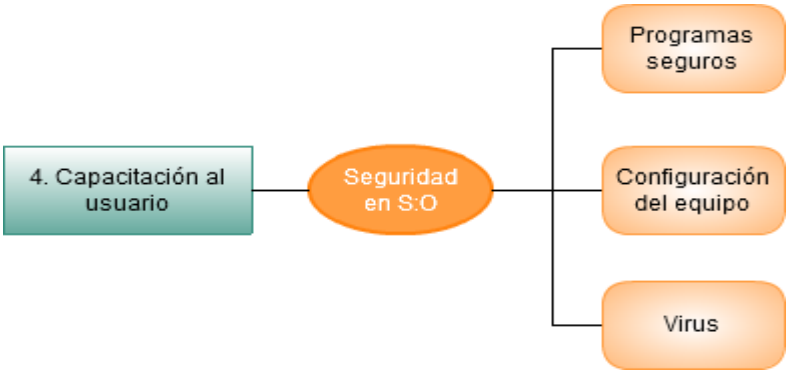

Figura 5-3 Fase 4 Capacitación al Usuario
REALIZADO POR: (CRUZ NUBE, 2015)

Y por último se tiene el informe final que estará compuesto y desglosado por las fases que se explicó anteriormente y tomadas del manual de OSSTMM ya que cuenta con fases, módulos y secciones que se acoplado para la Detección de vulnerabilidades de SO

3.4 Evaluación de los sistemas operativos Windows de 64 bits

- Análisis y evaluación de riesgos de la infraestructura que cuenta con SO Windows de 64 bits.

Como punto inicial para la evaluación SO Windows de 64 bits se centra en tres riesgos que se presentan a continuación:

a) Riesgos de robo de información

Es un punto muy impórtate que hay que tomarlo en cuenta ya que hoy en día es lo cotidiano el robo de información con fin de alterar la integridad confidencialidad, disponibilidad de datos de las empresas públicas o privadas con la finalidad de lucro.
El riesgo de un robo de información conlleva a una infinidad de problemas que puede cargar la empresa desde robo de contraseñas, alteración de la información original para dar mal uso

b) Riesgos Técnicos

Generalmente se presentan cuando un usuario encuentra un problema y es difícil resolverlo, pone en riesgo la calidad del software y hardware del sistema haciendo dificultoso o en ocasiones imposible su implementación o arreglo.
Todo esto se da a varios aspectos como dificultades de diseño, configuración, interfaz, desconocimiento técnico, falta de mantenimiento y la evolución de la tecnología.

c) Riesgos económicos

Son consideradas como incertidumbres monetarias producidas por el rendimiento de la inversión y que pueden ser por diferentes motivos en especial si la economía depende de los equipos de cómputo y si no tienen la mejor seguridad se pondría en riesgo a las empresas en la economía.

-análisis, valoración de los riesgos encontrados en los sistemas operativos Windows de 64 bits por los usuarios finales.

Con las vulnerabilidades encontradas se analizaran por versión y el número de usuarios que comete el mismo error de seguridad en los SO y serán datos estadísticos.
Estos datos estadísticos serán descritos por medio de una población lo cual se tomara cierta muestra para obtener resultados de cuantos usuarios finales cometen errores al no capacitarse con el tema de seguridad de la información esto puede ser a nivel de sistemas operativos o cualquier sistema que comprometa la integridad confidencialidad y disponibilidad de los datos de un equipo de cómputo.
En la tabla 1-3 muestra las vulnerabilidades en Windows Xp

Tabla 1-3 Vulnerabilidades del sistema operativo Xp de 64 bits

VULNERABILIDADES DEL SISTEMA OPERATIVO XP DE 64 BITS	
VULNERABILIDAD	DESCRIPCIÓN
Microsoft Server Service / CanonicalizePathName() Remote Code Execution Vulnerability (dcerpc-ms-netapinetpathcanonicalize-dos)	Desbordamiento de buffer remoto que compromete un equipo de destino
MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687) (windows-hotfix-ms09-001)	Ejecución de códigos maliciosa que podrían instalar programas ver cambiar, modificar datos y crear cuentas de usuarios nuevas con todos los derechos.
MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468) (windows-hotfix-ms10-012)	Crea un paquete SMB especialmente diseñado y enviado a paquetes en un sistema
MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (windows-hotfix-ms10-054	Compromete un equipo destino ejecuta un código arbitrario y realizar denegación de servicio
MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (windows-hotfix-ms11-020)	crea un paquete SMB especialmente diseñado y lo envía a un sistema afectado,
CIFS NULL Session Permitted (cifs-nt-0001)	Permite a los usuarios no identificados a establecer sesiones CIFS no autenticados
MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution(917159)(windows-hotfix-ms06-035)	Ejecución de código remoto a sistemas
SMB signing disabled (cifs-smb-signing-disabled)	no permite la firma SMB ya que lo que hace es confirmar su autenticación y permite evitar los ataques del hombre en el medio
SMB signing not required (cifs-smb-signing-not-required	permite pero no requiere de la firma de SMB, ESTA permite que el destinatario de los paquetes SMB se autentique
ICMP timestamp response (generic-icmp-timestamp	La respuesta ICMP contiene fecha y hora de la máquina virtual lo cual llegaría a ser perjudicial para generar números aleatorios basados en el tiempo para solucionar se aplica Deshabilitar timestamp
NetBIOS NBSTAT Traffic Amplification (netbios-nbstat-amplification)	esto puede ser utilizado para realizar ataques de amplificaciones de tráficos contra activos

REALIZADO POR: (CRUZ NUBE, 2015)

En la tabla 9-3 se observa en que campos y protocolos afecta el no contar con un buen conocimiento de seguridad en sistemas informáticos

Tabla 2-3 Vulnerabilidades del sistema operativo vista de 64 bits

VULENERABILIDADES DEL SISTEMA OPERATIVO VISTA DE 64 BITS	
VULNERABILIDAD	DESCRIPCION
MS09-050: Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517) (windows-hotfix-ms09-050)	Permita la ejecución remota de código si un atacante envía un paquete SMB especialmente diseñado a un equipo que ejecuta el servicio de servidor.
MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (windows-hotfix-ms10- 054)	Consiste en un desbordamiento de buffer remoto que compromete un equipo destino ejecuta un código arbitrario y realizar denegación de servicio.
MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (windows-hotfix-ms11-020)	Permite la ejecución remota de un código si un atacante crea un paquete SMB especialmente diseñado y lo envía a un sistema afectado
SMB signing disabled (cifs-smb-signing-disabled)	no permite la firma SMB ya que lo que hace es confirmar su autenticación y permite evitar los ataques del hombre en el medio
SMB signing not required (cifs-smb-signing-not-required)	este permite pero no requiere de la firma de SMB, la firma SMB permite que el destinatario de los paquetes SMB se autentique y
ICMP timestamp response (generic-icmp-timestamp)	La respuesta ICMP contiene la fecha y la hora de la máquina virtual lo cual llegaría a ser perjudicial para generar números aleatorios basados en el tiempo para solucionar se aplica Deshabilitar timestamp
TCP timestamp response (generic-tcp-timestamp)	Se puede utilizar para aproximar un host remoto del tiempo de actividades y podría ayudar a nuevos ataques su solución deshabilitar TCP
NetBIOS NBSTAT Traffic Amplification (netbios-nbstat-amplification)	esto puede ser utilizado para realizar ataques de amplificaciones de tráficos contra activos

REALIZADO POR: (CRUZ NUBE, 2015)

En la tabla 10-3 muestra los errores de seguridad que presenta Windows server 2008

Tabla 8-3 vulnerabilidades del sistema operativo Windows server 2008

VULNERABILIDADES DEL SISTEMA OPERATIVO WINDOWS SERVER 2008 DE 64 BITS	
VULNERABILIDAD	DESCRIPCIÓN
SMB signing disabled (cifs-smb-signing-disabled)	no permite la firma SMB ya que lo que hace es confirmar su autenticación y permite evitar los ataques del hombre en el medio
SMB signing not required (cifs-smb-signing-not-required)	este permite pero no requiere de la firma de SMB, la firma SMB permite que el destinatario de los paquetes SMB se autentique y
ICMP timestamp response (generic-icmp-timestamp)	La respuesta ICMP contiene la fecha y la hora de la máquina virtual lo cual llegaría a ser perjudicial para generar números aleatorios basados en el tiempo para solucionar se aplica Deshabilitar timestamp
TCP timestamp response (generic-tcp-timestamp)	Se puede utilizar para aproximar un host remoto del tiempo de actividades y podría ayudar a nuevos ataques su solución deshabilitar TCP
NetBIOS NBSTAT Traffic Amplification (netbios-nbstat-amplification)	esto puede ser utilizado para realizar ataques de amplificaciones de tráficos contra activos

REALIZADO POR: (CRUZ NUBE, 2015)

Si se va observando en las tablas cada sistema operativo va decrementando el número de vulnerabilidades debido a que salen nuevas actualizaciones pero el problema más común es la configuración del usuario ver tabla 11-3

Tabla 4-3 Vulnerabilidades del sistema operativo Windows seven de 64 bits

VULNERABILIDADES DEL SISTEMA OPERATIVO WINDOWS SEVEN DE 64 BITS	
VULNERABILIDAD	DESCRIPCIÓN
SMB signing disabled (cifs-smb-signing-disabled)	no permite la firma SMB ya que lo que hace es confirmar su autenticación y permite evitar los ataques del hombre en el medio
SMB signing not required (cifs-smb-signing-not-required)	este permite pero no requiere de la firma de SMB, la firma SMB permite que el destinatario de los paquetes SMB se autentique y
TCP timestamp response (generic-tcp-timestamp)	Se puede utilizar para aproximar un host remoto del tiempo de actividades y podría ayudar a nuevos ataques su solución deshabilitar TCP
UPnP SSDP Traffic Amplification (upnp-ssdp-amplification)	Se utiliza para buscar una red para dispositivos UPnP puede afectar cuando una respuesta M-SEARCH es aproximadamente 30 veces la tamaño de la solicitud y puede ser distribuido a través de múltiples respuestas de múltiples hosts,
NetBIOS NBSTAT Traffic Amplification (netbios-nbstat-amplification)	esto puede ser utilizado para realizar ataques de amplificaciones de tráficos contra activos

REALIZADO POR: (CRUZ NUBE, 2015)

En la tabla 5-3 encontramos una vulnerabilidad en Windows eight

Tabla 5-3 Vulnerabilidades en el sistema Operativo eight de 64 bits

VULNERABILIDADES DEL SISTEMA OPERATIVO WINDOWS EIGHT DE 64 BITS	
VULNERABILIDAD	DESCRIPCIÓN
NetBIOS NBSTAT Traffic Amplification (netbios-nbstat-amplification)	esto puede ser utilizado para realizar ataques de amplificaciones de tráficos contra activos

REALIZADO POR: (CRUZ NUBE, 2015)

3.5 Requerimientos

Para obtener las vulnerabilidades en los sistemas operativos se utiliza las siguientes herramientas software como se ve en la tabla 6-3

Tabla6-3 Requerimientos de la investigación

INSTRUMENTO	CARACTERISTICAS
Kali Linux	386i versión 2.3 -2015
VMware Workstation	
Windows8	64bits
Windos7	64bits
Windows vista	64bits
Windows XP	64bits
Windows server 2008	64bits
Nessus	
Nexpose	

REALIZADO POR : (CRUZ NUBE,2015)

3.6 Validación de instrumentos

Para la realización de pruebas para detectar la vulnerabilidades de los Sistema operativos se utiliza Kali Linux es la nueva generación de Linux Backtrack es una distribución que generalmente se utiliza para auditorias informáticas y pruebas de penetración ya que cuenta con herramientas que se dedican a buscar, controlar, explotar las vulnerabilidades de un sistema informático.

Cuenta con más de 300 herramientas para realizar pruebas de penetración, tiene un entorno seguro cuenta con parches, y lo más importante es gratuito.

Se proporcionará una breve explicación de los demás instrumentos software que se utilizan en la investigación.

- *VMware Workstation*

Es un programa que me permite virtualización, es decir que me permite correr varias máquinas virtuales en una sola maquina física, estas máquinas virtuales instaladas comparten recursos de la física en diferentes entornos.

Las maquinas instaladas pueden tener diferentes sistemas operativos y muchas aplicaciones.

- *Windows8*

Es un sistema operativo de la familia de Windows es uno de las últimas versiones que puso en el mercado Microsoft, sobresalen ciertas características de las anteriores como el que cambio los menús de inicio, en la interacción y la conectividad.

Se utiliza este SO para analizar los niveles de seguridad que han ido evolucionando Windows

- *Windows7*

Pertenece a la familia de Microsoft son versiones pasadas pero se utiliza cada una de las versiones para analizar los niveles de seguridad que contaban y observar que Windows iba mejorando en el tema de seguridad.

Las características más notables de Windos7 n fueron la mejora en el reconocimiento en la escritura, soporte de discos duros virtuales, se integraron características de seguridad.

- *Windows vista*

Son versiones antiguas pero que en la investigación se lo utiliza para observar si los errores que cometen los usuarios finales son las mismas que las versiones actuales solo con actualizaciones anteriores.

En esta versión sus características eran menos confiables.

- *Windows Xp*

Esta versión de Windows fue con la que más se familiarizaron los usuarios por su fácil manejo, cuenta con varias versiones de la misma. Es el sistema operativo más popular lo que llevo a desarrollar casi la mayoría de drives para este sistema operativo es decir es compatible con la mayoría de aplicaciones por eso se usa hasta la actualidad, ejemplo los cajeros automáticos posen un sistema que solo puede ser instalado y ejecutado en este sistema operativo.

- *Windows server 2008*

Es uno de los últimos sistemas operativos para servidores, sus características relevantes se centran en la seguridad, administración, mejora en la pila IPv6.

- *Nessus*

Es un programa que permite escanear vulnerabilidades de cualquier sistema operativo, reside en nessud que es nessus demonio que realiza escaneos al objetivo y nessus al cliente que muestra el reporte de escaneos.

- *Nexpose*

Nexpose es un programa que está diseñado para el análisis de vulnerabilidades en redes, también identifica cada exploración de vulnerabilidades encontradas en los sistemas operativos detecta programas maliciosos.

3.7 Ambiente de pruebas.

Para el ambiente de pruebas se instaló sistemas operativos Windows de 64 bits debido a que el laboratorio de cisco solo posee un sistema operativo que corren sus máquinas y

es Windows 7. Por otra parte para la comprobación de la hipótesis se usó un ambiente común en donde coexistían sistemas operativos como Windows xp, vista, server 2008, Windows seven, eight . Para representar didácticamente se usa el siguiente Figura 6-3

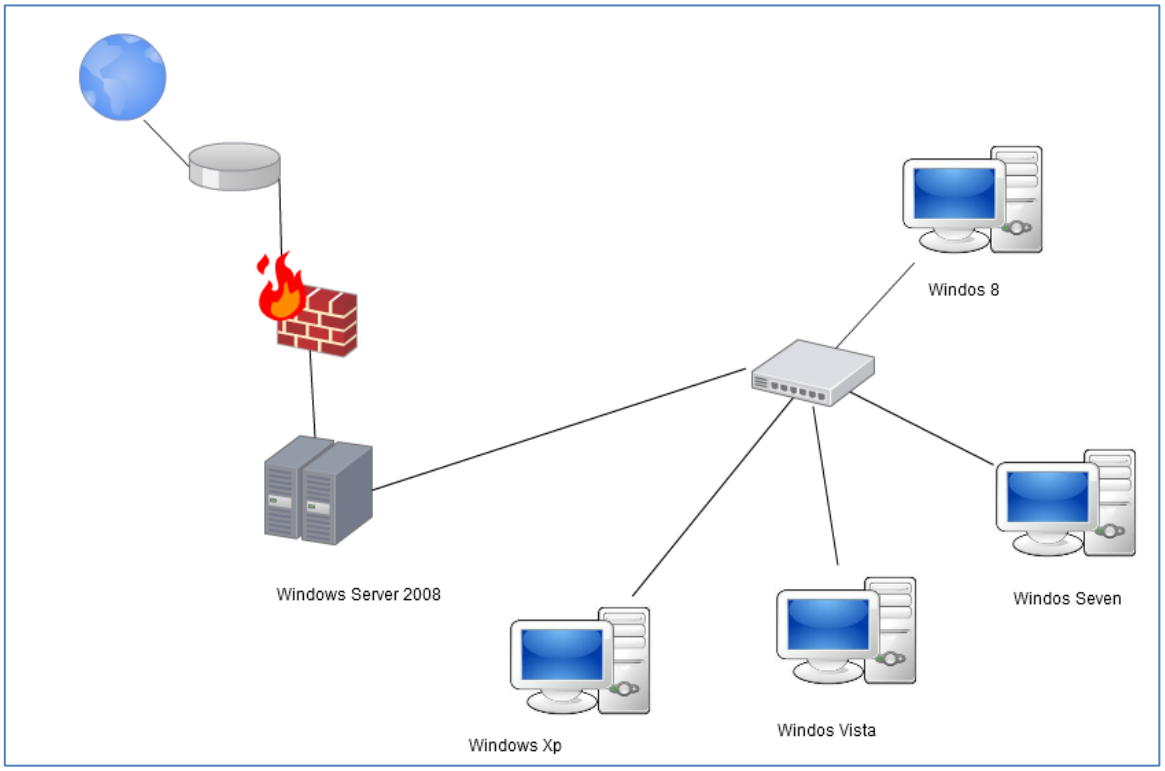

Figura 6-3 Ambiente de pruebas de la investigación
REALIZADO POR: (CRUZ, NUBE, 2015)

CAPITULO IV

4. SOLUCIÓN DE ERRORES EN LOS SISTEMAS OPERATIVOS WINDOWS DE 64 BITS A NIVEL DE USUARIO FINAL CON LA APLICACIÓN DE LA METODOLOGÍA OSSTMM

4.1 Preparación de Sistemas Operativos

Se procede a la preparación de todos los elementos primero los sistemas operativos empleados en este trabajo investigativo

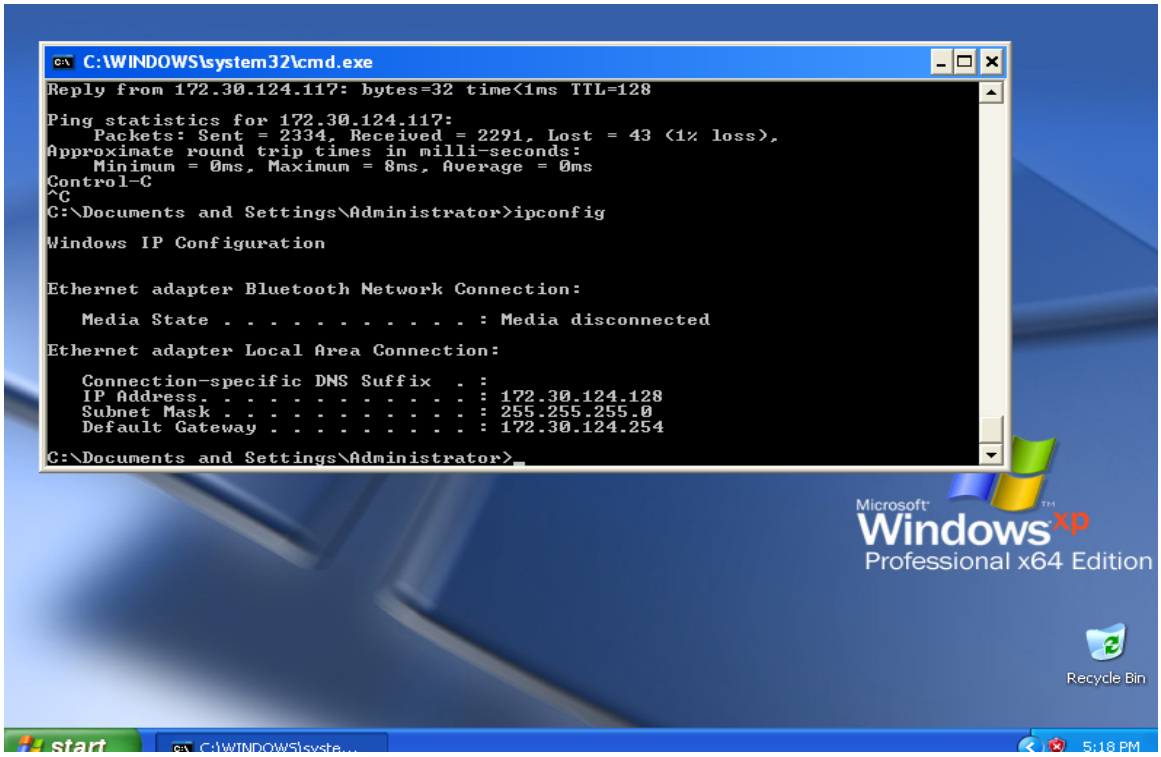

Figura 1-4 Sistema Operativo Windows de 64 bits Xp
REALIZADO POR: (CRUZ, NUBE, 2015)

Para preparar este sistema operativo Xp primero se levantó un ipconfig que es un comando que verifica la conectividad de las redes obteniendo la dirección Ip 172.30.124.128, mascara de la red 255.255.255.0 y el gateway 172.30.124.254 se verifica en la figura 1-4

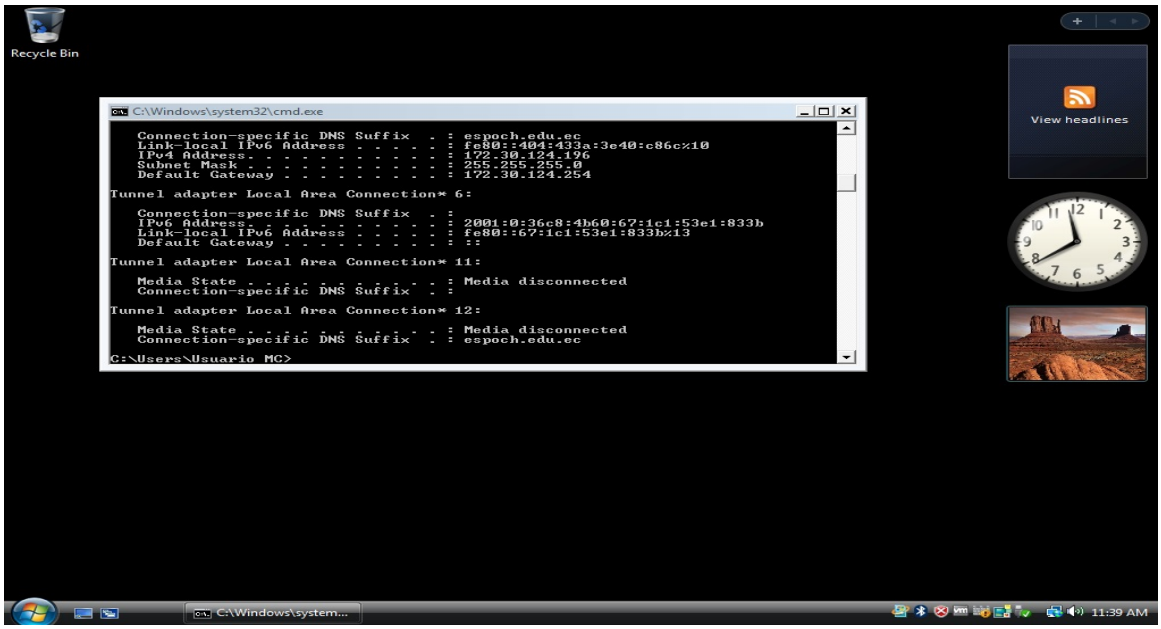

Figura 2-4 Sistema Operativo Windows Vista de 64 bits
REALIZADO POR: (CRUZ, NUBE, 2015)

Sistema operativo Vista se realizó un up de servicio de red con un ipconfig obteniendo la dirección Ip 172.30.124.196, mascara de la red 255.255.255.0 y el gateway 172.30.124.254 ver figura 2-4

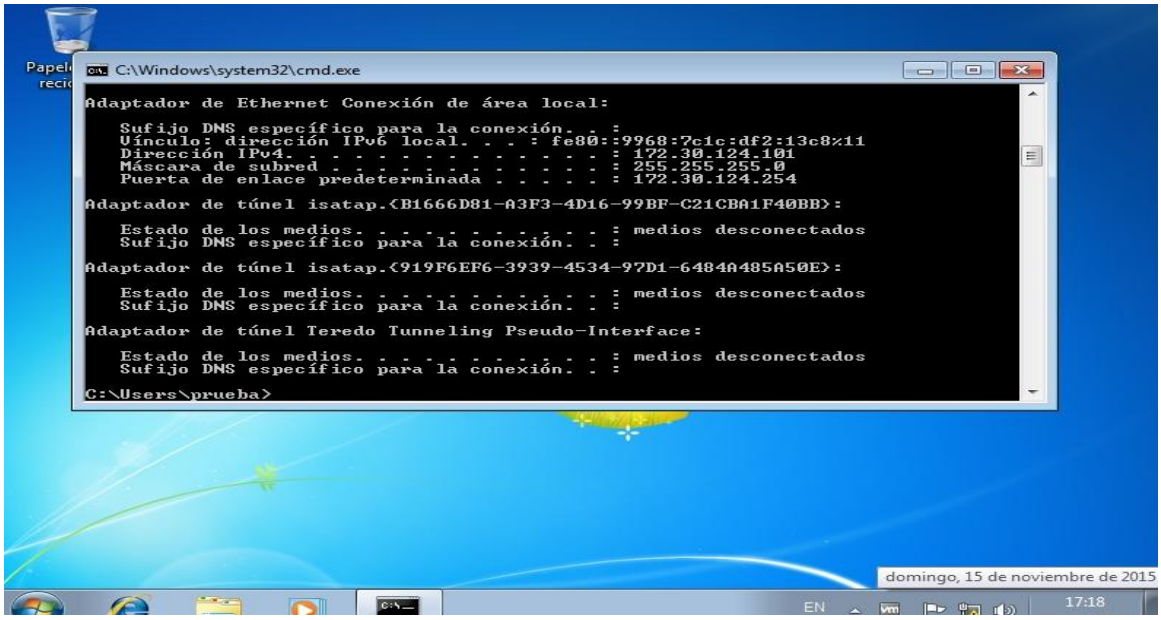

Figura 3-4 Sistema Operativo Windows 7 de 64 bits
REALIZADO POR: (CRUZ, NUBE, 2015)

Para la práctica que se realizo es fundamental que todos los equipos informáticos se encuentren en red y conectadas para lo cual es necesario el levantamiento del servicio con el comando que me visualiza la ip, mascara de red y Gateway ver figura 3-4

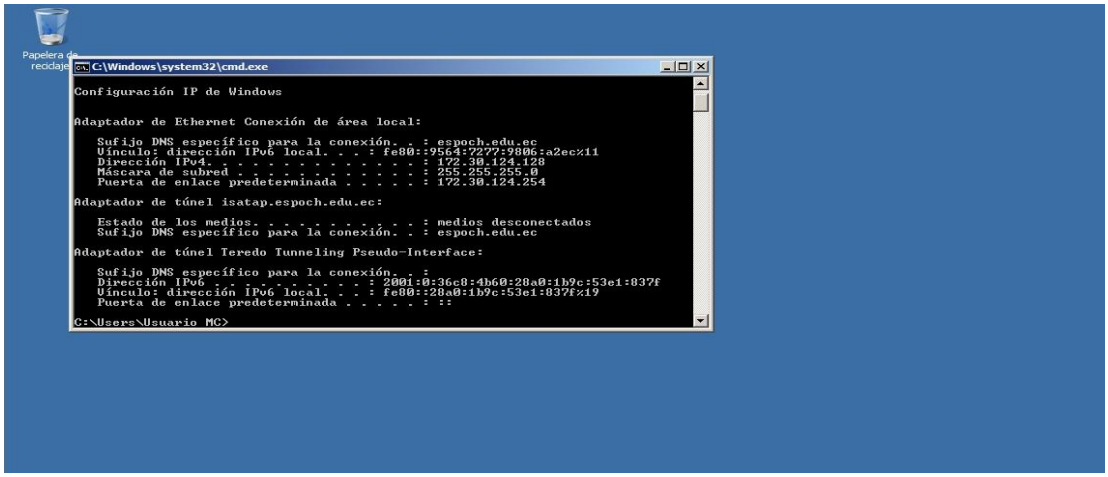

Figura 4-4 Sistema Operativo Windows server 2008 de 64 bits
REALIZADO POR: (CRUZ, NUBE, 2015)

Windows server 2008 es una de las familias de Windows que se dedica específicamente a los servidores como se lo ha hecho en los anteriores sistemas operativos se levanta el servicio de red y con lo cual obtenemos su dirección ip, mascara de red y gateway por defecto ver figura 4-4

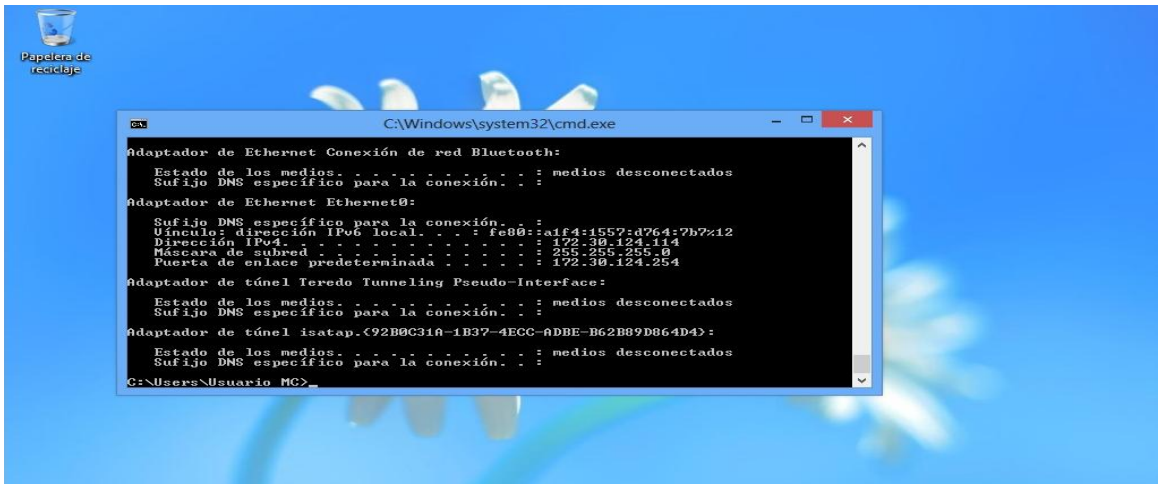

Figura 5-4 Sistema Operativo Windows 8 de 64 bits
REALIZADO POR: (CRUZ, NUBE, 2015)

Como se observa en la pantalla observamos el adaptador de red está en conexión utilizando el comando ipconfig para rastrear su dirección 172.30.124.114 mascara de red 255.255.255.0 ya que pertece a la clase c y un Gateway por defecto 172.30.124.254

4.2 Rastreo de vulnerabilidades

Luego de tener listo los sistemas operativos y de verificar la conectividad entre toda la red se procede a seguir la metodología para el análisis y corrección de vulnerabilidades en sistemas operativos de 64 bits.

A continuación se procede a ejecutar NESSUS y NEXPOUSE que son analizadores de vulnerabilidades. Se ha usado los dos para mejorar los resultados de búsqueda.

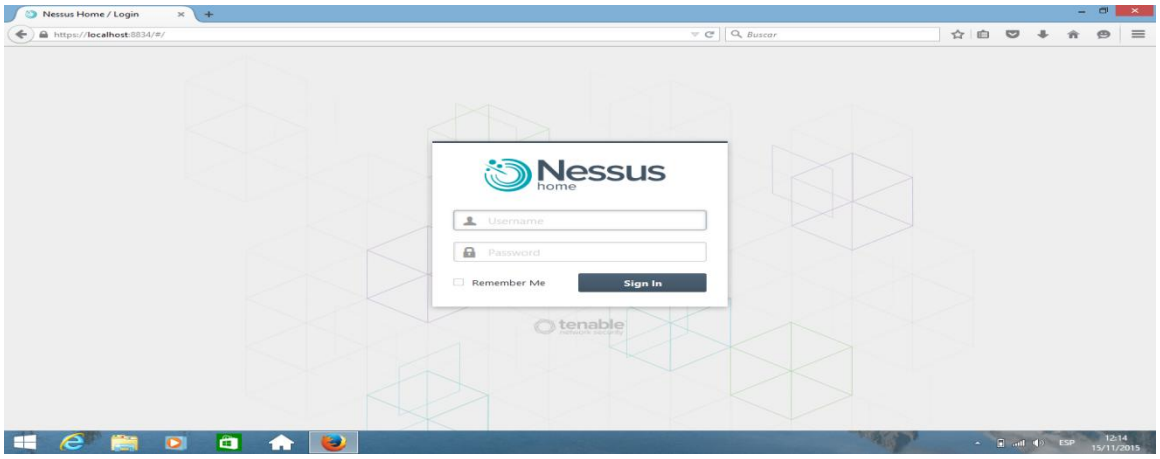

Figura 6-4 Ejecución de Nessus
REALIZADO POR: (CRUZ, NUBE, 2015)

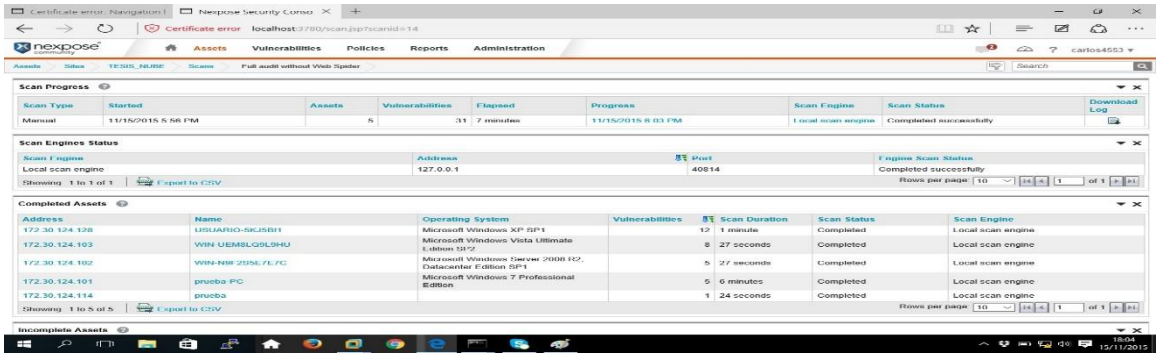

Figura 7-4 Ejecución de Nexpose
REALIZADO POR: (CRUZ, NUBE, 2015)

4.3 Análisis del Levantamiento de Información

Con los resultados obtenidos se realizó la siguiente matriz de vulnerabilidades en donde se puede usar como un marco de trabajo para la comprobación y a su vez para la mitigación debido a que todas las vulnerabilidades encontradas a nivel del sistema operativo son mitigables.

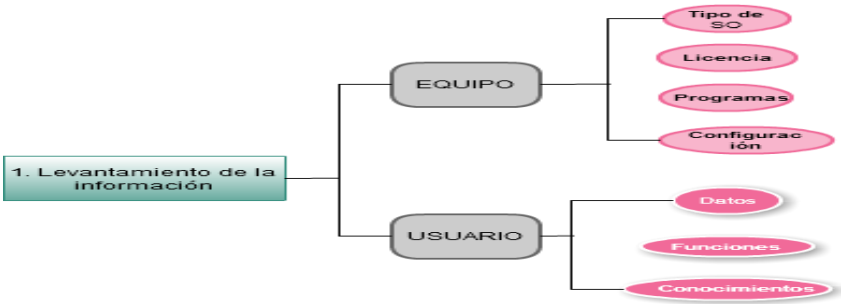

Figura 8-4 Proceso para recopilar información del equipo y usuario
REALIZADO POR: (CRUZ, NUBE, 2015)

El levantamiento de la información hace referencia al proceso en el cual se tiene que recopilar datos tanto del usuario como del equipo. Los datos del usuario son a cerca del conocimiento sobre informática y seguridad de la información, sobre el equipo es para tener una visión clara con respecto al uso que se da al equipo, componentes de hardware es decir capacidad del equipo en cuanto a velocidad y almacenamiento, además las aplicaciones que corren con el resumidas en el uso que se da al equipo mismo que se cotejara con el conocimiento del usuario para saber si está capacitado o no. Ver tabla1-4

Tabla 1-4 Plantilla de equipo

PLANTILLA PARA EL LEVANTAMIENTO DE INFORMACION (EQUIPO)

MARCA	PROCESADOR	DISCO DURO	SISTEMA OPERATIVO	PROGRAMAS INSTALADOS	ANTIVIRUS Y FIREWALL	OBSERVACIONES EN LAS CONFIGURACIONES

REALIZADO POR: (CRUZ, NUBE, 2015)

Como se observa en la tabla anterior se realizó plantillas para obtener información tanto del equipo como del usuario ver tabla 2-4

Tabla 2-4 Plantilla de usuario

PLANTILLA PARA EL LEVANTAMIENTO DE INFORMACION (USUARIO)

DAROS DEL USUARIO	CARGO	TIEMPO DE TRABAJO	TITULO PROFESIONAL	CONOCIMIENTOS DE INFORMATICA	CONOCIMIETNO SOBRE SEGURIDAD	CONOCIMIENTOS SOBRE REDES

REALIZADO POR: (CRUZ, NUBE,2015)

4.4 Análisis y solución de vulnerabilidades

Una vez que la información en cuanto al sistema operativo y usuario se tenga levantada procedemos al segundo paso que se detalla a continuación.

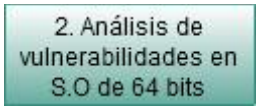

Figura 9-4 Análisis de Vulnerabilidades
Realizado por: Investigador (Nube Cruz)

En este punto se es un profesional quien hace uso de esta metodología puede levantar analizadores de vulnerabilidades en cuanto a sistemas operativos se refiera mismos que pueden ser NESSUS o NEXPOUSE; o caso contrario se puede verificar el siguiente marco de trabajo y poner en práctica las soluciones detalladas en la matriz obviamente dependido del sistema operativo que usa ver Figura 3-4.
Las vulnerabilidades que se identifican en los sistemas operativos son:

Microsoft Server Service / CanonicalizePathName() Remote Code Execution Vulnerability (dcerpc-ms-netapinetpathcanonicalize-dos)

Trata de un desbordamiento de buffer remoto que compromete un equipo de destino, esta vulnerabilidad surge cuando el servicio procesa un mensaje malicioso en las comunicaciones RPC, un atacante puede tener éxito y ejecutar códigos arbitrarios y realizar denegación de servicios.

La solución para este tipo de vulnerabilidad es instalar el parche http://download.microsoft.com/download/9/0/b/90b8dbba-09c1-4b27-b0c40cc13706823a/Windows2000-KB921883-x86-ENU.EXE

Es una vulnerabilidad que afecta a Windows Xp

MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687) (windows-hotfix-ms09-001)

Este tipo de vulnerabilidad afecta a Xp y podrían permitir la ejecución de códigos remotos en sistemas afectados, se podrían instalar programas ver cambiar, modificar datos y crear cuentas de usuarios nuevas con todos los derechos.

Aquí se recomienda que los puertos de accesos sean mínimas para evitar estos contratiempos para corregir se instala el parche a partir de http://go.microsoft.com/fwlink/?LinkId=132991

MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468) (windows-hotfix-ms10)

Esta vulnerabilidad permite la ejecución remota de códigos si un atacante crea un paquete SMB especialmente diseñado y enviado a paquetes en un sistema afectado su solución es instalar el parche http://go.microsoft.com/fwlink/?LinkId=155976.

MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (windows-hotfix-ms10-054

Es una vulnerabilidad típica de Xp consiste en un desbordamiento de buffer remoto que compromete un equipo destino ejecuta un código arbitrario y realizar denegación de servicio.

Su solución es instalar el parche recomendado desde la página http://download.microsoft.com/download/9/0/b/90b8dbba-09c1-4b27-b0c4-0cc13706823a/Windows2000-KB921883-x86-ENU.EXE

MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (windows-hotfix-ms11-020)

Permite la ejecución remota de un código si un atacante crea un paquete SMB especialmente diseñado y lo envía a un sistema afectado, aqueja al SO Xp su solución instalar el parche http://go.microsoft.com/fwlink/?LinkId=212236

CIFS NULL Session Permitted (cifs-nt-0001)

Permite a los usuarios no identificados a establecer sesiones CIFS no autenticados, esos usuarios son capaces de enumerar locales, usuarios dominios, servidores, acciones y capaces de acceder a varios servicios y permite que los atacantes realicen ataques sofisticados para mitigar se Configurar a partir Microsoft Knowledge Base Article Q246261afecta sistemas operativos XP.

MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (windows-hotfix-ms06-35)

Ejecución de código remoto a sistemas vulnerables Xp su solución instalar o descargar el Update o el parche a partir de http://go.microsoft.com/fwlink/?LinkId=64331

SMB signing disabled (cifs-smb-signing-disabled)

Esta vulnerabilidad en Xp, Server 2008, y seven no permite la firma SMB ya que lo que hace es confirmar su autenticación y permite evitar los ataques del hombre en el medio su solución es la configuración a partir del siguiente enlace this TechNet article

SMB signing not required (cifs-smb-signing-not-required)

Esta vulnerabilidad afecta a Xp y a Vista este permite pero no requiere de la firma de SMB, la firma SMB permite que el destinatario de los paquetes SMB se autentique y evitar los ataques del hombre en el medio. Su solución configurar a partir del siguiente articulo this TechNet article.

ICMP timestamp response (generic-icmp-timestamp)

La respuesta ICMP contiene la fecha y la hora de la máquina virtual lo cual llegaría a ser perjudicial para generar números aleatorios basados en el tiempo para solucionar se aplica Deshabilitar timestamp ICMP a partir del comando de control firewalls de windows
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/enus/

hnw_understanding_firewall.mspx?mfr=true . Afecta a Xp y a vista

NetBIOS NBSTAT Traffic Amplification (netbios-nbstat-amplification)

NetBIOS NBSTAT utiliza UDP afecta en Xp, vista seven y eigh esto puede ser utilizado para realizar ataques de amplificaciones de tráficos contra activos su solución es Restringiendo el acceso a los netBios solo a servicios activos de confianza.

TCP timestamp response (generic-tcp-timestamp)

Se puede utilizar para aproximar un host remoto del tiempo de actividades y podría ayudar a nuevos ataques su solución deshabilitar TCP desde panel de control afecta a los SO Windows vista

UPnP SSDP Traffic Amplification (upnp-ssdp-amplification)

Se utiliza para buscar una red para dispositivos UPnP puede afectar cuando una respuesta M-SEARCH es aproximadamente 30 veces la tamaño de la solicitud y puede ser distribuido a través de múltiples respuestas de múltiples hosts, y porque utiliza UDP, esto puede ser usado para llevar a cabo ataques de amplificación de tráfico contra otros activos, por lo general en forma de distribuyen reflejado denegación de servicio su solución es Restringir el acceso a la función UPnP para activos solamente de confianza.

Como se indicó anteriormente a continuación se indica las tablas de soluciones de vulnerabilidades de los sistemas informáticos de Windows de 64 bits

Tabla 3-4 Solución de vulnerabilidades del Sistema operativo 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 a partir 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-	Configurar a partir this TechNet article

signing-disabled)	
SMB signing not required (cifs-smb-signing-not-required	Configurar a partir 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

REALIZADO POR: (CRUZ, NUBE, 2015)

Solución de errores de Windows vista

Tabla 4-4 Solución de vulnerabilidades del sistema operativo windows Vista

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

REALIZADO POR: (CRUZ, NUBE, 2015)

Para dar Solución a las vulnerabilidades se configuran desde ciertas herramientas y protocolos Windows server 2008

Tabla 5-4 Solución de vulnerabilidades en el sistema operativo 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 a partir this TechNet article
SMB signing not required (cifs-smb-signing-not-required)	Configurar a partir 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

REALIZADO POR: (CRUZ, NUBE, 2015)

En la tabla 6-4 muestra que las vulnerabilidades en el protocolo TCp, UPnP , SMB y NetBios y su solución

Tabla 6-4 Solución de vulnerabilidades en el sistema operativo windows seven de 64 bits

VULNERABILIDADES DEL SISTEMA OPERATIVO WINDOWS SEVEN DE 64 BITS	
VULNERABILIDAD	SOLUCIÓN
SMB signing disabled (cifs-smb-signing-disabled)	Configurar a partir this TechNet article
SMB signing not required (cifs-smb-signing-not-required)	Configurar a partir this TechNet article
TCP timestamp response (generic-tcp-timestamp)	deshabilitar TCP desde paanel 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)	Restirngiendo el acceso a los netBios solo a servicios activos de confianza

REALIZADO POR: (CRUZ, NUBE, 2015)

Ver soluciones de las vulnerabilidades en la tabla 18-4 del sistema operativo Windows eight

Tabla7-4 solución vulnerabilidades del sistema operativo Windows eight de 64 bits

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

REALIZADO POR: (CRUZ, NUBE, 2015)

4.5 Análisis de riesgos

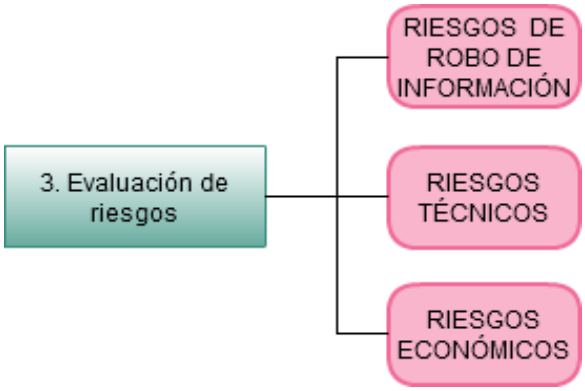

Figura 10-4 Análisis de riesgos
Realizado por: (CRUZ, NUBE, 2015)

Una vez que se tiene detectados los errores y vulnerabilidades que poseen los sistemas operativos en este punto se hace una evaluación de riesgos que se presentan por ejemplo en cuanto a información se refiere , si es que con el problema que se tiene conlleva a riesgos de información técnicos o económicos que se detalla a continuación.

a) *Riesgos de la información*

La información que es maneja en los laboratorios de CISCO no conlleva a un riesgo de mayor volumen debido a que no se manejan datos de relevancia que pueda afectar a futuro.

b) *Riesgos Técnicos*

En el Laboratorio de CISCO que se ejecutaron las pruebas no existen riesgos técnicos ya que el departamento cuenta con sus debidas actualizaciones y configuraciones de los Equipos, además cave recalcar que son laboratorios que cuentan con el personal que manejan y conocen sobre el tema, pero en caso de no ser así en otros equipos corrieran riesgos de ser infectados con virus y troyanos puerta de atrás que darán acceso a atacantes que tendrán consecuencia con pérdida de información daño a los equipos y conllevaría a riegos técnicos.

c) *Riesgos económicos*

En este literal se hace referencia con el literal anterior se hablaba de una perdida de información y daño de equipos que obviamente tuviera que soportar riesgos económicos cundo el equipo de cómputo soporta un daño una mala configuración implica economía algo que no sucede en este laboratorio ya que cuentan con un muy buen soporte técnico.

4.6 Comprobación de la Hipótesis.

¿La utilización de una Metodología OSSTMM permitirá la detección de errores de seguridad y vulnerabilidad en sistemas operativos de 64 bits a nivel de usuario final?

Para la comprobación de la hipótesis 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 la comprobación de la hipótesis 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.

Tabla 8-4 Muestra única

Estadísticos para una muestra

	N	Media	Desviación típ.	Error típ. de la media
Nu_Vulnerabilidad	40	4,13	2,323	,367

Realizado por: (CRUZ, NUBE, 2015)

Tabla 9-4 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

Realizado por: (Cruz, Nube, 2015)

Como se puede observar la significancia bilateral es mayor a alfa (α=0,05) por tanto se comprueba la hipótesis.

CONCLUSIONES

- Si las aplicaciones instalados por los usuarios finales en los sistemas operativos son inadecuados pueden ser burlados fácilmente
- Se puede revelar que información puede obtenerse desde el exterior
- Esta investigación pone a prueba la seguridad que le dan los usuarios a sus sistemas operativos y observar si resistirán a un ataque.
- En la investigación los usuarios finales a los que se realizaron la prueba no tienen conocimientos básicos de seguridad en los sistemas operativos ya que en su mayor parte es personal administrativo y no técnico, por lo que exponen sus equipos a vulnerabilidades informáticas.
- En la institución no cuentan con antivirus con licencias y esto conlleva a que en los sistemas operativos no estén activados es decir no acceden a las actualizaciones miceisof que incluyen importantes parches de seguridad
- 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

RECOMENDACIONES

- Utilizar aplicaciones seguras y garantizadas para obtener un sistema operativo confiable y difícil de ser burlado
- Tener mayor seguridad en los sistemas operativos para que no se fugue información desde el exterior
- Capacitar con mayor frecuencia a los usuarios finales que tienen a cargo equipos informáticos en el tema de seguridad en Sistemas operativos ya que tienen a su cargo información importante
- Que todos los usuarios tengan en sus equipos informáticos antivirus con licencias para que puedan acceder a las actualizaciones de seguridad sobre su sistema operativo y que tengan conocimiento en configuración de la seguridad de SO
- En todas las entidades públicas y privadas pongan más énfasis a la seguridad informático y no lo tomen como una pérdida de dinero.
- Se siga utilizando la metodología OSSTMM par a detectar los errores de seguridad en los SO ya que vienen actuales sistemas operativos con mayor seguridad en los errores que fueron detectados pero con nuevos errores.

BIBLIOGRAFIA

1. GARCIA ALFONSO, CERVIGON HURTADO, & MARIA DEL PILAR ALEGRE RAMOS. (2011). *Seguridad Informatica Ed.11 Paraninfo* (primera). España: Editorial Paraninfo.

2. GAINZA SANCHEZ SABINO ISAO. (2009). *Propuesta de aplicación de una metodología para la seguridad informática en la división de ciencias básicas*. Universidad Nacional Autonoma de Mexico, Mexico.

3. BONIVENTO.GERMAN (2014, mayo). *Analisis y diseño de sistemas cap 1*. Colombia. Recuperado a partir de http://es.slideshare.net/GermanBonivento/analisis-y-diseo-de-sistemas-cap-1

4. HERZOG PETE. (2003). OSSTMM 2.1. Manual de la Metodología Abierta de Testeo de Seguridad. ISECOM.

5. ING FERRER RODRIGO. (2001). Como lograr una estrategia confiable y efectiva de seguridad de la información. Recuperado 29 de septiembre de 2015, a partir de http://www.sisteseg.com/files/Microsoft_Word_-_SEMINARIO_SEGURIDAD_DE_LA_INFORMACION_web2.pdf

6. GUTIERRES.JANNETH (2013). Sistemas Operativos I [Plan de Estudio o Currículo de Asignatura]. Recuperado 26 de octubre de 2015, a partir de https://sites.google.com/site/sisoper1/plan-de-estudio-o-curriculo

7. AREITIO BERTOLÍN JAVIER. (2008). S*eguridad de la información. Redes, informática y sistemas de información* (Clara M. de la Fuente Rojo). Madrid España: Editorial Paraninfo.

8. RAMIREZ LOPEZ JORGE. (2009). *DESARROLLO DE UN ESQUEMA DE ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN E N SISTEMAS OPERATIVOS PARA UNA ORGANIZACIÓN DE LA ADMINISTRACIÓN PUBLICA FEDERAL* (Tesis). Instituto Politécnico Nacional, Mexico. Recuperado a partir de http://tesis.ipn.mx/bitstream/handle/123456789/8451/40.pdf?sequence=1

9. ALBORS JOSEP. (2015, febrero). Las vulnerabilidades en sistemas operativos marcan el inicio de 2015. Recuperado a partir de http://blogs.protegerse.com/laboratorio/2015/02/04/las-vulnerabilidades-en-sistemas-operativos-marcan-el-inicio-de-2015/

10. MAGISTER DAVID LUIS LA RED MARTINEZ. (2001). *Sistemas Operativos*. Universidad Nacional del Nordeste de argentina. Recuperado a partir de http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/computot.PDF

11. MICROSOFT. (2009). Índice de explotabilidad de Microsoft. Recuperado 13 de noviembre de 2015, a partir de https://technet.microsoft.com/es-es/security/cc998259.aspx

12. MICROSOFT WINDOWS. (2015). Firewall de Windows de principio a fin. Recuperado 2 de julio de 2015, a partir de http://windows.microsoft.com/es-419/windows-8/windows-firewall-from-start-to-finish

13. PATIÑO SANCHEZ, J., & LAMILLA RUBIO, E. (2009). *Desarrollo de politicas de seguridad informatica e implantación de cuatro dominios en base a la norma 27002 para el área de hardware en la empresa uniplex systems s.a en Guayaquil*. Universidad Poliecnica de Litoral, Guayaquil. Recuperado a partir de http://www.dspace.espol.edu.ec/handle/123456789/7709

14. HERZOG.PETO (2010). OSSTMM.3.

15. PINZON LILIANA CAROLINA MIHDIBADI TALERO Y JHON A. BOHADA. (2014). Pruebas de Intrusión y Metodologías Abiertas. *Ciencia, Innovación y Tecnología*, *1*(0), 25-38.

16. POLICIA CIBERNETICO DE GERRERO. (2014). Seguridad Informatica Para Usuarios Finales 01 [ciberneticagro.blogspot.mx]. Recuperado a partir de http://ciberneticagro.blogspot.mx/2014/08/seguridad-informatica-para-usuarios.html

17. GUTIERRES YANNETH. (2013). ¿Qué es Seguridad Informática? - Sistemas Operativos I [Plan de Estudios]. Recuperado a partir de https://sites.google.com/site/sisoper1/home/conceptos-de-seguridad-y-proteccion

ANEXOS

ANEXO A.

PLANTILLAS DE IMNFORME DE LA, METODOLOGIA OSSTMM

Security Test Audit Report

OSSTMM 3.0 Security Verification Certification

Report ID		Date	
Lead Auditor		Test Date Duration	
Scope and Index		Vectors	
Channels		Test Type	

I am responsible for the information within this report and have personally verified that all information herein is factual and true.

SIGNATURE	COMPANY STAMP/SEAL
ISECOM Certification #	ISECOM Certification #

OPERATIONAL SECURITY VALUES		CONTROLS VALUES	
Visibility		Authentication	
Access		Indemnification	
Trust		Resilience	
		Subjugation	
LIMITATIONS VALUES		Continuity	
Vulnerability		Non-Repudiation	
Weakness		Confidentiality	
Concern		Privacy	
Exposure		Integrity	
Anomaly		Alarm	
OpSec		True Controls	
Limitations		Security Δ	
True Protection		Actual Security	

OVERVIEW

This Open Source Security Testing Methodology Manual provides a methodology for a thorough security test. A security test is an accurate measurement of security at an operational level, void of assumptions and anecdotal evidence. A proper methodology makes for a valid security measurement that is consistent and repeatable.

ABOUT ISECOM

ISECOM, the creator and maintainer of the OSSTMM, is an independent, non-profit security research organization and certification authority defined by the principles of open collaboration and transparency.

RELATED TERMS AND DEFINITIONS

This report may refer to words and terms that may be construed with other intents or meanings. This is especially true within international translations. This report attempts to use standard terms and definitions as found in the OSSTMM 3 vocabulary, which has been based on NCSC-TG-004 (Teal Green Book) from the US Department of Defense where applicable.

PURPOSE

The primary purpose of this Audit Report is to provide a standard reporting scheme based on a scientific methodology for the accurate characterization of security through examination and correlation in a consistent and reliable way. The secondary purpose is to provide guidelines which when followed will allow the auditor to provide a certified OSSTMM audit.

PROCESS

This Audit Report must accompany the full security test report document that provides evidence of the test and the results as defined in the statement of work between the testing organization and the client.

VALIDITY

For this OSSTMM Audit Report to be valid, it must be filled out clearly, properly, and completely. The OSSTMM Audit Report must be signed by the lead or responsible tester or analyst and accompany include the stamp of the company which holds the contract or sub-contract of the test. This audit report must show under COMPLETION STATUS which Channel and the associated Modules and Tasks have been tested to completion, not tested to completion, and which tests were not applicable and why. A report which documents that only specific parts of the Channel test have been completed due to time constraints, project problems, or customer refusal may still be recognized as an official OSSTMM audit if accompanied by this report clearly showing the deficiencies and the reasons for those deficiencies.

CERTIFICATION

OSSTMM certification is the assurance of an organization's security according to the thorough tests within the OSSTMM standard and is available per vector and channel for organizations or parts of organizations that maintain vigilance over their rav levels and have them validated yearly from an independent third-party auditor. Validation of security tests or quarterly metrics is subject to the ISECOM validation requirements to assure consistency and integrity.

1. POSTURE REVIEW

	TASK	COMMENTS	COMPLETION STATUS
1.1	Identified business objectives and markets.		
1.2	Identified legislation and regulations applicable to the targets in the scope.		
1.3	Identified business policies.		
1.4	Identified business and industry ethics policies.		
1.5	Identified operation cultures and norms.		
1.6	Identified operation times and flows applicable to the targets in the scope.		
1.7	Identified all necessary Channels for this scope.		
1.8	Identified all Vectors for this scope.		

2. LOGISTICS

	TASK	COMMENTS	COMPLETION STATUS
2.1	Applied testing safety measures.		
2.2	Determined and accounted for test instabilities.		
2.3	Determined and accounted for downtime in scope.		
2.4	Determined and accounted for test pace according to the test environment and the security presence.		

3. ACTIVE DETECTION VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
3.1	Determined and accounted for interferences.		
3.2	Tested with both interferences active and inactive.		
3.3	Determined restrictions imposed on tests.		
3.4	Verified detection rules and predictability.		

4. VISIBILITY AUDIT

	TASK	COMMENTS	COMPLETION STATUS
4.1	Determined targets through all enumeration tasks.		
4.2	Determined new targets by researching known targets.		

5. ACCESS VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
5.1	Verified interactions with access points to all targets in the scope.		
5.2	Determined type of interaction for all access points.		
5.3	Determined source of interaction defined as a service or process.		
5.4	Verified depth of access.		
5.5	Verified known security limitations of discovered access points.		
5.6	Searched for novel circumvention techniques and security limitations of discovered access points.		

6. TRUST VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
6.1	Determined interactions that rely on other interactions to complete the test interaction according to the tasks.		
6.2	Determined targets with trust relationships to other targets in the scope to complete interactions.		
6.3	Determined targets with trust relationships to other targets outside the scope to complete interactions.		
6.4	Verified known security limitations of discovered trusts between the trusts.		
6.5	Verified known security limitations of discovered trusts between targets in the scope and the trusted interactions.		
6.6	Searched for novel circumvention techniques and security limitations of discovered trusts.		

7. CONTROLS VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
7.1	Verified controls for Non-Repudiation functioning according to all tasks.		
7.2	Verified controls for Confidentiality functioning according to all tasks.		
7.3	Verified controls for Privacy functioning according to all tasks.		
7.4	Verified controls for Integrity functioning according to all tasks.		
7.5	Verified controls for Alarm functioning according to all tasks.		
7.6	Verified known security limitations of all controls Class B categories.		
7.7	Searched for novel circumvention techniques and security limitations of all controls Class B categories.		

8. PROCESS VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
8.1	Determined all processes controlling the action of interactivity with each access.		
8.2	Verified the interaction operates within the confines of the determined process.		
8.3	Verified the interaction operates within the confines of the security policy for such interactions.		
8.4	Determined the gap between the operations of interactions and the requirements of posture from the Posture Review.		
8.5	Verified known security limitations of discovered processes.		
8.6	Searched for novel circumvention techniques and security limitations of discovered processes.		

9. CONFIGURATION AND TRAINING VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
9.1	Verified configuration/training requirements according to the posture in the Posture Review.		
9.2	Verified the application of appropriate security mechanisms as defined in the Posture Review.		
9.3	Verified the functionality and security limitations within the configurations/training for the targets in the scope.		
9.4	Searched for novel circumvention techniques and security limitations within configurations/training.		

10. PROPERTY VALIDATION

	TASK	COMMENTS	COMPLETION STATUS
10.1	Determined the amount and type of unlicensed intellectual property distributed within the scope.		
10.2	Verified the amount and type of unlicensed intellectual property available for sale/trade with the seller originating within the scope.		

11. SEGREGATION REVIEW

	TASK	COMMENTS	COMPLETION STATUS
11.1	Determined the amount and location of private information as defined in the Posture Review available through the targets.		
11.2	Determined the type of private information as defined in the Posture Review available within the scope.		
11.3	Verified the relationship between publicly accessible information outside the target detailing private or confidential information defined in the Posture Review and the scope.		
11.4	Verified the accessibility of public accesses within the target to people with disabilities.		

12. EXPOSURE VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
12.1	Searched for available targets through publicly available sources outside of the scope.		
12.2	Searched for available organizational assets as defined in the Posture Review through publicly available sources outside of the scope.		
12.3	Determined access, visibility, trust, and controls information available publicly within the targets.		
12.4	Determined a profile of the organization's channel infrastructure for all channels tested through publicly available information within the targets.		
12.5	Determined a profile of the organization's channel infrastructure for all channels tested through publicly available information outside the scope.		

13. COMPETITIVE INTELLIGENCE SCOUTING

	TASK	COMMENTS	COMPLETION STATUS
13.1	Determined the business environment of partners, suppliers, workers, and market through publicly available information on targets within the scope.		
13.2	Determined the business environment of partners, vendors, distributors, suppliers, workers, and market through publicly available information outside the scope.		
13.3	Determined the organizational environment through publicly available information on targets within the scope.		
13.4	Determined the organizational environment through publicly available information outside the scope.		

14. QUARANTINE VERIFICATION

	TASK	COMMENTS	COMPLETION STATUS
14.1	Verified quarantine methods for interactions to the targets in the scope.		
14.2	Verified quarantine methods for interactions from the targets to other targets outside the scope.		
14.3	Verified length of time of quarantine.		
14.4	Verified quarantine process from receive to release.		
14.5	Verified known security limitations of discovered quarantines.		
14.6	Searched for novel circumvention techniques and security limitations of discovered quarantines.		

15. PRIVILEGES AUDIT

	TASK	COMMENTS	COMPLETION STATUS
15.1	Verified the means of legitimately obtaining privileges for all authenticated interactions.		
15.2	Verified the use of fraudulent identification to obtain privileges.		
15.3	Verified the means of circumventing authentication requirements.		
15.4	Verified the means of taking non-public authentication privileges.		
15.5	Verified the means hijacking other authentication privileges.		
15.6	Verified known security limitations of discovered authentication mechanisms to escalate privileges.		
15.7	Searched for novel circumvention techniques and security limitations of discovered authentication mechanisms to escalate privileges.		
15.8	Determined depth of all discovered authentication privileges.		
15.9	Determined re-usability of all discovered authentication privileges on the authentication mechanisms on all targets.		
15.10	Verified requirements towards obtaining authentication privileges for discriminatory practices according to the Posture Review.		
15.11	Verified means towards obtaining authentication privileges for discriminatory practices for people with disabilities.		

16. SURVIVABILITY VALIDATION AND SERVICE CONTINUITY

	TASK	COMMENTS	COMPLETION STATUS
16.1	Determined measures applicable to disrupt or stop service continuity to and from the targets.		
16.2	Verified continuity processes and safety mechanisms active for the targets.		
16.3	Verified known security limitations of discovered safety and service continuity processes and mechanisms.		
16.4	Searched for novel circumvention techniques and security limitations of discovered safety and service continuity processes and mechanisms.		

17. END SURVEY, ALERT AND LOG REVIEW

	TASK	COMMENTS	COMPLETION STATUS
17.1	Verified methods for recording and alerting interactions to the targets in the scope.		
17.2	Verified methods for recording and alerting interactions from the targets to other targets outside the scope.		
17.3	Verified speed of recording and alerting.		
17.4	Verified persistence of recording and alerting.		
17.5	Verified integrity of recording and alerting.		
17.6	Verified distribution process of recording and alerting.		
17.7	Verified known security limitations of discovered recording and alerting methods.		
17.8	Searched for novel circumvention techniques and security limitations of discovered recording and alerting methods.		