ASPECTOS DE ANÁLISIS DE VULNERABILIDADES Y ETHICAL HACKING

Rangel, Erika. Sotto, Julian.
erangel@outlook.com, linkfree.julian@gmail.com
Universidad Piloto de Colombia

Resumen—La implementación de nuevas aplicaciones, la falta de pruebas antes de su puesta en producción, la protección inapropiada de sistemas, redes y la falta de controles de seguridad de la información, da como resultado la generación de errores significativos, los cuales pueden ser aprovechados por usuarios mal intencionados con el fin de obtener beneficios, extraer información y poner en riesgo una organización. Uno de los retos más importantes de la gestión de la seguridad se enfoca en satisfacer la Confidencialidad, Integridad y Disponibilidad de la información a través de un conjunto de metodologías, técnicas y herramientas que permitan evaluar un sistema o red con el fin de encontrar vulnerabilidades.

Abstract—The implementation of new applications, the lack of testing before being put into production, inadequate protection of systems, networks and the absence of security controls of information results in the generation of significant errors, which can be exploited by malicious users in order to make a profit, extract information and put at risk an organization. One of the most important challenges of security management focuses on meeting the Confidentiality, Integrity and Availability of information through a set of methodologies, techniques and tools to evaluate a system or network to find vulnerabilities.

Índice de Términos—Aplicaciones WEB, Ethical Hacking, Pentest, vulnerabilidades.

Index Terms—Ethical Hacking, Pentest, vulnerabilities, WEB Applications.

I. INTRODUCCIÓN

Las debilidades en sistemas operativos, aplicaciones, redes informáticas, la carencia de planes de concientización y capacitación y la falta de definición e implementación de políticas y controles de seguridad, exponen grandes riesgos de seguridad, que hacen que realizar un análisis de vulnerabilidades sea un requisito indispensable dentro del proceso de gestión de la seguridad de la información en toda organización.

Los Análisis de Vulnerabilidades son un mecanismo fundamental de un esquema de seguridad de la información, estos deben ser realizados por un Hacker Ético, o por expertos en temas de seguridad que garantice la protección y confidencialidad de los datos y la información, que se encuentra en las aplicaciones, dispositivos y servicios analizados. A través de la definición de fases, aplicación de procedimientos y uso de herramientas especializadas que permiten establecer causas, grados de exposición, tipos de impacto, recursos afectados, contribuyendo a definir pautas y sugerir recomendaciones para la solución de los mismos y para el aseguramiento de los datos.

II. SEGURIDAD INFORMÁTICA.

Seguridad informática como muchos expertos la definen es: una ciencia de la informática que incluye la protección de la infraestructura tecnológica, los usuarios y la información contenida.

Para los profesionales en seguridad informática o carreras a fines del mundo de hoy, el proteger la información dentro de una organización es una tarea difícil, debido a que cada día son más las compañías que producen nuevas herramientas tecnológicas volátiles en hardware y software, dejando al departamento de TI, desactualizado y en una constante sed de conocimiento.

Las organizaciones han venido sufriendo, drásticamente las consecuencias del avance tecnológico en seguridad

del mundo, en especial los países latinoamericanos, Brasil, México, Venezuela y donde Colombia es el cuarto país más vulnerable en seguridad informática, según estudios realizado a principios del 2011 por el laboratorio de kaspersky, quien demostró que los países de América Latina, les falta aplicar políticas de gestión de la seguridad, políticas para dispositivos USB y políticas de seguridad en general. Este tipo de puertas les ha permitido a intrusos realizar múltiples ataques, por no contar con un esquema de seguridad adecuado.

Es por esto que los pilares fundamentales de la seguridad de la información se enfocan en garantizar las siguientes características:

Confidencialidad: garantiza que el contenido de la misma solo es conocido y accesible por usuarios autorizados.[1]

Integridad: Propiedad de la información que se caracteriza por mantener sin alteraciones y en completitud el contenido; esta solo puede ser modificada por usuarios autorizados con previo registro para llevar control de versiones o auditorias. [2]

Disponibilidad: Es la propiedad que asegura el acceso a la información y a sus recursos, para ser consultada y procesada por usuarios autorizados en el momento que lo requieran.[3]

Autenticidad. Característica que permite garantizar el origen de la información, verificando tanto el emisor como el receptor de la misma, con el fin de evitar la usurpación de identidad.[4]

No Repudio: Característica de la información mediante la cual se afirma que un usuario o entidad envió o recepcionó datos, sin posibilidad a negarlo posteriormente.[5]

Consistencia: Propiedad asociada a la integridad, que garantiza que el sistema se comporte de la forma como se supone con los usuarios previamente autenticados, sin que estos evidencien problemas inesperados.[6]

Auditoria: Capacidad para determinar que acciones o procesos se han ejecutado en un sistema, relacionando en los logs de acceso la hora y fecha de las transacciones, el nombre de usuario, los errores presentados y las aplicaciones donde se accedió.

III. ESTÁNDARES, METODOLOGÍAS Y BUENAS PRÁCTICAS PARA LA SEGURIDAD INFORMÁTICA[7]

A continuación se listan una serie de estándares de seguridad que se pueden aplicar en las organizaciones

Familia ISO/IEC 27000 de las que se destacan:

- ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799.
- ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información.
- ISO 27004: Guía de técnicas de gestión de riesgo.
- ISO 27011: Guía de continuidad de negocio en cuanto a TIC.
- ISO 27031: Guía de ciber-seguridad.
- ISO 27032: Guía de seguridad en redes.
- ISO 27033: Guía de seguridad en aplicaciones.
- ISO 27035:2011 Gestión de incidentes de seguridad de la información.

NTC5411- 1 Gestión de la seguridad de la tecnología de la información y las comunicaciones. (Catálogo publicaciones ICONTEC Internacional)

Recomendación UIT-T X.805: Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo.

[1] Confidencialidad, [en línea]. https://www.ccn-cert.cni.es/publico/serieCCN-STIC401/es/c/confidentiality.htm

[2] Antonio Villalón Huerta, El Sistema de Gestión de Seguridad de la Información "la nueva norma UNE 71502", [en línea]. Disponible: <http://www.shutdown.es/ISO17799.pdf> (2013, Marzo 28).

[3] Introducción a la Seguridad Informática. Conceptos Básicos- La Seguridad informática en números, [en línea]. http://seginfo.tripod.com/files/17799a.pdf

[4] Introducción a la Protección y Seguridad de la Información, [en línea].http://alarcos.inf-cr.uclm.es/doc/PSI/tema1Marian.pdf

[5] Diseño de Protocolos de No-Repudio, [en línea].<http://revistasic.com/revista38/pdf_38/SIC_38_1agora.PDF>

[6] Seguridad en Redes, [en línea]. <http://www.slideshare.net/tec37045/seguridad-en-redes-ii>

[7] Introducción a la Protección y Seguridad de la Información, [en línea].

TCSEC - Trusted Computer System Evaluation Criteria: Criterios de evaluación de la seguridad de los sistemas de computación, conocidos también con el nombre de Orange Book (Libro naranja).

ITSEC (White Book): criterios para evaluar la seguridad informática de productos y sistemas.

COBIT: Objetivos de Control para Información y Tecnologías Relacionadas.

ITIL: Norma de mejores prácticas para la administración de servicios de Tecnología de Información (TI).

OSSTMM: Manual de la Metodología Abierta de Testeo de Seguridad.

IV. COMPONENTES DE SEGURIDAD

A. Seguridad física.

Consiste en establecer medidas y/o procedimientos de control del acceso físico como mecanismos de prevención de amenazas para los recursos y la información incorporada en archivos, contraseñas, perfiles y otro tipo de datos, que son de vital importancia para la organización y que se encuentran albergados en los diferentes servidores, estaciones de trabajo y puntos de conexión de red.

1. Componentes de la Seguridad Física.

Estas medidas en su mayoría son adoptadas por las entidades u organizaciones con el fin de establecer un perímetro con las barreras básicas, donde se tiene en cuenta la criticidad de cada activo y/o recurso de la red; los cuales se mencionan a continuación:[8]

Factores Ambientales y/o naturales: Se enfocan en proteger el sistema de los desastres naturales como incendios, terremotos, inundaciones, polvo, altas temperaturas, cortos eléctricos, entre otras.

Factores de vigilancia: El sistema de red se asegura a través de cámaras, circuitos cerrados de tv, guardias de seguridad, detector de metales, entre otros.

Factores de acceso físico: El sistema se salvaguarda de la intrusión por personal no autorizado, material comestible, dispositivos, vehículos al centro de red principal, con el apoyo de biométricos, sensores, tarjetas inteligentes, firmas digitales, animales, entre otros.

Factores de contingencia: La seguridad de la red se conserva a través de plantas eléctricas, fuentes de enfriamiento y ventilación, extinguidores, etc.

Factores de Recuperación: El sistema de administración de la red se preserva con la programación de backups, ejecución de aplicaciones en paralelo en caso de ser vulnerado el sistema, etc.

2. Dispositivos para la seguridad física.

La seguridad física utilizada en las organizaciones involucra el manejo de artefactos, que se han dedicado a proteger los activos de información, durante los últimos años.

Dado el incremento de riesgos que se han evidenciado como fallas en la seguridad física, las empresas encargadas de ofrecer este tipo de dispositivos, se han enfocado en fabricar nuevos diseños con mejoras en su portabilidad, en su costo y en su eficiencia, características que han suministrado a las organizaciones herramientas con las que se puede identificar el personal, validar los privilegios y permitirle el acceso al usuario.

Algunos de los dispositivos que se dedican a mejorar la seguridad física para el acceso tanto a instalaciones como a equipos en la red se listan a continuación:

- Tarjetas magnéticas
- Tarjetas inteligentes
- Biométricos
- Sistemas de Identificación por radiofrecuencia (RFI- radio frequency identification)
- Sistemas de circuito cerrado de televisión (CCTV-closed circuit televisión)
- Sistemas de sensores y alarmas
- Sistemas de vigilancia ambiental
- Sistemas de vigilancia del personal.

[8] Seguridad Fisica, [en línea].< http://www.slideshare.net/tecnodelainfo/seguridad-fsica>

B. Seguridad Lógica.

Son las técnicas y métodos que salvaguardan los privilegios o permiso a los datos y solo autoriza a usuarios o perfiles que tienen el rol de acceso para el ingreso a la arquitectura de red.

C. Protección de la red a través de los cortafuegos.

Es necesario implementar mecanismos que permitan la administración y control de comunicaciones desde y hacia la red de la organización, limitando el tráfico entre las diferentes zonas (intranet, e internet) a través de la aplicación de una serie criterios y reglas establecidas en el cortafuegos, y que tiene como función examinar cada petición y bloquear aquellas que no satisfacen los criterios de seguridad definidos.

Cada estación de trabajo que pertenezca a la red de la organización, debe disponer de mecanismos de protección, pues cada nodo representa un foco de exposición de seguridad alto, que puede ser aprovechado para el acceso no autorizado, generando exposición de información confidencial, causando robo o distorsión de la misma, exponiendo secretos organizacionales, que logran desencadenar fraudes, evitando la continuidad de las operaciones del negocio.

D. Administración de puertos y servicios activos.

Es importante incorporar medidas básicas de seguridad que permitan conocer puertos y servicios activos, identificar cuales facilitan la intrusión, representan puntos vulnerables y conllevan a una mayor exposición de riesgos de seguridad.

Por eso es indispensable aplicar mecanismos que contribuyan a la gestión, administración y monitoreo de la seguridad, determinando el alcance y el nivel de importancia en la categorización de los servicios de red, ofreciendo funciones para definir políticas de bloqueo de puertos y servicios que no sean necesarios, su incidencia en la red y los usuarios responsables del control de éstos, todo esto para reducir el impacto de cada uno de esos riesgos.

E. Administración de usuarios y contraseñas.

Es la forma administrativa que tiene el departamento de TI para parametrizar la red, a través de políticas de perfiles con base a los usuarios que están registrados. La mayoría de problemas de seguridad se centran en este aspecto, debido a la errada gestión que tienen los usuarios sobre las contraseñas asignadas. Una organización puede invertir dinero en la adquisición de software para la red, en capacitaciones para los usuarios, en personal altamente calificado, en soporte técnico a los dispositivos conectados vendidos por los diferentes proveedores, sin tener en cuenta que el mayor riesgo de seguridad en la administración de perfiles, es la falta de compromiso de los usuarios en cumplir las políticas asignadas, esto conlleva a que estos evadan constantemente su responsabilidad frente a alguna amenaza de seguridad.

F. Inventario de perfiles.

La administración de servidores, software, equipos y dispositivos conectados puede ser controlada con los inventarios de perfiles. Estos almacenan las IP, los usuarios y permisos válidos para entrar a la estructura de la red. A su vez son de gran ayuda porque limitan el acceso a algunos recursos, con la configuración de reglas a puertos o protocolos dispuestos para el ingreso.

El avance que han tenido los mecanismos de intrusión en las redes, han determinado que el grado de protección de las mismas requiere del desarrollo de nuevas tecnologías, protocolos y sistemas para elevar la seguridad a los dispositivos y recursos enlazados a la red.

Estos índices conllevan a que las organizaciones quieran proteger mucho más sus conexiones para lo que han implementado diferentes esquemas de autenticación, cifrado y autorización, como instrumentos tecnológicos necesarios para crear políticas de seguridad de control de acceso (ISO 17799).

G. Autenticación y autorización de usuarios para dispositivos de red.

Dado el crecimiento y evolución de herramientas informáticas utilizadas para suplantar la identidad de los usuarios; la autenticación se convierte en el punto de inicio para controlar el acceso a los elementos de la red, siendo este un sistema de protección desarrollado que permite identificar y validar que la persona es quien dice ser, para que posteriormente a través del proceso de autorización se le conceda el acceso a los usuarios, a un sistema o a un dispositivo especifico de la red.

La restricción del acceso a los dispositivos, proporciona una defensa contra amenazas de confidencialidad, disponibilidad e integridad, y se constituye en un elemento fundamental para garantizar la seguridad de red.

Existe un cierto grado de confusión en el ámbito de la seguridad sobre la diferencia entre la prueba de penetración y el análisis de vulnerabilidades, con frecuencia muchas personas lo clasifican como lo mismo pero en realidad no lo es.

Una prueba de penetración se compone principalmente de un análisis de vulnerabilidades, y un poco más.

El Pentest se define como "Método de evaluación de seguridad de un sistema o red informática mediante la simulación de un ataque de un intruso"[9], La OSSTMM (Open Source Security Testing Methodology Manual) lo define como "Una prueba de seguridad con un objetivo específico que termina cuando dicho objetivo se obtiene o se acaba el tiempo disponible". El NIST (National Institute of Standards and Technology), NIST Special Publication 800-115, define pruebas de penetración como "Prueba de seguridad donde los evaluadores imitan ataques reales para identificar los métodos para burlar las medidas de seguridad de una aplicación, sistema o red. A menudo consiste en lanzar ataques reales en condiciones reales y utilizando datos, herramientas y técnicas utilizadas por los atacantes."[10] Según la guía de pruebas owasp define las pruebas de intrusión como el "arte" de comprobar una aplicación en ejecución remota, sin saber el funcionamiento interno de la aplicación, para encontrar vulnerabilidades de seguridad.

En conclusión el proceso del Pentest implica un análisis activo del sistema, de las debilidades, fallas técnicas o vulnerabilidades. Este análisis se realiza desde la posición de un atacante potencial, y puede implicar la explotación activa de vulnerabilidades de seguridad, cualquier problema de seguridad encontrado es presentado al administrador del sistema junto con un análisis de su impacto y una propuesta de solución o mitigación.

V. CICLO DE VIDA DE LA SEGURIDAD EN REDES.

Las organizaciones, empresas u entidades contemplan un ciclo de vida, para poder evaluar la seguridad en la red, a continuación se evidencian tanto sus fases como las actividades en cada una de ellas.[11]

A. Identificación de Posibles amenazas

Es importante determinar el rango de amenazas internas y externas al que está expuesto cada uno de los elementos que hacen parte de la arquitectura de la red, con el fin de minimizar el riesgo de ocurrencia e impacto, para asegurar la confidencialidad, integridad, disponibilidad y autenticidad de los datos, procesos e información que circulan a través de la red de la organización.

Con el fin de dar seguimiento a los problemas encontrados, se diseña un plan de acción, que es la forma como se va a implementar el programa, cuyo inicio invoca normas de buenas prácticas, que abarquen la seguridad de los usuarios, artefactos, recursos, procesos y contenidos de la información de la red, desarrollados a través de políticas de seguridad.

B. Formulación de Políticas de Seguridad.

Una política de seguridad es un conjunto protocolario de controles, normas o procedimientos que deben cumplir los usuarios y aplicaciones, que tienen legalmente acceso a la infraestructura tecnológica de la organización.

La finalidad de una política de seguridad, es comunicar a los usuarios oportunamente las directrices para proteger los recursos de la información, las múltiples plataformas computacionales y los dispositivos que hacen parte de la red.
Es evidente que las políticas de seguridad se deben integrar a los procesos estratégicos de negocio, a los objetivos, a la misión y visión, con el fin de apoyar y participar en la toma de decisiones y proyecciones futuras.

[9] Penetration test, [en línea].Wikipedia ,<http://en.wikipedia.org/wiki/Penetration_Testing>

[10] Computer Security Division - Computer Security Resource Center, [en línea].NIST, <http://csrc.nist.gov/publications/PubsSPs.html>

[11] Seguridad Informática en redes de computadoras, [en línea]. <http://www.slideshare.net/wbarriosb/seguridad-informtica-en-redes-de-computadores/>

La creación de políticas requiere del esfuerzo y compromiso de toda la organización, algunos temas para definir políticas de seguridad se sitúan en:

- Política de manejo de la red.
- Política de conexión remota.
- Política de acceso a Internet.
- Política de Incidentes.
- Política de acceso físico.
- Política de acceso mail.
- Política de autenticación de usuarios.
- Política de protocolos de servicios.

C. Manejo y Gestión de Incidentes.

La gestión de incidentes de seguridad se encarga de ofrecer una guía que le indica al departamento de TI, como presentar y documentar los procedimientos correspondientes al descubrimiento de vulnerabilidades, incidentes y amenazas de seguridad, al igual que las alertas emitidas, los controles configurados y los resultados producto de las valoraciones individuales.

El no mantener segura la información a través de la aplicación de una norma para la Gestión de incidentes, eleva la probabilidad de ser víctima de intrusión en la arquitectura de red, dispositivos, recursos y sistemas computacionales a los que la red de la entidad tiene acceso.

La aplicación eficaz y respuesta inmediata de estas medidas a incidentes de seguridad de la información, permite que las entidades públicas puedan responder y gestionar variedad de controles y técnicas, ante una violación de seguridad, al igual que la presentación de estadísticas de intentos de intrusión a la misma.

Un buen desarrollo de software que apoyaría al departamento de TI, estaría enmarcado en una solución tecnológica por módulos del "Diseño e implementación de la herramienta para la Seguridad de la Información y Gestión de Incidentes ISO / IEC 27035:2011"

VI. ANALISIS DE VULNERABILIDADES

El análisis de vulnerabilidades tiene muchas cosas en común con la evaluación de riesgos. De acuerdo a las mejores prácticas el proceso de Análisis de vulnerabilidades consiste de los siguientes pasos:

1. Descubrimiento: Descubrimiento de todos los activos de la red e identificación los detalles de cada elemento, incluyendo el sistema operativo y los servicios abiertos.

2. Priorización de los activos: Administrar la red, clasificando los activos en grupos o unidades de negocio. (Catalogación de recursos y capacidades (recursos) en un sistema.)

Asignar un valor cuantificable y la importancia de los recursos, en función de la criticidad para la operación la entidad.

3. Evaluación: Determinar un perfil de riesgo de referencia que le permita enfocarse en la eliminación de los riesgos con base en la criticidad de los activos. Identificación de las vulnerabilidades o amenazas potenciales a cada recurso.

4. Informe: Consiste en medir el nivel de riesgo de la entidad, asociado con los activos de acuerdo a sus políticas de seguridad. Presentar un informe que permita Mitigar o eliminar las vulnerabilidades más graves para los recursos más valiosos.

Dentro de los tipos de Análisis de Vulnerabilidades se pueden enumerar los siguientes:

A. Análisis de Vulnerabilidades Interno

Se trata de pruebas de penetración desde la Red Interna que identifican los riesgos de las redes y sistemas internos, demostrando lo que podría hacer un usuario que ha ganado acceso a la red, simulando ser un usuario interno malintencionado, muchos de los estudios realizados sobre la seguridad de la información demuestran que varias de las violaciones de seguridad se originan desde usuarios internos.

B. Análisis de Vulnerabilidades Externo

Se trata de pruebas de penetración desde Internet que identifiquen los riesgos de la red perimetral y analizen si estos pueden ser utilizados para acceder a la red de una entidad, violando sus medidas de seguridad, y en tal caso examinar si se produce el debido registro de lo que está sucediendo y si se accionan o no las alertas apropiadas, verificando la efectividad de los firewalls, de los sistemas de detección de intrusos (IDS), de los sistemas

operativos y de los dispositivos de comunicaciones visibles desde Internet.

C. Análisis de Vulnerabilidades de Aplicaciones Web

Identifica los riesgos de las Aplicaciones Web, verificando los esquemas de autenticación y testeando las tecnologías utilizadas en la implementación de las mismas.[12]

Los Análisis de Vulnerabilidades deben efectuarse periódicamente, pues a diario se descubren Nuevas Vulnerabilidades debido a su carácter evolutivo.

VII. TIPOS DE VULNERABILIDADES

Las vulnerabilidades, nacieron a la par de la invención del pc y con el paso de tiempo se ha vuelto más crítico su control y eliminación. Dichos problemas a los que se expone una red, activos, usuarios y recursos de información son muy elevados por lo que no se puede garantizar la protección total de la misma. El incremento de los incidentes de seguridad, grupos de hackers, la propagación de nuevas técnicas de intrusión y software malicioso, nos evidencia que el conocimiento no es suficiente y que la tecnología es una aliada de los casos donde ya se ha tenido éxito en accesos no autorizados.

Las vulnerabilidades se clasifican en[13]:

Vulnerabilidad Física: Se define como la entrada material a un lugar no autorizado (Centro de redes, sistemas, Departamento de TI), para alterar o sustraer información.
Vulnerabilidad natural: Es el nivel con que puede verse comprometido un sistema por incidentes naturales y/o ambientales.
Vulnerabilidad del hardware y del software: Dado el avance tecnológico que han tenido las arquitecturas de Hardware y de software, algunos dispositivos se hacen menos fiables que otros, al igual que los fallos en los sistemas operativos son evidentes garantizando el acceso a los mismos.
Vulnerabilidad de los medios de almacenamiento: Es la probabilidad de destruir, plagiar, hurtar información contenida en unidades o bodegas de depósito.
Vulnerabilidad por Irradiación: Son las ondas electromagnéticas que se derivan de dispositivos electrónicos y que quedan en el ambiente, que al ser interceptadas y descifradas se puede deducir la información contenida.
Vulnerabilidad de las comunicaciones: Esta debilidad es la principal preocupación de la seguridad de las arquitecturas de redes, puesto que al aumentar la interconexión de PCs, los servicios, aplicaciones y usuarios se eleva la posibilidad de penetrar, interceptar, modificar y robar los datos que han sido transmitidos.
Vulnerabilidad humana: Se ha comprobado que el riesgo más alto para la seguridad de la red, en especial para la información que se envía a través de esta son los usuarios, siendo uno de los problemas más difíciles de controlar en una organización.

Es importante resaltar que dentro del proceso para vulnerar la infraestructura informática de una organización existen diferentes métodos y combinaciones para su ejecución, que se pueden resumir en las siguientes actividades, estas hacen parte de las etapas típicas de un ataque:
Planeación y elección del objetivo a atacar: Obtención de información que puede ser desde dentro o fuera de la organización o a través de técnicas de ingeniería social.
Búsqueda y exploración de vulnerabilidades, aprovechando alguna debilidad en el objetivo a atacar.
Ataque e Intrusión: Identificación de puertas traseras que aseguran el control posterior y por último la eliminación de huellas con el fin de eliminar el rastro del ataque.

En cuanto a los medios y herramientas disponibles en la actualidad para llevar a cabo las pruebas de penetración, se pueden citar las siguientes[14]:

Sniffer: Programa de registro y captura de tramas de red, tiene como fin monitorear redes para detectar y analizar fallos, o para realizar ingeniería inversa en protocolos, permitiendo rastrear la actividad realizada en un determinado computador, sin embargo en ocasiones es

[12] Alt 126 - Análisis de Vulnerabilidades, [en línea].<http://www.alt126.com/secciones.aspx?IdSection=18&IdSubSection=80&IdChildSection=114>

[13] Introducción a la Protección y Seguridad de la Información, [en línea]. <http://alarcos.inf-cr.uclm.es/doc/PSI/tema1Marian.pdf >

[14] Hacking, [en línea]. usbseguridad.files.wordpress.com/2012/05/hacking.pptx>

utilizado para fines maliciosos, como robar contraseñas, interceptar correos electrónicos, espiar conversaciones entre otros.

Escáneres de puertos: Permiten detectar, comprobar y analizar los estados de los puertos en un determinado sistema informático y posibles vulnerabilidades de seguridad según los puertos abiertos. Es usado por administradores de sistemas para analizar posibles problemas de seguridad, sin embargo en ocasiones es utilizado por individuos malintencionados que intentan comprometer la seguridad de la máquina o la red.

Exploits: Son segmentos de código, o secuencias de comandos que tienen como fin explotar vulnerabilidades o causar un error o un fallo en alguna aplicación, y ocasionar un comportamiento no deseado en software y hardware.

Existen diferentes metodologías, y guías de pruebas para realizar un análisis de vulnerabilidades y un test de penetración, enfocadas a la auditoria de aplicaciones, redes, procesos, comunicaciones, información entre otros, que abarcan los aspectos de seguridad que se deben contemplar para obtener un diagnostico lo más completo posible, permitiendo verificar todas las acciones que aseguren el cumplimiento regulatorio, el cumplimiento legal y el cumplimiento de las políticas de seguridad de la entidad.

VIII. OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM):

Metodología abierta de comprobación para la seguridad, donde cualquier individuo puede, estudiar, ampliar, sugerir y contribuir, y donde las críticas constructivas continuarán ayudando a su desarrollo y evolución. Esta metodología constituye uno de los estándares profesionales más completos y comúnmente utilizados en Auditorías para revisar la Seguridad de los Sistemas[15], el objetivo de esta metodología es crear un método para ejecutar un test de seguridad minucioso y completo que permita de manera óptima llevar a cabo serie de pasos, durante la realización de un test exhaustivo, sin que sea restrictiva en la manera que obligue a seguir la metodología como si se tratase de un diagrama de flujo, lo que resulta realmente valioso, ya que los diferentes tests son evaluados y ejecutados donde sean aplicables, hasta conseguir los resultados esperados dentro de un período de tiempo determinado.

El ámbito de aplicación de esta metodología define un conjunto de reglas y lineamientos para identificar "cuando, que y cuales" eventos son evaluados desde un entorno no privilegiado hacia un nivel alto privilegiado sin protección, a través de la evasión de componentes de seguridad, procesos y alarmas, con el fin de ganar acceso.
Este Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM 2.1 provee un procedimiento estandarizado para realizar una exhaustiva revisión y evaluación de seguridad de cada elemento con presencia de seguridad dividido por secciones:

OWASP: Open Web Application Security Project (Proyecto Abierto de Seguridad de Aplicaciones Web): comunidad abierta dedicada a permitir a las organizaciones realizar el desarrollo, adquisición y mantenimiento de aplicaciones fiables.

Todas las herramientas, documentos, foros y representaciones del OWASP son libres y abiertos a cualquier interesado en mejorar la seguridad de las aplicaciones. OWASP se centra exclusivamente en tests de intrusión para aplicaciones web, proporcionando un exhaustivo catálogo de controles de seguridad a revisar en toda aplicación web, a través de indicaciones sobre procedimientos y herramientas para probar la seguridad.

IX. HACKING ÉTICO

Esta práctica consiste en la penetración a sistemas Informaticos de una organización de la misma forma que lo haría un Hacker o Ciber delincuente solo que de forma autorizada y controlada. Como resultado de esta actividad se desprende un informe en el cual se identifican las vulnerabilidades de los sistemas a los cuales se ha logrado acceder y que información sensible fue expuesta.

[15] Metodología Abierta De Testeo De Seguridad, [en línea]. http://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml>

Procedimiento para un Hacking Ético:

La EC-Council ha provisto una metodología en su certificación C|EH (Certifield Ethical Hacker) que lista los siguientes elementos:

1. Reconocimiento: Hace referencia a la recopilación inicial de toda la información posible acerca del objetivo, con el fin de identificar posibles vectores de ataque.
2. Escaneo: Tiene que ver con la Identificación de equipos, servicios y puertos en la red objetivo y sus posibles vulnerabilidades, adicional a esto se puede extraer nombres de usuarios, nombres de máquinas, recursos compartidos, servicios del sistema y contraseñas.
3. Obtención de Acceso: Es la entrada a un sistema haciendo uso de diversas tecnologías ofensivas entre las que están los virus, troyanos, exploits, botnets, entre otros. Una vez dentro de la red se escalan privilegios hasta alcanzar permisos elevados.
4. Mantenimiento de acceso: En este paso se realiza la instalación de rootkits, troyanos, backdoors, keyloggers y algunas otras herramientas que permitan mantener el acceso fácil y continuo a la red.
5. Borrado de evidencias: Por último se elimina cualquier rastro del ataque a través de la manipulación de logs, quitando programas implantados y algunas otras técnicas que evitan al máximo el rastreo de intrusión.

Se tienen también algunos tipos de pruebas de Hacking Ético dependiendo del tipo de solicitud realizada por el cliente, entre estos están:
Hacking Ético de Caja Blanca: Facilita información por parte del cliente para realizar la intrusión, se realiza un análisis en profundidad de las brechas de seguridad de los sistemas sometidos a estudio.
Hacking Ético de Caja Negra: El cliente no facilita información para realizar la intrusión, se realiza un análisis en profundidad y extensión de las brechas de seguridad de los sistemas sometidos a estudio.[16]

X. CONCLUSIONES

El éxito de la definición de un buen esquema de seguridad, se centra en la planeación y directrices que se hayan establecido, para notificar los hallazgos inusuales, y en la rapidez para determinar y evaluar los riesgos, mediante el análisis, gestión y solución oportuna de los incidentes, de igual forma incorporando auditorias eventuales, cuyas resultados permitan verificar y validar la emisión de alertas de seguridad.
Las organizaciones deben invertir en programas de capacitación del personal, en temas actualizados de tecnologías, políticas de seguridad, métodos de autenticación, configuración de dispositivos, criptografía, gestión, detección, protocolos y demás áreas a fines, apoyadas y concientizadas previamente por los directivos, involucrando un compromiso integral, con la apropiación de "Seguridad Informática", no solo como mecanismos de defensa en la arquitectura de red, sino también como un componente estratégico en todos los procesos, para el cumplimiento de los objetivos de la entidad.

REFERENCIAS

[1] CCN-Cert, "Confidencialidad," [en línea]. Disponible: <https://www.ccn-cert.cni.es/publico/serieCCN-STIC401/es/c/confidentiality.htm> (2013, Marzo 28).

[2] Antonio Villalón Huerta, El Sistema de Gestión de Seguridad de la Información "la nueva norma UNE 71502", [en línea]. Disponible: <http://www.shutdown.es/ISO17799.pdf> (2013, Marzo 28).

[3] Introducción a la Seguridad Informática. Conceptos Básicos- La Seguridad informática en números, [en línea]. Disponible: <http://seginfo.tripod.com/files/17799a.pdf> (2013, Marzo 30).

[4] Grupo Alarcos, Escuela Superior de Informática de Ciudad Real, Introducción a la Protección y Seguridad de la Información, [en línea]. Disponible: <http://alarcos.inf-cr.uclm.es/doc/PSI/tema1Marian.pdf> (2013, Marzo 30).

[5] La revista SIC, Diseño de Protocolos de No-Repudio, [en línea]. Disponible: <http://revistasic.com/revista38/pdf_38/SIC_38_1agora.PDF> (2013, Marzo 30).

[6] Seguridad en Redes, [en línea]. Disponible: <http://www.slideshare.net/tec37045/seguridad-en-redes-ii> (2013, Marzo 30).

[7] Introducción a la Protección y Seguridad de la Información, [en línea].

[16] (http://www.eccouncil.org/)

[8] Seguridad Física, [en línea].< http://www.slideshare.net/tecnodelainfo/seguridad-fsica> [Online]. (2013, Marzo 28).

[9] Penetration test, [en línea].Wikipedia,<http://en.wikipedia.org/wiki/Penetration_Testing>[Online]. (2013, Marzo 30).

[10] Computer Security Division - Computer Security Resource Center, [en línea].NIST, Disponible: <http://csrc.nist.gov/publications/PubsSPs.html> [Online]. (2013, Marzo 30).

[11] Seguridad Informática en redes de computadoras, [en línea]. Disponible: <http://www.slideshare.net/wbarriosb/seguridad-informtica-en-redes-de-computadores/> [Online]. (2013, Marzo 31).

[12] Alt 126 - Análisis de Vulnerabilidades, [en línea]. Disponible: <http://www.alt126.com/secciones.aspx?IdSection=18&IdSubSection=80&IdChildSection=114> [Online]. (2013, Marzo 31).

[13] Introducción a la Protección y Seguridad de la Información, [en línea]. Disponible: <http://alarcos.inf-cr.uclm.es/doc/PSI/tema1Marian.pdf > (2013, Marzo 31).

[14] Hacking, [en línea]. Disponible: <usbseguridad.files.wordpress.com/2012/05/hacking.pptx > (2013, Abril 7).

[15] Metodología Abierta De Testeo De Seguridad, [en línea]. Disponible: <http://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml> (2013, Abril 7).

[16] <http://www.eccouncil.org/> [Online]. (2013, Abril 10).

Autores

Erika Lucia Rangel Palencia
Ingeniera de Sistemas, Estudiante Especialización Informática, Cursante del Diplomado en Gestión en Seguridad de la Información.
Actualmente trabaja en: Archivo General de la Nación.

Julian Andres Sotto Bastidas
Ingeniero de sistemas, Cursante de la Especialización en Seguridad Informatica, Cursante del Diplomado en Gestión en Seguridad de la Información.
Actualmente trabaja en: Fiscalia General de la Nación.