ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"APLICAR UN ESQUEMA SE SEGURIDAD DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO 27001 EN EL ÁREA DE POSVENTA EN UNA EMPRESA DE TELECOMUNICACIONES."

TRABAJO DE TITULACIÓN
PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

AUTOR:
SUÉSCUM TREJOS EVEN ANDRÉS

LUGAR:
GUAYAQUIL – ECUADOR
2021

AGRADECIMIENTO

Gracias a Dios y a la Virgen Santísima, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el período de estudio.

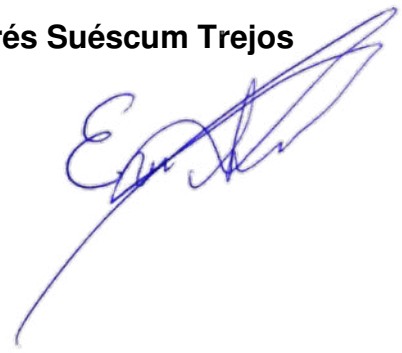
A mis padres Rocío Trejos de Suéscum y Juan Alberto Suéscum González, por el apoyo incondicional en mis estudios y por la mejor herencia que me hayan podido dar “la educación”, por hacer de mí una mejor persona a través de su amor, consejo, apoyo y confianza para cumplir con mis metas en la vida.

A mis hermanos Juan Alberto Jr. y David Eduardo Suéscum Trejos, por sus valiosos ejemplos, apoyo, comprensión y alegría que son parte de mi fortaleza para seguir adelante. Agradezco a los directivos de la Escuela Superior Politécnica del Litoral, ESPOL, especialmente a quienes conforman el programa MSIG.

Mi reconocimiento a mi esposa Cinthya Janeth Andrade por el apoyo incondicional y sus valiosos consejos durante el proceso de titulación.

De manera particular agradezco, al Ing. Karina Astudillo Barahona, MBA, tutora de la presente tesis, por su valioso aporte, sugerencia y generosa guía en el desarrollo de esta tesis y la culminación de la misma. Agradezco, a todas aquellas personas que de una u otra manera contribuyeron con la realización de la presente tesis.

Even Andrés Suéscum Trejos



DEDICATORIA

A Dios y a la Virgen Santísima, por ser mis más valiosas guías y soporte espiritual.

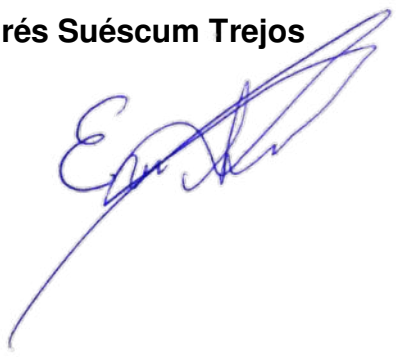
A mi Madre Rocío Trejos de Suéscum, quien sembró en mí el ímpetu, la perseverancia para la consecución de las metas.

A mis Familia Juan Alberto Padre, Juan Alberto Jr. y David Eduardo Suéscum Trejos, por ser mi ejemplo a seguir, por estar dispuestos a ayudarme y escucharme en cualquier momento.

A mis sobrinos Juan Andrés y Xavier Francisco con el ánimo de contribuir con un pequeño aporte en su formación educacional.

A mi Esposa Cinthya Andrade de Suéscum por ser mi apoyo en los momentos difíciles en mi vida.

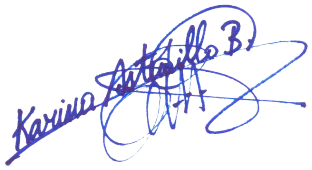
Even Andrés Suéscum Trejos



TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire Cobo, MBA

COORDINADOR MSIG



Ing. Karina Astudillo Barahona, MBA

DIRECTOR DEL TRABAJO DE TITULACION

Ing. Juan Carlos García, MBA

MIEMBRO DEL TRIBUNAL

RESUMEN

La presente Trabajo de titulación de posgrado, tiene como objetivo analizar los esquemas de seguridad dentro de una empresa que vende soluciones en telecomunicaciones, analizando las vulnerabilidades, riesgos dentro del sistema de red operativo involucrado en actividades de varios proyectos que la empresa brinda a diferentes compañías de telecomunicaciones nacionales. El desarrollo consta de un marco teórico donde se menciona importantes conceptos en torno a los riesgos que están presentes en la red de una empresa; tratando de abarcar los ataques más comunes y que podrían afectar en su desarrollo. Esto nos permite demostrar la importancia que tiene la configuración de forma correcta y tener controlados los usuarios que tienen acceso. Para esto se tomó como referencia la metodología OSSTMM que nos permite identificar brechas de seguridad en la empresa. El análisis de seguridad informático desarrollado permitió demostrar las limitaciones y el nivel de vulnerabilidad encontrados con pruebas de hacking técnico.

Se realizó un ataque controlado como comprobación de la vulnerabilidad existente en a la red empresarial; para lo cual, se penetró una computadora Windows y se logró extraer documentación importante del equipo.

Concluyendo, que como resultado de esta tesis se logró que la empresa le otorgue importancia sobre la implementación de la norma ISO 27002:2013 con la que se logró reducir los riesgos de vulnerabilidad en todos los niveles, permitiendo aplicar medidas preventivas, correctivas logrando un mejor control, mejoras y recomendaciones para garantizar la confiabilidad e integridad en la documentación.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

HVA	Planear hacer verificar y actuar.
IPS	Sistemas de prevención de intrusiones.
ISC2	Certificación internacional de seguridad en sistemas de información.
ISECOM	Institute for Security and Open Methodologies
ISO	Organización Internacional de Normalización.
ISSAF	Marco de Evaluación de Seguridad de Sistemas de Información.
MITM	Men in The Middle Attack, Hombre en el medio.
OSSTMM	Manual de la Metodología Abierta de Comprobación de Seguridad.
OWISAM	metodología Abierta para el Análisis de Seguridad Wireless.
PYMES	Pequeñas y medianas empresas.
SGSI	Sistema de Gestión de Seguridad Informática.
VPN	Red privada virtual.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En vista de los cambios trascendentales que se vienen dando en el mundo moderno, ocasionados por su constante desarrollo, que involucra la economía, el incremento de la cantidad de información, los sistemas que la proveen; y la presencia de la vulnerabilidad ante las constantes amenazas tecnológicas, las empresas de seguridad informáticas que continúan su desarrollo interno se han impuesto verdaderos retos a la protección entorno a los diferentes sistemas tecnológicos, sobre la infraestructura de las redes, comunicaciones y sistemas de información de punta, para minimizar a través de políticas internas un control que garantice la protección frente a eventos no deseados. Por lo tanto, considerando que el sistema informático se ha convertido en un usuario necesario para el éxito empresarial en el entorno global y dinámico de hoy, la administración apropiada de los sistemas de información es un desafío importante para los representantes empresariales.

La seguridad informática consta de normas, procedimientos y herramientas, que tienen como finalidad garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información. El ingreso a equipos o en una red informática que no está autorizado pueden ocasionar en la gran mayoría de los casos graves problemas.

Muchas veces las pequeñas y medianas empresas (PYMES) no han entrado en la etapa de concientización del riesgo de las amenazas en la administración apropiada de los sistemas de información que es un desafío importante por lo que se deben tomar medidas preventivas y reactivas; considerándose la primera como la minimización de ocurrencia de eventos no deseados y la reactiva que es la que se activa una vez ocurrido el evento indeseado.

Por todo lo anteriormente mencionado es indispensable conocer la identidad, puesto de trabajo, antivirus en red y sobre todo garantizar el acceso personal. En las PYMES los sistemas de información constituyen una herramienta para la organización, recopilación, procesamiento de datos que permiten toma de decisiones acertadas. Pero, estos procesos informáticos se han venido actualizando hasta lograr en la actualidad procesos veloces y muy eficientes. Otros de los factores importantes es la participación del técnico, los contenidos de la información, el equipamiento con programas autorizados. La información y los procesos que la apoyan, los sistemas y las redes, son bienes importantes de las empresas, por lo que requieren ser protegidos convenientemente frente a amenazas que pongan en peligro la disponibilidad, la integridad, la confidencialidad de la información, la estabilidad de los procesos, los niveles de competitividad, la imagen corporativa, la rentabilidad y la legalidad, aspectos necesarios para alcanzar los objetivos de la organización.

En el presente documento describiré en forma puntual amenazas muchas veces minimizadas ante la constante evolución de los equipos de una corporación, por lo que es fundamental conocer que recursos se aplicarían de acuerdo a la vulnerabilidad detectada, protegiendo no solo los bienes tangibles: maquinaria, servidores, etc.; sino bienes intangibles como la propiedad intelectual e información sensible de la corporación.

Considerando que todos son activos importantes de la empresa es necesario concientizarse sobre las consecuencias que tendría la pérdida o fuga de la información confidencial que tenemos sobre nuestros clientes o las propiedades intelectuales de nuestra empresa. Se hace necesario incorporar correctivos aplicables para llevar a cabo tareas de una forma eficiente y lograr un cumplimiento de excelencia.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

Muchas corporaciones internacionales han venido apoyando tecnológicamente a empresas en cualquier región del mundo con el fin de satisfacer las necesidades de los clientes más exigentes con resultados de alta calidad. Las empresas proveedoras mantienen una relación con el cliente después de la implementación, proporcionando un soporte de asistencia para las plataformas como una garantía de su servicio.

Los diferentes sistemas operativos han sido utilizados como recursos de las organizaciones de pequeñas y grandes empresas.

1.2 Descripción del problema

En consideración a la importancia de la seguridad de la información empresarial actualmente, es prioritario implementar seguridad en el área de gestión informática, de tal manera que la empresa cuente con verdaderos procesos frente a amenazas internas y externas. La empresa de origen extranjera cuenta con una sucursal ubicada en dos ciudades importantes en el Ecuador: Quito y Guayaquil; esta última es la oficina seleccionada para realizar el presente estudio, la misma que se dedica a la implementación de soluciones de telecomunicaciones dentro del Ecuador. El sistema empresarial cuenta con un esquema de servicios prestados por requerimiento del proyecto en forma esporádica, por la que se transfieren los recursos y la administración con el consiguiente cumplimiento de ciertas tareas en torno al personal previamente seleccionado por la empresa.

Las vulnerabilidades detectadas en el sistema de telecomunicaciones se describen a continuación:

1. Poco control de ingreso a la red en equipos que no pertenecen directamente a la empresa.

El control de ingreso a la red es garantizar su acceso con políticas, incluyendo preadmisión, chequeo de políticas de seguridad en el usuario inicial, compartido y final. Incluyendo controles post-admisión sobre los recursos a los que pueden acceder en la red los usuarios, dispositivos y su aplicación.

La empresa no cuenta con política de control para equipos proporcionados por otras entidades.

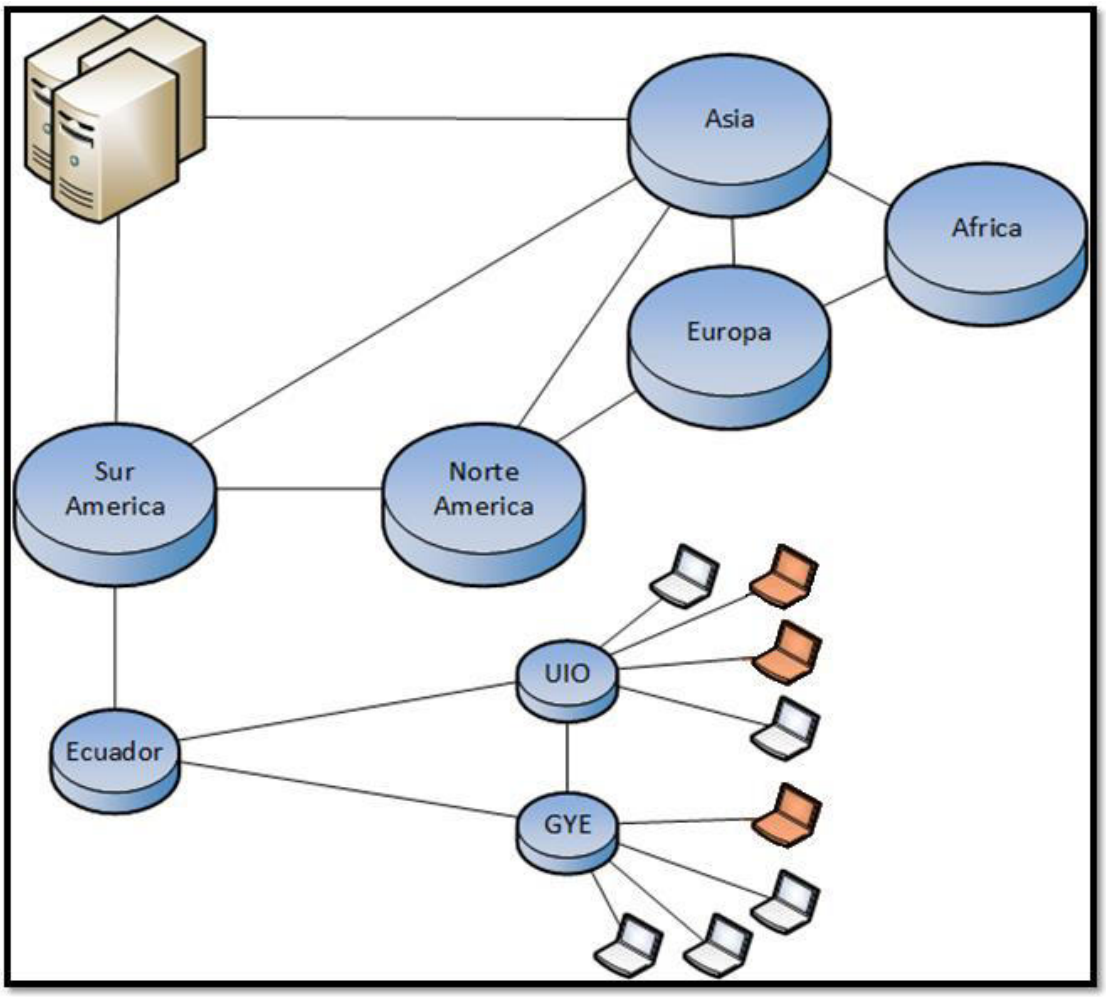


Figura 1.1 *– Arquitectura de la red empresarial*

Los servidores principales se encuentran en casa matriz (HQ), estos tienen acceso a una red de distribución global, donde todas las oficinas pueden acceder a la información.

Las oficinas dentro del Ecuador, consta de dos sucursales en Quito y Guayaquil las que están conectadas a servidores latinoamericanos (Sur América).

Los equipos dentro de las oficinas son proporcionados por una empresa de tercero (PC color rojo) donde representa una gran mayoría.

2. No se aplican políticas de control de seguridad de la información dentro de los equipos.

De las políticas de seguridad de la información establecidas en una empresa dependen la seguridad de esta. En la actualidad, es difícil contar con un sistema completamente seguro y resistente a las innumerables amenazas presentes por el avance tecnológico.

En la empresa en estudio, si bien es cierto que cuenta con políticas de seguridad a nivel del núcleo y en la distribución; no cuenta con controles a nivel de los elementos en la red de acceso, donde el usuario contando con la red corporativa podría ingresar un dispositivo que le facilitaría el almacenamiento masivo de la información para utilizarlos en propósitos ajenos a la empresa.

3. No se cuenta con un compromiso de confiabilidad que garantice la seguridad de la información corporativa.

Las empresas deben contar con política de confiabilidad apoyados en el compromiso desde la dirección general, incluyendo absolutamente todo el personal involucrado en el sistema sea interno o externo.

La empresa tiene como función principal la contratación y prestación de servicios lo que implica la confianza en el insumo recibido y la de proporcionar a un tercero acceso a la información propio de la empresa.

La empresa en estudio no cuenta con un compromiso de confiabilidad sobre el acceso de la información dentro de los contratos laborales,

comerciales o un tercero en relación con la gestión de la información sobre cómo se debe tratar la información durante el servicio. Por lo tanto, para proteger riesgos que esto pueda suponer se debería tomar los correctivos necesarios, estableciendo normativas en los contratos de confidencialidad entre la empresa y cliente, con el fin proteger y defender los intereses del cliente y del proveedor.

4. No existe un programa periódico y sistemático de control de flujo de información en los diferentes dispositivos proporcionados a la empresa.

La mayoría de las empresas para llevar a cabo su misión necesitan del sistema de información para cumplir con el comercio y la administración de proyectos a una escala global. Considerando como conjunto de componentes interrelacionados que permiten capturar, procesar, almacenar y distribuir la información para apoyar en la toma de decisiones y el control de una empresa. Para el correcto cumplimiento de las actividades es necesario que cubran la alimentación o insumo, en la captura o recolección de datos primarios dentro de la empresa o de su entorno para procesarlos en un sistema de información. También, el procesamiento la conversión del insumo en forma que sea más comprensible y finalmente el producto de salida donde se transfiere la información procesada a las personas o actividades donde deba ser empleado.

La empresa en estudio se ajusta a lo anteriormente expuesto en torno a las actividades relacionadas con la contratación y prestación de servicios;

sin embargo, no se cuenta con una herramienta precisa que implique un control tipo auditoría de los insumos que garanticen su seguridad.

1.3 Solución propuesta

Aplicando mejoras y recomendaciones basadas en varios dominios, objetivos de control y controles de la norma ISO 27002:2013 se logrará reducir los riesgos de vulnerabilidad en todos los niveles.

Estableciendo como estrategia la aplicación de Hacking Ético, que permita identificar las amenazas, riesgos y vulnerabilidades de la red.

Implementando procedimientos que permitan garantizar la seguridad de la información de forma correcta sobre todo con el uso de los activos informáticos.

Estableciendo que los accesos a los servidores empresariales, así como la gestión de usuarios se deben regir por la "Política de gestión de privilegios" que debe ser cumplida para asegurar la eficiencia dentro de los proyectos de la empresa.

Concientizando a los usuarios respecto de su responsabilidad frente a la utilización de la información proporcionada por la empresa.

1.4 Alcance

El presente documento pretende implementar un mejor control de la información sensible utilizada para el área de preventa donde se

encuentran datos de gran valor, tanto para el cliente como para la empresa, que actualmente, puede ser fácilmente manipulada.

1.5 Objetivo general

Diseñar y aplicar estrategias considerando los medios, las normas y políticas de seguridad informática que contengan información sensible.

1.6 Objetivos específicos

- Identificar la información sensible, con el fin de protegerla mediante la implementación de políticas aplicables en la empresa.
- Reforzar los protocolos de seguridad en el flujo informático dentro de las áreas claves.

1.7 Metodología

Se aplica Modelo PHVA empleando a los procesos del Sistema de Gestión de la Seguridad Informática (SGSI) que se compone de cuatro procesos básicos:

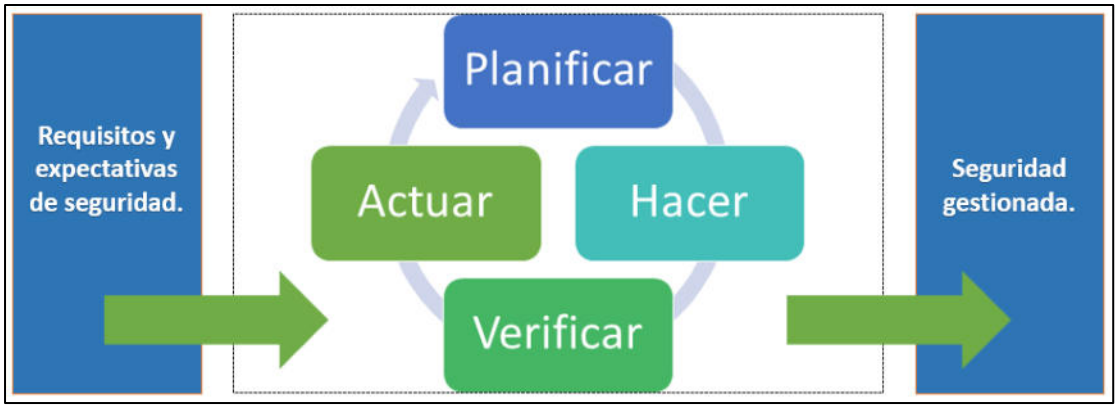


Figura 1.2 *– Modelo PHVA*

Planificar, que sería establecer en el SGSI.

Hacer, que sería establecer un proceso adecuado que enfoque las posibles vulnerabilidades en la red a analizar, implementando las medidas correctivas sugeridas por especialistas de seguridad y que éstas sean políticas rentables para la empresa a futuro.

Actuar, que sería mantener y mejorar en el SGSI, implementar de forma correcta, las actividades que garanticen la seguridad necesaria acorde a los objetivos de la empresa.

Verificar que sería revisar y dar seguimiento en el SGSI.

Verificar los resultados de los ataques controlados contra la seguridad implementada en la empresa, para así identificar las posibles vulnerabilidades y reportarlos al área correspondiente.

Además, asegurarse de que estas políticas sean implementadas en forma rentable para la empresa a futuro.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Hacking Ético

El Hackeo Ético es considerado la acción de burlar la seguridad de un sistema o software con técnicas avanzadas en informática, con el fin de identificar vulnerabilidades, lo que contribuye a fortalecer y mejorar la seguridad empresarial implementada.

Según Yanes (2015) el hacking ético es una prueba de intrusión controlada a sistemas informáticos para detectar vulnerabilidades con la finalidad de proteger. Mientras que, para Jara (2012) el hacking ético, el usuario solo conoce el alcance de las pruebas y el personal auditado esta consiente de las pruebas a ejecutar.

Las etapas del hacking ético son:

1. Análisis de vulnerabilidades
2. Explotación
3. Post Explotación

Existen tres clases de Hacking:

1.- Sombrero blanco, también conocido como el hacking ético, esta acción ilícita es considerada como legal; debido a que son contratados por empresas con el fin de identificar sus vulnerabilidades dentro del sistema implementado en la empresa.

2.- Sombrero gris, estos hacen referencia a un hacker que actúa ilegalmente pero no cuentan con malas intenciones, por lo que se los ubican en una situación un tanto cuestionable.

López Santoyo (2015) manifestó que en este tipo de prueba el auditor, tiene conocimiento de la organización; pero el objetivo es identificar vulnerabilidades.

3.- Sombrero Negro, identificado como hacker malicioso que son los que actúan de forma personal y egoísta por ganancia económica, venganza o simplemente para causar daños. Según Benchimol (2010) este tipo de pruebas es similar al hacking ético, pero los usuarios de seguridad de la empresa no están alertados por lo que permite medir las capacidades de respuesta ante un evento de ataque.

En la presente investigación se aplicará el pentesting, que es una práctica que permite descubrir las debilidades en la seguridad de los sistemas informáticos, descubriendo las vulnerabilidades u otras amenazas de seguridad presentes en el sistema a analizar lo mismo que se haría simulando un ataque que nos permitirá potencial la afectación de un activo propio de la empresa. Las técnicas empleadas que se utilizan en este tipo de investigación son considerando siempre la seguridad de no perjudicar la organización ni realizar actividades ilícitas.

Pasos para la prueba de intrusiones

- Identificar el alcance de los parámetros de pentesting considerando la limitación y la justificación y acciones a realizar.
- Estas acciones deben ser realizadas por especialistas en el campo.
- Elegir la prueba a realizar, considerando relación costo beneficio.
- Elaborar un documento de resultados con pruebas detalladas para la empresa seleccionada; detallando el hallazgo y recomendaciones para que se establezcan medidas correctivas.

En la aplicación del pentesting se realizan un conjunto de ataques dirigidos de acuerdo a la tecnología que se aplica en la empresa. Entre estas podríamos elegir diferentes estrategias de penetración que podrían ser:

Caja Blanca - En la que se dispone de toda la información sobre el sistema, su aplicación y equipamiento, pudiendo simular alguien que tiene el conocimiento total del área de la empresa.

Caja Gris - En la que se dispone de información parcial sobre el sistema.

Caja Negra - En la que los pentesters no disponen de información sobre la empresa, pudiendo simular un ataque real por alguien que no tiene conocimiento alguno.

Estas pruebas de penetración pueden realizarse en 2 vías:

Con conocimiento - Se intenta comprometer los sistemas o la red de la empresa, con la cooperación del personal, identificando los puntos vulnerables de las mismas.

Sin conocimiento - Se intenta comprometer los sistemas o la red de la empresa, sin la cooperación del personal, identificando los puntos vulnerables de las mismas. Las ventajas de la prueba "sin conocimiento" es que los resultados son mucho más reales y recogen debilidades las que podrían ser explotadas.

2.2 Elementos de Seguridad Informática aplicables

Contamos con tres tipos diferentes de seguridad informática para la protección de datos en una red, sus comunicaciones o un dispositivo especifico.

Seguridad de Hardware

Esta seguridad se refiere a la seguridad física de los equipos en torno a un daño o disponibilidad no permitida a terceros. Este tipo de seguridad podría ser considerado el más importante debido a que el atacante no tendría acceso físico a los equipos.

Seguridad de Software

Esta seguridad no es tan confiable debido a que tiene defectos en su diseño, por lo que en ocasiones es considerado poco efectivo contra ataques maliciosos.

Seguridad de red

La seguridad de red, se responsabiliza de mantener la integridad de su información; teniendo en cuenta que existen un sin número de amenazas hacia la seguridad de red tales como: Virus, gusanos y caballos de Troya. Estos elementos maliciosos son la herramienta para realizar entre otros los siguientes ataques.

- Ataques de día cero, también llamados ataques de hora cero.
- Ataques de hackers.
- Ataques de denegación de servicio.
- Intercepción o robo de datos.
- Robo de identidad.

En consideración a los tipos de ataques es indispensable realizar constante actualizaciones del software. Los elementos descritos a continuación son esenciales para permanecer seguro en línea:

- Antivirus y antispyware.
- Firewall, para bloquear el acceso no autorizado a su red.
- Sistemas de prevención de intrusiones (IPS), para identificar las amenazas de rápida propagación, como el día cero o cero horas ataques.

- Redes privadas virtuales (VPN), para proporcionar acceso remoto seguro.

Elementos de la Seguridad Informática aplicables

La seguridad informática engloba características que dan forma y representan los pilares que encierran aplicaciones, acciones y herramientas.

Entre las medidas de seguridad aplicadas en trabajo son tres: integridad, confidencialidad y disponibilidad.

Integridad: Que es la autentificación de la información que es correcta y que no ha sido modificada.

Confidencialidad: Es la confianza de no ser divulgada a personas ajenas y no autorizadas a la red.

La confidencialidad se pierde muchas veces por la poca importancia que se da y no contar con normas que aseguren la vulnerabilidad de la información. Generalmente, se da cuando no se tiene el cuidado en uso dando lugar a que ocurran ataques directos al servidor.

Disponibilidad: Con la disponibilidad es otra forma de asegurar el libre ingreso a un sistema de red, pero, la empresa debe establecer a los usuarios el cumplimiento de estrictas normas de acceso cada vez que se desea extraer información de la base de datos o del sistema en general.

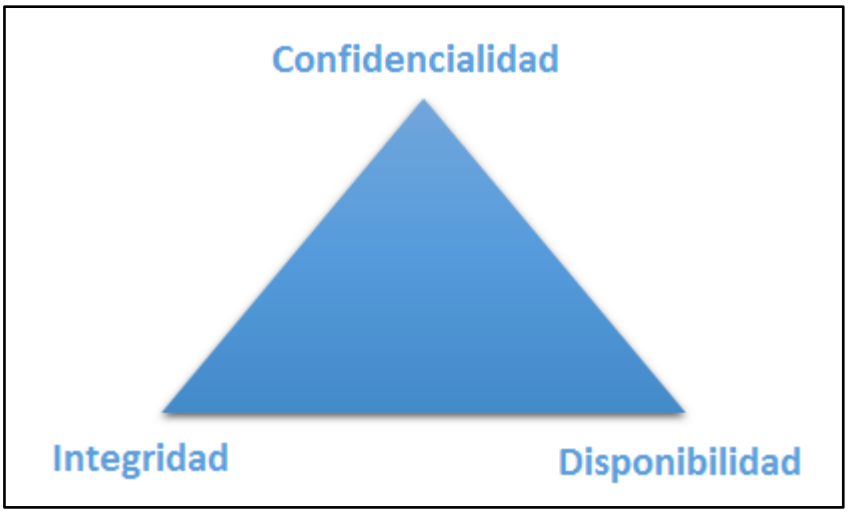


Figura 2.1 *– Elementos de seguridad informática*

Información de la red local de la empresa

La institución en referencia del estudio cuenta con 2 sedes en el país, Guayaquil y Quito. Para nuestro estudio se ubica la cede ubicada en Guayaquil, y cuenta con el proveedor ISP para el servicio de internet. La infraestructura de la red, que cuenta la empresa, provee sus servicios de interacción de aplicaciones propias de la empresa por a través de internet. La red cuenta con 20 usuarios internos, de los cuales 12 son de tipo subcontrados que tienen acceso a toda la información de la empresa.

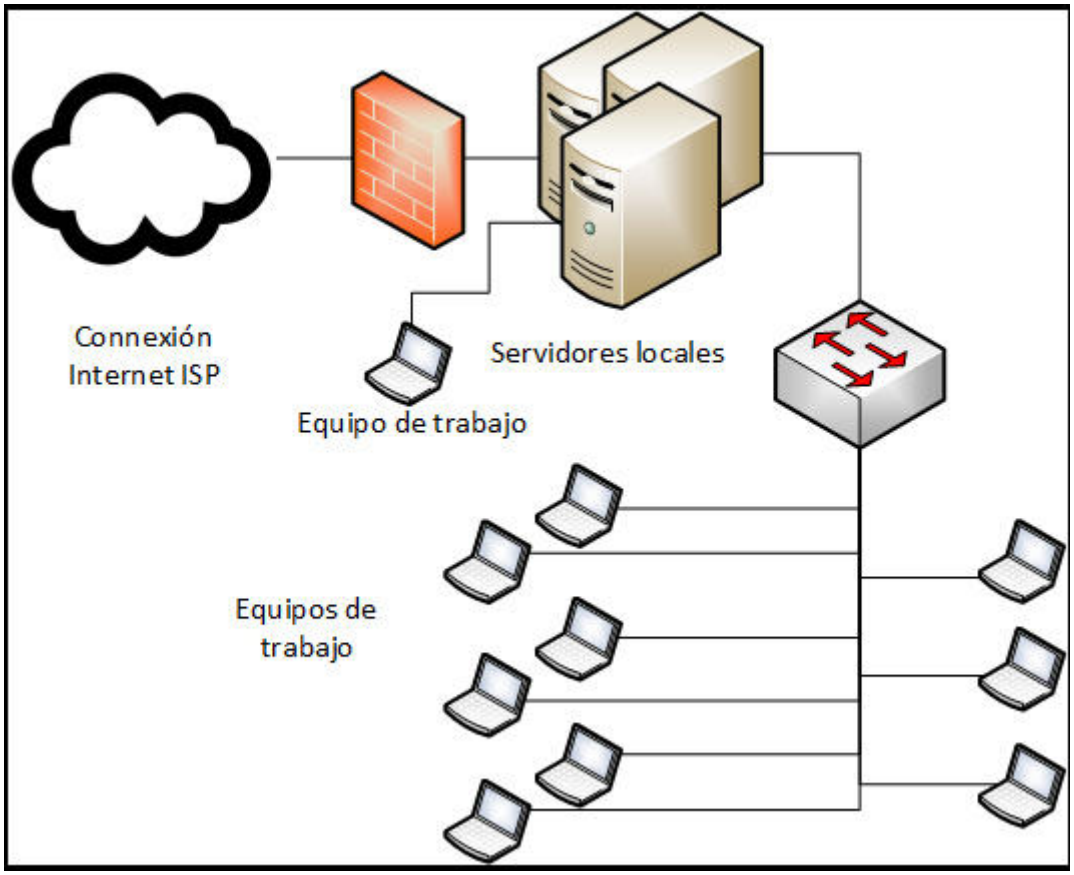


Figura 2.2 *– Red empresarial que cuenta con servidores locales y estaciones de trabajos*

2.3 Políticas de Seguridad de la Información

De acuerdo con el desarrollo informático que diariamente se da en el mundo entero, se puede encontrar la solución de cooperación mutua para compartir información segura. Este avance también cuenta con incremento de vulnerabilidades del sistema, que continúa creciendo, lo que da lugar a que usuarios hostiles puedan desarrollar herramientas a la par de los avances ya mencionados.

Según Borghello C. (2009) [1], en lo referente a las políticas de seguridad definen como: “un conjunto de requisitos definidos por los responsables

encargados de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema" los mismos que deben de ser conocidos por usuarios internos de la empresa, incluyendo normas y políticas propias.

Mientras, que Ochoa y Cervantes (2012), se apoyan en: "técnicas que se utilizan para implementar un servicio, y están diseñados para detectar, prevenir o recobrarse de un ataque de seguridad" como protocolos técnicos que protejan la información [5].

2.4 Políticas de Seguridad Informática

Las políticas de seguridad se implementan con el objetivo de poder preservar la información, independiente de las políticas de la seguridad informática. Estas políticas en una empresa nos garantizan la integridad, confiabilidad y disponibilidad de la información requerida hacia los usuarios de la empresa o personas autorizadas de la misma.

Estas políticas deben contar con el aval de la máxima dirección de la empresa, ya que son reglas y procedimientos que se deben implementar, conocer y hacer cumplir, considerando el nivel de información que se debe compartir con usuarios externos.

2.5 Tipos de técnicas para robo de información

En la actualidad, existen varios tipos de ataques cibernéticos donde se caracterizan por el objetivo a realizar, ya sea robar información o negar el servicio. En el caso empresarial, unos de los ataques más utilizados y en

el cual nos vamos a orientar el presente documento, especializar, es el robo de la información; entre estos tenemos el ataque de “Phishing”, XSS y “Hombre en el medio”.

Phishing – Este ataque se especializa en atacar al usuario mas no al sistema directamente, donde podría obtener información valiosa enviando un mensaje masivo, a la espera que uno de los usuarios pueda caer y otorgarnos la información para poder ingresar a la red.

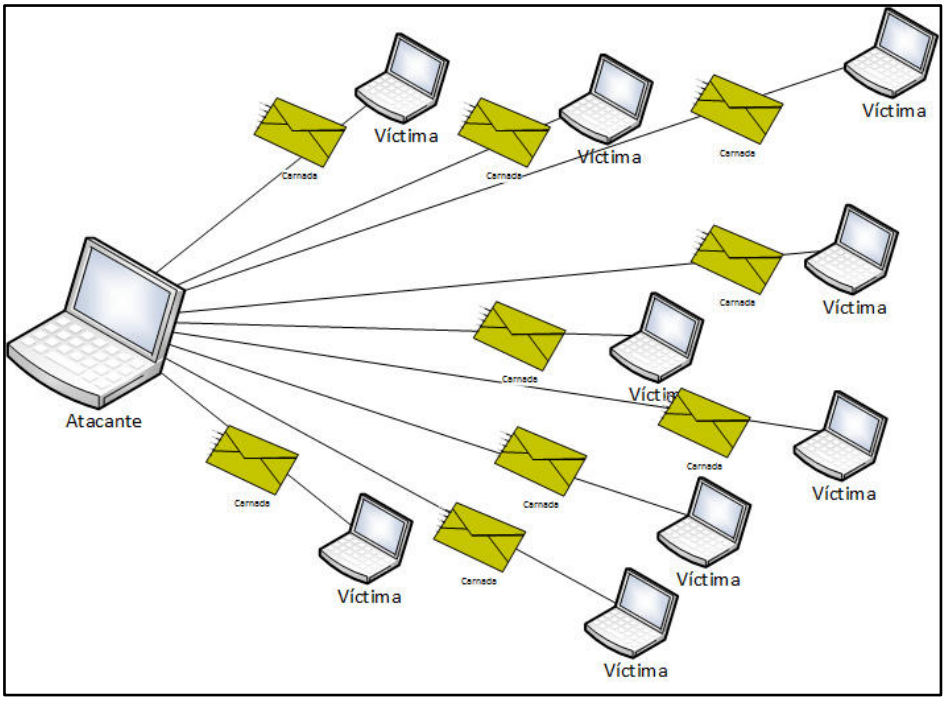


Figura 2.3 *– Usuario atacante envía un mensaje carnada a las víctimas.*

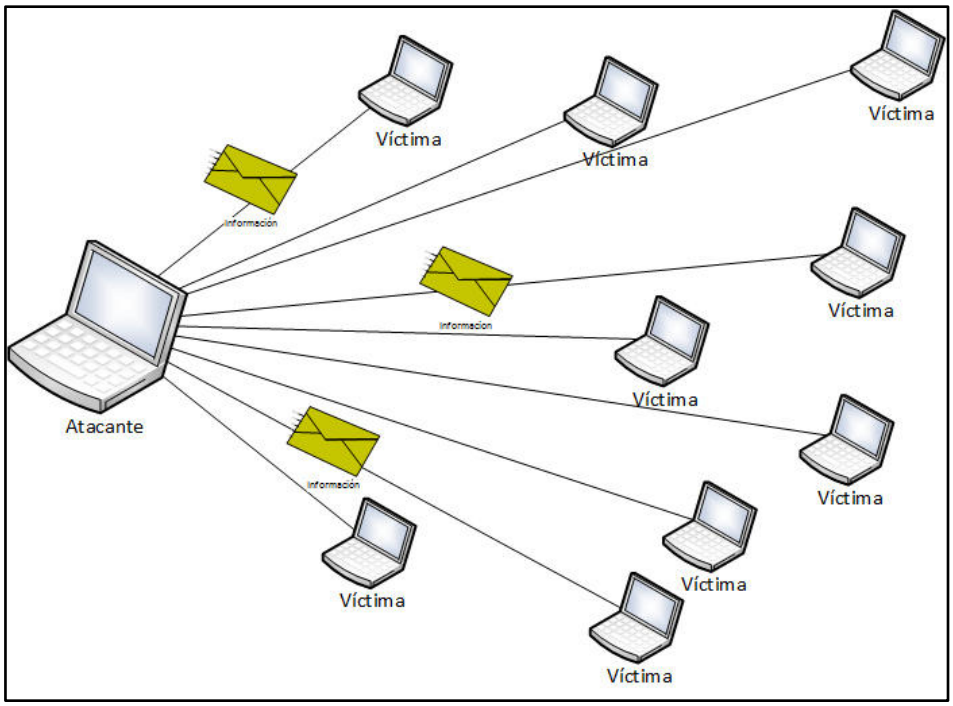


***Figura 2.4**.– Victimas enviando información al atacante*

XSS – Para el siguiente ataque, se especializa en ingresar un código con lenguaje HTTP, donde la victima al ingresar por medio de explorador a una aplicación web, otorga acceso al atacante información de credenciales logrando suplantar a la víctima o el atacante podría ingresar al sitio web, donde se obtiene la información completa como si se tratara de la víctima.

Hombre en el medio – También conocido como “Men in The Middle Attack” (MITM), se basa en ser el canal entre el servidor o punto de acceso a la red y la víctima, así el usuario (víctima) no se dará cuenta que una tercera persona está siendo el canal, el atacante puede capturar paquetes que envía o debe recibir la víctima, esto podrían ser datos de vital importancia como contraseñas, directorios o hasta transacciones personales que el usuario hace en la red donde se está obteniendo información.

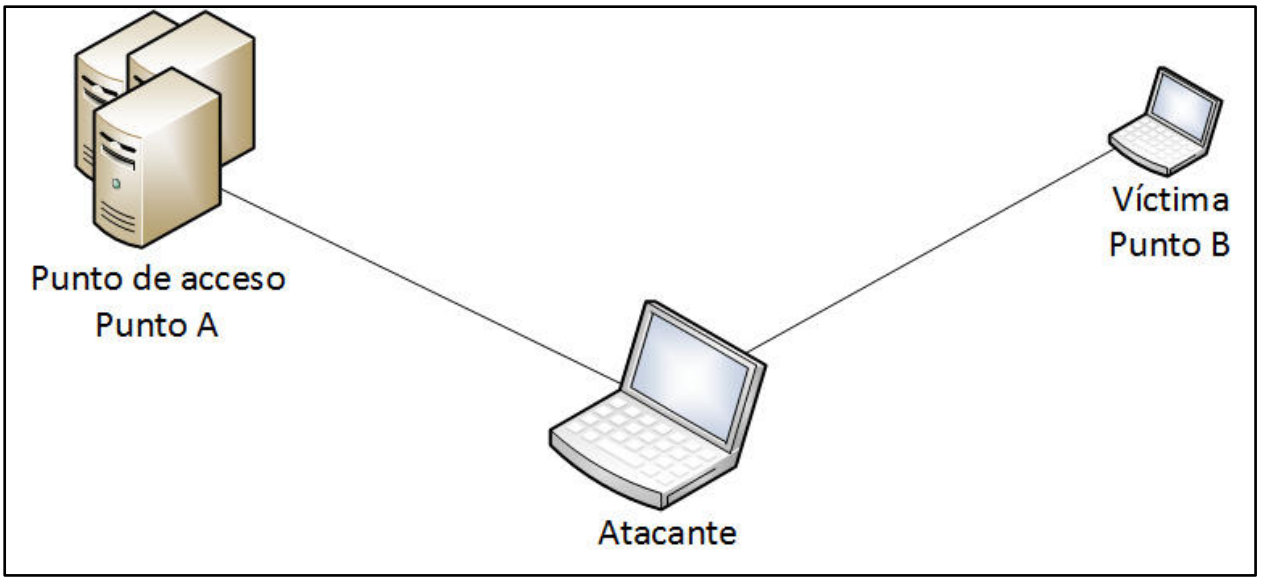


Figura 2.5 *– Conexión establecida donde el atacante es canal entre punto A y punto B*

2.6 Implicaciones éticas y legales

El aspecto legal y la ética, mantienen una estrecha relación. La ética definitivamente, depende del entorno del ser humano relacionado a la familia, entorno social, trabajo, etc. En lo referente a la ética en el campo informático, es atribuido a los estándares modernos de la seguridad informática, debido a la competencia por la demanda existente en el mundo.

Una empresa para lograr tener la certificación internacional de seguridad en sistemas de información (ISC2 – International Information Systems Security Certification Consortium) que otorga una de las más importantes certificaciones en el tema de seguridad, se apoya con un esencial compromiso de ética interno empresarial.

Considerando el objetivo de la presente investigación sobre evitar que la información confidencial de la empresa sea copiada por otros se debería

implantar una cultura jurídica en materia de TI (Tecnología de la información) de tal manera que sea una fortaleza de las normas existentes en la empresa. En la actualidad es correcto este tipo de seguridad en países como el nuestro, ya que en el día a día se amplía y se enriquece el campo informático, por lo tanto, se hace una obligación implementar la seguridad.

Para concluir, podemos asumir que el derecho y la ética, son herramientas indispensables para mantener la seguridad informática en una empresa. Por lo tanto, todos los usuarios, independientes del cargo laboral, deben estar involucrados con responsabilidad, lo que fortalecería a las medidas preventivas existente como una mejora al sistema de seguridad interno.

Dentro de las funciones legales de la empresa se consideran:

a) Elaborar procedimientos del campo jurídico y administrativo con el fin de apoyar y asesorar en el campo jurídico
b) Examinar y gestionar documentaciones y transacciones.
c) Obtener opiniones propias del desarrollo de la actividad administrativa de la empresa.
d) Inspeccionar y emitir informes legales normas, procedimientos y reglamentos.

2.7 Norma ISO/IEC 27002:2013

La Norma oficial ISO/IEC 27002:2013[2], es una guía de buena práctica de seguridad de la información. Esta guía es una norma internacional emitida por la organización de la normalización ISO; el objetivo es la de gestionar

la seguridad de la información de una empresa. Se puede implementar en cualquier empresa y con ello obtener toda la garantía de confiabilidad, integridad y disponibilidad de la información empresarial.

La norma nos permite realizar la evaluación y tratamiento de riesgos; además de la implementación de medidas de seguridad, las mismas que están amparadas en políticas, procedimientos e implementación técnica para prevenir las violaciones de seguridad.

Según el requerimiento en el presente trabajo de titulación, se apoyó en la revisión de la norma mencionada, considerando dominios puntuales previamente definidos, enfocándose directamente en el objetivo planteado. Entre los seleccionados están los siguientes:

Control de accesos

- Requisitos de negocios para el control de accesos.
- Gestión de acceso de usuarios.
- Responsabilidad del usuario.
- Control de acceso de sistemas y aplicaciones.

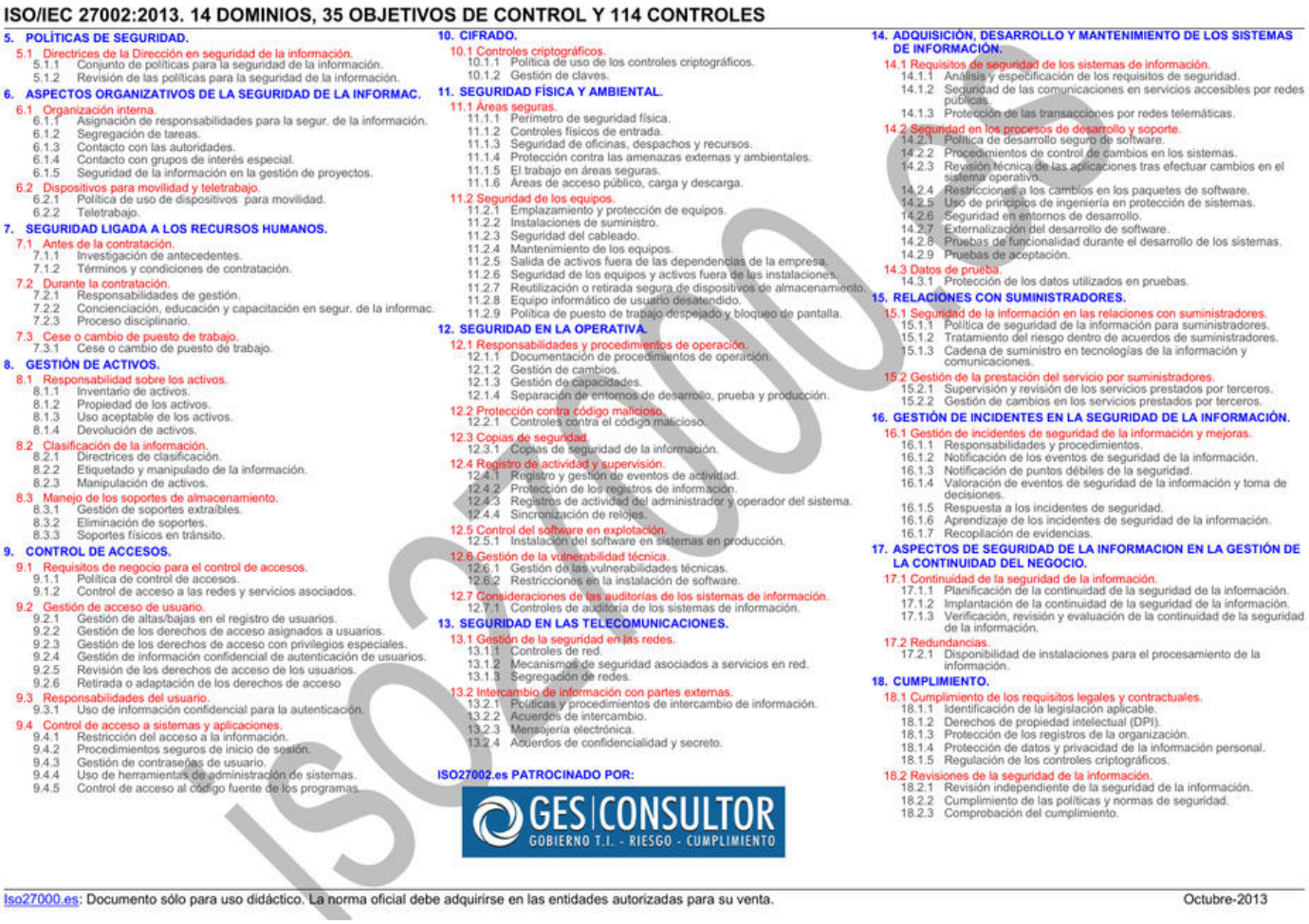
Cifrado

- Controles criptográficos.

Seguridad de las telecomunicaciones

- Gestión de la seguridad en las redes.
- Intercambio de información con partes externa.

Posterior al análisis con la norma, se pudo comprobar que la empresa no mantiene la seguridad total de la información ya que no cuenta con políticas de seguridad sobre la red que normalmente estas operan con sus riesgos en la actividad diaria. Lo que demuestra que a pesar que existen vulnerabilidades en la empresa, los jefes máximos no le otorgan la debida atención dentro de los protocoles normales de la empresa.



ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.
9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.
10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.
ISO27002.es PATROCINADO POR:
GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

Iso27000.es: Documento sólo para uso didáctico. La norma oficial debe adquirirse en las entidades autorizadas para su venta. Octubre-2013

Figura 2.6 *– Norma ISO 27002:2013*

2.8 Metodología

2.8.1 OWISAM (Open Wireless Security Assessment Methodology).

OWISAM es la metodología de evaluación de seguridad inalámbrica abierta. Actualmente se ha dado un gran incremento uso de redes inalámbricas domésticas y empresariales, con el uso de dispositivos portátiles y móviles, que pueden ser considerados objetivo de ataques informáticos. La principal función de OWISAN es cumplir con una metodología ágil, precisa y flexible que permite realizar con éxito un análisis completo del entorno sobre estos elementos [6].

Esta metodología surge frente a la necesidad de seguridad que existe actualmente para proteger y colabore con los administradores de sistemas, analistas y los usuarios, con el fin de eliminar incidentes informáticos garantizando el uso correcto de la misma.

2.8.2 ISSAF (The Information Systems Security Assessment Framework).

Esta metodología está diseñada para evalúa red, sistema y centro de aplicaciones de trabajo. Son muy útiles para detectar intrusiones en el ordenador y dan lugar a reaccionar lo mejor posible.

Incluyen 3 pasos.

1. **Planificación** – un intercambio de información y preparación para el test basado en el acuerdo entre las partes determinando fechas, tipo y tiempo de pruebas.
2. **Evaluación** – es la aplicación de la prueba. Generalmente se siguien los siguientes pasos
   a. Recopilación de información
   b. Mapeo de red de trabajo
   c. Detección de puntos débiles
   d. Test de penetración
   e. Apertura de acceso como un administrador
   f. Enumeración
   g. Comprometer su confiabilidad a usuarios remotos
   h. Mantener el acceso

3. **Reporte limpieza y destrucción de objetos**

   En el transcurso de la operación, se debe reportar eventos críticos para garantizar que el staff esta consiente de las pruebas.

   Al finalizar se debe elaborar un informe detallado de las pruebas con las recomendaciones para mejora

2.8.3 OSSTMM (Open Source Security Testing Methodology Manua)

De acuerdo con la OSSTMM, un test de intrusión es un test de seguridad con un objetivo definido que concluye cuando el objetivo es alcanzado o el tiempo ha terminado. Esta metodología fue creada en el año 2000 por ISECOM (Institute for Security and Open Methodologies); a partir del 2006 pasa a ser el estándar de facto en Estados Unidos, enriqueciéndose con los análisis de riesgos.

La OSSTMM se enfoca en los estados antes, durante y después de las pruebas en elementos técnicos que deben de ser probados y además como medir los resultados. Se dividen en los siguientes grupos:

1. **Seguridad de la información**
   - Reconocimiento de la Inteligencia Competitiva.
   - Reconocimiento de la Privacidad.
   - Recolección de Documentos.
2. **Seguridad de los procesos**
   - Prueba de Solicitud.
   - Prueba de Sugerencia Dirigida.

- Prueba de las Personas Confiables.

3. **Seguridad en las tecnologías de internet**
    - Rastreo de red.
    - Escaneo de puertos.
    - Reconocimiento de los servicios del sistema.
    - Reconocimiento del sistema operativo.
    - Indagación de vulnerabilidad y verificación.
4. **Seguridad de la comunicación**
    - Testeo de router.
5. **Seguridad inalámbrica**
    - Comprobación de Radiación Electromagnética.
    - Comprobación de redes inalámbricas.
    - Comprobación bluethoot.
    - Comprobación Dispositivos de Entrada Inalámbricos.
    - Comprobación Dispositivos de biometría.
6. **Seguridad física**
    - Inspección del área de datos.
    - Inspección de monitorización.
    - Verificación de ubicación.
    - Verificación de entorno.

2.9 Herramientas para Análisis de Riesgos

Nmap

En la actualidad, los sistemas informáticos exigen pasos importantes como identificar, analizar y tratar riesgo existente en todas las organizaciones, que les permite conocer ventas y debilidades para no obstruir sus objetivos de negocios y lograr una acción gestión proactiva. Entre las metodologías más relevantes de análisis de riesgos, contamos con algunas herramientas aplicables en la seguridad informática, lo que permite concientizar a las corporaciones en su necesidad de aplicarlas de acuerdo vulnerabilidades identificadas.

La implementación de un Sistema de Gestión Seguridad Informática (SGSI) en una empresa, abarca características de tipo, tamaño, objetivo, servicio, proceso, personal y requerimiento de seguridad que establece la misma, para lo cual se apoya en estándares internacionales ISO-IEC 27002:2013, norma que con sus herramientas contribuye a la identificación para solucionar problemas de seguridad a nivel técnico, organizativo y legislativo de una empresa. Estos sistemas emplean como requisitos, estrategias como análisis, evaluación y gestión de riesgos dentro del ciclo PHVA (planear hacer verificar y actuar). Dentro de la planeación se enfoca en el requerimiento de la selección de la metodología sistemática que permita visualizar y priorizar los riesgos con lo que se enfrenta una empresa, identificando los más importantes y priorizando la implementación para minimizar la posible materialización del riesgo.

Inicialmente para realizar una prueba de penetración es necesario usar una herramienta de escaneo de redes como NMAP útil para

identificar vulnerabilidades, la que nos permite identificar entre otros, qué servicios se están ejecutando en un dispositivo remoto, así como la identificación de equipos activos, sistemas operativos en el equipo remoto, existencia de filtros o firewalls.

NMAP es una herramienta necesaria en la iniciación de una prueba de penetración, porque nos permite detectar las direcciones IPs que están en toda la red pertenecientes a equipos activos, sistemas operativos, existencia de enrutadores o firewalls.

Además, de indicar parámetros que se afectaran durante la prueba y los resultados obtenidos, como respuesta final del comando tendríamos un listado de los puertos abiertos o cerrados de las direcciones dentro de la red.

Durante la prueba, en caso de agregar parámetros adicionales con el fin de obtener mejores resultados, en el presente trabajo utilizará también los siguientes parámetros

-**sS** = detecta los puertos sin dejar rastros

-**O** = Detecta el sistema operativo

NESSUS

Nessus es un scanner para el análisis de vulnerabilidades más usado del mundo habiendo tenido un reconocimiento mundial en los años 2000, 2003 y 2006 como la mejor herramienta de seguridad en la red. Su principal función es la de advertir las debilidades para un posible ataque. Siendo Nessus una de las herramientas más usadas

identificando las vulnerabilidades, en la presente tesis se utilizó de la siguiente forma:

- Se escaneó de forma general la red.
- Se detectó puertos innecesariamente abiertos.
- Mediante informe se pone en conocimiento los problemas de vulnerabilidad presentes en la red empresarial.

Metasploit

Metasploit es una herramienta ideal que nos permite explotar las medidas de control que no fueron consideradas en los pasos anteriores, así como otras seguridades o diferentes variables que podrían hacer difícil a la explotación. Existe una herramienta gráfica, que nos ayuda a tener un comienzo para el uso de metasploit, pero si realmente se requiere tener un trabajo más elaborado y automatizado, se recomienda utilizar el ambiente de comandos.

Kali Linux

Por último, contamos con una distribución de Linux orientada al pentesting y al campo de la seguridad informática. Las herramientas descritas anteriormente, como NMAP u Metasploit están disponibles y cuentan con muchas más herramientas; pero para el presente trabajo, las herramientas seleccionadas fueron las mencionadas. Finalmente, ya experimentando con NMAP y Metasploit, se procede completamente con Kali Linux que es una excelente herramienta reconocida a nivel mundial,

en el mundo del hacking ético, la misma que nos permite buscar, encontrar limite dentro de las seguridades de las redes y sistemas informáticos.

Dentro del sistema operativo se encuentran un aproximado de 600 aplicaciones de hacking y seguridad, entre las que encontramos a herramientas mencionadas. Kali dispone de algunas funciones para sondear redes de computadora, donde se puede encontrar detección de equipo y sistemas operativos. Estas funciones mediante la serie de comandos permiten detecciones avanzadas, vulnerabilidades y otras. Inclusive, la herramienta durante el escaneo se puede adaptar a las condiciones actuales de la red ya sea por congestión o latencia.

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACIÓN Y METODOLOGÍAS A IMPLEMENTAR.

3.1 Selección y Justificación de las Metodologías

Es importante establecer una metodología de análisis de riesgos dentro de los Sistema de Gestión de Seguridad Informática (SGSI), lo que nos permite detectar debilidades y fortalezas con que cuenta una organización para cada uno de sus activos informáticos; se lograra identificar y valorar los procesos más críticos de la empresa con el fin de evaluar el nivel de protección adecuada y determinar las amenazas frente a los riesgos.

La metodología seleccionada para el desarrollo del presente trabajo es la metodología de OSSTMM porque considero una guía apropiada para la identificación y descubrimiento de nuevos dispositivos en la red. Adicional a las configuraciones de autenticación y de cifrados que puedan estar presentes en la plataforma.

De Herzog (2010) la metodología OSSTMM esta alineada a la norma ISO 27001, que nos permite realizar pruebas de seguridad informática repetible y consistente. Su función se centra en separa un activo de amenazas, implementado controles que permitan garantizar, la confidencialidad, integridad y disponibilidad de la información.

Esta metodología OSSTMM según Emiliani y Sierra (2015) se centran en detalles técnicos que requieren ser auditados, buscando el mejoramiento en el campo de seguridad. Las pruebas a aplicarse deben contar con la información de los elementos que intervienen en el ensayo los elementos, que la metodología se refiere son:

- Factores humanos
- Factores físicos
- Redes inalámbricas
- Servicio
- Aplicaciones
- Telecomunicaciones
- Redes de datos.

En donde se aplican diferentes faces como parte de una auditoria relacionado a la metodología OSSTMM.

La metodología OSSTMM de acuerdo a lo descrito en paper de Gordon Diego (2017), donde se describe diferentes fases de la metodología en mención; el presente estudio se ajusta a la fase de investigación ya que se realizaron actividades con comprobación de procesos y exposiciones que pudieran provocar una comunicación ya que la información podría ser mal administrada debido a que no cuenta con alguna precaución dentro de la red.

3.2 Caracterización y aplicación de la Metodología

Esta metodología OSSTMM, está diseñada para el desarrollo de trabajo estándar y da la facilidad de aplicación en donde no se cuenta con la estructura de red a la cual se va analizar, debido a que es relativamente más amplia en comparación con otras metodologías.

Esta metodología aplicada en el presente proyecto, se enfoca en tres operaciones:

1. Planeación
2. Procedimiento
3. Resultados

Planeación

Dentro de la planificación se caracteriza los elementos de la red previo a la prueba de intrusión a desarrollar, analizando la información existente, la prueba en sí, es decir que se establece un escenario identificando los elementos disponibles para realizar el ataque.

Se analiza la estructura empresarial y los elementos de la red, donde se logra identificar la arquitectura tipo estrella, en la que todos los elementos de la red se conectan por medio de cable UTP hacia un switch central para el acceso a la red interna de la empresa, el acceso a la red de internet y comunicación con otros elementos externos.

El software donde se autentica, el usuario monitorea su actividad Web generando registros. En el caso de que alguien intente ingresar a la red, solo bastaría ingresar a la red interna para tener acceso al material disponible sin ser detectado por el software en mención

Además, de identificar los elementos de la red que intervienen, también se logra determinar en qué momento se realizará la prueba para obtener el resultado requerido.

Procedimiento

En esta operación se inicia la prueba de penetración y para poder identificar todos los activos se aplica un escaneo entero de la red. Una vez detectados todos los elementos, identificamos al usuario más vulnerable y procedemos a ejecutar el ataque dirigido al equipo víctima; donde este queda expuesto a robo y quedar a disponibilidad del atacante teniendo la oportunidad de tomar el control completo del equipo.

Resultados

En esta operación se obtiene prueba irrefutable que el equipo no es completamente seguro y es vulnerable a un ataque donde la víctima puede ser blanco de robo o manipulación para ataque empresarial.

Por los resultados obtenidos se elabora un informe detallado y preciso que demuestre las falencias existentes, con las debidas recomendaciones para que se tomen los correctivos necesarios.

3.3 Diagrama de Red

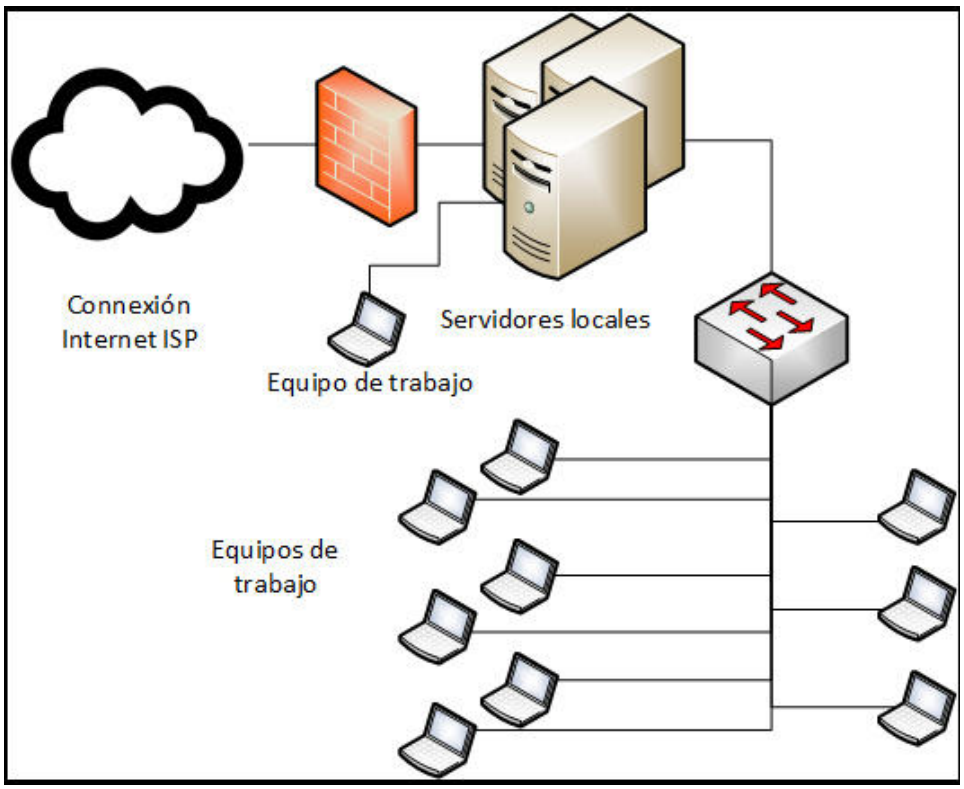


Figura 3.1 *– Diagrama interno actual de la oficina - Guayaquil*

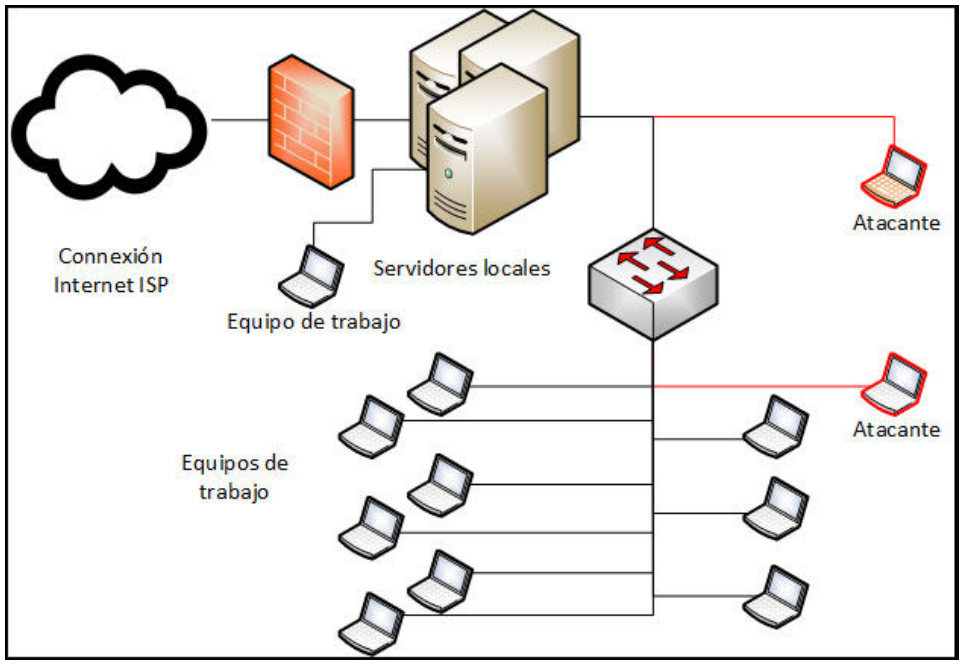


Figura 3.2 *– Arquitectura de red con los atacantes*

CAPÍTULO 4

ANÁLISIS Y EVALUACIÓN DE RIESGOS

4.1 Aplicación de Pruebas de Penetración

Cuando se inicia una prueba de penetración, se deben de llevar acabo un escaneo de la red, para poder identificar los puertos habilitados y las direcciones donde se podría ingresar y al mismo tiempo realizar saltos de unos elementos a los otros.

Este escaneo se lo podría aplicar con el siente comando en Linux:

nmap -sS -O xxx.xxx.xxx.xxx/xx

-sS = detecta los puertos sin dejar rastros

-O = Detecta el sistema operativo

Donde este comando revisará toda la red y los puertos disponibles para poder ingresar. Una vez detectado, se podría intentar ingresar a los elementos por medio de comando y sería tal como telnet IP puerto o un simple SSH.

Pruebas NMAP dentro de la red

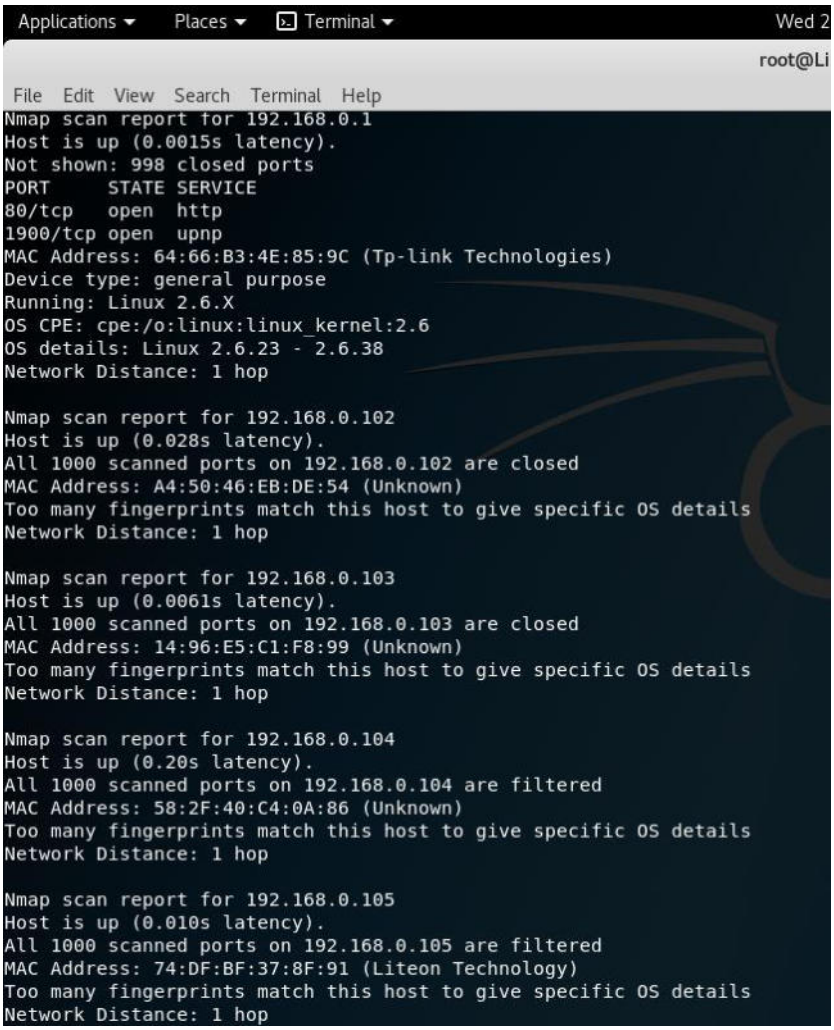


Figura 4.1 *– Comando NMAP en la red*

Para realizar la prueba de penetración se utilizó como herramienta Metasploit, empleando un payload, como la carga que se hace nuestra vulnerabilidad a explotar.

Debo aclarar que un mismo payload puede ser utilizado por distintos exploits y un mismo exploit puede utilizar varios payloads. El Metasploit tiene sobre 1800 exploits y más de 1000 payloads. Existen diferentes payloads, cada payload es para una vulnerabilidad, que además hay de diferentes tipos, como pueden ser self-reverse, CND, HTTP, HTTPS, reversa, inversa etc., es decir que no tienen por qué existir en una proporción 1:1.

4.2 Planeación y Preparación

#	Tareas	Enero				Febrero				Marzo			
		1	2	3	4	1	2	3	4	1	2	3	4
1	Planificación de proyecto												
2	Evaluación												
2.1	Identificaciones de la red												
2.2	Escaneo de la Red												
2.3	Análisis de resultados												
3	Pruebas de Penetración												
4	Limpieza de equipos												
5	Preparación de informe												

Tabla 1 *– Cronograma de actividades*

1er Paso – Escaneo de la Red

En primer lugar, se utilizaría el comando NMAP, que es el comando global de Linux, el mismo que nos permite escanear todos los elementos presentes en la red.

El alcance, permite conocer el número de elementos conectados, sus direcciones y puertos habilitados.

2do Paso – Pruebas de Penetración

Una vez, con los elementos descubiertos y sus direcciones se procede a probar el equipo y lograr obtener acceso a la información del usuario.

El alcance, es el acceso exitoso a un equipo dentro de la red.

3er Paso – Limpieza

Limpiar rastros del acceso y poder descargar la información satisfactoriamente.

4 to Paso – Opcional

Instalar software malicioso que nos sirve como puerta trasera. Aunque este paso no se aplicaría en la presente investigación porque puede ser considerado una violación directa a la seguridad de la empresa; es necesario mencionarlo por su aplicación en un ambiente virtual en donde no se ve afectado la integridad de la red real.

4.3 Evaluación

Al momento se ha podido escanear la red y se pudo analizar e identificar todos los elementos conectados al servidor de la empresa, estos

elementos se pueden actuar como puertas de acceso para el atacante, al momento de adquirir información de la empresa. Con esta información, el atacante podrá obtener un número de operadores dentro de la instalación.

También se pudo detectar los puertos disponibles en algunos equipos, por lo general, aquellos equipos que son provenientes de los usuarios no pertenecientes a la empresa directamente; estos computadores, que nos sirven de puerta de enlace, pueden ser monitoreados y brindar información sensible no solo sobre la empresa, sino también sobre el cliente asignado al usuario la cual se le está brindando soporte y se le asigna acceso remoto desde una red de internet, tomando como VPN el equipo atacado, y lograr extraer información o tener control sobre el equipo de tercero.

Previo a al ensayo se deben tomar en consideración las amenazas, los riesgos y las vulnerabilidades presentes en la prueba controlada.

El riesgo corresponde al impacto que podría ocasionar la amenaza para la empresa por las vulnerabilidades presentes en la red por las probabilidades que estas se puedan dar; lo que con el siguiente grafico nos muestra.

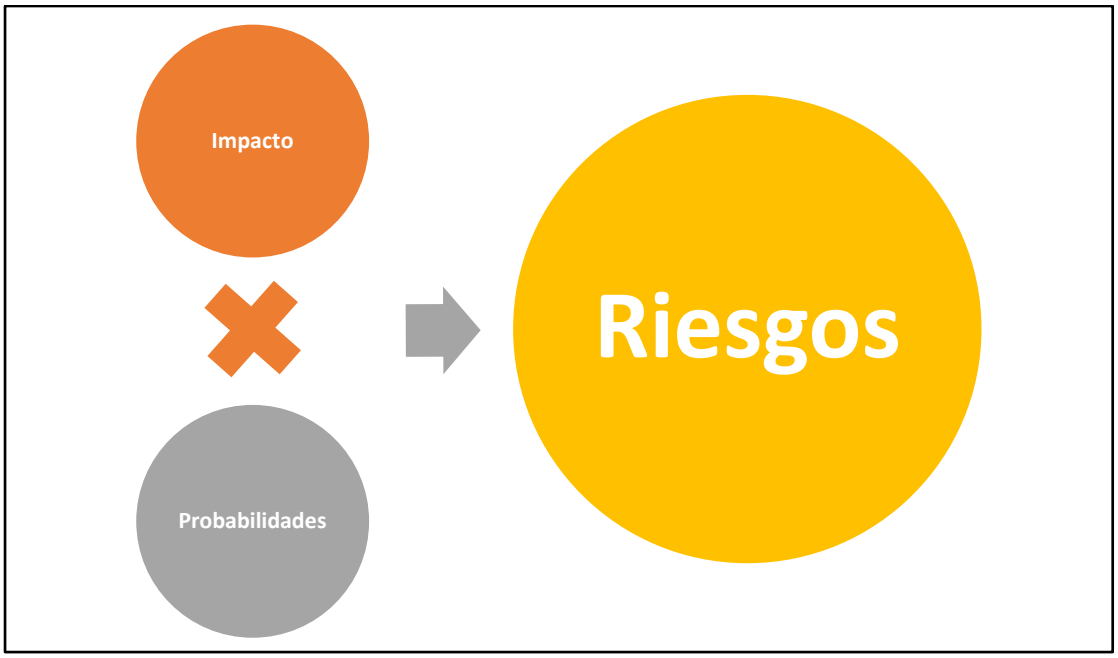


Figura 4.2 *– relación del Riesgo con impacto y probabilidad*

En base a los objetivos descrito en la presente tesis y otorgando un valor numérico en torno a las amenazas en un análisis comparativo, tenemos lo siguiente:

Amenazas	Impacto	Probabilidades	Riesgos	Nivel de Riesgo
Falta de ética profesional	3	1	3	Medio
Ataque de virus al usuario	1	2	2	Bajo
Robo físico de equipos	2	1	2	Bajo
Robo de información	3	2	6	Alto

Tabla 2 *– Riesgo generales de la empresa*

Con el cuadro comparativo, Tabla 2, se demuestra que el robo de información tiene uno de los mayores riesgos dentro de las actividades cotidianas para lo cual fue creada la empresa, por lo tanto, se debe tomar

correctivos en forma urgente con el fin de evitar repercusiones negativas, sobre todo en el campo económico y la garantía empresarial.

Por lo tanto, es necesario contar con un equipo laboral de profesionales que evalúen y controlen las vulnerabilidades que están presente en las actividades de los equipos internos a la red y aquellos que no son asociados directamente con la red.

En el presente estudio, la vulnerabilidad no se considera como un recurso, tampoco está considerado como una parte sensible, sino que se refiere a la instrucción de un agente externo que pueda acceder al sistema y a la red local desde donde pueda ejecutar el ataque que lo favorecería para su uso personal o comercial, repercutiendo esto en grandes pérdidas económicas para la empresa.

En la prueba de laboratorio controlada, para la demostración de la vulnerabilidad a nivel empresarial, se utilizó 2 equipos víctimas, en la que se logró identificar los puestos disponibles, utilizando el siguiente comando de “nmap” con el que se logró obtener los puertos disponibles.

nmap -T4 -A -v -sS -O 192.168.1.1/24

Esta herramienta otorga facilidades al atacante con el fin de identificar la red y lograr descubrir todos los elementos que tiene a su disposición. De esta manera el atacante podrá efectuar su tarea satisfactoriamente.

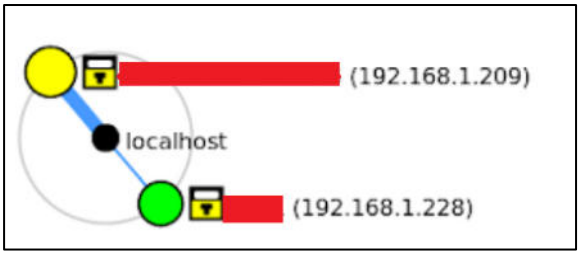


Figura 4.3 *– Victimas de la empresa en la red*

Una vez identificados los usuarios donde se efectuará el ataque, se procede a investigar los puertos disponibles y preparar las herramientas para proceder con el ataque.

192.168.1.228

1	0	1	0	26
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 28

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	46180	Additional DNS Hostnames
INFO	N/A	12634	Authenticated Check : OS Name and Installed Package Enumeration
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	117886	Local Checks Not Enabled (info)

Figura 4.4 *– Vulnerabilidades en usuarios 192.168.1.228*

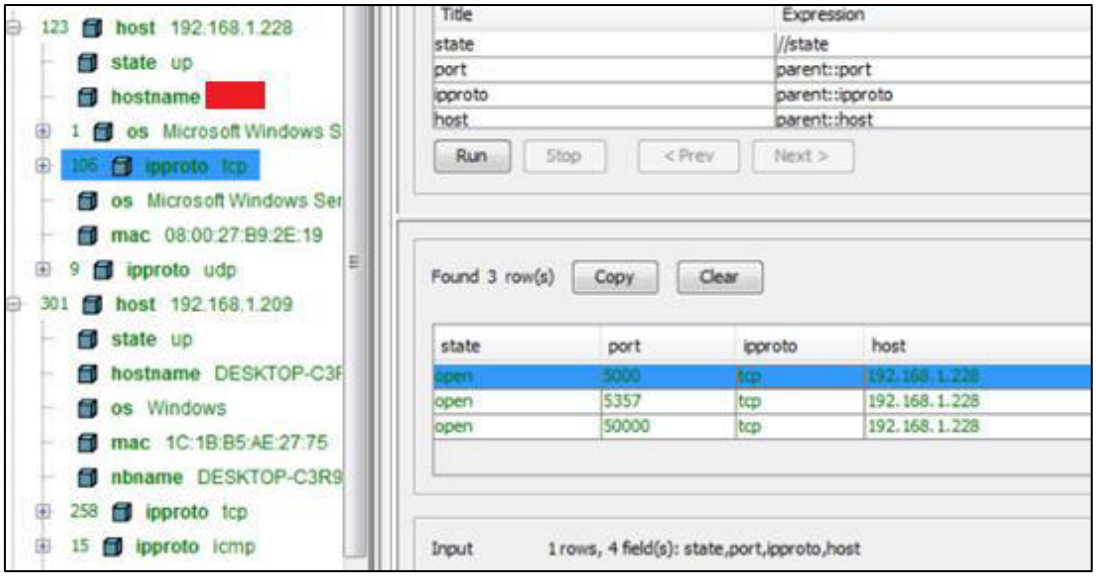


Figura 4.5 *– Puertos abiertos en el usuario 192.168.1.228*

Se logró identificar que el equipo no propietario de la empresa, con IP 192.168.1.228, con los puertos TCP 5000, 5357 y 50000 innecesariamente abiertos, esta es una de las vías más comunes para realizar un ataque por medio del software “metasplot” y poder aprovechar las vulnerabilidades dentro del equipo víctima. Estas vulnerabilidades no la pudimos observar en el equipo proveniente de la empresa. Con esto, se puede asumir que los equipos externos no cuentan con un plan de control periódico y sistemático, que otorga la herramienta de seguridad empresarial, con la que cuentan todos los equipos internos. En la siguiente tabla, se establece una comparación entre las “Victimas”, que son equipos utilizados dentro de la empresa por usuarios internos y externos; mientras que, los “Usuarios” considerados en el estudio, corresponden los diversos elementos de la red.

Dirección IP	Identificación	Sistema Operativo	número de puertos innecesariamente abiertos	Puertos abiertos	Riesgos
192.168.1.228	Víctima	Windows 10	3	5000, 5357, 500000	Alto
192.168.1.209	Víctima	Windows 10	0		Bajo
192.168.1.222	Usuario	Linux	0		Bajo
192.168.1.220	Usuario	Linux	0		Bajo
192.168.1.211	Usuario	Linux	0		Bajo
192.168.1.210	Usuario	Windows 10	0		Bajo
192.168.1.208	Usuario	Windows 7	0		Bajo

Tabla 3 *– Riesgo generales de la empresa.*

4.4 Identificación del Activo Crítico

Para la información critica que se puede sustraer de los equipos y de la empresa, se encuentran varios documentos de clientes asignados a los usuarios que tienen acceso y documentación de proyecto para su manejo dentro de la red. Estos documentos nos proporcionan información valiosa al atacante, tal como:

- Direcciones IP de equipos cliente.
- Documentos de productos de la empresa.
- Software de la empresa para instalación en equipos.
- Software de gestión de proyectos.
- Credenciales y contraseñas.
  - Para Cliente.
  - Internas de la empresa.

Aplicación de meterpreter a través de la interfaz web

En la siguiente imagen del comando de entrada, se observa como un usuario sin autorización podría obtener acceso al servidor mediante un módulo de meterpreter para Windows.

- Meterpreter: Es un payload bastante conocido y su nombre proviene de las palabras “meta” e “interpreter”. Es multifacética y se ejecuta en memoria a abajo nivel, es decir, que aporta una indetectabilidad optima, ya que los sistemas de protección se encuentran varias capas por encima. Es una de las Shell por defecto de Metasploit Framework y tiene muchas opciones y subcomandos propios, por lo que resulta una muy buena herramienta para auditores de seguridad informática.

Aplicación de meterpreter a través de la interfaz web

1) Se realiza el escaneo de la red utilizando la herramienta nmap.

2) Se crea nuestro payload utilizando msfvenom:

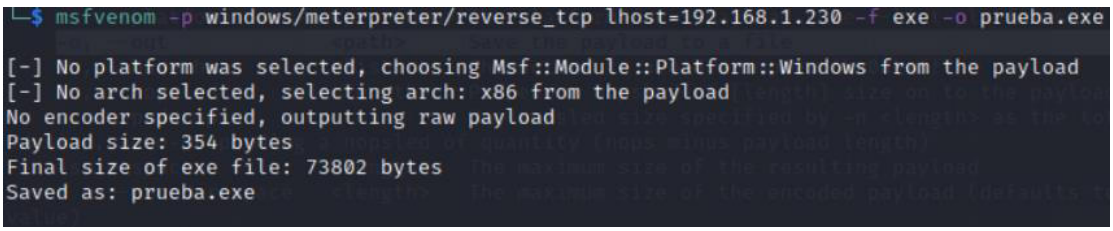


Figura 4.6 *– Creacion del payload*

3) Una vez creado el payload, se inicia el programa de Metasploit, que es con el cual se inicia el ataque esperando a que se dé el ataque.
4) La máquina víctima se conecta a la página web, deberemos dejar el payload en un lugar accesible para ser descargado desde

Internet, para ejecutar. En la red de la empresa es más fácil transmitir el payload de forma FTP.

Una vez ejecutado el payloads se inicia el ataque desde la máquina atacante a la víctima sin tocar el disco duro, la computadora atacante, ya tiene completo control desde la consola de metasploit.

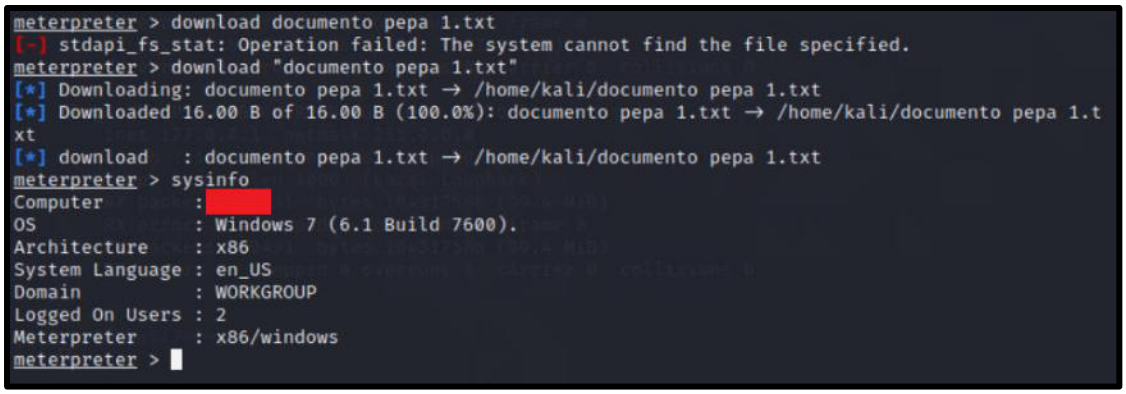


Figura 4.7 *– información de la victima*

Con esta herramienta se obtiene el control completo sobre la víctima; lo que permitiría un libre acceso a las siguientes acciones:

- Descarga de archivos.
- Cargar archivos.
- Activar la cámara web.
- Compartir la pantalla.
- Tomar captura de pantalla.
- Apagar el computador.
- Reiniciar el computador.

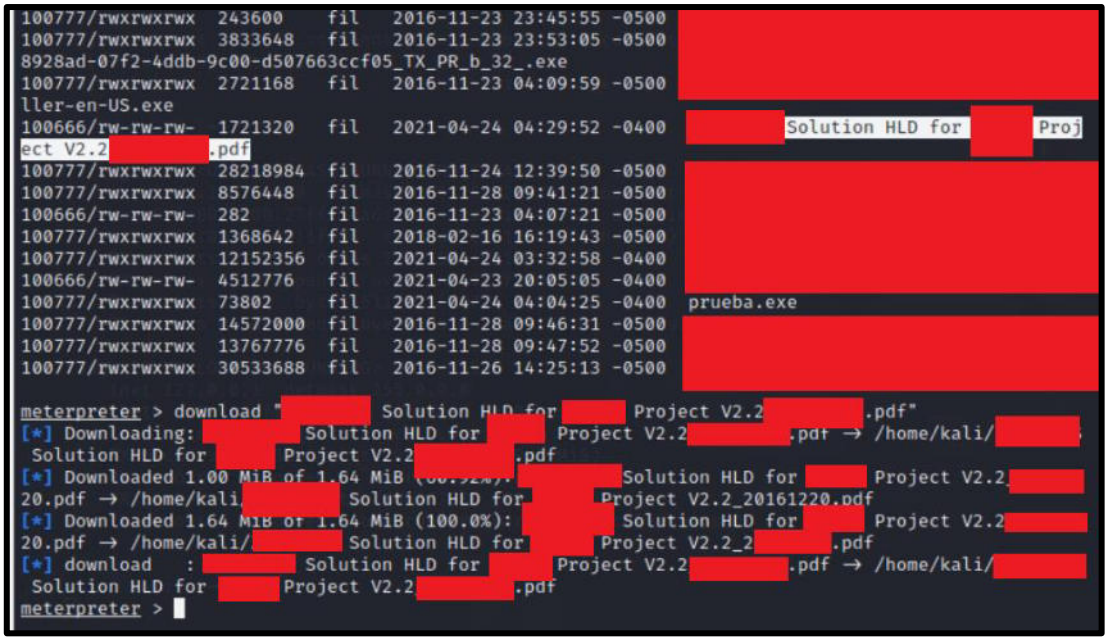


Figura 4.8 *– Proceso de descargada a la victima*

Concluyendo, los privilegios del programa meterpreter serán los mismos que los del usuario que ejecuta el script, si de forma incorrecta se ha configurado el usuario root tendremos acceso total a la máquina.

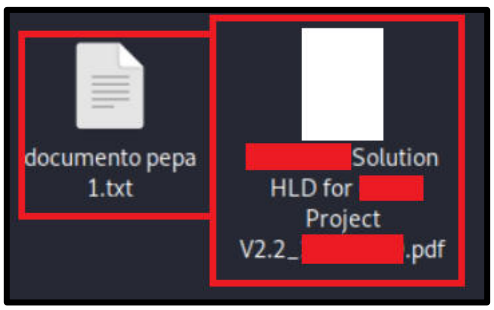


Figura 4.9 *– Información descargada a la victima*

4.5 Identificación de Errores encontrados

Dentro de los errores detectados durante todo el proceso o la aplicación, se pueden mencionar los siguientes:

- Puertos abiertos para la explotación.
- Falta de detección de software malicioso (payloads).
- Controlar los accesos físicos de los computadores.
- Fácil acceso a la red LAN.

Puertos abiertos para la explotación

La empresa cuenta con un software propio de protección, que se debe implementar obligatoriamente a todos los usuarios que se comunican con la red de la empresa. Estos softwares no son obligatorios para el personal que no es directamente asociados con la empresa. Unos de los objetivos principales de este software se encargan de limitar y asegurar el equipo donde fue instalado, así el atacante no tendrá oportunidad de explotar estos puertos abiertos que vienen por defecto en Windows.

Falta de detección de software malicioso (payloads)

Recapitulando lo anteriormente descrito en el punto anterior en torno al software de la empresa, este no es obligatorios para el personal que no es directamente asociados con la empresa. Los usuarios que no cuentan con el software empresarial, solamente tendrán acceso a la red local de la oficina más no a la red empresarial general que contiene los softwares destinados para los servicios externos.

Controlar los accesos físicos de los computadores y fácil acceso a la red LAN

Uno de los principales errores que se dan a nivel empresarial es la falta de control a la red local en la que intervienen usuarios internos y externos. Errores que guardan estrecha relación con la falta de implementación de normas y protocolos que permitan identificar el uso ilegal de las instalaciones para que el atacante pueda efectuar libremente robo o saboteo ya que cuenta con libre acceso a la red. Por lo tanto, el control de acceso a la red, representa una medida emergente para su seguridad.

4.6 Análisis de Riesgos

En lo relacionado con la ciberseguridad, el análisis de riesgo, es una evaluación de las distintas vulnerabilidades que afectan al sistema de red y con ellos producir grandes pérdidas empresariales ocasionados por robos, instrucción que afectarían directamente a un proyecto de servicio.

Se procede a evaluar las consecuencias de los peligros existentes en la red, orientándonos a tomar medidas de protección para todos los activos informáticos de la empresa, en este caso se empleó como la herramienta, la norma iso 27002:2013, para que, por medio de sus soluciones, se logre establecer las medidas correctivas y preventivas al sistema informático de la empresa.

CAPÍTULO 5

PLAN DE MITIGACIÓN DE RIESGOS

5.1 Justificación de la Metodología

Se conoce como plan de mitigación, como la herramienta estratégica con la cuenta las empresas aplicables a clientes, empleados, procesos y resultados finales; con el fin de menguar las probabilidades de ocurrencia del riesgo, minimizando el impacto que podría causar.

La OSSTMM es uno de los estándares más completos con la que se cuenta en la actualidad, se basa en el proceso para la verificación de los sistemas y la redes que dispone del acceso a internet revisando la seguridad total desde interne. Esta metodología está continuamente en desarrollo, por lo tanto, nos permite escalar mucho más el conocimiento de las redes presentes y de la seguridad; para garantizar la protección de la documentación en la empresa.

La metodología OSSTMM es una metodología empleada para realizar pentesting, que es una forma predefinida para seguir ciertos pasos y de esta manera lograr lo que el cibernauta requiere.

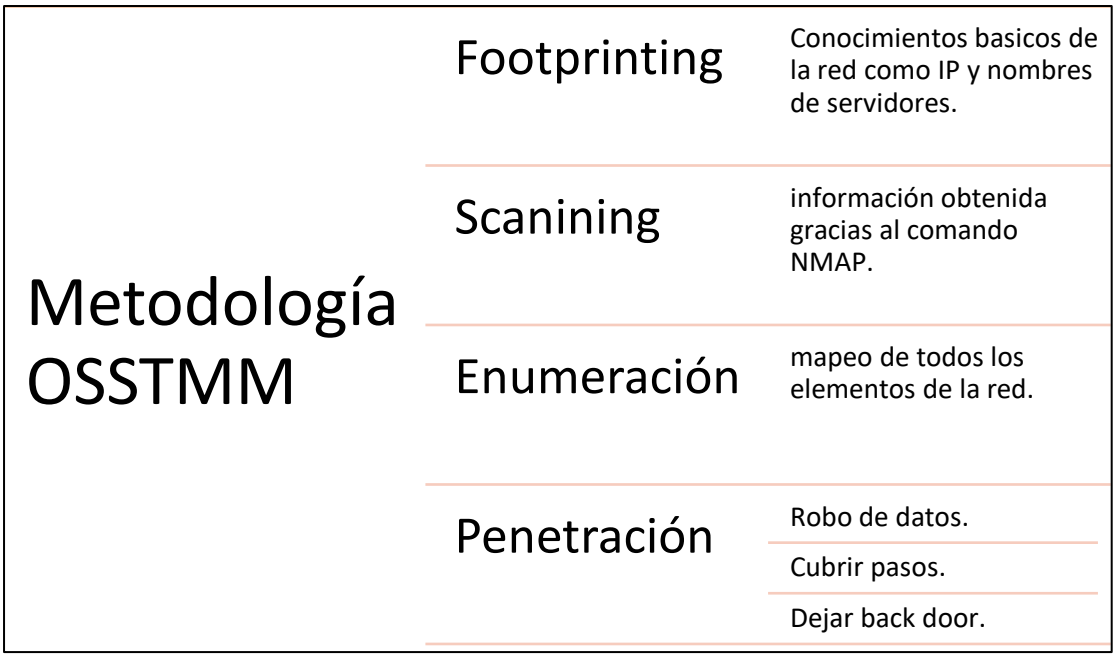


Figura 5.1 *– Metodología OSSTMM*

5.2 Plan de Mitigación

Lo que elimina la amenaza dentro de la empresa son los planes de mitigación, porque dan la razón a los riesgos que están expuestos porque reconocen que ciertos riesgos siempre formaran parte de la gestión dentro de los diferentes proyectos de servicios de la empresa.

Si bien es cierto que, muchas empresas aplican técnicas de estrategias de mitigación en sus operaciones diarias, pero no representan una garantía como ocurre con un verdadero plan de mitigación.

El plan de mitigación de riesgo de la empresa, tiene como objetivo principal fortalecer logros de la empresa en su finalidad, tratando de eliminar riesgos que podrían tener efectos negativos en el normal desarrollo de las actividades. Además, forma parte del ciclo de mejoras continuas que está basado en estrategia y acciones necesarias permitiendo identificar riesgos que afectarían al desarrollo normal del soporte a las empresas Carrier que da servicio de telecomunicaciones.

Dentro de la empresa en estudio los riesgos internos y externos han sido identificados por funcionarios de la empresa involucrados en diferentes proyectos que se ejecutan en los diferentes proyectos de servicio. Por consiguiente, se designó un funcionario especifico que tiene acceso directo al Resource manager, además de contar con el apoyo del operativo, para la implementación de los siguientes ítems.:

1) Identificación de riesgos que podrían afectar a los diferentes proyectos, considerando factores internos y externos.
2) Matriz de riesgos con la identificación de puntos vulnerables en la empresa tomando en cuenta la interacción con terceros, identificando las amenazas que pueden darse.
3) Identificar el cambio de condiciones en el entorno.
4) Plan de mitigación de riesgos e identificación de personal responsable.

5) Evaluación de los riesgos por técnicos.
6) Tipificación a cada una de los riesgos identificados, con el fin de tomar disposiciones, para minimizarlos y tomar medidas correctivas.

Con el fin de lograr una valoración continua de riesgos se elaboró la siguiente matriz en la cual se considera la probabilidad de ocurrencia en el eje horizontal: menos probable, más probable y muy probable versus el impacto: menor, mayor y crítico en el eje vertical.

5.3 Plan de Factibilidad

Este plan incluye un análisis de factibilidad técnico, operativo y económico que nos permite realizar un cálculo de costos, y el tiempo necesario. Además, este plan nos permite confirmar la acción que propone el plan de mitigación y como parte fundamental en la toma de decisiones para la empresa,

Sintetizando, los recursos mencionados detallo a continuación:

Análisis técnico: Observa recursos humanos (conocimientos y destrezas); los técnicos (dispositivos y materiales) y el tiempo necesario para su cumplimiento.

Análisis Operativo: En el que se realiza la confirmación del profesional escogido para el desarrollo del proyecto y que sea competente con experiencia para el desarrollo de plan de mitigación.

Por la importancia de la ejecución del proyecto es necesario que el Administrador de red, este capacitado en:

- Metodología OSSTMM (Manual de la Metodología Abierta de Comprobación de Seguridad).
- Metodología ISSAF (Marco de Evaluación de Seguridad de Sistemas de Información).
- Controles OWISAM (Metodología Abierta para el Análisis de Seguridad Wireless).
- Estándar Internacional ISO/IEC 27002:2013(Sistemas de Gestión la Seguridad de la Información).
- Herramientas para Hacking Ético (Sistemas y Aplicaciones de libre distribución).
- Infraestructura de Redes y Comunicación Inalámbrica.

Análisis Económico: El costo del plan fue mínimo, por lo que su implementación lo asumió la empresa.

Cabe mencionar que las metodologías ISSAF, OWISAM y OSSTMM se obtuvieron a través de sus páginas oficiales, por lo que no presentaron costo alguno por su acceso público; además, las herramientas para hacking tampoco tienen un costo.

Para el caso de las normas ISO/IEC 27002:2013 se utilizó la vía oficial que corresponde al apartado de “Código de prácticas para los controles de seguridad de la información”, disponible en la página oficial.

5.4 Reportes de Riesgos presentes en la red

Para cumplir con el Reportes de Riesgos presentes en la red, se apoya en la documentación de reportes realizados, previamente organizado que son analizados en conjunto con un equipo técnico auditor.

Lo que primero se realiza es una clasificación de la documentación considerado las amenazas y las vulnerabilidades detectadas durante su uso. Además, se realizan sugerencias de recomendaciones sobre las falencias de la red, con el fin de minimizar los riesgos que podrían repercutir en la obtención de los objetivos planteados.

La estructura del informe final para el presente estudio, se basa de acuerdo a lo descrito por OSSTMM.

- Resumen.
- Alcance del proyecto.
- Objetivos.
- Cronograma de actividades.
- Pruebas de seguridad realizadas (herramientas).
- Resumen de los resultados obtenidos (amenazas y vulnerabilidades).
- Análisis de Riesgos.
- Plan de Mitigación de riesgos (controles y Recomendaciones).

El informe técnico preparado, debe guardar la estructura mencionada; además, que debe estar respaldado de gran información, en forma gráfica

con el fin de demostrar y recomendar a los directivos, para proteger los riesgos y de esa manera tomar los correctivos necesarios con el fin proteger y defender los intereses del cliente y del proveedor.

CAPÍTULO 6

ANÁLISIS DE RESULTADOS

6.1 Informes y Resultados

De acuerdo a las pruebas controladas que se realizaron se pudo apreciar que fue el usuario no perteneciente a la empresa el que tuvo el problema de seguridad, los puertos TCP 5000, 5357 y 50000 se encontraban abiertos innecesariamente, debido a que la computadora no es auditada correctamente, carece de control técnico y además no cuenta con el catálogo completo de software propio de la empresa acorde a sus actividades. Estos equipos son preparados para el campo laboral por el mismo empleado y no por un grupo certificado en IT para la operación; por lo tanto, se recomienda cumplir con un riguroso control bajo las normas de la empresa al equipo del operador que no pertenece directamente a la misma, con el fin de garantizar la seguridad.

Uno de los controles principales de los que carecen estos equipos es un antivirus apropiado que impida la ejecución de archivos ".EXE", estos pueden ser muy peligrosos al momento de no conocer el origen del software, incluso otro control aplicable es poder impedir el ingreso de una memoria flash y para poder ejecutar un payload, lo que impediría que el atacante tendría acceso completo sobre la víctima.

6.2 Comparativas de Aplicación de Seguridad

Entre los parámetros técnicos comparativos observados en el presente estudio contamos con: permiso de uso, control de acceso, cifrado, verificación de 2 pasos

Permisos de uso: La parte principal en el acceso a la red, son los permisos obligatorios que permiten la operatividad dentro de la red. Los permisos se deben solicitar en el escenario que se requiere, para el caso de equipos internos. En el caso de los usuarios externos, se requiere un permiso más exigente, en comparación a lo que normalmente se aplica a nivel de equipos internos.

Protección de acceso: Se debe establecer una protección de acceso física o virtual, aunque su uso sea de forma puntual o momentánea, ya que el ingreso a la red o a las aplicaciones de la empresa, debería contarse con opciones disponible de control para mayor seguridad del personal.

Cifrado: Se cuenta con un cifrado de documentación para la información sensible en equipos de la compañía, en relación al emisor y receptor, sin la intervención de servidores como intermediario.

Verificación de 2 pasos: Para garantizar la seguridad, es necesario implementar una protección adicional por medio de token personalizado, ya que en el caso de que un atacante robe una contraseña, este no podría ingresar sin la autenticación adicional.

VULNERABILIDAD	Equipo cooperador	Equipos Empresarial
Cuenta con permisos obligatorios	NO	SI
Protección de acceso	NO	SI
No cuenta con cifrado de documentos	NO	SI
No cuenta con verificación de 2 pasos	SI	SI
Uso no controlado de memoria flash	NO	NO
Ejecución de archivos EXE	NO	SI

Tabla 4 *– Diferencia en los equipos empresariales*

En el cuadro de las vulnerabilidades comparando los equipos de la empresa y de los cooperadores (Personal técnicos dentro de la empresa que no está directamente asociados a la misma), en el análisis de la información obtenida, se observó que las maquinas propietarias de la empresa, son las más seguras por contar con un control interno. Resultados que no se obtienen en las máquinas de uso externo, debido a la falencia de los controles generales de protección a las vulnerabilidades ya identificadas.

Comparando los equipos cooperadores antes y después de la implementación de las medidas de seguridad consideradas en el presente

estudio, obtuvimos resultados que demuestran la seguridad de los equipos dentro de la empresa, por lo que podemos asumir que esto será garantía para evitar futuros ataques.

	ANTES				DESPUÉS			
VULNERABILIDAD	CRÍTICO	MAYOR	MEDIO	MENOR	CRÍTICO	MAYOR	MEDIO	MENOR
Cuenta con permisos obligatorios	X							X
Protección de acceso	X						X	
No cuenta con cifrado de documentos		X						x
No cuenta con verificación de 2 pasos	X							X
Uso no controlado de memoria flash		x					X	
Ejecución de archivos EXE	X						X	
Total	4	2	0	0	0	0	3	3

Tabla 5 *– Cuadro comparativo riesgos.*

El ensayo controlado realizado para el presente estudio, nos otorga un conocimiento que nos permitirá realizar un mejor análisis de protección en los diferentes niveles, dentro de la red, de las vulnerabilidades y por algún espacio que pueda existir. Finalmente, se aplicará técnicas de defensa con identificación automática realizados en controles periódicos de pentesting en redes, de tal forma que los administradores de la red puedan tomar correctivos inmediatos.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. La presente tesis, en su desarrollo nos permitió demostrar la importancia que tiene la configuración de forma correcta y tener controlados los usuarios cooperadores que tienen acceso a la red.
2. Se hace indispensable contar con un estado de alerta activo permita actualizar continuamente ya que la seguridad es un proceso que exige avanzar de acuerdo al ritmo del desarrollo de la tecnología.
3. La empresa carece de auditorías periódicas en los equipos presentes en la red y esto ha incrementado el riesgo de seguridad a todos los demás elementos presentes.

RECOMENDACIONES

1. Aplicando medidas preventivas y correctivas basados en el objetivo de control dentro de la norma ISO/IEC 27002:2013, se logró reducir los riesgos debidos a las falencias que estuvieron presentes. Por lo que se recomienda implementar esta metodología y con ella lograr un mejor respaldo en la seguridad informática.
2. En preciso que se tome serias acciones de concientización, preparación y difusión de mejores prácticas para minimizar los riesgos que por falta de conocimiento se ocasionan tanto a nivel personal, como empresarial.
3. Establecer auditorias periódicas en los equipos desde su ingreso considerando cada paso en los procesos establecidos.

BIBLIOGRAFÍA

[1]. Borghello, C. (2009). Firewalls - Cortafuegos. Obtenido de Seguridad de la Informacion: http://www.segu-info.com.ar/firewall/firewall.htm

[2]. ISO 27002. [En línea]. Disponible en: https://iso27002.wiki.zoho.com/.

[3]. Guía de referencia de Nmap (Página de manual). [En línea]. Disponible en: https://nmap.org/man/es/index.html.

[4]. K. Astudillo, Hacking Etico 101: Como Hackear Profesionalmente En 21 Dias O Menos! Createspace Independent Pub, 2013.

[5]. Ochoa Ovalles S. y Cervantes Sánchez, O. (2012) Seguridad informática. Contribuciones a las ciencias sociales.

[6]. OWISAM. [En línea]. Disponible en: https://www.owisam.org/es/P%C3%A1gina_principal.

GLOSARIO

1. **Amenaza –** Es Se refiere a las circunstancias o eventos de seguridad que pueden causar daños aprovechando las vulnerabilidades.
2. **Análisis de riesgo** – El proceso cuyo objetivo es identificar los componentes informáticos, sus vulnerabilidades y amenazas.
3. **Antispyware** – Es un programa utilizado para evitar que otros usuarios tengan acceso a contraseña, información de navegación e incluso información del computador.
4. **Hacking ético –** Burlar la seguridad de un sistema, con el fin de encontrar las vulnerabilidades del mismo.
5. **Firewall –** Software que evita que usuarios o programa ingresen a la red sin autorización.
6. **Impacto –** Es el daño producido por la materialización de una amenaza.
7. **Metasploit –** Es una herramienta que permite explotar seguridades o diferentes variables que impiden controlar a la víctima.
8. **OSSTMM –** Un test de intrusión es un test de seguridad con un objetivo definido que concluye cuando el objetivo es alcanzado o el tiempo ha terminado.
9. **Pentesting –** Es la práctica de ataque a la red, por la que nos permite descubrir las debilidades existentes.
10. **Phishing –** Este ataque se especializa en atacar al usuario más no al sistema directamente.
11. **Riesgo –** Es la posibilidad de que una vulnerabilidad sea explotada.
12. **Seguridad –** Se refiere a la protección de los elementos informáticos y su entorno.

13. **VPN –** Túnel virtual que garantiza la seguridad de los datos de un punto A a un punto B.
14. **Vulnerabilidad –** En una debilidad que podría ser aprovechada por un hacker con el fin de obtener acceso o privilegios no autorizados.

Anexos

Anfitrión: 192.168.1.228

Puertos y servicios abiertos:

puerto	estado	servicio	software
5000 tcp	abrir	upnp	
5000 tcp	abrir	commplex-principal	
5357 tcp	abrir	HTTP	Microsoft HTTPAPI httpd
50000 tcp	abrir	ibm-db2	
50000 tcp	abrir	pop3proxy	

Resumen de los hallazgos:

hallazgo	CVE IDs	afectado	severidad	fuente
Enumeración de plataforma común (CPE)		192.168.1.228	información	Nessus
Información de Nessus Scan		192.168.1.228	información	Nessus
Tipo de dispositivo		192.168.1.228	información	Nessus
Identificación del sistema operativo		192.168.1.228	información	Nessus
Detección del fabricante de tarjetas Ethernet		192.168.1.228	información	Nessus
Direcciones MAC Ethernet		192.168.1.228	información	Nessus
Resolución de nombre de dominio completo (FQDN) del host		192.168.1.228	información	Nessus
Tcp/IP Marcas de tiempo compatibles		192.168.1.228	información	Nessus
Escáner Nessus SYN		192.168.1.228:5000 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.228:50000 (tcp)	información	Nessus
Información de Traceroute		192.168.1.228	información	Nessus

Anfitrión: 192.168.1.209

Puertos y servicios abiertos:

puerto	estado	servicio	software
445 tcp		netbios-ssn	
135 tcp		epmap	
139 tcp		netbios-ssn	
49689 tcp		epmap	

49668 tcp		epmap	
49667 tcp		epmap	
49664 tcp		epmap	
49665 tcp		epmap	
49666 tcp		epmap	
137 udp		netbios-ns	

Resumen de los hallazgos:

hallazgo	CVE IDs	afectado	severidad	fuente
No se requiere firma de SMB		192.168.1.209:445 (tcp)	Medio	Nessus
Divulgación de información de relleno de trama de múltiples controladores Ethernet (Etherleak)	CVE-2003-0001	192.168.1.209	Bajo	Nessus
Comprobaciones locales no habilitadas (info)		192.168.1.209	información	Nessus
Enumeración de plataforma común (CPE)		192.168.1.209	información	Nessus
Información de Nessus Scan		192.168.1.209	información	Nessus
Estado de credenciales de destino por protocolo de autenticación - Sin credenciales proporcionadas		192.168.1.209	información	Nessus
Tipo de dispositivo		192.168.1.209	información	Nessus
Identificación del sistema operativo		192.168.1.209	información	Nessus
Detección del fabricante de tarjetas Ethernet		192.168.1.209	información	Nessus
Direcciones MAC Ethernet		192.168.1.209	información	Nessus
Resolución de nombre de dominio completo (FQDN) del host		192.168.1.209	información	Nessus
Microsoft Windows SMB2 y SMB3 Dialectos compatibles (comprobación remota)		192.168.1.209:445 (tcp)	información	Nessus
Versiones SMB de Microsoft Windows compatibles (comprobación remota)		192.168.1.209:445 (tcp)	información	Nessus
WMI no disponible		192.168.1.209:445 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.209:445 (tcp)	información	Nessus
Enumeración de servicios DCE		192.168.1.209:445 (tcp)	información	Nessus
Detección de servicios SMB		192.168.1.209:445 (tcp)	información	Nessus

de Microsoft Windows				
Escáner Nessus SYN		192.168.1.209:135 (tcp)	información	Nessus
Enumeración de servicios DCE		192.168.1.209:135 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.209:139 (tcp)	información	Nessus
Detección de servicios SMB de Microsoft Windows		192.168.1.209:139 (tcp)	información	Nessus
Enumeración de servicios DCE		192.168.1.209:49689 (tcp)	información	Nessus
Enumeración de servicios DCE		192.168.1.209:49668 (tcp)	información	Nessus
Enumeración de servicios DCE		192.168.1.209:49667 (tcp)	información	Nessus
Enumeración de servicios DCE		192.168.1.209:49664 (tcp)	información	Nessus
Enumeración de servicios DCE		192.168.1.209:49665 (tcp)	información	Nessus
Enumeración de servicios DCE		192.168.1.209:49666 (tcp)	información	Nessus
Información de Traceroute		192.168.1.209	información	Nessus
Divulgación de información de host remoto de Windows NetBIOS / SMB		192.168.1.209:137 (udp)	información	Nessus

Anfitrión: 192.168.1.222

Puertos y servicios abiertos:

puerto	estado	servicio	software
25 tcp		SMTP	

Resumen de los hallazgos:

hallazgo	CVE IDs	afectado	severidad	fuente
Información de Nessus Scan		192.168.1.222	información	Nessus
Error en la identificación del sistema operativo		192.168.1.222	información	Nessus
Detección del fabricante de tarjetas Ethernet		192.168.1.222	información	Nessus
Direcciones MAC Ethernet		192.168.1.222	información	Nessus
Resolución de nombre de dominio completo (FQDN) del host		192.168.1.222	información	Nessus
Comprobación de conexión del servidor SMTP		192.168.1.222:25 (tcp)	información	Nessus

Anfitrión: 192.168.1.220

Puertos y servicios abiertos:

puerto	estado	servicio	software
110 tcp		pop3	
143 tcp		Imap	
587 tcp		SMTP	
25 tcp		SMTP	
995 tcp			
993 tcp			
563 tcp			
465 tcp		Urd	
119 tcp		Nntp	
7200 tcp		fodms	

Resumen de los hallazgos:

hallazgo	CVE IDs	afectado	severidad	fuente
Divulgación de información de relleno de trama de múltiples controladores Ethernet (Etherleak)	CVE-2003-0001	192.168.1.220	Bajo	Nessus
Información de Nessus Scan		192.168.1.220	información	Nessus
Error en la identificación del sistema operativo		192.168.1.220	información	Nessus
Direcciones MAC Ethernet		192.168.1.220	información	Nessus
Resolución de nombre de dominio completo (FQDN) del host		192.168.1.220	información	Nessus
Tcp/IP Marcas de tiempo compatibles		192.168.1.220	información	Nessus
Detección de servicios desconocidos: Recuperación de banners		192.168.1.220:110 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.220:110 (tcp)	información	Nessus
Recuperación de banners de servicio IMAP		192.168.1.220:143 (tcp)	información	Nessus
Detección de servicios (solicitud GET)		192.168.1.220:143 (tcp)	información	Nessus

Escáner Nessus SYN		192.168.1.220:143 (tcp)	información	Nessus
Comprobación de conexión del servidor SMTP		192.168.1.220:587 (tcp)	información	Nessus
Detección de servicios		192.168.1.220:587 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.220:587 (tcp)	información	Nessus
Comprobación de conexión del servidor SMTP		192.168.1.220:25 (tcp)	información	Nessus
Detección de servicios		192.168.1.220:25 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.220:25 (tcp)	información	Nessus
Detección de servicios		192.168.1.220:995 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.220:995 (tcp)	información	Nessus
Detección de servicios		192.168.1.220:993 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.220:993 (tcp)	información	Nessus
Detección de servicios		192.168.1.220:563 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.220:563 (tcp)	información	Nessus
Detección de servicios		192.168.1.220:465 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.220:465 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.220:119 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.220:7200 (tcp)	información	Nessus
Icmp Timestamp Solicitud Divulgación remota de fecha	CVE-1999-0524	192.168.1.220	información	Nessus
Información de Traceroute		192.168.1.220	información	Nessus

Anfitrión: 192.168.1.211

Puertos y servicios abiertos:

puerto	estado	servicio	software
8000 tcp		HTTP	
1386 tcp		HTTP	
7100 tcp		HTTP	
8121 tcp		apollo-data	
5555 tcp		agente personal	
5353 udp		mdns	
1900 udp		upnp	

Resumen de los hallazgos:

hallazgo	CVE IDs	afectado	severidad	fuente
Directorio del servidor Web atraviesa el acceso arbitrario a archivos	CVE-2000-0920 CVE-2007-6483 CVE-2008-5315 CVE-2010-1571 CVE-2010-3459 CVE-2010-3460 CVE-2010-3487 CVE-2010-3488 CVE-2010-3743 CVE-2010-4181 CVE-2011-1900 CVE-2011-2524 CVE-2011-4788 CVE-2012-0697 CVE-2012-1464 CVE-2012-5100 CVE-2012-5335 CVE-2012-5344 CVE-2012-5641 CVE-2013-2619 CVE-2013-3304 CVE-2014-3744	192.168.1.211:8000 (tcp)	Alto	Nessus
J Walk Application Server codificado Directorio Traversal Acceso arbitrario a archivos	CVE-2003-1529	192.168.1.211:8000 (tcp)	Medio	Nessus
Apache WebDAV Módulo PROPFIND Listado de Directorios Arbitrarios	CVE-2000-0869	192.168.1.211:8000 (tcp)	Medio	Nessus
Divulgación de información de relleno de trama de múltiples controladores Ethernet (Etherleak)	CVE-2003-0001	192.168.1.211	Bajo	Nessus
Enumeración de plataforma común (CPE)		192.168.1.211	información	Nessus
Información de Nessus Scan		192.168.1.211	información	Nessus
Tipo de dispositivo		192.168.1.211	información	Nessus
Identificación del sistema operativo		192.168.1.211	información	Nessus
Detección del fabricante de tarjetas Ethernet		192.168.1.211	información	Nessus
Direcciones MAC Ethernet		192.168.1.211	información	Nessus
Resolución de nombre de dominio completo (FQDN) del host		192.168.1.211	información	Nessus
Tcp/IP Marcas de tiempo compatibles		192.168.1.211	información	Nessus
Detección de WebDAV		192.168.1.211:8000 (tcp)	información	Nessus
Información del Protocolo de transferencia de hipertexto		192.168.1.211:8000 (tcp)	información	Nessus

(HTTP)				
Tipo y versión del servidor HTTP		192.168.1.211:8000 (tcp)	información	Nessus
Métodos HTTP permitidos (por directorio)		192.168.1.211:8000 (tcp)	información	Nessus
Detección de servicios		192.168.1.211:8000 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.211:8000 (tcp)	información	Nessus
Detección de UPnP del servidor web		192.168.1.211:1386 (tcp)	información	Nessus
Tipo y versión del servidor HTTP		192.168.1.211:1386 (tcp)	información	Nessus
Detección de servidor web integrado		192.168.1.211:1386 (tcp)	información	Nessus
Detección de servicios		192.168.1.211:1386 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.211:1386 (tcp)	información	Nessus
Detección de servicios (solicitud HELP)		192.168.1.211:7100 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.211:7100 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.211:8121 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.211:5555 (tcp)	información	Nessus
Icmp Timestamp Solicitud Divulgación remota de fecha	CVE-1999-0524	192.168.1.211	información	Nessus
Información de Traceroute		192.168.1.211	información	Nessus
Detección de mDNS (red local)		192.168.1.211:5353 (udp)	información	Nessus
Detección de protocolo universal plug and play (UPnP)		192.168.1.211:1900 (udp)	información	Nessus

Anfitrión: 192.168.1.210

Puertos y servicios abiertos:

puerto	estado	servicio	software
5353 udp		mdns	

Resumen de los hallazgos:

hallazgo	CVE IDs	afectado	severidad	fuente

Divulgación de información de relleno de trama de múltiples controladores Ethernet (Etherleak)	CVE-2003-0001	192.168.1.210	Bajo	Nessus
Información de Nessus Scan		192.168.1.210	información	Nessus
Detección del fabricante de tarjetas Ethernet		192.168.1.210	información	Nessus
Direcciones MAC Ethernet		192.168.1.210	información	Nessus
Resolución de nombre de dominio completo (FQDN) del host		192.168.1.210	información	Nessus
Icmp Timestamp Solicitud Divulgación remota de fecha	CVE-1999-0524	192.168.1.210	información	Nessus
Información de Traceroute		192.168.1.210	información	Nessus
Detección de mDNS (red local)		192.168.1.210:5353 (udp)	información	Nessus

Anfitrión: 192.168.1.208

Puertos y servicios abiertos:

puerto	estado	servicio	software
445 tcp		netbios-ssn	
2869 tcp		HTTP	
1026 tcp		epmap	
1072 tcp		epmap	
1029 tcp		epmap	
1025 tcp		epmap	
1027 tcp		epmap	
135 tcp		epmap	
139 tcp		netbios-ssn	
5353 udp		mdns	
1900 udp		upnp	
137 udp		netbios-ns	

Resumen de los hallazgos:

hallazgo	CVE IDs	afectado	severidad	fuente
Sistema operativo Windows no compatible (remoto)		192.168.1.208	Alto	Nessus
No se requiere firma de SMB		192.168.1.208:445 (tcp)	Medio	Nessus
Comprobaciones locales no habilitadas (info)		192.168.1.208	información	Nessus

Enumeración de plataforma común (CPE)		192.168.1.208	información	Nessus
Información de Nessus Scan		192.168.1.208	información	Nessus
Estado de credenciales de destino por protocolo de autenticación - Sin credenciales proporcionadas		192.168.1.208	información	Nessus
Tipo de dispositivo		192.168.1.208	información	Nessus
Identificación del sistema operativo		192.168.1.208	información	Nessus
Detección del fabricante de tarjetas Ethernet		192.168.1.208	información	Nessus
Direcciones MAC Ethernet		192.168.1.208	información	Nessus
Nombres de host DNS adicionales		192.168.1.208	información	Nessus
Comprobación autenticada: Nombre del sistema operativo y Enumeración de paquetes instalados		192.168.1.208	información	Nessus
Identificación del sistema operativo y enumeración de software instalado a través de SSH v2 (uso de nueva biblioteca SSH)		192.168.1.208	información	Nessus
Resolución de nombre de dominio completo (FQDN) del host		192.168.1.208	información	Nessus
Nessus Windows Scan No realizado con privilegios de administrador		192.168.1.208	información	Nessus
Microsoft Windows SMB2 y SMB3 Dialectos compatibles (comprobación remota)		192.168.1.208:445 (tcp)	información	Nessus
Protocolo de bloque de mensajes de servidor (SMB) versión 1 habilitado (comprobación sin credenciales)		192.168.1.208:445 (tcp)	información	Nessus
Versiones SMB de Microsoft Windows compatibles (comprobación remota)		192.168.1.208:445 (tcp)	información	Nessus
Registro SMB de Microsoft Windows: Nessus no puede acceder al Registro de Windows		192.168.1.208:445 (tcp)	información	Nessus
WMI no disponible		192.168.1.208:445 (tcp)	información	Nessus

Divulgación de información del sistema remoto SMB de Microsoft Windows		192.168.1.208:445 (tcp)	información	Nessus
Enumeración de servicios DCE		192.168.1.208:445 (tcp)	información	Nessus
Detección de servicios SMB de Microsoft Windows		192.168.1.208:445 (tcp)	información	Nessus
Detección de UPnP del servidor web		192.168.1.208:2869 (tcp)	información	Nessus
Enumeración de servicios DCE		192.168.1.208:1026 (tcp)	información	Nessus
Enumeración de servicios DCE		192.168.1.208:1072 (tcp)	información	Nessus
Enumeración de servicios DCE		192.168.1.208:1029 (tcp)	información	Nessus
Enumeración de servicios DCE		192.168.1.208:1025 (tcp)	información	Nessus
Enumeración de servicios DCE		192.168.1.208:1027 (tcp)	información	Nessus
Enumeración de servicios DCE		192.168.1.208:135 (tcp)	información	Nessus
Detección de servicios SMB de Microsoft Windows		192.168.1.208:139 (tcp)	información	Nessus
Detección de mDNS (red local)		192.168.1.208:5353 (udp)	información	Nessus
Detección de protocolo universal plug and play (UPnP)		192.168.1.208:1900 (udp)	información	Nessus
Divulgación de información de host remoto de Windows NetBIOS / SMB		192.168.1.208:137 (udp)	información	Nessus

Anfitrión: 192.168.1.1

Puertos y servicios abiertos:

puerto	estado	servicio	software
445 tcp		netbios-ssn	
49152 tcp		HTTP	
80 tcp		HTTP	
53 tcp		dominio	
139 tcp		netbios-ssn	
53 udp		dominio	
67 udp		bootps	

1900 udp		upnp	
137 udp		netbios-ns	

Resumen de los hallazgos:

hallazgo	CVE IDs	afectado	severidad	fuente
Reenvío IP habilitado	CVE-1999-0511	192.168.1.1	Medio	Nessus
No se requiere firma de SMB		192.168.1.1:445 (tcp)	Medio	Nessus
Divulgación de información remota de Snooping de caché del servidor DNS		192.168.1.1:53 (udp)	Medio	Nessus
Divulgación de información de relleno de trama de múltiples controladores Ethernet (Etherleak)	CVE-2003-0001	192.168.1.1	Bajo	Nessus
Detección de servidor DHCP		192.168.1.1:67 (udp)	Bajo	Nessus
Información de Nessus Scan		192.168.1.1	información	Nessus
Tipo de dispositivo		192.168.1.1	información	Nessus
Identificación del sistema operativo		192.168.1.1	información	Nessus
Detección del fabricante de tarjetas Ethernet		192.168.1.1	información	Nessus
Direcciones MAC Ethernet		192.168.1.1	información	Nessus
Resolución de nombre de dominio completo (FQDN) del host		192.168.1.1	información	Nessus
Microsoft Windows SMB2 y SMB3 Dialectos compatibles (comprobación remota)		192.168.1.1:445 (tcp)	información	Nessus
WMI no disponible		192.168.1.1:445 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.1:445 (tcp)	información	Nessus
Detección de servicios SMB de Microsoft Windows		192.168.1.1:445 (tcp)	información	Nessus
Detección de UPnP del servidor web		192.168.1.1:49152 (tcp)	información	Nessus
Información del Protocolo de transferencia de hipertexto (HTTP)		192.168.1.1:80 (tcp)	información	Nessus
Tipo y versión del servidor HTTP		192.168.1.1:80 (tcp)	información	Nessus
Detección de servicios		192.168.1.1:80 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.1:80 (tcp)	información	Nessus
Detección de versiones de servidor DNS		192.168.1.1:53 (tcp)	información	Nessus

Detección de servidores DNS		192.168.1.1:53 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.1:53 (tcp)	información	Nessus
Escáner Nessus SYN		192.168.1.1:139 (tcp)	información	Nessus
Detección de servicios SMB de Microsoft Windows		192.168.1.1:139 (tcp)	información	Nessus
Icmp Timestamp Solicitud Divulgación remota de fecha	CVE-1999-0524	192.168.1.1	información	Nessus
Información de Traceroute		192.168.1.1	información	Nessus
Divulgación del nombre de host del servidor DNS.bind		192.168.1.1:53 (udp)	información	Nessus
Detección de servidores DNS		192.168.1.1:53 (udp)	información	Nessus
Detección de protocolo universal plug and play (UPnP)		192.168.1.1:1900 (udp)	información	Nessus
Divulgación de información de host remoto de Windows NetBIOS / SMB		192.168.1.1:137 (udp)	información	Nessus