INSTITUTO TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

“Estudio de la Seguridad Informática y sus aplicaciones para prevenir la infiltración de los Hackers en las empresas”

Estudiante

Carlos Alberto Albarracín Lazo

Tutor

Ing. Pablo Tamayo

Cuenca Ecuador

Diciembre 2011

CERTIFICADO DE RESPONSABILIDAD

Yo, Ing. Pablo Tamayo, certifico que el señor Carlos Alberto Albarracín Lazo con cedula, No 01037631008 realizo la presente tesis con el título "Estudio de la Seguridad Informática y sus aplicaciones para prevenir la infiltración de los Hackers en las empresas", y que es autor intelectual del mismo, que es original autentico y personal.

_____

Ing. Pablo Tamayo

ACTA DE CESION DE DERECHOS

Yo Carlos Alberto Albarracín Lazo, estudiante de Ingeniería de Sistemas Informáticos, declaro conocer y aceptar las disposiciones del programa de estudio, que en lo pendiente dice: "*Es patrimonio de la universidad tecnológica Israel, todos los resultados provenientes de investigaciones, de trabajos científicos, técnicos o tecnológicos y de tesis o trabajos que se realicen a través o con el apoyo de cualquier tipo de Universidad tecnológica Israel. Esto significa la cesión de los derechos de propiedad intelectual a la universidad tecnológica Israel* "

_____

CERTIFICADO DE AUTORIA

El documento de tesis con titulo “Estudio de la Seguridad Informática y sus aplicaciones para prevenir la infiltración de los Hackers en las empresas” ha sido desarrollado por Carlos Alberto Albarracín Lazo con C.C. No. 0103763108 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de esta tesis sin previa autorización.

_____

Carlos Albarracín L.

DEDICATORIA

A Dios, a mis padres a mis hermanos y a todas las personas que conforman mi familia, y amigos, que con su apoyo me han sabido guiar en este largo camino de mi vida.

AGRADECIMIENTO

El agradecimiento más grande va dedicado a mi madre Zoila Lazo C. Que con su apoyo y fortaleza me ha sabido guiar para poder alcanzar los objetivos que me he planteado en la vida, Por ella vivo y a Dios agradezco cada día que respiro.

Agradezco a mis hermanos, y a mi padre aunque el ya no esté conmigo sé que me ha bendecido para poder terminar con mis estudios satisfactoriamente, la admiración que siento por cada uno de ellos es indescriptible y les agradezco por su apoyo y ejemplo que supieron darme.

A mi tutor el Ing. Pablo Tamayo y a cada una de los profesores de la institución, que con su sabiduría y comprensión supo guiarme en el desarrollo de mi tesis, para así poder formarme en la vida profesional.

RESUMEN

El siguiente proyecto tiene como objetivo, hacer conciencia sobre la seguridad informática que se debe implementar tanto en las más grandes organizaciones o todo individuo en particular que maneja información de gran valor económico o personal, ya que en este mundo tecnológico que avanza a pasos agigantados debemos protegernos de los intrusos que merodean las redes de información, tratando de vulnerar la seguridades que están implementadas en los sistemas ya sea por el simple modo de curiosidad con la finalidad de perjudicar a alguna institución u individuo.

Para poder contrarrestar estos malos inconvenientes existen muchas soluciones en nuestra actualidad, con una gran cantidad de herramientas desarrolladas especialmente para cumplir con la función de proteger nuestra información, existe herramientas de con licencia propietario y otras que son software libre, cada una de ellas con sus diferentes características y valor económico.

Dependerá mucho de las políticas de seguridad de la empresa que se ha planteado, y del funcionamiento que estas realicen para poder adquirir un software que se adapte a sus respectivas necesidades, ninguna institución pública o privada está libre de ataques por mas que se utilice las más grandes herramientas de protección ya que los Hackers cada día se inventan métodos de infiltración para vulnerar los sistemas de seguridad.

Por esta razón, y mediante el desarrollo de la presente tesis de grado se quiere apoyar con un pequeño estudio sobre una de las tantas herramientas que existen en nuestro medio, y al cual se ha rescatado la herramienta de seguridad informática “NESSUS”, el motivo de la selección de dicha herramienta es sencillo, pues nos ayuda a protege nuestra red a grandes distancias y nos permite realizar auditorías remotas, y devolviéndonos resultados por si algún intruso está intentado vulnerar nuestra red.

SUMMARY

The next project has the objective to raise awareness about computer security that must be implemented both in the larger organizations or any particular individual who manages information of great economic or personal, because in this technological world that we making strides guard against intruders who roam the networks, trying to breach the security systems are implemented either by the simple way of curiosity with the purpose of harming any institution or individual.

To counteract these disadvantages there are many solutions evil in our present, with a large number of tools developed specifically to meet the function of protecting our information, there owner licensed tools and others that are free software, each with its different characteristics and economic value.

Much will depend on the security policies of the company that has been raised and the operation they carry out in order to acquire software that suits their needs, any public or private institution is free of attacks rather than using the most great protection tools as hackers invent every day infiltration methods to undermine the security systems.

For this reason, and through the development of this thesis is to support a small study on one of the many tools that exist in our environment, and to which he has rescued the security tool "Nessus", the reason the selection of this tool is simple, it helps us to protect our network over long distances and allows us to audit remote and return results if an intruder is attempting to undermine our network.

INDICE

LISTA DE CUADROS Y GRAFICOS

INTRODUCCION

En nuestro medio, los sistemas de información son esenciales en la gran mayoría de las organizaciones tanto públicas o privadas que cuentan con una tecnología de punta y en constante crecimiento, por ello la viabilidad de los proyectos o servicios que están en evolución y desarrollo dependen no solo de las características y ventajas de la tecnología en uso, sino también de la disponibilidad, confidencialidad, integridad, escalabilidad y seguridad de sus equipos, servicios, y datos. Ya que la información ha sido desde siempre un bien invaluable y protegerla ha sido una tarea continua y de vital importancia. A medida que se crean nuevas técnicas para la transmisión de la información.

En la actualidad, se pude realizar una diversidad de tareas o transacciones a través de Internet y para muchas de ellas, es imprescindible que se garantice un nivel adecuado de seguridad. Esto es posible si se siguen ciertas normas que se pueden definir según la necesidad de la Organización.

La seguridad no es solo la aplicación de nuevos programas para protegernos, es más bien un cambio de conducta y de pensar. Hay que adueñarse del concepto de seguridad e incluso volverse algo paranoico para que en cada área y servicio que presta la Universidad se piense en seguridad y en cómo incrementarla.

Los intrusos (Hackers) idean formas para acceder a la información sin ser autorizados o detectados, los ataques efectuados son por muchos motivos tales como: curiosidad, sabotaje, beneficio, en fin una gran cantidad de circunstancias que llevan a cometer estos ataques. Por eso es necesario estar preparado a la hora de actuar ante los incidentes que pueden sufrir los equipos ya que esto impediría que los servicios que presta la Organización que se lleven con total normalidad.

CAPITULO I

1. PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la realidad problemática

Antecedentes

Los nuevos delitos tecnológicos avanzan día a día y con ellos, quienes estudiamos el nuevo mundo que internet ha gestado, preocupados por el avance de los nuevos riesgos que ponen en vilo a las infraestructuras gubernamentales buscamos las colaboración mutua de los gobiernos para la lucha y prevención del crimen tecnológico.

Según el responsable de la Asociación para la Investigación de los Delitos de Alta Tecnología (High Technology Crime Investigative Association – HTCIA) las fuerzas de seguridad oficiales no cuentan con el personal o la tecnología suficiente para atender a las demandas de estos sectores frente a un problema calificado como "menor" frente a los delitos usuales.

¿Y qué ocurre en nuestro país?

Desde que en 1999 en el Ecuador se puso en el tapete de la discusión el proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, desde ese tiempo se puso de moda el tema, se realizaron cursos, seminarios, encuentros. También se conformo comisiones para la discusión de la Ley y para que formulen observaciones a la misma por parte de los organismos directamente interesados en el tema como el CONATEL, la Superintendencia de Bancos, las Cámaras de Comercio y otros, que ven el Comercio Telemático una buena oportunidad de hacer negocios y de paso hacer que nuestro país entre en el boom de la llamada Nueva Economía.

Por fin en abril del 2002 y luego de largas discusiones los honorables diputados por fin aprobaron el texto definitivo de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, y en consecuencia las reformas al Código Penal que daban la luz a los llamados Delitos Informáticos.

Hechos y situaciones que perjudicaron al país

Los hackers que se identifican como Anonymous Iberoamérica han publicado información de la Coorporación Nacional de Telecomunicaciones (CNT), de varios

trabajadores del Aeropuerto de Quito, entre otros. A esto lo denominan "sorpresas" y para miércoles se deben esperar más a lo largo del día, según han informado vía Twitter.

La "Sorpresa # 4" La página web de la empresa Hunter para Ecuador (http://www.hunter.com.ec/) mostraba en su página principal una imagen de personas enmascaradas en un metro y tenía la leyenda "Somos Anonymous".

A la imagen la acompañaba el texto que comenzaba con un "Somos Anonymous y estamos con ustedes pueblo ecuatoriano", que continuaba dirigiéndose directamente al Presidente del Ecuador apuntando que los esfuerzos con Corea del Sur para identificarlos serían inútiles.

Terminaban con el conocido lema "Somos Anonymous, somos legión, no perdonamos, no olvidamos, esperadnos", pero lo firmaban Colombianhackers, dando a entender que este ataque había sido realizado con su apoyo. Esto se confirmó con el tweet de Anonymous Iberoamérica (o Anonymous Hispano) que establecían que el ataque llegaba "patrocinado" por los piratas colombianos.

La "Sorpresa # 3" Se publicó varios links que, supuestamente, llevarían al panel de control del sistema de videoconferencia del Ministerio de Medio Ambiente.

"De hecho esa no era la sorpresa 3 originalmente, pero la web de la sorpresa 3 está offline, cuando se levante se las damos", publicaron los hackers en Twitter.

La "Sorpresa #2" fue la revelación de datos personales de varias personas que trabajan en el Aeropuerto de Quito. Los nombres, apellidos, correos electrónicos, cargo, teléfonos, números de cédula y usuarios fueron publicados en un boletín de pastebin.com

Asimismo, la "Sorpresa # 1" fue la publicación del diagrama físico de la red de servidores de CNT utilizando la página pastebin.com publicaron un link con el diagrama de los servidores.

Páginas gubernamentales saturadas

Las principales páginas saturadas fueron de la Presidencia, el Ministerio de Telecomunicaciones, Vicepresidencia y de la Alcaldía de Quito que se vieron fuera de

servicio a las 10:00 coincidiendo con el inicio del informe del Presidente Rafael Correa a la Nación y del ataque masivo de los hackers que se denominan Anonymous Iberoamérica.

El servicio de la página de la Presidencia y la de Telecomunicaciones fueron reactivadas rápidamente y las de la Alcaldía de la capital y Vicepresidencia tardaron más tiempo en volver a su funcionamiento normal.

En el momento de la caída, en la web oficial de la Presidencia se podía ver un mensaje que informaba que el sitio estaba teniendo problemas de mantenimiento.

Ante la alarma de un ataque a la web el equipo de la Presidencia por medio de Twitter (@Presidencia_EC) manifestó: **"Casi 10 mil usuarios saturaron la pág. web de la Presidencia, por lo que debió ser ampliada su capacidad. No ha sido hacheada".**

1.2 Diagnóstico o planteamiento de la problemática general

1.2.1 Causa – efectos

La gran pérdida de información mediante la infiltración de intrusos, hacen que las empresas inviertan de manera inadecuada en dispositivos y aplicaciones de seguridad que no brinda ninguna seguridad a la información, lo cual hace que el presupuesto plantado para la empresa sobrepasa sus expectativas.

Las autoridades intentan diferenciar dentro de redes como internet, a servidores con información pública y servidores con información clasificada, estos con severas restricciones de acceso.

1.2.2 Efectos:

La falta de implementación de un sistema de seguridad, producirá a las empresas ser un blanco fácil de infiltración de los hackers, lo cual podría llevarla a la quiebra.

Los hackers buscan fama y renombre perforando estas barreras. Cuestionan a la autoridad y demuestran ser poseedores de conocimiento y tecnología, de hecho tienen varias aplicaciones desarrolladas por ellos mismo para hachear información privada.

1.3 Pronóstico y control del pronóstico

1.3.1 Pronostico

Hoy en día, las cosas han cambiado y sobre todo en las organizaciones que manejan grandes cantidades de información valiosa como dinero o datos personales de usuarios

importantes: el objetivo más común en todos los programas maliciosos es el robo de información. Hoy en día, la información equivale a dinero y, afortunadamente para los criminales, la red está rebosante de datos e información de todo tipo.

Cuando una organización pública o privada es víctima de un ataque, el criminal puede utilizar la información que encuentra como más le convenga. Así, puede por ejemplo robar la personalidad de la víctima y cometer delitos en su nombre, puede robarle dinero de sus cuentas o puede vender sus datos personales a empresas especializadas en Spam. Por supuesto, supone también una forma de tener acceso libre a la lista de contactos de la víctima etc.

1.3.2 Control del pronóstico

Para poder proteger nuestra información, existen muchas alternativas de seguridad de información, ya sea mediante aplicaciones diseñadas contra ataque de intruso maligno o mediante políticas de seguridad estructuradas que establezca la empresa hacia el personal que labora en la misma.

Los auditores o administradores de seguridad deberán evaluar la correcta organización y administración del área de sistemas (Centro de Procesamiento de Datos), así como la asignación de tareas y responsabilidades del personal que la conforma; a fin de que ésta brinde condiciones óptimas de operación que posibiliten un ambiente adecuado de control y permitan mejorar la disponibilidad

1.4 Formulación de la problemática específica

1.4.1 Problema principal

¿Podrá un sistema de seguridad informática, evadir la infiltración de intrusos (HACKERS) que navegan a través de la Web, con intensiones de perjudicar la información de una entidad?.

1.4.2 Problemas secundarios

¿Mediante un estudio, se podrá asegurar que dichas aplicaciones nos garantizara la seguridad de la información?

¿Cómo se podría proteger la información de la empresa y de los usuarios contra la amenaza de los hackers?

¿Las organizaciones están preparadas para poder controlar el ataque de programas maliciosos creados por los hackers?

¿Deberían las empresas establecer políticas de seguridad informática para evitar perdida de su información?

1.5 Objetivos

1.5.1 Objetivo General

Proponer medidas básicas de seguridad informática en las empresas, para mantener la integridad, Disponibilidad, Privacidad, Control y Autenticidad de la información, contra la ingeniería social.

1.5.2 Objetivos Específicos

1.5.3 Específicos:

Describir los delitos informáticos que tiene mayor incidencia en la seguridad informática.

Como proteger la información contra la infiltración de los hackers.

Programas maliciosos: consecuencias y tipos.

Establecer políticas de seguridad informática.

1.6 Justificación

1.6.1 Teórica

En la actualidad muchas entidades públicas o privadas están expuestas a que la información sea blanco fácil de individuos con altos conocimientos informáticos que navegan atreves de la red, con aplicaciones especialmente diseñadas para romper cualquier tipo de seguridad y poder así extraer la información, ya sean con fines lucrativos o por el simple hecho de perjudicar a una entidad.

1.6.2 Metodológica

Uno de los principales problemas sociales que aqueja a las empresas que manejan información muy valiosa, es la seguridad, se propone cambiar este ambiente de vulnerabilidad de información, adaptando a las entidades con la más alta de las tecnologías de seguridad de información, el mismo que tendrá la capacidad de detectar las amenazas que provienes de los intrusos externos o internos.

1.6.3 Práctica

La solución que se propone es controlar los ataques que los intrusos (HACKERS) pretenden realizar, mediante dispositivos y aplicaciones de seguridad que nos ayudara a nuestra información no sea de fácil vulnerabilidad.

1.6.4 Metodología.

Para la realización del presente proyecto investigativo hemos decidido utilizar los siguientes métodos de Investigación:

1.7 Alcance y Limitaciones

1.7.1 Alcance

Para la elaboración de este proyecto es necesario delimitar la solución a realizar.

- Se realizara un estudio sobre la seguridad informática, y de las herramientas que nos permita interactuar al usuario con el proceso de controlar las vulnerabilidades que se presentan en las empresas, a través de las amenazas de los hackers.
- La herramienta o software nos permitirá interactuar con el usuario y poder controlar los accesos no permitidos hacia la información de las empresas.
- Se desarrollara un manual de usuario para la correcta utilización de la herramienta Nessus.

1.7.2 Limitaciones

- No se incluirá la implementación de la aplicación mencionada en una empresa.

1.8 Estudio de la factibilidad de la herramienta de Seguridad Nessus

1.8.1 Factibilidad Operativa

El sistema de seguridad informática **Nessus** tendrá las siguientes ventajas:

- Velocidad de respuesta inmediata mientras va detectando puertos abiertos.
- Velocidad en los escaneos a realizarse.
- Optimización del tiempo.
- Seguridad confiable en el ingreso al sistema.
- Control contra la detección de hackers
- Verificación del nivel de riesgo (baja, media, alta) al ahora de detectar alguna amenaza.

1.8.2 Factibilidad Técnica

La Factibilidad Técnica consiste en realizar una evaluación de la tecnología existente dependiendo de las diferentes tipos de organizaciones, este estudio estuvo destinado a obtener información sobre los componentes técnicos que deberán poseer las organizaciones y la posibilidad de hacer uso de los mismos en el desarrollo e implementación de un sistema de seguridad propuesto y de ser necesario, los requerimientos tecnológicos que deben tener adquiridos para el desarrollo y puesta en marcha del sistema en cuestión.

De acuerdo a la tecnología necesaria para la implantación del Sistema de Seguridad Informática se evaluó bajo dos parámetros: **Hardware y Software.**

Hardware

En cuanto a Hardware, específicamente el servidor donde debe estar instalado el sistema de seguridad informática, este debe cumplir con los siguientes requerimientos mínimos:

Procesador Pentium(R) 4 2.80Mhz. (Como mínimo)

1 GB de Memoria RAM (como mínimo)

Disco Duro de 160 GB.
Unidad de DVD-ROM
Tarjeta de Red.
Tarjeta de Vídeo.
Unidad de Protección UPS.
Cableado estructurado
Conexiones inalámbricas

Software.

En cuanto al software, las Organizaciones deben cumplir con todas las aplicaciones y funcionamiento del sistema de seguridad, lo cual amerita inversión alguna para la adquisición de los mismos. Las estaciones de trabajo y los servidores, operaran bajo diferentes ambientes de sistemas operativos como son: Windows, Linux, Solaris, Mac, etc. Para el uso general de las estaciones en actividades diversas se debe poseer las herramientas de escritorio y los navegadores que existen en el mercado actualmente y conexiones remotas.

Sistemas Operativos

Windows XP, Server 2003, Server 2008, Server 2008 R2, Vista and 7 (i386 and x86-64)
Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (i386 and x86-64)
Mac OS X 10.4, 10.5 and 10.6 (i386, x86-64, ppc)
Diversos antivirus
Browser o Navegador Internet Explorer Mozilla Firefox, etc.

1.8.3 Factibilidad Económica:

Análisis Costo Beneficio:

En este análisis permitió hacer una comparación entre la relación que podría costar a las organizaciones al momento de implementar el sistema de seguridad NESSUS en la versión de paga, ya que también existe la versión gratuita (Libre), pero esta a su vez posee varias contras ya que no consta con todos los pulgins de escaneo para su respectiva ejecución y no es muy recomendable para las grandes organizaciones como pueden ser los bancos, entidades gubernamentales o de gobierno, etc.

INVERSION			
Nombre Equipo	**Justificación uso en proyecto**	**No. Unidad**	**Costo mensual**
Computadores	Para acceso a Internet y la red	2 como mínimo (depende)	$800
Herramienta de seguridad Nessus	Protección y control	1	$1500
Soporte técnico y actualizaciones	Mantener actualizado la herramienta		$100
Capacitación y asesoría	Mantener capacitado al personal de seguridad		$500
Total gastos de inversión			**$2250**

Tabla1.1Costo del sistema Nessus propietario para su implementación

Esta tabla nos indica los valores estimados de cuánto podría llegar a costar la implementación de un sistema de seguridad informática Nessus con licencia, como se menciona anteriormente también existe l aversión gratuita que se puede descargar de la página oficial de Nessus *www.tenable.com/.../**nessus**/**nessus**-download-agr.*

1.9 Metodología de Trabajo

A continuación se detallará la metodología de desarrollo para llevar a cabo el proyecto planteado.

La entrevista.- Será aplicada hacia las personas en cargadas de la seguridad en la empresa, como al personal encargado de manejar la información, para poder obtener información concreta y exacta de los problemas que se está dando dentro de la misma.

Técnica de Observación.- La cual consistirá en observar atentamente el funcionamiento del sistema, tomar información y registrarla para su posterior análisis.

Técnica de Observación Científica.- Significa observar con un objetivo claro, definido y preciso, para saber específicamente cuales son los problemas que se están dando a la hora de proteger la información de las empresas, y así poder analizar cuidadosamente la solución que se pretende dar.

Posibles Preguntas: (Ficticias)

¿Cuál es la preocupación con respecto a la seguridad informática de su empresa, sobre todo comparándola con otros países del mundo en los que también está presente?

A comparación de otros países, la tecnología en el Ecuador poco actual, y las infiltraciones son más concurrentes, y se llega a una gran pérdida de información.

¿Qué sistema de seguridad posee actualmente su empresa?

No se posee en la actualidad un sistema de protección de información

En un momento en el que su empresa está despidiendo empleados de forma masiva, ¿cuáles son sus perspectivas en este campo? ¿Pueden asegurarse que la información no ha sido substraída con anterioridad?

No existe un plan de seguridad para la protección de la información, y no se puede asegurar en su totalidad que la información ha sido substraída.

CAPITULO II

2 MARCO TEORICO

2.1 MARCO DE REFERENCIA

Grafico 2.1 Proceso de Seguridad Informática en las Organizaciones

2.2 MARCO TEORICO

2.2.1 FUNDAMENTOS TEORICOS DE LA INVESTIGACION

2.2.2La seguridad informática

2.2.3Definición

Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore y signifique un riesgo si ésta llega a manos de otras personas mal intencionadas. Este tipo de información se conoce como información privilegiada, confidencial o valiosa.

2.2.4 Elementos de la Seguridad Informática:

Integridad:

Los componentes del sistema permanecen inalterados a menos que sean modificados por los usuarios autorizados. Uno de los problemas principales de la integridad puede ser por daños propios de hardware, software, virus o por la manipulación de personas no autorizadas.

Disponibilidad

Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

Privacidad:

Los componentes del sistema son accesibles sólo por los usuarios autorizados.

Si la privacidad falta dentro de la organización, la información puede producir perdidas a las altas autoridades de la misma.

Control

Solo los usuarios autorizados deciden cuando y como permitir el acceso a la información.

Autenticidad

Definir que la información requerida es válida y utilizable en tiempo, forma y distribución.

Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

No Repudio

Evita que cualquier entidad que envió o recibió información alegue, que no lo hizo.

Auditoria

Determinar qué, cuándo, cómo y quién realiza acciones sobre el sistema.

2.3 Seguridad física

Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información.

2.3.1 Amenazas:

Incendios
Inundaciones
Terremotos
Trabajos no ergo métricos
Instalaciones eléctricas
Estática
Subministro ininterrumpido de corriente
Cableado defectuoso
Seguridad de equipamiento

2.3.2 Controles

Sistemas de alarmas
Control de personas
Control de vehículos
Barreras infrarrojas-ultrasónicas
Control de hardware
Controles biométricos
Huellas digital
Control de voz
Patrones oculares
Verificación de firmas

2.4 Seguridad lógica

La Seguridad Lógica se trata de aplicaciones, barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlos.

Los objetivos que se plantean son:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

2.4.1Control de acceso:

Los controles son implementados en los sistemas operativos, y a su vez son implementados en las aplicaciones, en las base de datos o en algún paquete especifico de seguridad.

Identificación: El usuario se da a conocer al sistema, y este a su vez le informa mediante un mensaje, si tiene permiso para acceder al mismo o lo rechaza.

Autentificación: Verificación del sistema ante la identificación.

Formas de Autentificación - Verificación

Password: Contraseña o clave (en español) es una forma de autentificación que se utiliza para acceder hacia algún recurso de la información secreta para poder tener el control total del mismo. Caso contrario si no conoce la contraseña se le negara el acceso al recurso.

Huella digital: Se trata identificar de manera única a un individuo por medio biométrico. Certificando la autenticidad de las personas de manera única e inconfundible por medio de un dispositivo electrónico que captura la huella digital y de un programa que realiza la verificación.

Firma digital: Puede ser almacenada en un contenedor electrónico, tanto en soportes de hardware como de software.

Tokencard: Es un mecanismo de la tarjeta de token de seguridad incorporado está en sincronía con el servidor back-end, con el que será el código de autorización generado por la tarjeta ficha verificada.
Cada ficha tiene un número de serie único que forma parte de la clave de cifrado para el uso de la generación dinámica de códigos de acceso a la red que cambian cada vez que el cliente necesita para conectarse a la aplicación.

2.5 Amenazas a la seguridad de la información

Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Principalmente se debe proteger los datos, se pueden realizar multitud de ataques o, ya que están expuestos a diferentes amenazas ya sean estos internos o externos.

La clasificación de estas amenazas se divide en cuatro grupos:

Interrupción: Se trata cuando un objeto del sistema se pierde quede inservible o no disponible.

Interceptación: Cuando un elemento del sistema no autorizado consigue un acceso a un objeto del sistema.

Modificación: Cuando un elemento del sistema además de conseguir el acceso logra modificar el objeto.

Fabricación: Cuando una modificación logra conseguir un objeto igual o similar de manera que sea poco probable distinguir del objeto original. [1][2]

[1] http://securityfocus.com
[2] www.securityportal.com.ar

Matriz de análisis de riesgo y su impacto en las Empresas

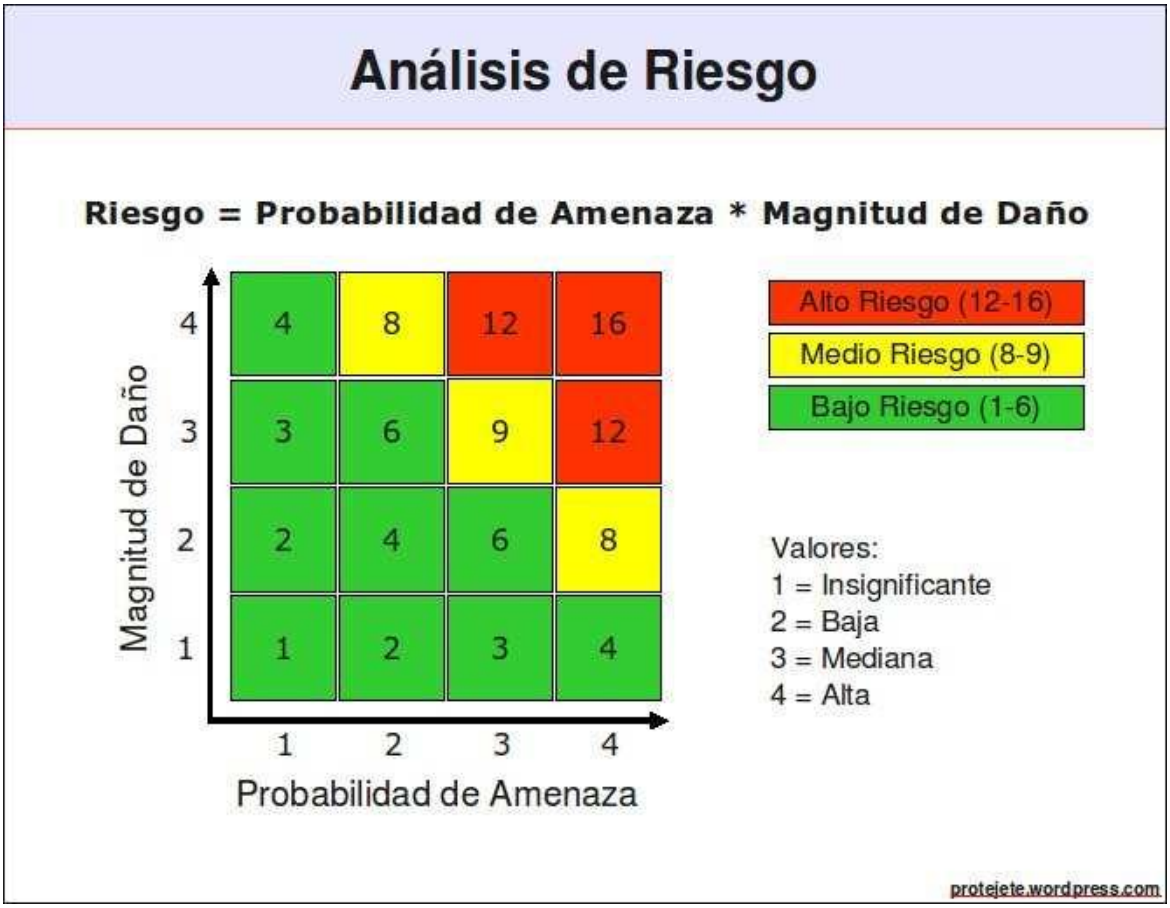


Grafico 2.2 Análisis de riesgo Fuente estriada: protegetwordpress.com

Existen varios métodos de como valorar un riesgo y al final, todos tienen los mismos retos las variables son difíciles de precisar y en su mayoría son estimaciones y llegan casi a los mismos resultados y conclusiones.

En el ámbito de la Seguridad Informática, el método más usado es el Análisis de Riesgo.

Riesgo = Probabilidad de Amenaza x Magnitud de Daño

Para la presentación del resultado (riesgo) se usa una gráfica de dos dimensiones, en la cual, el eje-x (horizontal, abscisa) representa la "Probabilidad de Amenaza" y el eje-y (vertical, ordenada) la "Magnitud de Daño". La Probabilidad de Amenaza y Magnitud de Daño pueden tomar condiciones entre Insignificante (1) y Alta (4). En la práctica no es necesario asociar valores aritméticos a las condiciones de las variables, sin embargo facilita el uso de herramientas técnicas como hojas de cálculo.

Matriz de Análisis de Riesgo		Probabilidad de Amenaza					
Elementos de Información	Magnitud de Daño	Criminalidad		Sucesos físicos		Negligencia	
		Robo	Virus	Incendio	Falta de Corriente	Compartir contraseñas	No cifrar datos críticos
		3	4	2	3	4	3
Datos e Información							
RR.HH	3	9	12	6	9	12	9
Finanzas	4	12	16	8	12	16	12
Sistema e Información							
Computadoras	2	6	8	4	6	8	6
Portátiles	3	9	12	6	9	12	9
Personal							
Coordinador	4	12	16	8	12	16	12
Personal técnico	3	9	12	6	9	12	9

Grafico2.3 Matriz de análisis de riegos y sus probabilidades de amenazas

Dependiendo del color de cada celda, podemos sacar conclusiones no solo sobre el nivel de riesgo que corre cada elemento de información de sufrir un daño significativo, causado por una amenaza, sino también sobre las medidas de protección necesarias

- Proteger los datos de RR.HH de las organizaciones, Finanzas contra virus o hackers
- Proteger los datos de Finanzas y el Coordinador contra robo o sabotaje
- Evitar que se compartan las contraseñas de los portátiles
- Etc, etc.

- Proteger el Personal (Coordinador y Personal técnico) contra Virus de computación
- Evitar la falta de corriente para el Coordinador
- Etc, etc.

2.5.1 Áreas de negocio o sectores donde se aplican estas soluciones

- Empresas bancarias

- Empresas de logística, distribución o reparto de productos.

- Empresas con necesidades de control de stock y gestión de almacenes.
- Empresas encuestadoras
- Empresas Industriales
- Cooperativas Supermercado
- Empresas Comerciales
- Empresas de Servicios
- Empresa publicas

2.5.2 Ventajas de tener una aplicación de seguridad informática en las empresas

- Aumento de la Productividad
- Información al instante, resolución de problemas en el acto
- Aumento de eficiencia
- Información sin errores
- Tecnología Disponible en el mercado
- Rápido recupero de la inversión
- Mejora de la atención al cliente y confianza de los mismos

2.6 MARCO CONCEPTUAL

Gráfico 2.4 – Amenazas para la Seguridad

En la seguridad informática podemos clasificar en grupos de posibles amenazas que pueden atacar a los sistemas de información.

Amenazas humanas (Personas)

La mayoría de ataques a nuestro sistema provienen en última instancia de personas que, intencionada o bienintencionadamente, pueden causarnos enormes pérdidas.

Aquí se listan los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas.

Personal: Fisgonea los sistemas y no destruyen los datos de la organización dependiendo de la situación concreta.

Ex-empleados: Realizan ataques con intenciones de perjudicar a la organización ya sea de manera intencional por algún tipo de venganza contra la misma.

Hackers: Es aquella persona con altos conocimientos informáticos y curiosa, inconformista que busca la manera de aprovecharse de las facilidades que los sistemas brindan para su infiltración.

Crackers: Son aquellas personas con intenciones dañinas.

Pheaker: Personajes que engañas a las compañías telefónicas para su beneficio propio.

Creador de virus – Diseminadores de virus

Insider: Aquellas personas que trabajan internamente en una organización que amenazan de cualquier forma al sistema de las misma.

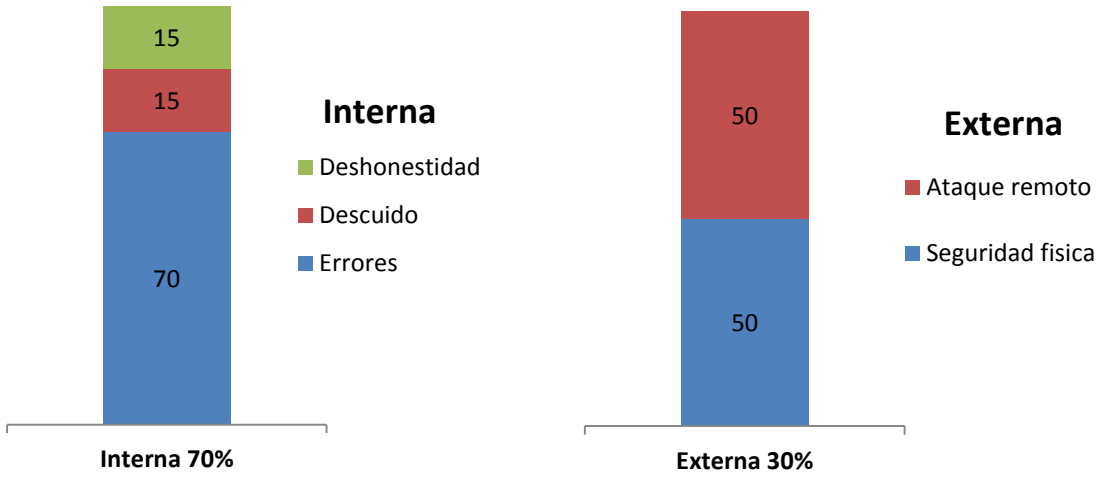


Grafico 2.5 Intrusión y Amenazas

Como podemos observar en el grafico 1.2, las amenazas más frecuentes que se dan en las organizaciones son las internas con un porcentaje del 70% y dentro de ellas se divide en un porcentajes del 70% de errores y el 15% en descuido y deshonestidad.

Mientras que las externas son solo del 30% en intrusión y amenazas, y están divididas el 50% en ataques remotos y el otro 50% en seguridad física, lo cual nos concluye que debemos tener más precaución en la seguridad interna de la organización.

Amenazas lógicas:

En las amenazas lógicas nos encontramos con todo tipo de programas que pueden dañar a nuestro sistema operativo, que son creados de manera mal intencionado por hackers o crackers, software malicioso conocido como MALWARE o programas creados por error GUGS o AGUJEROS.

Software incorrecto. Las amenazas más habituales a un sistema provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones.

Herramientas de Seguridad. Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar [3]fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.

Ingeniería Social: Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos llevándolos a revelar información sensible, o bien a violar las políticas de seguridad típicas.

Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos. Generalmente se está de acuerdo en que "los usuarios son el eslabón débil" en seguridad; éste es el principio por el que se rige la ingeniería social.

Puertas traseras. Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar "atajos". A estos atajos se les denomina puertas traseras. Algunos programadores pueden dejar estos atajos en las versiones definitivas de su software; la cuestión es que si un atacante descubre una de estas puertas traseras (no nos importa el método que utilice para hacerlo) va a tener un acceso global a datos que no debería poder leer.

Bombas lógicas. Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas. Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos ficheros, la llegada de una fecha concreta; cuando la bomba se activa va a poder realizar cualquier tarea que pueda realizar la persona, los efectos pueden ser fatales.

Virus. Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

[3] http://windsofthesky.wordpress.com/2008/07/11/tipos-de-amenazas-informaticas/

Gusanos. Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que conecta para dañarlos.

Caballos de Troya. Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas sin el conocimiento del usuario.

Entre otros que también son de mucho cuidado

Ingeniería Social Inversa
Trashing (Cartonero)
Ataques de Monitorización
Ataques de Autenticación
Denial of Service (DoS)
Ataques de Modificación - Daño
Catástrofes
Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales: simplemente por su ubicación geográfica, a nadie se le escapa que la probabilidad de sufrir un terremoto o una inundación que afecte a los sistemas informáticos en una gran ciudad, es relativamente baja, al menos en comparación con el riesgo de sufrir un intento de acceso por parte de un pirata o una infección por virus. Sin embargo, el hecho de que las catástrofes sean amenazas poco probables no implica que contra ellas no se tomen unas medidas básicas, ya que sí se produjeran generarían los mayores daños.

2.6.1 Herramientas de seguridad

2.6.2 Herramientas de seguridad para la seguridad en las empresas

Security Scanners

Dentro de éste grupo nos encontramos con las siguientes herramientas: **Nessus, Nmap, SATAN, Whisker, Saint, Santa y SARA**

2.6.3 NESSUS

Proporciona a la comunidad de Internet un escáner de seguridad remoto de la red, de gran alcance y fácil de usar. Permite realizar auditorías remotas de una red dada y determinar si algún intruso ha logrado acceder al sistema, si hay bugs en el software, si hay puertas traseras...

Al contrario que otros escáners de seguridad, Nessus no da nada por sentado. Es decir, no considera que un servicio determinado corra en un puerto fijo. Por ejemplo, si nuestro servidor web corre en el puerto 1234, Nessus lo detectará y lo testeará. Nessus no realiza su test conforme a la versión de los servicios remotos, sino que intenta explotar todas las vulnerabilidades.

Una característica de Nessus es que es capaz de proporcionar informes detallados y que a menudo sugieren una solución para las vulnerabilidades encontradas. Estos informes se pueden guardar como texto plano, HTML, HTML con gráficos... y permite realizar una comparativa entre dos escaneos diferentes.

Actualmente hay un producto basado en servicios de escaneo de puertos por línea que utiliza como motor de escaneo Nessus sin mencionarlo.

Corre en la mayoría de las plataformas. Interactúa con Nmap

Se ha recomendado el uso de Nessus para detectar vulnerabilidades de sistemas operativos mediante un escaneo incluyendo la posibilidad de mostrar en consola o gráficamente el progreso y el reporte del mismo. Los resultados de este escaneo pueden ser exportados en varios formatos: texto plano, XML, HTML y LaTeX; o bien guardados en una base de referencias para futuros escaneos del sistema.

Existe una larga lista de plugins para realizar las distintas pruebas de vulnerabilidad, además se permite la interacción personalizada en redes mediante el lenguaje NASL.

Las principales características y posibilidades de Nessus son:

- Proporcionar credenciales a Nessus permite determinar: falta de parches de seguridad y la configuración del sistema vulnerable, cumplimiento e incumplimiento de los parámetros de configuración y la presencia de los datos sensibles como números de seguro social o tarjeta de crédito.
- Cada escáner Nessus puede hacer uso de un dominio de Microsoft Windows, claves UNIX Secure Shell o SNMPv2.
- Escaneo rápido.
- Los escáneres Nessus pueden ser empleados para testear un rango de direcciones IP, DNS o direcciones MAC si las IP's son dinámicas.
- Tras las exploraciones se pueden detectar cambios en los distintos dispositivos.

Ventajas:

- Fácil de instalar, se ha reducido a la mínima expresión
- Interfaz limpia: Se debe reconocer que es agradable a la vista
- Se supone que tendremos los nuevos plugins más rápido que en el caso de OpenVAS
- Soporte por una única empresa

Desventajas:

- En el caso del HomeFeed (versión gratuita) tiene limitaciones bastante molestas. Por ejemplo, no podemos programar scans (se tienen que lanzar a mano) ni hacerlos de un rango demasiado amplio
- Si la interfaz es más simple, también implica que faltan algunas características como por ejemplo el escalado de eventos ni la posibilidad de crear filtros para evitar los falsos positivos
- El fallo de un plugin al identificar los emails como fueran open relays me parece un fallo bastante complejo.

2.6.4 NMAP

Nmap (‘Network Mapper’) en español mapeador de redes, es una herramienta open source, diseñada para explorar y para realizar auditorías de seguridad en una red de computadoras.

Esta herramienta cumple con en funcionamiento de realizar auditorías de seguridad en las redes, y también puede ser utilizado para objetivos delictivos, ya que reconoce puertos abiertos en los computadores conectados a una red, puede reconocer la infraestructura de la red y de cuantas maquinas están conectadas

Características

- Descubrimiento de servidores: Identifica computadoras en una red, por ejemplo listando aquellas que responden ping.
- Identifica puertos abiertos en una computadora objetivo.
- Determina qué servicios está ejecutando la misma.
- Determinar qué sistema operativo y versión utiliza dicha computadora, (esta técnica es también conocida como *fingerprinting*).
- Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

Aplicaciones típicas

Ha llegado a ser uno de las herramientas imprescindibles para todo administrador de sistema, y es usado para pruebas de penetración y tareas de seguridad informática en general.

Como muchas herramientas usadas en el campo de la seguridad informática, es también una herramienta muy utilizada para hacking.

Los administradores de sistema pueden utilizarlo para verificar la presencia de posibles aplicaciones no autorizadas ejecutándose en el servidor, así como los crackers pueden usarlo para descubrir objetivos potenciales.

Nmap permite hacer el inventario y el mantenimiento del inventario de computadores de una red. Se puede usar entonces para auditar la seguridad de una red, mediante la identificación de todo nuevo servidor que se conecte:

Nmap es a menudo confundido con herramientas para verificación de vulnerabilidades como Nessus. Nmap es difícilmente detectable, ha sido creado para evadir los Sistema de detección de intrusos (IDS) e interfiere lo menos posible con las operaciones normales de las redes y de las computadoras que son analizadas.

Ventajas:

Este programa incluso en sus versiones graficas es muy poderoso, y tiene opciones para realizar escaneos muy difícilmente detectables por las "victimas" o supervisores de red. Escanea cualquier rango de puertos que desees e incluso detecta el sistema operativo de la víctima, dando lugar a que el hacker identifique más claramente cómo puede acceder al equipo remoto.

Desventajas:

Entre más complejo sea el tipo de escaneo que se quiere realizar, el proceso de escaneo puede ser mas tardado y tardar varios minutos antes de finalizar, la velocidad del escaneo depende básicamente de 3 factores, velocidad de la computadora de quien escanea (hacker), latencia en la red (si la red es lenta o rápida), y velocidad de respuesta y medidas de seguridad de la computadora escaneada (victima)[4]

2.6.5 MANAGER PKI (PUBLIC KEY INFRASTRUCTURE)

La seguridad y la confianza son partes integrales de los negocios hoy en día.

[4] http://www.unamcert.unam.mx/herramientasSeguridad.html[4]

Hoy más que nunca, los negocios deben proteger sus recursos de ataque así como la implementación en medidas de seguridad en procesos administrativos, de personal, clientes y socios de negocios.

El managed PKI engloba los valores de:

- Autenticación.
- Autorización.
- Confidencialidad.
- Integridad.

El managed PKI es un servicio administrado, por lo tanto se puede implementar una solución PKI de una forma rápida, para englobar los componentes importantes de confianza. Actualmente el managed PKI da servicio a millones de negocios y usuarios a nivel internacional.

El managed PKI asegura sus:

- Aplicaciones.
- Comunicaciones.
- Transacciones.

De esta manera, asegurando estos tres conceptos, logra una infraestructura confiable entre uno y el mundo.

Debido a que la CA (Autoridad Certificadora), cumple con los parámetros de verificación y autenticación, todos los certificados emitidos por ésta son confiables, el Managed PKI permite comunicaciones y transacciones seguras entre uno y personas confiables, usando métodos de criptografía probados.

La empresa que hospeda y administra los CA´s es VeriSign, empresa reconocida mundialmente; esta se basa en su experiencia e infraestructura de seguridad, bajo los estándares más estrictos:

- Centro de datos de alta disponibilidad.

- Escalables a millones de usuarios.
- Servicio al Cliente las 24 horas del día.
- Infraestructura de alta seguridad.
- Controles internos auditables.
- Cuenta con los mejores expertos de seguridad en la industria.

Todos estos respaldados por los mejores Acuerdos de Servicio en la Industria, para que uno desarrollé sus requerimientos legales y de seguridad.

Dependiendo de las políticas de confianza de la empresa, VeriSign hospedará CA´s privadas o públicas. Las privadas permiten que el usuario personalice sus propias políticas confianza, mientras que las públicas se convierten, de forma inmediata, en parte de la Red de Confianza de Verisign (VTN).

Cuando un usuario pertenece a la Red de Confianza de Verisign, inmediatamente puede acceder a millones de usuarios confiables, sin tener que establecer su propia comunidad de confianza.

El servicio de Managed PKI permite que el usuario obtenga certificados digitales firmados por una Autoridad Autenticadota hospedada por Verisign, aprovechando las capacidades de infraestructura, confianza y seguridad que brinda esta, para que el usuario pueda enfocarse solamente a su negocio.

Funcionamiento de Managed PKI:

Por ejemplo si un nuevo usuario intenta acceder a una aplicación segura en un servidor empresarial, su acceso será denegado si éste no cuenta con el certificado digital correspondiente. Para que pueda acceder al servidor seguro, el usuario será diseccionado a un servidor de inscripción para obtener su certificado digital, que será hospedado en Verisign o en la empresa.

Cuando el usuario navega en la página de inscripción, llena un formato personalizado para solicitar su certificado digital, y lo manda al servidor de inscripción.

La petición de certificado será guardada para una aprobación manual, o se mandará a un servidor de autenticación, el cual la aprueba o la rechaza en base a la información

personal proporcionada en la inscripción. Si se aprueba la petición Verisign genera un certificado firmado digitalmente por una Autoridad Certificadora, y es mandado directamente al usuario. El acceso a la aplicación segura es concedido en base al nuevo certificado digital del usuario y a la llave privada correspondiente, y el usuario podrá acceder a la aplicación segura por el tiempo en que el certificado digital sea válido.

El servicio administrado Managed PKI puede soportar las aplicaciones de seguridad más fuertes del mercado, tales como:

- Banca Electrónica.
- Comercio Electrónico.
- Administración de Proveedores.
- Servicios Médicos.
- Gobierno.

2.6.6 APPSCAN DE

AppScan DE brinde una solución para automatizar los análisis de vulnerabilidades y pruebas de penetración de sus aplicaciones y plataformas Web.

Elimina los exámenes manuales que eran necesarios antes de implementar una aplicación, genera reportes que determinan la mejor manera de cumplir con estas auditorías para asegurar sus aplicaciones, antes de su implementación.

AppScan DE es una poderosa herramienta de pruebas que permite el rápido desarrollo de la seguridad. Esta herramienta ayuda a hacer que la lógica de la aplicación sea resistente a ataques sin tocar su presentación o eficacia. AppScan DE detecta los defectos de la seguridad automáticamente; como un componente integrado al desarrollo de la empresa,

esta herramienta, automatiza las pruebas de creación de escritura, modificación y proceso de mantenimiento, asegurando confiabilidad y pruebas que son repetibles.

AppScan DE es una herramienta que ayuda a las empresas a reducir costos y a crear aplicaciones confiables y resistentes contra hackers, en el ambiente de desarrollo.

AppScan DE crea "Vulnerabilidades Potenciales" que son los defectos potenciales de la seguridad en el código y entonces los prueba para verificar que ellos existen.

AppScan DE reporta los errores o defectos de la aplicación, luego se los proporciona al usuario para empezar a arreglar estos errores.

Después de estas breves descripciones de estos dos sistemas, podemos decir que las dos son muy buenas opciones para asegurar las Aplicaciones Web del CENTIA. Sin embargo, considero que AppScan DE es una opción mejor que el Managed PKI porque se enfoca más a descubrir cuáles son las vulnerabilidades potenciales que tienen las Aplicaciones Web, y es ahí, donde los hackers pueden atacar el sistema. Como observamos, Manager PKI asegura las Aplicaciones creando certificados digitales, pero no sabe cuáles son las vulnerabilidades del sistema; si un hacker encuentra estas vulnerabilidades puede ser un gran problema para la empresa, o bien, si emplea cualquier técnica de hackers avanzadas para penetrar al sitio, rompiendo el esquema del certificado digital, sería un caos total.

AppScan realiza pruebas para detectar vulnerabilidades en las aplicaciones Web más comunes, como Cross-Site Scripting, desbordamiento del almacenamiento intermedio y exploraciones de riesgos de nuevas aplicaciones flash/flex y Web 2.0.

Entre las características más resaltantes están:

Permite probar más de 40 regulaciones de la industria y estándares.
Señalamiento de código HTML que contenga vulnerabilidades y adicionalmente realiza una explicación de los mismos.
Realiza reportes correctivos.
Posee la habilidad de incorporar "screen shots" del explorador interno de Rational AppScan en los reportes.
Cubre la validación de asuntos basados en las pruebas de Secure Sockets Layer (SSL) y cross-site request forgery (CSRF).
Realiza simulaciones de hackers.

Posee la información de los últimos tipos de ataques y se actualiza automáticamente.
Soporte para las tecnologías Web 2.0 más recientes: incluye el análisis y la ejecución de aplicaciones JavaScript y Adobe Flash; un conocimiento profundo de protocolos relacionados con AJAX y Adobe Flex, como JSON, AMF y SOAP, y un soporte global para entornos SOA complejos, así como configuración e informes personalizados para aplicaciones de Mashup y basadas en procesos.
Resultados de la exploración simplificados gracias a un asistente experto en resultados: proporciona las recomendaciones avanzadas de correcciones necesarias para solucionar los problemas que hayan surgido durante la inspección.

Sniffers

Los sniffers existentes en el mercado de software libre son varios, entre ellos podríamos destacar: Ethereal, dSniff, SSLDump

2.6.7 ETHEREAL

Es uno de los mejores sniffers.
Tiene una potente gestión de filtros, análisis de protocolos y reconstrucción de sesiones, todo ello bajo interfaz gráfico aunque inicialmente fue desarrollado para Linux, se ha portado también a otros sistemas operativos como Windows y Solaris Permite examinar datos directamente de la red o a partir de ficheros capturados.

Aspectos importantes de Ethereal

- Mantenido bajo la licencia GPL.
- Trabaja tanto en modo promiscuo como en modo no promiscuo.
- Puede capturar datos de la red o leer datos almacenados en un archivo (de una captura previa).
- Basado en la librería pcap.
- Tiene una interfaz muy flexible.

- Gran capacidad de filtrado.
- Admite el formato estándar de archivos tcpdump.
- Reconstrucción de sesiones TCP
- Se ejecuta en más de 20 plataformas.
- Es compatible con más de 480 protocolos.
- Puede leer archivos de captura de más de 20 productos.

Seguridad

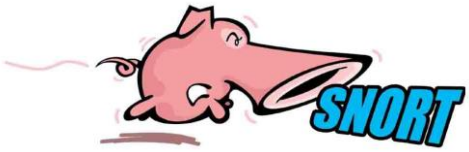
Para capturar paquetes directamente de la interfaz de red, generalmente se necesitan permisos de ejecución especiales. Es por esta razón que Wireshark es ejecutado con permisos de Superusuario. Tomando en cuenta la gran cantidad de analizadores de protocolo que posee, los cuales son ejecutados cuando un paquete llega a la interfaz, el riesgo de un error en el código del analizador podría poner en riesgo la seguridad del sistema (como por ejemplo permitir la ejecución de código externo). Por ésta razón el equipo de desarrolladores de OpenBSD decidió quitar Ethereal antes del lanzamiento de la versión 3.6.

Una alternativa es ejecutar tcpdump o dumpcap que viene en la distribución de Wireshark en modo Superusuario, para capturar los paquetes desde la interfaz de red y almacenarlos en el disco, para después analizarlos ejecutando Wireshark con menores privilegios y leyendo el archivo con los paquetes para su posterior análisis.

Detección de Intrusos

Dentro de este grupo podemos englobar a los siguientes productos: Snort, Shadow y Tripwire.

2.6.8 SNORT



Es un sistema de detección de intrusos capaz de realizar un análisis del tráfico en tiempo real en redes IP.

Puede realizar análisis de protocolos, y se puede usar para detectar distintos tipos de ataque, buffer overflows, escaneo de puertos, ataques al CGI, detección del sistema operativo...

Usa reglas sencillas para describir el tráfico que se puede dejar pasar y el que no.

Y tiene la capacidad de alertar en tiempo real ante cualquier ataque

Se puede usar en tres modos: sniffer de paquetes, el cual lee los paquetes que atraviesan la red y los muestra por consola, packet logger, que al igual que el otro modo lee los paquetes pero los almacena en un fichero, y detección de intrusos

Lo soportan la mayoría de las plataformas.

Características de Snort:

Imposición y chequeo de políticas

Monitor de Honeypot

Honeypots son "deception systems" que permiten analizar el comportamiento de intrusos en el sistema

Trampas y detección de mapeos de puertos

Análisis de tráfico en tiempo real

Detección de nuevos eventos a través de la escritura de reglas; SQL/ODBC, ActiveX, Java/Java Script, Virus de macros, cadenas de HTTP...[5] **[[6]]**

Controlar y monitorizar el acceso a Internet puede detectar, en fases de recuperación, cómo se ha introducido el virus. (Wikipedia n.d)[2]

[5] http://www.maestrosdelweb.com/editorial/snort 2009-04-05

[6] http://www.unamcert.unam.mx/herramientas.html

2.7 LOS HACKERS.

Un Hacker es una persona que está siempre en una continua búsqueda de información con grandes habilidades informáticas, vive para aprender y todo para él es un reto, no existen barreras, y lucha por la difusión libre de información, distribución de software sin costo y la globalización de la comunicación.

El concepto de hacker, generalmente es confundido erróneamente con los mitos que existen acerca de este tema:

Un hacker es pirata. Esto no es así ya que los piratas comercian con la información que obtienen, entre otras cosas, y un verdadero hacker solo obtiene esa información para su uso personal.

Un hacker es el que entra en los sistemas ajenos y se dedica a destruir la información almacenada en ellos. El error consiste en que el que destruye información y sistemas ajenos, no es el hackers sino el Cracker.

2.7.1 Que es un Hacker

1. Un verdadero Hacker es curioso y paciente. Si no fuera así terminarían por hartarse en el intento de entrar en el mismo sistema una y otra vez, abandonando el objetivo.

2. Un verdadero Hacker no se mete en el sistema para borrarlo todo o para vender lo que consiga. Quiere aprender y satisfacer su curiosidad. Esa es la única finalidad de introducirse en el sistema. Buscan dentro de un lugar en el que nunca han estado, exploran todos los pequeños rincones de un mundo diferente del que ya conoce y se aburre.

3. Un Hacker es discreto, es decir que cuando entra en un sistema es para su propia satisfacción,

4. Un Hacker programa de forma entusiasta (incluso obsesiva), rápido y bien.

5. Un Hacker es experto en un programa en particular, o realiza trabajos utilizando plataformas de programación muy conocidas.

2.7.2 Origen de los hackers

Los hackers existen desde los años 60, es decir, desde antes de que existieran las computadoras personales. Por aquellas épocas eran personas que se encargaban de utilizar líneas telefónicas en forma ilegal. Actualmente, quienes violan redes telefónicas son apodados phreakers.

Uno de los primeros hackers de renombre fue John Draper, alias "Cap'nCrunch". En 1970, Draper descubrió que el silbato de juguete que se incluía en las cajas de la marca de cereales Cap'nCrunch coincidía exactamente con la frecuencia de la red telefónica de AT&T. Gracias a Draper, miles de personas comenzaron a hacer llamadas de larga distancia sin costo alguno.

Al poco tiempo la pasión por hackear líneas telefónicas se trasladó a los sistemas computacionales. Las grandes computadoras o mainframes han estado conectados entre sí desde los años 60, pero las computadoras personales, manejadas por individuos desde sus casas, empezaron a conectarse a finales de los años 70. De allí en más se comenzaron a popularizar los BulletinBoardSystems (BBS).

2.7.3 Generación de los hackers

Las generaciones de los hackers están clasificadas en tres tipos:

Los Phreakers son aquellos expertos en la materia, y a los cuales se les vincula especialmente con el crecimiento de los BBS (BulletinBoardSystems)

En la segunda generación aparecen los hackers expertos en la manipulación de los computadores personales, alrededor de los años 90 se hicieron muy conocidos en los hogares, y dejaron de ser utilizados solo por ingenieros o técnicos.

En la tercera generación aparecen los hackers de la era del Internet, lo cual se da por la popularidad de la red de redes, en el año de 1995. [7]

2.7.4 Hackers famosos:

Richard Matthew Stallman

Sus mayores logros como programador incluyen el editor de texto Emacs, el compilador GCC, y el depurador GDB, bajo la rúbrica del Proyecto GNU.

Pero su influencia es mayor por el establecimiento de un marco de referencia moral, político y legal para el movimiento del software libre, como una alternativa al desarrollo y distribución de software privativo. Es también inventor del concepto de Copyleft (aunque no del término), un método para licenciar software de tal forma que éste permanezca siempre libre y su uso y modificación siempre reviertan en la comunidad.

Kenneth Lane Thompson

Conocido como Ken Thompson, es un pionero en las ciencias de la computación. Trabajó con el lenguaje de programación B y el sistema operativo UNIX y Plan 9 para los laboratorios Bell. Se le adjudica a Thompson, junto a Dennis Ritchie, la creación de UNIX.

Eric Steven Raymond

También conocido como **ESR**, es el autor de La Catedral y el Bazar y el responsable actual del Jargon File (también conocido como The New Hacker´s Dictionary). Si bien con el Jargon File obtuvo fama como historiador de la cultura hacker, se convirtió después de 1997 en una figura líder en el Movimiento del Software Libre y el Código Abierto.

Kevin Mitnick

[7] **http://www.casadellibro.com/libro-defensa-contra-hackers-proteccion-de-informacion-privada-incluy-e-cd-rom/2900000759545**

Como hacker, su carrera comenzó a los 16 años cuando, obsesionado por las redes de ordenadores, rompió la seguridad del sistema administrativo de su colegio. Para Kevin, el quehacer diario en sus últimos diez años fue el explorar y "explotar "computadoras ajenas y sistemas telefónicos.

Los Escuadrones Mod Y Lod

En 1993, los Maestros de Decepción (Masters of Deception) fueron los primeros crackers en ser capturados gracias a la intervención de líneas telefónicas.

Tipos de gran fama por tener numerosas formas de evitar el pago de llamadas telefónicas de larga distancia, los MOD además podían escuchar conversaciones privadas e incluso crear enormes líneas multiconferencias que compartían con sus amigos. [8]

2.8 POLÍTICAS DE SEGURIDAD

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

2.8.1 Razones que impiden la aplicación de las políticas de seguridad informática

A pesar de que un gran número de organizaciones canalizan sus esfuerzos para definir directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan el éxito, ya que la primera barrera que se enfrenta es convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática.

Otros inconvenientes lo representan los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los Gerentes de Informática o los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: "más dinero para juguetes del Departamento de Sistemas".

[8] Mc Graw, Gill (2000). Los Hackers. II Congreso Mundial De La Informática.

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensitiva y por ende su imagen corporativa. Ante esta situación, los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que quienes toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la empresa.

Finalmente, es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la empresa, ellas deben responder a intereses y necesidades empresariales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la empresa.

2.8.2 Normatividad

Es el área responsable de la documentación de políticas, procedimientos y estándares de seguridad así como del cumplimiento con estándares internacionales y regulaciones que apliquen a la organización. Dado que debe interactuar de forma directa con otras áreas de seguridad y garantizar cumplimiento, es conveniente que no quede al mismo nivel que el resto de las áreas pero todas reportan al CISO (**Chief Information Security Officer) Oficial de seguridad de información**. Por esta razón se le suele ver como un área que asiste al CISO en las labores de cumplimiento.

Operaciones: Es el área a cargo de llevar a cabo las acciones congruentes con la estrategia definida por el CISO lograr los objetivos del área (en otras palabras, la "gente que está en la trinchera"). Entre sus responsabilidades se encuentran:

* Implementación, configuración y operación de los controles de seguridad informática (Firewalls, IPS/IDS, antimalware, etc.)
* Monitoreo de indicadores de controles de seguridad
* Primer nivel de respuesta ante incidentes (típicamente a través de acciones en los

controles de seguridad que operan)
* Soporte a usuarios
* Alta, baja y modificación de accesos a sistemas y aplicaciones
* Gestión de parches de seguridad informática (pruebas e instalación)

Supervisión: Es el área responsable de verificar el correcto funcionamiento de las medidas de seguridad así como del cumplimiento de las normas y leyes correspondientes (en otras palabras, brazo derecho del área de normatividad). Entre sus responsabilidades se encuentran:

*Evaluaciones de efectividad de controles
*Evaluaciones de cumplimiento con normas de seguridad
* Investigación de incidentes de seguridad y cómputo forense (2° nivel de respuesta ante incidentes)
* Atención de auditores y consultores de seguridad

2.8.3 Lineamientos de seguridad informática

En aplicaciones web es común encontrar fallas de seguridad. Entre las causas están: debilidades en las fuentes o en los programas de las que dependen, labores o procedimientos administrativos insuficientes, exceso de confianza de desarrolladores, administradores y usuarios. Algunos lineamientos son:

- Emplear aplicaciones de fuentes abiertas pues resultan auditables y sus desarrolladores no se confían en la seguridad por inobservabilidad.
- Preferir aplicaciones cuyos desarrolladores acudan a políticas de apertura total en cuanto a fallas de seguridad.
- Preferir aplicaciones y protocolos que empleen cifrado fuerte. Cifrar datos sensibles.
- Emplear aplicaciones que tengan bajo registro de vulnerabilidades y cuyas fallan sean cerradas tan pronto como son encontradas.
- Mantener actualizadas fuentes, librerías, lenguajes, ambientes de desarrollo y sistema operativo.
- No emplear claves fáciles. Mejor que sean palabras de más de 8 caracteres que no aparezcan en diccionario alguno, con mayúsculas, minúsculas, números y símbolos. Procurar cambiarlas al menos cada 6 meses.

- Documentarse sobre posibles fallas de seguridad en el lenguaje de programación empleado y como cerrarlas.

2.8.4 Lineamientos en Informática

La información almacenada en medios magnéticos se deberá inventariar, anexando la descripción y las especificaciones de la misma, clasificándola en tres categorías:

- Información histórica para auditorias.
- Información de interés de la Empresa
- Información de interés exclusivo de alguna área en particular.

Los jefes de área responsables de la información contenida en los departamentos a su cargo, delimitarán las responsabilidades de sus subordinados y determinarán quien está autorizado a efectuar operaciones emergentes con dicha información tomando las medidas de seguridad pertinentes.

Se establecen tres tipos de prioridad para la información:

- Información vital para el funcionamiento del área;
- Información necesaria, pero no indispensable en el área.
- Información ocasional o eventual.

En caso de información vital para el funcionamiento del área, se deberán tener procesos colaborativos, así como tener el respaldo diario de las modificaciones efectuadas, rotando los dispositivos de respaldo y guardando respaldos históricos semanalmente.

La información necesaria pero no indispensable, deberá ser respaldada con una frecuencia mínima de una semana, rotando los dispositivos de respaldo y guardando respaldos históricos mensualmente.

El respaldo de la información ocasional o eventual queda a criterio del área.

La información almacenada en medios magnéticos, de carácter histórico, quedará documentada como activos del área y estará debidamente resguardada en su lugar de almacenamiento.

Es obligación del responsable del área, la entrega conveniente de la información, a quien le suceda en el cargo.

Los sistemas de información en operación, como los que se desarrollen deberán contar con sus respectivos manuales. Un manual del usuario que describa los procedimientos de operación y el manual técnico que describa su estructura interna, programas, catálogos y archivos.

Ningún colaborador en proyectos de software y/o trabajos específicos, deberá poseer, para usos no propios de su responsabilidad, ningún material o información confidencial de SASF tanto ahora como en el futuro.

2.8.5 Beneficios de implantar políticas de seguridad informática

Los beneficios de un sistema de seguridad con políticas claramente concebidas bien elaboradas son inmediatos, ya que se trabajará sobre plataformas confiable, que se refleja en los siguientes puntos:

Aumento de la productividad.

- Aumento de la motivación del personal.
- Compromiso con la misión de la compañía.
- Mejora de las relaciones laborales.
- Ayuda a formar equipos competentes.
- Mejora de los climas laborales para los Recursos Humanos.

2.9 MARCO TEMPORAL/ESPACIAL

2.9.1 MARCO TEMPORAL

De acuerdo al tema de investigación, se puede establecer un estimado del tiempo de implementación de un mes para plasmar en tema de investigación planteado.

Durante la implementación de la aplicación se podrían presentar ciertos inconvenientes a la hora de hacer uso de la herramienta de seguridad.

2.9.2 MARCO ESPACIAL

El lugar donde se va a realizar la investigación, será principalmente en las empresas que ofertan servicios de transferencias bancarias o que manejen información de todo un país como puede ser tarjetas de crédito, correos electrónicos, contraseñas, etc. Estas empresas están ubicadas en Cuenca/Ecuador, ya que es donde se puede obtener toda la información necesaria para llevar a cabo la investigación y obtención de requerimientos en forma satisfactoria

2.9.3 MARCO LEGAL

Para este caso es necesario tomar en cuenta lo siguiente:

- Condiciones de acceso y utilización de la aplicación.
- Permisos y responsabilidades de uso tanto en la parte tangible e intangible por parte del usuario.
- Protección de información clasificada.
- Derechos de propiedad intelectual e industrial.

Todos estos ítems deben ser cumplidos, según menciona la constitución del Ecuador.

Los delitos que aquí se describen se encuentran como reforma al Código Penal por parte de la Ley de Comercio Electrónicos, Mensajes de Datos y Firmas Electrónicas publicada en Ley No. 67. Registro Oficial. Suplemento 557 de 17 de Abril del 2002.
Artículo 63.- A continuación del artículo 553 del Código Penal, añádanse los siguientes artículos enumerados: **Art. Inn.-Apropiación Ilícita.-** Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la

transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Fraude informático

Utilización fraudulenta de sistemas de información o redes electrónicas.

PRISION 6 MESES A 5 AÑOS Y MULTA 5000 A 10000 USD

Y SI EMPLEA LOS SIGUIENTES MEDIOS:

- Inutilización de sistemas de alarma seguridad o guarda
- Descubrimiento o descifrado de claves secretas o encriptados
- Utilización de tarjetas magnéticas o perforadas
- Utilización de controles o instrumentos de apertura a distancia.
- Violación de seguridades electrónicas

La seguridad informática en la empresa

Actualmente es indispensable que las empresas tomen en cuenta la Seguridad Informática para su Análisis de Riesgos.

Desde que se incorpora la informática y la tecnología a los procesos de las empresas, esto ha implicado que las actividades que se realicen sean sistemáticas, sean más ágiles y sencillas. Sin embargo, toda Facilitación debe ir de la mano con la Seguridad y Protección.

La seguridad informática, consiste en asegurar que los recursos del sistema de información **(material informático o programas)** de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Las medidas de Seguridad Informática se implementan para mitigar algún eventual "Delito Informático" en la empresa. Se define como delito informático, "cualquier actividad o conductas ilícitas, susceptibles de ser sancionadas por el derecho penal, que en su realización involucre el uso indebido de medios informáticos".

La Seguridad Informática debe ser parte de la Cultura de Seguridad de las Organizaciones e igualmente parte del Sistema de Gestión en Control y Seguridad de las mismas. Al

encontrarse bajo el marco de Sistema de Gestión, se logran añadir los beneficios de Planeación, Implementación, Verificación y Acciones Correctivas, que con cada ciclo irán depurando el Sistema en general.

Los sistemas de hardware y software al ser creados por seres humanos y más aún los usuario en sí por su naturaleza, le imprimen a la Informática un sentimiento de inseguridad que debe estar controlado; y nadie mejor que los dueños de cada proceso en conjunto con algún especialista en esta materia, para orientarnos hacia qué medidas efectivas adoptar para estar protegidos.[9]

2.9.4 Riesgo de la información en la Organización

Las organizaciones, sus sistemas y redes de información enfrentan amenazas de seguridad:

Pérdida de Confidencialidad, Disponibilidad o Integridad

Algunos como:

Fraude por computadora
Espionaje
Sabotaje
Vandalismo

Las causas que provocan o el daño son:

Código malicioso
Pirateo computarizado
Negación de servicios
Acceso no autorizado

2.9.5 Las vulnerabilidades

Las vulnerabilidades tecnológicas afectan a todas las plataformas y se convierten en uno de los riesgos más extensos que afrontan los profesionales de la seguridad informática.

Una vulnerabilidad informática es un elemento de un sistema informático que puede ser aprovechado por un atacante para violar la seguridad, así mismo pueden causar daños por sí mismos sin tratarse de un ataque intencionado.

(**antirrobo.net/seguridad/seguridad-empresarial)**[7]

A las vulnerabilidades se les consideran un elemento interno del sistema, por lo que es tarea de los administradores y usuarios el detectarlos, valorarlos y reducirlos.

2.9.6 Tipos de Vulnerabilidades.

Las vulnerabilidades son el resultado de errores de programación (bugs), fallos en el diseño del sistema, incluso las limitaciones tecnológicas pueden ser aprovechadas por los atacantes.

Para esta investigación, se clasifican las vulnerabilidades en seis tipos: Físicas, naturales, de hardware, de software, de red y de factor humano.

Física

Está relacionada con el acceso físico al sistema. Es todo lo referente al acceso y de las instalaciones donde se tienen los equipos de cómputo que contienen la información o forman partes de los procesos esenciales del sistema.

Las vulnerabilidades de este tipo se pueden presentar en forma de malas prácticas de las políticas de acceso de personal a los sistemas y uso de medios físicos de almacenamiento de información que permitan extraer datos del sistema de manera no autorizada.

Natural

Recordemos que las amenazas naturales son todo tipo de desastres causados por fuerzas naturales que causan daño a un sistema, por el lado de las amenazas naturales, estas se refieren al grado en que el sistema se puede ver afectado por este tipo de eventos.

Las vulnerabilidades de tipo natural se presentan principalmente en deficiencias de las medidas tomadas para afrontar los desastres, por ejemplo no disponer de reguladores, no-breaks, mal sistema de ventilación o calefacción, etc.

Hardware

Las vulnerabilidades de hardware representan la probabilidad de que las piezas físicas del sistema fallen (ya sea por mal uso, descuido, mal diseño etc.) dejando al sistema desprotegido o inoperable. También trata sobre las formas en que el hardware puede ser usado por personas para atacar la seguridad del sistema, por ejemplo el sabotaje de un sistema al sobrecargarlo deliberadamente con componentes de hardware que no han sido diseñados correctamente para funcionar en el sistema.

Software

Cada programa (ya sea de paquetería o de sistema operativo) puede ser usado como medio para atacar a un sistema más grande, esto se da debido a errores de programación, o porque en el diseño no fueron considerados ciertos aspectos (por ejemplo controles de acceso, seguridad, implantación, etc.).
Ambos factores hacen susceptible al sistema a las amenazas de software.

Red

Las redes pueden llegar a ser sistemas muy vulnerables, al tratarse de una serie de equipos conectados entre sí compartiendo recursos, es posible atacar a toda la red penetrando primero en uno de los equipos y posteriormente expandirse al resto.

En una red la prioridad es la transmisión de la información, así que todas las vulnerabilidades están relacionadas directamente con la posible intercepción de la información por personas no autorizadas y con fallas en la disponibilidad del servicio. Estos dos puntos hacen que las vulnerabilidades de las redes lleguen a ser una combinación de vulnerabilidades de hardware, software, físicas e incluso naturales.

Factor humano

Los elementos humanos de un sistema son los más difíciles de controlar lo que los convierte en constantes amenazas y al mismo tiempo una de las partes más vulnerables del sistema.

Las vulnerabilidades de origen humano más comunes son la falta de capacitación y concienciación, lo que puede dar lugar a la negligencia en el seguimiento de las políticas de seguridad, y mal uso del equipo de cómputo.

2.9.7 Amenazas Lógicas

Los protocolos de comunicación utilizados carecen (en su mayoría) de seguridad o esta ha sido implementada en forma de "parche" tiempo después de su creación.

- Existen agujeros de seguridad en los sistemas operativos.
- Existen agujeros de seguridad en las aplicaciones.
- Existen errores en las configuraciones de los sistemas.
- Los usuarios carecen de información respecto al tema.

Las empresas u organizaciones no se pueden permitir el lujo de denunciar ataques a sus sistemas, pues el nivel de confianza de los clientes bajaría enormemente.

Los Administradores de la seguridad informática dentro de la organización tienen cada vez mayor conciencia respecto de la seguridad de sus sistemas y arreglan por sí mismos las deficiencias detectadas. A esto hay que añadir las nuevas herramientas de seguridad disponibles en el mercado.

Acceso - Uso - Autorización

Específicamente "Acceso" y "Hacer Uso" no son el mismo concepto cuando se estudian desde el punto de vista de un usuario y de un intruso. Por ejemplo:

Cuando un usuario tiene acceso autorizado, implica que tiene autorizado el uso de un recurso.
Cuando un atacante tiene acceso desautorizado está haciendo uso desautorizado del sistema.
Pero, cuando un atacante hace uso desautorizado de un sistema, esto implica que el acceso fue autorizado (simulación de usuario).

Luego un **Ataque** será un intento de acceso, o uso desautorizado de un recurso, sea satisfactorio o no. Un **Incidente** envuelve un conjunto de ataques que pueden ser distinguidos de otro grupo por las características del mismo (grado, similitud, técnicas utilizadas, tiempos, etc.)

CAPITULO III

3 METODOLOGÍA

3.1 METODOLOGÍA DE INVESTIGACIÓN

3.1.1 UNIDAD DE ANÁLISIS

Para garantizar el avance en la investigación y estudio de este proyecto, es necesario contar con el apoyo de las empresas, mismas que necesitan asegurar su información contra las infiltraciones internas o externas.

3.1.2 TIPO DE INVESTIGACIÓN

El tipo de investigación que se utilizara será la combinación de la metodología aplicada, documental y de campo.

- **Documental.-** Identificación y búsqueda de información tanto virtual como de contenido de libros y manuales necesarios para el estudio de la aplicación del software.
- **Campo.-** Esta me permitirá realizar entrevistas, y en si verificar como viene funcionando actualmente la empresa que se pretende proteger mediante un sistema sofisticado de información.

3.1.3 MÉTODOS

Para este caso se utilizara un método de síntesis ya que permite al investigador reunir varios elementos que están causando el problema para llegar a plantear una solución y aplicarla. Y el método inductivo servirá para generalizar explícitamente las actividades de administrador de seguridad y el área en que estos se desenvuelven.

3.1.4 TÉCNICAS

Se utilizara las técnicas de investigación como entrevistas, encuestas para obtención y recolección necesaria y pertinente para esté caso.

3.1.5 FUENTES DE INFORMACIÓN

Para el desarrollo adecuado del tema de investigación es necesario recurrir tanto a las fuentes primarias como secundarias. Como fuentes primarias es necesaria la información directa de las personas que hayan sufrido algún tipo de ataque o amenaza, también a directivos, personas especializadas en la seguridad informática de la universidad Israel, jefes y empleados; así como investigación bibliográfica que se va obteniendo durante el desarrollo de la investigación y manuales físicos sobre la herramienta estudiada. Como fuentes secundarias obtenida y consultada desde varias páginas de internet y opiniones de personas ajenas a las empresas o procesos.

3.1.6 INSTRUMENTOS

Se utilizara instrumentos metodológicos y tecnológicos tales como: Cuestionarios, Encuestas, e internet.

ANALISIS DE LA APLICACIONES DE SEGURIDAD INFORMÁTICA PARA LAS EMPRESAS NESSUS

En nuestra actualidad se sabe de la existencia de ciertas amenazas que en cualquier momento pueden afectar al funcionamiento de las máquinas: **troyanos, virus, spam y ataques por parte de hackers,** suelen ser los principales riesgos que pueden afectar al funcionamiento de los sistemas informáticos de cualquier empresa**.** La diversidad es tan grande, que las compañías de seguridad informática de todo el mundo presentan de manera continuada nuevas soluciones. Cada empresa y cada usuario particular debe ser capaz de discernir cuales son las aplicaciones informáticas que les interesa instalar para proteger su información**.**

Existen compañías que tienen la creencia de que con la instalación de un antivirus es más que suficiente, sin embargo, está probado que cualquier **Hacker** puede invadir fácilmente los sistemas y tener acceso a información valiosa. Todo lo que necesita es una vulnerabilidad del software, que utilizará para conectar con la computadora y

ejecutar un malware. Debe entenderse que la instalación de un antivirus no es suficiente para proteger nuestros sistemas**. [10]**

Por lo cual mediante este estudio de seguridad informática hemos seleccionado una aplicación que cumple con todas las características necesarias para proteger la información de las empresas, y así estar a salvo de los intrusos que navegan atreves de la web.

3.2.1 Tipos de seguridad informática

<table>
<tr><th>SEGURIDAD FÍSICA</th><th>SEGURIDAD LÓGICA</th><th>SEGURIDAD EN LAS ORGANIZACIONES</th><th>SEGURIDAD JURIDICA</th></tr>
<tr><td>Consiste en la aplicación de barreras físicas y procedimientos de Control, como medidas de prevención.</td><td>El activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren</td><td rowspan="3">Las más grandes organizaciones pretenden cubrir todas las vulnerabilidades, que en algunos casos se les escapa a la seguridad física y lógica.

Por lo cual establece :

Política de seguridad, políticas de personal, de contratación, análisis de</td><td rowspan="3">Pretende, a través de la aprobación de normas legales, fija el marco jurídico necesario para proteger los bienes informáticos.</td></tr>
<tr><td>Es uno de los aspectos más olvidados a la hora del diseño de un sistema informático.
Tipos de desastres:
Incendios
Inundaciones
Terremotos
Instalación eléctrica.</td><td>Algunas técnicas de seguridad lógica:
Control de acceso
Autenticación
Encriptación
Firewalls
Antivirus (en caso de Usar Windows).</td></tr>
<tr><td>CONTRAMEDIDA</td><td>CONTRAMEDIDA</td></tr>
</table>

[10] www.antirrobo.net/**seguridad**/**seguridad-empresarial**.html

-Cerrar con llave el centro de cómputos. -Tener extintores por eventuales incendios. -Instalación de cámaras de seguridad. -Guardia humana. -Control permanente del sistema eléctrico, de ventilación, etc. -UPS o SAI (Sistema de alimentación ininterrumpida).	-Cortafuegos. -Antivirus. -Antispam. -Antispyware. -Números de serie. -Protección anti copia.	riesgos, plan de contingencia. 	

Cuadro 3.1 Tipo de seguridad informática

3.2.2 Identificación de las amenazas

La identificación de amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del atacante.

Las consecuencias de los ataques se podrían clasificar en:

- **Data Corruption**: la información que no contenía defectos pasa a tenerlos.
- **Denial of Service (DoS)**: servicios que deberían estar disponibles no lo están.
- **Leakage**: los datos llegan a destinos a los que no deberían llegar.

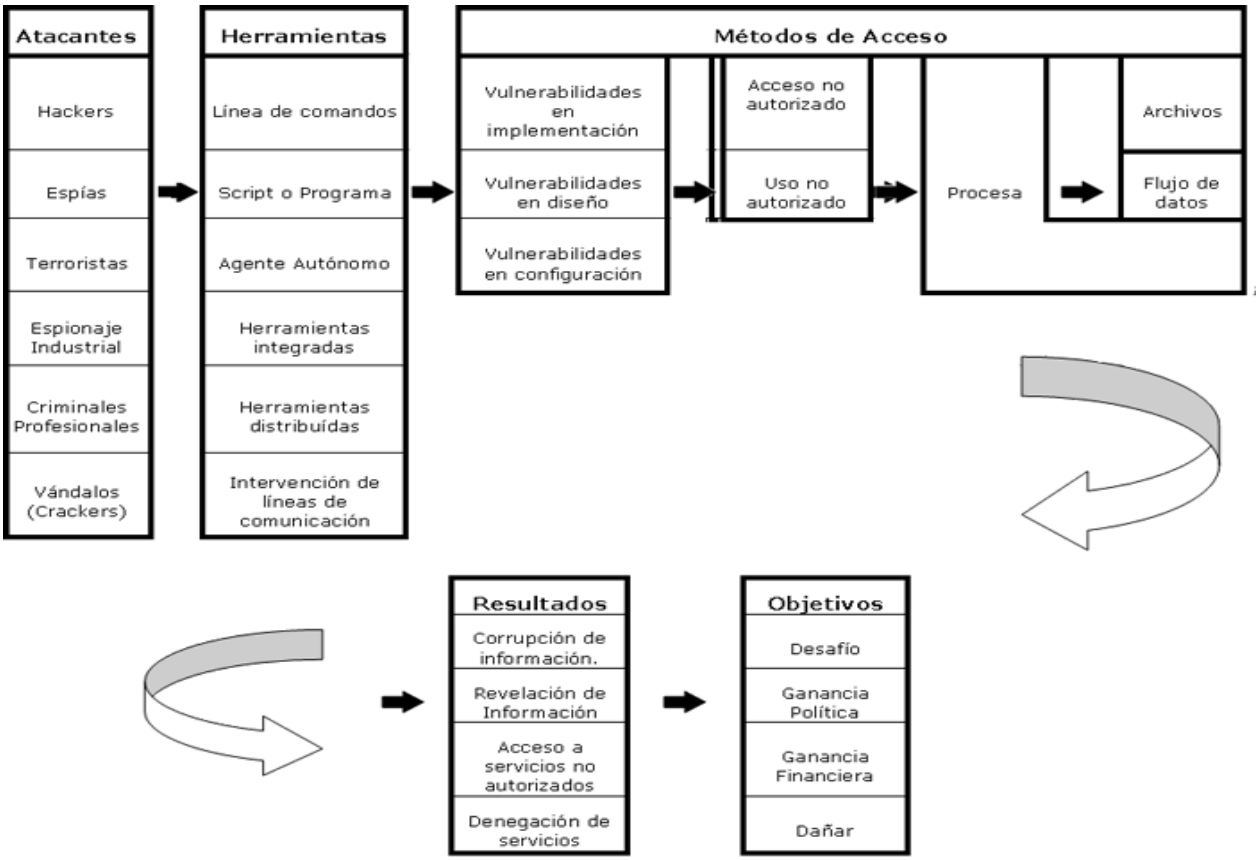


Grafico 3.2 Ataques Herramientas y métodos de acceso. **Fuente:** extraída de HOWARD John D. Libro An Analysis of security on the Internet 1995.

El grafico 1.1 detalla el tipo de atacante, las herramientas utilizadas, en qué fase se realiza el ataque, los tipos de procesos atacados, los resultados esperados y/u obtenidos y los objetivos perseguidos por los intrusos.

3.2.3 Análisis de riesgos de la información

Existen muchos tipos de riesgos que pueden perjudicar la información o los equipos informáticos de una organización.

La organización internacional por la normativa ISO define riesgo tecnológico (Guía para la gestión de la seguridad de TI /TEC TR 13335-1, 1996) como:

"La prioridad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generando perdidas o daños"

Amenazas	Probabilidad	Servidores	Terminales	Datos	Personal	Riesgo Total	Efectividad de Control
Incendios	1%	10	5	8	41	1,26	100%
Inundaciones	1%	10	1	8	8	0,24	90%
Acceso no autorizado(*HACKERS*)	**40%**	**1**	**0**	**20**	**0**	**2,6**	**50%**
Fallas	20%	0,5	0,5	2	0	0,75	50%
Virus	30%	2	3	1	0	1,8	80%

Grafico 3.3 Grado de impactos de las amenazas

Esta matriz nos presenta que existen muchas maneras de amenazas, y abundantes metodologías que ponen en riesgo la información de las empresas.

Información posible sobre el sistema objetivo.

3.2.4 Prevención de amenazas informáticas

Las medidas de prevención que deben tomar muy en cuenta las grandes organizaciones son, Codificar la información: Criptología, Criptografía y Criptociencia, contraseñas difíciles de averiguar a partir de datos personales del individuo. -Vigilancia de red. Zona desmilitarizada -Tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software, etc. Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad. -Sistema de Respaldo Remoto. Servicio de backup remoto. [11]

3.2.5 Medidas de Prevención

- Mantener las máquinas actualizadas y seguras físicamente.
- Mantener personal especializado en cuestiones de seguridad.
- Los administradores de red, los cuales deben configurar adecuadamente sus routers.
- Mantenerse informado constantemente sobre cada unas de las vulnerabilidades encontradas y parches lanzados.
- Utilizar protocolos seguros como https, ssh.

[11] www.piramidedigital.com/.../pdictsegurindadinformaticariesgos.pdf

- Encriptación de mails mediante GPG.

Migrar a otros sistemas operativos como GNU/Linux, Solaris, BSD.

MATRIZ COMPARATIVA DE LAS HERRAMIENTAS DE SEGURIDAD INFORMATICA MÁS COMUNES

	Nessus	Nmap	Managedpki	AppScan DE	Ethereal	Snort
Objetivo	Diseñado especialmente detectar vulnerabilidades en las aplicaciones	Su objetivo principal es la detección de mapeo redes	Se encarga de asegurar los procesos administrativos en las empresas	El objetivo principal es el análisis de vulnerabilidades y pruebas de penetración de sus aplicaciones y plataformas Web	Permite examinar tráfico en la red a partir de ficheros capturados	Detecta intrusos y analiza el trafico de la red en tiempo real
Compatibilidad con Windows. Linux, Solaris, Unix, Mac.	✓	✗	✓	✓	✗	✓
Gestion de porteccion de datos	80%	60%	54%	75%	40%	40%
Analisis de Vulnerabilidades	✓	✗	✗	✓	✗	✗
Proteccion de redes	✓	✓	✗	✗	✗	✓
Ataques contra Hackers	✓	✓	✓	✓	✓	✓
Audiatoria de Seguridad	✓	✗	✗	✓	✗	✓

Grafico 3.4 Cuadro comparativo de las herramientas de seguridad informática

3.3 MANUAL DE USUARIO DE LA HERRAMIENTA DE SEGURIDAD NESSUS

1. Los primero que debemos hacer es instalar el programa, que podemos encontrar en la página oficial de Tenable Network Security o se adquirimos la versión pagada, y una vez instalado ejecutamos el servidor desde la aplicación grafica para poder acceder al cliente desde nuestro navegador en la dirección:
http://localhost:8834/

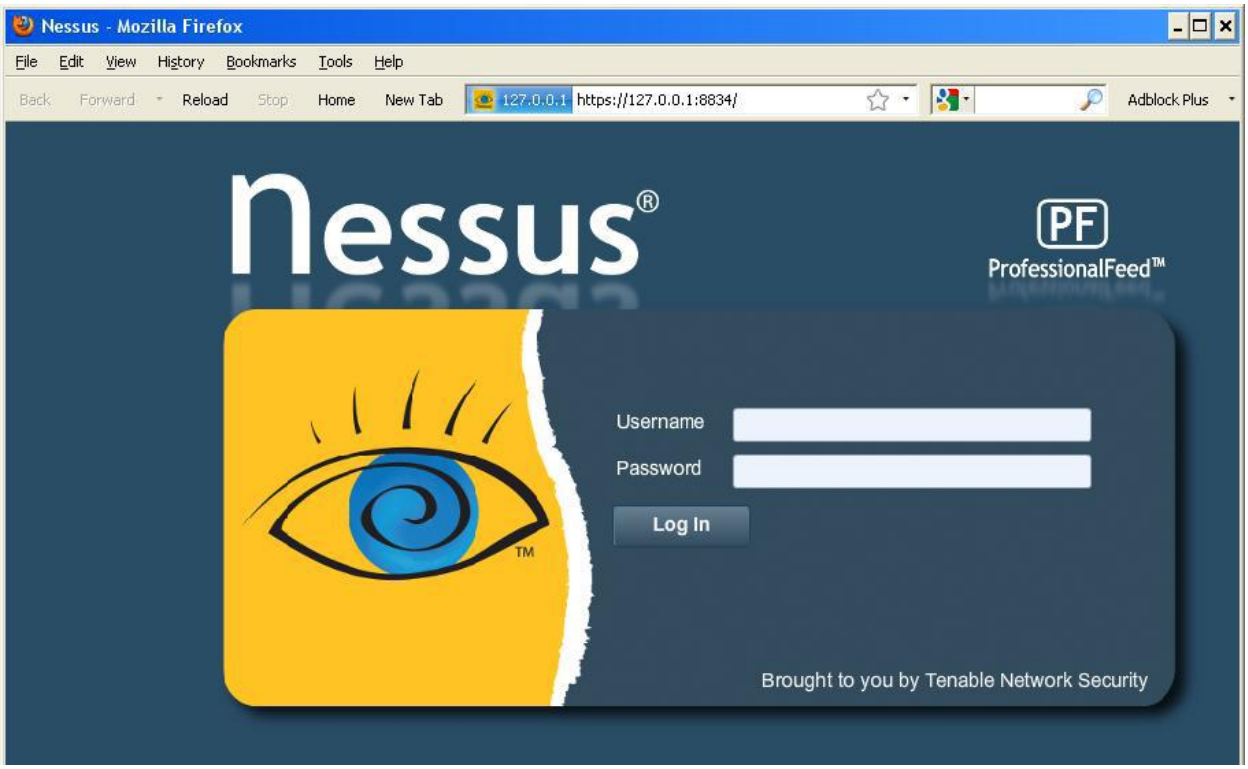


Figura1.1 Autenticación en la consola de configuración Nessus

Titulo: Pantalla de acceso

Campos:

1. Username.- tipo: carácter, longitud: 8;
2. Password: tipo: carácter, longitud: 10;

Realiza una autenticación mediante una cuenta y una contraseña previamente creadas con el administrador del servidor. Después de que la autenticación se haya realizado correctamente, la UI presentará menús para llevar a cabo análisis:

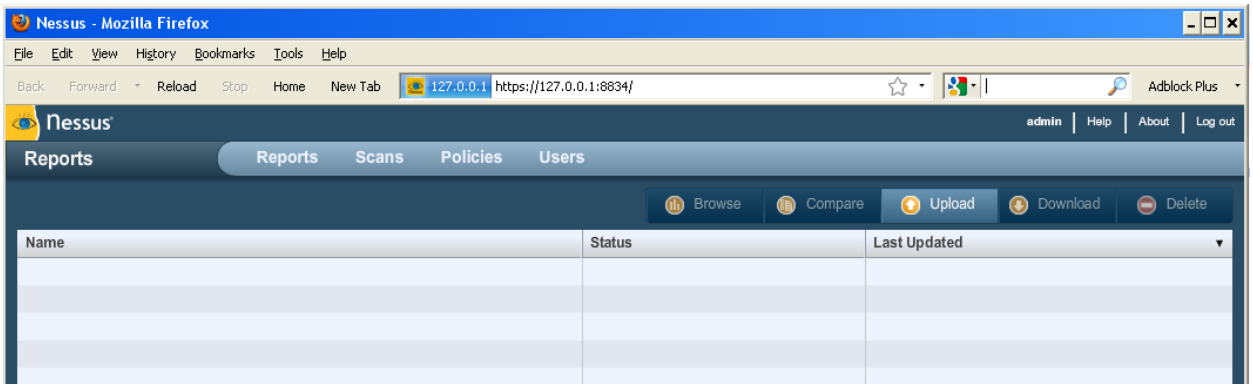


Figura1.2 Consola de configuración

2. Una vez dentro de la aplicación, lo primero que debemos hacer es configurar una política de escaneo, desde la pestaña **"Policies">"Add":**

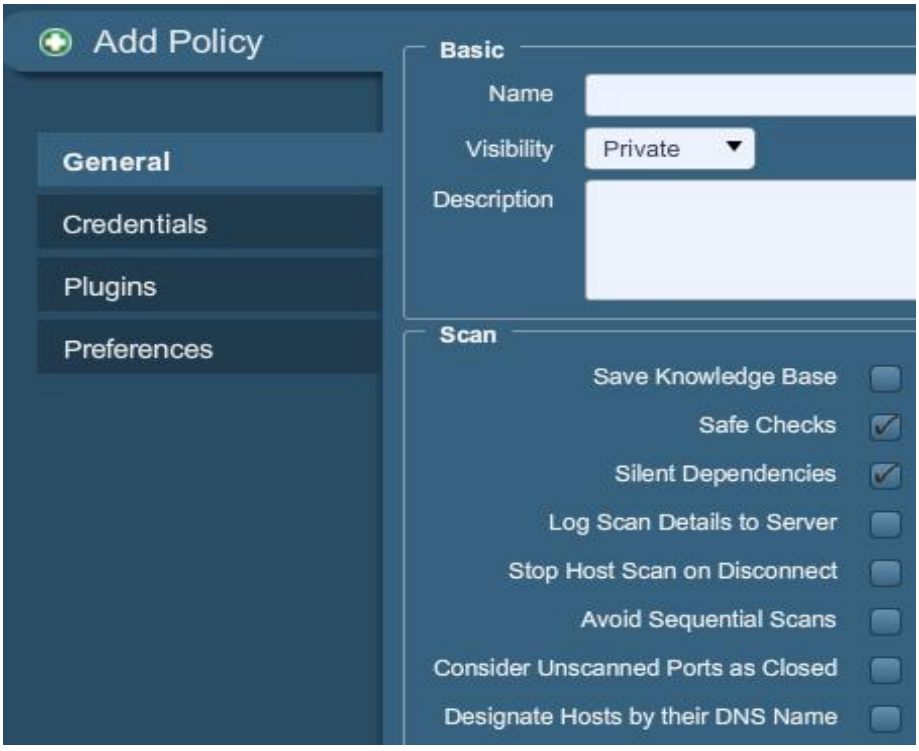


Figura 1.3 Creación de política de escaneo

En esta pestaña tenemos cuatro opciones:

General: La ficha General nos permite nombrar la directiva y configurar las operaciones relacionadas con el análisis. Hay 3 cuadros de opciones agrupadas que controlan el comportamiento del analizador:

OPCION	DECSRIPCION
Name	Establece el nombre que aparecerá en la UI de Nessus para identificar la directiva.
Visibility	Controla si la directiva se comparte con otros usuarios ("Shared"), o se mantiene *privada* para su uso exclusivo ("Private"). Solo los usuarios administrativos pueden compartir directivas.
Description	Se usa para brindar una breve descripción de la directiva de análisis, que es habitualmente una buena opción para resumir el propósito general (por ejemplo, "El servidor web analiza sin comprobaciones locales ni servicios que no sean HTTP").

Credenciales: La ficha Credentials, cuya imagen se incluye a continuación, le permite configurar el analizador Nessus para que use credenciales de autenticación durante los análisis. Al configurar las credenciales, Nessus podrá realizar una variedad más amplia de comprobaciones que produzcan resultados de análisis más precisos, los cuales se deberá configurar de acuerdo a al tipo de análisis que se ejecutar.

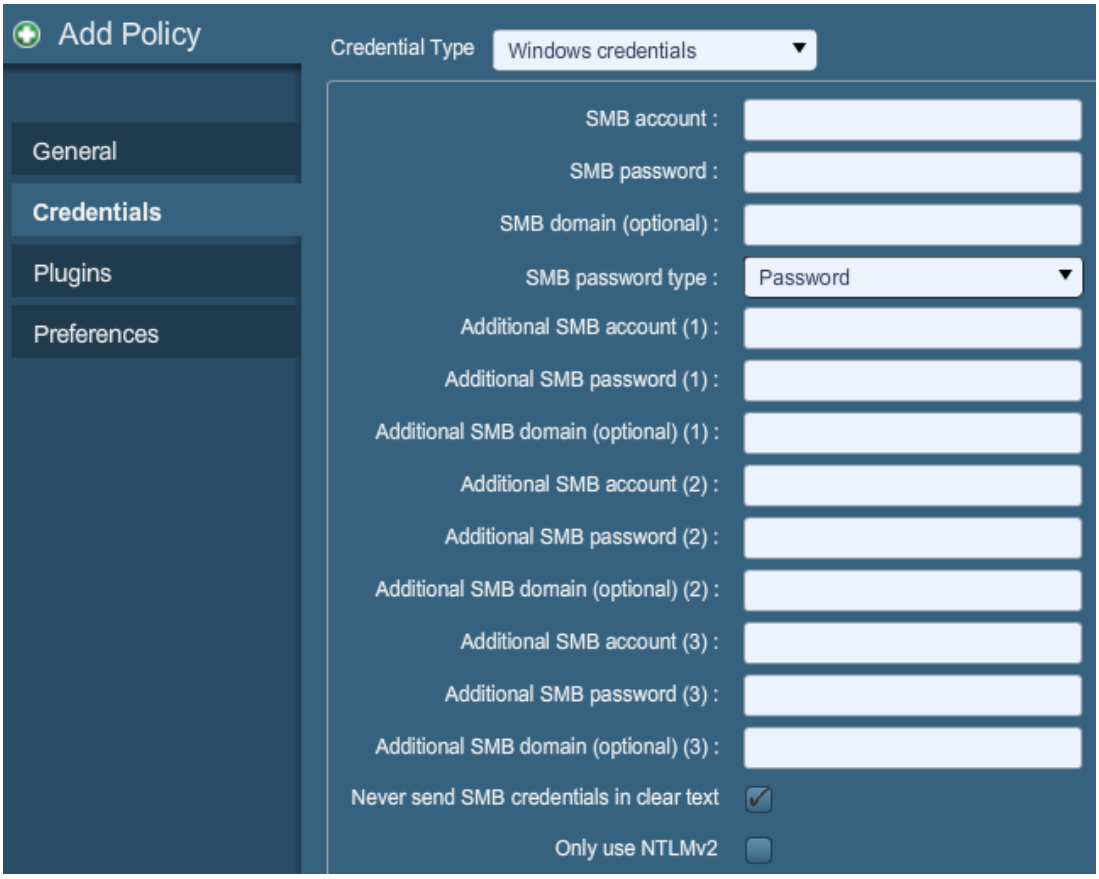


Figura 1.4 Creación de políticas de escaneo Credenciales

Plugins: Es de las opciones más importantes en ella marcamos solo los que necesitamos, ya que si no el programa tardara una eternidad en completar el escaneo.

La ficha Plugin Selection permite al usuario elegir comprobaciones de seguridad específicas por familia de plugins o comprobaciones individuales.

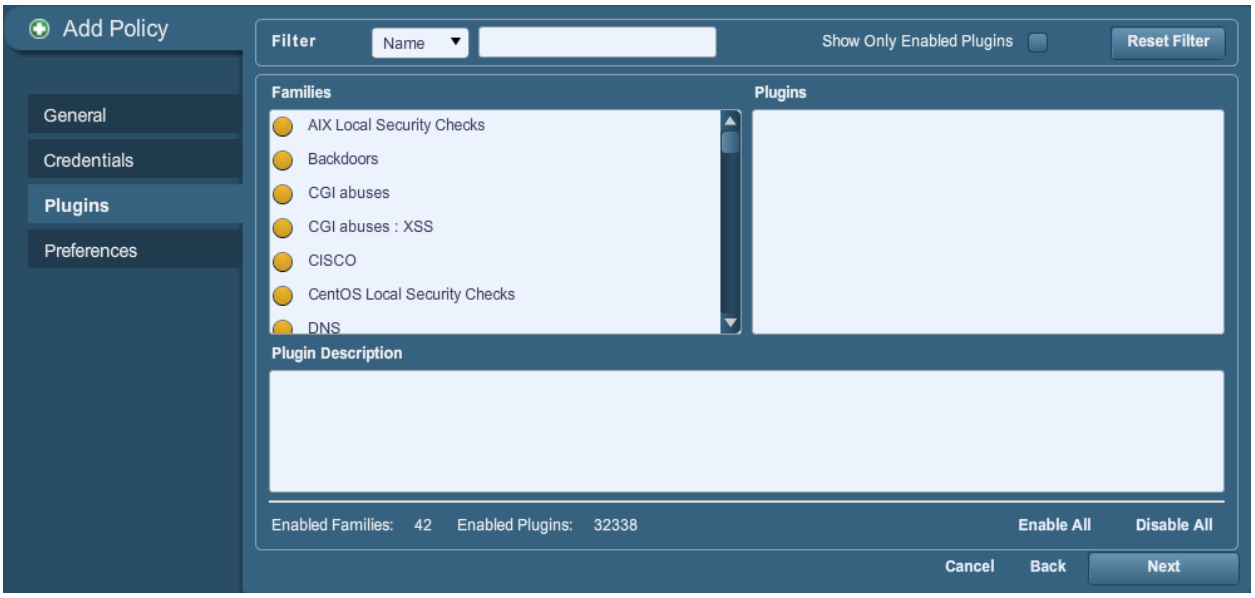


Figura 1.5 Creación de políticas plugins

Si hace clic en el círculo amarillo junto a una familia de plugins, podrá habilitar o deshabilitar la familia entera. Si selecciona una familia, aparecerá en pantalla la lista de sus plugins en el panel superior derecho. Se pueden habilitar o deshabilitar plugins individuales para crear directivas de análisis muy específicas. A medida que se efectúan ajustes, la cantidad total de familias y plugins seleccionados aparece en la parte inferior. Si el círculo que está junto a una familia de plugins es mitad gris y mitad amarillo, esto indica que algunos de los plugins están habilitados, pero no todos ellos.

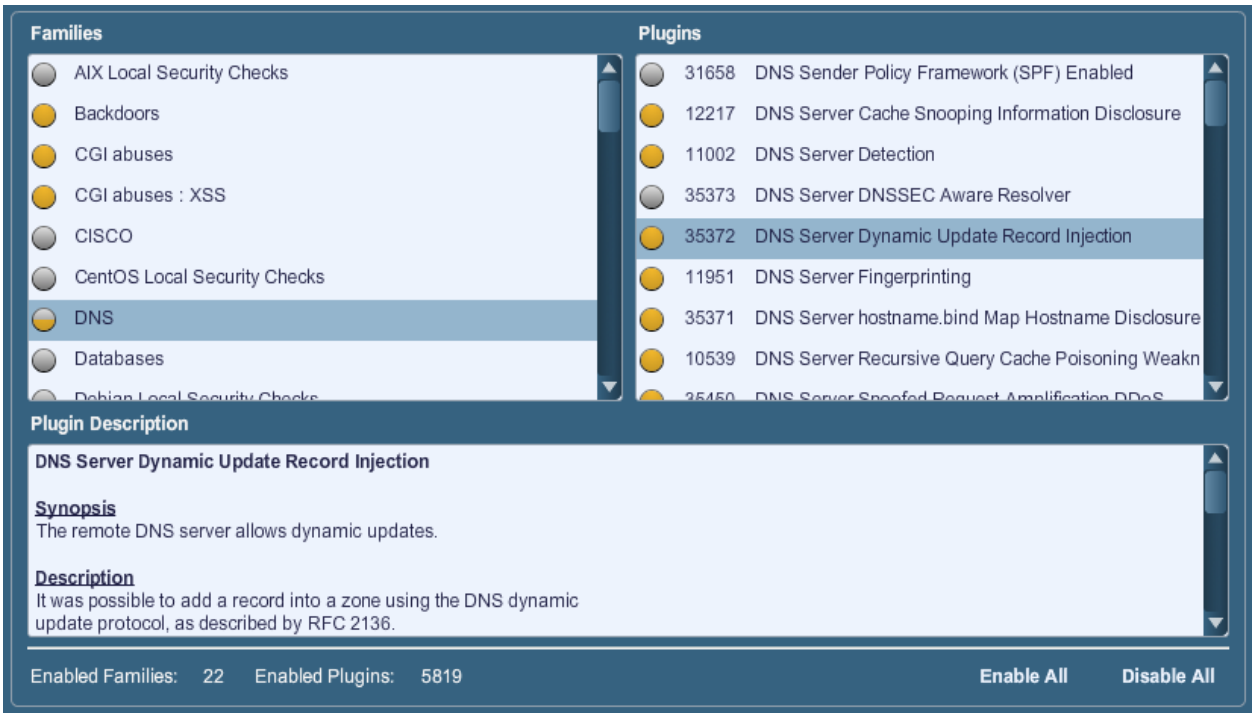


Figura 1.6 Creación de políticas habilitar y deshabilitar plugins

Si selecciona un plugin específico, el resultado de ese plugin aparecerá como se visualiza en un informe. La sinopsis y la descripción brindarán más detalles de la vulnerabilidad que se está examinando. Si se desplaza hacia abajo por el panel "Plugin Description" encontrará también información sobre soluciones, referencias adicionales si están disponibles y el puntaje CVSSv2 que ofrece una clasificación del riesgo básica.

Preferences: La ficha **"Preferences"** incluye medios para lograr un control pormenorizado de la configuración de los análisis. Si selecciona un elemento del menú desplegable, aparecerán elementos de configuración adicionales para la categoría seleccionada. Tenga en cuenta que se trata de una lista dinámica de opciones de configuración que depende de la fuente de plugins, las directivas de auditoría y otras funciones a las que tenga acceso el analizador Nessus conectado. Un analizador con una ProfessionalFeed puede contar con opciones de configuración más avanzadas que un analizador configurado con la HomeFeed. Esta lista también puede cambiar a medida que se añaden o modifican plugins.

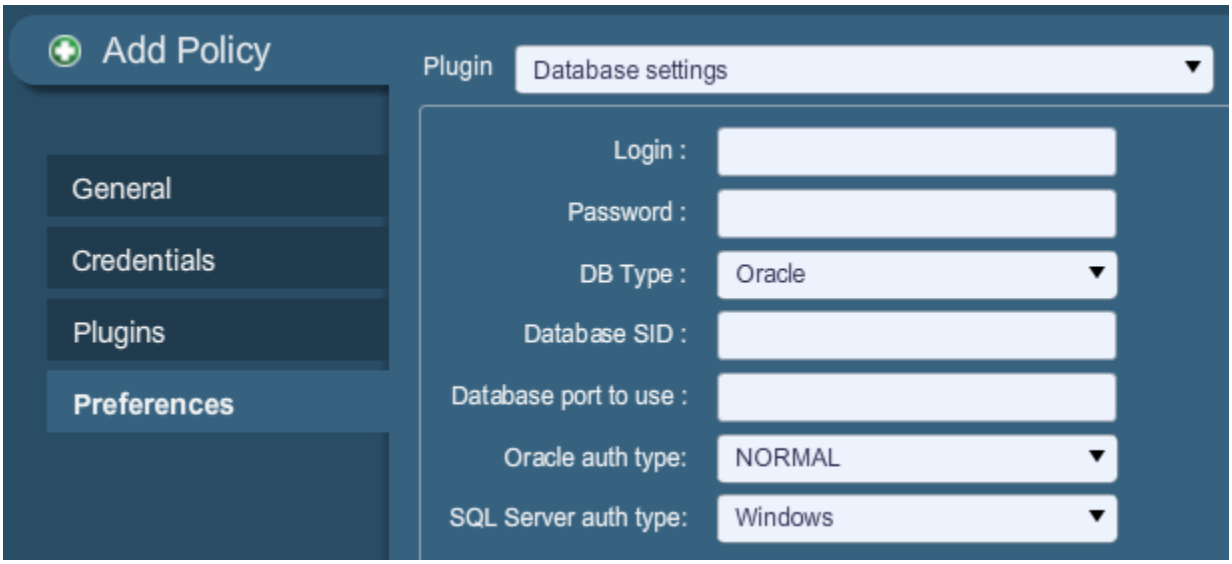


Figura1.7 Creación de políticas preferencias

Las opciones de **"Database settings"** se usan para especificar el tipo de base de datos que se probará, la configuración correspondiente y las credenciales:

OPCIÓN	DESCRIPCIÓN
Login	El nombre de usuario para la base de datos.
Password	La contraseña correspondiente al nombre de usuario proporcionado.
DB Type	Se admiten Oracle, SQL Server, MySQL, DB2, Informix/DRDA y PostgreSQL.
Database SID	La identificación de sistema de la base de datos para auditar.
Database port to use	Puerto en el que escucha la base de datos.
Oracle auth type	Se admiten NORMAL, SYSOPER y SYSDBA.
SQL Server auth type	Se admiten Windows o SQL.

Una vez tenemos una política de escaneo bien configurada para una maquina objetivo, nos dirigimos a la pestaña "scan", y pulsamos en "add" para añadir uno nuevo:

Si queremos obtener la IP asociada a un nombre de dominio, podemos obtener mediante el comando "ipconfig" ejecutado en la consola, tanto para Windows como para Linux, etc.

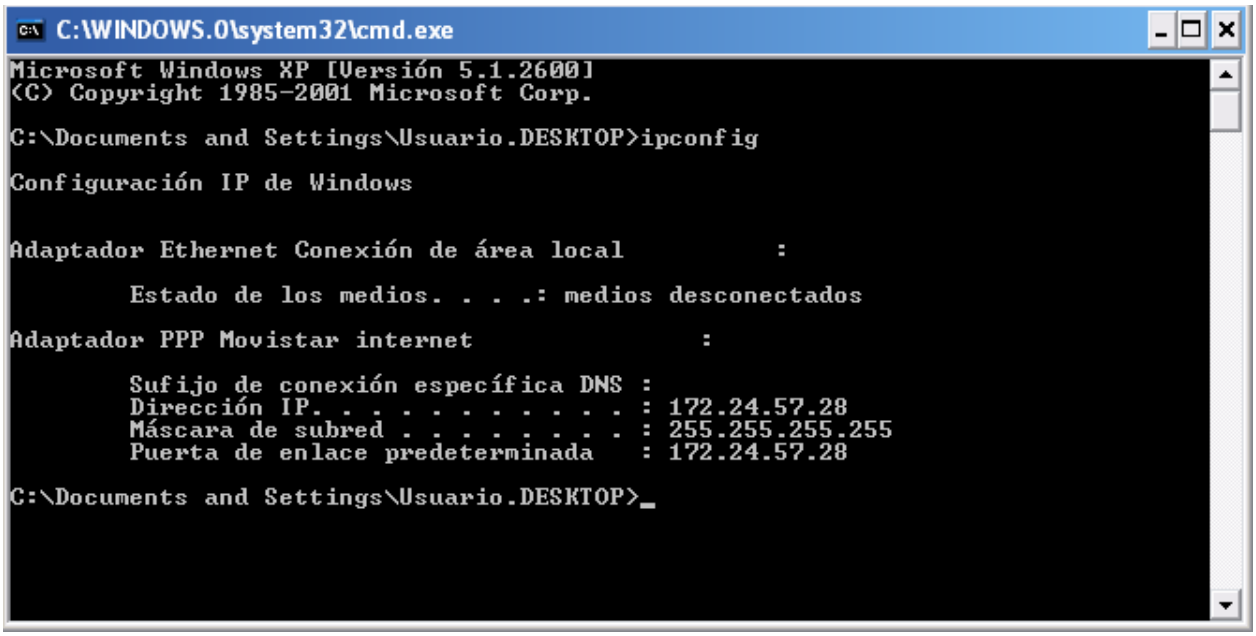


Figura 1.8 Consola del sistema operativo Windows, comando ipconfig.

CREACIÓN, INICIO Y PROGRAMACIÓN DE UN ANÁLISIS

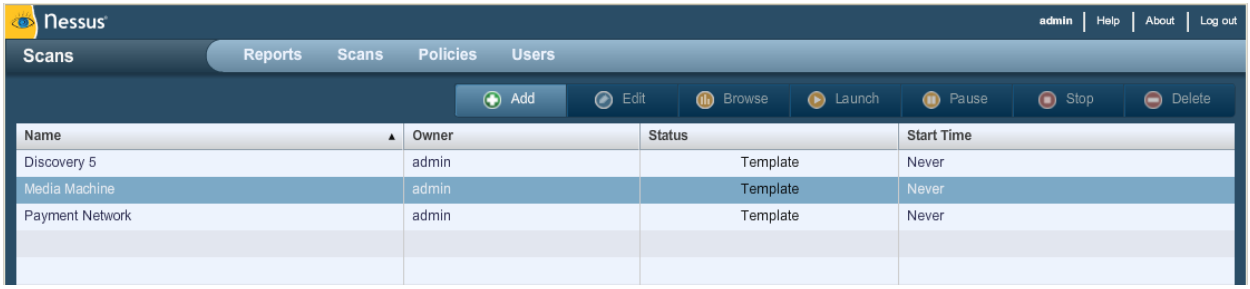


Figura 1.9 Pantalla de inicio de análisis

Después de crear una directiva puede crear un nuevo análisis; para ello haga clic en la opción **"Scans"** de la barra de menús situada en la parte superior y luego haga clic en el botón **"+ Add"** de la derecha. Aparecerá la pantalla **"Add Scan"**, como se muestra a continuación:

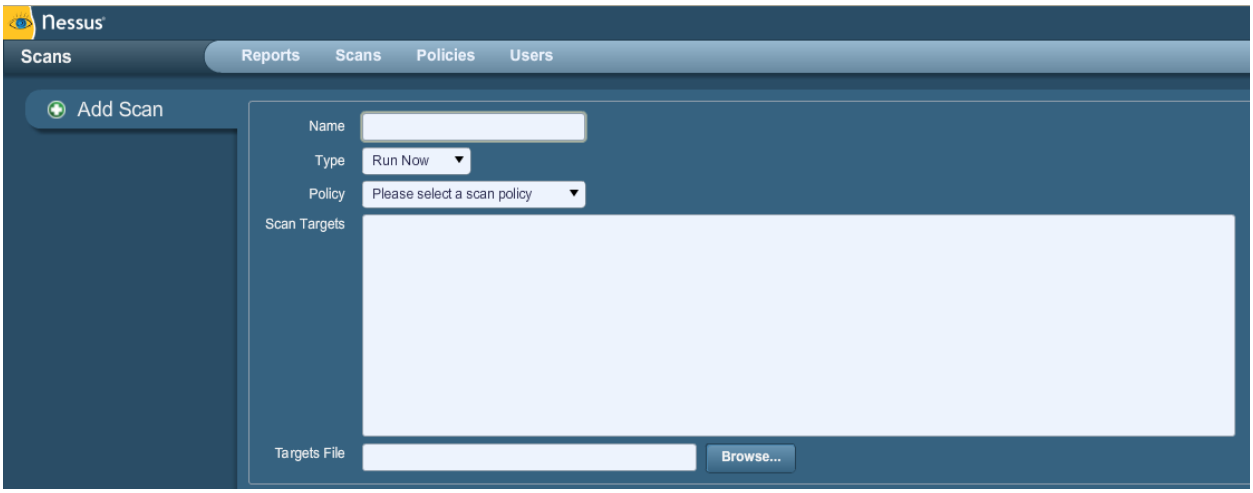


Figura 1.10 Crear un nuevo análisis

Hay cinco campos para introducir el destino del análisis:

> **Name:** establece el nombre que aparecerá en la UI de Nessus para identificar el análisis.

> **Type:** seleccione entre "Run Now" (para ejecutar el análisis inmediatamente después de ejecutar el comando "Submit" [Enviar]), "Scheduled" (para seleccionar la hora en que debe comenzar el análisis) o "Template" (para guardar como plantilla para otro análisis posterior).

> **Policy:** seleccione una directiva creada anteriormente que usará el análisis para establecer los parámetros que controlan el comportamiento de análisis del servidor Nessus.

> **Scan Targets:** los destinos se pueden introducir mediante una dirección IP única (por ejemplo, 192.168.0.1), un intervalo de IP (por ejemplo, 192.168.0.1-192.168.0.255), una subred con notación CIDR (por ejemplo, 192.168.0.0/24) o un host que se pueda resolver (por ejemplo, www.nessus.org).

> **Targets File:** se puede importar un archivo de texto con una lista de hosts haciendo clic en **"Browse…"** y seleccionando un archivo del equipo local.

Después de haber introducido la información del análisis, haga clic en "Submit". Después de realizar esta acción (Enviar) el análisis comenzará de inmediato (si se seleccionó "Run Now"), antes de que la pantalla vuelva a la página general "Scans".

Figura 1.11 proceso de escaneo

Una vez iniciado el análisis, en la lista Scans se mostrará una lista de todos los análisis que estén en curso en ese momento, pausados o basados en plantillas, junto con la información básica del análisis. Después de seleccionar un análisis de la lista en particular, los botones de acción situados en la parte superior derecha le permitirán explorar ("Browse") los resultados del análisis en curso, poner en pausa ("Pause") y reanudar ("Resume") el análisis, o detenerlo ("Stop") y eliminarlo ("Delete") por completo. Los usuarios también pueden modificar ("Edit") los análisis basados en plantillas.

Explorar

Para explorar los resultados de un análisis, seleccione un nombre de la lista "Reports" y haga clic en **"Browse"**. Esto le permite ver resultados al navegar por hosts, puertos y vulnerabilidades específicas. La primera pantalla de resumen muestra cada host analizado, junto con un detalle de las vulnerabilidades y los puertos abiertos:

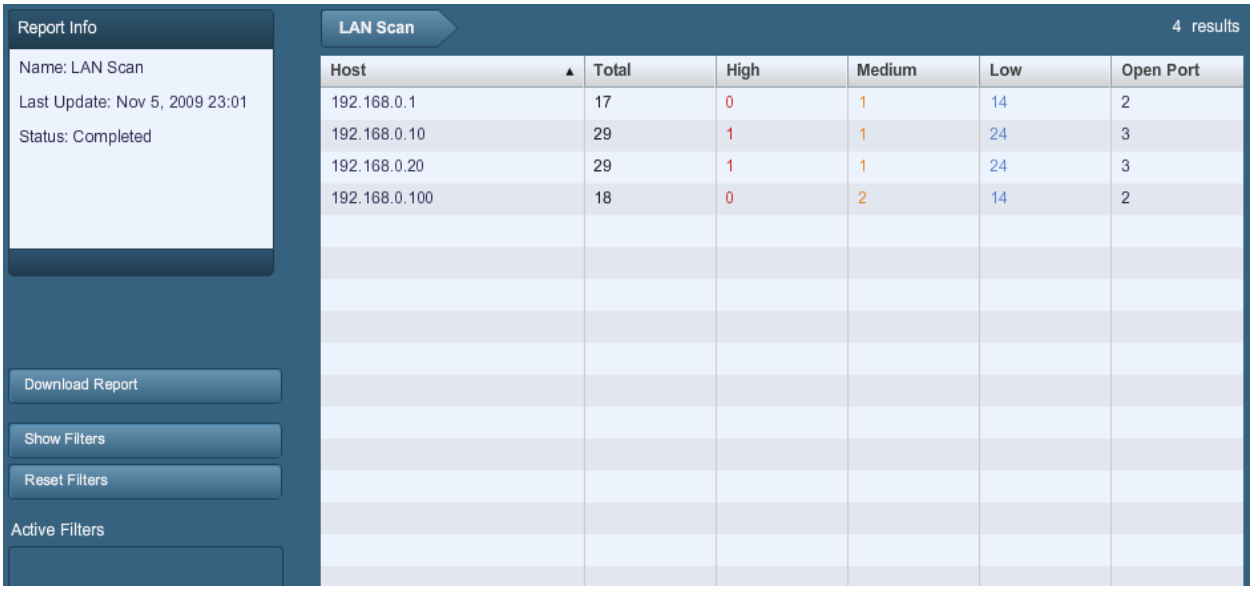
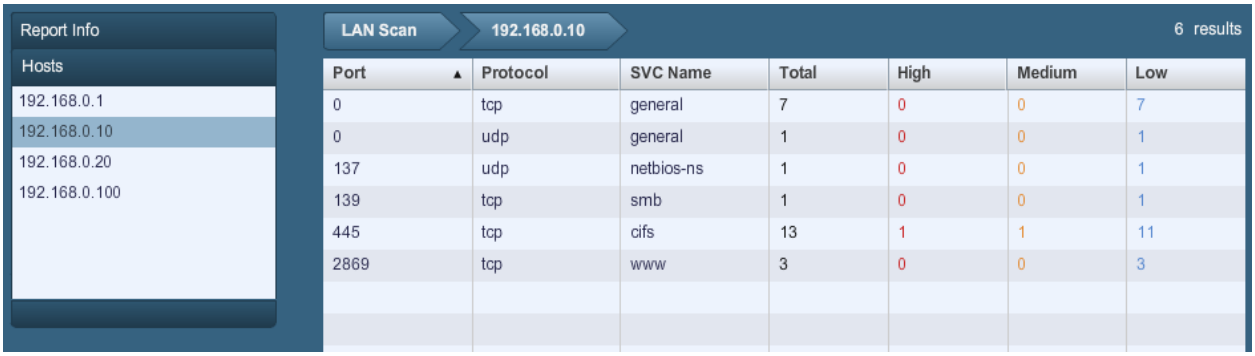


Figura 1.12 Listado de puertos abiertos que fueron escaneados

Con un host seleccionado, el informe se dividirá por números de puerto y aparecerá información relacionada, tal como el protocolo y el nombre del servicio, así como también un resumen de las vulnerabilidades clasificadas por gravedad del riesgo. A medida que navega por los resultados del análisis, la interfaz de usuario mantendrá la lista de hosts y una serie de flechas interactivas para ayudarle a navegar rápidamente hasta un componente específico del informe:



Port	Protocol	SVC Name	Total	High	Medium	Low
0	tcp	general	7	0	0	7
0	udp	general	1	0	0	1
137	udp	netbios-ns	1	0	0	1
139	tcp	smb	1	0	0	1
445	tcp	cifs	13	1	1	11
2869	tcp	www	3	0	0	3

Figura 1.13 Listado de vulnerabilidades detectados

Si selecciona un puerto, aparecerán todos los resultados de las vulnerabilidades que se relacionan con el puerto y el servicio:

Plugin ID	Name	Port	Severity
11011	SMB Detection	cifs (445/tcp)	Low
10785	SMB NativeLanMan	cifs (445/tcp)	Low
10394	SMB log in	cifs (445/tcp)	Low
10859	SMB get host SID	cifs (445/tcp)	Low
10860	SMB use host SID to enumerate local users	cifs (445/tcp)	Low
10395	SMB shares enumeration	cifs (445/tcp)	Low
26919	SMB guest account for all users	cifs (445/tcp)	Medium
10397	SMB LanMan Pipe Server browse listing	cifs (445/tcp)	Low
10396	Microsoft Windows SMB Shares Access	cifs (445/tcp)	High
23974	SMB Share Hosting Office Files	cifs (445/tcp)	Low
10400	SMB accessible registry	cifs (445/tcp)	Low
10428	SMB fully accessible registry	cifs (445/tcp)	Low
26920	SMB NULL session	cifs (445/tcp)	Low

Figura 1.14 Listado de vulnerabilidades detectadas y su nivel de riesgo

Si selecciona una vulnerabilidad de la lista aparecerán detalles completos de los resultados, incluidos una sinopsis, una descripción técnica, la solución, el factor de riesgo, el puntaje CVSS, salidas relevantes que prueben los resultados, referencias externas, la fecha de publicación de la vulnerabilidad, la fecha de publicación o modificación de los plugins y la disponibilidad de las vulnerabilidades de seguridad:

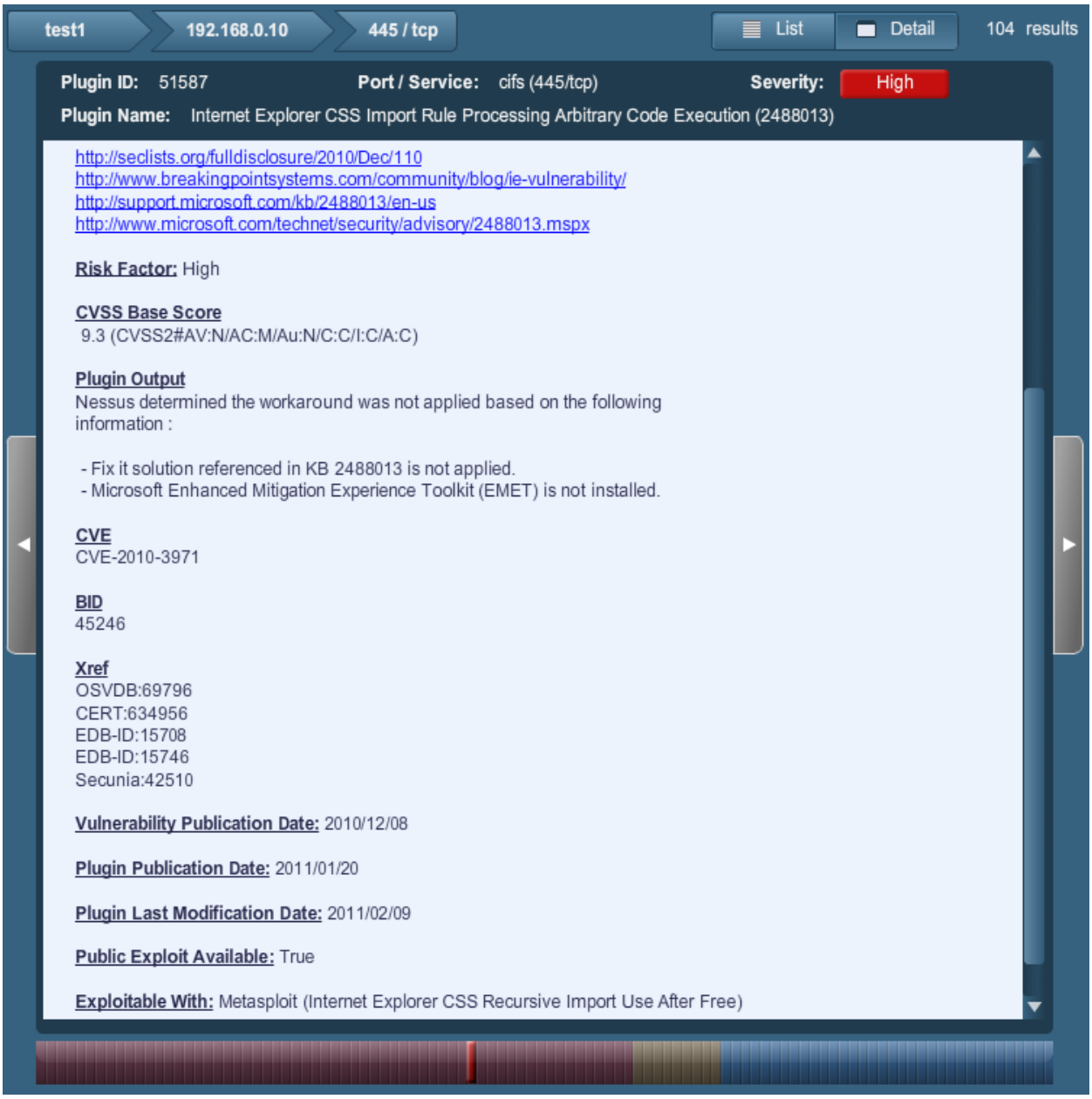


Figura 1.15 Informe de reporte de los vulnerabilidades

En la disponibilidad de las vulnerabilidades de seguridad se mostrarán las vulnerabilidades de seguridad conocidas y públicas, incluidas las encontradas en marcos de trabajo de vulnerabilidades (públicos o comerciales), tales como CANVAS, CORE o Metasploit.

Por últimos, recordar que sise quiere que el programa trabaje al 100% se debe tener actualizados los plugins al día, y hacer una buena configuración de la política de escaneo antes de comenzar.

La pantalla de detalles de vulnerabilidades brinda varios métodos para navegar por el informe:
> Se pueden seleccionar las teclas de flechas de la parte superior para retroceder a la descripción general de un análisis, un puerto o un host.
> Los botones “List” y “Detail” alternan entre el detalle de las vulnerabilidades y la última vista de lista (en el ejemplo anterior, las vulnerabilidades relacionadas con el algún puerto).

> Las flechas grises hacia la izquierda o la derecha recorrerán las otras vulnerabilidades relacionadas con el puerto seleccionado.

> La barra de botones de la parte inferior proporciona una forma de saltar a una vulnerabilidad particular de la lista, de acuerdo con la gravedad del riesgo. En el ejemplo anterior se destacan las vulnerabilidades de riesgo bajo, medio y alto.

SECURITYCENTER Después de añadir correctamente el analizador, aparecerá la siguiente página tras la selección del analizador:

Configuración de SecurityCenter
Se puede añadir un servidor “Nessus Server” mediante la interfaz de administración de SecurityCenter para la corrección de las vulnerabilidades y los puertos detectados. Con ella, SecurityCenter se puede analizar, configurar para obtener acceso y controlar prácticamente cualquier analizador Nessus.
A continuación se muestra una captura de pantalla de un ejemplo de la página “Add Scanner” de SecurityCenter:

Después de añadir correctamente el analizador, aparecerá la siguiente página tras la selección del analizador:

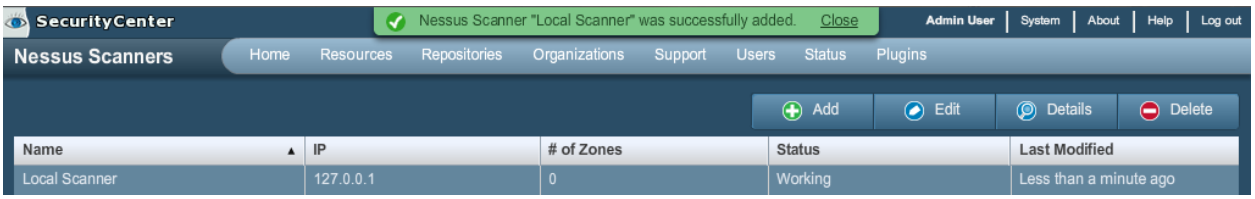


Figura 1.6 SecurityCenter correcccion de la vulnerabilidades detectadas

Por los cual luego de realizar todas las configuraciones en la aplicación podremos controlar las vulnerabilidades y los puertos abiertos que nuestra herramienta nos informa mediante un reporte, para poder tomar las medidas de seguridad que nos informa.

CONCLUSIÓNES

El estudio realizado en este proyecto podemos entender que la seguridad informática en las empresas es una de los aspectos más primordiales que hay que tomar en cuenta cuando de proteger los datos se trate, ya que los recursos destinados a lograr que la información y los activos de una organización sean confiables, íntegros y disponibles para los usuarios que tengan acceso a dicha información.

Hay que tomar muy en cuenta que no se puede proteger en su totalidad la información, ya que existen muchos riesgos dentro o fuera de la organización, sin embargo se debe estar preparado y dispuesto a reaccionar con rapidez contra los ataques las amenazas y vulnerabilidades que invaden las redes de internet.

Muchas de la empresas implementan políticas de seguridad, esto a su vez provoca un gran reto a la misma, por lo contrario se sabe que es impredecible sobre todo si se tiene en cuenta que cada vez los ataque de hackers son más constante hacia las mas grades instituciones públicas o privadas.

Para concluir, espero que mediante el estudio de este trabajo inspire en las personas una a realizar nuevas investigaciones futuras que profundicen mas en el temas planteado en este proyecto, ya que cada vez la tecnología avanza a gran velocidad y así mismo los ataques son cada vez más peligrosos.

RECOMENDACIONES

Ya que la tecnología informática avanza cada vez más rápido a pasos agigantados, es recomendable estar al día con las nuevas actualizaciones de nuestros equipos sobre todo nuestro sistema operativo, ya que posee muchos fallos, poseer un sistema de seguridad informático avanzado como lo es **"Nessus",** ya que nos ayudara a la detección de intrusos en la red.

Instale un Antivirus y actualícelo con frecuencia. Analice con su antivirus todos los dispositivos de almacenamiento de datos que utilice y todos los archivos nuevos, especialmente aquellos archivos descargados de internet.

Instale un Firewall o Cortafuegos con el fin de restringir accesos no autorizados de Internet.

Utilice contraseñas seguras, es decir, aquellas compuestas por ocho caracteres, como mínimo, y que combinen letras, números y símbolos. Es conveniente además, que modifique sus contraseñas con frecuencia. En especial, le recomendamos que cambie la clave de su cuenta de correo si accede con frecuencia desde equipos públicos.

Navegue por páginas web seguras y de confianza. Para diferenciarlas identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. Extreme la precaución si va a realizar compras online o va a facilitar información confidencial a través de internet.

En general, es fundamental estar al día de la aparición de nuevas técnicas que amenazan la **seguridad de su equipo informático**, para tratar de evitarlas o de aplicar la solución más efectiva posible.

BIBLIOGRAFIA

[1]http://securityfocus.com

[2]www.hispasec.com

[3]www.securityportal.com.ar
http://windsofthesky.wordpress.com/2008/07/11/tipos-de-amenazas-informaticas/
http://www.cert.org

[**4]** LISTA DE HERRAMIENTAS DE SEGURIDAD. http://www.unamcert.
unam.mx/herramientas.html

[5]http://www.casadellibro.com/libro-defensa-contra-hackers-proteccion-de-informacion-privada-incluy-e-cd-rom/2900000759545

[5]http://www.informatica-juridica.com/anexos/Ley_67_2002_Comercio_Electronico_Firmas_Mensajes_Datos_27_febrero_2002.asp

[6] Mc Graw, Gill (2000). Los Hackers. II Congreso Mundial De La Informática.
HACKING EXPOSED. http://www.hackingexposed.com

[7] CERT – Coordinatin Center. http://www.cert.org. 2004
(antirrobo.net/seguridad/seguridad-empresarial)
Estrategias de Seguridad Inobis Consulting Pty Ltd. Microsoft Solutions
http://www.microsoft.com/latam/technet/articulo/200011

[8] Definición de Políticas de Seguridad. http://www.rediris.es/cert

[11] www.antirrobo.net/seguridad/seguridad-empresarial.html

[12] www.piramidedigital.com/.../pdictsegurindadinformaticariesgos.pdf

[11] http://www.maestrosdelweb.com/editorial/snort 2009-04-05